

Министерство науки и высшего образования Российской Федерации

**Федеральное учебно-методическое объединение
в системе высшего образования
по УГСНП 10.00.00 «Информационная безопасность»**

Институт криптографии, связи и информатики Академии ФСБ России

Кубанский государственный технологический университет



**МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ
XXII ПЛЕНУМА ФУМО ВО ИБ**

**СБОРНИК МЕТОДИЧЕСКИХ УКАЗАНИЙ
ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ
ПО ДИСЦИПЛИНАМ БАКАЛАВРИАТА
И СПЕЦИАЛИТЕТА
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Краснодар
2018

УДК 004.45
ББК 32.972.5
М54

Составители:

Белов Е.Б., Бердник М.В., Зангиев Т.Т.

Ответственный за выпуск – Частикова В.А.

- М54 **Методические материалы XXII Пленума ФУМО ВО ИБ. Сборник методических указаний по выполнению лабораторных работ по дисциплинам бакалавриата и специалитета в области информационной безопасности (Краснодар, 2–7 октября 2018 г.) / Сост.: Е.Б. Белов, М.В. Бердник, Т.Т. Зангиев; Отв. за выпуск: В.А. Частикова; Федеральное учебно-методическое объединение в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность»; Институт криптографии, связи и информатики Академии ФСБ России; Кубанский государственный технологический университет. – Краснодар : Издательский Дом – Юг, 2018. – 314 с.**

Сборник содержит методические указания по выполнению лабораторных работ по дисциплинам бакалавриата и специалитета в области информационной безопасности. Методические указания включают: требования к результатам обучения основной образовательной программы, перечень материально-технического обеспечения, задания на исследование, краткие теоретические сведения, порядок выполнения лабораторных работ и контрольные вопросы.

ФУМО ВО ИБ выражает свою признательность всем научно-педагогическим коллективам образовательных организаций, принявшим непосредственное участие в составлении данного сборника.

Особую благодарность выражаем Кубанскому государственному технологическому университету.

ББК 32.972.5
УДК 004.45

- © Коллектив составителей, 2018
- © Федеральное учебно-методическое объединение в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность», 2018
- © Институт криптографии, связи и информатики Академии ФСБ России, 2018
- © Кубанский государственный технологический университет, 2018
- © Оформление ООО «Издательский Дом – Юг», 2018

Содержание

Бакалавриат 10.03.01 Информационная безопасность	4
Дисциплина: Защита программ и данных	4
Дисциплина: Криптографические методы защиты информации	13
Дисциплина: Методы оценки безопасности компьютерных систем	26
Дисциплина: Моделирование процессов и систем защиты информации	34
Дисциплина: Программно-аппаратные средства защиты информации	36
Дисциплина: Сети и системы передачи информации	59
Дисциплина: Современные компьютерные полиграфные системы	66
Дисциплина: Техническая защита информации	68
Дисциплина: Физические основы защиты информации	85
Специалитет 10.05.01 Компьютерная безопасность	99
Дисциплина: Анализ программных реализаций	99
Дисциплина: Аппаратная реализация криптоалгоритмов	103
Дисциплина: Защита компьютерных систем	106
Дисциплина: Защита программ и данных	109
Дисциплина: Криптографические методы защиты информации	111
Дисциплина: Модели безопасности компьютерных систем	114
Специалитет 10.05.02 Информационная безопасность телекоммуникационных систем	121
Дисциплина: Защита информации в компьютерных сетях	121
Дисциплина: Оптические телекоммуникационные системы и сети	125
Дисциплина: Проектирование защищенных телекоммуникационных систем	133
Дисциплина: Сети и системы передачи информации	138
Дисциплина: Техническая защита информации	174
Специалитет 10.05.03 Информационная безопасность автоматизированных систем	187
Дисциплина: Безопасность систем баз данных	187
Дисциплина: Криптографические методы защиты информации	191
Дисциплина: Криптографические протоколы	201
Дисциплина: Обеспечение доверия к информационной безопасности автоматизированных систем	222
Дисциплина: Программно-аппаратные средства защиты информации	226
Дисциплина: Системы радиомониторинга	244
Дисциплина: Техническая защита информации	248
Дисциплина: Технические средства охраны объектов	267
Дисциплина: Управление средствами защиты информации	272
Дисциплина: Управление информационной безопасностью	275
Дисциплина: Языки программирования	279
Специалитет 10.05.04 Информационно-аналитические системы безопасности	283
Дисциплина: Безопасность операционных систем	283
Дисциплина: Управление информационной безопасностью	288
Специалитет 10.05.05 Безопасность информационных технологий в правоохранительной сфере	296
Дисциплина: Техническая защита информации	296
Специалитет 10.05.07 Противодействие техническим разведкам	306
Дисциплина: Защита информации от несанкционированного доступа	306
Дисциплина: Информационно-телекоммуникационные системы	309

БАКАЛАВРИАТ 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Дисциплина: Защита программ и данных

Образовательная программа: 10.03.01. Информационная безопасность, Безопасность компьютерных систем, Информационная безопасность объектов информатизации на базе компьютерных систем, Безопасность открытых информационных систем.

Дисциплина: Защита программ и данных.

Лабораторная работа.

Исследование программы, защищённой от дизассемблирования

1. Учебные цели:

Изучить на практике ряд основных антиотладочных методов

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

- Уметь проводить дизассемблирование элементарных программ, защищённых от дизассемблирования.
- Владеть методами и инструментами для дизассемблирования программ.

3. Перечень материально-технического обеспечения

Программный продукт IDAPro

4. Задание на исследование:

- Дизассемблировать программу «hello2.exe» с помощью IDAPro;
- Следуя порядку выполнения лабораторной работы определить точку входа в программу, тело программы, точку покидания программы.

5. Краткие теоретические сведения

Краткие теоретические сведения приведены в сборнике методических указаний «Защита программ и данных. Теория и практика»

6. Порядок выполнения лабораторной работы

Запустите «hello2.exe» и посмотрите, что делает эта программа. Появится главное окно (см. рис. 1).



Рис. 1. Главное окно программы

После нажатия на кнопку «Ок» приложение будет завершено. Программа имеет весьма незамысловатый функционал. Её главная особенность – в приложении используются методы для затруднения дизассемблирования и исследования приложения.

Дизассемблируйте файл «hello2.exe» с помощью IDAPro. После разбора программы управление будет передано на точку входа по адресу 401000 (см. рис. 2).

```
CODE:00401000      public start
CODE:00401000 start  proc near
CODE:00401000      push  offset loc_40101F
CODE:00401005      mov   edi, 401030
CODE:0040100A      add   edi, 500h
CODE:00401010      add   edi, 0000h
CODE:00401016      jmp  edi
CODE:00401016 start  endp
CODE:00401016      ;-----
CODE:00401018      ;----- dd 40EBDE75h
CODE:0040101C      ;-----
CODE:0040101C      push  ebp
CODE:0040101D      cwd  edi
CODE:0040101E      stc
```

Рис. 2. Точка входа в программу, демонстрация косвенного перехода

Точка входа отличается от стандартной, созданной компилятором. Из рисунка 2 видно, что после осмысленного кода, начиная с адреса «401018», идёт «мусор», который IDA не смогла правильно обработать. Это может быть исполняемый код, могут быть данные приложения, могут быть просто ненужные инструкции, необходимые для усложнения анализа программы.

Косвенный переход. Определим, что делает приложение по адресам 401000-401016. Инструкция «pushoffsetloc_40101F» сохраняет в стеке адрес 40101F. Далее, идёт набор инструкций, изменяющих значение регистра EDI и инструкция перехода по новому значению, находящемуся в регистре EDI. Сделано это для того, чтобы исследователь не смог сразу определить, куда будет передано управление. Чем больше и сложнее инструкции работы с регистром, тем труднее будет вычислить верное значение адреса перехода. В нашем случае адрес перехода вычисляется следующим образом: $400043h + 500h + 0B00h = 401043h$. Следовательно, по адресу 401016 инструкция «jmpedi» передаст управление по адресу 401043. Посмотрим, что находится по этому адресу, – «Мусорные» инструкции. Для перехода по адресу 401043 нажмите клавишу «G». В появившемся окне введите адрес перехода 401043 и нажмите «Ok». Из рисунка 3 видно, что дизассемблер не смог определить правильный адрес перехода, и не смог дизассемблировать оставшуюся часть программы.

```

CODE:00401032      loop    loc_401029
CODE:00401034      mov     esi, offset unk_402000
CODE:00401039      jmp     esi
CODE:00401039 ; -----
CODE:0040103B      db 75h
CODE:0040103C      dd 4B01EBDEh, 6AF99855h, 0EE840h, 44490000h, 78452041h
CODE:0040103D      dd 6C706D61h, 322065h, 10E8h, 6C654800h, 57206F6Ch, 646C726Fh
CODE:0040103E      dd 0FF000021h, 0BE006A25h
CODE:0040103F      dd ██████████
CODE:00401074 ; -----

```

Рис. 3. Неудачная попытка дизассемблирования

IDA интерпретировала набор байтов с адреса 40103B по 401070 как данные приложения, хотя, на самом деле это код, на который передаётся управление (как мы уже выяснили). Чтобы снять формат данных, неверно выставленный IDA, выделите мышью блок с адреса 40103B по 401070 и нажмите клавишу «U». В появившемся окне подтверждения выберите «Yes». Результат действий показан на рисунке 4.

```

CODE:00401032      loop    loc_401029
CODE:00401034      mov     esi, offset unk_402000
CODE:00401039      jmp     esi
CODE:00401039 ; -----
CODE:0040103B      db 75h ; u
CODE:0040103C      db 0DEh ; i
CODE:0040103D      db 0EBh ; m
CODE:0040103E      db 1
CODE:0040103F      db 48h ; K
CODE:00401040      db 55h ; U
CODE:00401041      db 98h ; W
CODE:00401042      db 0F9h ; *
CODE:00401043      db 6Ah ; j
CODE:00401044      db 40h ; @
CODE:00401045      db 0E8h ; w

```

Рис. 4. Изменение формата данных в IDA

В начале исследования мы выяснили, что программа первоначально передаёт управление по адресу 401043, поэтому с этого адреса должен начинаться код. Кликните мышью по адресу 401043 и нажмите клавишу «C» для дизассемблирования с этого адреса. Результат показан на рисунке 5.

```

CODE:00401032      loop    loc_401029
CODE:00401034      mov     esi, offset unk_402000
CODE:00401039      jmp     esi
CODE:00401039 ; -----
CODE:0040103B      db 75h ; u
CODE:0040103C      db 0DEh ; i
CODE:0040103D      db 0EBh ; m
CODE:0040103E      db 1
CODE:0040103F      db 48h ; K
CODE:00401040      db 55h ; U
CODE:00401041      db 98h ; W
CODE:00401042      db 0F9h ; *
CODE:00401043 ; -----
CODE:00401043      push   40h
CODE:00401045      call   near ptr unk_401058
CODE:0040104A      dec    ecx
CODE:0040104B      inc    esp
CODE:0040104C      inc    ecx
CODE:0040104D      and    [ebp+78h], al

```

Рис. 5. Использование «мусорных» инструкций

Из листинга видно, что с адреса 40103B расположены 8 мусорных байт, из-за которых IDA не смогла корректно выполнить дизассемблирование приложения.

Неявная передача параметров и вызов функций. Приложение продолжает выполняться с адреса 401043. В стек заносится число «40h», дальше происходит вызов функции по адресу 401058. Из рисунка 3 видно, что дизассемблер и здесь не смог правильно дизассемблировать приложение, так как переход по адресу 401058 попадает на середину инструкции «addal, ch». Кликните мышью по следующему за инструкцией «call» адресу (40104A) и нажмите «U» (см. рис. 6). Видно, что сразу за инструкцией «call» по адресу 401045 идёт текст «IDAExample 2» (c-string, заканчивающаяся нулевым байтом). Кликните по адресу 40104A и нажмите «A», чтобы преобразовать набор байтов в ASCII-строку.

```

CODE:00401041          db  98h ; Ⅱ
CODE:00401042          db 0F9h ; *
CODE:00401043 ; -----
CODE:00401043          push  40h
CODE:00401045          call  near ptr unk_401058
CODE:0040104A          dec   ecx
CODE:0040104B          inc   esp
CODE:0040104C          inc   ecx
CODE:0040104D          and   [ebp+78h], al
CODE:00401050          popa
CODE:00401051          ins   dword ptr es:[edi], dx
CODE:00401052          jjo   short near ptr dword_40108C+34h
CODE:00401054          and   gs:[edx], dh
CODE:00401057          add   al, ch ; CODE XREF: CODE:00401045↑p
CODE:00401059          adc   [eax], al
CODE:0040105B          db   0
CODE:0040105C          db   0

```

Рис. 6. Неявный переход

Чтобы дальше дизассемблировать программу, кликните по адресу 401058 и нажмите «C». С адреса 401058 идёт такой же приём противодействия дизассемблеру – инструкция «call», а за ней набор неправильно определённых инструкций.

```

CODE:00401041          db  98h ; Ⅱ
CODE:00401042          db 0F9h ; *
CODE:00401043 ; -----
CODE:00401043          push  40h
CODE:00401045          call  near ptr unk_401058
CODE:00401045 ; -----
CODE:0040104A          db  49h ; I
CODE:0040104B          db  44h ; D
CODE:0040104C          db  41h ; A
CODE:0040104D          db  20h
CODE:0040104E          db  45h ; E
CODE:0040104F          db  78h ; x
CODE:00401050          db  61h ; a
CODE:00401051          db  60h ; m
CODE:00401052          db  70h ; p
CODE:00401053          db  6Ch ; l
CODE:00401054          db  65h ; e
CODE:00401055          db  20h
CODE:00401056          db  32h ; 2
CODE:00401057          db   0
CODE:00401058          unk_401058 db 0E8h ; Ⅱ ; CODE XREF: CODE:00401045↑p
CODE:00401059          db  10h

```

Рис. 7. Недизассемблированный участок кода

Кликните по адресу 40105D и нажмите «U», а затем «A». Так как по адресу 401058 расположена инструкция «call 40106D», то продолжать дизассемблировать приложение нужно именно с адреса 40106D. Кликните по адресу мышкой и нажмите «C» (см. рис. 8).

```

CODE:00401043          push  40h
CODE:00401045          call  loc_401058
CODE:00401045 ; -----
CODE:0040104A          aIdaExample2 db 'IDA Example 2',0
CODE:00401058 ; -----
CODE:00401058          loc_401058: call  loc_40106D ; CODE XREF: CODE:00401045↑p
CODE:00401058 ; -----
CODE:0040105D          aHelloWorld db 'Hello World!',0
CODE:0040106A          db   0
CODE:0040106B          db 0FFh
CODE:0040106C          db  25h ; %
CODE:0040106D ; -----
CODE:0040106D          loc_40106D: ; CODE XREF: CODE:loc_401058↑p
CODE:0040106D          push  0
CODE:0040106F          mov   esi, ██████████
CODE:00401074          inc   esi
CODE:00401075          add   esi, 0FFFh
CODE:00401078          call  esi
CODE:0040107D          retn

```

Рис. 8. Ещё одна попытка запутать исследователя

Из листинга видно, что в данном фрагменте программы выполняется неявная передача параметров в какую-то функцию. Сам вызов функции тоже происходит неявно, через манипуляции со значениями регистра ESI (по адресам 40106F-401075) и выполнением инструкции «callesi». Новый адрес перехода вычисляется следующим образом: $400080h + 1 + 0FFFh = 401080h$.

Посмотрите, куда будет передано дальнейшее управление – для этого кликните по адресу 40107E, нажмите «U», а затем нажмите «C» с адреса 401080h (см. рис. 9).

```

CODE:0040107B          call    esi
CODE:0040107D          retn
CODE:0040107D ; -----
CODE:0040107E          db     0FFh
CODE:0040107F          db     25h ; %
CODE:00401080 ; -----
CODE:00401080          jmp     ds:MessageBoxA
CODE:00401080 ; -----
CODE:00401086          db     0FFh
CODE:00401087          db     25h ; %

```

Рис. 9. Вызов функции MessageBoxA

Это вызов функции MessageBoxA. Вернёмся к рисунку 8, чтобы определить, какие параметры передаются в эту функцию.

Первый параметр передаётся по адресу 401043 инструкцией «push 40h». Обратите внимание на инструкции «call» по адресам 401045 и 401058. Как известно, команда «call» используется для вызова процедур, но здесь она используется для других целей. При выполнении этой инструкции, процессор помещает значение регистра EIP, соответствующее следующей за «call» команде, в стек и загружает в EIP новое значение, осуществляя тем самым передачу управления. Из рисунка 8 видно, что инструкции «call» по адресам 401045 и 401058 используются для сохранения в стеке адресов текстовых строк и одновременно для нарушения работы дизассемблера, который будет считать эти строки кодом и будет пытаться дизассемблировать этот код.

По адресу 40106D в стек сохраняется последний параметр для функции MessageBox, вызов которой происходит по адресу 40107B инструкцией «callesi».

Динамическое расшифровывание и выполнение кода. Возникает вопрос: куда будет передано управление дальше? По адресу 40107D инструкция «getn» (см. рис. 9) передаст управление на адрес, находящийся в данный момент в стеке. Что это за адрес? Обратите внимание на инструкцию «pushoffset loc_40101F» по адресу 401000 (см. рис. 8). Эта инструкция и поместила адрес возврата для инструкции «getn» по адресу 40107D. Перейдите по адресу 40101F для дальнейшего исследования программы (см. рис. 10).

Из листинга видно, что по адресам 40101F-401032 происходит расшифровка куска кода, на который по адресу 401039 осуществляется переход. Расшифровка осуществляется с помощью инструкции XOR по значению «0FAFAFAFAh».

```

CODE:0040101D          cwde
CODE:0040101E          stc
CODE:0040101F
CODE:0040101F loc_40101F:          ; DATA XREF: startfo
CODE:0040101F          mov     ecx, 4
CODE:00401024          mov     esi, offset unk_402000
CODE:00401029
CODE:00401029 loc_401029:          ; CODE XREF: CODE:00401032↓j
CODE:00401029          xor     dword ptr [esi], 0FAFAFAFAh
CODE:0040102F          add     esi, 4
CODE:00401032          loop   loc_401029
CODE:00401034          mov     esi, offset unk_402000
CODE:00401039          jmp     esi
CODE:00401039 ; -----
CODE:0040103B          db     75h ; u
CODE:0040103C          db     0DEh ; !

```

Рис. 10. Расшифровка тела программы

Шифрование кода с последующей его расшифровкой перед выполнением является лучшим методом противодействия дизассемблированию. На рисунке 11 показан кусок зашифрованного кода, дизассемблировать который абсолютно бесполезно.

В IDA есть несколько возможностей для исследования зашифрованного кода:

- написать специальный скрипт для расшифровки кода;
- использовать встроенный в IDA отладчик для исследования программы, которая при выполнении сама себя расшифрует.

Напишем скрипт для расшифровки нужного нам участка программы. Написание скрипта расшифровки участка программы. Откройте окно скриптового языка IDA нажатием комбинации клавиш «Shift+F2». В появившееся окно введите скрипт (см. рис. 12).

```

DATA:00402000 DATA          segment para public 'DATA' use32
DATA:00402000                assume cs:DATA
DATA:00402000                ;org 402000h
DATA:00402000 unk_402000     db  90h ; P                ; DATA XREF: CODE:00401024fo
DATA:00402000                ; CODE:00401034fo
DATA:00402001                db  0FAh ; -
DATA:00402002                db  45h ; E
DATA:00402003                db  7Fh ; M
DATA:00402004                db  0EAh ; b
DATA:00402005                db  0DAh ; -
DATA:00402006                db  0FAh ; -
DATA:00402007                db  0BDh ; -
DATA:00402008                db  7Bh ; {
DATA:00402009                ..  --- ; {

```

Рис. 11. Зашифрованный код

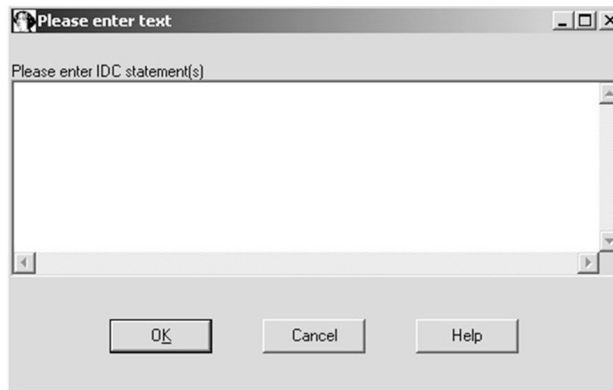


Рис. 12. Встроенный интерпретатор IDAPro

Введите следующий текст скрипта и нажмите «Ок» для его выполнения.

```

1 auto i;
2 for (i =0x402000; i<=40200F;i++){
3 PatchByte(i, Byte(i)^0xFA);
4 }

```

Синтаксис IDA-скриптов похож на синтаксис языка C, с некоторыми отличиями. IDA не позволяет разработчику задавать тип переменных: дизассемблер определяет тип автоматически по её первому использованию. Объявление переменной осуществляется ключевым словом «auto».

Во введённом скрипте была определена одна переменная «i», организован цикл с адреса 402000 по адрес 40200F, и в программе по этим адресам каждого байта вставлялся результат операции «XOR» между текущим байтом и значением «0xFA». После выполнения этого скрипта участок программы по адресу 402000 будет расшифрован. Кликните мышкой по этому адресу и нажмите «С»: вы увидите расшифрованный код (см. рис. 13).

```

DATA:00402000 loc_402000:                ; DATA XREF: CODE:00401024fo
DATA:00402000                ; CODE:00401034fo
DATA:00402000                push    0
DATA:00402002                mov     edi, 201085h
DATA:00402007                inc     edi
DATA:00402008                add     edi, 200000h
DATA:0040200E                push   edi
DATA:0040200F                retn
DATA:0040200F ; -----
DATA:00402010                db     0

```

Рис. 13. Дешифрованный код

По адресу 40200E в стек помещается значение регистра EDI (201085h + 1 + 200000h = 401086h), а затем по адресу 40200F выполняется инструкция «retn». Посмотрим, что находится по адресу возврата 401086 – для этого кликните по адресу 401086 и нажмите «С» (см. рис. 14).

```

CODE:00401080                jmp     ds:MessageBoxA
CODE:00401086 ; -----
CODE:00401086                jmp     |ds:ExitProcess
CODE:00401086 ; -----

```

Рис. 14. Завершение работы программы

Из рисунков 13 и 14 видно, что по адресу 40200F осуществляется вызов функции ExitProcess, которая и завершит выполнение программы. Исследование программы завершено.

7. Контрольные вопросы:

1. Что делает программа «hello2.exe»?
2. Какие конструкции кода используются для усложнения процесса дизассемблирования?
3. Имеет ли смысл проводить дизассемблирование зашифрованных участков кода?
4. Зачем был составлен скрипт на языке IDAPro в данной лабораторной работе?

Время на выполнение лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: ФГАОУ ВО «Сибирский Федеральный Университет», руководитель НУЛ ИБ, Шниперов А.Н. Ashniperov@sfu-kras.ru

Образовательная программа: 10.03.01. Безопасность компьютерных систем, 10.05.01. Информационная безопасность объектов информатизации на базе компьютерных систем, 10.05.03. Безопасность открытых информационных систем.

Дисциплина: Защита программ и данных.

Лабораторная работа. **WinAPI-шпионы**

1. Учебные цели:

- получить навыки использования WinAPI-шпионов;
- подобрать правильный пароль.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

- Уметь проводить дизассемблирование и исследование программ, написанных с использованием WinAPI.
- Владеть методами и инструментами для дизассемблирования и исследования программ.

3. Перечень материально-технического обеспечения

- Программный продукт APIMonitorv2 Alpha-r 13;
- Программный продукт ImmunityDebugger.

4. Задание на исследование:

- Запустить программу «prog9.exe».
- Следуя порядку выполнения лабораторной работы произвести исследование и взлом программы в APIMonitorv2 Alpha-r 13.

5. Краткие теоретические сведения

Краткие теоретические сведения приведены в сборнике методических указаний «Защита программ и данных. Теория и практика»

6. Порядок выполнения лабораторной работы

Запустим «prog9.exe». Появится окно с сообщением о просьбе «чистого» взлома приложения (см. рис. 1).

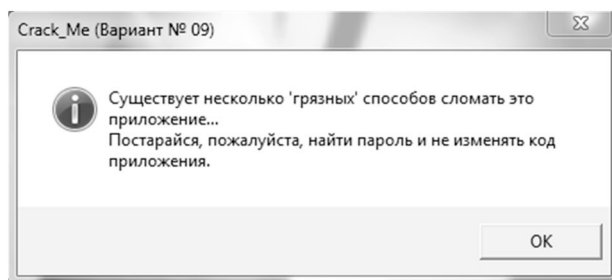


Рис. 1. Просьба «чистого» взлома

А затем главное окно, запрашивающее пароль (см. рис. 2).

Введем произвольный пароль и нажмем кнопку «Check!», программа сообщит, что попытка удачей не удалась (см. рис. 3)

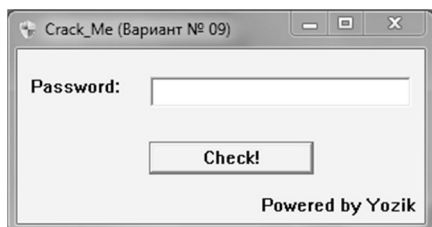


Рис. 2. Главное окно приложения

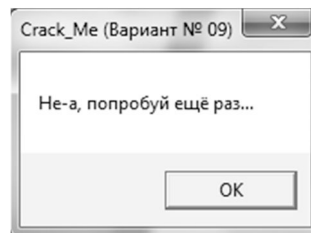


Рис. 3. Констатация неудачной попытки

Для взаимодействия с пользователем программа оперирует пользовательским интерфейсом, который (с большой вероятностью) реализуется при помощи WindowsAPI. С «большой вероятностью», потому что это не единственный метод создания пользовательского интерфейса, но методы, отличные от WinAPI гораздо сложнее для программиста по времени и силам.

Откроем APIMonitor для платформы x86 и в окне RunningProcesses выберем исследуемую программу (см. рис. 4).

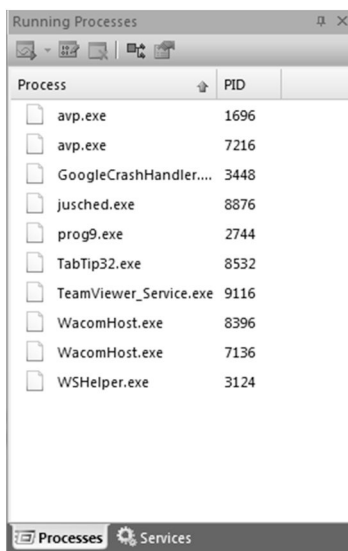


Рис. 4. Выбор процесса для исследования

Прежде чем производить дальнейшие действия, мы должны настроить фильтры API-функций. Возможно, исследуемая программа получает пароль из текстового поля функцией GetWindowTextA(). Проверим это. Для этого необходимо кликнуть на самую верхнюю строку в окне «API Filter», нажать «Ctrl+f» для поиска, ввести имя функции, нажать кнопку «Найти далее» и активировать checkbox рядом с нужной функцией (см. рис. 5).

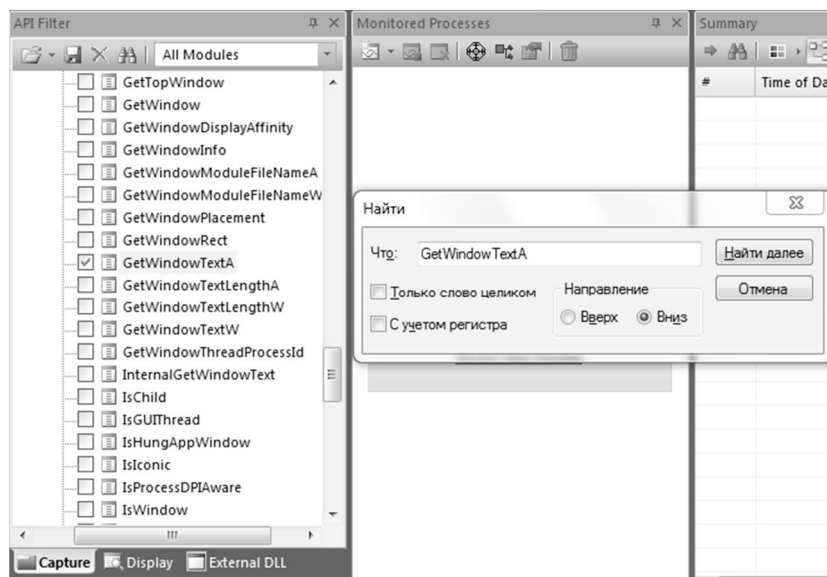


Рис. 5. Выбор отслеживаемых функций

Затем в окне исследуемой программы нажать кнопку «Check!». В итоге в окне «Summary» API Monitor появится строка, фиксирующая обращение к API-функции GetWindowTextA() (см. рис. 6).

#	Time of Day	Thread	Module	API
1	2:08:23.282 PM	1	prog9.exe	GetWindowTextA (0x001504f6, 0x00403128, 17)

Рис. 6. Зафиксированное обращение к WinAPI

При нажатии на неё отобразится адрес вызванной функции в окне «CallStack» (см. рис. 7). Он-то нам и нужен.

#	Module	Address	Offset	Location
1	prog9.exe	0x00401266	0x1266	
2	USER32.dll	0x757a62fa	0x162fa	gapfnScSendMessage + 0x332
3	USER32.dll	0x757a6d3a	0x16d3a	GetThreadDesktop + 0xd7
4	USER32.dll	0x757a6de8	0x16de8	GetThreadDesktop + 0x185
5	USER32.dll	0x757a6e44	0x16e44	GetThreadDesktop + 0x1e1

Рис. 7. Последовательность вызовов

Запишем в блокнот адрес «00401266» и закроем APIMonitor с исследуемой программой.

Далее откроем нашу программу в ImmunityDebugger, нажмем «Ctrl+g» и введем адрес «00401266». Окажемся поблизости от вызова функции GetWindowTextA() (см. рис. 8).

00401261	- E8 F8000000	<JMP.&user32.GetWindowTextA>
00401266	- 68 28314000	PUSH prog9.00403128
0040126B	- E8 4A000000	prog9.004012BA

Рис. 8. Вызов функции GetWindowTextA()

Очевидно, что процедура, вызываемая по адресу «0040126B» (сразу после считывания введенного пользователем текста из поля ввода), является процедурой проверки введенного пароля, перейдем в эту процедуру, установив на нее указатель и нажав «Enter». Увидим следующий код, изображенный на рисунках 9–10.

004012C2	- 8B75 08	MOV ESI,DWORD PTR SS:[EBP+8]	
004012C5	- 33C9	XOR ECX,ECX	
004012C7	- 33C0	XOR EAX,EAX	
004012C9	- 8A46 03	MOV AL,BYTE PTR DS:[ESI+3]	
004012CC	- 2C 30	SUB AL,30	Switch (cases 30..39)
004012CE	- 72 68	SHORT prog9.00401338	
004012D0	- 3C 09	CMP AL,9	
004012D2	- 77 64	SHORT prog9.00401338	
004012D4	- 8A5E 02	MOV BL,BYTE PTR DS:[ESI+2]	Cases 30 ('0'),31 ('1
004012D7	- 80EB 30	SUB BL,30	
004012DA	- 04 FF	ADD AL,0FF	
004012DC	- B2 0A	MOV DL,0A	
004012DE	- F6F2	DIV DL	
004012E0	- 38E3	CMP BL,AH	
004012E2	- 75 01	SHORT prog9.004012E5	
004012E4	- 41	INC ECX	
004012E5	> 33C0	XOR EAX,EAX	
004012E7	- 8A46 03	MOV AL,BYTE PTR DS:[ESI+3]	
004012EA	- 2C 30	SUB AL,30	
004012EC	- 8A5E 01	MOV BL,BYTE PTR DS:[ESI+1]	
004012EF	- 80EB 30	SUB BL,30	
004012F2	- 04 FE	ADD AL,0FE	
004012F4	- B2 0A	MOV DL,0A	
004012F6	- F6F2	DIV DL	
004012F8	- 38E3	CMP BL,AH	
004012FA	- 75 01	SHORT prog9.004012FD	
004012FC	- 41	INC ECX	
004012FD	> 33C0	XOR EAX,EAX	
004012FF	- 8A46 03	MOV AL,BYTE PTR DS:[ESI+3]	
00401302	- 2C 30	SUB AL,30	
00401304	- 8A1E	MOV BL,BYTE PTR DS:[ESI]	

Рис. 9. Функция проверки пароля

00401306	- 80EB 30	SUB BL,30	
00401309	- 04 01	ADD AL,1	
0040130B	- B2 0A	MOV DL,0A	
0040130D	- F6F2	DIU DL	
0040130F	- 38E3	CMP BL,AH	
00401311	- 75 01	SHORT prog9.00401314	
00401313	- 41	INC ECX	
00401314	> 33C0	XOR EAX,EAX	
00401316	- 8A46 03	MOV AL,BYTE PTR DS:[ESI+3]	
00401319	- 2C 30	SUB AL,30	
0040131B	- 8A5E 04	MOV BL,BYTE PTR DS:[ESI+4]	
0040131E	- 80EB 30	SUB BL,30	
00401321	- 04 02	ADD AL,2	
00401323	- B2 0A	MOV DL,0A	
00401325	- F6F2	DIU DL	
00401327	- 38E3	CMP BL,AH	
00401329	- 75 01	SHORT prog9.0040132C	
0040132B	- 41	INC ECX	
0040132C	> 83F9 04	CMP ECX,4	
0040132F	- 75 07	SHORT prog9.00401338	
00401331	- B8 01000000	MOV EAX,1	
00401336	- EB 05	SHORT prog9.0040133D	
00401338	> B8 00000000	MOV EAX,0	Default case of swit

Рис. 10. Функция проверки пароля (продолжение)

Инструкции, расположенные в диапазоне адресов 004012C9-004012E2, осуществляют проверку четвертого и третьего символа введенного пароля (нумерация символов от 0). От каждого символа отнимается 30h (это значение является кодом нуля в таблице ASCII), чтобы из кода символа получить число, а также четвертый символ должен быть не больше 9. Данный факт говорит о том, что пароль должен состоять из цифр. Обратим внимание, что первый символ находится по адресу ESI, обращение к остальным символам осуществляется путем добавления смещения к ESI. Проанализировав процедуру проверки пароля видно, что максимальное смещение, которое добавляется к ESI – это 4, следовательно, пароль должен состоять из пяти символов. Проверка пароля начинается с четвертого символа, и все остальные символы зависят от него.

Напишем генератор паролей приложения («кейген») на Python, который выведет на экран все возможные пароли. Его код будет следующим:

```

1 passwd = [0 for i in range(5)]
2 for i in range(10):
3     passwd[3] = i
4     passwd[2] = ((passwd[3] + 255) % 256) % 10
5     passwd[1] = ((passwd[3] + 254) % 256) % 10
6     passwd[0] = ((passwd[3] + 1) % 256) % 10
7     passwd[4] = ((passwd[3] + 2) % 256) % 10
8     for i in range(5):
9         print(passwd[i], end="")
10    print("\n", end="")

```

Введем любой из десяти паролей, сгенерированных кейгеном, в исследуемую программу. Получим радостное сообщение об удачной попытке (см. рис. 11).

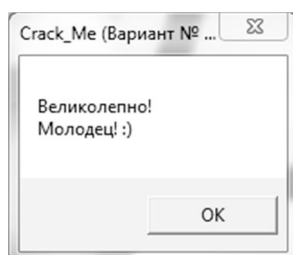


Рис. 11. Констатация удачной попытки

Исследование программы завершено.

7. Контрольные вопросы:

1. Что делает программа «prog9.exe»?
2. Что позволяет производить программа APIMonitorv2 Alpha-r 13?
3. Зачем был составлен скрипт на языке Python в данной лабораторной работе?

Время на выполнение лабораторной работы – 2 часа

Образовательная организация, авторы, эл. почта: ФГАОУ ВО «Сибирский Федеральный Университет», руководитель НУЛ ИБ, Шниперов А.Н. Ashniporov@sfu-kras.ru

Дисциплина: Криптографические методы защиты информации

Образовательная программа: 10.03.01 Информационная безопасность

Дисциплина: Криптографические методы защиты информации

Лабораторная работа. Криптоанализ функций хеширования

1. Учебные цели:

Отработать навыки криптоанализа функций хеширования методом перебора по словарю с использованием программного обеспечения Hashcat.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

В результате изучения дисциплины «Криптографические методы защиты информации» студенты должны:

Знать:

- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- модели шифров и математические методы их исследования;
- принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;

Уметь:

- использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки;
- применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;
- применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- уметь пользоваться научно-технической литературой в области криптографии;

Владеть:

- криптографической терминологией;
- навыками использования типовых криптографических алгоритмов;
- навыками использования ПЭВМ в анализе простейших шифров;
- навыками математического моделирования в криптографии

3. Перечень материально-технического обеспечения:

Лабораторное оборудование и программное обеспечения, прилагаемое к лабораторной работе.

4. Задание на исследование

Задание на практикум состоит из двух частей. Первая часть представляет собой три значения хеша для алгоритмов MD5, SHA-1 и SHA-256 (рис. 1), которые необходимо восстановить к прообразу с использованием Hashcat.

№ варианта: [7 ▼]

Восстановите информацию по её хешу

MD5	e99a18c428cb38d5f260853678922e03	<input type="text"/>	<input type="button" value="Проверить"/>
SHA-1	59c826fc854197cbd4d1083bce8fc00d0761e8b3	<input type="text"/>	<input type="button" value="Проверить"/>
SHA-256	db9fbddb7caeff7a326645c1bb47116eb3fd4ae3834bf5039fc5d47386786f5	<input type="text"/>	<input type="button" value="Проверить"/>

Рис. 1. Задание на практикум

Второе задание представляет собой часть Базы данных (БД) в виде учётных записей пользователей (рис. 2), в которых пароль был захеширован с использованием известной соли. Необходимо восстановить пароли пользователей с использованием Hashcat (не все пароли могут быть восстановлены).

№ варианта: [1 ▼]

Вам удалось похитить БД с паролями пользователей, но пароли были предварительно захешированы с использованием соли следующим образом MD5(pass + salt). Восстановите пароли пользователей.

ID	Имя	Фамилия	Пароль	Соль
1	Вася	Пупкин	9fe99c41f9495c3a5b2e26ca86fc3091	82sk21f
2	Дима	Кузнецов	be3e288263053a8f04ce5b31fa08504b	234sdf
3	Петя	Аляпкин	ab28b7ba658502e1e39d101ba65ee97f	fk20fk
4	Игорь	Савенков	c58b08013f1bdc458ccf6bf8e3ab9419	f2ffn2
5	Федя	Чуприн	a9738d77be72fd0565c2028394daad92	fov02f

Рис. 2. Пример второй части задания

5. Краткие теоретические сведения

Хеширование – это однонаправленное преобразование битовой строки произвольной длины в строку фиксированной длины по определённому алгоритму. Однонаправленность функции означает, что функция должна работать только в одну сторону: преобразовать битовую строку в выходное значение (хеш). Не должно быть такой функции, которая сможет преобразовать хеш в оригинальный текст. При использовании некоторых хеш-функций может возникнуть коллизия – это ситуация при которой двум различным битовым последовательностям соответствует одинаковое выходное значение. Хорошая функция хеширования должна обладать минимальной вероятностью коллизии.

MD5

MD5 – алгоритм хеширования, разработанный в 1991 году для создания дайджестов (хеш-суммы) сообщений. Выходная битовая строка алгоритма имеет длину 128 бит. Ниже приведён пример использования алгоритма MD5. Обычно выходное значение алгоритма представляют в виде 32 шестнадцатеричных цифр.

MD5('mtuci'): 423238ac7f8404b0ef12a8c9eaf19222

Даже при смене одной буквы сообщения на другую выходное значение полностью изменится. Данное свойство называется лавинным эффектом.

MD5('ntuci'): f4b9cf57844ff03661b253fd98debc3c

SHA-1

Алгоритм SHA-1 – это алгоритм хеширования для сообщений произвольной длины с выходным блоком размером 160 бит. Алгоритм разработан в 1995 году и рекомендован к использованию в госучреждениях США. Ниже представлены хеши сообщений для алгоритма SHA-1.

SHA-1('mtuci'): 66189e3d12383350546b0257022d60af3e2050c00

При изменении одного символа наблюдается лавинный эффект, как и для алгоритма MD5.

SHA-1('ntuci'): 2ed5410360e0714b401eaf0e1259e33c9c246cb1

SHA-256

SHA-256 – алгоритм хеширования, относящийся к семейству алгоритмов SHA-2, которое также включается в себя алгоритмы SHA-224, SHA-384 и SHA-512. SHA-256 имеет выходной размер хеша размером 256-бит, что уменьшает вероятность возникновения коллизии. Все три рассматриваемых алгоритма построены на основе общего метода – структура Меркла-Дамгарда. Ввиду найденных проблем в алгоритмах MD5 и SHA-1, принято решение, что новый алгоритм SHA-3 будет базироваться на совершенном новом принципе. Ниже приведены примеры хешей при использовании алгоритма SHA-256:

SHA-256('mtuci'):

962F1530F7B9531A0C9070EBD619FD80DD55F94C8A5A13B53B8297418F852EDE

SHA-256('ntuci'):

E21CA4B333E9678D34BF0BCC9506E1AB26A76F6C6FA1B55CE6FB16B076EE7508

Криптоанализ функций хеширования

Криптоанализ хеш-функций может быть проведён по нескольким направлениям: поиск коллизий, полный перебор и перебор по словарю.

Рассмотрим взлом некоторого хеша по словарю. Предположим, что имеется MD5 хеш: 5EBE2294ECD0E0F08EAB7690D2A6EE69.

И словарь, состоящий из слов (на практике словари состоят из миллионов или миллиардов вероятных слов):

1. word
2. war
3. secret
4. forest

Предварительно необходимо произвести преобразование вероятных слов в хеш значения. Получим следующий результат:

1. C47D187067C6CF953245F128B5FDE62A
2. 4CA9D3DCD2B6843E62D75EB191887CF2
3. 5EBE2294ECD0E0F08EAB7690D2A6EE69
4. F379CFD7A55B621577A8389D1817A102

Следующий шаг – это перебор полученных значений по порядку. Дойдя до третьего слова, можно обнаружить совпадение с исходным хешом. То есть для создания хеша использовалось слово «secret». Отметим, что некоторые значения хешей могут быть получены с использованием соли. Соль – это некоторая строка данных, которая хешируется вместе с исходным сообщением. Данная техника особенно популярна при хранении паролей в базах данных (БД).

Предположим, что некоторый пользователь использует в качестве пароля слово «secret», значение хеша которого показано выше. Если злоумышленник похитит из базы данных хешированный пароль пользователя, то ему не составит труда восстановить пароль по словарю. Но если в базе данных хранятся пароли, полученные хешированием с использованием соли, то восстановление будет маловероятным без знания соли.

Допустим, что соль – это строка «8*\$3h#92», тогда прежде чем сохранить пароль пользователя в БД, соль конкатенируется с исходным паролем, то есть будет получена строка: «secret8*\$3h#92». После этого полученная строка подвергается хешированию, то есть при использовании алгоритма MD5 будет получено следующее значение: 863417B487BFCF99B47C9A4F105FF115.

Как видно, полученное значение отличается от предыдущего. То есть использование соли повысило надёжность пароля. Маловероятно, что какой-либо словарь будет содержать значение «secret8*\$3h#92». При этом пользователю не нужно знать значение соли, при авторизации он, как и прежде будет вводить пароль «secret», после чего на сервере будет добавляться известная соль, полученный результат будет хеширован и сравнен со значением из БД.

Для перебора значений хеша по словарю существует множество программ, например, John The Ripper, PasswordsPro и другие.

В данной работе используется бесплатное мультиплатформенное приложение с открытым исходным кодом – Hashcat. Hashcat обладает большим количеством преимуществ: способен задействовать для работы как CPU, так и GPU, поддерживает распределённый взлом по сети, поддерживает большое количество алгоритмов хеширования и способен осуществить взлом хешей с солью и многое другое. Hashcat – это консольное приложение, но для работы может быть загружен GUI с ресурса, который представляет собой оболочку поверх консольной версии.

6. Порядок выполнения лабораторной работы

1. Создадим отдельные файлы с хешами (рис. 3) и добавим словарь.

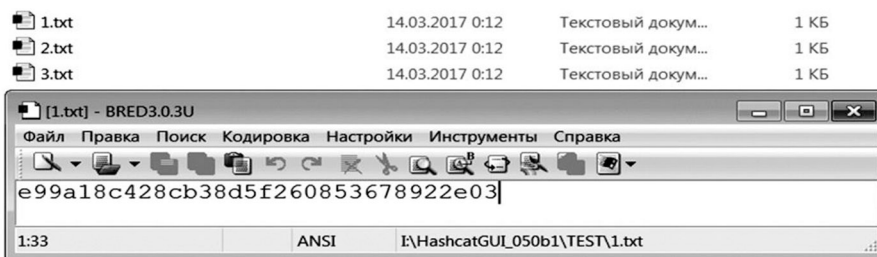


Рис. 3. Создание файлов с хешами

2. Установим необходимые опции Hashcat: тип хеша, файл с хешем для взлома, выходной файл и используемое консольное приложение (рис. 4). Если устройство не поддерживает взлом с использованием GPU, то также выберите значение «CPU only». Опция «Remove found hashes» включает удаление найденных хешей из входного файла.

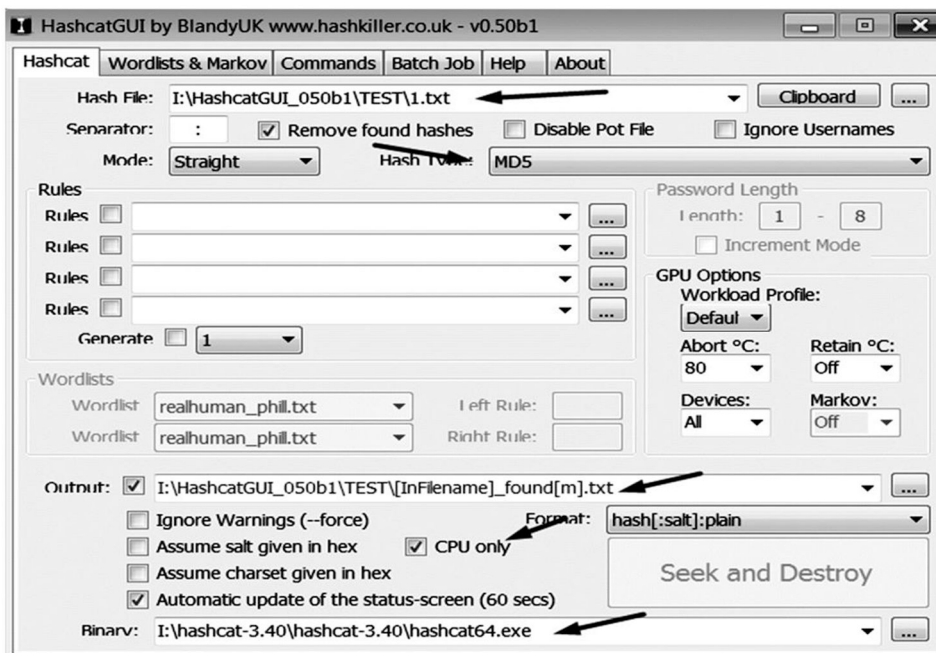


Рис. 4. Установка необходимых опций в Hashcat

3. В результате работы Hashcat был получен оригинал хешированной строки (рис. 5).

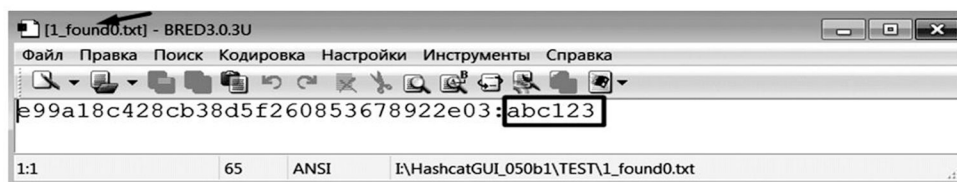


Рис. 5. Восстановленное значение хеша

Аналогичным образом могут быть восстановлены остальные хеш-значения.

Для выполнения второй части задания установим в опциях Hashcat вид хеша с использованием соли и проведём взлом аналогично первому заданию. Хеш и соль во входном файле должен быть разделен выбранным разделителем.

7. Контрольные вопросы

1. Что такое хеш-функция? Какие хеш-функции вы знаете?
2. Как может быть проведён криптоанализ хеш-функции?
3. Что такое коллизия? Для каких алгоритмов вы знаете коллизии? Чем они опасны?
4. Что такое криптографическая «соль»?

Время выполнения лабораторной работы – 2 часа

Образовательная организация, авторы, эл. почта: Ордена трудового красного знамени Федеральное Государственное Бюджетное Образовательное Учреждение Высшего Образования «Московский Технический Университет Связи и Информатики» (МТУСИ), Костин Денис Владимирович, d.v.kostin@mail.ru

Образовательная программа: 10.03.01 Информационная безопасность.

Дисциплина: Криптографические методы защиты информации.

Лабораторная работа. **Криптоанализ алгоритма шифрования RSA**

1. Учебные цели:

Изучить проведение криптоанализа алгоритма RSA на основе факторизации целых чисел методами перебора делителей, Ро-алгоритма Полларда и метода общего решета числового поля.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

В результате изучения дисциплины «Криптографические методы защиты информации» студенты должны:

Знать:

- основные задачи и понятия криптографии;
- принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;
- знает принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы

Уметь:

- использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки;
- выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
- применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- уметь пользоваться научно-технической литературой в области криптографии;

Владеть:

- криптографической терминологией;
- навыками использования типовых криптографических алгоритмов;
- навыками использования ЭВМ в анализе простейших шифров;
- навыками математического моделирования в криптографии

3. Перечень материально-технического обеспечения:

Лабораторное оборудование и программное обеспечения, прилагаемое к лабораторной работе

4. Задание на исследование

Для выполнения практикума необходимо факторизовать три числа различной длины с помощью метода перебора делителей, алгоритма По Полларда и общего метода решета числового поля. На основе полученных многочленов необходимо расшифровать сообщение, зашифрованное алгоритмом RSA. Полученные открытые тексты необходимо сдать проверочной системе.

5. Краткие теоретические сведения

RSA – это алгоритм ассиметричного шифрования, который основан на вычислительной сложности факторизации целых чисел большой длины.

Рассмотрим схему работы алгоритма RSA.

1. Создание ключей

Создание ключей состоит из нескольких этапов:

- 1) Выбираются два простых случайных числа p и q длиной n -бит.
- 2) Находится произведение чисел p и q , которое называется модулем (1).

$$N = p * q, \quad (1)$$

- 3) Определяется значение функции Эйлера для числа N по формуле (2).

$$\varphi(N) = (p-1) * (q-1), \quad (2)$$

- 4) Выбирается целое число e из интервала $1 < e < \varphi(N)$ взаимно простое со значением $\varphi(N)$. Обычно в качестве e выбирают простое число.
- 5) Находят число d по формуле (3).

$$d = e^{-1} \bmod \varphi(N), \quad (3)$$

Полученные значения (e, N) будут являться открытым ключом и могут быть опубликованы. Значения (d, N) являются закрытым ключом и должны храниться в тайне.

2. Шифрование и расшифровывание

Чтобы зашифровать сообщение, необходимо представить сообщение в виде массива байт, который в свою очередь можно представить одним десятичным числом, после чего над полученным числом необходимо провести следующую операцию (формула 4):

$$c = m^e \bmod N, \quad (4)$$

где m – это шифруемое сообщение, c – полученное зашифрованное сообщение. Обычно полученное число представляют в виде HEX (шестнадцатеричного) значения, которое будет являться зашифрованной строкой.

Расшифровка сообщения происходит столь же тривиально (формула 5):

$$d = c^e \bmod N, \quad (5)$$

где d – расшифрованное сообщение.

Полученное число переводится обратно в массив байт, которые в свою очередь могут быть преобразованы в исходное сообщение.

Криптоанализ алгоритма RSA

Стойкость алгоритма RSA основана на сложности разложения большого числа N на два простых числа p и q . При этом во время генерации ключей можно легко сформировать два случайных простых числа и найти их произведение. Обратная же операция (факторизация) выполняется намного сложнее и часто требует применения специальных алгоритмов. Факторизация целого числа на множители в основном зависит от длины факторизируемого числа. Числа длиной около 20–30 бит могут быть легко найдены даже методом простого перебора делителей за приемлемое время. Более длинные числа требуют использования специальных алгоритмов, которые позволяют сократить количество необходимых операций.

Метод перебора делителей

Перебор делителей – это простейший метод, суть которого заключается в последовательном переборе всех целых чисел от 2 до квадратного корня из исследуемого числа n . Если при делении n на очередное число t остаток от деления равен нулю, то это число является делителем n . Если остаток от деления не равен нулю, то t увеличивается на единицу, и процедура повторяется. В том случае, если делитель не найден, число объявляется простым. Неоптимизированный алгоритм имеет сложность $O(n^{1/2})$. Опти-

мизация алгоритма может быть проведена за счёт исключения чётных делителей, кроме числа 2, а также всех делителей, кратных трём, кроме числа 3.

Ро-алгоритм Полларда

Ро-алгоритм (ρ -алгоритм) Полларда – вероятностный алгоритм факторизации основанный на алгоритме Флойда и следствий из парадокса дней рождений. Сложность алгоритма оценивается как $O(n^{1/4})$. Данный алгоритм достаточно эффективен для факторизации чисел размером до 128-бит за приемлемое время.

Алгоритм выглядит следующим образом:

- 1) Случайным образом выбираются два числа x и c ;
- 2) Число $y = x$, $g = 1$;

В цикле про3) веряем условие, что $g = 1$ и пока условие выполняется, вычисляем следующие значения:

$$\begin{aligned}x &= f(x), \\y &= f(f(y)), \\g &= \gcd(x-y, N).\end{aligned}$$

- 4) Если $g \neq 1$, то g является найденным делителем.

В качестве функции $f(x)$ можно выбрать различные простые функции, но обычно выбираются функцию $f(x) = x^2 \pm 1 \pmod{N}$ или $f(x) = x^2 \pm c \pmod{N}$, которая используется в листинге 2. Листинг 2 содержит реализацию данного алгоритма на языках Java и Python. Следует также отметить, что в некоторых случаях алгоритм не способен найти верное решение, если это происходит, то необходимо использовать другую функцию $f(x)$.

Общий метод решета числового поля

Самый эффективный алгоритм факторизации целых чисел длиной от 110 знаков на момент написания данной работы. Алгоритм является усовершенствованной версией метода квадратичного решета. В данном пособии не приводится алгоритм и программная реализация данного метода в виду его сложности.

6. Порядок выполнения лабораторной работы

На рисунке 1 приведён пример задания на практикум.

№ варианта:

Расшифруйте зашифрованное сообщение, если вам известен только открытый ключ (e , N). Для этого произведите факторизацию числа N на простые множители.

Факторизуйте N с помощью полного перебора
Сообщение: 7820433e68
 e : 487218339947
 N : 921809561437
Расшифрованное сообщение:

Факторизуйте N с помощью Ро-алгоритма Полларда
Сообщение: 1074b64cef9417d0429e18521
 e : 374893278718192505282233231067
 N : 795266777254820365581461589251
Расшифрованное сообщение:

Факторизуйте N с помощью общего метода решета числового поля
Сообщение: 16eb1acae5d2227b2c33d1041b55df472bca6240798007cf5a0aed84f59
 e : 273842542184891212131408834864046716117496075835138688950759516706829651
 N : 829492194624780665896003975203295313214465619004807308809968633524995841
Расшифрованное сообщение:

Рис. 1. Пример задания на практикум

1. Факторизуем число $N = 921809561437$ с помощью перебора делителей. Чтобы найти второй делитель, необходимо число N разделить на найденный первый делитель. Получены следующие результаты: $p = 992603$, $q = 928679$

2. Так как открытый ключ известен, можем вычислить закрытый ключ RSA по формуле 3. На языке Java данная формула будет представлена в следующем виде:

```
BigInteger e = new BigInteger("487218339947");  
BigInteger phi = p.subtract(BigInteger.ONE).multiply(q.subtract(BigInteger.ONE)); //phi=(p-1)(q-1)  
BigInteger d = e.modInverse(phi); // d=e^-1 mod phi
```

Листинг 2. Определение закрытого ключа d

Полученное значение: $d = 277718271507$.

3. Преобразуем сообщение из шестнадцатеричного формата в десятичный и расшифруем в соответствии с формулой 5. Полученное значение преобразуем в массив байт, после чего в строку (листинг 3).

```
BigInteger message = new BigInteger("7820433e68", 16); //hex to dec
byte[] decrypted = message.modPow(d, N).toByteArray();
String decMessage = new String(decrypted);
```

Листинг 3. Расшифровка сообщения

Полученный результат: «easy», что также подтверждает проверочная система (рис. 2).

Факторизуйте N с помощью полного перебора

Сообщение: 7820433e68

e: 487218339947

N: 921809561437

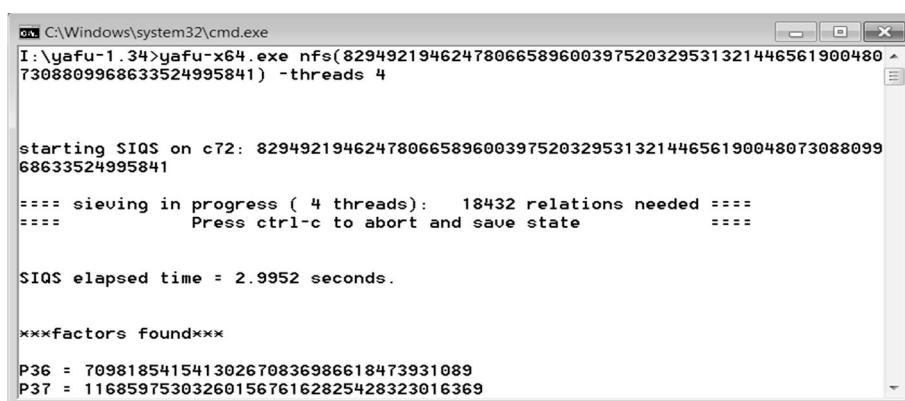
Расшифрованное сообщение: easy

Проверить

Рис. 2. Верный ответ в проверочной системе

Решение второго задания аналогично вышерассмотренному, за исключение того, что для факторизации чисел должен быть использован Рo алгоритм Полларда. Для решения третьего задания воспользуемся приложением YAFU.

4. Зайдём в папку с приложением и запустим консоль. В консоли выполним команду следующего вида (рис. 3):



```
C:\Windows\system32\cmd.exe
I:\yafu-1.34>yafu-x64.exe nfs(82949219462478066589600397520329531321446561900480
7308809968633524995841) -threads 4

starting SIQS on c72: 8294921946247806658960039752032953132144656190048073088099
68633524995841

==== sieving in progress ( 4 threads): 18432 relations needed ====
==== Press ctrl-c to abort and save state =====

SIQS elapsed time = 2.9952 seconds.

***factors found***

P36 = 709818541541302670836986618473931089
P37 = 1168597530326015676162825428323016369
```

Рис. 3. Факторизация числа в YAFU

Где nfs – вызов факторизации с помощью метода решета числового поля, в качестве параметров которого выступает факторизируемое число. Параметр threads указывает количество потоков для проведения факторизации. Обычно в качестве значения данного параметра следует указывать *число_ядер_процессора* * 2. Последние две строки вывода – это найденные множители факторизируемого числа.

Полученный результат: «May the force be with you» (рис. 4).

Факторизуйте N с помощью общего метода решета числового поля

Сообщение: 16eb1aeaed5d2227b2c33d1041b55df472bca6240798007cf5a0aed84f59

e: 273842542184891212131408834864046716117496075835138688950759516706829651

N: 829492194624780665896003975203295313214465619004807308809968633524995841

Расшифрованное сообщение: May the force be with you

Проверить

Рис. 4. Верный ответ в проверочной системе

7. Контрольные вопросы

1. Объясните принцип работы алгоритма RSA.
2. Как может быть проведён криптоанализ алгоритма RSA?
3. Какие методы факторизации простых чисел вы знаете? Какие из них наиболее эффективны?
4. Объясните принцип работы метода перебора делителей.

Время выполнения лабораторной работы – 2 часа

Образовательная организация, авторы, эл. почта: Ордена трудового красного знамени Федеральное Государственное Бюджетное Образовательное Учреждение Высшего Образования «Московский Технический Университет Связи и Информатики» (МТУСИ), Костин Денис Владимирович, d.v.kostin@mail.ru

Образовательная программа: 10.03.01 Информационная безопасность.

Дисциплина: Криптографические методы защиты информации / Защита информационных процессов в компьютерных системах.

Лабораторная работа.

Исследование защищенных сетей, построенных по цифровым технологиям блокчейн и хэшчейн с использованием методов криптографии

1. Учебные цели:

Изучить принципы построения блокчейн-сетей и их функционирования, отработать навыки проектирования и построения структур, работы с функциями хеширования и криптографии.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь работать с блокчейн-сетями, владеть функциями хеширования и криптографии.

3. Перечень материально-технического обеспечения:

Компьютерный класс, программы шифрования хеширования, языки программирования

4. Задание на исследование:

Пройти все этапы формирования блока в роли абонента и майнера, провести расчеты требований к сети + дополнительно наблюдение за поведением блокчейн-сети.

5. Краткие теоретические сведения

Блокчейн – выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию. Чаще всего копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга.

Цепочка блоков позволяет надежно хранить информационные записи в силу того, что данные каждого блока вычислены, исходя из данных предыдущего, в силу чего практически невозможно изменить данные в прошлом так, чтобы при проверке не было найдено несоответствий.

В известных на сегодняшний день блокчейн-системах для формирования блоков используются майнеры, выполняющие работу по формированию блока из списка текущих записей. Любой абонент может быть майнером, и доверенность новых блоков обеспечивается установкой сложности их формирования, обычному пользователю непосильной. Майнеров, в свою очередь, мотивируют конкурировать между собой, заставляя наращивать мощности для избежания ситуации, когда один майнер будет доминировать в области формирования блоков и единолично формировать несколько блоков подряд.

Процесс закрепления данных выглядит следующим образом:

- абонент либо несколько абонентов (блок может содержать любое количество записей), заявляют участникам системы о том, что хотят зафиксировать данные, в примере — денежный перевод от одного абонента другому;
- свободный майнер объединяет оглашенные системе информативные записи, после чего формирует данные блока – индекс блока в цепочке, информативные записи в нем, хэш предыдущего блока и проч. информацию, после чего объявляет новый блок участникам системы, и если блок корректно построен, то все участники встраивают этот блок в свою цепочку;
- абоненты, получающую информацию о новом блоке, сверяются с копией данных, находящихся у них – такой же хэш у предыдущего блока, как в новом, адекватный ли порядковый номер, правильно ли вычислены данные для контроля целостности блока, после чего, если все хорошо, записывает этот блок себе и при запросе других абонентов делится с ними новыми блоками цепочки.

Пример того, как выглядит блок с одиночной записью в нем на языке Python:

```
block = {
    'index': 1,                #номер блока в цепочке
    'timestamp': 1506057125.900785,    #дата-время его формирования
    'transactions': [        #список информативных записей, в этом примере – транзакций
        { #сама запись, в данном случае состоящая из отправителя, получателя и количества
            'sender': "8527147fe1f5426f9dd545de4b27ee00",
            'recipient': "a77f5cdfa2934df3954a5c7c7da5df1f",
            'amount': 5,
        }
    ],
    'proof': 324984774000,    #доказательство работы
    'previous_hash': "2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824"
}
```

Доказательство работы (поле proof) в данном примере является результатом затратной по вычислительным мощностям операции, которая одновременно используется для контроля целостности блока и как доказательство того, что майнер провел вычисления, непосильные большинству пользователей за короткое время. К примеру, взять доказательство работы предыдущего блока и подобрать такое число, чтобы хэш sha-256 от суммы этих чисел начинался с n-го количества нулей. Получить такое число на сегодняшний день можно только перебором, продолжительность которого увеличивается в разы за каждый ноль в условии.

К примеру, для получения доказательства работы следующего блока нужно вычислить $\text{sha256}(324984774000+y) = 000\dots$ (примечание – сумма в данном примере преобразована в строку и хэш вычисляется из байтов, составляющих строку).

тогда:

$y=0, \text{sha256}(324984774000+y) = 90327880a7e58b3814\dots$

$y=1, \text{sha256}(324984774000+y) = 33c0b810906bb6713b\dots$

$y=26455, \text{sha256}(324984774000+y) = 00007554923a2c\dots$

Как видно, это заняло 26455 итераций. Будь в требовании большей нулей, итераций было бы в разы больше.

Для того, чтобы блокчейн-сеть стала анонимной, используется также шифрование информационных записей – если абонент, прежде чем выдавать информацию в блокчейн-сеть, зашифрует ее, то прочитать запись сможет только тот, кому она предназначена, либо же возможно использовать обезличенные данные, как в большинстве криптовалют, где используются только номер кошелька, который не привязан к конкретному лицу.

Известной проблемой блокчейн-систем, использующих майнеров, заключается в атаке 51 %, как ее принято называть. Она основывается на системе обработки коллизий в большинстве блокчейнов. Допустим, есть абонент, у которого в блокчейне n блоков. Он запрашивает обновления у других абонентов, и один отдает ему 3 новых блока, а другой один, причем цепочки обоих абонентов корректны. В большинстве случаев для присоединения выбирается более длинная цепочка блоков, даже если информация в них различается. И даже если перед этим абонент уже присоединил n+1-й блок к своей цепочке, то получив подходящие к его цепочке блоки с номерами от n+1 до n+3, он может заменить n+1-й блок, который уже был присоединен, поскольку целостность цепочки от этого не страдает.

Возьмем блок, который использовался для примера:

```
block = {
  'index': 1,                #номер блока в цепочке
  'timestamp': 1506057125.900785, #дата-время его формирования
  'transactions': [        #список информативных записей, в этом примере – транзакций
    {                       #сама запись, в данном случае, состоящая из отправителя, получателя и количества
      'sender': "8527147fe1f5426f9dd545de4b27ee00",
      'recipient': "a77f5cdfa2934df3954a5c7c7da5df1f",
      'amount': 5,
    }
  ],
  'proof': 324984774000,    #доказательство работы
  'previous_hash': "2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824"
}
```

Если представить, что пока рядовой майнер создает этот блок, майнер с доминирующими мощностями создает 3-5 блоков:

```
{
  'index 1': ,
  'timestamp': 1506057125.910785,
  'transactions': [
    {
      'sender': "8527147fe1f5426f9dd545de4b27ee00",
      'recipient': "другой счет",
      'amount': 5,
    }
  ],
  'proof': 324984774000,
  'previous_hash': "2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824"
},
{
  'index 2': ,
```

```

'timestamp': 1530518790.7397919,
'transactions': [
{
'sender': "любой счет майнера",
'recipient': "другой любой счет майнера",
'amount': 5,
}
],
'proof': 26455,
'previous_hash': "7ad968210259ceea07fb6eb6528d05003297c2ef752a6cef5ebfb96e26480d0b"
},
{
'index 3': ,
'timestamp': 1530518808.369221,
'transactions': [
{
'sender': "любой счет майнера",
'recipient': "другой любой счет майнера",
'amount': 5,
}
],
'proof': 62029,
'previous_hash': "94c410ad3559604d5237df4c2bbe13a467d94752fa69b2a56e30bd8974e01cf7"
}

```

Получив такую цепочку, абонент может решить, что у него неправильная версия блокчейна и заменить ее данной, в которой майнер заменил счет получателя в первом блоке и добавил мусорных операций в последующих.

6. Порядок выполнения лабораторной работы (этапы)

- Выбрать некоторую задачу, чьи этапы требуют надежной фиксации.
- Описать структуру блоков для этой задачи – поля, методы хэширования, расчета доказательства сложности и саму сложность, разрешение коллизий, модель майнера, количество информативных записей в блоке и т.д., обосновать перед преподавателем свои решения;
- Рассчитать максимальный прирост объема, занимаемого блокчейном, за n транзакций, где $n = 10, 100, 1000, 10000, 100000, 1000\ 000$. Спрогнозировать объем блокчейн сети через месяц, год, 10 лет с учетом того, что в неделю совершается n транзакций.
- Любым образом (разработать программу на любом языке, рассчитать самостоятельно иным образом) создать цепочку блоков, создать несколько транзакций и обработать их от лица абонента, майнера и других участников сети.
- Предъявить свой блокчейн и его правила преподавателю, доказать корректность цепочки.

Время на выполнение лабораторной работы – 6 часов

Образовательная организация, авторы, эл. почта: ФГБОУ ВО «Пятигорский Государственный Университет», Макаров Анатолий Михайлович, mellin_22@mail.ru

Образовательная программа: 10.03.01 Информационная безопасность; 10.03.02 Организация и технология защиты информации.

Дисциплина: Криптографические методы защиты информации.

Лабораторная работа.

Генерация открытых и секретных ключей в алгоритме RSA

1. Учебные цели:

Формирование у студентов необходимого объема понятий и знаний, касающихся математических основ криптографии, методов преобразования информации в различных криптосистемах; умение генерировать простые числа длиной 512 бит и более с последующей проверкой на простоту, умение формировать открытые и секретные ключи в криптографическом алгоритме RSA.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Умение применять программные средства и системы программирования для решения задач обеспечения аутентификации и защиты информации в информационных системах. Приобретение навыков генерации простых чисел длиной не менее 512 бит в программном комплексе Microsoft Visual Studio Express 2012 на языке программирования C# для формирования открытых и секретных ключей в криптографическом алгоритме RSA.

3. Перечень материально-технического обеспечения:

Персональный компьютер; программный комплекс Microsoft Visual Studio Express 2012 или более поздняя версия; Microsoft Office Word не ниже 2007 года; методические указания, включающие в себя инструкцию по выполнению работы, описание методов генерации чисел длиной не менее 512 бит, тесты для проверки чисел на простоту.

4. Задание на исследование:

Реализуйте программу осуществляющую генерацию двух пар чисел $\{R, N\}$ и $\{D, N\}$, где $\{R, N\}$ публикуется в качестве открытого ключа RSA, а $\{D, N\}$ играет роль закрытого ключа RSA.

5. Краткие теоретические сведения

5.1. Общие понятия

Простое число – натуральное число, имеющее ровно два различных натуральных делителя – единицу и самого себя.

Взаимно простые числа – целые числа, не имеющие никаких общих делителей.

Тестом простоты (или проверкой простоты) называется алгоритм, который, приняв на входе число, позволяет либо не подтвердить предположение, что рассматриваемое число составное, либо точно утверждать его простоту. Во втором случае он называется истинным тестом простоты. Таким образом, тест простоты представляет собой только гипотезу о том, что если алгоритм не подтвердил предположение о составности числа, то это число может являться простым с определённой вероятностью. Это определение подразумевает меньшую уверенность в соответствии результата проверки истинному положению вещей, нежели истинное испытание на простоту, которое даёт математически подтвержденный результат.

Криптография – наука о методах обеспечения конфиденциальности и аутентичности информации. Математическая криптография возникла как наука о шифровании информации, т.е. как наука о криптосистемах. В классической модели системы секретной связи имеют место два полностью доверяющих друг другу участника, которым необходимо передавать между собой информацию, не предназначенную для третьих лиц. Такая информация называется конфиденциальной или секретной. Задача обеспечения конфиденциальности, т.е. защита секретной информации от противника – первая задача криптографии.

Шифрование – обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

Электронная подпись – цифровой аналог ручной подписи, обеспечивающий возможность проверки подлинности и корректности документа. Существует техническая возможность проверки электронной подписи: если документ подменен или искажен при передаче, подпись при проверке будет признана некорректной.

Криптографическая система с открытым ключом (разновидность асимметричного шифрования, асимметричного шифра) – система шифрования и/или электронной подписи, при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки электронной подписи и для шифрования сообщения. Для генерации электронной подписи и для расшифровки сообщения используется закрытый ключ.

Закрытый ключ – сохраняемый в тайне компонент ключевой пары, применяющейся в асимметричных шифрах, то есть таких шифрах, в которых для прямого и обратного преобразований используются разные ключи. В отличие от закрытого ключа, другой компонент ключевой пары – открытый ключ, как правило, не хранится в тайне, а защищается от подделки и публикуется.

Открытый ключ – тот из двух ключей асимметричной системы, который свободно распространяется.

Функция Эйлера от переменной – мультипликативная арифметическая функция, равная количеству натуральных чисел, меньших этой переменной и взаимно простых с ней.

5.2. Тесты на простоту

5.2.1. Первая интерпретация малой теоремы Ферма. Если p – это предполагаемое простое число, то p , с некоторой вероятностью, будет простым числом, если a^p сравнимо с a по модулю:

$$a^p \equiv a \pmod{p}.$$

5.2.2. Вторая интерпретация малой теоремы Ферма. Если p – это предполагаемое простое число, то p , с некоторой вероятностью, будет простым числом, если a^{p-1} сравнимо с 1 по модулю p :

$$a^{p-1} \equiv 1 \pmod{p}.$$

5.2.3. Тест Миллера – Рабина опирается на проверку ряда равенств, которые выполняются для простых чисел. Если хотя бы одно такое равенство не выполняется, это доказывает, что число составное. Пусть $p > 2$ – простое число. Представим число $p - 1$ в виде $p - 1 = 2^s * d$, где d – нечетно. Тогда для любого a выполняется одно из условий:

1. $a^d \equiv 1 \pmod{p}$;
2. существует такое r , $0 \leq r \leq s - 1$: $a^{2^r d} \equiv -1 \pmod{p}$.

5.3. Способы генерации чисел

5.3.1. 30 апреля 2000 года Владимир Хренов сделал научное открытие, которое гласит, что простые числа не произвольно взяты из ряда натуральных чисел. 7 января 2001 года был описан "закон простых чисел", а вместе с ним – закономерности формирования всех чисел натурального ряда. Простые числа по "закону простых чисел" получаются по формуле:

$$X = 6 * n \pm 1,$$

где n – любое натуральное число.

5.3.2. Центрированное квадратное число (K_v) – относится к классу фигурных формул, каждое такое число расположено вокруг центральной точки, окруженной точками, расположенными на квадратных слоях. Не все квадратные числа являются простыми. Формула для получения таких чисел:

$$K_v = n^2 + (n - 1)^2,$$

где n – любое целое число ≥ 0 .

5.3.3. Центрированное семиугольное число (S_m) – относится к классу фигурных формул, каждое такое число расположено вокруг центральной точки, окруженной точками, расположенными на семиугольных слоях. Не все семиугольные числа являются простыми. Центрированное семиугольное число можно получить по формуле:

$$S_m = \frac{7n^2 - 7n + 2}{2},$$

где n – любое целое число ≥ 0 .

5.3.4. Центрированное десятиугольное число (D_s) – относится к классу фигурных формул, каждое такое число расположено вокруг центральной точки, окруженной точками, расположенными на десятиугольных слоях. Не все десятиугольные числа являются простыми. Центрированное десятиугольное число можно задать с помощью формулы:

$$D_s = 5(n^2 - n) + 1,$$

где n – любое целое число ≥ 0 .

5.4. RSA

RSA – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и других.

Пользователь RSA создает и затем публикует открытый ключ, основанный на двух больших простых числах вместе со вспомогательным значением. Простые числа должны храниться в тайне. Любой человек может использовать открытый ключ для шифрования сообщения, но если он достаточно большой, то только со знанием простых чисел может декодировать сообщение. До сих пор остается открытой дискуссия о том, насколько это надежный механизм. Алгоритм RSA состоит из четырех этапов: генерации ключей, их распределения, шифрования и дешифрования. Данная лабораторная работа направлена на реализацию первого этапа – генерации ключей.

Алгоритм создания открытых и секретных ключей в RSA заключается в следующем:

- 1) генерируются два простых числа q и p длиной 512 или 1024 бит каждое;
- 2) вычисляется произведение сгенерированных простых чисел N , которое называется модулем:

$$N = q \cdot p;$$

- 3) определяется значение функции Эйлера от этого числа $\varphi(N)$:

$$\varphi(N) = (p - 1) \cdot (q - 1);$$

- 4) выбирается целое число R , которое называется открытой экспонентой. При выборе R необходимо чтобы оно было взаимно простым со значением $\varphi(N)$ и находилось в интервале $1 < R < \varphi(N)$. Обычно в качестве R берут простые числа, содержащие небольшое количество единичных бит в двоичной записи, например, простые из чисел Ферма: 17, 257 или 65537, так как в этом случае время необходимое для шифрования, с использованием быстрого возведения в степень, будет меньше. Слишком малые значения, например, 3, потенциально могут ослабить безопасность схемы RSA;
- 5) D вычисляется число D (число D называется секретной экспонентой, обычно, оно вычисляется при помощи расширенного алгоритма Евклида), мультипликативно обратное к числу R по модулю $\varphi(N)$, то есть число, удовлетворяющее сравнению:

$$D \cdot R \equiv 1 \pmod{\varphi(N)};$$

- 6) пара чисел $\{R, N\}$ публикуется в качестве открытого ключа;
- 7) пара чисел $\{D, N\}$ играет роль закрытого ключа.

6. Порядок выполнения лабораторной работы (этапы)

- 1) Получить вариант задания у преподавателя.
- 2) Изучить теоретическую часть.
- 3) Запустить Microsoft Visual Studio Express 2012.
- 4) Используя предоставленный материал разработать подпрограмму для генерации чисел на основе одной из формул, представленных в разделе 5.4, формула для генерации чисел определяется в соответствии с вариантом.
- 5) Преобразовать разработанный код для возможности генерировать числа длиной 512 или 1024 бит, длина генерируемого числа определяется согласно варианту.
- 6) Разработать подпрограмму проверки чисел на простоту, тест на простоту выбрать согласно варианту.
- 7) Разработать программу создания открытых и секретных ключей криптографического алгоритма RSA, для генерации и проверки на простоту чисел использовать подпрограммы, разработанные согласно пунктам 5 и 6.
- 8) Создать программный интерфейс.
- 9) Запустить и отладить программу.
- 10) Оформить пояснительную записку в Microsoft Office Word.

7. Контрольные вопросы:

1. Какие числа называются простыми?
2. Какие два целых числа можно назвать взаимно простыми?
3. На чем основан криптографический алгоритм RSA? Где он используется?
4. Какая пара чисел составляет открытый ключ в алгоритме RSA?
5. Какая пара чисел составляет секретный ключ в алгоритме RSA?
6. Сколько простых чисел используется для формирования, открытого и секретного ключей в криптографическом алгоритме RSA?
7. Как определяется модуль в алгоритме создания открытых и секретных ключей RSA?
8. Что может произойти с безопасностью шифрования алгоритма RSA, если открытая экспонента будет слишком мала?
9. Какие числа и почему рекомендовано использовать при выборе открытой экспоненты?
10. Как вычисляется значение функции Эйлера от простого числа, от произведения двух простых чисел?
11. Каким образом вычисляется секретная экспонента?
12. Что понимается под тестом на простоту числа?
13. Сформулируйте теорему Ферма?
14. Какие два условия должны быть выполнены для определения простоты числа согласно тесту Миллера-Рабина?
15. Какое число называется центрированное десятиугольное, квадратное, семиугольное?
16. Что подразумевают под криптографической системой с открытым ключом?

Образовательная организация, авторы, эл. почта: Санкт – Петербургский государственный морской технический университет, авторы – Буковский И.В., Согонов С.А., Шавинская С.К., эл.почта – sankar52@mail.ru, ssogonov@mail.ru

Дисциплина: Методы оценки безопасности компьютерных систем

Образовательная программа: 10.03.01 Информационная безопасность.

Дисциплина: Методы оценки безопасности компьютерных систем.

Лабораторная работа. **Тестирование компьютерной сети на проникновение**

1. Учебные цели:

В работе изучается эксплуатирование уязвимостей в удалённой системе с помощью программного обеспечения Metasploit.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

В результате изучения дисциплины «Методы оценки безопасности компьютерных систем» студенты должны:

Знать:

- уязвимости используемого программного обеспечения и методы их эксплуатации;
- принципы работы и правила эксплуатации программно-аппаратных средств защиты информации;
- состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях.

Уметь:

- анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия;
- осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения;
- конфигурировать и контролировать корректности настройки программно-аппаратных средств защиты информации в компьютерных сетях.

Владеть:

- выполнением работ по обнаружению вредоносного программного обеспечения;
- определением состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях;
- формированием шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях.

3. Перечень материально-технического обеспечения:

Лабораторное оборудование и программное обеспечение, входящие в операционную систему Kali Linux (<https://www.kali.org/>)

4. Задание на исследование

Выполнить тестирование на проникновение для заданной преподавателем удаленной машины.

5. Краткие теоретические сведения

Тестирование на проникновение (жарг. пентест) – оценка безопасности компьютерной системы методом моделирования действий злоумышленника. Данный процесс состоит из трёх этапов: поиск уязвимостей, эксплуатация уязвимостей, разработка рекомендаций по устранению уязвимостей.

Для поиска уязвимостей может быть использована утилита Nmap. В случае обнаружения открытых портов на удалённой системе следует перейти к поиску эксплойтов. Эксплойт (exploit) – компьютерная программа (программный код), использующий уязвимости в ПО для атаки на вычислительную систему. Для поиска эксплойтов можно воспользоваться ресурсом www.exploit-db.com, который содержит обширную, постоянно пополняющуюся, базу данных уязвимостей, либо воспользоваться эксплойтами входящими в состав Metasploit.

Metasploit – платформа для создания и тестирования эксплойтов, которая помогает разрабатывать новые сигнатуры для IDS и других систем информационной безопасности. Программа работает в различных операционных системах, в том числе в Windows.

6. Порядок выполнения лабораторной работы

1. Запустите Zenmap (<https://nmap.org/zenmap/>), введите IP-адрес целевой машины, выберите профиль и произведите сканирование на наличие открытых портов (рис. 1).

Программа обнаружила 3 открытых порта (80, 9255, 9256), причём последние два порта принадлежат одной программе – Achat (у вас может быть другая программа).

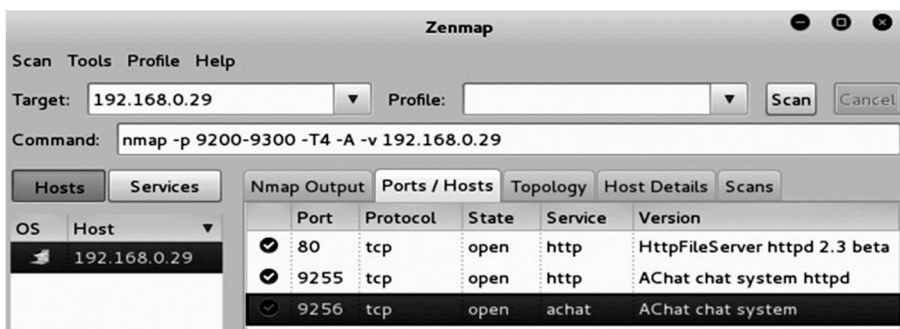


Рис. 1. Результаты сканирования Zenmap

2. Произведите поиск эксплойта для программы Achat. Для этого посетите www.exploit-db.com. На рисунке 2 показаны уязвимости, найденные на сайте. Как можно заметить, один из эксплойтов подходит для нашего ПО.



Рис. 2. Найденные эксплойты

3. Запустите Metasploit. Для этого зайдите в папку `metasploit-framework\bin` и запустите файл `msfconsole.bat`.

4. Найдите эксплойт для программы Achat выполнив команду «`search achat`» (рис. 3).

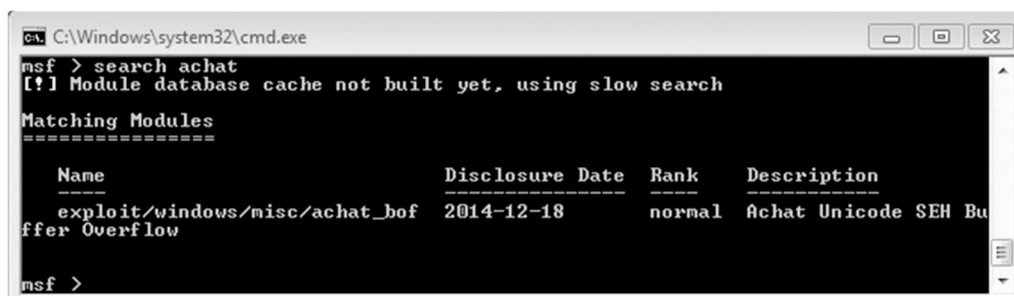


Рис. 3. Поиск эксплойта

5. Для работы с найденным эксплойтом введите команду «`use`» с названием эксплойта (рис. 4). После чего выполните команду «`info`» для вывода подробностей по уязвимости.

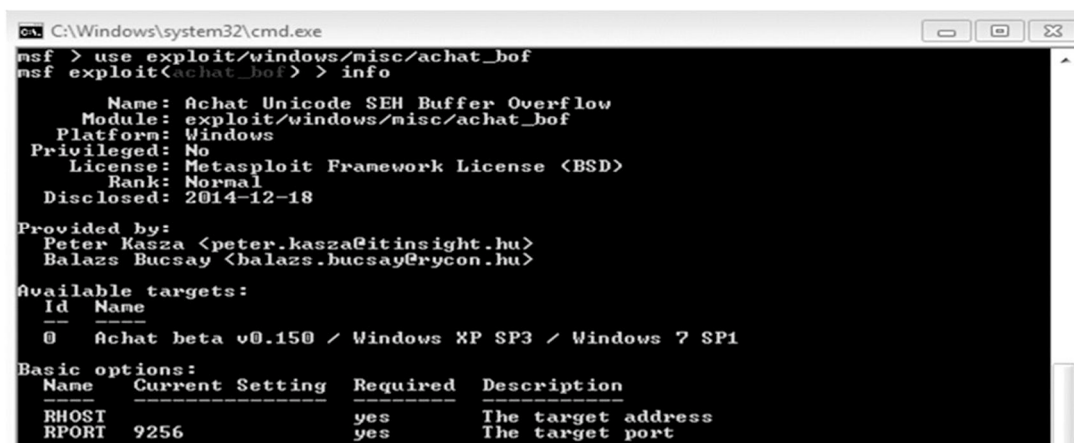


Рис. 4. Выбор эксплойта и просмотр информации по уязвимости

При просмотре информации обратите внимание на раздел Basic options, который указывает какие параметры удалённой машины необходимо задать для взлома. Некоторые из них могут быть необязательными или уже заполненными.

Чаще всего обязательными параметрами являются: RHOST – установка адреса удалённого хоста, LHOST (не указывается в info) – установка вашего локального адреса для обратной связи, PAYLOAD – полезная нагрузка. Для каждого эксплойта может быть своя нагрузка.

6. Metasploit предлагает огромный выбор полезных нагрузок, чтобы посмотреть весь список выполните команду «show payloads». В данном практикуме используется нагрузка windows/meterpreter/reverse_tcp (в случае если эксплойт не выполняется с данной нагрузкой используйте windows/shell_reverse_tcp или другую нагрузку). Первая нагрузка более универсальна и имеет множество дополнительных возможностей. Вторая нагрузка лишь даёт доступ к командной строке (cmd для Windows) для выполнения каких-либо действий с удалённой машиной.

7. Установите вышеуказанные параметры.

8. Проверить возможность взлома удалённой машины можно командой «check». Команда работает не со всеми эксплойтами.

9. После установки необходимых параметров приступите ко взлому. Для этого необходимо выполнить команду «exploit» и дождаться установления сеанса (рис. 5).

Рис. 5. Установление сеанса с удалённой машиной

В случае работы с нагрузкой meterpreter вызовите команду «help» для просмотра возможностей.

Примечание: в случае работы с полезной нагрузкой в режиме shell пропустите пункты 10–13!

10. Сделайте и получите скриншот с удалённой машины используя команду «screenshot».

11. Скачайте произвольный файл с удалённой машины, используя команду «download».

Рис. 6. Скачивание файла с удалённой машины

12. Загрузите файл с предупреждением (рис. 7) на удалённую машину, используя команду «upload».

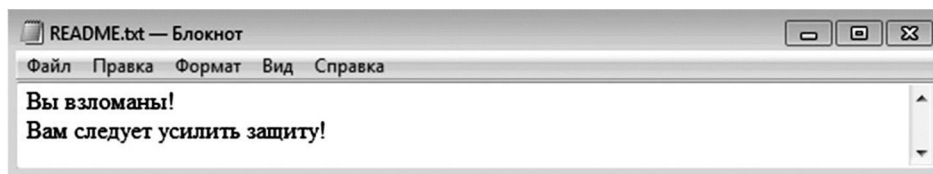


Рис. 7. Пример текстового файла с предупреждением

13. Войдите в режим командной строки используя команду «shell». В случае некорректного вывода кириллических символов попробуйте изменить кодировку командой «chcp 65001».

14. Для того чтобы убедиться, что вы находитесь на удалённой машине, выполните команду «!rconfig» для просмотра сетевых параметров системы (рис. 8).

```

C:\Windows\system32\cmd.exe
C:\Users\Asus\Desktop>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter ?????????? ?? ??????? ??:

    Connection-specific DNS Suffix  . : Dlink
    Link-local IPv6 Address . . . . . : fe80::b895:7eb8:1e91:ee0d%16
    IPv4 Address. . . . . : 192.168.0.29
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

```

Рис. 8. Просмотр сведений о сети удалённой машины

15. Перейдите на диск D:\ и выведите список файлов в текущей директории, используя команду «dir» (рис. 9).

```

C:\Windows\system32\cmd.exe
D:\>dir
dir
Volume in drive D has no label.
Volume Serial Number is EE5F-F773

Directory of D:\

30.06.2015  23:19      <DIR>          123
14.09.2015  08:05      <DIR>          2a2fc6a485213232dbf5c5
06.07.2015  15:57      <DIR>          Dropbox
24.11.2015  20:38      <DIR>          Google Диск
27.02.2015  15:35      <DIR>          Programs
24.11.2015  21:39      <DIR>          16 secret.txt
17.08.2015  14:46      <DIR>          temp
07.11.2015  23:58      <DIR>          test
08.01.2015  23:47      <DIR>          VirtualBox
23.11.2015  23:51      <DIR>          Скаченное
                1 File(s)          16 bytes
                9 Dir(s)    145 745 092 608 bytes free

D:\>

```

Рис. 9. Список файлов в текущей директории

- 16. Выведите содержимое файла secret.txt в консоль, используя команду «type».
- 17. Завершите сессию с удалённой машиной, используя команду «exit», либо комбинацию клавиш Ctrl+C.

7. Контрольные вопросы

- 1. Для чего необходимы Metasploit и Nmap?
- 2. Что такое эксплойт? Как эксплойты могут быть использованы злоумышленником?
- 3. Приведите пример средств защиты от применения эксплойтов.
- 4. Приведите пример средств защиты от сканирования Nmap.
- 5. Что такое payload, какие виды вы знаете?
- 6. Что такое пентест?
- 7. Какие виды эксплойтов вы знаете?
- 8. Что такое шелл-код?

Время выполнения лабораторной работы – 2 часа

Образовательная организация, авторы, эл. почта: Ордена трудового красного знамени Федеральное Государственное Бюджетное Образовательное Учреждение Высшего Образования «Московский Технический Университет Связи и Информатики» (МТУСИ), Костин Денис Владимирович, d.v.kostin@mail.ru

Лабораторная работа.
Исследование способов выполнения и предотвращения атак типа
ARP-spoofing и DNS-spoofing

1. Учебные цели:

Получить практические навыки реализации атак типа ARP-spoofing, DNS-spoofing и HSTS-spoofing, а также методов обнаружения и предотвращения данных типов атак.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Знать:

- стек протоколов сетевого оборудования;
- состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях;
- источники угроз информационной безопасности программного обеспечения и меры по их предотвращению.

Уметь:

- конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях;
- проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях;
- осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения.

Владеть:

- навыками выявления и устранения угроз информационной безопасности;
- формированием шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях.

3. Перечень материально-технического обеспечения:

Лабораторное оборудование и программное обеспечение Interceptor-NG (<http://sniff.su/>)

4. Задание на исследование

- Выберите бригаду – жертву, для которой вы будете злоумышленником.
- Будучи злоумышленником произведите атаку типа APR-spoofing и украдите пароль жертвы от любого сайта.
- Будучи жертвой, используя arpwatch, обнаружьте использующуюся против вас атаку типа ARP-spoofing.
- Будучи злоумышленником произведите атаку типа DNS-spoofing для перенаправления пользователя на любой сайт.
- Будучи жертвой зафиксируйте перенаправление на другой сайт.
- Поменяйтесь ролями.

5. Краткие теоретические сведения

ARP-spoofing

ARP-spoofing представляет собой атаку типа «человек посередине» в сетях, использующих протокол ARP. Данный тип атаки возможен из-за недостатков протокола ARP, который не проверяет подлинность запросов и ответов. Таким образом, протокол может принять ARP-ответ без предварительного ARP-запроса.

Проведение атаки ARP-spoofing

На рисунке 1 приведена схема атаки типа ARP-spoofing. Атака имеет следующий принцип работы:

- 1) Два узла А и В в локальной сети обмениваются сетевыми пакетами. До применения атаки ARP-spoofing на сетевом интерфейсе узла А ARP-таблица содержит IP и MAC адрес узла В, а таблица узла В содержит IP и MAC узла А.
- 2) Во время атаки ARP-spoofing узел С отправляет два ARP ответа (без запроса) – узлу А и узлу В. ARP-ответ узлу А содержит IP-адрес В и MAC-адрес С. ARP-ответ узлу В содержит IP адрес А и MAC-адрес С.

- 3) После получения ARP-ответа узлы А и В изменяют свои ARP таблицы, и теперь ARP-таблица А содержит MAC адрес С, привязанный к IP-адресу В, а ARP-таблица В содержит MAC адрес С, привязанный к IP-адресу А.
- 4) Таким образом все сетевые пакеты между А и В проходят через С. Если А хочет передать пакет компьютеру В, то А смотрит в свою ARP-таблицу, находит запись с IP-адресом узла В, выбирает оттуда MAC-адрес С и передает пакет. Пакет поступает на узел С, анализируется им, после чего перенаправляется узлу В.



Рис. 1. Схема проведения атаки ARP-spoofing

Обнаружение и предотвращение атаки ARP-spoofing

Для обнаружения данного типа атаки может быть использовано приложение *arpwatch*, которое позволяет выявлять аномалии в трафике, например, изменение MAC адреса без изменения IP адреса. Однако, *arpwatch* не предпринимает никаких активных мер, то есть для предотвращения ARP-spoofing необходимо вмешательство администратора хоста.

Для предотвращения атаки возможно использование следующих сценариев:

- Использовать статическую ARP таблицу, в которой связки IP адрес – MAC адрес прописаны вручную. К недостаткам данного подхода следует отнести большое количество рутинной работы для заполнения ARP таблицы.
- Использовать VLAN, так как атака типа ARP-spoofing возможна только если компьютеры жертвы и злоумышленника находятся в одной сети. Если атакуемый хост находится за маршрутизатором, то атаку провести невозможно, так как происходит сегментирование сетей.
- Использовать протоколы, осуществляющие шифрование данных для защиты от злоумышленника. Например, PPPoE или IPSec.

DNS-spoofing

DNS представляет собой протокол для получения IP адреса по имени хоста. Компьютер после получения ответа от DNS сервера сохраняет полученную запись в DNS кэш, который может быть повторно использован для ускорения работы и снижения нагрузки на DNS сервер.

Проведение атаки DNS-spoofing

Чтобы произвести атаку типа DNS-spoofing, злоумышленнику необходимо перехватить ответ DNS сервера жертве и подставить необходимый IP адрес, после чего отправить изменённый сетевой пакет жертве. Таким образом, в DNS кэше жертвы будет участвовать поддельная запись соответствия IP адреса доменному имени.

Interceptor-NG

Interceptor-NG представляет собой программную реализацию многих атак типа «человек посередине» с работой в графической оболочке. Программа сочетает в себе не только инструмент для проведения ARP-spoofing и DNS-spoofing, но и позволяет обнаружить атаку с помощью встроенного *arpwatch*. К особенностям работы программы следует отнести возможность подмены IP и MAC адреса атакующего, режим sniffing сетевых пакетов подобный Wireshark, автоматический анализ перехваченного трафика для извлечения паролей и другой информации, проведение атак на зашифрованный веб-трафик путём подмены сертификатов и много другое.

6. Порядок выполнения лабораторной работы

1. Запустите Interceptor-NG и выберите сетевой интерфейс для работы.
2. Войдите в Scan Mode и произведите сканирование вашей сети (рис. 2). Для этого нажмите правую кнопку мыши в пустой области и выберите режим Smart Scan.

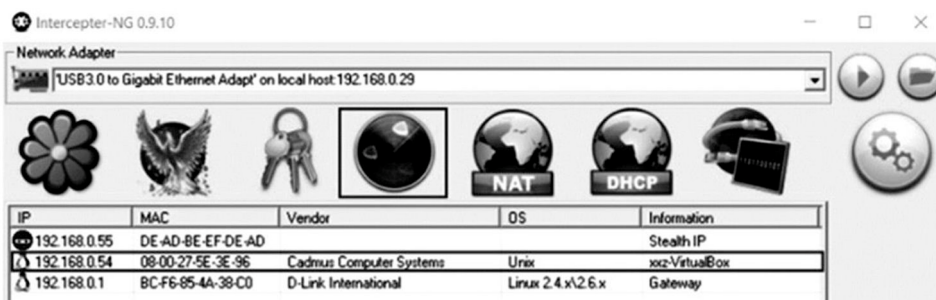


Рис. 2. Результаты сканирования в Smart Mode

После выполнения сканирования Ingercepter-NG определил IP и MAC адреса маршрутизатора (gateway) и подключенного помимо нас хоста (IP: 192.168.0.54), а также предложил IP и MAC адрес для осуществления скрытой атаки (Stealth IP).

3. Чтобы использовать найденный маршрутизатор для атаки, выделите его и используя правую кнопку мыши выберите пункт Add as Gateway.
4. Выберите жертву для атаки. Для этого выделите необходимый хост и используя правую кнопку мыши выберите пункт Add to NAT.
5. Указанные настройки позволяют вклиниться между выбранным хостом и маршрутизатором, поэтому весь трафик, поступающий из сети Интернет или других хостов на маршрутизатор и предназначенный жертве, будет проходить через нас.
6. Перейдите в режим NAT. Если поле Stealth IP не заполнено, то заполните его IP адресом с которого будет производиться атака. Обратите внимание, что адрес должен принадлежать той же сети и не должен совпадать ни с одним IP адресом хоста, найденным на шаге 2.
7. Чтобы произвести ARP-spoofing не требуются никакие дополнительные настройки. Необходимо лишь включить режим sniffing (рис. 4 (1)) и режим ARP Poison сети (рис. 4 (2)).

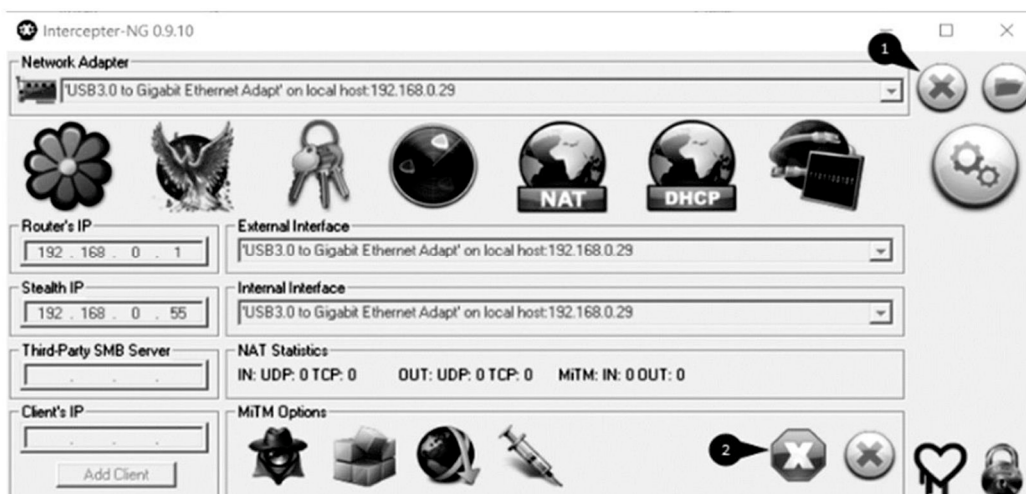


Рис. 4. Запуск ARP-spoofing

8. Перейдите в режим Password Mode чтобы посмотреть перехваченные пароли атакуемого хоста. На рисунке 5 видно, что хост посещал сайт yandex.ru и вошёл на сайт 4rda.ru по небезопасному протоколу HTTP с логином test и паролем 12345678.

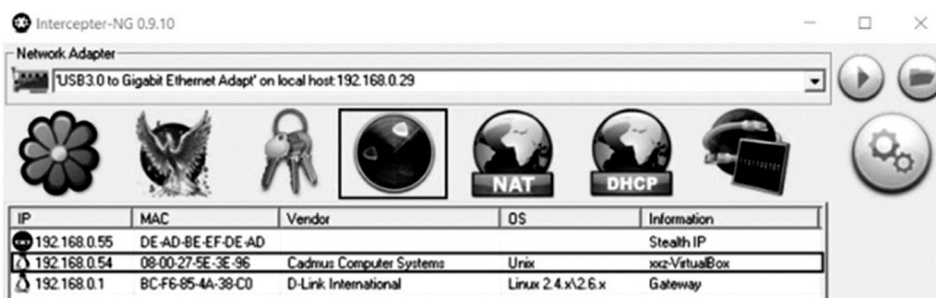


Рис. 5. Перехваченная информация в процессе атаки типа ARP-spoofing

9. На данном шаге произведём обнаружения атаки, проводящийся на наш компьютер. Для это отключите режим sniffing. Произведите повторное сканирование хостов и нажмите иконку щита справа на панели, чтобы запустить arpwatc. Перейдите в режим NAT.
10. В случае обнаружения атаки, Interceptor-NG проинформирует нас сообщением «ARP POISON DETECTED». Обратите внимание, что Interceptor-NG определил MAC адрес хоста, который производит атаку.
11. Произведём атаку типа DNS-spoofing. Для этого перезагрузите Interceptor-NG и произведите сканирование хостов в режиме Scan Mode, после чего добавьте необходимый хост и маршрутизатор в NAT.
12. С помощью командной строки и запроса nslookup «домен» определите IP адрес домена, на который необходимо перенаправлять жертву (рис. 7 (1)).
13. Войдите во вкладку NAT и произведите настройки спуфинга согласно рисунку 7 (п. 2–7).
14. Запустите sniffing и ARP Poison для проведения атаки. В случае успешного проведения атаки вы увидите сообщение о перенаправлении пользователя в Interceptor-NG.



Рис. 7. Настройки для проведения атаки типа DNS-spoofing

7. Контрольные вопросы

1. Что такое спуфинг?
2. Что такое sniffing?
3. Что такое ARP-spoofing? Как происходит атака?
4. Что такое DNG-spoofing? Как происходит атака?
5. Как защититься от ARP-spoofing?
6. Что делать, если вы заметили, что ваш DNS кэш скомпрометирован?
7. Что такое arpwatc. Как работает?

Время выполнения лабораторной работы – 2 часа

Образовательная организация, авторы, эл. почта: Ордена трудового красного знамени Федеральное Государственное Бюджетное Образовательное Учреждение Высшего Образования «Московский Технический Университет Связи и Информатики» (МТУСИ), Костин Денис Владимирович, d.v.kostin@mail.ru

Дисциплина: Моделирование процессов и систем защиты информации

Образовательная программа: 10.03.01 Информационная безопасность, Организация и технология защиты информации.

Дисциплина: Моделирование процессов и систем защиты информации.

Лабораторная работа. **Основы администрирования ПАК VipNet**

1. Учебные цели

- Изучить базовые возможности администрирования ПАК VipNet Coordinator HW.
- Отработать навыки базовой настройки ПАК VipNet Coordinator HW.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы.

Уметь:

- осуществлять выбор средств и методов моделирования для анализа защищенности систем;
- осуществлять выбор исходных данных для моделирования;
- анализировать и интерпретировать результаты эксперимента;
- проводить планирование эксперимента.

Владеть:

- подходами к организации исходных данных для моделирования;
- построением моделирующих алгоритмов;
- инструментальными средствами и языками моделирования.

3. Перечень материально-технического обеспечения

Компьютерный класс с предустановленным программным обеспечением.

4. Задания на выполнение лабораторной работы

1. Подготовить к установке операционную систему на компьютер.
2. Установить операционную систему на компьютер.
3. Установить ПАК VipNet Coordinator HW.
4. Выполнить первоначальную настройку ПАК VipNet Coordinator HW.
5. Настроить ПАК VipNet Coordinator HW для работы в защищенной сети.

5. Краткие теоретические сведения

Краткие теоретические сведения приведены в теоретической части описания лабораторной работы № 1.

6. Порядок выполнения лабораторной работы

1. Подготовить схему подключения ПАК VipNet Coordinator HW. Типовая схема приведена на рисунке.

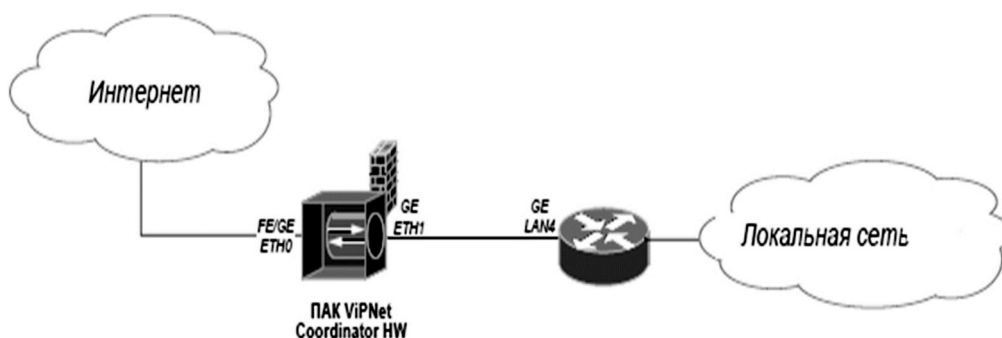


Рис. 1. Типовая схема

2. По согласованию с преподавателем записать образ ОС на USB-носитель и установить его на компьютер.
3. Установить ПАК VipNet Coordinator HW на компьютер, в соответствии с инструкцией.
4. Выполнить первоначальную настройку, в соответствии с командами мастера настроек.
5. Установить конфигурационный файл с расширением *.dst на ПАК.
6. Ввести настройки и сетевые реквизиты для подключения к сети Интернет (ip-адрес и маску подсети).

7. Ввести настройки и сетевые реквизиты для подключения к локальной сети (ip-адрес и маску подсети).
8. Перейти в режим администратора и провести тонкую настройку ПАК для работы в защищённой сети:
 - используя командную строку остановить работу службы ipIir;
 - изменить режим работы интерфейсов на указанный преподавателем;
 - используя командную строку запустить работу службы ipIir;
 - используя командную строку убедиться в доступности локальной сети и сети интернет:
 - 1) после проверки корректности настроек, выйти из режимов администратора и пользователя;
 - 2) сообщить преподавателю о готовности ПАК к дальнейшей работе.

7. Контрольные вопросы:

1. Какими способами можно записать образ ПАК ViPNet Coordinator HW на носитель информации?
2. При соблюдении каких условий установка dst-файла на ПАК ViPNet Coordinator HW пройдет успешно?
3. С помощью какой команды можно изменить системное время на ПАК ViPNet Coordinator HW?
4. Где задаются режимы безопасности на ПАК ViPNet Coordinator HW?
5. В каких режимах можно работать в командной оболочке?
6. С помощью какой команды производится настройка ViPNet-драйвера?
7. Какие из разновидностей ПАК ViPNet Coordinator HW могут работать в качестве сервера-маршрутизатора?

Время на выполнение лабораторной работы – 6 часов.

Образовательная организация, авторы, эл. почта: «Северный (Арктический) федеральный университет имени М.В. Ломоносова», Высшая школа информационных технологий и автоматизированных систем, Кафедра информатики и информационной безопасности, Васи́лишин Игорь Иванович, i.vasilishin@narfu.ru, Кунаков Олег Валерьевич, o.kunakov@narfu.ru

Дисциплина: Программно-аппаратные средства защиты информации

Образовательная программа: 10.03.01 Информационная безопасность.

Дисциплина: Программно-аппаратные средства защиты информации.

Лабораторная работа.

Установка и администрирование средства защиты информации Secret Net 7

1. Учебные цели:

- Изучить возможности средства защиты информации Secret Net 7.
- Отработать навыки по установке и администрированию средства защиты информации Secret Net 7.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь:

- устанавливать и настраивать средство защиты информации Secret Net 7;
- работать с журналом событий в программе Secret Net 7.

Владеть:

- формированием отчетов по записям журналов событий;
- фильтрованием записи журналов событий.

3. Перечень материально-технического обеспечения. Лабораторное оборудование и программное обеспечение:

- операционная система не ниже Windows 7;
- операционная система MS Windows Server 2003 или другая сетевая операционная система;
- эмуляция виртуальных машин (VM-vare, VM-box или др.);
- автоматизированное рабочее место преподавателя (1 шт.);
- автоматизированные рабочие места студентов (11 шт.);
- средство защиты информации Secret Net 7.

4. Задание на исследование

- установка средства защиты информации Secret Net 7;
- отработка навыков настройки средства защиты информации Secret Net 7;
- проверка наличия в журнале средства защиты информации Secret Net 7 событий входа пользователей в систему;
- изучение компонентов средства защиты информации Secret Net 7.

5. Краткие теоретические сведения

Общие принципы управления

В системе Secret Net информационная безопасность компьютеров обеспечивается механизмами защиты. Механизм защиты – совокупность настраиваемых программных средств, разграничивающих доступ к информационным ресурсам, а также осуществляющих контроль действий пользователей и регистрацию событий, связанных с информационной безопасностью.

Функции администратора безопасности

Основными функциями администратора безопасности являются:

- настройка механизмов защиты, гарантирующая требуемый уровень безопасности ресурсов компьютеров;
- контроль выполняемых пользователями действий с целью предотвращения нарушений информационной безопасности.

Функциональные возможности Secret Net позволяют администратору безопасности решать следующие задачи:

- усилить защиту от несанкционированного входа в систему;
- разграничить доступ пользователей к информационным ресурсам на основе;
- принципов избирательного и полномочного управления доступом
- замкнутой программной среды;
- контролировать и предотвращать несанкционированное изменение целостности ресурсов;

- контролировать вывод документов на печать;
- контролировать аппаратную конфигурацию защищаемых компьютеров и предотвращать попытки ее несанкционированного изменения;
- загружать системные журналы для просмотра сведений о событиях, произошедших на защищаемых компьютерах;
- не допускать восстановление информации, содержащейся в удаленных файлах;
- управлять доступом пользователей к сетевым интерфейсам компьютеров.

Для решения перечисленных и других задач администратор безопасности использует средства системы Secret Net и ОС (операционной системы) Windows.

Организация управления системой защиты

В автономном режиме функционирования системы Secret Net доступны только локальные функции управления системой.

В сетевом режиме функционирования доступны возможности как локального, так и централизованного управления системой защиты, применяются принципы сетевого администрирования с использованием механизма групповых политик и делегирования административных полномочий.

Централизованное и локальное управление

Локальное управление – это управление работой механизмов защиты отдельного компьютера, которое осуществляется администратором безопасности непосредственно на компьютере. Локальное управление используется в тех случаях, когда возможности централизованного управления для отдельного компьютера недоступны или нецелесообразны. Например, локальное управление применяется, если требуется обеспечить безопасную работу локальных пользователей компьютера. Программные средства для локального управления установлены по умолчанию и могут использоваться пользователями, входящими в локальную группу администраторов компьютера.

Централизованное управление параметрами Secret Net осуществляется администратором безопасности со своего рабочего места. Для этих целей может использоваться любой компьютер сети с установленными средствами централизованного управления.

В соответствии с концепцией Secret Net управление безопасностью в защищаемом домене рекомендуется осуществлять централизованно. Централизованное управление имеет приоритет перед локальным управлением. Например, если в групповой политике некоторые параметры заданы централизованно, то локально на компьютере их изменить нельзя. В качестве средств централизованного управления параметрами групповых политик и параметрами доменных пользователей могут использоваться:

- стандартные средства централизованного управления ОС Windows;
- средства, входящие в состав ПО (программного обеспечения) системы Secret Net: программа оперативного управления и программа управления пользователями.

Средства управления параметрами групповых политик и параметрами доменных пользователей можно использовать по отдельности (только стандартные средства Windows или только средства системы Secret Net) или комбинированно.

Для централизованного управления параметрами механизмов контроля целостности и замкнутой программной среды используется программа "Контроль программ и данных" в централизованном режиме работы. Программа входит в состав ПО системы Secret Net.

Ниже представлены общие сведения о развертывании средств централизованного управления на рабочем месте администратора безопасности.

Средства централизованного управления системы Secret Net

Для использования средств централизованного управления, входящих в состав ПО системы Secret Net, на компьютере администратора должны быть установлены следующие компоненты:

- компонент "Secret Net 7" в сетевом режиме функционирования (при установке необходимо включить)
- параметр "установить средства централизованной настройки";
- компонент "Secret Net 7 – Программа управления".

Использование групповых политик

В сетевом режиме функционирования системы Secret Net для централизованной настройки и применения параметров безопасности на защищаемых компьютерах могут использоваться групповые политики. Заданные параметры объектов групповых политик хранятся в Active Directory и применяются без учета значений, указанных для тех же параметров в локальной политике безопасности компьютера.

Параметры системы Secret Net могут быть заданы в групповых политиках домена, организационного подразделения и сервера безопасности.

Соответственно эти параметры будут применяться на компьютерах, входящих в домен, включенных в организационное подразделение или подчиненных серверу безопасности. При этом действуют приоритеты применения групповых политик. Наименьший приоритет имеют параметры политики безопасности домена, заданные в стандартных оснастках ОС Windows. Эти параметры применяются на компьютерах домена, если отсутствуют другие значения в групповых политиках более высокого уровня.

В системе Secret Net могут использоваться следующие групповые политики в порядке возрастания приоритета применения параметров:

- политика безопасности домена, заданная в стандартных оснастках ОС Windows;
- политика организационного подразделения, заданная в стандартных оснастках ОС Windows, – для всех компьютеров, входящих в это организационное подразделение;
- политика домена, заданная в программе оперативного управления системы Secret Net;
- политика организационного подразделения, заданная в программе оперативного управления системы Secret Net, – для всех компьютеров, входящих в это организационное подразделение;
- политика, заданная для сервера безопасности в программе оперативного управления системы Secret Net, – применяется на всех компьютерах, подчиненных этому серверу безопасности.

За счет использования разных групповых политик можно реализовать централизованное управление параметрами с учетом особенностей информационной системы. Например, можно настроить общие параметры для всех компьютеров в политике домена и дополнительно указать значения отдельных параметров в политиках организационных подразделений. Это позволит применять на компьютерах различных организационных подразделений единые общие параметры и при этом задать специфические значения для компьютеров отдельных подразделений.

Обновление групповых политик

Параметры групповых политик на защищаемых компьютерах обновляются автоматически, в соответствии с действием механизма применения политик ОС Windows. При необходимости администратор может использовать средства принудительного обновления политик, чтобы ускорить процесс применения централизованно заданных параметров на компьютерах.

Принудительное обновление групповых политик можно осуществлять с помощью следующих средств:

- команда применения групповых политик в программе оперативного управления;
- стандартные инструменты командной строки gpupdate и secedit.

После обновления политик может потребоваться перезапуск компьютера или завершение текущего сеанса работы пользователя – чтобы применить параметры, которые действуют только при загрузке ОС или при входе пользователя в систему. Для этого предусмотрены специальные возможности как в программе оперативного управления (команды для перезагрузки или выключения компьютера), так и в указанных инструментах командной строки.

Делегирование административных полномочий

В сетевом режиме функционирования системы Secret Net можно делегировать полномочия для администратора безопасности. Делегирование подразумевает возложение некоторых функций по настройке и управлению работой механизмов защиты на пользователей, не являющихся членами доменной группы администраторов. При этом настройка и управление будут осуществляться только в рамках определенных организационных подразделений, созданных внутри домена.

Ниже приводится порядок действий для делегирования административных полномочий. Процедуру делегирования следует выполнять в случае, если хранилище объектов централизованного управления Secret Net размещается в базе данных доменных служб Active Directory. Если хранилище объектов размещается вне AD – достаточно включить администратора безопасности в доменную группу Group Policy Creator Owners.

Порядок действий для делегирования полномочий:

1. Используя стандартные средства ОС, создайте в Active Directory структуру организационных подразделений.
2. Пользователям, уполномоченным настраивать механизмы защиты в рамках организационного подразделения, предоставьте полные права на управление объектами, входящими в подразделение, и групповыми политиками подразделения.

В результате такие пользователи получают возможность:

- управлять объектами "Пользователь" и "Компьютер", входящими в соответствующее организационное подразделение;
- в стандартных оснастках ОС Windows создавать, редактировать и удалять групповые политики, назначенные для данного подразделения (обязательным условием является включение пользователя в группу Group Policy Creator Owners).

3. Включите пользователя, которому делегированы права на управление объектами организационного подразделения, в группу SecretNetAdmins.

Параметры механизмов защиты и средства управления

Параметры механизмов защиты Secret Net в зависимости от места их хранения в системе и способа доступа к ним можно разделить на следующие группы:

- параметры объектов групповой политики;
- параметры пользователей;
- атрибуты ресурсов;
- параметры механизмов контроля целостности (КИ) и замкнутой программной среды (ЗПС).

Ниже представлены разделы с общими сведениями о работе с перечисленными параметрами в соответствующих программных средствах.

Параметры объектов групповой политики

К общим параметрам безопасности ОС Windows добавляются параметры Secret Net. Эти параметры применяются на компьютере средствами групповых политик и действуют в рамках локальной политики безопасности (в автономном режиме функционирования системы защиты) или как объединение параметров локальной политики с политиками более высокого уровня (в сетевом режиме функционирования).

В системе Secret Net предусмотрены возможности настройки параметров групповых политик в стандартных оснастках ОС Windows и в программе оперативного управления.

6. Порядок выполнения лабораторной работы (этапы)

- 1) установить программу Secret Net 7 с CD-диска;
- 2) освоить интерфейс программы Secret Net 7;
- 3) рассмотреть основные возможности управления системой защиты информации при помощи программы Secret Net 7;
- 4) просмотреть записи журналов регистрации событий;
- 5) сформировать отчет по просмотренным записям событий;
- 6) ВКЛЮЧИТЬ в отчет о лабораторной работе ответы на контрольные вопросы.

7. Контрольные вопросы:

1. Назовите основные компоненты средства защиты информации Secret Net 7.
2. Как сформировать отчет по записям журнала регистраций событий?
3. Как произвести фильтрацию записей журналов событий?
4. В чем особенность централизованного управления системой защиты?
5. Назовите основные виды групповых политик, доступных в Secret Net

Время на выполнение лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: Московский государственный областной технологический университет, к.т.н. Журавлев С.И., Zhuravlev_2007@mail.ru

Образовательная программа: 10.03.01 Информационная безопасность.

Дисциплина: Программно-аппаратные средства защиты информации.

Лабораторная работа. Инициализация Криптографического Шлюза (КШ)

1. Учебные цели:

- Изучить основы функционирования сети КШ «Континент»;
- Получить навыки ввода в эксплуатацию КШ.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

В результате освоения дисциплины бакалавр должен:

Знать:

- современные аппаратные средства защиты систем ЭВМ на примере КШ «Континент»;
- методы защиты передаваемой информации в сетях ЭВМ;
- современные методы разграничения доступа в компьютерных системах на примере КШ «Континент».

Уметь:

- использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникших в ходе профессиональной деятельности;
- использовать нормативные правовые документы в своей профессиональной деятельности;
- оценивать угрозы системе ЭВМ;
- строить эффективные и экономически выгодные системы защиты ЭВМ и сети ЭВМ на примере КШ «Континент».

Владеть:

- навыками самостоятельной программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности на примере КШ «Континент»;
- навыками выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации на примере КШ «Континент».

3. Перечень материально-технического обеспечения:

Выполнение работы возможно на виртуальном стенде, установленном на Персональном Компьютере (ПК) или на стенде, включающем компоненты Аппаратно-Программного Комплекса Шифрования (АПКШ) «Континент» версии 3.7:

- Виртуальный лабораторный стенд в составе 4 виртуальных машин: Автоматизированное Рабочее Место (АРМ) администратора, Виртуальная Машина (ВМ) с ЦУС, ВМ с КШ, виртуальный маршрутизатор.
- АПКШ Континент 3.7 ЦУС Платформа IPC25, АПКШ Континент 3.7 КШ Платформа IPC25, ПК с установленным ПО ПУ ЦУС «Континент», маршрутизатор.

4. Задание на исследование:

Установить ПО КШ, настроить сетевое взаимодействие КШ с ЦУС, подключить КШ к ЦУС.

- Строка конфигурации КШ: «000000025em0*02BDem1*02BDem2*02BDem3*02BDem4*02BDffff»
- Сетевой интерфейс «em0»: IP адрес 216.115.92.1/24
- Сетевой интерфейс «em2»: IP адрес 10.0.2.1/24
- Маршрутизация по умолчанию: 0.0.0.0/0 шлюз 216.115.92.254

5. Краткие теоретические сведения:**Порядок ввода комплекса в эксплуатацию**

Ввод комплекса в эксплуатацию осуществляют в следующем порядке:

1. Инициализация и подключение ЦУС.
2. Инициализация и настройка параметров Программно-Аппаратного Комплекса (ПАК) «Соболь» на АРМ администратора комплекса.
3. Установка подсистемы управления.
4. Постановка на контроль программных модулей, подлежащих контролю целостности.
5. Конфигурирование базы данных журналов.
6. Запуск подсистемы управления и выбор режима управления ключевой информацией.
7. Настройка агента.
8. Регистрация сетевых устройств, входящих в комплекс.
9. Запись конфигураций сетевых устройств на отчуждаемые носители.

В АПКШ «Континент» конфигурация КШ представляет собой файл с именем «gate.cfg», который содержит информацию о сетевых параметрах устройства. Ключ КШ – файл с именем «keyset» – содержит главный ключ КШ и ключ связи с ЦУС. Последний необходим для установки защищенного соединения КШ с ЦУС. Формирование файлов с конфигурацией КШ и с ключом КШ производится в ПУ ЦУС (на ВМ ARM).

1. Запись ключей сетевых устройств на отчуждаемые носители.

В зависимости от выбранного на этапе 6 режима управления ключевой информацией запись ключей выполняют в соответствии с одной из следующих схем: базовая схема. Ключи сетевого устройства, сгенерированные при его регистрации, записывают на USB-флеш-накопитель в Программу Управления (ПУ) ЦУС; усиленная схема. На автоматизированном рабочем месте генерации ключей изготавливают ключи сетевого устройства при выпуске серии ключевых документов и записывают на USB-ключи Rutoken ЭЦП.

2. Инициализация и подключение зарегистрированных сетевых устройств.
3. Ввод в эксплуатацию инициализированных сетевых устройств.
4. Настройка комплекса.

Если на пути зашифрованного трафика находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов, необходимо создать для них правила, разрешающие прохождение служебных пакетов комплекса.

Краткое описание стенда:

Для выполнения лабораторных работ следует использовать специально подготовленный лабораторный стенд из 8 виртуальных машин, которые распределены по нескольким подсетям, как показано на рисунке 1.

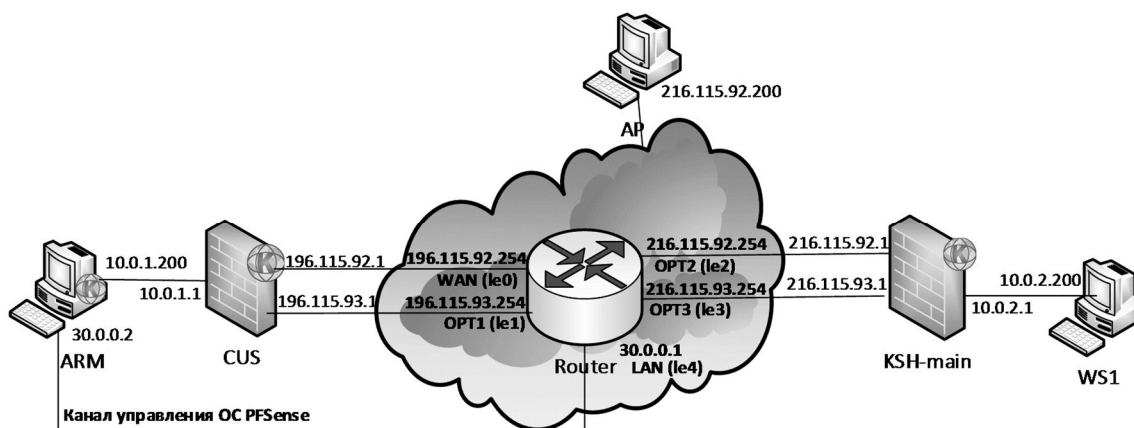


Рис. 1. Схема виртуального стенда «Континент»

Стенд содержит следующие виртуальные локальные подсети:

- 10.0.1.X/24 – имитирует внутреннюю / защищаемую сеть организации;
- 196.115.92.X/24 и 196.115.93.X/24 – имитируют внешние сети организации;
- 216.115.92.X/24 и 216.115.93.X/24 – имитируют внешние сети филиала;
- 10.0.2.X/24 – имитирует внутреннюю / защищаемую сеть филиала;
- 196.168.169.X/30 – подсеть для резервирования КШ.

Описание всех VM стенда:

VM Router выполняет функции роутера. VM CUS выполняет функции ЦУС, на котором установлено ПО криптографического шлюза с центром управления сетью «Континент». VM ARM предназначена для рабочего места администратора Аппаратно-Программного Комплекса Шифрования (АПКШ) «Континент» с установленными программой управления ЦУС, программой просмотра журналов и пр. VM KSH-main предназначена для установки ПО основного криптографического шлюза «Континент». VM AP выполняет роль удаленного компьютера, с которого будет выполняться подключение к защищаемой сети. VM WS1 выполняет роль компьютера в защищаемой сети.

6. Порядок выполнения лабораторной работы:

1. Включить VM с КШ и дождаться появления предложения предъявить съемный диск с конфигурацией и ключами КШ.
2. Перейти на VM с АРМ администратора и подключить к ней USB-флеш-накопитель с ключом администратора ЦУС. Для того чтобы получить файл конфигурации и ключевой файл для КШ, в окне ПУ ЦУС необходимо зарегистрировать этот КШ. Для этого в левой части окна нужно выбрать папку «Сетевые устройства Континент / Криптошлюзы», вызвать контекстное меню «Криптошлюзы» и выбрать опцию «Создать криптошлюз».
3. После появления окна «Создание криптошлюза» необходимо заполнить поля «Название» – KSH_main, «Строка конфигурации» – 000000025em0*02BDem1*02BDem2*02BDem3*02BDem4*02BDffff, указать часовой пояс.

Состав строки конфигурации:

- 00000002 – идентификатор криптошлюза в шестнадцатеричной системе;
 - 5 – количество сетевых интерфейсов КШ;
 - em0, em1, ..., em4 – названия сетевых интерфейсов (условные в FreeBSD);
 - *02BD – режим работы сетевого интерфейса (автовыбор);
 - ffff – условное обозначение окончания строки конфигурации.
4. Далее необходимо убедиться в наличии отметки «Продолжить настройку параметров созданного криптошлюза в окне свойств» и нажать кнопку «ОК».
 5. В появившемся окне «Свойства криптошлюза» необходимо выбрать вкладку «Интерфейсы» и установить адреса для интерфейсов em0, em2 и маршрутизацию по умолчанию.

6. После задания основных параметров КШ появится в ПУ ЦУС на вкладке «Криптошлюзы» в состоянии «Включен: НЕТ; Введен в эксплуатацию: НЕТ».
7. Далее необходимо создать на USB-флеш накопителе файлы конфигурации и ключей. В окне ПУ ЦУС нужно вызвать контекстное меню зарегистрированного КШ и выбрать опцию «Сохранить конфигурацию КШ», указать в открывшемся окне пароль (11111), который будет запрошен при считывании информации, и USB-флеш накопитель, на который будет сохранена конфигурация. Аналогичным образом нужно записать ключевую информацию через пункт «Сохранить текущий комплект ключей на носитель».
8. Затем необходимо переключиться на ВМ с КШ и подключить к нему носитель с созданными ключами. При считывании информации с USB-флеш накопителя будет запрошен пароль, заданный ранее в пункте 8. Необходимо считать и установить настройки из файла и новый (созданный и записанный на накопитель) ключ, следуя указаниям программы.
9. После установки конфигурации и ключа проинициализированное устройство необходимо ввести в эксплуатацию в ПУ ЦУС. На ВМ с АРМ администратора необходимо в ПУ ЦУС открыть свойства КШ KSH_main и во вкладке «Общие сведения» установить галочку на пункте «Введен в эксплуатацию», нажать «ОК». В завершение необходимо убедиться, что КШ KSH_main в ПУ ЦУС сменил статус на «Включен: ДА; Введен в эксплуатацию: ДА». Также стали доступны опции управления, например, удаленная перезагрузка.

7. Контрольные вопросы:

1. Какие функции выполняют программные модули – КШ, ЦУС, СД, КК, ДА, АП АПКШ «Континент»?
2. Что означает число 7 в строке конфигурации КШ 00000074em0*02BDem1*02BDem2*02BDem3*02BDfff?
3. Можно ли установить и использовать одновременно программу управления комплексом на нескольких компьютерах?
4. Как осуществляется журналирование событий в АПКШ «Континент»?
5. Какое число нужно вводить в качестве номера КШ при инициализации, если он должен иметь следующую строку инициализации: 000000E4em0*02BDem1*02BDem2*02BDem3*02BDfff?
6. Как будет работать КШ, если в его свойствах не активировать команду «Введен в эксплуатацию»?

Время выполнения лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: Московский Технический Университет Связи и Информатики (МТУСИ), Пугачев Д.А. инженер кафедры «Информационная безопасность, эл. почта: 16pda16@mail.ru

Образовательная программа: 10.03.01 Информационная безопасность.

Дисциплина: Программно-аппаратные средства защиты информации.

Лабораторная работа.

Настройка правил фильтрации в сети Криптографических Шлюзов (КШ)

1. Учебные цели:

Изучить принципы межсетевого экранирования, уметь устанавливать правила фильтрации IP пакетов в АПКШ «Континент», современные аппаратные средства защиты систем ЭВМ и методы разграничения доступа в компьютерных системах. Приобрести навыки организации и проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

В результате освоения дисциплины «Программно-аппаратные средства защиты информации» студенты должны:

Знать:

- принципы функционирования Межсетевого Экрана (МЭ) в АПКШ «Континент»;
- современные аппаратные средства защиты систем ЭВМ и методы разграничения доступа в компьютерных системах на примере КШ «Континент»;

Уметь:

- использовать принципы функционирования Межсетевого Экрана (МЭ) в АПКШ «Континент»;
- строить эффективные и экономически выгодные системы защиты ЭВМ и сети ЭВМ на примере КШ «Континент»;

Владеть:

- навыками настройки правил фильтрации на примере КШ «Континент»;
- программными средствами системного, прикладного и специального назначения на примере КШ «Континент»;
- навыками настройки и обслуживания технических и программно-аппаратных средств защиты информации на примере КШ «Континент».

3. Перечень материально-технического обеспечения:

Выполнение работы возможно на виртуальном стенде, установленном на Персональном Компьютере (ПК) или на стенде, включающем компоненты Аппаратно-Программного Комплекса Шифрования (АПКШ) «Континент» версии 3.7:

- Виртуальный лабораторный стенд в составе 6 виртуальных машин: Автоматизированное Рабочее Место (АРМ) администратора, Виртуальная Машина (ВМ) с ЦУС, ВМ с КШ, виртуальный маршрутизатор, ВМ с АРМ пользователя (в подсети КШ), ВМ во внешней сети (ВМ AP).
- АПКШ Континент 3.7 ЦУС Платформа IPC25, АПКШ Континент 3.7 КШ Платформа IPC25, ПК с установленным ПО ПУ ЦУС «Континент», маршрутизатор, 2 предварительно настроенных ПК.

4. Задание на исследование:

Настроить правила фильтрации, позволяющие прохождение сетевого трафика между компьютерами в защищаемой сети и внешней сети и между компьютерами во внутренних сетях разных КШ.

5. Краткие теоретические сведения:

В АПКШ «Континент» в качестве Межсетевого Экрана (МЭ) используется встроенный в FreeBSD межсетевой экран OpenBSD PacketFilter для выполнения следующих задач:

- защита и изоляция пользователей внутренней сети от нежелательного трафика, поступающего из внешней сети Интернет;
- ограничение или запрещение доступа пользователей внутренней сети к сервисам внешней сети;
- обеспечение отказоустойчивости канала связи;
- выполнение приоритезации трафика (QoS);
- поддержка преобразования сетевых адресов (Network Address Translation, NAT), что дает возможность задействовать во внутренней сети локальные IP-адреса и совместно использовать одно подключение к сети Интернет (либо через один выделенный IP-адрес, либо через адрес из пула автоматически присваиваемых публичных адресов).

Схема фильтрации трафика в АПКШ «Континент» показана на рисунке 1 совместно для входящего и исходящего интерфейсов.

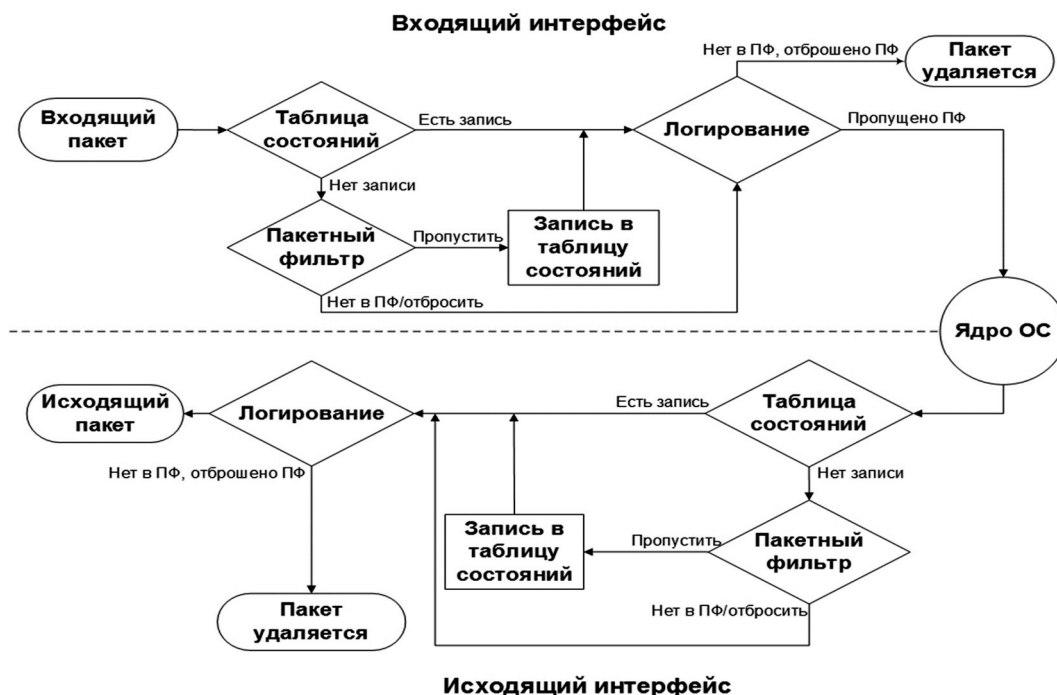


Рис. 1. Правила фильтрации пакетов в АПКШ «Континент» с включенным контролем состояния соединений

МЭ выполняет фильтрацию входящего и исходящего трафика, идущего через КШ, при этом фильтрация сетевого пакета выполняется дважды – на входящем и исходящем сетевом интерфейсе. МЭ функционирует на 3 уровне модели OSI. Реализация проверки сетевых пакетов обеспечивается с помощью набора правил. Правила фильтрации формируются на основе IP-адресов отправителя и получателя, типов протоколов IP, сервисов. МЭ позволяет контролировать прохождение трафика или блокирует его.

МЭ поддерживает технологию контроля состояния соединений (Stateful Packet Inspection, SPI). МЭ при включенной функции SPI для каждого установленного соединения сохраняет определенную информацию (адрес отправителя, адрес получателя, номера портов) в динамической таблице состояния соединений. При прохождении пакета через криптошлюз МЭ определяет, принадлежит ли данный пакет установленному соединению. Если информация о нем есть в таблице состояния соединений – пакет пропускается, минуя правила фильтрации.

Технология контроля состояния соединений повышает производительность МЭ. При включенной функции SPI написание правил фильтрации, разрешающих прохождение трафика в обратном направлении, не требуется. Например, браузер из доверенной сети соединяется с сервером в Интернете, разрешение для прохождения исходящего трафика администратор указывает явно правилом. Запрос от браузера поступает на сервер, МЭ устанавливает соединение, означающее ожидание данных с сервера.

При написании правила, разрешающего прохождение исходящего трафика без SPI, запрос от браузера на сервер поступит, а ответ от него МЭ заблокирует. Вот для чего необходимо включение функции SPI. Таблица состояния соединений поддерживается динамически.

Обработка IP-пакетов осуществляется криптографическими шлюзами и зависит от статуса абонента сети (компьютера, отправляющего или получающего IP-пакеты) по отношению к данному КШ:

- внутренний абонент – входит в состав сегмента сети, защищаемого данным КШ;
- внешний абонент – относится к сегменту сети, защищаемому любым другим (отличным от данного) КШ комплекса;
- сторонний абонент – любой абонент IP-сети, не входящий в состав защищаемых сегментов.

Все IP-пакеты, проходящие через КШ, подвергаются фильтрации в соответствии с правилами, сформированными на основе IP-адресов отправителя и получателя, названия протокола, номеров портов UDP/TCP и имен сетевых интерфейсов. Проверяются также время, факт аутентификации (для защищаемого сегмента), а при фильтрации прикладных протоколов – содержимое пакетов. По умолчанию прохождение любого IP-пакета запрещено, если это не разрешено явно соответствующим правилом фильтрации.

Если пакет не удовлетворяет установленным правилам фильтрации, он отбрасывается без уведомления отправителя.

Правила фильтрации IP-пакетов подразделяются на два типа: правила, сформированные комплексом автоматически; правила, заданные администратором. Автоматическое формирование правил фильтрации для данного КШ осуществляется при инициализации ЦУС и КШ. Правила этого типа не отображаются на экране и не могут быть удалены или изменены администратором.

Правила, сформированные комплексом автоматически, разрешают соединения: ЦУС с программой управления и агентом; ЦУС с зарегистрированными сетевыми устройствами; между двумя КШ (КК), имеющими парную связь, для служебных пакетов проверки связи между ними; основного и резервного КШ.

Для всех остальных соединений в рамках корпоративной сети правила фильтрации формирует администратор.

При создании администратором правил фильтрации и трансляции комплекс автоматически формирует набор правил, которые администратор не видит и не может изменить.

В комплексе предусмотрены два режима работы пакетного фильтра:

- основной – IP-пакеты, прохождение которых не разрешено, отбрасываются с регистрацией этого события в журнале НСД;
- мягкий – IP-пакеты, прохождение которых не разрешено, только регистрируются в журнале НСД, но пропускаются фильтром. Данный режим предназначен только для настройки КШ при вводе его в эксплуатацию.

6. Порядок выполнения лабораторной работы:

1. В ПУ ЦУС необходимо создать сетевой объект ARM с IP адресом 10.0.1.200/32, типом привязки «Внутренний», криптошлюзом КШ с ЦУС, интерфейсом em2
2. Далее необходимо создать правило фильтрации с названием «from AP to ARM», отправителем «Любой», получателем «ARM», сервисами «http», действием «Пропустить» и включенными контролем состояния соединений и пунктом «Применить и завершить обработку».
3. Для применения и выполнения новых правил необходимо на панели инструментов нажать «Сохранить изменения». Таким образом, правила будут сохранены в БД и переданы на соответствующий КШ.
4. Далее нужно найти созданные правила в конфигурации самого КШ. Для этого на ВМ с ЦУС нужно открыть консоль сочетанием клавиш Alt+F2 и выбрать пункт «Список правил фильтрации».
5. Далее необходимо в браузере на ВМ AP открыть адрес <http://10.0.1.200/test1.txt>. Если написанное правило функционирует, то можно прочитать соответствующее сообщение.

6. Затем нужно просмотреть таблицу соединений в консоли КШ с ЦУС, выбрав пункт «Просмотр таблицы состояний».
7. Для дальнейшей работы необходимо отключить созданное правило фильтрации в ПУ ЦУС и применить изменения, используя кнопку «Сохранить изменения».
8. Далее необходимо создать сетевой объект WS1 с IP адресом 10.0.2.200/32, типом привязки «Внутренний», криптошлюзом «KSH_main» и интерфейсом em2.
9. Затем нужно описать правило фильтрации «from WS1 to ARM» с отправителем «WS1», получателем «ARM», сервисом «http», действием «пропустить», включенным контролем состояния соединений и включенным пунктом «Применить и завершить обработку».
10. Аналогично пункту 4 необходимо просмотреть созданные правила на КШ.
11. Далее необходимо в браузере на ВМ WS1 открыть адрес <http://10.0.1.200/test2.txt>. Если написанное правило функционирует, то можно прочитать соответствующее сообщение.
12. В завершение необходимо отключить созданное правило аналогично пункту 7.

7. Контрольные вопросы:

1. Для чего предназначена технология «Контроль состояния соединений» в пакетном фильтре, применяемом в АПКШ «Континент»?
2. Благодаря какой технологии межсетевой экран предотвращает атаки, блокирующие доступ пользователей к ресурсам VPN?
3. Что происходит с IP-пакетами, если по правилам фильтрации их прохождение запрещено, а межсетевой экран установлен в мягком режиме?
4. Какой из трех типов привязки к КШ – «защищаемый», «внутренний», «без привязки» – должен иметь сетевой объект, чтобы на него распространялось правило фильтрации?

Время выполнения лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: Московский Технический Университет Связи и Информатики (МТУСИ), Пугачев Д.А. инженер кафедры «Информационная безопасность», 16rda16@mail.ru

Образовательная программа: 10.03.01 Информационная безопасность, Комплексная защита объектов информатизации, Техническая защита информации.

Дисциплина: Программно-аппаратные средства защиты информации.

Лабораторная работа.

Организация изолированных пользовательских сред

1. Учебные цели:

Изучение особенностей и отработка навыков настройки замкнутой программной среды (ЗПС) в средствах защиты информации (СЗИ) от несанкционированного доступа (НСД) «SecretNet 7.7» – автономный и «DallasLock 8.0-С».

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь:

- квалифицированно оценивать область применения конкретных механизмов защиты;
- подбирать под необходимые задачи, осваивать и внедрять распространенные средства защиты информации;
- интегрировать средства защиты информации в имеющиеся компьютерные системы и сети организации, а также обеспечивать их использование совместно с иными применяемыми средствами и системами защиты;
- тестировать эффективность функционирования применяемых средств защиты информации;

Владеть:

- профессиональной терминологией в предметной области;
- навыками работы с различными программными средами, оболочками и интерфейсами;
- навыками настройки распространенных программных и программно-аппаратных средств защиты информации;
- навыками централизованного управления применяемыми средствами защиты информации.

3. Перечень материально-технического обеспечения

Лабораторные работы выполняются на гостевой операционной системе в среде виртуализации VMware Workstation Player или Oracle VM VirtualBox. Для выполнения необходимы операционные системы (ОС) Windows 7 SP1 редакции Professional или Enterprise, на любой архитектуре (32-бит, 64-бит), Windows Server 2008R2, Windows Server 2012R2.

Для выполнения лабораторных работ необходимо программное обеспечение (ПО) «SecretNet 7.7» и «DallasLock 8.0-C», а также документация к данному ПО.

4. Задание на исследование

Задание № 1. Провести настройку замкнутой программной среды в СЗИ от НСД «SecretNet 7.7»

Задание № 2. Провести настройку замкнутой программной среды в СЗИ от НСД «DallasLock 8.0-C»

5. Краткие теоретические сведения

Начальная моделируемая инфраструктура для задания № 1:

Клиентский компьютер COMP (ОС Windows 7 SP1 и выше) без подключения к домену. На компьютере присутствует только локальный пользователь Администратор. Политики безопасности операционной системы имеют настройки по умолчанию.

Инструкция по настройке механизма замкнутой программной среды средством защиты информации Secret Net 7.7:

1. Запустите программу управления в локальном режиме. Для этого выберите элемент "Контроль программ и данных" в списке программ.

2. Сформируйте новую модель данных (фрагмент модели) с настройкой контроля по умолчанию.

Для этого выберите команду "Файл | Новая модель данных". В появившемся диалоге настройте параметры для режима замкнутой программной среды:

- отметьте представленные стандартные задачи для ОС и СЗИ;
- оставьте отмеченным поле "Производить подготовку для ЗПС";
- установите отметку в поле "Добавить другие задачи из списка" и нажмите кнопку для выбора задач. В появившемся диалоге выберите в списке элементы, необходимые для работы любого пользователя компьютера. Список содержит установленные на компьютере программы, представленные в меню "Пуск". Для выбора нескольких элементов используйте клавиши <Ctrl> или <Shift>;
- оставьте отмеченным поле "Рассчитывать эталоны";
- если модель данных содержит ранее сконфигурированные объекты, которые нужно сохранить в новой модели – удалите отметку из поля "Предварительная очистка модели данных".

3. Нажмите кнопку "ОК". При появлении диалога запроса на продолжение операции нажмите кнопку "Да". По окончании процесса формирования модели данных в списке заданий появится задание ЗПС, которое будет применяться для всех пользователей группы Users и блокировать запуск программ, не включенных в список ресурсов задания.

4. Для проверки и дополнительной настройки механизма ЗПС включите мягкий режим работы механизма. Для этого выберите категорию "Субъекты управления", вызовите диалоговое окно настройки свойств компьютера и в диалоге "Режимы" установите отметки в полях "Режим ЗПС включен" и "Мягкий режим".

5. Закройте программу управления с сохранением сделанных изменений и выполните вход в систему с учетными данными пользователя компьютера. В пользовательском сеансе выполните запуск всех приложений, которые необходимы пользователю для исполнения функциональных обязанностей.

6. Завершите сеанс работы пользователя, войдите в систему с учетными данными администратора и снова запустите программу управления.

7. Добавьте в модель данных группы ресурсов, в которых будут представлены ресурсы, необходимые для работы пользователя. Для этого выберите категорию "Группы ресурсов" и в меню выберите команду "Группы ресурсов | Создать группу | По журналу". При появлении диалога для выбора типа ресурсов выберите тип "Загружаемые модули" и нажмите кнопку "ОК". В появившемся диалоге настройки параметров добавления ресурсов укажите в качестве источника журнал Secret Net, настройте параметры интервала времени для анализа событий (укажите время, соответствующее сеансу работы пользователя) и нажмите кнопку "ОК". В списке групп ресурсов появится новая группа ресурсов, сформированная по результатам анализа журнала.

8. Проверьте наличие ресурсов в созданных группах. Если группы пустые, это означает, что ранее созданное задание ЗПС полностью обеспечивает возможность работы пользователя. В этом случае перейдите к действию 12.

9. Создайте новое задание ЗПС, которое будет применяться для пользователя. Для этого выберите категорию "Задания" и в меню "Задания" выберите команду "Создать задание". В появившемся диалоге выберите тип задания для ЗПС и нажмите кнопку "ОК". В следующем диалоге введите имя и описание задания, после чего нажмите кнопку "ОК". Включите созданные группы ресурсов в задание. Для этого вызовите контекстное меню задания и выберите команду "Добавить задачи/группы | Существующие". В появившемся диалоге для выбора объектов выберите созданные группы и нажмите кнопку "ОК".

10. Добавьте пользователя в модель данных в качестве субъекта управления и установите связь с созданным заданием. Для этого выберите категорию "Субъекты управления" и в меню "Субъекты управления" выберите команду "Добавить в список". В стандартном диалоге выбора объектов выберите учетную запись пользователя и нажмите кнопку "ОК". После этого вызовите контекстное меню добавленного элемента и выберите команду "Добавить задания | Существующие". В появившемся диалоге выберите задание и нажмите кнопку "ОК".

11. Выполните процедуру расчета эталонов для ресурсов созданного задания. Для этого вызовите контекстное меню задания и выберите команду "Расчет эталонов". В появившемся диалоге нажмите кнопку "ОК". Далее в диалоге запроса на сохранение модели данных нажмите кнопку "Да" и дождитесь завершения процесса расчета.

12. При необходимости выполнить настройку для другого пользователя повторите действия 5–11.

13. Включите жесткий режим работы механизма. Для этого выберите категорию "Субъекты управления", вызовите диалоговое окно настройки свойств компьютера и в диалоге "Режимы" удалите отметку из поля "Мягкий режим". Сохраните сделанные изменения в программе управления.

Начальная моделируемая инфраструктура для задания № 2:

Клиентский компьютер COMP (ОС Windows 7 SP1 и выше), подключенный к домену test.local. Сервер WIN2012R2 (ОС Windows Server 2012 R2) с добавленной ролью контроллера домена (домен test.local). Сервер WIN2008R2 (ОС Windows 2008 R2), подключенный к домену test.local. На компьютере и серверах присутствуют только локальные пользователи Администратор. Политики безопасности операционных систем имеют настройки по умолчанию.

Инструкция по настройке механизма замкнутой программной среды средством защиты информации DallasLock 8.0-С с использованием режима обучения:

Пусть пользователь, для которого нужно организовать ЗПС, уже создан и инициализирован (к примеру, он называется zps). Далее для настройки ЗПС, необходимо выполнить следующие шаги по настройке:

1. Необходимо создать специальную группу, например, ZPS, и включить пользователя zps в группу ZPS-gr.

2. Для группы ZPS-gr в глобальных настройках запретить запуск всего (вкладка «Контроль ресурсов» → «Глобальные» → «Параметры ФС по умолчанию»).

3. В дескрипторе «Параметры ФС по умолчанию» включить полный аудит отказов.

4. Далее необходимо настроить неактивный режим работы СЗИ НСД (пункт меню кнопки основного меню «Настройка режимов работы» → «Настроить неактивный режим»). В окне настройки необходимо включить «мягкий режим» контроля доступа. Дополнительно желательно очистить (архивировать) журнал ресурсов.

5. Отправить компьютер в перезагрузку.

Примечание. Необходимо именно перезагрузить компьютер, просто завершить сеанс работы одного пользователя и зайти другим недостаточно – при загрузке компьютера используется другой набор исполняемых модулей. При смене пользователя событие загрузки ОС не попадет в журнал ресурсов, и в результате настройки ЗПС данным способом этот пользователь не сможет осуществить вход.

6. Осуществить вход в ОС под учетной записью пользователя zps. Запустить все те приложения, с которыми пользователь имеет право работать (но, не запускать ничего лишнего). Следует помнить, что не для всех приложений является достаточным просто их запуск. Некоторые сложные приложения на своем старте загружают не все исполняемые модули, а только необходимые, остальные модули они подгружают динамически, в процессе работы. Поэтому после запуска приложения лучше выполнить все основные действия приложения для работы. На этом этапе в журнале доступа к ресурсам формируется список файлов, которые нужны данному пользователю для работы.

7. Далее следует осуществить смену пользователя и войти под учетной записью администратора безопасности. Запустить оболочку администратора СЗИ НСД, открыть журнал ресурсов.

8. Настроить и применить фильтр журнала доступа к ресурсам: пользователь – «zps», результат – «ошибка»

9. Далее необходимо выделить поле с записями журнала и выбрать на панели действий «Права для файлов» (или нажать эту кнопку в появившемся отдельном окне выбранной записи журнала или выбрать из контекстного меню).

В появившемся окне редактирования дескриптора безопасности назначить дискреционные права для группы ZPS-gr «только чтение» и нажать «ОК». После нажатия кнопки «ОК» система защиты попросит пользователя выбрать еще одно действие для настройки параметров безопасности.

10. В этом случае, если назначаются права на доступ к ресурсам для группы ZPS-gr впервые, то параметры безопасности будут созданы независимо от выбранного значения «Да» или «Нет». Если же необходимо добавить параметр (например, право запускать еще какую-либо программу), то в этом случае следует нажать кнопку «Да», чтобы добавить параметр и не потерять существующие.

11. Таким образом, замкнутая программная среда организована. Теперь необходимо отключить «мягкий режим» и зайти пользователем zps. Этот пользователь сможет работать только с необходимыми программами.

Следует помнить, что вполне вероятна ситуация, когда не все нужные для работы пользователя исполняемые файлы занесли в список. Так как некоторые приложения вызывают какие-либо другие исполняемые файлы только при активизации определенных функций. Если после включения ЗПС у пользователя zps какое-либо приложение стало работать неправильно – это можно сразу же увидеть в журнале доступа к ресурсам. Скорее всего, для какого-то еще исполняемого файла необходимо добавить право на исполнение (действие «Права для файлов» → «Только чтение») для данного пользователя (группы).

6. Порядок выполнения лабораторной работы (этапы)

Для задания № 1:

1. Установить на клиентский компьютер COMP СЗИ от НСД «SecretNet 7.7» – автономный.
2. Создать ЗПС для пользователя USER со следующими доступными задачами: Acrobat Reader, Windows Movie Maker. Запуск иных задач (кроме тех, что расположены в c:\windows\) должен быть запрещен. Запуск встроенных игр (Сапер, Косынка и т.д.) должен быть запрещен.

Для задания № 2:

1. Развернуть на сервере WIN2008R2 сервер управления DallasLock.
2. С использованием возможностей сервера управления провести удаленную установку DallasLock на клиентский компьютер COMP.
3. Создать ЗПС, которая будет применяться на доменного пользователя USER при включении его в доменную группу ZPS, со следующими доступными задачами: WordPad, Windows Movie Maker. Запуск иных задач (кроме тех, что расположены в c:\windows\) должен быть запрещен. Запуск встроенных игр (Сапер, Косынка и т.д.) должен быть запрещен.

7. Контрольные вопросы:

Для задания № 1:

1. Проверить корректность применения настроек СЗИ от НСД, реализующих ЗПС под пользователем USER на клиентском компьютере COMP, проверив возможность запуска только разрешенных программ в соответствии с заданием.

Для задания № 2:

1. Проверить корректность настроек сети, выполнив команду ping win2012r2.test.local и ping win2008r2.test.local с клиентского компьютера COMP, а также ping comp.test.localc сервера win2008r2.
2. Проверить корректность установки СЗИ от НСД на клиентский компьютер, проанализировав журнал системных событий операционной системы.
3. Проверить корректность применения настроек сервера управления, реализующих ЗПС под пользователем USER на клиентском компьютере COMP, проверив возможность запуска только разрешенных программ в соответствии с заданием.

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: ФГБОУ ВО «СГУ им. Питирима Сорокина», Басенко Алексей Олегович, Носов Леонид Сергеевич, Некрасов Александр Николаевич, kib@syktsu.ru

Образовательная программа: 10.03.01 Информационная безопасность, Комплексная защита объектов информатизации, Техническая защита информации.

Дисциплина: Программно-аппаратные средства защиты информации.

Лабораторная работа. **Централизованное управление полномочиями** **и доступом к информационным ресурсам**

1. Учебные цели:

Изучение и отработка навыков:

- управления полномочиями пользователей с применением доменных групп безопасности и групповых политик;
- управления доступом к ресурсам сети с использованием ролевой модели, реализованной через применение доменных групп безопасности.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь:

- формулировать и настраивать политики безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;

Владеть:

- профессиональной терминологией в предметной области.

3. Перечень материально-технического обеспечения

Лабораторные работы выполняются на гостевой операционной системе в среде виртуализации VMware Workstation Player или Oracle VM VirtualBox. Для выполнения необходимы операционные системы (ОС) Windows 7 SP1 редакции Professional или Enterprise, на любой архитектуре (32-бит, 64-бит), Windows Server 2012R2 или более высокой версии.

4. Задание на исследование

Задание № 1. Провести настройку управления полномочиями в Microsoft Active Directory

Задание № 2. Провести настройку ролевого доступа к ресурсам в Microsoft Active Directory

5. Краткие теоретические сведения

Начальная моделируемая инфраструктура для задания № 1:

Клиентский компьютер COMP (ОС Windows 7 SP1 и выше) без подключения к домену. Сервер WIN2012 (ОС Windows 2012 R2) с добавленной ролью контроллера домена (домен test.local). На компьютере и сервере присутствуют только локальные пользователи Администратор. Политики безопасности операционных систем имеют настройки по умолчанию.

Рекомендации по многоуровневой модели привилегий:

Приведем простую модель быстрой классификации существующих ресурсов и настройки зон для ограничения использования учетных записей. Эта модель использует иерархические модели Viba и Bell-LaPadula, адаптированные для управления администрированием, и представлена тремя уровнями прав администратора (плюс уровень для конечных пользователей, не являющихся администраторами домена). Для лучшего разделения прав доступа администраторов и управления ими все учетные записи и приложения группируются по четырем уровням прав доступа в зависимости от их возможности повлиять на работу организации.

Уровень 0. Администраторы леса – прямой или косвенный административный контроль над лесом, доменами и контроллерами доменов Active Directory.

Уровень 1. Администраторы серверов – прямой или косвенный административный контроль над одним или несколькими серверами.

Уровень 2. Администраторы рабочих станций – прямой или косвенный административный контроль над несколькими устройствами.

Уровень 3. Пользователи – непривилегированные пользователи или административный контроль над одним устройством.

В некоторых организациях могут потребоваться другие уровни для дополнительной сегментации, но все равно в качестве отправной точки можно использовать эту модель.

Данная модель предназначена для предотвращения повышения привилегий злоумышленником, несанкционированно использующим чужие учетные данные. Она определяется следующими правилами.

Все управляемые ресурсы (группы, учетные записи, серверы, рабочие станции, объекты Active Directory и приложения) классифицируются в один уровень во избежание повышения привилегий злоумышленником, несанкционированно получившим доступ к чужим учетным данным.

Сотрудники, которым требуется входить в систему и управлять ресурсами на разных уровнях, должны иметь отдельные учетные записи администратора для каждого уровня. Все учетные записи, в данный момент входящие в несколько категорий, должны разделяться на несколько учетных записей, каждая – только для одного определения уровня. Эти учетные записи также должны иметь разные пароли.

Учетные записи администратора не должны предоставлять контроль над ресурсами более высокого уровня через административный доступ, в частности через списки управления доступом (ACL), агенты приложений или контроль учетных записей служб. Учетным записям, управляющим ресурсами более высокого уровня, не должен быть разрешен вход на компьютеры более низкого уровня, так как при входе на эти компьютеры есть риск раскрыть учетные данные такой учетной записи и непреднамеренно предоставить сопоставленные с ней права доступа. Имеются некоторые исключения для подключений удаленного рабочего стола, использующих RDP с ограниченным административным режимом, которые могут использоваться без предоставления учетных данных.

Учетные записи администраторов могут управлять ресурсами более низкого уровня согласно требованиям роли, но только через интерфейсы управления, работающие на более высоком уровне и не

предоставляющие учетных данных. Например, из учетной записи администратора домена (уровень 0) можно управлять объектами учетной записи Active Directory администратора сервера (уровень 1) через консоли управления Active Directory на контроллере домена (уровень 0).

Каждое подразделение, содержащее учетные записи компьютеров, может содержать только учетные записи компьютеров для определенного уровня. Если подразделение содержит учетные записи компьютеров для нескольких уровней, учетные записи компьютеров для одного уровня должны перемещаться в другой домен или подразделение либо должно быть создано отдельное подчиненное подразделение для размещения каждого такого уровня.

Учетные записи пользователей, служб и приложений, которым предоставляются постоянные полные права администраторов в лесах Windows Server Active Directory, значительно повышают риск для бизнеса организации. Эти учетные записи часто становятся целью злоумышленников, поскольку в случае их раскрытия злоумышленник обычно получает права для подключения к произвольным серверам и приложениям данного домена.

В некоторых развернутых службах домены настроены таким образом, что операторы учетных записей и операторы серверов являются фактически полными администраторами посредством учетных записей, серверов и приложений, которыми могут управлять эти роли. В большинстве случаев такие настройки делаются из-за того, что какому-либо приложению для работы нужны права администратора либо для всех клиентов или серверов домена, либо для всех учетных записей пользователей и компьютеров в этом домене. Тем не менее очень немногим приложениям требуются оба этих вида прав, поэтому предоставление прав администратора каталога для обеих категорий создает состояние избыточных полномочий, выгодное для взломщика или злоумышленника внутри организации.

Начальная моделируемая инфраструктура для задания № 2:

Клиентский компьютер COMP (ОС Windows 7 SP1 и выше) без подключения к домену. Сервер WIN2012 (ОС Windows 2012 R2) с добавленной ролью контроллера домена (домен test.local). На компьютере и сервере присутствуют только локальные пользователи Администратор. Политики безопасности операционных систем имеют настройки по умолчанию.

Ролевое управление доступом с помощью диспетчера серверов:

1. Необходимо создать роль пользователя для управления доступом, для этого в диспетчере серверов щелкните IPAM. Откроется консоль IPAM-клиента.

2. В области навигации щелкните КОНТРОЛЯ доступа и в нижней области навигации щелкните роли.

3. Щелкните правой кнопкой мыши на роли, а затем нажмите кнопку добавить роль пользователя.

4. Откроется диалоговое окно. Введите имя для роли. Если вы хотите создать роль, которая позволяет администраторам управлять записями ресурсов DNS SRV, можно присвоить имя роли IPAMSRV. Найдите тип операции, которую требуется определить для роли.

5. Разверните «Управление записями ресурсов DNS-сервера», а затем найдите операции записи SRV.

6. Разверните и выберите операции записи SRV, а затем нажмите кнопку ОК.

7. В консоли IPAM-клиента выберите роль, которую вы только что создали. В Просмотр подробностей отображаются допустимые операции для роли.

8. Для создания политики доступа в диспетчере серверов щелкните IPAM. Откроется консоль IPAM-клиента.

9. В области навигации щелкните «контроль доступа». В нижней области навигации щелкните правой кнопкой мыши «политика доступа», а затем нажмите кнопку «добавить политику доступа».

10. Нажмите «добавить политику доступа» откроется диалоговое окно. В параметрах пользователя, нажмите кнопку добавить.

11. Выберите пользователя или группу, откроется диалоговое окно. Нажмите кнопку расположение.

12. Расположения откроется диалоговое окно. Перейдите в расположение, в котором находится учетная запись пользователя, выберите расположение и нажмите кнопку ОК. Расположения закрывает диалоговое окно.

13. Организовать доступ созданных пользователей к наборам ресурсов с использованием ролевой модели разграничения доступа. В системе должно существовать минимум 2 роли (например, Директор и Бухгалтер). Роль предоставляется пользователю посредством включения его в соответствующую доменную группу, соответствующую роли.

14. Выберите пользователя или группу, в диалоговом окне введите имена выбираемых объектов, введите имя учетной записи пользователя, для которого требуется создать политику доступа. Нажмите кнопку «ок».

15. Добавьте политику доступа в параметры пользователя, псевдоним пользователя теперь содержит учетную запись пользователя, к которому применяется политика. В параметрах доступа, нажмите кнопку «новый».

16. Добавьте в политику доступа, параметры доступа изменения новый параметр.
17. Нажмите кнопку «выбрать роль» для открытия списка ролей. Выберите один из ролей, или создайте новую роль.
18. Нажмите кнопку добавить параметр.
19. Роль будет добавлена в политику доступа. Для создания политики дополнительного доступа, щелкните применить, а затем повторите эти действия для каждой политики, который вы хотите создать. Если вы не хотите создать дополнительные политики, щелкните ОК.
20. На панели отображения консоли клиента IPAM убедитесь, что создана новая политика доступа.

6. Порядок выполнения лабораторной работы (этапы)

Для задания № 1:

1. Включить клиентский компьютер в домен.
2. Создать доменных пользователей USER1 и USER2 (включены только в группу Пользователи домена).
3. Организовать возможность предоставления пользователям прав локального администратора на клиентском компьютере COMP посредством включения пользователя в созданную доменную группу. При этом пользователи не должны получать права администратора домена.
4. Организовать возможность локального входа пользователя на клиентский компьютер COMP только на основании членства в определенной доменной группе (настройки локального входа в систему должны применяться через групповую политику).

Для задания № 2:

1. Включить клиентский компьютер в домен.
2. Создать доменных пользователей USER1 и USER2 (включены только в группу Пользователи домена).
3. На сервере создать 3 файловых ресурса, доступных по сети. На каждый из ресурсов могут быть предоставлены следующие права: доступ только на чтение (выполнение запрещено), доступ на чтение и выполнение, полный доступ к содержимому, отсутствие прав на доступ. Каждый набор прав доступа для каждого ресурса должен определяться соответствующей доменной группой.

7. Контрольные вопросы:

Для задания № 1:

1. Проверить корректность настроек сети, выполнив команду ping win2012.test.local с клиентского компьютера COMP.
2. Проверить получение пользователем USER1 прав локального администратора на клиентском компьютере COMP после включения в созданную доменную группу (например, проверив возможность открытия оснастки Локальные политики безопасности).
3. Проверить невозможность входа пользователя USER2 в операционную систему без включения в соответствующую созданную доменную группу.

Для задания № 2:

1. Проверить корректность настроек сети, выполнив команду ping win2012.test.local с клиентского компьютера COMP.
2. Проверить видимость созданных файловых ресурсов с клиентского компьютера COMP по пути \\win2012.test.local\.
3. Проверить получение пользователями необходимых прав по доступу к созданным ресурсам при их добавлении в доменные группы, соответствующие различным ролям. Проверку необходимо проводить, разместив в каждом из созданных ресурсов любой текстовый документ и исполняемый файл.

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: ФГБОУ ВО «СГУ им. Питирима Сорокина», Басенко Алексей Олегович, Носов Леонид Сергеевич, Некрасов Александр Николаевич, kib@syktsu.ru

Образовательная программа: 10.03.01 Информационная безопасность, Организация и технология защиты информации.

Дисциплина: Программно-аппаратные средства защиты информации.

Лабораторная работа.

Методы и алгоритмы стеганографического сокрытия данных

1. Учебные цели:

Изучение методов и алгоритмов стеганографического сокрытия данных; знакомство с программным продуктом Steganos.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Владеть навыками работы в программе Steganos.

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение: класс персональных компьютеров (12 шт.) с подключением к сети Интернет, программа Steganos Privacy Suit.

4. Задание на исследование:

Используя различные контейнеры (фото, растровые изображения, аудио и видео файлы) скрыть текстовые сообщения различной длины. Сравнить программно и визуально изображения до и после стеганографического преобразования.

5. Краткие теоретические сведения

Стеганография – это метод организации секретной связи между абонентами, который скрывает собственно само наличие связи. В отличие от криптографии, где неприятель точно может определить, является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование в них встроенного тайного послания.

Сокрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения. А если это сообщение, к тому же, зашифровано, то оно имеет еще один, дополнительный уровень защиты.

Передаваемое сообщение скрывается в некоторых безобидных данных: тексте, изображении, звуке, видеофайле и т.п., которые называются контейнером.

В прошлом веке широко использовались так называемые симпатические чернила, невидимые при обычных условиях. Скрытое сообщение размещали в определенные буквы невинных словосочетаний, передавали при помощи внесения в текст незначительных стилистических, орфографических или пунктуационных погрешностей. С изобретением фотографии появилась технология микрофотоснимков, успешно применяемая Германией во время мировых войн. Крапление карт шулерами – это тоже пример стеганографии. Сокрытие информации перечисленными методами возможно лишь благодаря тому, что противнику неизвестен метод сокрытия. Между тем, еще в 1883 году Кирхгофф писал о том, что система защиты информации должна обеспечивать свои функции даже при полной информированности противника о ее структуре и алгоритмах функционирования. Вся секретность системы защиты передаваемых сведений основана на ключе, т.е. на предварительно (как правило) разделенном между адресатами фрагменте информации. Несмотря на то, что этот принцип известен уже более 100 лет, сейчас встречаются разработки, пренебрегающие им. Конечно, они не могут применяться в серьезных целях. Развитие средств вычислительной техники в последнее десятилетие дало новый толчок для развития компьютерной стеганографии. Появилось много новых областей применения. Сообщения встраивают теперь в цифровые данные, как правило, имеющие аналоговую природу. Это – речь, аудиозаписи, изображения, видео. Известны также предложения по встраиванию информации в текстовые файлы и в исполняемые файлы программ.

Существуют два основных направления в компьютерной стеганографии: связанное с цифровой обработкой сигналов и не связанное. В последнем случае сообщения могут быть встроены в заголовки файлов, заголовки пакетов данных. Это направление имеет ограниченное применение в связи с относительной легкостью вскрытия и/или уничтожения скрытой информации. Большинство текущих исследований в области стеганографии, так или иначе, связаны с цифровой обработкой сигналов. Это позволяет говорить о цифровой стеганографии. Можно выделить две причины популярности исследований в области стеганографии в настоящее время: ограничение на использование криптосредств в ряде стран мира и появление проблемы защиты прав собственности на информацию, представленную в цифровом виде.

Цифровая стеганография включает в себя следующие направления:

- встраивание информации с целью ее скрытой передачи;
- встраивание цифровых водяных знаков (ЦВЗ) (*watermarking*);
- встраивание идентификационных номеров (*fingerprinting*);
- встраивание заголовков (*captioning*).

При построении стegosистемы должны учитываться следующие соображения:

- противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной потенциальному противнику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;
- если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь сообщение из контейнера до тех пор, пока ключ хранится в тайне;
- потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

Рассмотрим подробнее понятие *контейнера*. До стегокодера – это пустой контейнер, после него – заполненный контейнер, или стего. Стего должен быть визуально неотличим от пустого контейнера. Различают два основных типа контейнеров: потоковый и фиксированный.

Потоковый контейнер представляет собой непрерывно следующую последовательность бит. Сообщение вкладывается в него в реальном масштабе времени, так что в кодере неизвестно заранее, хватит ли размеров контейнера для передачи всего сообщения. В один контейнер большого размера может быть встроено и несколько сообщений. Интервалы между встраиваемыми битами определяются генератором псевдослучайной последовательности с равномерным распределением интервалов между отсчетами. Основная трудность заключается в осуществлении синхронизации, определении начала и конца последовательности.

У фиксированного контейнера размеры и характеристики заранее известны. Это позволяет осуществлять вложение данных оптимальным в некотором смысле образом. Контейнер может быть выбранным, случайным или навязанным. Выбранный контейнер зависит от встраиваемого сообщения, а в предельном случае является его функцией. Этот тип контейнера больше характерен для стеганографии. Навязанный контейнер может появиться в сценарии, когда лицо, предоставляющее контейнер, подозревает о возможной скрытой переписке и желает предотвратить ее. На практике же чаще всего сталкиваются со случайным контейнером.

Встраивание сообщения в контейнер может производиться при помощи ключа, одного или нескольких. Ключ – псевдослучайная последовательность (ПСП) бит, порождаемая генератором, удовлетворяющим определенным требованиям (безопасный криптографический генератор). Числа, порождаемые генератором ПСП, могут определять позиции модифицируемых отсчетов в случае фиксированного контейнера или интервалы между ними в случае потокового контейнера. Скрываемая информация внедряется в соответствии с ключом в те отсчеты, искажение которых не приводит к существенным искажениям контейнера. Эти биты образуют стегопуть. В зависимости от приложения, под существенным искажением можно понимать искажение, приводящее как к неприемлемости для человека-адресата заполненного контейнера, так и к возможности выявления факта наличия скрытого сообщения после стегоанализа.

Стеганографический ключ называется стегоключом. Существует множество программных продуктов, реализующих стеганографическое скрытие информации. Один из них – продукт фирмы Steganos.

Данный программный продукт реализует встраивание в контейнеры секретную информацию. В качестве контейнеров могут использоваться файлы изображений (*.bmp), звуковые файлы (*.wav), текстовые файлы (*.txt).

Продукт содержит следующие модули:

1. Модуль сокрытия данных (Steganos Explorer).
2. Модуль управления паролями (Password Management).
3. Модуль управления секретным диском (Steganos Safe).
4. Модуль безопасного удаления файлов и каталогов (Steganos Shredder).
5. Модуль ограничения доступа к ЭВМ (Steganos SysLock).
6. Модуль защиты от перехвата излучения монитора (Zero Emission Pad).

Назначение модуля сокрытия данных – предоставить пользователю интерфейс для сокрытия информации в стеганографических контейнерах. Пользователь может выбирать как скрываемые файлы, так и контейнеры, которые называются секретным пространством (Security Space) и представляются для пользователя как каталоги, в которых скрываются данные пользователя. Контейнерами могут быть изображения, звуковые файлы и тексты. Существует ограничение на объем скрываемых данных – порядка 5–10 % (в зависимости от типа файла).

Назначение модуля управления паролями – сокрытие в контейнерах паролей доступа к другим контейнерам. Кроме этого, в этих контейнерах могут скрываться контрольные суммы защищенных файлов (отпечатки), идентификаторы пользователей, номера мобильных телефонов, и другая конфиденциальная информация, связанная с пользователем. Скрытая в контейнере информация может передаваться по назначению. Назначение модуля управления секретным диском – создать виртуальный диск, доступ к которому защищен паролем.

Назначение модуля безопасного удаления файлов и каталогов – удалять информацию не только из FAT-таблицы (таблицы расположения информации о файлах), но и на соответствующем месте их хранения на диске. Назначение модуля ограничения доступа к ЭВМ – защитить паролем доступ к компьютеру. Назначение модуля защиты от перехвата излучения монитора – предотвратить перехват специализированными средствами излучения, создаваемого монитором, по которому можно восстановить информацию.

6. Порядок выполнения лабораторной работы (этапы)

1. Знакомство со стеганографическими методами с привлечением электронного учебника.
 - 1.1. Запустить электронную лабораторную модель «Защита конфиденциальности информации методами стеганографии» и познакомиться с содержанием теоретического курса работы.
 - 1.2. В разделе лабораторной модели «Текстовая стеганография» познакомиться с реализациями методов стеганографического сокрытия информации в текстах. Запустить из модели демонстрационные мультимедийные примеры реализации методов текстовой стеганографии, использующие пробелы между фразами и внедрение пробелов между словами. Детально разобраться с реализациями данных методов.
 - 1.3. Запустить программы, реализующие метод внедрения пробелов между фразами, между словами, в конце строк. В качестве контейнера выбрать файл («Grygory_Adamov.txt»).
 - 1.4. Какой максимальный объем секретной информации можно внедрить в данный файл при использовании каждого из трех методов?
 - 1.5. Набрать в редакторе потеррад некоторый текст для внедрения в контейнер и внедрить его каждым из трех методов.
 - 1.6. Изучить получившиеся текстовые файлы со встроенным секретным сообщением. Что вы можете сказать о наличии секретного текста в данном файле?
 - 1.7. Извлечь секретный текст из стегосообщения.
2. Работа с программным продуктом Steganos II. Модуль STEGANOS EXPLORER
 - 2.1. Запустить STEGANOS и выбрать компоненту Steganos Explorer.
 - 2.2. Перед Вами два окна. Верхнее – рабочий каталог, нижнее – область контейнера. Установите в качестве рабочего каталога – каталог с лабораторной работой. Для контейнера укажите Hide Encrypt (будем скрывать данные).
 - 2.3. В качестве контейнера определить изображение Рай.bmp (нажав кнопку View carrier file).
 - 2.4. Осуществить внедрение в выбранный контейнер файл lha.exe и изучить вид получившегося контейнера, после чего закрыть контейнер с сохранением результатов.
 - 2.5. Скрыть тот же самый файл в звуковом и текстовом контейнерах.
 - 2.6. Проанализировать вид контейнеров со скрытыми файлами. Заметна ли потеря качества контейнеров?
 - 2.7. В Security Space выбрать режим unhide-decrypt и извлечь из всех контейнеров скрытые данные.
 - 2.8. Набрать в текстовом редакторе текст, скрыть его в произвольном контейнере. Передать другому пользователю на извлечение. Перед извлечением изучить вид контейнера.
3. Модуль Password Management
 - 3.1. Запустить модуль Password Management. В качестве контейнера, указать один из существующих.
 - 3.2. Внести в контейнер различную секретную информацию – записи, включающие пароль, подпись некоторого текстового файла (из рабочего каталога), информацию о пользователе и онлайн-соединении, номер телефона, и другие. Попытаться внести пароли, набранные Вами, и пароли, сгенерированные компьютером.
 - 3.3. Изменить содержание файла, для которого была внесена подпись. Сравнить данные подписи. Были ли распознаны изменения?
 - 3.4. Скрыть все пароли в контейнере и передать другому пользователю для просмотра.
4. Модуль Steganos Safe
 - 4.1. Создать и открыть секретный диск.
 - 4.2. Скопировать на секретный диск несколько файлов из рабочего каталога.
 - 4.3. Попытаться выполнять различные операции над секретным диском, в том числе включение и отключение.
5. Другие модули
 - 5.1. Из проводника удалить файл LHA.EXE физически с диска посредством Steganos Shreder.
 - 5.2. Определить пароль в Steganos Syslock. Отключить и включить доступ к ЭВМ посредством данного модуля.
 - 5.3. Запустить модуль Zero Emission Pad, открыть текстовый файл из рабочего каталога и посмотреть результат работы данной программы.

7. Контрольные вопросы:

1. Что понимают под стеганографией?
2. На чем основана работа стеганографических методов?
3. В чем заключается основное отличие между криптографией и стеганографией?
4. Перечислите основные виды стеганографических контейнеров.
5. В какой контейнер можно внедрить большее количество информации без обнаружения модификаций – в текст или в насыщенное изображение?
6. В какой контейнер можно внедрить большее количество информации без обнаружения модификаций – в оперную увертюру, записанную с CD-качеством, или в репортаж со спортивного стадиона?

Время на выполнение лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: ФГБОУ ВО «Казанский национальный исследовательский технологический университет», старший преподаватель кафедры информационной безопасности Сафиуллина Лина Хатыповна, lina.kh.safiullina@mail.ru

Образовательная программа: 10.03.01 Информационная безопасность, Организация и технология защиты информации.

Дисциплина: Программно-аппаратные средства защиты информации.

Лабораторная работа.

Поиск уязвимостей информационной системы с помощью средств анализа защищенности

1. Учебные цели:

- Изучить принципы работы и возможности средств анализа защищенности;
- Отработать навыки работы со средствами анализа защищенности с части поиска уязвимостей информационной системы.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь:

- реализовывать на практике принципы политики безопасности; использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности; зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; пользоваться нормативными документами по защите информации; формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;

Владеть:

- навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью; навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации.

3. Перечень материально-технического обеспечения:

Лабораторное оборудование и программное обеспечение: для работы предлагается применять технологии виртуализации на базе Oracle VM VirtualBox, позволяющие на одном компьютере имитировать наличие нескольких сетевых узлов, дистрибутив средства анализа защищенности «Сканер-ВС» (разработчик – АО «НПО «Эшелон», Россия).

4. Задание на исследование:

- Провести сканирование сети с помощью веб-интерфейса «Сканер-ВС» (фаза Поиск целей), определить открытые порты и версию операционной системы.
- Провести сканирование сетевого узла с помощью веб-интерфейса Сканер-ВС (фаза Поиск уязвимостей).
- Сформировать отчет по результатам сканирования уязвимостей.

5. Краткие теоретические сведения:

Угрозы безопасности информации в информационных системах, как правило, реализуются через уязвимости – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Конкретный набор уязвимостей может отличаться от рассматриваемого в зависимости от того, насколько структура рассматриваемой системы отличается от типовой, какие операционные системы установлены на рабочих станциях и серверах, какие приложения, службы, типы сетевых устройств используются и т.д.

Комплекс «Средство анализа защищенности «Сканер-ВС» предназначен для поиска уязвимостей сетей, исследования топологии сети и инвентаризации сетевых сервисов, сетевого и локального аудита паролей, поиска остаточной информации и анализа сетевого трафика.

«Сканер-ВС» реализует следующие основные функции:

- контроль использования сертифицированных средств защиты информации;
- обеспечение автоматизированного анализа конфигурационных параметров подсистемы обеспечения информационной безопасности;
- обеспечение анализа безопасности и обнаружения уязвимостей сетевых сервисов;
- выполнение анализа стойкости парольной подсистемы;
- удаленная идентификация операционных систем;
- обеспечение оценки эффективности механизмов гарантированной очистки памяти и поиск остаточной информации на носителях информации;
- проведение низкоуровневого анализа сетевого трафика.

К основным классам решаемых «Сканер-ВС» задач относятся локальный и сетевой аудит безопасности.

6. Порядок выполнения лабораторной работы:

1. Перед началом работы запустить виртуальные машины, при необходимости настроить сетевые подключения.

2. Создать тестовый проект:

- в веб-интерфейсе Сканер-ВС нажмите кнопку «Проекты», щелкнув левой кнопкой мыши по соответствующей области в левой части экрана или нажав на кнопку в верхнем правом углу экрана (рис. 1);
- на вкладке «Проекты» нажмите кнопку «Новый проект»;
- на вкладке «Добавление нового проекта» введите «Имя проекта», нажмите кнопку «Сохранить». Вход в рабочую панель проекта произойдет автоматически.

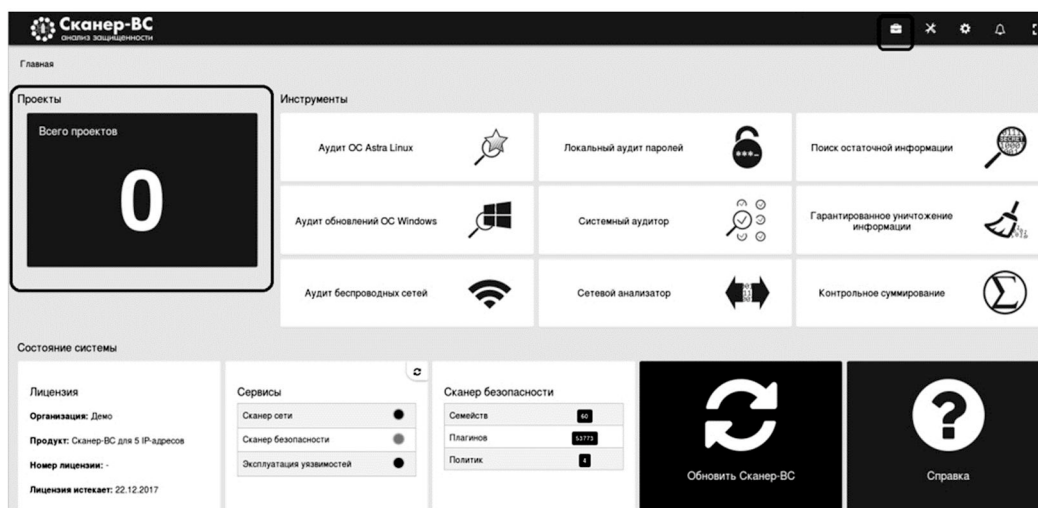


Рис. 1. Интерфейс пользователя

3. Провести поиск открытых портов:

- на рабочей панели проекта выберите фазу «Поиск целей», нажмите кнопку «Задачи» (рис. 2);
- нажмите кнопку «Новое сканирование»;
- задайте требуемые настройки, необходимые для запуска сканирования сети: например, адрес сети 192.168.1.0/24;
- нажмите кнопку «Запустить»;
- в зависимости от цвета статуса возможны три состояния: Желтый – Сканирование выполняется; Зеленый – Сканирование успешно завершено; Красный – Сканирование завершено с ошибкой;
- дождитесь окончания сканирования.

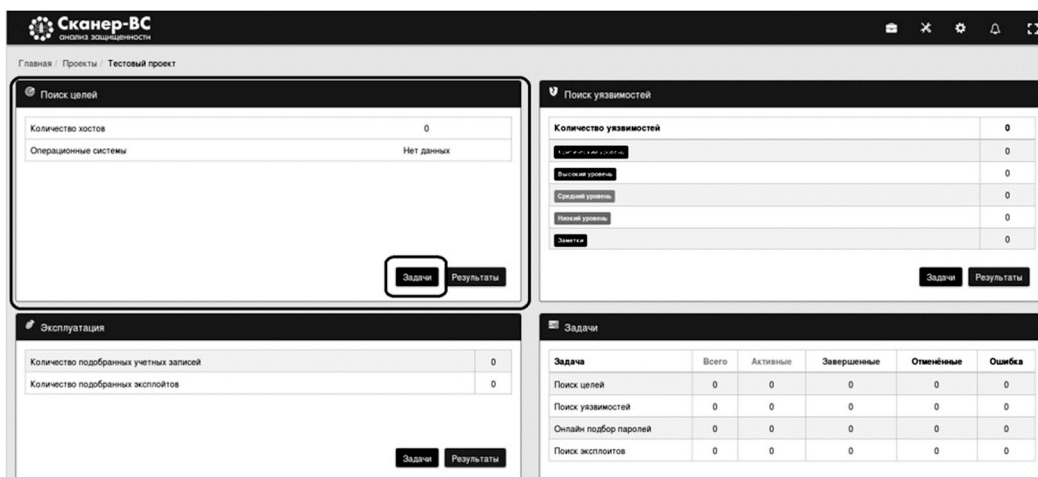


Рис. 2. Фаза Поиска целей

4. Провести поиск уязвимостей системы:

- в рабочей панели проекта выберите фазу «Поиск уязвимостей», нажмите кнопку «Задачи» (рис. 3);
- нажмите кнопку «Новое сканирование»;
- задайте настройки, необходимые для запуска сканирования уязвимостей: задайте цель с помощью импорта «Импорт целей из активов»; политика сканирования – по умолчанию;
- нажмите кнопку «Запустить». После запуска сканирования в таблице на вкладке «Задачи» появится номер задачи, ее имя и статус, отражающий текущее состояние сканирования;
- в зависимости от цвета статуса возможны три состояния: Желтый – Сканирование выполняется; Зеленый – Сканирование успешно завершено; Красный – Сканирование завершено с ошибкой;
- дождитесь окончания сканирования. Примерное время сканирования – 15–20 минут. После завершения сканирования, данные об обнаруженных уязвимостях доступны на вкладке «Уязвимости» (рис. 4).

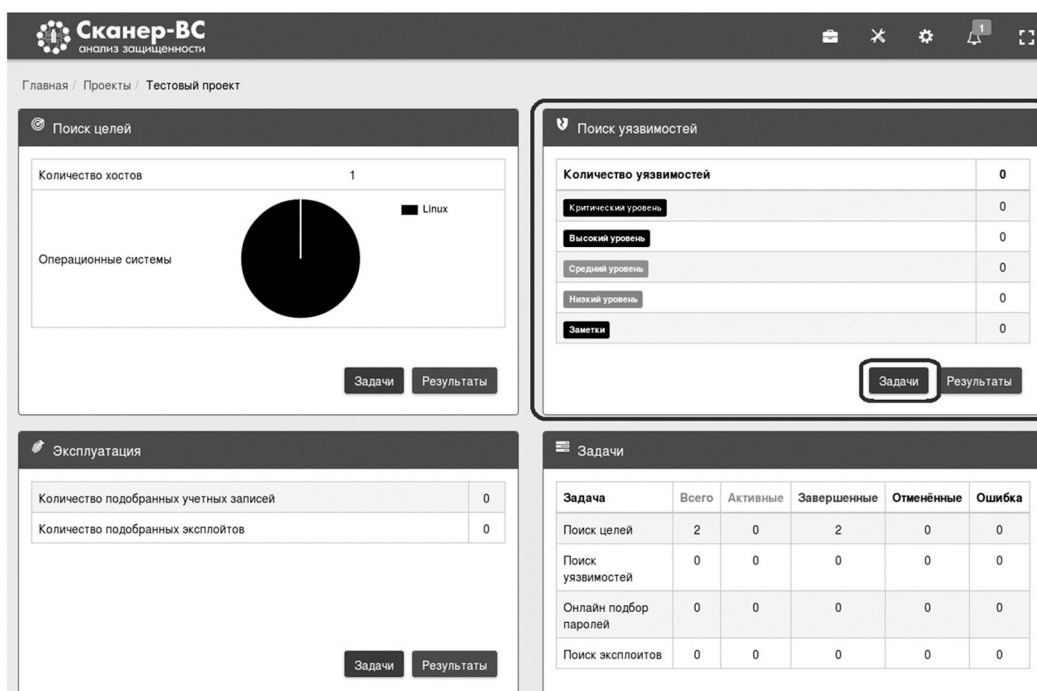


Рис. 3. Фаза поиска уязвимостей

Сканер-ВС
анализ защищенности

Главная / Проекты / Тестовый проект / Поиск уязвимостей

Уязвимости Задачи

Поиск:

Хост	Порт	Описание	Уровень риска
192.168.1.100	0	Этот плагин обнаруживает серверы X Window, X11 - это протокол клиент-сервер. В основном, сервер отвечает за экран, и клиенты подключаются к нему и отправляют несколько запросов, например, рисование окна или меню, а сервер отправляет события обратно клиентам, такие как щелчки мыши, штрихи клавиш и т. Д. ... Неправильно настроенный сервер X будет принимать соединения от клиентов из любого места. Это позволяет злоумышленнику заставить клиента подключиться к X-серверу для записи нажатий клавиш пользователя, которые могут содержать конфиденциальную информацию, такую ​​как пароли учетной записи. Этого можно предотвратить с помощью файлов xauth, MIT или предотвращения прослушивания X-сервера на TCP (носок Unix используется для локальных подключений)	Критический
192.168.1.100	1099	Несколько продуктов Java, реализующих сервер RMI, содержат уязвимость, которая может позволить не прошедшему проверку подлинности удаленным злоумышленникам выполнить произвольный код в целевой системе с повышенными привилегиями.	Критический
192.168.1.100	8787	Системы, использующие Distributed Ruby (dRuby / DRb), которые доступны в версиях Ruby версии 1.6 и более поздних версий, могут позволить несанкционированным системам выполнять распределенные команды.	Критический
192.168.1.100	0	Прекращение поддержки вендором Прекращена поддержка операционной системы на удаленном хосте, данная операционная система не должна больше использоваться	Критический
192.168.1.100	1524	Бэкап устанавливается на удаленном хосте	Критический
192.168.1.100	3632	DistCC 2.x, используемый в XCode 1.5 и других, когда он не настроен на ограничение доступа к серверному порту, позволяет удаленным злоумышленникам выполнять произвольные команды с помощью заданной компиляции, которые выполняются сервером без проверки полномочий.	Критический
192.168.1.100	3632	DistCC - это программа для распространения сборок кода C, C++, Objective C или Objective C на нескольких машинах в сети. DistCC должен всегда генерировать те же результаты, что и локальная сборка, прост в установке и использовании и часто в два или более раза быстрее, чем локальный компилятор.	Высокий

Рис. 4. Вкладка «Уязвимости»

5. Создать отчет по результатам сканирования:

- перейти в рабочую панель проекта;
- выбрать фазу «Отчет» (рис. 5);
- ознакомиться с созданным отчетом.

Сканер-ВС
анализ защищенности

Количество хостов

Операционные системы

Задачи Результаты

Количество уязвимостей

Критический уровень	6
Высокий уровень	8
Средний уровень	12
Низкий уровень	4
Заметки	69

Задачи Результаты

Эксплуатация

Количество подобранных учетных записей	0
Количество подобранных эксплоитов	0

Задачи Результаты

Отчёт

Название проекта Тестовый проект

Задачи

Задача	Всего	Активные	Завершённые	Отменённые	Ошибка
Поиск целей	2	0	2	0	0
Поиск уязвимостей	1	0	1	0	0
Онлайн подбор паролей	0	0	0	0	0
Поиск эксплоитов	0	0	0	0	0

Рис. 5. Фаза создания отчета

7. Контрольные вопросы:

1. Определение термина «уязвимость информационной системы»;
2. Назначение и основной функционал средств анализа защищенности;
3. Необходимые условия для проведения сканирования портов сетевых узлов;
4. Необходимые условия для поиска уязвимостей.

Время на выполнение лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный лингвистический университет» (ФГБОУ ВО МГЛУ); Макеев Сергей Александрович, isic@linguanet.ru

Дисциплина: Сети и системы передачи информации

Образовательная программа: 10.03.01 Информационная безопасность, Организация и технология защиты информации.

Дисциплина: Сети и системы передачи информации.

Лабораторная работа.

Исследование mesh-сети на примере беспроводной сети Wi-Fi

1. Учебные цели:

- Изучить топологию mesh на примере беспроводной сети Wi-Fi.
- Отработать навыки построения топологии mesh.
- Изучить принципы организации защиты информации при построении сети Wi-Fi при топологии mesh.
- Провести экспериментальные исследования по распространению сигнала Wi-Fi в здании со сложной планировкой.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

- Знать технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.
- Уметь анализировать и оценивать угрозы информационной безопасности объекта, а также проводить мониторинг угроз безопасности информационных систем.
- Владеть методами и средствами выявления угроз безопасности автоматизированным системам, а также методами формирования требований по защите информации.

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение: Аппаратная часть реализована на микроконтроллере Wemos D1 mini с разработанным на кафедре ИВТиИБ Борисовым А.П. и Антиповой Л.А. программным обеспечением. Программная часть, разработанная на кафедре ИВТиИБ Борисовым А.П. и Антиповой Л.А., защищена свидетельством о регистрации программы для ЭВМ: Антипова Л.А., Борисов А.П. Программа для передачи данных по каналу Wi-Fi с применением топологии mesh // Свидетельство о государственной регистрации программы для ЭВМ №2017662654, заявл. 26.09.17, опублик. 13.11.17.

4. Задание на исследование

- В зависимости от варианта, количество узлов сети варьируется от 3 до 5.
- В зависимости от варианта, студентами выбирается несколько помещений в ВУЗе для организации беспроводной Wi-Fi сети на основе топологии mesh и проводится передача данных без и с шифрованием.
- Проводится исследование на дальность распространения сигнала и расчет затухания сигнала, как при использовании шифрования, так и без него.

5. Краткие теоретические сведения

IEEE 802.11s входит в состав стандарта IEEE 802.11. В этой реализации одним из основных принципов является то, что точки доступа образуют отказоустойчивую сеть (так как единичные точки отказа исключаются). Данная архитектура подразумевает бесперебойное покрытие сети, причем подключение точек доступа возможно, как при помощи кабеля, так и без такого рода физических соединений. На практике ячеистые сети состоят из узлов, разработанных разными производителями, поэтому, чаще всего, их приходится настраивать каждое обособленно, однако маршрут передаваемых пакетов данных между узлами ячеистых сетей определяется уже в динамическом режиме.

В данном стандарте введены новые протоколы на физическом уровне и MAC-подуровне канального уровня с поддержкой ширококвещательной и многоадресной передач, а также одноадресную поставку по самоконфигурирующейся системе точек доступа Wi-Fi. С этой целью в стандарте введен четырехадресный формат кадра (рис. 1).

В существующих сетях стандарта 802.11 конечные станции-клиенты (англ. STA) связаны с точками доступа (англ. Access Point – AP) и могут взаимодействовать только с ними. AP имеют выход в другие сети (например, Internet), но не могут обмениваться данными друг с другом.

В mesh-сетях, помимо терминальных станций и точек доступа, присутствуют особые устройства – узлы mesh (англ. Mesh Point – MP), способные взаимодействовать друг с другом и поддерживающие mesh-службы. Одно устройство может совмещать несколько функций. Так, узлы mesh-сети, совмещенные с точками доступа, называются точками доступа сети mesh (англ. Mesh Access Point, MAP). Порталы mesh-сети (Mesh Point Portal, MPP), являясь MP, соединяют mesh-сеть с внешними сетями. Таким образом, mesh-сеть с

точки зрения других устройств и протоколов более высокого уровня функционально эквивалентна широковещательной Ethernet-сети, все узлы которой непосредственно соединены на канальном уровне.

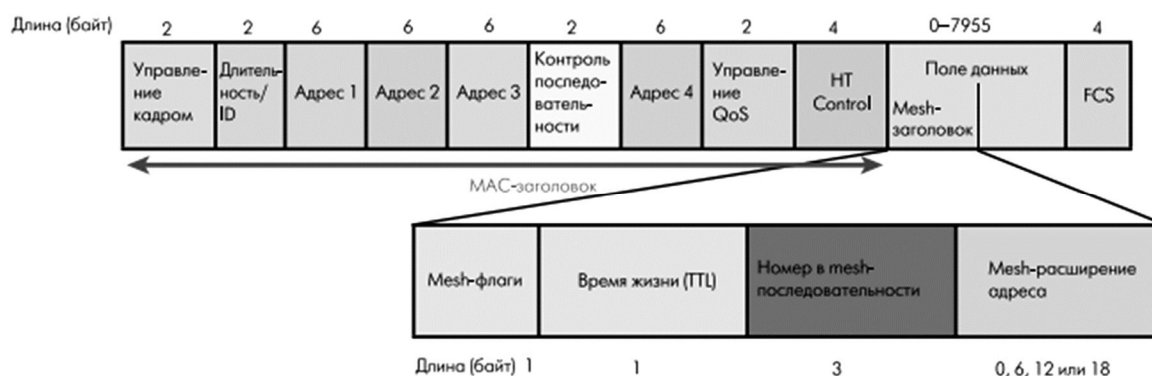


Рис. 1. Формат MAC-кадра с mesh-заголовком

Отличие MAC-пакетов описываемого стандарта заключается в наличии mesh-заголовка в начале поля данных. Этот заголовок присутствует в пакетах данных тогда и только тогда, когда они передаются от mesh-узла к mesh-узлу по установленному между ними соединению.

Mesh-заголовок содержит четыре поля. Байт mesh-флагов регулируют обработку mesh-заголовка. Пока используются только первые два бита, которые просто определяют размер расширенного mesh-адреса. Поле "время жизни пакета в mesh-сети" (англ. Mesh Time To Live – MTL) содержит оставшееся максимальное число шагов между узлами, которое может совершить пакет в mesh-сети. Таким образом ограничивается время жизни пакета при многошаговой пересылке, что помогает бороться с образованием циклических маршрутов. Номер пакета в последовательности (Mesh Sequence Number) пресекает появление дубликатов пакетов при широковещательной и многоадресной посылке. Поле расширения mesh-адреса (Mesh Address Extension) может включать дополнительные адреса (Адрес 4, Адрес 5 и Адрес 6, каждый по 6 байт), что позволяет mesh-пакетам содержать до 6 адресов. Адрес 4 используется в управляющих пакетах типа Multihop Action (при эстафетной передаче в mesh-сети), поскольку в формате управляющих пакетов MAC-уровня поле Адрес 4 отсутствует. Адреса 5 и 6 могут служить для передачи адресов конечных отправителя и получателя, если они оба или один из них не являются MR. Это возможно, если узлы вне mesh-сети общаются через mesh-сеть. Возможен и случай, когда два MR-устройства взаимодействуют через корневой узел mesh-сети, т.е. используются два отдельных mesh-пути (от отправителя до корневого узла и от корневого узла до получателя).

Обязательный для всех устройств стандарта 802.11s профиль использует гибридный беспроводной mesh-протокол маршрутизации (HWMP, Hybrid Wireless Mesh Protocol) и метрику времени передачи в канале (Airtime Link Metric). Механизм установки соединений основан на периодической посылке стандартного сообщения "открыть соединение". В ответ на него может быть получено сообщение "подтверждение соединения" или "закрытие соединения". Соединение между двумя соседними MR считается установленным тогда и только тогда, когда оба MR послали друг другу команды "открыть соединение" и ответили подтверждением соединения (в любой последовательности). Для каждого установленного соединения предусмотрено время жизни, в течение которого оно должно быть использовано либо подтверждено.

Стандарт IEEE 802.11 поддерживает два режима работы беспроводных сетей: hot spot и ad hoc. В режиме hot spot одна из станций работает в качестве точки доступа, и данные могут передаваться только между точкой доступа и другими станциями сети. В режиме ad hoc передача возможна между любыми двумя станциями.

6. Порядок выполнения лабораторной работы (этапы)

1. Для подачи питания на каждую точку устройство должно быть подключено напрямую к сети, либо используя USB-подключение. Конечные точки, используемые в качестве отправителя и получателя, необходимо подключать только вторым способом для ввода, отображения и анализа данных в графическом интерфейсе.
2. Выполняется запуск программы. При подключении устройства рекомендуется сделать сброс при помощи кнопки RESET (рис. 2).
При выполнении сброса в нижнем левом углу отображается идентификатор устройства (рисунок 3).
4. В текст-боксе, предназначенном для ввода получателя, вводим цифры без (!) стандартного префикса. При обработке и отправке сообщения он добавляется автоматически.
5. Далее вводим необходимые данные для передачи (желательно использование латиницы). При необходимости многократной отсылки указываем в соответствующем месте.
6. При получении сообщения на другом конце (сообщение визуально отмечается красным только при финальной доставке, у посредников указывается промежуточное сообщение с последующими полу-

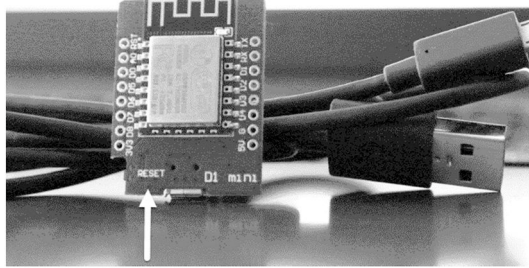


Рис. 2. Кнопка RESET

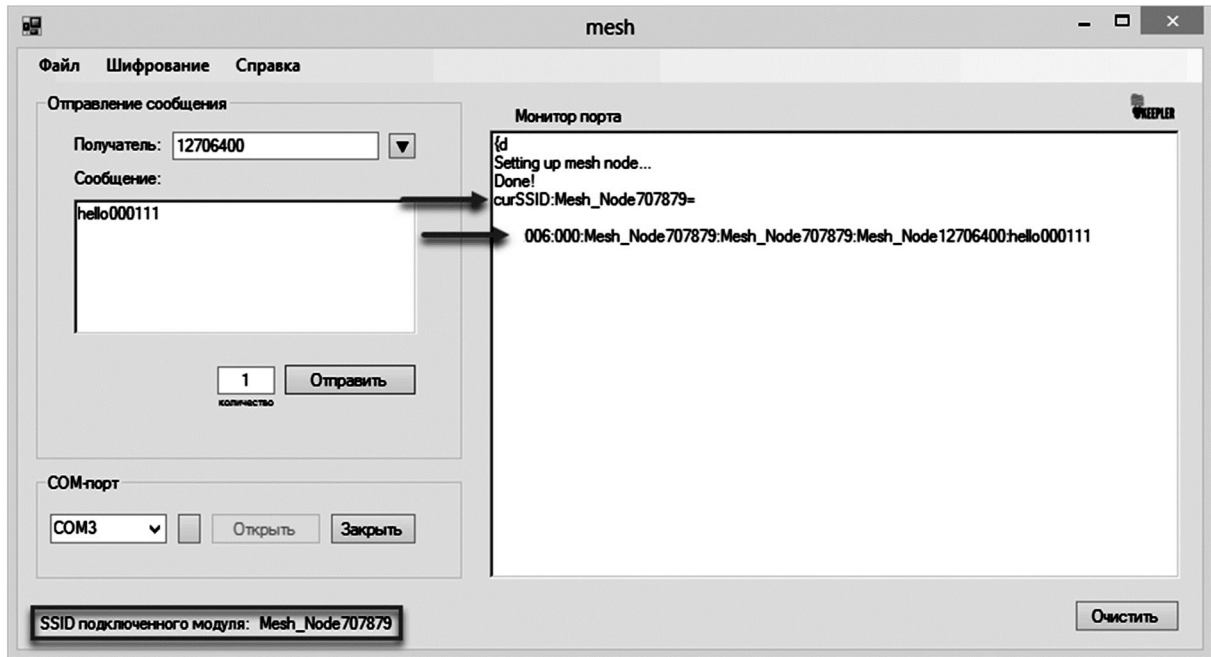


Рис. 3. Данные о модуле

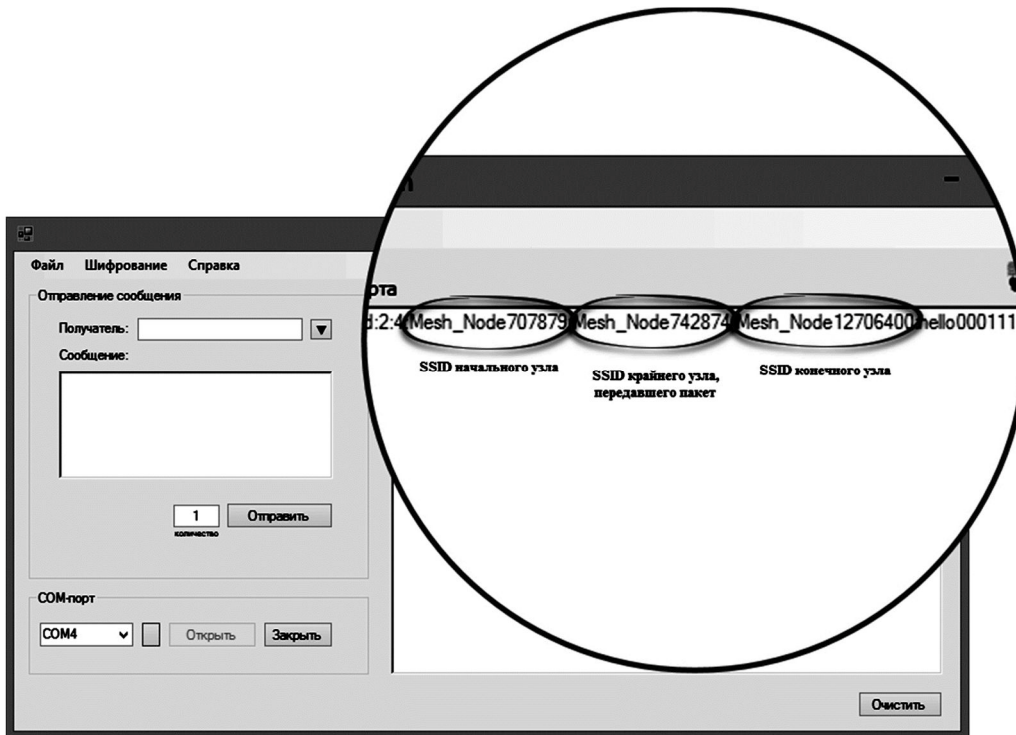


Рис. 4. Разбор полученного сообщения с отметкой используемых адресов

чателами) можно увидеть, через сколько точек прошел пакет (номер в последовательности, первая цифра), время жизни данного пакета (TTL, вторая цифра), используемые адреса согласно установленному заголовку и непосредственно сами данные (рисунок 4).

Примечание. При получении сообщения наподобие "Hello world request #n" без mesh-заголовка воспринимать как подтверждение доставки с последующих узлов относительно текущего.

7. Для фиксации результата в отчете работы, необходимо проследить весь путь сообщения через указанное количество узлов (вставляется скриншот работы программы с сообщением на конечном узле с пояснениями параметров mesh-заголовка).

7. Контрольные вопросы:

1. Помехозащищенность сети Wi-Fi
2. Спецификация стандарта IEEE 802.11s, структура пакета
3. Безопасность стандарта IEEE 802.11
4. Общий формат кадра ассоциирования.
5. Общий формат кадра зондирования.

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: ФГБОУ ВО Алтайский государственный технический университет им. И.И. Ползунова, Борисов Алексей Павлович, alex.borisov84@gmail.com

Образовательная программа: 10.03.01 Информационная безопасность, Организация и технология защиты информации.

Дисциплина: Сети и системы передачи информации.

Лабораторная работа. **Исследование технологии беспроводной высокочастотной связи** **малого радиуса действия NFC**

1. Учебные цели:

- Изучить принципы передачи информации по технологии NFC.
- Изучить принцип использования технологии NFC в составе системы контроля и управления доступом.
- Провести экспериментальные исследования по распространению сигнала NFC через различные препятствия.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

- Знать принципы построения систем связи.
- Уметь настраивать оборудование связи.
- Владеть навыками настройки оборудования связи.

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение: Аппаратная часть реализована на микроконтроллере Arduino при использовании платы RFID/NFC с разработанным на кафедре ИВТиИБ Борисовым А.П. и Николаевой В.К. программным обеспечением. Программная часть, разработанная на кафедре ИВТиИБ Борисовым А.П. и Николаевой В.К., защищена свидетельством о регистрации программы для ЭВМ: Николаева В.К., Борисов А.П. Программа контроля управления доступом на базе технологии NFC // Свидетельство о государственной регистрации программы для ЭВМ №2016660764; заявл. 25.07.16; опублик. 21.09.16.

4. Задание на исследование

- Проверить на каком максимальном расстоянии происходит установление связи между стендом и телефоном.
- Выбрать три препятствия и попробовать передать данные через них. Получить максимальное расстояние при прохождении сигнала через препятствие.
- Узнать принцип, по которому блокируются пользователи в системе. Описать его и предоставить фотографии, доказывающие, что предположения верны.

5. Краткие теоретические сведения

Упрощенная схема распространения сигнала представлена на рисунке 1, где стрелочками обозначен сигнал. Преграда поглощает часть сигнала, в зависимости от толщины преграды или ее материала, сигнал может прийти со значительными потерями или вообще не прийти до приемника.

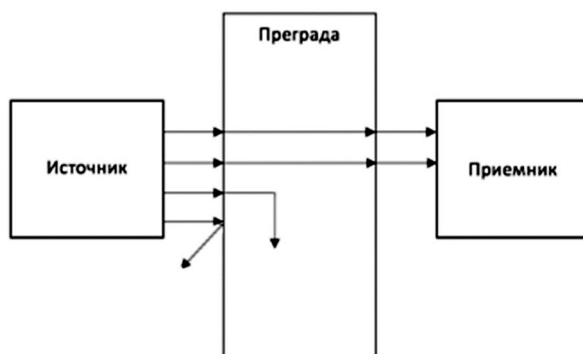


Рис. 1. Распространение сигнала в среде, где есть преграда

После сборки установки был проведен эксперимент по распространению сигналов в пространстве. Производителем заявлено, что максимально данный модуль может устанавливать связь на 7 сантиметрах без каких-либо преград. На практике же это число чуть меньше и составляет 6 сантиметров, что дает стабильный обмен данными между устройствами, хотя увеличить расстояние до 7 см возможно, что приведет к нестабильному обмену данными – в 7 случаях из 10 будет происходить установление связи, а отправка данных в четырех случаях из семи. Данные сведения наглядно отражены на рисунке 2.

Затем были произведены эксперименты для различных преград: гипсокартон, дерево разной толщины, бумага, картон, стекло, стеклопакет и лист жести.

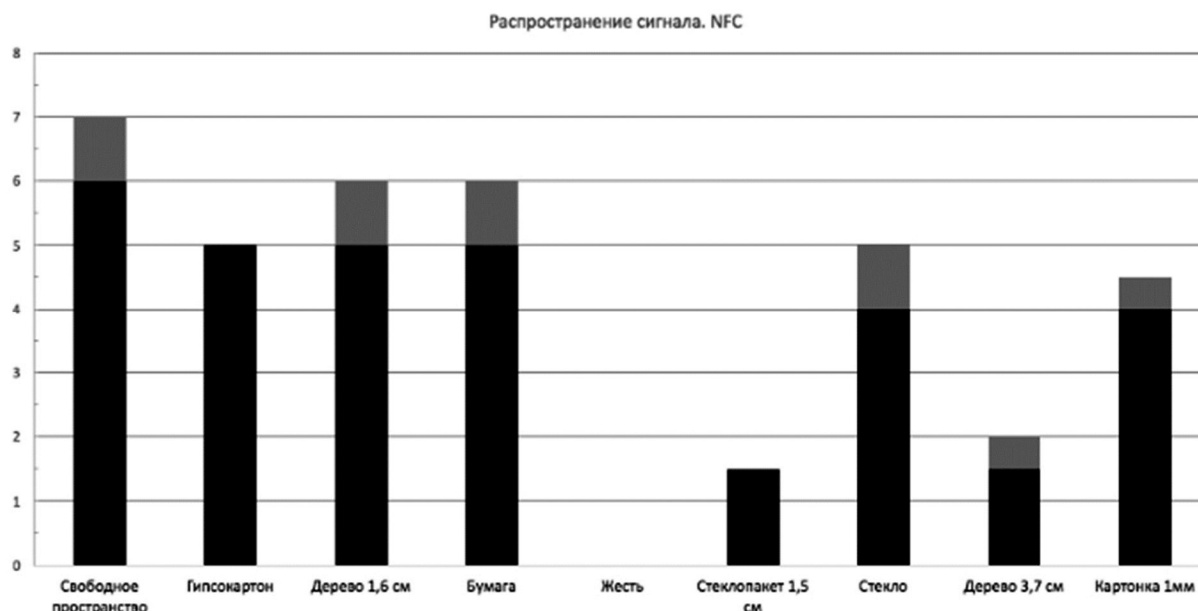


Рис. 2. Распространение сигнала с различными преградами

В случае с листом жести сигнал не устанавливался даже если поднести приемник вплотную к передатчику, то есть абсолютно весь сигнал был поглощен материалом, либо рассеян в пространстве. У гипсокартона, дерева толщиной 1,6 см и бумаги, оказалось почти одинаковое влияние на распространения сигнала, за исключением того, что через дерево и бумагу есть еще запас в 1 см, который позволяет установить связь и переслать данные, но в 4–6 случаях из десяти. Стекло и картон сокращают максимальное расстояние до 4 см для стабильной связи, хоть и стекло дает запас в полсантиметра больше, чем картон. Деревянная дверь (3,7 см) и стеклопакет сокращают расстояние до полутора сантиметров для стабильной связи, у двери есть запас в полсантиметра.

5. Порядок выполнения лабораторной работы (этапы)

1. Человек подходит к точке доступа, где находится считыватель, запускает приложение на смартфоне (с поддержкой NFC) и подносит мобильное устройство к считывателю. При контакте отсылается уникальная последовательность битов, однозначно идентифицирующая данное устройство, а следовательно, и его владельца (рис. 3).

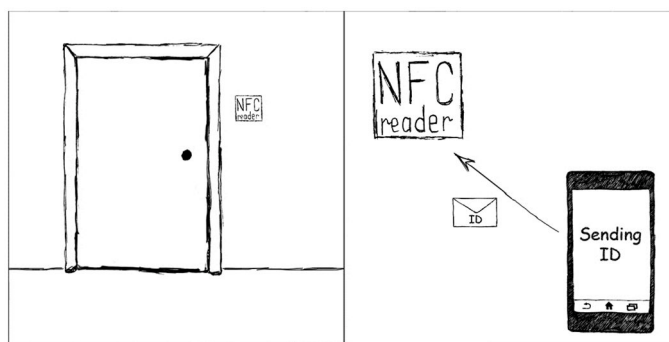


Рис. 3. Опрос идентификатора

- Считыватель обрабатывает полученный сигнал от смартфона и проверяет наличие такого идентификационного номера в базе данных. Если есть совпадение, то на мобильное устройство отсылается случайная последовательность цифр. В обратном случае в доступе отказывается (рис. 4).

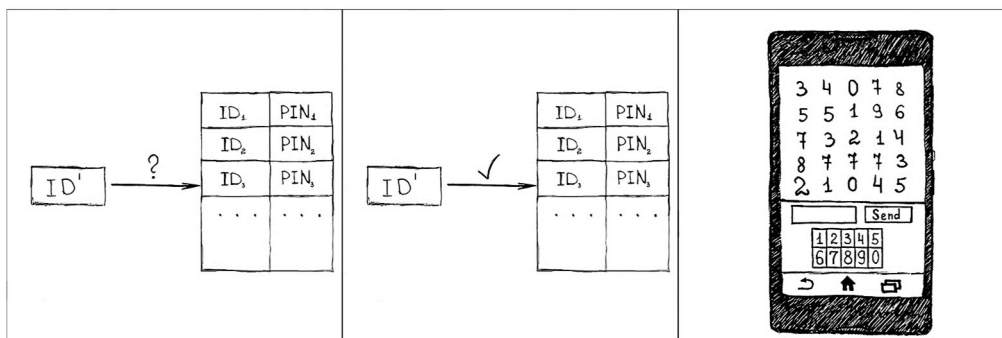


Рис. 4. Проверка идентификатора

- Владелец мобильного устройства из полученного набора вводит цифры по заранее определенному алгоритму. Например, пользователь получает всегда набор из десяти цифр, по своему алгоритму, записанному в базе данных, ему нужно ввести третью, пятую, первую и седьмую цифры. Он выбирает именно эти цифры из полученной последовательности и вводит их на экране мобильного в обозначенном порядке. Затем полученный PIN-код отсылается на считыватель (рис. 5).

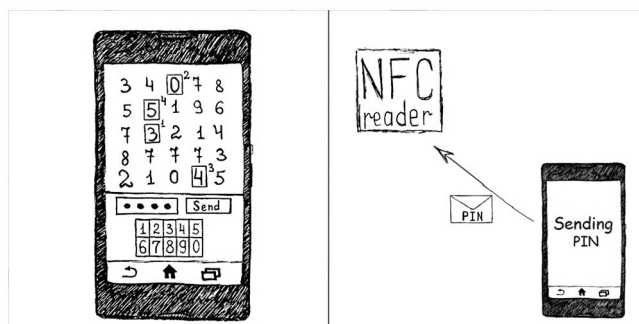


Рис. 5. Отправка PIN-кода

- Считыватель обрабатывает полученный PIN-код, проверяет соответствие введенного PIN-кода и PIN-кода полученного в ходе применения алгоритма пользователя к полученной последовательности. При совпадении PIN-кодов человек допускается на режимный объект, в ином случае – запрещается (рис. 6).

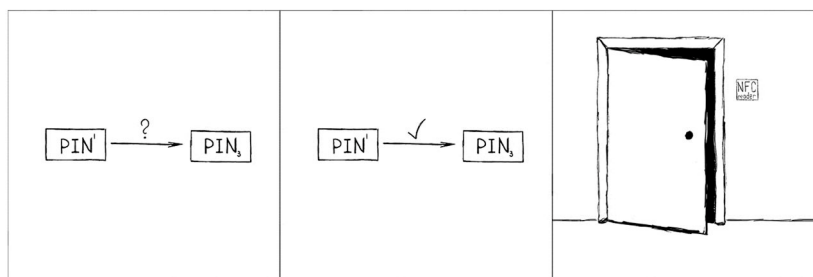


Рис. 6. Сверка пароля и открытие доступа

При первом запуске приложение на телефон у пользователя будет запрошен ID, который будет выдаваться пользователю администратором и иметь определенную длину и сложность. Идентификационный номер будет записан в память приложения. Далее приложение при запуске будет отправлять персональный ID, не спрашивая для этого разрешение у пользователя. Пользователь сразу увидит полученную последовательность цифр и поле для ввода PIN-кода.

Двухфакторная идентификация (ID, отсылаемый смартфоном, и PIN-код, вводимый человеком) предусматривает случай кражи или утери мобильного устройства – злоумышленнику недостаточно иметь смартфон, нужно знать алгоритм. Перехватить данные во время обмена довольно затруднительно за счет малого радиуса действия NFC, порядка 10–20 см.

7. Контрольные вопросы:

1. Что такое NFC? Что такое RFID? Каковы различия между ними
2. Схема распространения сигнала NFC.
3. Распространение сигнала NFC.
4. Будут ли сигналы NFC и RFID наводить помехи друг на друга?
5. Что такое NDEF?
6. Какие данные можно передавать с помощью NDEF? Пример NDEF-сообщения. Структура NDEF-сообщения. Максимальная длина NDEF-сообщений.

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: ФГБОУ ВО Алтайский государственный технический университет им. И.И. Ползунова, Борисов Алексей Павлович, alex.borisov84@gmail.com

Дисциплина: Современные компьютерные полиграфные системы

Образовательная программа: 10.03.01. Информационная безопасность.

Дисциплина: Современные компьютерные полиграфные системы.

Лабораторная работа.

Составление тестовых вопросников кадровых проверок.

Анализ полиграмм

1. Учебные цели:

- отработать навык наложения датчиков, отработать навык составления и проведения тестов полиграфных проверок;
- сформировать навык качественного анализа полиграмм;
- сформировать навык составления и проведения всех видов бесед.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Знать:

- роль и место применения полиграфных проверок в системе мер по защите информации на предприятии;
- естественнонаучные основы проведения психофизиологических исследований.

Уметь:

- правильно организовывать распределение задач в коллективе с учетом индивидуальных психофизиологических особенностей исполнителей
- использовать различные методики проведения психофизиологических исследований.

Владеть:

- навыками составления справки по результатам психофизиологических исследований;
- навыками работы с техническими средствами, используемыми при проведении психофизиологических исследований.

3. Перечень материально-технического обеспечения

- мультимедийный проектор, экран для проекции;
- полиграфы «РИФ» в количестве одной штуки на каждые 4 учащихся учебной группы.

4. Краткие теоретические сведения

Краткий алгоритм собеседования с использованием полиграфа

1. Предварительная беседа со специалистом.

Оценка общего состояния собеседника-проверяемого, заполнения документа (заявления) о добровольном согласии на проведение тестирования.

Собеседуемое лицо знакомится с методом проверки, общими принципами исследования, правилами поведения и рекомендациями о том, как вести себя во время тестирования.

2. Обсуждение вопросов.

Собеседуемое лицо знакомится с вопросами, которые будут использоваться при исследовании. Обдумывает их, при необходимости обсуждает их содержание со специалистом, даёт пояснения.

3. Проверка на полиграфе (непосредственное тестирование).

Установка датчиков на проверяемое лицо, инструктаж, собеседование.

Собеседуемое лицо в ходе тестирования отвечает на вопросы однозначно "да" или "нет". В случае невозможности принять однозначное решение собеседуемое лицо может промолчать (воздержаться от ответа).

Одновременно в ходе данного этапа с помощью полиграфа фиксируется динамика изменений психофизиологических параметров собеседуемого лица.

Общее время процедуры проверки на полиграфе варьируется от 1,5 до 3,5 ч. Имеются перерывы (по согласованию со специалистом-полиграфологом).

Процедура проверки на полиграфе абсолютно безвредна.

Итоговый результат собеседования оформляется в виде документа – "заключения" (суждения специалиста).

Информация, которая была получена во время процедуры проверки, является конфиденциальной и передаётся только заказчику (инициатору проверки).

В дальнейшем, переданная инициатору тестирования информация обычно не хранится, если не было других договоренностей с заказчиком (например, в случае долгосрочного сотрудничества на проведение проверок сотрудников компании).

5. Порядок выполнения лабораторной работы (этапы)

Подготовительный этап:

1. Учебная группа разбивается на ячейки (по 4–5 человек).
2. Накануне занятия в каждой ячейке выбираются новый «тестируемый» и новый «полиграфолог».
3. Накануне занятия все члены ячейки, кроме «тестируемого», готовят анкеты для сбора автобиографических данных «тестируемого» при его приеме на работу, текст предтестовой беседы, стимулирующие тесты (угадывание имени, чисел, карточный тест), тесты для проверки анкетных данных «тестируемого» (по 3 общим тестам по всем направлениям кадровых проверок и по 3 тестам проверки единичных данных по всем направлениям кадровых проверок).
4. Студенты ячейки готовят задание на полиграфную проверку в отношении «тестируемого» (считается, что «тестируемый» будет проходить кадровую полиграфную проверку при приеме его на работу на должность специалиста по защите информации в ОАО «Банк Рога и Копыта»).
5. Студенты ячейки готовят заявление о добровольном согласии «тестируемого» на полиграфную проверку.

Очный этап:

1. «Тестируемый» от ячейки проходит анкетирование. Заполненные анкеты меняются между ячейками.
2. «Полиграфолог» проводит с «тестируемым» кадровую проверку на полиграфе (проверяет правдивость биографических данных, мотивы поступления на работу, мотивы ухода с предыдущей работы, пристрастие к азартным и компьютерным играм, интернет-зависимость, пристрастие к курению, склонность к жестокости при общении, склонность к неумеренному употреблению пищи. Не следует проверять в учебных целях связь с криминальными элементами, пристрастие к алкоголю или наркотическим веществам).
3. Студенты ячейки готовят заключение полиграфной проверки в отношении «тестируемого» (в заключении приведены все вопросы тестов, дословные ответы «тестируемого» на вопросы тестов, реакции «тестируемого» на вопросы тестов, выводы полиграфолога).
4. Студенты ячейки готовят отчет о лабораторной работе (титальный лист, анкеты для сбора данных, конспект предтестовой беседы, задание на проверку, заявление о согласии, заключение проверки, скриншоты полиграмм, вывод по лабораторной работе).
5. Защищают отчет, отвечая на вопросы преподавателя.

6. Контрольные вопросы:

1. Раскройте особенности составления тестов для данного вида проверок.
2. Раскройте особенности процедуры проведения данного вида проверок.
3. Какое количество тестов необходимо для данного вида проверок?
4. Укажите виды тестов, применяемых для данного вида проверок.
5. Какие сведения подлежат проверке, при проведении данного вида проверки?
6. Что, как правило, скрывает тестируемый при проведении данного вида проверки?

Время на выполнение лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: ФГБОУ ВО «Кубанский государственный технологический университет», доцент кафедры КТИБ, Шарай В.А., wsharay@yandex.ru

Дисциплина: Техническая защита информации

Образовательная программа: 10.03.01 Информационная безопасность.

Дисциплина: Техническая защита информации.

Лабораторная работа.

Обнаружение скрытых видеокамер с помощью поискового прибора «Оптик»

1. Учебные цели:

Изучить методику поиска объектива скрытой видеокамеры. Отработать навыки предотвращения утечки видовой информации по визуально-оптическому каналу.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

- **Уметь** осуществлять технические мероприятия по обеспечению защиты информации от ее утечки по техническим каналам с учетом организационной структуры объекта защиты и вероятных угроз; проводить специальные исследования технических средств и систем для аттестации объектов на соответствие требованиям нормативных документов.
- **Владеть** навыками безопасного применения ТСЗИ в профессиональной деятельности.

3. Перечень материально-технического обеспечения

Лабораторное оборудование: Профессиональный обнаружитель скрытых видеокамер «Оптик» – 1 шт., Миниатюрная цветная камера RVi-C100 (2.5 мм) – 2 шт.

4. Задание на исследование:

- произвести визуальный осмотр защищаемого помещения на предмет наличия скрытых видеокамер;
- произвести осмотр помещения на предмет наличия скрытых видеокамер с помощью профессионального обнаружителя скрытых видеокамер «Оптик»;
- отобразить результаты осмотра на схеме исследуемого помещения, используя схему помещения (рис. 5);
- сделать выводы.

5. Краткие теоретические сведения

Современная концепция защиты информации, циркулирующей в помещениях или технических системах коммерческого объекта, требует не периодического, а постоянного контроля в зоне расположения объекта. Защита информации включает в себя целый комплекс организационных и технических мер по обеспечению информационной безопасности техническими средствами. Одна из решаемых задач – защита информации по каналу утечки видовой информации. В зависимости от характера информации можно выделить следующие способы ее получения: наблюдение за объектами, съемка объектов, съемка документов. Съемка объектов с использованием телевизионной видеокамеры закамуфлированной под интерьер зачастую осуществляется с последующей передачей изображения по радиоканалу. Задача предотвращения утечки видовой информации решается исключительно способами и средствами инженерно-технической защиты информации.

Для обнаружения скрытых видеокамер применяется различное поисковое оборудование, основанное на различных способах обнаружения:

- поиск видеокамер с помощью нелинейного локатора;
- поиск беспроводных видеокамер с помощью средств радиомониторинга;
- поиск видеокамер с помощью средств анализа побочного электромагнитного излучения;
- поиск видеокамер по оптическому принципу.

В данной лабораторной работе будем производить поиск скрытых видеокамер по оптическому принципу. В качестве оборудования будем использовать прибор «Оптик». Профессиональный обнаружитель скрытых видеокамер «Оптик» предназначен для поиска и локализации скрытых (камуфлированных в интерьер) видеокамер типа «пинхол» независимо от их состояния (включено/выключено) и типа передачи видеосигнала. Внешний вид прибора показан на рисунке 1.

Поиск объектива видеокамеры осуществляется методом световой локации. При обнаружении объектива скрытой камеры в объективе прибора «Оптик» будет наблюдаться точечное пятно зеленого или красного цвета – результат отражения подсветки от видеокамеры. Технические характеристики прибора представлены в таблице 1.

ВНИМАНИЕ: прибор работает от встроенного аккумулятора, установленного на предприятии изготовителе. Заряд аккумулятора прибора осуществляется от зарядного устройства (5 В, 0,6 А) из комплекта поставки. Заряд осуществляется при выключенном приборе. Полностью разряженный прибор заряжается в течение 4 часов.



Рис. 1. Прибор «Оптик»

Таблица 1 – Технические характеристики прибора «Оптик»

№ п/п	Параметр	Значение
1.	Дальность обнаружения: (зависит от световой обстановки (освещённости помещения))	от 0,5 до 50 метров
2.	Угол обзора:	7,5 град.
3.	Кратность	6,5х
4.	Диапазон фокусировки:	от 0,5 метра до ∞
5.	Режим работы:	– непрерывный зелёный – непрерывный красный – импульсный зелёный – импульсный красный – импульсный красно-зелёный
6.	Тип питания:	Li-ion аккумулятор 3,7 В
7.	Вид подсветки:	светодиодная
8.	Количество светодиодов	22 шт.
9.	Цвет подсветки	зелёная, красная, красно/зелёная
10.	Масса прибора (грамм)	450 гр.
11.	Масса прибора в транспортной сумке, с зарядным устройством	800 гр.
12.	Время работы (при полностью заряженном аккумуляторе)	– в импульсном режиме при работе красно/зелёной подсветки: не менее 4-х часов – в непрерывном режиме: не менее 6-ти часов

Вставьте зарядное устройство в сеть 220 В (50 Гц). Светодиод на зарядном устройстве должен загореться красным цветом при подключении к сети 220 В.

Подключите штекер зарядного устройства в разъем прибора с надписью +5v. При подключении загорится индикатор CNG на приборе, подтверждающий начало заряда. Светодиод на зарядном устройстве при заряде горит красным цветом.

По окончании заряда, как показано на рисунке 2, индикатор CNG на приборе погаснет.

Отключите зарядное устройство от прибора, затем от сети 220 В.



Рис. 2. Внешний вид зарядного устройства

Прибор готов к работе.

6. Порядок выполнения лабораторной работы

Работа с прибором заключается в равномерном осмотре с его помощью проверяемого помещения.

Для обнаружения видеокамеры необходимо находиться в том месте, которое предположительно является объектом скрытого видеонаблюдения. Если ходить по помещению и просто осматривать интерьер через «Оптик», камера может быть не обнаружена.

Например, если предполагается ведение скрытого видеоконтроля стола руководителя, необходимо сесть в кресло руководителя и вести поиск именно с этой точки.

При обнаружении бликующего точечного пятна необходимо осмотреть это место с близкого расстояния и определить источник блика.

Основной режим работы прибора – непрерывный. Импульсный режим является дополнительным и используется при проверке в обычной световой обстановке. В затемнённом помещении рекомендуется использовать непрерывный режим.

На рисунках 3–4 показан пример выявленной видеокамеры.



Рис. 3. Осмотр предмета без прибора «Оптик»

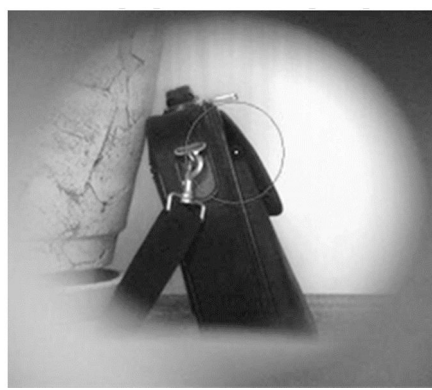


Рис. 4. Осмотр предмета с помощью прибора «Оптик»

Рекомендации по поиску скрытых камер. Основным правилом при обнаружении скрытых камер является необходимость находиться в месте, которое вероятнее всего интересует лиц, установивших камеру (или между предполагаемым местом установки видеокамеры и местом съёмки).

Вероятнее всего такими местами являются: места работы (столы с сидящими за ними людьми), места отдыха (кресла, диваны, кровати). В случае если интерес может представлять, посещало ли то или иное лицо помещение – камера может быть направленно на дверной проём.

Необходимо учитывать, что видеокамер может быть несколько. Обнаружение одной или двух видеокамер не даёт право сделать вывод, что помещение проверено. Для этого необходимо проверить все места, из которых возможен видеоконтроль.

Наиболее сложен поиск в помещениях с большим количеством бликующих объектов – большое количество зеркал, стекла и т.д. В случае обнаружения блика, мешающего осмотру какой-либо поверхности, необходимо сменить угол, под которым осматривается поверхность. Зачастую достаточно переместиться на шаг и блик исчезнет. При этом блик от объектива останется.

Необходимо при проверке помещений стараться не стоять под прямым углом к бликующей поверхности.

Видеокамеры могут быть установлены в любую деталь интерьера, подходящую для такой установки. Это может быть подвесной потолок, видео- и аудиоаппаратура, картины, декоративные украшения и т.д.

Поиск значительно облегчается и яркость видимого пятна от засветки объектива возрастает, если в помещении нет прямых солнечных лучей. Нет необходимости «делать темноту» – достаточно создать нормальную для работы световую обстановку. При необходимости можно работать и практически в сторону Солнца, но при этом глаз оператора способен различить пятно объектива с 1-2 метров.

Данные рекомендации справедливы при работе с любым обнаружителем скрытых видеокамер, работающим по принципу обнаружения бликующих объектов.

Правила техники безопасности. Внимание! В приборе установлены стеклянные оптические элементы. В случае разбития любого из них запрещается эксплуатация прибора во избежание получения травм.

Не наводить включенную подсветку на глаза людей. Кратковременная засветка глаз безопасна.

Избегать попадания прямых солнечных лучей и нагрева прибора.

Не разбирать и не бросать прибор.

Не оставлять на длительное время под воздействием низких температур – прибор предназначен для работы в обычных помещениях при температуре от +5 до +40 °С

Для чистки загрязненной оптики используйте только салфетки, предназначенные для протирки оптических устройств.

7. Контрольные вопросы:

1. По какому принципу работает обнаружитель скрытых видеокамер?
2. Какова дальность обнаружения прибора?
3. При каких условиях облегчается поиск скрытых видеокамер?

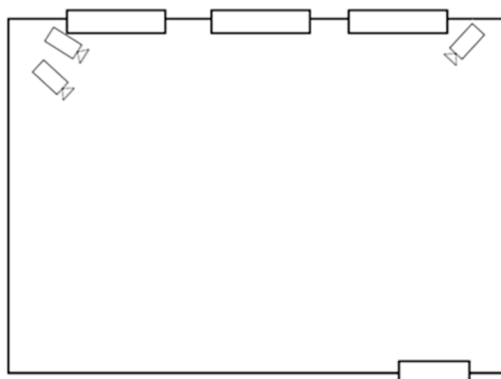


Рис. 5. Схема исследуемого помещения

Время на выполнение лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: ФГБОУ ВО «Пятигорский Государственный Университет», Калиберда Игорь Владимирович, kaliberda-igor@yandex.ru

Образовательная программа: 10.03.01 Информационная безопасность, Организация и технология защиты информации.

Дисциплина: Техническая защита информации.

Лабораторная работа.

Исследование звукоизоляционных свойств различных материалов

1. Учебные цели:

Изучение возможностей организации пассивных мер защиты охраняемого объекта от перехвата информации по акустическому каналу.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Выпускник умеет: анализировать и оценивать угрозы информационной безопасности объекта; проводить мониторинг угроз безопасности информационных систем. Выпускник владеет: методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации.

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение: Измеритель акустического и вибрационных шумов ВШВ-002, измерительный микрофон СМ-100, акустический излучатель, штатив для установки микрофона di.com, генератор тестовых сигналов, шумоизоляционная камера камера.

4. Задание на исследование

Исследовать звукоизоляционные свойства различных материалов.

5. Краткие теоретические сведения

Звукоизоляция – это свойство конструкций задерживать часть энергии попадающих на них звуковых волн, которое определяется отношением интенсивностей падающих волн и волн, отраженных от ограждающей поверхности, т.е. снижение уровня шума, проникающего в помещения извне.

Звукопоглощение – это процесс преобразования звуковой энергии в тепловую при распространении звука в среде или при падении звука на границу двух сред «воздух/ограждающая конструкция». Звукопоглощение, характеризуется коэффициентом звукопоглощения

6. Порядок выполнения лабораторной работы (этапы)

- 1) собрать лабораторную установку;
- 2) измерить общий уровень шума;
- 3) измерить уровень шума в шумоизоляционной камере, при размещении на пути звука пенопласта и картона;
- 4) перевести значения звукового давления в Вт с помощью формулы;
- 5) вычислить значение звукоизоляционного коэффициента по формуле;
- 6) сделать вывод о звукоизоляционных свойствах материала.

Общая структурная схема лабораторной установки представлена на рисунке 1.

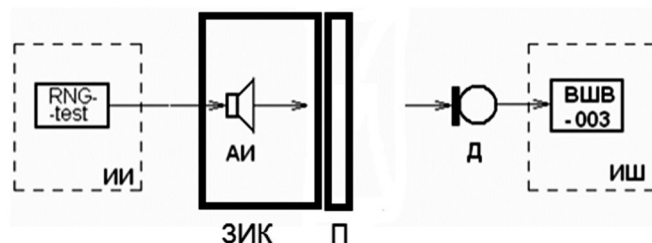


Рис. 1. Схема лабораторной установки

Используемые сокращения:

- ИИ – источник информации;
- АИ – акустический излучатель;
- ЗИК – звукоизоляционная камера;
- П – препятствие, исследуемый материал;
- Д – датчик (измерительный микрофон);
- ИШ – измеритель шума ВШМ – 003 – М2.

В качестве тестовых сигналов используются тональные гармонические сигналы, соответствующие серединам октавных полос. Источником гармонических сигналов служит устройство RNG-test представленное на рисунке 2. Прибор предназначен для проведения исследований по защищенности помещений от утечки информации по акустическим и виброакустическим каналам. Для проведения подобных исследований, формируются акустические сигналы с разными частотами.

Для сборки экспериментальной установки, схема которой приведена на рисунке 1, нужно подключить акустический излучатель к генератору тестовых сигналов. Включить прибор. После включения прибора светодиоды, индицирующие значения формируемых частот будут последовательно загораться, отображая нормальную работу прибора. Таких циклов индикации будет три. После этого прибор готов к работе. Для формирования необходимой частоты тестового сигнала необходимо нажать соответствующую кнопку. После этого над кнопкой загорится светодиод, отображая начало формирования тестового сигнала. Для прекращения формирования сигнала нужно повторно нажать кнопку, расположенную под горящим диодом. Для перехода к формированию сигнала с другой частотой необходимо нажать соответствующую кнопку. Вращением регулятора уровня выходного сигнала можно установить необходимую громкость.

Предусилитель микрофонный ВПН-101 с капсулом микрофонным конденсаторным М-101, помещается перед шумоизоляционной камерой на расстоянии 1 м. Предусилитель микрофонный соединяется с измерителем шума и вибраций ВШМ-003-М2. Измеряется общий уровень шума, без материалов. После чего между АИ и микрофоном размещаются звукоизолирующие материалы.



Рис. 2. Подключение и размещение

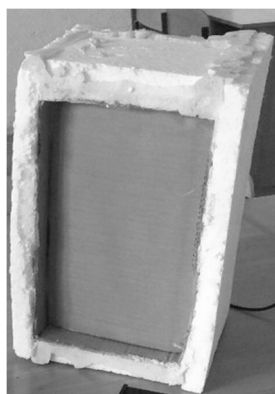


Рис. 4. Картон, помещенный в шумоизоляционную камеру

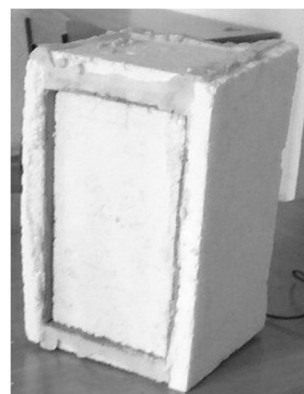


Рис. 5. Пенопласт, помещенный в шумоизоляционную камеру

После измерения уровня шума различных материалов результаты записываются в таблицу 1.

Таблица 1

	Частота, Гц				
	250	500	1000	2000	4000
Без материала, Вт					
Изолирующий материал 1, Вт					
Изолирующий материал 2, Вт					

7. Контрольные вопросы:

1. В чем заключается отличие понятий звукового давления, уровня звукового давления и уровня звука?
2. Какая полоса частот называется октавной?
3. Объясните физическую сущность звукоизоляции.
4. Что такое коэффициент звукоизоляции?
5. От чего зависит звукоизоляция ограждения?
6. Каким образом можно оценить эффективность применения различных звукопоглощающих материалов?
7. На чем основан эффект звукопоглощения и какими свойствами должны обладать звукопоглощающие материалы?
8. Эффективность установки звукопоглощающих облицовок.

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: Сибирский государственный университет геосистем и технологий, Кафедра Информационной безопасности, Поликанин Алексей Николаевич, ст. преподаватель, polikanin.an@yandex.ru

Образовательная программа 10.03.01 Информационная безопасность, Организация и технология защиты информации.

Дисциплина: Техническая защита информации.

Лабораторная работа. Экспериментально-расчетная оценка разборчивости речи

1. Учебные цели:

Изучение возможности съема акустической информации в помещении защищаемого объекта в зависимости от уровня полезного сигнала и естественных шумов.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Выпускник умеет: контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем. Выпускник владеет: навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты.

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение: Измеритель акустического и вибрационных шумов ВШВ-002, измерительный микрофон СМ-100, акустический излучатель, штатив для установки микрофона di.com, генератор тестовых сигналов.

4. Задание на исследование

Измерить уровень акустического шума и полезного сигнала в различных точках помещения и рассчитать индексы артикуляции и словесной разборчивости.

5. Краткие теоретические сведения

Разборчивость речи – это параметр, определяющий степень защищенности речевой информации, выражается процентным количеством правильно принятых элементов речи (звуков, слогов, слов, фраз) на выходе технического канала из их общего числа. Разборчивость речи делится на формантную R, слоговую S, словесную W и фразовую I. Между ними существует связь, установленная с помощью артикуляционных испытаний. Разборчивость речи тесно связана с характеристикой «понятность» речи.

Оценка разборчивости речи сводится к следующим этапам:

- принимается деление всего частотного диапазона на определенное число полос n (250, 500, 1000, 2000, 4000 Гц);
- для каждой «средней» частоты f_i , определяется относительный уровень интенсивности формант Q ;
- определяются соответствующие коэффициенты восприятия формант P_i ;
- рассчитывается интегральный индекс артикуляции (формантная разборчивость) R ;
- осуществляется переход к любым другим видам разборчивости (D, S, W), по известным для данного языка зависимостям.

6. Порядок выполнения лабораторной работы (этапы)

- 1) сборка и подключение лабораторного стенда согласно схеме эксперимента;
- 2) проверка функциональности оборудования;
- 3) измерение уровня акустического шума и полезного сигнала на пяти октавных полосах во всех исследуемых точках помещения;
- 4) измерение отдельно акустического шума в тех же точках и на тех же октавных полосах;
- 5) занесение экспериментальных данных в таблицу и расчет индексов артикуляции и словесной разборчивости согласно формулам.

Общая структурная схема лабораторной установки для анализа потенциального канала утечки информации, представлена на рисунке 1.

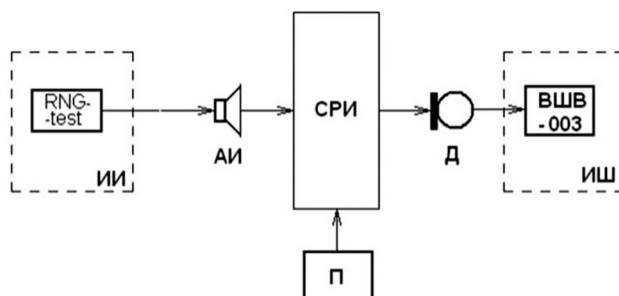


Рис. 1. Структурная схема установки

Используемые сокращения:

- ИИ – источник информации;
- АИ – акустический излучатель;
- СРИ – среда распространения информации;
- П – помехи;
- Д – датчик (измерительный микрофон);
- ИШ – измеритель шума ВШМ – 003 – М2.

В качестве тестовых сигналов используются тональные гармонические сигналы, соответствующие серединам октавных полос. Источником гармонических сигналов служит устройство RNG-test представленное на рисунке 2. Прибор предназначен для проведения исследований по защищенности помещений от утечки информации по акустическим и виброакустическим каналам. Для проведения подобных исследований, формируются акустические сигналы с разными частотами. Измеряя уровень сигнала в возможных каналах утечки информации (стены, стекла, вентиляция и т.д.), можно оценить степень защищенности помещения.



Рис. 2. RNG-test

Средой распространения информации (СРИ) служит помещение, степень защищенности которого оценивается. В помещении, где проводятся исследования, должно быть достаточно тихо (уровень шума 1–2 дБ). Для того чтобы смоделировать шум внутри помещения и за его пределами можно использовать аудиокolonку, на которую подается запись «белого» шума.

Для сборки экспериментальной установки, схема которой приведена на рисунке 1, нужно подключить акустический излучатель к генератору тестовых сигналов, как показано на рисунке 3. Включить прибор. После включения прибора светодиоды, индицирующие значения формируемых частот будут последовательно загораться, отображая нормальную работу прибора. Таких циклов индикации будет три. После этого прибор готов к работе. Для формирования необходимой частоты тестового сигнала необходимо нажать соответствующую кнопку. После этого над кнопкой загорится светодиод, отображая начало формирования тестового сигнала. Для прекращения формирования сигнала нужно повторно нажать кнопку, расположенную под горящим диодом. Для перехода к формированию сигнала с другой частотой необходимо нажать соответствующую кнопку. Вращением регулятора уровня выходного сигнала можно установить необходимую громкость.



Рис. 3. Подключение RNG-test к акустическому излучателю

В качестве измерителя шума и вибрации используется устройство ВШМ-003-М2, представленное на рисунке 4. Данный прибор предназначен для определения источников шумов и вибраций, а также для измерения параметров шума в свободных и диффузионных звуковых полях.



Рис. 4. ВШМ – 003 – М2

Измерение шума осуществляется предусилителем микрофонным ВПН – 101, показанным на рисунке 5, и присоединенным к нему капсулем микрофонным конденсаторным М-101. В измеритель шума и вибрации вставляется предусилитель микрофонный с предварительно помещенным в него капсулем М-101, как показано на рисунке 6.

Выбор расположения контрольных точек

Выбор контрольных точек от особенностей ограждающих конструкций располагаются следующим образом:

- за сплошной однородной конструкцией (за стеной);
- за окном и дверью;
- в случае наличия вентиляционного канала.

Данный выбор точек обусловлен тем, что акустический съем информации в этих точках легче всего производить.



Рис. 5. Предусилитель микрофонный ВПН – 101

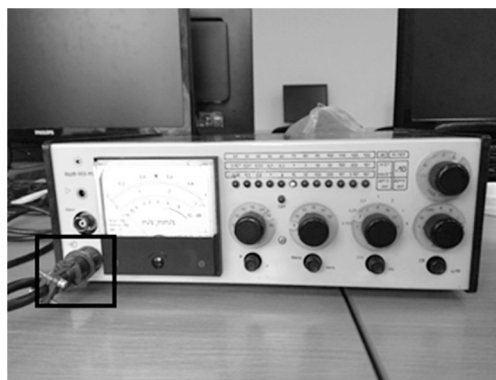


Рис. 6. Вход для предусилителя

7. Контрольные вопросы:

1. Акустический канал утечки информации.
2. Акустические речевые сигналы. Особенности их восприятия.
3. Фонемы, октавы и форманты в акустическом речевом сигнале.
4. Разборчивость речи. Определение, физическая сущность.
5. Словесная, слоговая и другие виды разборчивости речи
6. Характеристики речевого сигнала.
7. Обстоятельства, влияющие на разборчивость речи.
8. Порядок расчёта словесной разборчивости.
9. Наиболее опасные объекты с точки зрения акустической разведки.
10. Средства перехвата акустической информации.
11. Особенности использования виброакустического канала.

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: Сибирский государственный университет геосистем и технологий, Кафедра Информационной безопасности, Поликанин Алексей Николаевич, ст. преподаватель, polikanin.an@yandex.ru

Образовательная программа: 10.03.01 Информационная безопасность, Организация и технология защиты информации.

Дисциплина: Техническая защита информации.

Лабораторная работа.

Выявление несанкционированного съёма информации с помощью измерения физических характеристик сигнала в телефонной линии

1. Учебные цели:

Изучение работы средств контроля телефонных линий от возможности снятия информации по токоведущим линиям.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Выпускник умеет: анализировать и оценивать угрозы информационной безопасности объекта; проводить мониторинг угроз безопасности информационных систем. Выпускник владеет: методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации.

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение: Мини-АТС MAXICOM MP35, телефонные аппараты Panasonic, осциллограф, кабель RS-232, мультиметр, генератор регулируемых шумов по сети SELSP-44, переходники и адаптеры подключения к телефонной линии, диктофон.

4. Задание на исследование

Измерить параметры сигнала телефонной линии при работе приборов зашумления и без них.

5. Краткие теоретические сведения

Среди методов прослушивания телефонной линии и помещения переговоров можно выделить следующие:

- метод ВЧ-навязывания;
- использование микрофонного эффекта;
- использование выносных микрофонов;
- подслушивание с параллельного телефона;
- запись телефонных переговоров на диктофон;
- индуктивный съёмник;
- параллельный телефонный передатчик.

Для выявления несанкционированного доступа к информации в телефонной линии средства технической защиты используют следующие физические параметры:

- напряжение;
- сила тока;
- частота;
- электромагнитный фон;
- активное и реактивное сопротивление;
- фаза.

В данной лабораторной работе предстоит изучить способы защиты телефонной линии с помощью контроля физических параметров сигнала.

6. Порядок выполнения лабораторной работы (этапы)

- 1) калибрование;
- 2) подключение к телефонной линии осциллографа;
- 3) измерение напряжения и частоты;
- 4) подключение мультиметра последовательно к телефонной линии;
- 5) измерение силы тока и сопротивления;
- 6) подключение параллельного телефона к телефонной линии;
- 7) повторное измерение физических характеристик сигнала;
- 8) подключение телефонного радиосъёмника;
- 9) измерение физических характеристик;
- 10) подключение трансформатора;
- 11) измерение физических характеристик;
- 12) подключение генератора регулируемых шумов по сети SELSP-44;
- 13) настройка генерации ВЧ-сигналов;
- 14) измерение физических характеристик;
- 15) подключение осциллографа к ПЭВМ, запуск программы выявления несанкционированного съёма информации;
- 16) подключение параллельного телефона, телефонного радиосъёмника;
- 17) определение несанкционированного подключения с помощью программы;
- 18) подключение в общую сеть генератор высоких частот SELSP-44;
- 19) определение ВЧ-навязывания с помощью программы;
- 20) выполнение задания;
- 21) ответ на контрольные вопросы.

Осуществление калибрования. В меню «Utility» (Сервис) осциллографа (рис. 1) студент выбирает пункт «Do selfcalibration» (Выполни автокалибровку).

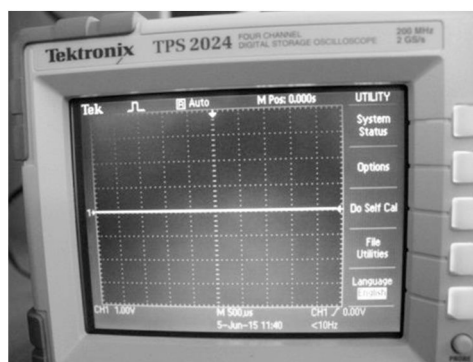


Рис. 1. Меню «Utility»

На экране появится сообщение о необходимости отключения всех пробников и кабелей из всех 4-х каналов, а затем нажать кнопку «ОК» (рис. 2).

Появится сообщение о калибровке с пройденными и оставшимися стадиями.



Рис. 2. Выполнение автокалибровки

Подключение осциллографа к телефонной линии. Для подключения используется телефонный адаптер (рис. 3, 4).



Рис. 3. Телефонный адаптер, аудио выход



Рис. 4. Телефонный адаптер. RJ-переходник

Осциллограф подключается к телефонной линии к каналу 1 с помощью кабеля и телефонного адаптера (рис. 5).



Рис. 5. Подключение осциллографа к телефонной линии

Чтоб увидеть реальную осциллограмму напряжения в телефонной линии, необходимо настроить развёртку по горизонтали и вертикали. Самым быстрым способом сделать это- нажать кнопку «autoset» (авто-установка). После этого студент переходит непосредственно к измерению физических характеристик сигнала.

Осциллограф позволяет измерить напряжение и частоту. Для получения данных характеристик сигнала, студент должен зайти в меню «measure» (измерения), и задать для каждого пункта требуемое значение (по умолчанию «none» – ни один из имеющихся). Для измерения частоты и напряжения, студент выбирает первые две ячейки, оставив источником 1 канал, и задав тип измеряемых данных для первой ячейки частота (frequency), а для второй, – напряжение (P1-P2). Напряжение берётся как расстояние между максимальным и минимальным значением осциллограммы (рис. 6, 8).

Подключение мультиметра к телефонной линии

Чтобы измерить силу тока, нужно так подключить мультиметр, чтобы ток прошёл через измеряющий прибор. Для этого подключаются пробники мультиметра типа «крокодилы» в разрыв несущей жилы последовательно (рис. 7).

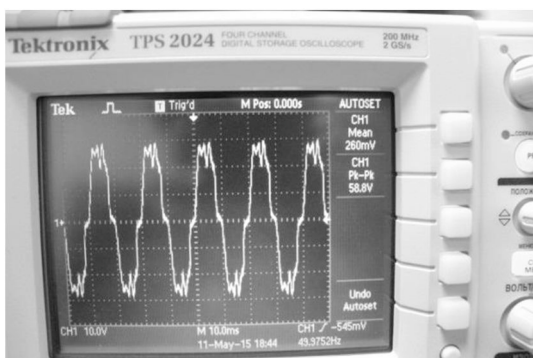


Рис. 6. Осциллограмма сигнала в телефонной линии при положенной трубке



Рис. 7. Последовательное подключение мультиметра к телефонной линии

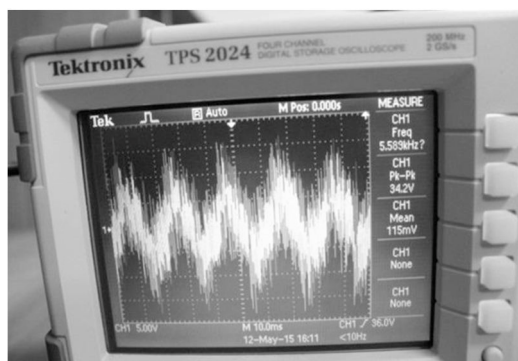


Рис. 8. Осциллограмма сигнала в телефонной линии при громком разговоре

Подключение параллельного телефона

Используя бухту кабеля КСПВ длиной 200 метров как имитацию протяжённой телефонной линии, выходящей за пределы контролируемой зоны, подключается один её конец к телефонному аппарату, а другой, – к мини АТС (рис. 9).

Затем к зачищенным контактам подключается параллельный телефонный аппарат.



Рис. 9. Подключение параллельного телефона к телефонной линии

Повторение пунктов 3) и 5).

Подключение телефонного радиосъёмника к телефонной линии (рис. 10)

Повторение пункта 8).

Подключение трансформатора (рис. 11)

Повторение пункта 10).

Включение в сеть генератора регулируемых шумов SELSP-44 (рис. 12).

Настройка генерации ВЧ-шумов.

В меню генератора выбирается пункт OutputLFSerup и снижается уровень генерации низкочастотных сигналов до нуля.

Повторение пункта и).



Рис. 10. Подключение телефонного радиосъёмника к телефонной линии



Рис. 11. Подключение трансформатора к телефонной линии



Рис. 12. Настройка генерации ВЧ-сигналов в генераторе SELSP-44

Съём информации с помощью диктофона
 Подключается диктофон через телефонный адаптер к телефонной линии, и осуществляется звукозапись (рис. 13).

Повторение пункта 10).

Подключение осциллографа к ПЭВМ

Осциллограф подключается к ПЭВМ с помощью кабеля RS-232 (рис. 14).

Запуск программы «Controline» (рис. 15).

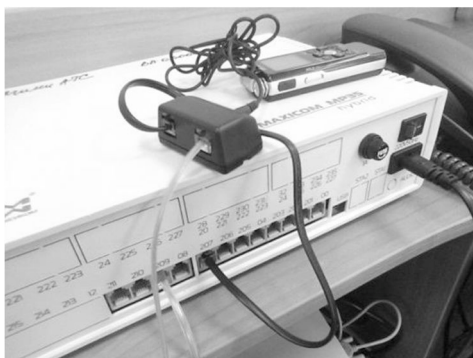


Рис. 13. Запись разговора с помощью диктофона, подключённого в разрыв



Рис. 14. Подключение осциллографа к ПЭВМ

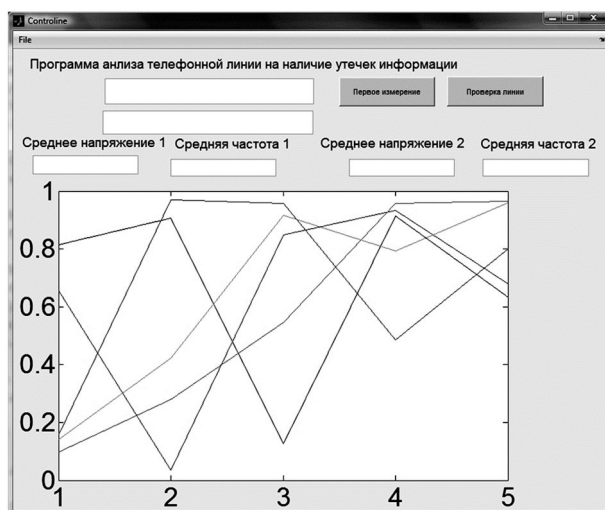


Рис. 15. Внешний вид окна программы Controline

Линия очищается от всех съёмных устройств, и нажимается кнопка «Первое измерение». Программа выводит осциллограмму на график, и выдаёт среднее арифметическое значение из 20 измерений напряжения и среднее арифметическое значение из 20 измерений частоты в полях «Среднее напряжение 1» и «Средняя частота 1», которые принимаются за эталонные (рис. 16).

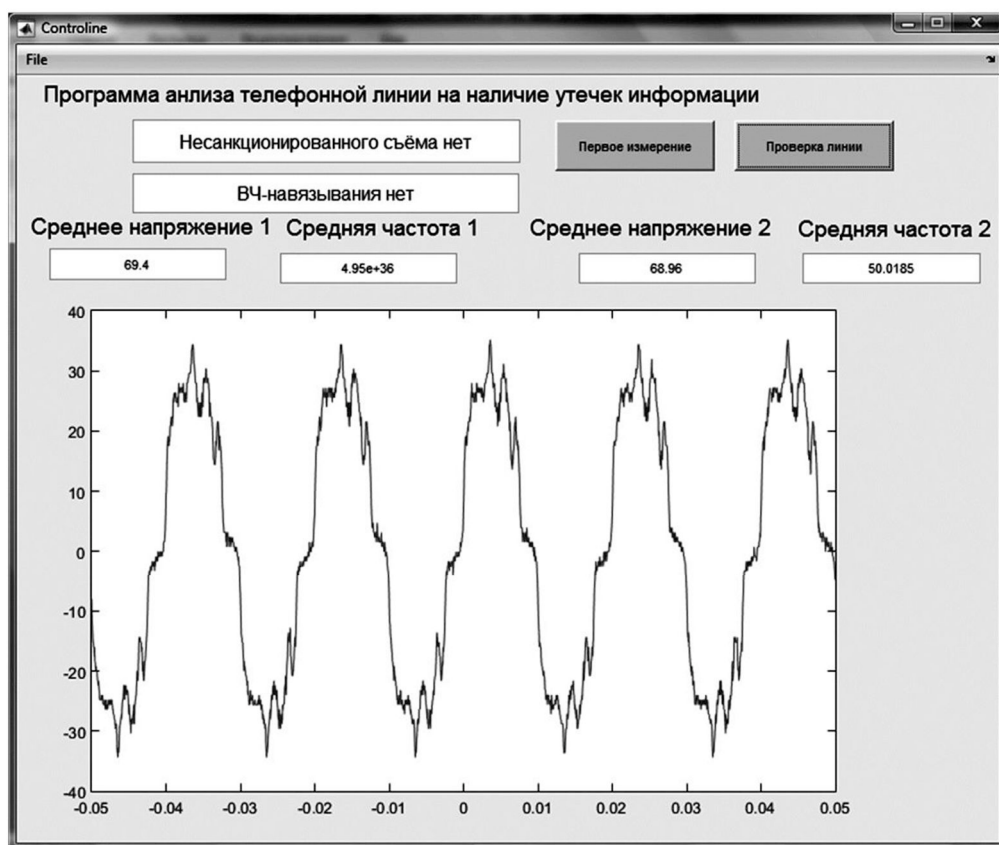


Рис. 16. Чистая линия

По нажатию кнопки «Проверка линии» происходит повторный замер напряжения и частоты проверяемой линии, и сравнение значения среднего арифметического замеренных значений с эталонными. В случае разницы между напряжением эталонным «Напряжение 1» и напряжением повторно измеренным «Напряжение 2» будет превышать 1 вольт, то программа выдаст сообщение «Несанкционированный съём информации» (рис. 17–19). Если напряжённе замеренное повторно превышает эталонное напряжение в 10 раз, то программа выдаст сообщение «ВЧ-навязывание» (рис. 20).

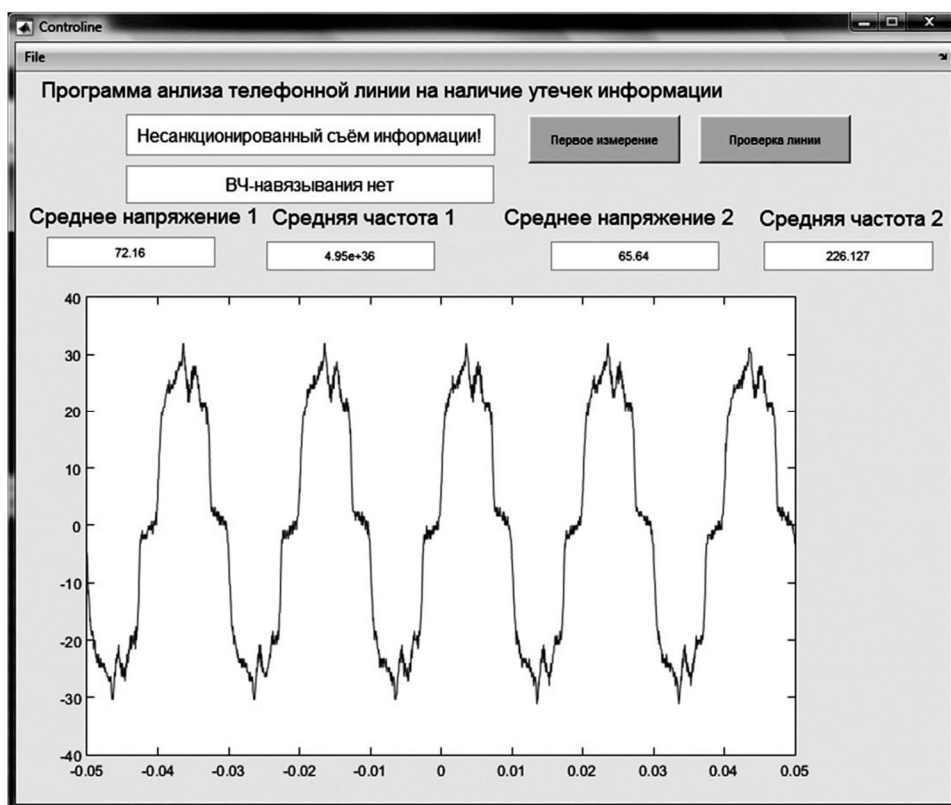


Рис. 17. Параллельный телефон

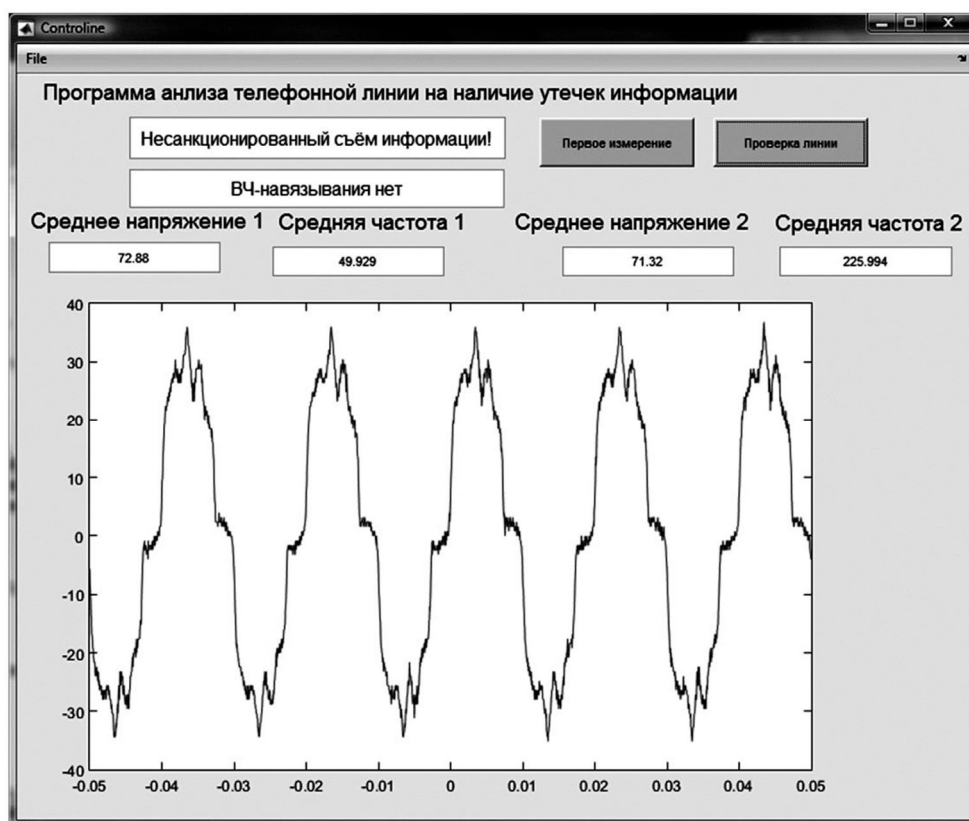


Рис. 18. Телефонный радиосъёмник

Результатом лабораторной работы является заполненная в ходе выполнения работ таблица. После её заполнения необходимо сделать вывод о том, как можно защититься от несанкционированного съёма информации (табл. 1).

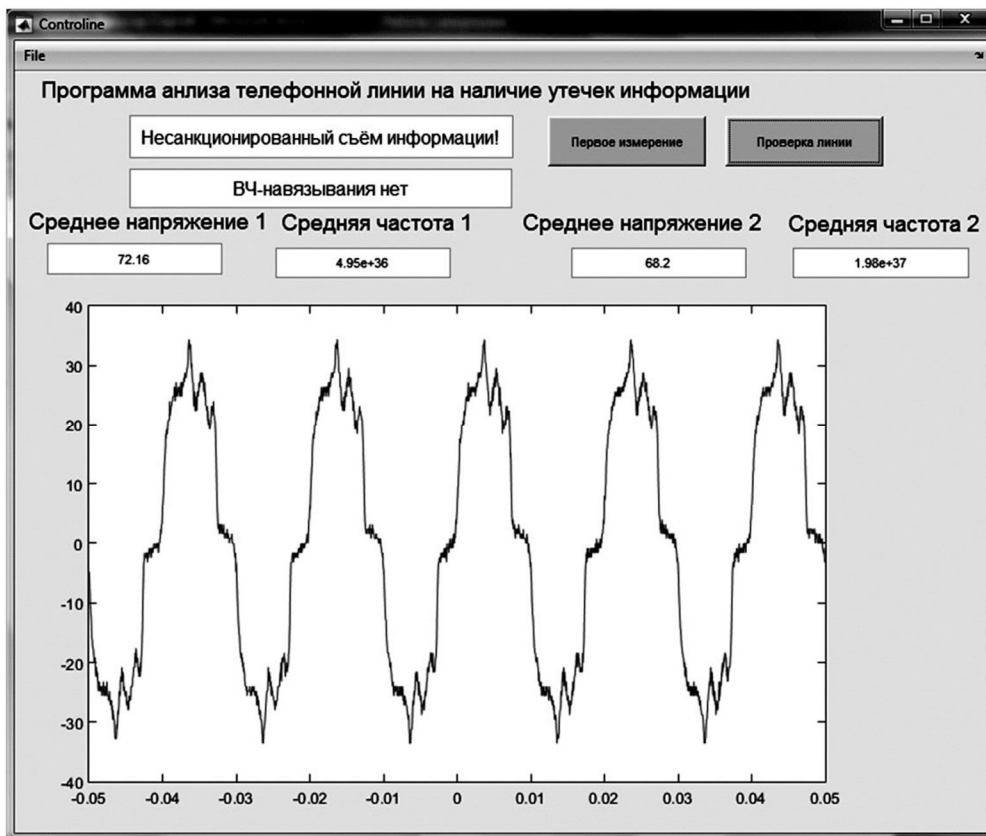


Рис. 19. Контактное подключение трансформатора

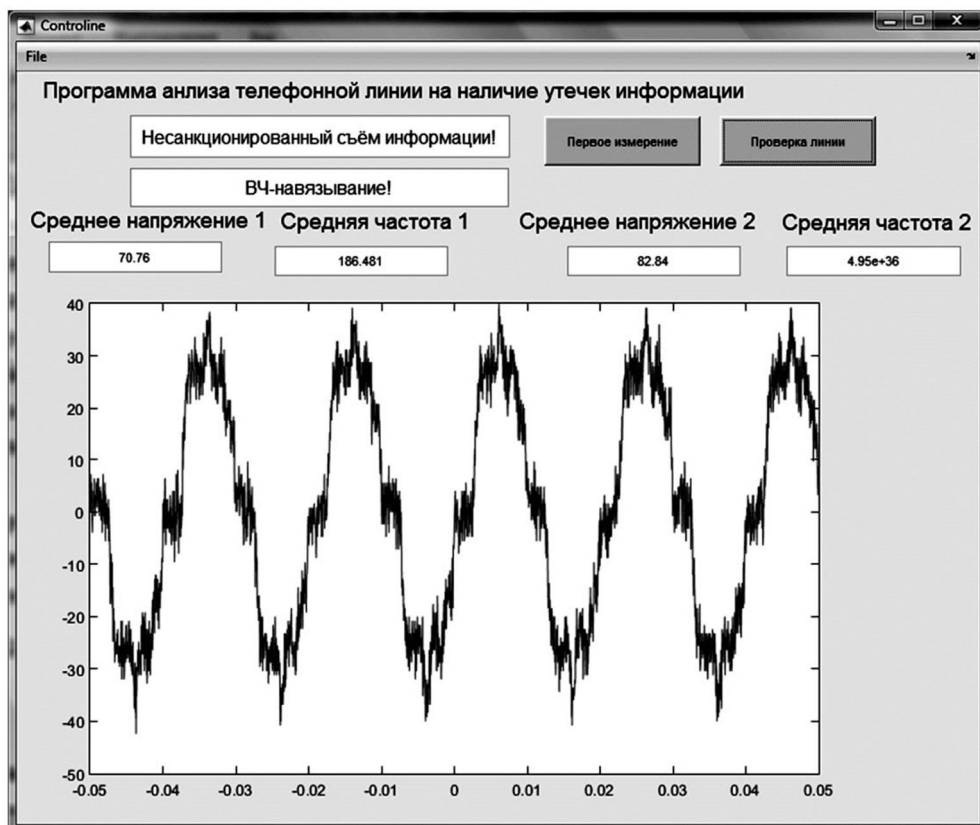


Рис. 20. Высокочастотное навязывание

Таблица 1 – Отчётность по лабораторной работе № 1

Режим работы линии	Значение изменения напряжения (Рк-Рк) (Вольт)	Значение изменения силы тока (мили Ампер)	Значение изменения частоты (Герц)
Чистая линия			
Параллельный телефон			
Диктофон			
Телефонный радиосъёмник			
Подключение через трансформатор			
ВЧ-навязывание			

7. Контрольные вопросы:

1. Какие каналы утечки информации есть в телефонной линии?
2. Как меняются физические параметры сигнала в телефонном кабеле при контактном подключении?
3. Как меняются физические параметры сигнала в телефонном кабеле при ВЧ-навязывании?
4. На каком принципе основан индуктивный съём информации?
5. Что такое амплитудно-частотная характеристика сигнала?
6. Что такое микрофонный эффект?
7. Каковы принципы работы устройств выявления утечки информации в телефонной линии?

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: Сибирский государственный университет геосистем и технологий, Кафедра Информационной безопасности, Поликанин Алексей Николаевич, ст. преподаватель, polikanin.an@yandex.ru

Дисциплина: Физические основы защиты информации

Образовательная программа: 10.03.01. Информационная безопасность, Организация и технология защиты информации.

Дисциплина: Физические основы защиты информации.

Лабораторная работа.

Формулы Френеля. Коэффициенты отражения от поверхности диэлектрика под различными углами

1. Учебные цели:

Изучить зависимость коэффициентов отражения для световой волны с различной поляризацией. Отработать навыки проведения эксперимента с компьютерной обработкой результатов.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

- Уметь выделять конкретную физическую сущность в прикладных задачах; применять полученные знания при освоении последующих инженерных дисциплин.
- Владеть навыками обработки результатов измерений и умения делать основные выводы; самостоятельной работой с учебной, научной и справочной литературой

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение. Лабораторный стенд состоит из источника поляризационного монохроматического света 1 (рис. 1), поворотной светоотражательной призмы 2, светоизмерительного устройства на магнитной платформе 3, датчика угла поворота. К приборам и принадлежностям относятся также компьютер с необходимым программным обеспечением.

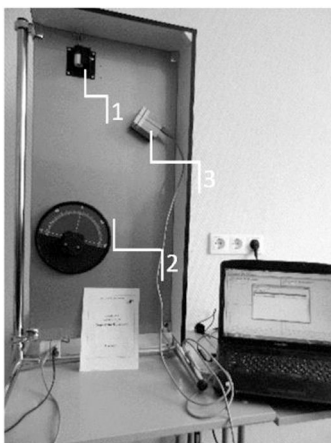


Рис. 1. Лабораторный стенд

4. Задание на исследование

- Получение экспериментальных зависимостей для коэффициента отражения от угла падения для волн различной поляризации.
- Сравнение с зависимостями по формулам Френеля.

5. Краткие теоретические сведения

Оптико-электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей. Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности) и принимается приемником оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация (рис. 2), причём лазер и приемник оптического излучения могут быть установлены в одном или разных местах (помещениях).

Физические принципы, лежащие в основе образования оптоакустического канала утечки информации, можно представить в виде следующей схемы: лазерный пучок используется для сканирования (в режиме отражения) поверхности стекла (рис. 3), участки которого испытывают микродвижения, сопровождающиеся распространением акустической волны.

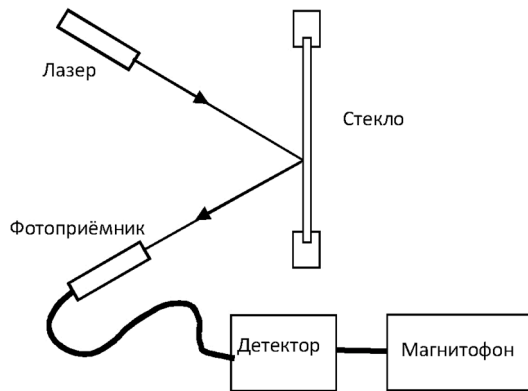


Рис. 2. Схема организации оптико-электронного канала утечки акустической информации

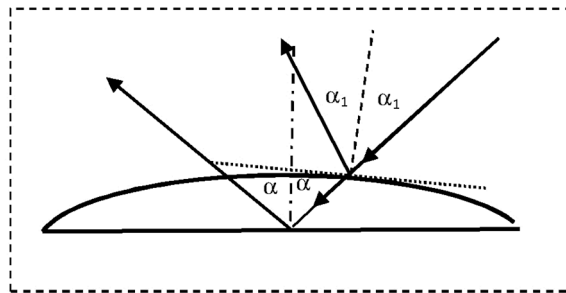


Рис. 3. Схема изменения условий отражения лазерного луча на вибрирующей поверхности

Вероятная последовательность преобразований информации о звуковом поле:

$$p(\Omega) \rightarrow \xi(\Omega) \rightarrow \varphi(\Omega) \rightarrow R(\Omega) \rightarrow E_{\text{отр}}(\Omega, \omega) \rightarrow I(\Omega, \omega) \rightarrow U(\Omega) \rightarrow p(\Omega).$$

Лазерный пучок падает на поверхность стекла. Плоская монохроматическая волна $p(\Omega)$ акустического поля помещения вызывает периодические, упругие деформации $\xi(\Omega)$ поверхности стекла. Из-за микродеформаций поверхности с частотой звука Ω изменяется угол падения (и, соответственно, угол отражения) сканирующего лазерного пучка – $\varphi(\Omega)$. Это изменение порождает изменение коэффициентов Френеля R , зависящих от $\varphi(\Omega)$, а следовательно, и от угловой частоты колебаний – Ω . Далее вследствие изменения коэффициентов Френеля происходит изменение вектора напряженности электрического поля отраженного пучка – $E_{\text{отр}}(\Omega, \omega)$. Изменение амплитуды вектора напряженности электрического поля во времени означает вариацию интенсивности отраженного пучка – $I_{\text{отр}}(\Omega, \omega)$. Поэтому следует, что изменение интенсивности отраженного лазерного пучка за счет изменения амплитуды $E_{\text{отр}}(\Omega, \omega)$ несет информацию об акустическом поле помещения. Работа фотоумножителя связана с его реакцией на изменение входного потока света, поэтому в нем образуется переменное напряжение звуковой частоты – $U(\Omega)$. Далее переменное напряжение звуковой частоты преобразуется в звуковое давление на выходе динамика – $p(\Omega)$.

Формулы Френеля для s-поляризации и p-поляризации различаются. Поскольку свет с разными поляризациями по-разному отражается от поверхности, то отраженный свет всегда частично поляризован, даже если падающий свет не поляризован. Угол падения, при котором отраженный луч полностью поляризован, называется углом Брюстера; он зависит от отношения показателей преломления сред, образующих границу раздела.

s-поляризация

$$S = \frac{2n_1 \cos \theta_i}{n_1 \cos \theta_i + n_2 \cos \theta_t} P, \quad Q = \frac{n_1 \cos \theta_i - n_2 \cos \theta_t}{n_1 \cos \theta_i + n_2 \cos \theta_t} P,$$

где θ_i – угол падения, θ_t – угол преломления, n_1 – показатель преломления среды, из которой падает волна, n_2 – показатель преломления среды, в которую волна проходит, P – амплитуда волны, которая падает на границу раздела, Q – амплитуда отраженной волны, S – амплитуда преломленной волны.

Углы падения и преломления связаны между собой законом Снеллиуса

$$\frac{\sin \theta_i}{\sin \theta_t} = \frac{n_2}{n_1}.$$

Коэффициент отражения

$$R_s = \frac{|Q|^2}{|P|^2} = \frac{\sin^2(\theta_i - \theta_t)}{\sin^2(\theta_i + \theta_t)}.$$

Коэффициент прохождения

$$T_s = \frac{|S|^2}{|P|^2} = \frac{\sin 2\theta_i \sin 2\theta_t}{\sin^2(\theta_i + \theta_t)}.$$

p-поляризация

$$S = \frac{2n_1 \cos \theta_i}{n_2 \cos \theta_i + n_1 \cos \theta_t} P, \quad Q = \frac{n_2 \cos \theta_i - n_1 \cos \theta_t}{n_2 \cos \theta_i + n_1 \cos \theta_t} P,$$

где P, Q и S – амплитуды волны, которая падает на границу раздела, отражённой волны и преломлённой волны, соответственно.

Коэффициент отражения

$$R_p = \frac{\operatorname{tg}^2(\theta_i - \theta_t)}{\operatorname{tg}^2(\theta_i + \theta_t)}.$$

Коэффициент прохождения

$$T_p = \frac{\sin 2\theta_i \sin 2\theta_t}{\sin^2(\theta_i + \theta_t) \cos^2(\theta_i - \theta_t)}.$$

6. Порядок выполнения лабораторной работы (этапы)

1. Войдите в программу «Физика-практикум» и выберите сценарий «Формулы Френеля».
2. Включите лазер. Поверните лазер вдоль его продольной оси в одно из крайних положений. Положение рукоятки вдоль рабочей поверхности установки соответствует s-волне, а перпендикулярно рабочей поверхности – p-волне.
3. Измерьте интенсивность излучения, падающего на поверхность призмы. Для этого поверните лазер так, чтобы его луч проходил мимо призмы и попадал в отверстие приемника излучения, расположенного вблизи нижней кромки лимба и ориентированного так, чтобы его продольная ось была параллельна направлению луча.
4. Нажмите экранную кнопку начала регистрации данных и убедитесь, что положение приемника обеспечивает максимальный уровень сигнала, (для этого следует немного изменять угол наклона приемника относительно направления луча, следя за тем, чтобы луч входил в отверстие приемника не задевая его кромок).
5. Остановите измерения и зарегистрируйте полученное значение в качестве мощности падающего излучения (регистрация ведется в относительных единицах). Внесите его (с клавиатуры) в таблицу исходных данных, которая открывается на экране одновременно с началом измерений.
6. Направьте луч на грань призмы.
7. Поверните лимб с призмой таким образом, чтобы угол падения был близок к максимально возможному (80° – 85°). Поворот призмы осуществляется вращением всего лимба за насечку, сделанную на его боковой поверхности. Запрещается прикладывать усилие к самой призме и рамке, удерживающей ее на поверхности лимба.
8. Поворачивая узел крепления лазера в плоскости рабочей поверхности, получите симметричное относительно ребер призмы расположение пятна лазерного излучения на поверхности грани.
9. Поверните лимб на угол, обеспечивающий нормальное падение луча на поверхность грани. Для этого установите на пути луча диафрагму диаметром 2-3 мм и следите, когда отраженный от поверхности луч (он будет перемещаться при вращении лимба) пойдет вдоль падающего луча (т.е. когда его след на бумажной диафрагме совпадет с отверстием, сквозь которое идет падающий луч).
10. Включите регистрацию данных, выберите данное положение лимба в качестве нулевого значения для датчика угла поворота и внесите его в таблицу «Исходные данные».

11. Поверните лимб на угол 5–10 градусов по часовой стрелке и измерьте мощность отраженного излучения. Закройте таблицу «Исходные данные» и откройте закладку с надписью «Таблица». Текущие измеряемые значения угла поворота лимба (он совпадает с углом падения луча) и мощности излучения будут отражаться на графиках и в соответствующих клетках таблицы. Проведите подстройку положения датчика по максимуму регистрируемого им сигнала и запишите полученные данные в таблицу. Для этого нужно нажать экранную кнопку «Запись» в окне таблицы.
12. После этого продолжите измерения и запись данных, каждый раз поворачивая лимб на угол 5–10 градусов. При записи данных в таблице возникает новая строка, а строка с текущими значениями параметров сдвигается вниз.
13. Дойдя до значений угла в 80–85 градусов, остановите измерения и выведите на график полученные данные (закладка «График»). Сравните характер полученной зависимости с литературными данными.
14. Повторите измерения для другой поляризации лазерного излучения. Поверните лазер на 90 градусов вокруг продольной оси и повторите процесс юстировки луча на середину призмы (в положении скользящего падения) и выбор начального значения для отсчета угла. Повторно измерять мощность падающего излучения не нужно.
15. Найдите на графике значение угла Брюстера, при котором отражение р-поляризованной волны отсутствует.
16. Подсчитайте по формуле $\operatorname{tg} \theta_{\text{бр}} = n_2 / n_1$ коэффициент преломления оптического стекла n_2 , полагая, что у воздуха n_1 практически равен единице

Указания по технике безопасности

- Перед выполнением работы получите инструктаж у лаборанта.
- Запрещается трогать руками оптические поверхности линзы, источника и экран. Все перемещения вдоль оптической скамьи следует производить, двигая приборы за металлические рейтеры.

7. Контрольные вопросы:

1. Охарактеризуйте области применения лазеров в качестве прибора технической разведки.
2. Расскажите об оптико-электронном канале утечки информации и его составных частях.
3. Назовите физические принципы, лежащие в основе образования оптоакустического канала утечки информации.
4. Какие формулы лежат в основе физического механизма образования канала утечки?
5. Нарисуйте схему организации съёма акустической информации с помощью лазерного облучения
6. Что такое угол Брюстера?
7. Что такое р-поляризация луча?
8. Что такое s-поляризация луча?
9. Существует ли угол Брюстера у металлов?

Время на выполнение лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: Ростовский государственный экономический университет (РИНХ), К.ф.-м.н., доцент Шейдаков Николай Евгеньевич, sheidakov@mail.ru

Образовательная программа: 10.03.01 Информационная безопасность, Организация и технология защиты информации.

Дисциплина: Физические основы защиты информации.

Лабораторная работа.

Измерение рассеянных низкочастотных магнитных полей

1. Учебные цели:

Изучить устройство и функционирование измерительного преобразователя индукционного типа, предназначенного для измерения слабых низкочастотных магнитных полей; исследовать распределение и измерить магнитное поле вблизи проводников с низкочастотным переменным током.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Выпускник умеет: выполнять анализ физических явлений и процессов с целью расчёта утечек информации в виде магнитных полей. Выпускник владеет: первичными навыками по экранированию защищаемых объектов от утечки информации.

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение: измерительный преобразователь индукционного типа; стенд для изучения переменных магнитных полей.

4. Задание на исследование

С помощью индукционного преобразователя измерить переменное магнитное поле трех объектов:

- А) проводник с током в железной трубе;
- Б) одиночный проводник стоком;
- В) два вплотную расположенные проводника с противоположными направлениями токов.

5. Краткие теоретические сведения

Индукционное измерение полей

В настоящей работе для измерения низкочастотных магнитных полей, существующих всегда в пространстве вблизи проводников с переменным током (например, вблизи сетевой проводки в квартирах), используется индукционный преобразователь. Чувствительной частью индукционного преобразователя является измерительная катушка, содержащая несколько тысяч витков тонкого провода. Под действием измеряемого внешнего переменного магнитного поля в катушке в соответствии с законом Фарадея-Ленца наводится ЭДС; к концам катушки подсоединяется устройство для усиления и индикации этой ЭДС, пропорциональной внешнему электромагнитному полю.

Формула закона Фарадея-Ленца следующая:

$$\varepsilon = -\frac{d\Psi}{dt}, \quad (1)$$

где ε – электродвижущая сила, возникающая в витке из проволоки или катушке, когда в области, охватываемой катушкой, возникнет переменный магнитный поток; Ψ – потокосцепление всех витков катушки с измеряемым магнитным полем.

На рисунке 1 показано расположение катушки в переменном измеряемом магнитном поле с индукцией $B_{\perp} = B_0 \cdot \cos \omega t$, где ω – круговая частота поля. Ось катушки образует с направлением поля угол α , поэтому:

$$\Psi = B_{\perp} S \cdot \cos \alpha = B_0 S \cdot \cos \alpha \cdot \cos \omega t, \quad (2)$$

где S – суммарная площадь, охватываемая всеми витками катушки.

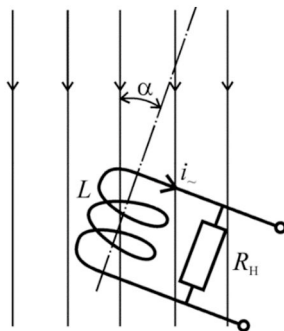


Рис. 1. Измерение индукции переменного магнитного поля индукционным преобразователем

В катушке возникнет ЭДС:

$$\varepsilon = -\frac{d(B_0 \cdot S \cdot \cos \alpha \cdot \cos \omega t)}{dt} = B_0 \cdot S \cdot \omega \cdot \cos \alpha \cdot \sin \omega t, \quad (3)$$

В измерительной цепи катушки проходит переменный ток i_{\sim} :

$$i_{\sim} = \varepsilon / Z, \quad (4)$$

где $Z = R_H + \omega L$ – полное сопротивление измерительной цепи, являющееся суммой омического R_H и индуктивного ωL сопротивлений цепи, L – индуктивность катушки. Подставив все известные величины в (4), получим:

$$i_{\sim} = \frac{\varepsilon}{R_H + \omega L} = \frac{B_0 \cdot S \cdot \cos \alpha}{R_H + \omega L} \cdot \sin \omega t = i_0 \cdot \sin \omega t, \quad (5)$$

Амплитуда i_0 переменного тока в цепи, как видно из (5), равна:

$$i_0 = \frac{B_0 \cdot S \cdot \omega \cdot \cos \alpha}{R_n + \omega L}. \quad (6)$$

Мы видим, что амплитуда тока, являющегося выходным сигналом измерительного преобразователя, зависит от частоты измеряемого магнитного поля. Эту зависимость можно исключить, если для знаменателя принять условие:

$$R_n \ll \omega L. \quad (7)$$

Тогда после сокращений вместо (6) получим:

$$i_0 = \frac{B_0 \cdot S}{L} \cdot \cos \alpha. \quad (8)$$

Из (8) видно, что, если поворачивать измерительную катушку при измерениях, изменяя угол α , то можно найти направление силовых линий магнитного поля в точке расположения катушки – при совпадении направления оси катушки с силовой линией $\alpha = 0$, и амплитуда тока максимальна. При таком положении катушки амплитуда тока является мерой амплитуды индукции измеряемого поля.

Измерительная катушка позволяет, таким образом, как измерять значение, так и определять направление индукции магнитного поля.

Для увеличения чувствительности преобразователя к направлению силовых линий поля часто катушку снабжают сердечником из магнитомягкого материала с большой величиной магнитной проницаемости μ , играющего роль «магнитной антенны». В качестве материала выбирают феррит, который, являясь диэлектриком, лишен потерь на токи Фуко при перемагничиваниях сердечника в быстропеременных магнитных полях.

Характеристика рассеянных магнитных полей

Измерительный индукционный преобразователь может быть применен для измерения магнитных полей, окружающих проводники с переменным током. Такие магнитные поля можно назвать полями рассеяния. Бесконечно длинный прямолинейный проводник с током i создает вблизи себя в немагнитной среде магнитное поле, индукция B которого равна:

$$B = \frac{\mu_0 i}{2\pi r}, \quad (9)$$

где $\mu_0 = 4\pi \cdot 10^{-7}$ А/м – магнитная постоянная; r – расстояние от проводника до точки А измерения поля.

Вектор B направлен по касательной к силовой линии поля, которая, в случае прямолинейности проводника, имеет форму окружности с центром в проводнике (рис. 2). Для измерения индукции в точке А необходимо поместить измерительную катушку так, чтобы ее сердечник своей осью симметрии был направлен по касательной к силовой линии поля. В этом случае ток, индуцированный переменным магнитным полем в катушке, будет наибольшим среди всех возможных положений катушки и покажет значение индукции B в точке А. Если катушку поворачивать в плоскости, перпендикулярной проводнику, то можно найти такое ее положение, что ток в ней будет минимально-возможным, при этом ось катушки укажет на проводник с током.

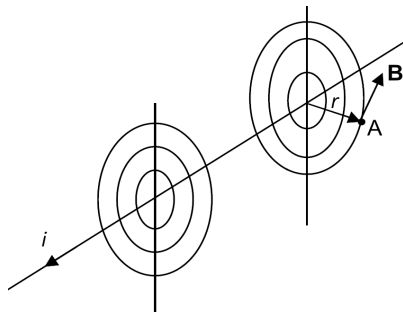


Рис. 2. Магнитное поле проводника с током

Иногда, для уменьшения воздействия магнитных полей проводников с током на другие приборы, прибегают к экранированию приборов. Рассмотрим возможность исключения таких магнитных полей путем размещения самого проводника с током i в ферромагнитном экране-трубе (рис. 3).

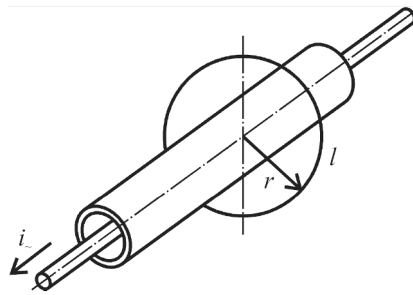


Рис. 3. К выяснению возможности экранирования магнитного поля проводников с током

Проведем в пространстве снаружи трубы воображаемый кольцевой контур по форме магнитной силовой линии, т. е. окружности с центром на оси провода. Циркуляция вектора магнитной индукции по этому контуру равна полному току, охватываемому этим контуром, умноженному на магнитную постоянную:

$$\oint B_{\ell} d\ell = 2\pi r B, \quad (10)$$

где $B_{\ell} = B$ – проекция вектора B на линию контура.

По теореме о циркуляции вектора магнитной индукции, известной из курса физики, циркуляция по контуру, окружающему ток, равна:

$$\oint B_{\ell} d\ell = \mu_0 i. \quad (11)$$

Сравнивая (10) и (11), получим:

$$B_{\ell} = B = \frac{\mu_0 i}{2\pi r} \text{ – обычную формулу для индукции магнитного поля тока.}$$

Это значит, что наличие железной трубы, надетой на проводник с током, не изменяет магнитного поля тока в окружающем трубу пространстве, не экранирует внешнее пространство от магнитного поля тока.

Стенд для измерения рассеянных полей

В настоящей лабораторной работе измеряется переменное магнитное поле трех объектов (рис. 4): А – проводник с током в железной трубе (переключатель Пр в положении 1); Б – одиночный проводник с током (переключатель Пр в положении 1); В – два параллельных проводника с противоположными направлениями токов, размещенные без зазора (переключатель Пр в положении 2).

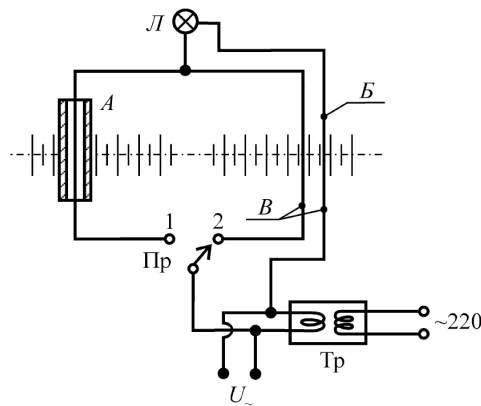


Рис. 4. К выяснению возможности экранирования магнитного поля проводников с током

Источником токов является понижающий трансформатор Tr , потребитель электрической энергии – лампа накаливания L . С помощью переключателя Pr переменный ток поочередно пропускается через исследуемые объекты. Напряжение $\sim U$ со второй обмотки трансформатора Tr используется для калибровки чувствительности измерительного преобразователя.

Измерительный преобразователь

Блок-схема преобразователя показана на рисунке 5. В немагнитном корпусе помещены: измерительная и калибровочная катушки, закрепленные на общем ферритовом стержне, играющем роль магнитной антенны для рассеянных магнитных полей; усилитель; в качестве индикатора применен мультиметр. Измерительная катушка своими выводными концами подсоединена ко входу усилителя. Усиленный сигнал $U_{\text{сигн}}$ из-

меряется мультиметром. Калибровочная катушка присоединена к клеммам $\sim U$, на которые при калибровке подается переменное напряжение от измерительного стенда. Усилитель имеет батарейное питание, включаемое переключателем «Вкл.» и имеет два режима работы. При нажатии кнопки на боковой стороне корпуса преобразователя его коэффициент усиления увеличивается примерно в 10 раз по сравнению с состоянием, когда кнопка не нажата. Для калибровки чувствительности измерительного преобразователя к магнитным полям, в магнитной антенне перед измерениями необходимо создать магнитное переменное поле известной величины $B_{\text{кал}}$ и измерить величину выходного сигнала $U_{\text{кал}}$ преобразователя. Отношение этих величин является чувствительностью S измерительного преобразователя:

$$S = \frac{U_{\text{кал}}}{B_{\text{кал}}} \text{ В/Тл} . \quad (12)$$

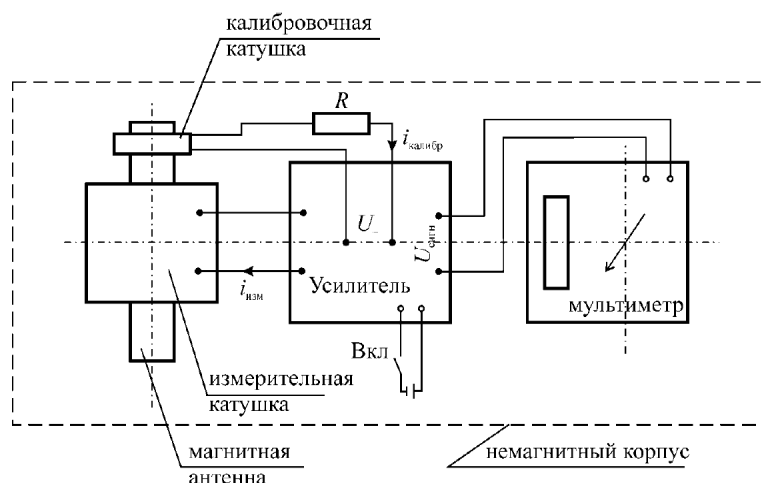


Рис. 5. Блок-схема измерительного преобразователя переменного магнитного поля

Калибровочное магнитное поле в воздухе, создаваемое калибровочной катушкой, намотанной поверх измерительной (рис. 5), с током $i_{\text{калибр}}$ можно рассчитать по формуле индукции в короткой катушке:

$$B_{\text{кал}} = i_{\text{калибр}} \frac{\mu_0 N}{2\pi r_0} , \quad (13)$$

где N – число витков в калибровочной катушке; r_0 – ее радиус.

В формулах (11) и (13) под $B_{\text{кал}}$ понимается индукция магнитного поля в воздушной среде без учета магнитной проницаемости вещества антенны. Напряжение питания U_{\sim} (рис. 5) калибровочной катушки необходимо подать на время калибровки с клемм U_{\sim} стенда измерений (см. рис. 4). При измерениях рассеянного магнитного поля напряжение U_{\sim} калибровки отключить, поместить магнитную антенну измерительного преобразователя в нужную точку пространства и, поворачивая антенну, найти ее положение, при котором напряжение сигнала $U_{\text{сигн}}$ на выходе преобразователя максимально. Индукция B магнитного поля в этой точке пространства вычисляется по формуле:

$$B = \frac{U_{\text{сигн}}}{S} . \quad (14)$$

Помещая измерительный преобразователь на разных удалениях от проводника с током, можно исследовать распределение магнитного поля проводника.

6. Порядок выполнения лабораторной работы (этапы)

I. Калибровка чувствительности измерительного преобразователя

1. Расположить преобразователь вдали от источников переменного поля. Включить преобразователь тумблером Вкл. Тумблер $U-N$ должен быть в положении U . Установить переключатель рода работы мультиметра в положение DCV 2000 m (2000 mV). Убедиться, что показания мультиметра не превышают 0,5–1,0 mV.
2. Соединить клеммы U измерительного преобразователя с такими же клеммами измерительного стенда парой проводов.
3. Включить измерительный стенд в сеть 220 В. Должна загореться лампочка на стенде.
4. Показания $U_{\text{кал}}$ мультиметра записать.
5. Вычислить по формуле (13) калибровочное значение индукции $B_{\text{кал}}$, считая $N = 5$, $r_0 = 2 \cdot 10^{-2}$ м, $I_{\text{калибр}} = 20 \cdot 10^{-3}$ А.
6. Вычислить по формуле (11) чувствительность S преобразователя.

II. Исследование рассеянных магнитных полей

1. Отсоединить используемые при калибровке провода от клемм U.
2. Переключателем стенда включить ток через объект А.
3. Устанавливая датчик преобразователя (катушку с магнитной антенной) на разных расстояниях от объекта А (рис. 4), записывать в таблицу 1 значения расстояния r и соответствующие значения сигнала U_c (показания мультиметра).
4. Добиваясь поворотами датчика, чтобы значения сигнала были наибольшими при данном расстоянии r . В диапазоне расстояний 5–50 см. провести измерения в 5–6 точках.

Таблица 1 – Результаты измерений и расчетов

№	S, В/Тл	r, м	$U_{\text{сигн}}$, В	B, Тл	i, А
1					
2					
3					

5. Рассчитать по формуле (7.14) значения индукции B в каждой точке и также занести в таблицу.
6. Повторить замеры для объектов Б и В на стенде, устанавливая переключатель P_r на стенде в соответствующее положение. Данные занести в аналогичные таблицы.
7. Построить графики зависимостей $B = B(r)$ (зависимости индукции магнитного поля проводников с током от расстояния до проводника)
8. Вычислить для объекта Б величину тока в проводнике по данным для каждого расстояния r , руководствуясь формулой (9).
9. Сделать выводы о влиянии железного экрана и наличия двух противоположно направленных токов в соседних проводниках на величину и распределения рассеянных магнитных полей этих токов.

7. Контрольные вопросы:

1. Каковы особенности магнитного поля, характеризующие его параметры (вектор магнитной индукции в вакууме и в веществе, магнитный поток, напряженность магнитного поля)?
2. Охарактеризуйте магнитные поля, создаваемого проводниками с током простейшей формы.
3. В чем состоит закон полного тока для магнитного поля?
4. В чем суть закона электромагнитной индукции?
5. В чем заключается принцип работы индукционных преобразователей?
6. Как зависит переменный ток в катушке индукционного преобразователя от индукции измеряемого переменного магнитного поля и его частоты?
7. Как распределяется в пространстве индукция магнитного поля проводника током?
8. Как происходит экранирование поля проводника?
9. Какие объекты исследовались на измерительном стенде?
10. Как устроен измерительный преобразователь переменного магнитного поля? Каков принцип его работы?
11. В чем заключаются особенности калибровки чувствительности измерительного преобразователя?

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: Сибирский Государственный Университет Геоистем и Технологий, Кафедра информационной безопасности Карманов Игорь Николаевич, заведующий кафедрой, к.т.н., доцент i.n.karmanov@ssga.ru; Кафедра физики, Чесноков Дмитрий Владимирович, к.т.н., доцент, D.V.Chesnokov@ssga.ru

Образовательная программа: 10.03.01 Информационная безопасность, Организация и технология защиты информации.

Дисциплина: Физические основы защиты информации.

Лабораторная работа. **Пьезоэлектрический эффект**

1. Учебные цели:

- Изучить закономерности пьезоэлектрического эффекта.
- Изучить возможности пьезопреобразования механической энергии в электрическую.
- Экспериментально исследовать пьезопреобразователь и измерить значение пьезоэлектрического модуля.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Выпускник умеет: выполнять анализ физических явлений и процессов преобразования механических колебаний в электрический сигнал с целью анализа возможности утечек информации. Выпускник владеет: первичными навыками по работе с пьезопреобразователями.

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение: механизм, передающий механическую нагрузку к преобразователю; пьезопреобразователь; мультиметр.

4. Задание на исследование

Исследовать зависимость пьезоэлектрического модуля от механической нагрузки на пьезопреобразователь.

5. Краткие теоретические сведения

Прямой пьезоэлектрический эффект заключается в образовании на поверхности некоторых кристаллических материалов, при приложении к ним механических усилий, электрических зарядов. Эффект наблюдается только в ионных кристаллах, молекулы которых, в целом нейтральные, содержат ионы разных знаков и потому обладают дипольным электрическим моментом. При деформации кристалла, вызванной приложенными силами, молекулы кристалла могут смещаться и поворачиваться, что приводит к переориентации их дипольных моментов. Кристалл в целом изменяет свой дипольный момент, который равен векторной сумме дипольных моментов всех его молекул; электрические заряды на поверхности кристалла изменяются. Заряды на поверхности индуцированы зарядами диполей молекул и являются связанными. Внутри кристалла и в окружающей среде имеется множество свободных зарядов (электроны, ионы), которые через короткий промежуток времени концентрируются на заряженных поверхностях и могут нейтрализовать поверхностный индуцированный заряд.

Для подсоединения к измерительным электрическим схемам на пьезокристалл наносят две металлические обкладки, и пьезопреобразователь в электрическом смысле можно считать конденсатором, в котором в качестве диэлектрика выступает сам пьезокристалл, работающий как генератор электрического напряжения на обкладках конденсатора. Пьезопреобразователь преобразует работу механической силы, деформирующей кристалл, в электрическую энергию заряда конденсатора. Величина заряда пропорциональна силе, приложенной к пьезокристаллу:

$$Q_x = d_{11}F_x, \quad (1)$$

где x означает направление приложения силы.

Электрическое напряжение между обкладками конденсатора равно:

$$U = \frac{Q_x}{C_{пр}} = \frac{d_{11}F_x}{C_{пр}}, \quad (2)$$

где $C_{пр}$ – электрическая емкость конденсатора (преобразователя).

Действие внешней силы F_x вызывает в кристалле упругое противодействие, и почти сразу упругая и внешняя сила уравниваются друг друга, перемещения и повороты молекулярных диполей прекратятся, прекратятся и изменения индуцированных зарядов на обкладках; начнется стадия стихийной нейтрализации этих зарядов свободными зарядами. Разность потенциалов между обкладками постепенно упадет до нуля. Если внешнюю силу в этот момент убрать, молекулы упруго вернуться в свое обычное положение, и на обкладках вновь возникнет на некоторое время электрическое напряжение. Это напряжение будет иметь обратный знак в сравнении с состоянием под нагрузкой. Пьезоэффект является обратимым физическим явлением: если к кристаллу приложить внешнее электрическое напряжение, произойдет его деформация под действием возникших внутренних механических напряжений. Явление носит название обратного пьезоэффекта.

В качестве материалов пьезопреобразователей применяют кристаллический кварц, турмалин, пьезоэлектрические керамики, некоторые полимеры. Наибольшим значением пьезомодуля обладают пьезокерамики. Пьезопреобразователи с прямым пьезоэффектом применяют в качестве чувствительных элементов измерителей силы, механических напряжений, вибраций, ускорений.

Метод измерения пьезомодуля

Схема измерений показана на рисунке 1. Керамический пьезопреобразователь 1 с обкладками, показанными толстыми линиями, размещается на основании 2 в отверстии охранного кольца 3. Механическая нагрузка (вес груза M) передается на преобразователь с помощью штока 4. К выводам преобразователя параллельно ему подсоединен конденсатор C ; напряжение U на конденсаторе измеряется мультиметром.

метром. Диод 5 предназначен для предотвращения стока заряда конденсатора С назад к преобразователю при самонейтрализации заряда.

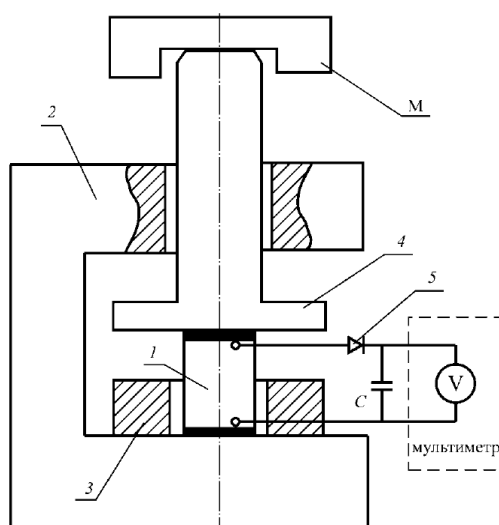


Рис. 1. Схема установки по исследованию пьезоэффекта

При помещении на шток груза М на преобразователь действует сила F:

$$F = Mg,$$

которая вызывает образование на обкладках преобразователя заряда Q:

$$Q = d_{ij} F = d_{ij} Mg, \quad (3)$$

где d_{ij} – пьезоэлектрический модуль преобразователя.

Этот заряд распределяется между емкостью преобразователя $C_{пр}$ и конденсатором С; так как $C_{пр} \ll C$, заряд, в основном, пройдет через диод, сосредоточится в конденсаторе и зарядит его до напряжения U:

$$U = \frac{Q}{C} = \frac{d_{ij} Mg}{C}. \quad (4)$$

Конденсатор необходим для того, чтобы увеличить постоянную времени самопроизвольного изменения напряжения U вследствие протекания токов разряда через входную цепь мультиметра и из-за эффекта самонейтрализации заряда обкладок преобразователя.

Преобразуя (4), находим значение пьезоэлектрического модуля преобразователя:

$$d_{ij} = \frac{UC}{Mg}. \quad (5)$$

Величина емкости С конденсатора подбирается индивидуально, под характеристики преобразователя, и составляет (10^{-7} – 10^{-6}) Ф.

6. Порядок выполнения лабораторной работы (этапы)

1. Подсоединить мультиметр к выходным гнездам устройства.
2. Провести измерение напряжения U при трех различных значениях груза М. Измерения проводить не при установке груза М, а при его снятии со штока. Результаты измерений и расчетов занести в таблице 1.

Таблица 1 – Результаты эксперимента и расчетов

№	М, кг	U, В	d_{ij} , Кл/Н
1			
2			
3			

3. Вычертить график зависимости значения d_{ij} от величины силы $F = Mg$, сделать вывод о степени линейности зависимости $d_{ij} = f(F)$.

7. Контрольные вопросы:

1. Что такое прямой и обратный пьезоэффекты?
2. Какова физическая природа пьезоэффекта?
3. Каковы особенности материалов, обладающих пьезоэффектом?
4. Как происходит вычисление поляризованного заряда в одномерном простом случае?
5. Что такое пьезоэлектрический модуль?
6. Объяснить причину временного характера возникающих под действием внешних сил пьезопотенциалов.
7. Как осуществляется расчет электрического напряжения, возникающего на обкладках.
8. Что является источником электрической энергии, возникающей при пьезоэффекте?

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: Сибирский Государственный Университет Геосистем и Технологий, Кафедра информационной безопасности, Карманов Игорь Николаевич, заведующий кафедрой, к.т.н., доцент, i.n.karmanov@ssga.ru; Кафедра физики, Чесноков Дмитрий Владимирович, к.т.н., доцент, D.V.Chesnokov@ssga.ru

Образовательная программа: 10.03.01 Информационная безопасность, Организация и технология защиты информации.

Дисциплина: Физические основы защиты информации.

Лабораторная работа. **Звуковая эхолокация**

1. Учебные цели:

- Изучить основы метода измерения положения тел по времени запаздывания отраженной от объекта звуковой волны;
- Изучить лабораторный прибор для звуковой эхолокации объектов.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Выпускник умеет: выполнять анализ физических явлений и процессов при излучении, распространении и отражении акустических волн. Выпускник владеет: первичными навыками по работе с устройствами, позволяющими получать информацию об объектах по акустическому каналу.

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение: лабораторный звуковой эхолот; экран; осциллограф.

4. Задание на исследование

Определить расстояния до отражающих объектов методом эхолокации. Оценить точность данного метода измерений.

5. Краткие теоретические сведения

Распространение звуковых волн в атмосфере. Отражение волн от препятствий

Распространение колебательного движения в жидкости или газе называется звуковыми волнами.

Жидкости и газы обладают только объемной упругостью, но не упругостью формы. Поэтому в них могут распространяться только продольные возмущения; поперечные не распространяются. В каждой точке жидкости или газа, участвующей в распространении звуковой волны, происходят попеременные сжатия и разрежения. Звуковые колебания в газе происходят настолько быстро, что тепло, выделившееся при сжатии локальной области газа, не успевает «рассасываться» за счет теплопроводности газа в окружающее пространство, разности температур между сгущениями и разрежениями газа в звуковой волне не успевают выровняться, так что распространение звука можно считать адиабатическим процессом. Для скорости звуковых волн в газе справедливы равноценные формулы:

$$c_{\text{эв}} = \sqrt{\gamma \frac{P}{\rho}}, \quad (1)$$

$$c_{\text{эв}} = \sqrt{\gamma \frac{RT}{\mu}}, \quad (2)$$

где $\gamma = \frac{c_p}{c_v}$ – отношение теплоемкостей газа при постоянном давлении и постоянном объеме: для двухатомного газа $\gamma = 1,4$; P и ρ – давление и плотность газа; $R = 8,31$ Дж/(моль · К) – универсальная газовая постоянная; T – термодинамическая температура газа, К; M – молярная масса газа (для воздуха $M = 0,0288$ кг/моль).

При попадании волны на границу двух сред, часть волны отражается, часть проходит во вторую среду и преломляется. Если волна падает на границу не под прямым углом, то направление преломленной волны не совпадает с направлением падающей.

Проникновение звуковой волны во вторую среду зависит от соотношения волновых сопротивлений $Z_{\text{зв}}$ или удельных акустических импедансов сред:

$$Z_{\text{зв}} = \rho \times c_{\text{зв}}. \quad (3)$$

Долю β прошедшей через границу раздела сред энергии волны можно определить как отношение интенсивности I_2 прошедшей волны к интенсивности I_1 падающей:

$$\beta = \frac{I_2}{I_1}, \quad (4)$$

где β – коэффициент проникновения звуковой волны.

Этот коэффициент можно вычислить по формуле:

$$\beta = 4 \frac{Z_{1\text{эв}}}{Z_{2\text{эв}} \left[\frac{Z_{1\text{эв}}}{Z_{2\text{эв}}} + 1 \right]^2}, \quad (5)$$

где $Z_{1\text{эв}}$ и $Z_{2\text{эв}}$ – волновые сопротивления первой и второй среды.

Если волновые сопротивления сред отличаются многократно, то коэффициент проникновения очень мал, и практически вся волна отражается от границы раздела. Поэтому отражение звуковых волн в атмосфере от твердых тел или поверхности воды – почти полное.

Определение положения тел методом звуковой эхо-локации

Звуковая локация – определение положения объекта по отражению от него звука, создаваемого специальными излучателями. При импульсной локации расстояние l до объекта определяют по времени запаздывания Δt отраженного эхо-сигнала:

$$l = \frac{1}{2} c_{\text{эв}} \Delta t. \quad (6)$$

При измерении расстояния по эхо-сигналу используется схема, изображенная на рисунке 1.

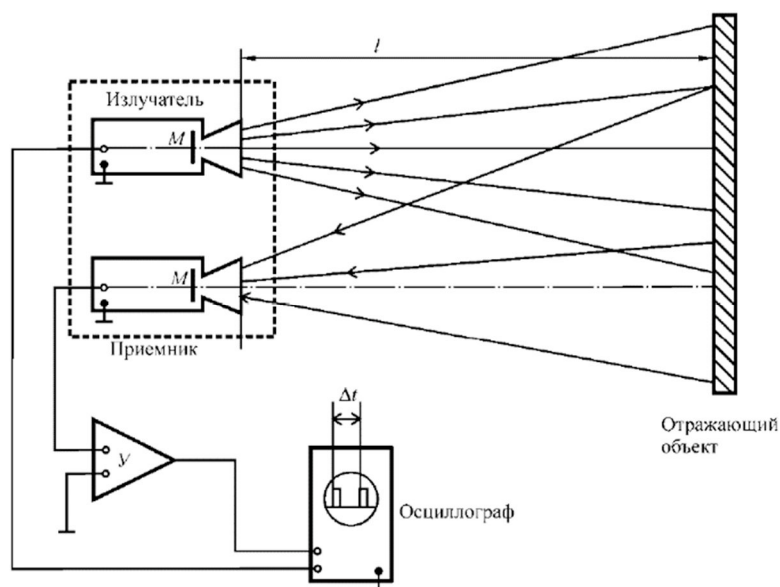


Рис. 1. Определение расстояний по времени прохождения волны до объекта и обратно

В лабораторной установке излучатель и приемник размещены в общем корпусе (пунктир). Каждый из них снабжен рупором, повышающим избирательность излучения и приема звуковых волн. Поэтому звуковые волны, достигшие поверхности объекта, отразившись, попадают только в рупор приемника. В излучателе источником звуковой волны является мембрана М микрофона, которая колеблется под действием электромагнитного поля катушки с током и создает короткий пакет звуковых волн – звуковой импульс. Одновременно со звуковым импульсом излучатель посылает электрический импульс на осциллограф, где сразу же запускается «развертка» электронного пучка по экрану – начинается движение светящегося пятна по экрану и формируется изображение пришедшего от излучателя импульса. Отраженный звуковой импульс в форме пакета волн, попав в рупор приемника, возбуждает колебания мембраны М микрофона, являющегося в приемнике преобразователем звуковых колебаний в колебания электрического напряжения. Эти колебания поступают на вход усилителя У, усиливаются и поступают в осциллограф, возбуждая на его экране импульс эхо-сигнала, сдвинутый относительно первого запускающего развертку импульса на временной промежуток Δt .

6. Порядок выполнения лабораторной работы (этапы)

1. Собрать схему опыта согласно рисунка 1.
2. Включить лабораторную установку (переключателем на ее корпусе), расположить экран-отражатель на расстоянии 3–5 м.
3. Настроить осциллограф (установить чувствительность в диапазоне 0,1–1 В/дел, длительность развертки в диапазоне 1–5 мс/дел). Убедиться в наличии на экране осциллографа картины импульсов, смещающихся при перемещении отражателя.
4. Измерить по экрану осциллографа время Δt запаздывания эхо-сигнала для пяти удаленностей экрана, измерить соответствующие расстояния l до отражателя, внести данные в таблицу 1.

Таблица 1 – Экспериментальные и расчетные результаты

№	l , м	Δt , с	l_p , м	$c_{зв}$, м/с	β	$L_{мин}$, м
1						
2						
3						

5. Рассчитать скорость звука в воздухе при комнатной температуре по формуле (2), занести результат в таблицу.
6. Рассчитать, используя формулы (3) и (5), коэффициент проникновения звуковой волны из воздуха в деревянный экран (плотность воздуха $\rho = 1,2 \text{ кг/м}^3$, плотность дерева $\rho = 0,8 \cdot 10^3 \text{ кг/м}^3$, скорость звука в дереве $c_{зв} \approx 10^3 \text{ м/с}$), результат занести в таблицу.
7. Рассчитать расстояние l_p до отражателя, используя (6) и результаты измерения времени запаздывания, занести полученные данные в таблицу.
8. Определить расстояние $L_{мин}$ обнаружения отражателя малых размеров (площадью 10 см^2), результат занести в таблицу.
9. Сделать вывод о точности измерения положения объекта с помощью лабораторного эхолокатора.

7. Контрольные вопросы:

1. Каковы особенности физической природы звуковых волн в атмосфере?
2. Как зависит скорость звука в воздухе от высоты подъема в горах?
3. Меняется ли скорость звука в воздухе при смене времени года? Обосновать ответ, привести количественные оценки.
4. Объяснить особенности прохождения звука через границу раздела разных сред, дать количественные оценки.
5. В чем заключается принцип определения положения объекта при эхо-локации?
6. Объяснить устройство и работу макета звукового эхолокатора.
7. Какую роль играют мембраны микрофонов в излучателе и приемнике звуковых волн?

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: Сибирский Государственный Университет Геосистем и Технологий, Кафедра информационной безопасности, Карманов Игорь Николаевич, заведующий кафедрой, к.т.н., доцент, i.n.karmanov@ssga.ru; Кафедра физики, Чесноков Дмитрий Владимирович, к.т.н., доцент, D.V.Chesnokov@ssga.ru

СПЕЦИАЛИТЕТ 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Дисциплина: Анализ программных реализаций

Образовательная программа: 10.05.01 Компьютерная безопасность, Разработка защищенного программного обеспечения.

Дисциплина: Анализ программных реализаций.

Лабораторная работа.

Профилирование приложений с использованием dotTrace Performance

1. Учебные цели дисциплины:

Изучение теоретических основ и технологий анализа программ и реализованных алгоритмических решений.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь:

- оценивать эффективность реализации систем защиты информации и политик безопасности в компьютерных системах;
- настраивать приложения и инструменты для использования статических и динамических анализаторов.

Владеть:

- базовыми навыками использования средств антивирусной и криптографической защиты;
- навыками использования инструментов для статического и динамического анализа разрабатываемых приложений.

3. Перечень материально-технического обеспечения

1. Операционная система Microsoft Windows текущей версии. Доступна в рамках подписки Microsoft DreamSpark Premium. Разработчик: компания Microsoft. Режим доступа: https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?cmi_mnuMain=bdba23cf-e05e-e011-971f-0030487d8897&ws=58727022-4bac-e211-88b7-f04da23e67f4&vsro=8
2. Офисный пакет Microsoft Office (Word, Excel, Power Point) текущей версии. Доступен в рамках лицензионного соглашения OVS-ES. Разработчик: компания Microsoft. Режим доступа: <https://products.office.com/en/home>
3. Среда разработки Microsoft VisualStudio текущей версии. Доступна в рамках подписки Microsoft DreamSpark Premium. Разработчик: компания Microsoft. Режим доступа: https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?cmi_mnuMain=bdba23cfe05e-e011-971f-0030487d8897&ws=58727022-4bac-e211-88b7-f04da23e67f4&vsro=8
4. Декомпилятор JetBrainsdotPeek текущей версии. Доступен бесплатно после принятия лицензионного соглашения. Разработчик: компания JetBrains. Режим доступа: <https://www.jetbrains.com/decompiler/download/>
5. Набор утилит администрирования WindowsSysinternalsSuite текущей версии. Доступен бесплатно. Разработчик: компания Microsoft. Режим доступа: <https://docs.microsoft.com/enus/sysinternals/>.
6. Анализатор сетевого трафика WireShark текущей версии. Доступен бесплатно по лицензии GPLv2. Разработчик: The Wireshark team. Режим доступа: <https://www.wireshark.org/>
7. Анализатор HTTP-трафика Fiddler текущей версии. Доступен бесплатно после принятия лицензионного соглашения. Разработчик: компания Progress Software Corporation. Режим доступа: [ps://www.telerik.com/download/fiddler-wizard](https://www.telerik.com/download/fiddler-wizard)

Материально-техническое обеспечение дисциплины:

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерным и мультимедийным оборудованием. Рабочие станции студентов и преподавателя объединены в локальную сеть с подключением к Интернет. Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным проектором и экраном. Лабораторные занятия проходят в компьютерных классах, в которых установлено оборудование: – системные блоки с процессором IntelCore 2 Duo; – мониторы модели Samsung 793 DF.

4. Порядок выполнения лабораторной работы (этапы)

1. Для выполнения заданий необходимо установить dotTrace Performance, его можно запускать как из Visual Studio (главное меню DOTTRACE -> Profile startup application... для запуска профилирования

текущего проекта или FOTTRACE -> Profile application... для профилирования другой программы или исполняющегося процесса), так и в качестве отдельного приложения через главное меню.

2. При выполнении заданий руководствоваться видео-файлами, приложенными к данной лабораторной работе.
3. Задания 1–7 выполняются для стандартной демонстрационной программы, которая идет вместе с dotTrace Performance – RayTraceDemo.exe (трассировщик лучей), которая будет располагаться по пути аналогичному «C:\Program Files (x86)\JetBrains\dotTrace\v5.5\Bin\Demo\RayTraceDemo.exe» (в той же папки расположены исходники), оно также доступно через главное окно dotTrace Performance, вкладка Home, область Profile Demo Application.

5. Задания на исследование

Задание 1. Запуск профилирования

Запустите dotTrace Performance через главное меню. В главном окне на вкладке Home нажмите кнопку Profile и выберите пункт Standalone application (отдельное приложение). В появившемся окне с помощью кнопки «...» возле текстового поля Application укажите путь к демонстрационной программе RayTraceDemo.exe. Нажмите кнопку со стрелкой вниз, находящуюся в области Application options и в раскрывшейся области установите флажок Profile child processes. В раскрываемом списке Profiling type укажите тип профилирования “Line-by-line” (построчно), а в списке Measure (мера) укажите Wall time (CPU instruction) (замер времени выполнения с помощью инструкций процессора). Установите флажок Start profiling immediately (немедленно запустить профилирование), затем запустите профилирование, нажав кнопку Run.

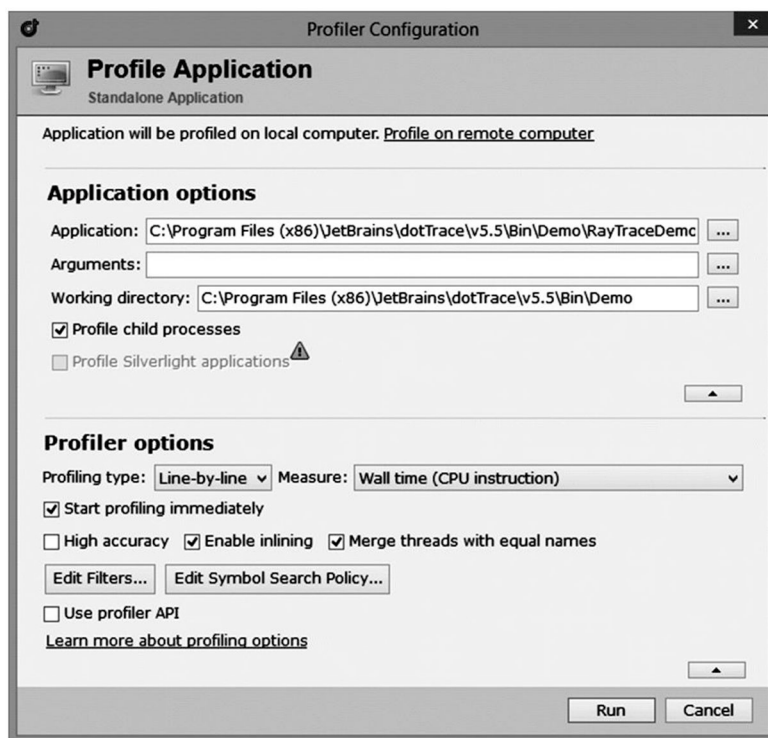


Рис. 1. Окно профилирования

В результате под контролем профилировщика запустится исследуемое приложение RayTraceDemo.exe, в его появившемся главном окне установите флажок Anti alias (сглаживание) и нажмите кнопку “Run”, в результате будет запущен трассировщик лучей, который постепенно отрисует трехмерную сцену.

Можно дождаться завершения работы трассировщика и закрыть программу с помощью кнопки «X», также можно закончить профилирование и создать снимок (набор результатов профилирования), нажав в появившемся окне профилировщика кнопку Get Snapshot. Также можно остановить профилирование, удалив полученные результаты – кнопка Drop Snapshot (потом профилирование можно возобновить) или убить процесс и закончить профилирование – кнопка Kill Process.

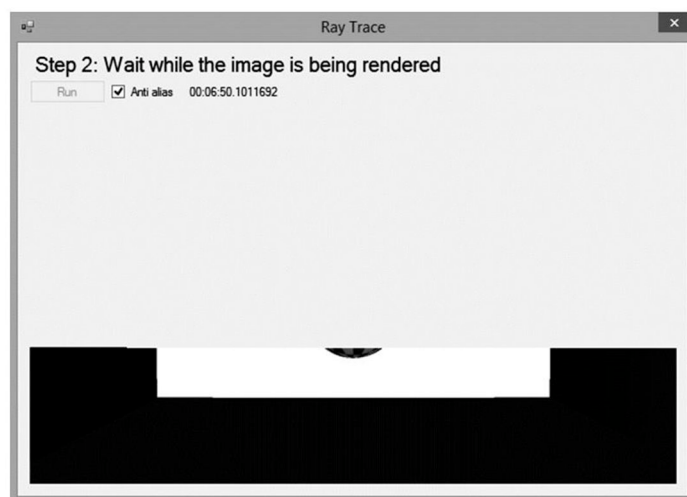


Рис. 2. Трассировщик лучей

Нажмите кнопку Get Snapshot, подождяв, когда исследуемая программа проработает минут пять.



Рис. 3. Окно управления трассировщика лучей

Задание 2. Обзор результатов профилирования (Overview)

Данная вкладка отображает результаты профилирования, в частности содержит сведения о:

- горячих точках (функциях, инструкции которых исполняются большую часть времени, с учетом возможного многократного вызова функций) – User code hotspots;
- распределение времени работы программы внутри главного потока (потока, выполняющего главную функцию приложения) по подсистемам – Main thread, а также внутри других потоков – Other threads, aggregated;
- параметрах снимка – Snapshot;
- приложении – Application;
- среде исполнения – Environment.

Задание 3. Изучение дерева потоков (Threads Tree)

Перейдите на вкладку Thread Tree и изучите деревья вызова функций внутри каждого исполняющегося потока. Для удобства потяните вправо экспендер, расположенный возле вкладок, чтобы появилась слева легенда, изображенная на рисунке 4.

Здесь в правой верхней части, раскрыв функцию можно узнать какие функции она вызывала в процессе исполнения программы. Для каждой функции указывается время ее исполнения в миллисекундах (включая время выполнения вызываемых из нее функций), процент времени ее выполнения, количество вызовов.

В нижней части окна отображается исходный код выбранной в дереве функции, также, например, при его отсутствии, можно посмотреть декомпилированный код или код в виде MSIL (для этого можно установить флажок Show IL code).

Руководствуясь легендой определите:

- Главный поток.
- Финализирующий поток.
- Функции с высоким собственным временем выполнения (собственное время выполнения функции – время ее операторов без учета времени выполнения вызываемых из нее функций).
- Критический путь – путь по дереву до функций, представляющих собой горячие точки.
- Концы критического пути – собственно горячие точки.

Обратите внимание, что функции библиотеки .NET отображаются приглушенным цветом.

Дисциплина: Аппаратная реализация криптоалгоритмов

Образовательная программа: 10.05.01 Компьютерная безопасность.

Дисциплина: Аппаратная реализация криптоалгоритмов.

Лабораторная работа. **Реализация на ПЛИС автоматного шифратора**

1. Учебные цели:

Изучить основные понятия теории автоматных шифров, элементы структурного синтеза конечных автоматов, в том числе способы кодирования состояний, а также возможности языка VHDL для описания цифровых автоматов; получить навыки проектирования цифровых автоматов и отработать навыки описания и моделирования проектов в САПР WebPack ISE.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь:

- корректно применять при решении профессиональных задач аппарат дискретной математики;
- учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности;

Владеть навыками:

- использования языков и систем программирования, инструментальных средств для решения различных профессиональных,
- исследовательских и прикладных задач;
- самостоятельного построения алгоритма, проведению его анализа и реализации в современных программных комплексах.

3. Перечень материально-технического обеспечения:

САПР Xilinx ISE WebPACK, отладочная плата Nexys 2

4. Задание на исследование:

Используя САПР Xilinx ISE WebPACK, провести синтез автоматного шифратора при различных способах кодирования состояний (One-Hot, Gray, Johnson, Sequential) и сравнить по быстродействию, ресурсоемкости, выделяемой мощности результаты синтеза с целью выявления оптимального способа кодирования.

5. Краткие теоретические сведения

Определение 1. Конечным автоматом A называется пятерка (S, X, Y, Ψ, φ) , где S – конечное непустое множество состояний, X и Y – конечные входной и выходной алфавиты соответственно (далее $X=Y$), а $\Psi: S \times X \rightarrow S$ и $\varphi: S \times X \rightarrow Y$ – функции переходов и выходов соответственно.

Определение 2. Автомат называется сильносвязным, если любое состояние автомата достижимо из любого другого состояния. Состояние s' достижимо из состояния s , если существует входное слово (последовательность букв входного алфавита), которое переводит автомат из состояния s в состояние s' .

Определение 3. Автомат называется приведенным, если автомат не имеет пар эквивалентных состояний. Состояния $s \in S$ и $s' \in S$ автомата A называются эквивалентными, если при любом входном слове реакции (последовательности букв выходного алфавита) автомата A на это слово в состояниях s и s' совпадают.

Определение 4. Автомат называется обратным к автомату A , если его диаграмма переходов получается из диаграммы переходов автомата A заменой дуг, помеченных парой x/y на дуги, помеченные парой y/x .

Определение 5. Приведенный сильносвязный автомат A называется шифрующим, если функция выходов автомата A при фиксированном любом состоянии определяет взаимно однозначное отображение X на Y .

Определение 6. Автоматная шифрсистема есть последовательная сеть из автоматов E и D , где E есть шифрующий автомат (автомат-шифратор), а D – автомат обратный к E (автомат-расшифратор). Перед началом работы автоматы E и D должны быть установлены в одинаковое начальное состояние, которое является секретом (ключом). Автоматная шифрсистема обладает следующим свойством.

Утверждение. Пусть при некотором заданом ключе β есть выходная реакция автомата E на произвольное входное слово α . Тогда автомат D дает выходную реакцию α при подаче входного слова β .

Для представления синхронного цифрового автомата следует использовать нижеприведенный шаблон VHDL-кода, предложенный в САПР WebPack ISE, на базе трех процессов SYNC_PROC, OUT-

PUT_DECODE, NEXT_STATE_DECODE, которые реализуют память для хранения текущего состояния автомата, функции выходов и переходов автомата соответственно. Данный шаблон представляет мульти-сегментный стиль программирования цифрового автомата, когда в коде имеется несколько процессов. Для обозначений состояний автомата используется перечисляемый тип данных (enumerated type). САПР WebPack ISE автоматически кодирует перечисляемые значения в битовые векторы, причем возможно выбрать способ кодировки (One-Hot, Gray, Johnson, Sequential).

```
-- This is a sample state-machine using enumerated types.
-- This will allow the synthesis tool to select the appropriate
-- encoding style and will make the code more readable.
-- Insert the following in the architecture before the begin
-- keyword. Use descriptive names for the states, like st1_reset, st2_search
type state_type is (st1_<name_state>, st2_<name_state>, ...);
signal state, next_state : state_type;
-- Declare internal signals for all outputs of the state-machine
signal <output>_i : std_logic; -- example output signal
--other outputs
-- Insert the following in the architecture after the begin keyword
SYNC_PROC: process (<clock>)
begin
if (<clock>'event and <clock> = '1') then
if (<reset> = '1') then
state <= st1_<name_state>;
<output> <= '0';
else
state <= next_state;
<output> <= <output>_i;
-- assign other outputs to internal signals
end if;
end if;
end process;
-- MEALY State-Machine – Outputs based on state and inputs
OUTPUT_DECODE: process (state, <input1>, <input2>, ...)
begin
--insert statements to decode internal output signals
--below is simple example
if (state = st3_<name> and <input1> = '1') then
<output>_i <= '1';
else
<output>_i <= '0';
end if;
end process;
NEXT_STATE_DECODE: process (state, <input1>, <input2>, ...)
begin
--declare default state for next_state to avoid latches
next_state <= state;
--default is to stay in current state
--insert statements to decode next_state
--below is a simple example
case (state) is
when st1_<name> =>
if <input_1> = '1' then
next_state <= st2_<name>;
end if;
when st2_<name> =>
if <input_2> = '1' then
next_state <= st3_<name>;
end if;
when st3_<name> =>
next_state <= st1_<name>;
when others =>
next_state <= st1_<name>;
end case;
end process;
```


6. Порядок выполнения лабораторной работы (этапы)

1. Спроектировать автоматную шифрсистему, задав диаграмму переходов автомата-шифратора E и автомата-расшифратора D.
2. Описать поведение автоматной шифрсистемы на языке VHDL, используя предложенный шаблон VHDL-кода.
3. Провести моделирование и синтез автоматной шифрсистемы, используя САПР WebPack ISE.
4. Изучить способы кодировки, представленные в САПР WebPack ISE.
5. Выполнить задание на исследование.
6. Подготовить и загрузить проект на ПЛИС, используя отладочную плату.
7. Составить отчет о выполнении лабораторной работы.

7. Контрольные вопросы:

1. Шифрующий автомат.
2. Обратный автомат.
3. Автоматная шифрсистема.
4. Перечисляемый тип данных.
5. Мульти-сегментный стиль программирования цифрового автомата.
6. Код Грея.
7. Код Джонсона.
8. Прямое кодирование.

Время на выполнение лабораторной работы – 3 часа.

Образовательная организация, авторы, эл. почта: Национальный исследовательский Томский государственный университет, Тренькаев В.Н., tvnik@sibmail.com

Дисциплина: Защита компьютерных систем

Образовательная программа: 10.05.01 Компьютерная безопасность.

Дисциплина: Защита компьютерных сетей.

Лабораторная работа.

Криптографическая защита каналов передачи данных

1. Учебные цели:

Изучение методов и средств защиты каналов передачи данных ГВС на основе технологии виртуальных частных сетей.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

- Знать возможные подходы к организации системы защиты ГВС.
- Уметь строить ГВС на основе технологии виртуальных частных сетей.
- Владеть навыками работы с сетевым оборудованием.

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение:

ПО Cisco Packet Tracer v7.0.

4. Задание на исследование:

Обеспечить криптографическую защиту подключения сетей филиалов компании к центральному офису по арендуемым каналам передачи данных, а также криптографическую защиту удаленного доступа клиентов через ГВС Интернет к АС компании. Для обеспечения гарантий защиты каналов связи при подключении клиентов через ГВС Интернет использовать немаршрутизируемые IP-адреса инфраструктуры АС компании. Централизованное управление доступом обеспечить путем использования протокола Radius и инфраструктуры службы AAA.

5. Краткие теоретические сведения

При организации обмена и передачи информации в ГВС, как правило, исходят из модели нарушителя, который контролирует каналы передачи данных, а также имеет возможность искажать информацию, передаваемую между абонентами (модель активного нарушителя). Для защиты информации применяют различные специализированные протоколы безопасности, работающие на одном (или нескольких) уровнях модели ISO/OSI. Ниже представлен краткий перечень наиболее распространенных протоколов безопасности. Так, на канальном уровне работают протоколы PPTP, L2TP, L2F, на сетевом уровне работают протоколы IPv6 и IPSec, на транспортном уровне – протокол SSL/TLS и на прикладном – SSH, PGP, S/MIME. Для обмена ключевой информацией в рамках одного или нескольких доменов применяют протокол Kerberos, в масштабах ГВС используют инфраструктуры обмена открытыми ключами PKI. Помимо этого, большинство протоколов передачи данных включают в себя возможность проведения аутентификации сторон прежде, чем будет установлен информационный канал связи.

Выбор протокола для защиты передаваемых данных диктуется необходимыми сервисами и возможностями предполагаемого нарушителя. Для защищенного обмена данными между сетями, расположенными удаленно друг от друга, или между абонентами и сетью, как правило, применяется семейство протоколов сетевого уровня IPSec. Защита данных на сетевом уровне обладает тем достоинством, что для транспортных и сеансовых протоколов работа по защите данных становится прозрачной. В этом случае нет необходимости создавать специальное ПО для защиты передаваемых данных протоколами верхних уровней.

Защищенная передача данных, реализуемая на транспортном уровне, используется преимущественно в модели клиент – сервер. Соответственно клиент и сервер должны поддерживать специальный протокол. Примером может служить протокол SSL и его модификация – TLS.

Выбор схемы для распределения ключевой информации зависит от модели нарушителя. Для модели с активным нарушителем подходят только те схемы, в которых участники информационного обмена заранее знают известный только им секрет, или у них есть общий доверенный посредник.

Большое распространение получили способы распределения ключей на основе протокола Kerberos и на основе инфраструктуры открытых ключей. Оба способа предполагают общего доверенного посредника, в роли которого выступает либо контроллер домена, либо удостоверяющий центр. Схема, основанная на предварительном знании общего секрета, предполагает административно-организационное решение, когда, например, администраторы сети договариваются об используемом пароле или ключе.

Виртуальная частная сеть (VPN) – это технология, использующая криптографические механизмы для защищенной передачи данных по общей или выделенной сетевой инфраструктуре.

В общем случае технология VPN решает следующие задачи: организация связи между филиалами, подключение партнеров и клиентов, а также мобильных сотрудников к корпоративной СПД.

Термин «частная сеть» означает принадлежность оборудования сети предприятия и гарантию конфиденциальности информации, передаваемой по этой сети. Такие сети не очень распространены, гораздо чаще предприятие арендует каналы связи для своих филиалов.

При аренде каналов предприятие делит пропускную способность магистральных каналов с другими абонентами провайдера. Полоса пропускания арендованного канала полностью выделяется предприятию и является его собственностью. Корпоративные данные практически не доступны для абонентов, не являющихся пользователями корпоративной СПД или сети провайдера.

Также возможна организация VPN на базе ГВС Интернет, что, с одной стороны, имеет преимущества в простоте и низкой стоимости реализации, но вместе с тем не гарантирует заданной пропускной способности.

Выделяют следующие виды VPN: интраниет (intranet VPN) – для организации связей с филиалами, удаленного доступа (remote access VPN) – для организации доступа к ресурсам компании сотрудников или клиентов, межкорпоративные (extranet VPN) – для организации связей с партнерами и клиентами.

В VPN для криптографической защиты данных на сетевом уровне предназначено семейство протоколов IPSec, обеспечивающее выполнение следующих задач: шифрование передаваемых данных, обеспечение их аутентичности и целостности, а также разграничение доступа (фильтрация IP-потоков) и защита от повторной передачи IP-дейтаграмм.

В состав семейства IPSec входят протокол аутентификации (AH), протокол шифрования (ESP) и протокол обмена ключами (IKE). Протокол IKE разработан на основе протоколов ISAKMP, Oakley и SKEME и предназначен для согласования используемых алгоритмов, ключей, продолжительности их действия и других параметров. Результатом такого согласования является «однонаправленная безопасная ассоциация» (security association – SA). Работа протокола IKE включает два этапа. Первый – идентификация и аутентификация сторон, установление защищенного канала для согласования параметров (результат – создание IKE SA). Второй – установление защищенного канала передачи данных.

Протоколы семейства IPSec могут работать в транспортном и туннельном режимах. В транспортном режиме заголовок исходной дейтаграммы остается неизменным, а в туннельном режиме происходит формирование нового IP-заголовка для AH или ESP-пакета.

Выделяют следующие основные варианты применения протокола IPSec: узел – узел, узел – сеть и сеть – сеть. При этом основными схемами включения VPN-шлюзов в сегменте LVP являются параллельная и последовательная.

6. Порядок выполнения лабораторной работы (этапы)

Этап 1. Создать и настроить политику безопасности протокола ISAKMP со следующими параметрами: метод аутентификации – PSK, алгоритм шифрования – AES, алгоритм хэширования – SHA1, номер группы Диффи-Хеллмана – 5, длина вырабатываемого ключа – 1 536 бит:

- crypto isakm policy 12;
- authentication pre-share encryption aes hash sha group 5;

Задать ключи аутентификации маршрутизаторов по методу PSK:

- crypto isakmp key R6N!Y4hG address Router_IP_addres;

Этап 2. Создать и настроить политику криптографической защиты каналов передачи данных:

- crypto ipsec transform-set WAN esp-aes esp-sha-hmac;

Этап 3. Определить защищаемые информационные потоки через механизм ACL:

- ip access-list extended *cryptoacl-wan*;
- permit ip 10.10.0.0 0.0.255.255 10.10.0.0 0.0.255.255;

Этап 4. Настроить криптографическую карту шифрования информационных потоков на канале передачи данных между маршрутизаторами и инициализировать ее на внешнем интерфейсе:

- crypto map WAN-map 12 ipsec-isakmp;
- set peer Router_IP_address;
- set transform-set WAN;
- match address *cryptoacl-wan* interface se0/0/0;
- crypto map WAN-map;

Этап 5. Выполнить настройки протокола IPSec на всех маршрутизаторах СПД.

Этап 6. Выполнить настройки службы AAA и протокол Radius на VPN-концентраторе:

- aaa new-model;

- aaa authentication login ASB group radius aaa authorization network ASB local radius-server host 192.168.1.100 key Yulewre!;

Этап 7. Создать и настроить политику ISAKMP:

- crypto isakmp policy 12 authentication pre-share encryption aes group 5;

Этап 8. Выделить диапазон выдаваемых IP-адресов для удаленных клиентов АС компании:

- ip local pool ASB 192.168.1.150 192.168.1.250;

Этап 9. Настроить параметры группы удаленного доступа:

- crypto isakmp client configuration group ASB key BankKey pool ASB netmask 255.255.255.0;

Этап 10. Настроить политику криптографической защиты данных:

- crypto ipsec transform-set CB esp-aes esp-sha-hmac;

Настроить криптографическую карту шифрования потоков удаленного доступа:

- crypto dynamic-map d-ASB 12;

- set transform-set CB crypto map s-ASB client authentication list ASB crypto map s-ASB isakmp authorization list ASB crypto map s-ASB client configuration address respond crypto map s-ASB 12 ipsec-isakmp dynamic d-ASB;

Инициализировать криптографическую карту:

- interface fa0/0 crypto map c-ACB;

Этап 11. Проверить корректность функционирования СПД и доступность служб АС компании. Изучить структуру шифрованных сетевых пакетов. Проверить доступность АС центрального офиса от-казе каналов связи или сетевого оборудования.

7. Контрольные вопросы:

1. Протоколы, используемые для защищенной передачи данных в ГВС.
2. Рекомендации к выбору параметров криптографической защиты протоколов.
3. Технология VPN.
4. Протокол IPSec.
5. Метод аутентификации PSK.
6. Алгоритм шифрования AES.
7. Алгоритм хэширования SHA1.
8. Сетевое оборудование, позволяющее реализовать поставленную задачу.
9. Основные аналоги российского производства, позволяющие реализовать поставленную задачу.
10. Альтернативные методы решения поставленной задачи.
11. Область возможных применений подходов в решении поставленной задачи.
12. Комбинированные методы защиты информации в решении поставленной задачи.
13. Надежность применяемого метода защиты информации в ГВС.

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: Пермский государственный национальный исследовательский университет, доцент кафедры Информационной безопасности и систем связи, к.т.н. Черников А.В., arsenyperm@mail.ru

Дисциплина: Защита программ и данных

Образовательная программа: 10.05.01 Компьютерная безопасность, Разработка защищенного программного обеспечения.

Дисциплина: Защита программ и данных.

Лабораторная работа.

Криптография в .NET

1. Учебные цели дисциплины:

Уметь:

- подбирать необходимую научно-техническую информацию, методические материалы по криптографическим алгоритмам, схемам и протоколам.

Владеть:

- навыками классификации и обобщения научно-технической информации по криптографическим методам защиты.

2. Задание на исследование:

Задание 1. Написать программу, осуществляющую шифрование и дешифрование файлов с помощью симметричных алгоритмов. Она должна поддерживать:

1. Генерацию ключа (использовать криптографические классы генераторов .NET).
2. Вычисление ключа по парольной фразе с применением функции хеширования (использовать классы .NET для хеширования).
3. Шифрование/дешифрование с использованием симметричных алгоритмов: AES и 3DES (использовать классы .NET). У пользователя должна быть возможность выбора алгоритма.
4. Не менее трех способов сцепления блоков для симметричных алгоритмов с возможностью выбора пользователем.
5. Выбор произвольных имен файлов для открытого текста и шифртекста.

При выполнении задания Вы должны:

1. Убедиться в правильности реализации криптографической схемы. Также обратите внимание, чтобы важные данные, например, ключи хранились в памяти программы в зашифрованном виде. Чувствительные данные должны открываться в памяти на ограниченное время, после использования они должны зануляться. Закрытые/секретные ключи в файлах должны быть зашифрованы.
2. Знать характеристики используемых алгоритмов хеширования и шифрования, режимы сцепления блоков.

Задание 2. Написать программу, осуществляющую шифрование и дешифрование файлов с помощью алгоритма RSA и любого выбранного симметричного алгоритма. Она должна поддерживать:

1. Генерацию ключей (использовать встроенные возможности классов .NET для RSA).
2. Возможность сохранения и загрузки открытого ключа.
3. Возможность сохранения и загрузки пары открытого и закрытого ключа.
4. Шифрование/дешифрование с использованием алгоритма RSA (использовать классы .NET), скомбинированным с симметричным алгоритмом. При каждом шифровании генерируется случайный ключ для симметричного алгоритма, на этом ключе шифруются данные, затем сам ключ шифруется с помощью RSA и приписывается к данным. При дешифровании, сначала от данных отделяется зашифрованный ключ, который затем дешифровывается с помощью RSA. Затем он используется симметричным алгоритмом для дешифрования данных.
5. Выбор произвольных имен файлов для открытого текста и шифртекста.
6. Безопасное хранение пары открытого и закрытого ключей в зашифрованном виде. Пара должна быть зашифрована симметричным алгоритмом, его ключ должен быть построен на основе хеширования парольной фразы.

Необходимо:

1. Убедиться в правильности реализации криптографической схемы. В защищенном хранении ключей в памяти программы, в очистки памяти (заполнении нулями).
2. Знать характеристики используемых алгоритмов.
3. Продемонстрировать защищенный обмен файлами двумя пользователями программы.

3. Контрольные вопросы:

1. Криптографические средства .NET.
2. Поддерживаемые криптографические примитивы.
3. Симметричные и асимметричные алгоритмы и их использования с помощью соответствующих классов .NET.
4. Генерация псевдослучайных чисел в .NET, классы обычных хеширующих алгоритмов и хеширующих алгоритмов с ключом.
5. Понятие HMAC.

Время на выполнение работы – 4 часа.

Образовательная организация, авторы, эл. почта: ФГБОУ ВО «Оренбургский государственный университет», Влацкая И.В., Полежаев П.Н., irina.vlatskaya@yandex.ru

Дисциплина: Криптографические методы защиты информации

Образовательная программа: 10.05.01. Компьютерная безопасность/ Математические методы защиты информации.

Дисциплина: Криптографические методы защиты информации.

Лабораторная работа. **Криптосистема Эль Гамала**

1. Учебные цели:

Овладение математическим и алгоритмическим аппаратом, используемым при проектировании и реализации криптографических систем

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Знать:

- математические методы криптографии с использованием конечных полей.

Уметь:

- строить криптографические функции для обеспечения конфиденциальности и целостности информации.

Владеть:

- способностью использовать базовые знания естественных наук, математики и информатики при разработке криптографических систем.

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение: персональный или многопользовательский компьютер с операционной системой типа Windows XP или выше, обучающая компьютерная программа El-Gamal_Tutor, пакет прикладных программ Maple.

4. Задание на исследование:

- Ознакомиться с обучающей компьютерной программой El-Gamal_Tutor.
- Изучить и привести описание алгоритма Эль Гамала, с доказательством корректности алгоритма, его достоинствами и недостатками.
- Зафиксировать (для отчета) последовательность этапов обучения в программе El-Gamal_Tutor.
- Провести тестирование программы El-Gamal_Tutor с целью выявления ошибок и недочетов.
- С помощью пакета прикладных программ Maple произвести шифрование и расшифрование сообщения, заданного в виде одного блока открытого текста. При этом длина ключей должна удовлетворять условиям:

$$|p|, |\delta| \geq 80 \text{ цифр}, \quad |\alpha|, |r| \geq 40 \text{ цифр}.$$

Ключи описываются соотношениями:

$$K = \{ (p, \alpha, \beta, \delta) : \alpha^\delta \equiv \beta \pmod{p} \},$$

где $K = (k_o; k_s)$; $k_o = (p, \alpha, \beta)$ – открытый ключ; $k_s = (\delta)$ – закрытый ключ.

- Сформулировать и обосновать принципы работы алгоритма Эль Гамала.
- Одним из методов решения задачи дискретного логарифмирования осуществить криптоанализ заданного шифрованного текста на основе известных составляющих открытого ключа (p, α, β) .
- Ответить на контрольные вопросы.
- Составить и защитить отчет о проделанной работе.

5. Краткие теоретические сведения:

Общие сведения о криптосистеме Эль-Гамала

Криптосистема Эль Гамала была предложена в 1985 году американцем арабского происхождения Тахер Эль Гамалем. Данная система базируется на сложности решения задачи дискретного логарифмирования, то есть определении числа x при известных a , b и n в сравнении $a^x \equiv b \pmod{n}$.

Пусть: X, Y, K – конечные множества возможных открытых текстов, шифрованных текстов и ключей соответственно;

$E_k : X \rightarrow Y$ – правило зашифрования на ключе $k \in K$; множество $\{E_k : k \in K\} = E$, а множество $\{E_k(x) : x \in X\} = E_k(X)$;

$D_k : E_k(X) \rightarrow X$ – правило расшифрования на ключе $k \in K$, и $D = \{D_k : k \in K\}$;

В соответствии с алгебраической моделью шифра

$\Sigma_A = \{X, K, Y, E, D\}$ шифрсистема Эль Гамала определяется следующим образом.

Обозначим: $Z_p = \{0; 1; 2; \dots; (p-1)\}$ – множество чисел, представляющее собой полную систему

вычетов для некоторого простого числа p ; Z_p^* – множество обратимых элементов совокупности Z_p ;

$X = Z_p^*$, $Y = Z_p^* \times Z_p^*$,

Правило зашифрования определяется следующей формулой:

$$E_{k_0}(M) = (C_1; C_2),$$

где M – открытый текст; $(C_1; C_2)$ – шифр.

$C_1 \equiv \alpha^r(\text{моф})$; $C_2 \equiv (M \cdot \beta^r)(\text{моф})$; r – рандомизатор – случайное целое число из интервала $1 \leq r \leq (p-2)$, необходимое для реализации схемы вероятностного шифрования, при которой зашифрование одинаковых блоков открытого текста будет давать различные зашифрованные тексты (открытый текст и ключ не определяют зашифрованный текст однозначно).

Правило расшифрования:

$$D_{k_s}(C_1, C_2) = (C_2 \cdot (C_1^\delta)^{-1}) \bmod p.$$

Замечание. При расшифровании используется секретный ключ δ и не используется рандомизатор r .

Так как криптостойкость системы Эль Гамала определяется сложностью решения задачи дискретного логарифмирования в совокупности Z_p^* , то следует учесть, что в настоящее время эта задача неразрешима при p , содержащем примерно 300 десятичных цифр. Рекомендуется также, чтобы число $(p-1)$ содержало большой простой делитель.

Вероятностный характер шифрования может быть отнесен к достоинствам системы Эль Гамала, такие схемы обладают, как правило, большей криптостойкостью, чем детерминированные алгоритмы.

Недостатками системы являются:

1. Удвоение длины зашифрованного текста по отношению к открытому тексту.
2. Отсутствие семантической стойкости: второй блок зашифрованного текста будет квадратичным вычетом, тогда и только тогда, когда открытый текст будет квадратичным вычетом. Таким образом, если известна пара: зашифрованный текст и открытый ключ, то можно получить некоторую полезную информацию об открытом тексте.
3. Делимость шифра: если даны оба блока зашифрованного текста, то можно получить другой зашифрованный текст, изменив только второй блок зашифрованного текста.
4. Необходимость использования различных значений рандомизатора для различных открытых текстов, так как в противном случае связанными будут соответствующие зашифрованные тексты и один из них может быть найден по известному второму без знания закрытого ключа.

Криптоанализ криптосистемы Эль-Гамала может быть осуществлен с использованием следующих алгоритмов:

1. Решение задачи дискретного логарифмирования методом перебора.
2. Алгоритм Шенкса (алгоритм больших и малых шагов).
3. Алгоритм Полига-Хелмана, работающий, если известно разложение части открытого ключа $(p-1)$ на простые множители.
4. Ро-метод Полларда.
5. Алгоритм Адлемана (1979 г.).
6. Алгоритм COS (Копперсмит, Одлышко, Шреппель, 1986 г.).
7. Решето числового поля (1993 г.).

Алгоритмы (1–4) обладают экспоненциальной сложностью, а – (5–7) – субэкспоненциальной, поэтому для реально используемых ключей, длиной в 300 и более десятичных разрядов, они не позволяют решать задачи криптоанализа схемы Эль-Гамала за приемлемое время.

К сожалению, до сих пор полиномиального алгоритма решения задачи дискретного логарифмирования не найдено, хотя и не доказано, что он не существует.

В предлагаемой обучающей программе рассматриваются перечисленные алгоритмы криптоанализа, студентам предлагается оценить сложность их для конкретных ключей, подробно изучить некоторые из алгоритмов и осуществить сравнительный анализ, подтвердив наличие как достоинств, так и недостатков у данной криптосистемы. Кроме того, в лабораторной работе по данной теме необходимо реализовать алгоритмы 1 и 2 и провести их исследование.

6. Содержание отчета о выполнении лабораторной работы

1. Описание криптосистемы Эль Гамала.
2. Последовательность этапов и результаты обучения с использованием программы El-Gamal_Tutor.
3. Выявление ошибок и недочетов в обучающей программе El-Gamal_Tutor.
4. Результаты шифрования и расшифрования с использованием ППП Maple.
5. Принципы работы алгоритма Эль Гамала.
6. Последовательность этапов и результаты криптоанализа.
7. Ответы на контрольные вопросы.

Выводы

Библиография

Время на выполнение лабораторной работы – 8 часов.

Образовательная организация, авторы, эл. почта: Воронежский государственный университет, факультет прикладной математики, информатики и механики, Абрамов Геннадий Владимирович, Воронков Борис Николаевич, Ковун Владислав Анатольевич, agwl@yandex.ru – Абрамов Г.В., vrnkv@mail.ru – Воронков Б.Н.

Дисциплина: Модели безопасности компьютерных систем

Образовательная программа: 10.05.01 Компьютерная безопасность.

Дисциплина: Модели безопасности компьютерных систем.

Лабораторная работа.

Настройка и конфигурирование локальных политики безопасности операционной системы Windows

1. Учебные цели:

Отработать навыки по настройке и работе с локальными политиками в операционной системы Windows версий 7/8/10 и/или Server 2008/2012 (32-64 bit).

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь работать с локальными политиками в пользовательской среде операционной системы Windows версий 7/8/10 и/или Server 2008/2012 (32-64 bit).

3. Перечень материально-технического обеспечения Лабораторное оборудование и программное обеспечение:

- компьютер с установленным гипервизором второго уровня (например, Oracle VM Virtual Box)
- установочный образ операционной системы Windows версий 7/8/10 и/или Server 2008/2012 (32-64 bit).

4. Задание на исследование

Используя административную учетную запись настроить локальные политики безопасности, выполнив следующий набор действий:

- отключить настройку панелей инструментов браузера;
- отключить вкладку "Дополнительно" в системном браузере;
- отключить вкладку "Подключения" в системном браузере;
- удалить все файлы из папки временных файлов интернета при закрытии браузера;
- запретить запись на *usb* любые накопители;
- запретить запись на компакт-диски и *dvd*-диски;
- отключить автозаполнение для форм;
- отключить изменения параметров домашней страницы;
- отключение изменения параметров прокси.

5. Краткие теоретические сведения

Групповые политики появились в операционной системе Windows 2000 и включали в себя около 900 настроек для пользователей и компьютеров, которые могли в полной мере применяться к клиентским компьютерам. Из утилиты, предназначенной для изменения данных системного реестра, групповые политики операционной системы Windows 2000 превратились в компонент, предназначенный для изменения параметров конфигурации операционной системы. Групповые политики по-прежнему расположены в шаблонах ADM. Система Windows 2000 Server уже позволяет распространять объекты групповых политик для компьютеров, расположенных в домене и подразделениях (OU) в Active Directory.

В операционных системах Windows XP и Windows Server 2003 возможности групповых политик были расширены. С появлением этих систем у администраторов появилась возможность управлять параметрами безопасности и установкой приложений, а количество политик увеличилось до 1400.

Политика – набор параметров конфигурации, которые применяются к одному или нескольким объектам одного класса. Предположим, имеется некий объект, пусть это будет рабочий стол Windows. У него есть свойства: фоновый рисунок, экранная заставка и т.д. Можно изменить любое свойство этого объекта, например, поменять фоновый рисунок.

Политика – это то же свойство объекта, но обладающее более высоким приоритетом и устанавливаемое администратором системы. Если установлена политика, то уже невозможно изменить свойство объекта самостоятельно – будет использовано значение политики. То есть, если администратор создал политику, задающую фон рабочего стола, и активировал (включил) ее, то пользователь уже не сможет изменить соответствующее свойство объекта (в данном случае – фон рабочего стола). Локальные политики можно применять при отсутствии домена, например, для настройки отдельных компьютеров или в небольших одноранговых сетях.

Раньше одним из основных недостатков использования локальных политик являлась невозможность их применения к конкретным пользователям. Так в Windows XP локальные политики применяются

ко всем без исключения пользователям компьютера, в том числе и входящим в группу локальных администраторов. Однако начиная с Vista появился функционал Множественные локальные групповые политики (Multiple Local Group Policy Objects, MLGPO), позволяющий разделять настройки для различных пользователей или групп.

Операционные системы Windows Vista и Windows Server 2008 уже поддерживают около 2500 настроек групповых политик. Новые категории управления политиками теперь уже обеспечивают управление питанием, возможность блокировки установки устройств, улучшенные параметры безопасности, расширение настроек Internet Explorer, а также возможность делегировать пользователям право устанавливать драйверы принтеров.

В операционных системах Windows 7 и Windows Server 2008 R2 уже насчитывается около 3200 настроек групповых политик.

Целью выполнения данной работы является исследование аспектов безопасности в ОС Windows.

6. Порядок выполнения лабораторной работы (этапы)

1. Установить ОС Windows версий 7/8/10 и/или Server 2008/2012 2012 (32-64 bit) на хостовую операционную систему и убедиться в корректности запуска через прохождение процесса аутентификации административной записи.
2. Завести на установленной операционной системе неадминистративную учетную запись с логином соответствующему вашему имени и фамилии. Установить пароль на учетную запись. Для этого надо было зайти в систему от имени администратора в Панель управления\Добавление и удаление учетных записей пользователей\Создание учетной записи.
3. Для работы с локальными политиками требуется запустить консоль управления. Для этого обходимо запустить консоль управления.
 - Нажать Win +R.
 - Ввести mms.
 - Выбрать «да».

В появившейся консоли в левом верхнем углу нажать «Файл» выбрать «Добавить или удалить оснастку» \ «Редактор объектов групповой политики», нажать «Добавить». Далее в мастере групповой политике нажать «обзор», в поиске объектов групповой политике выбрать созданного неадминистративного пользователя. Нажать «Готово» – «ОК». Нажать на «Политика локального компьютера» (рис. 1).

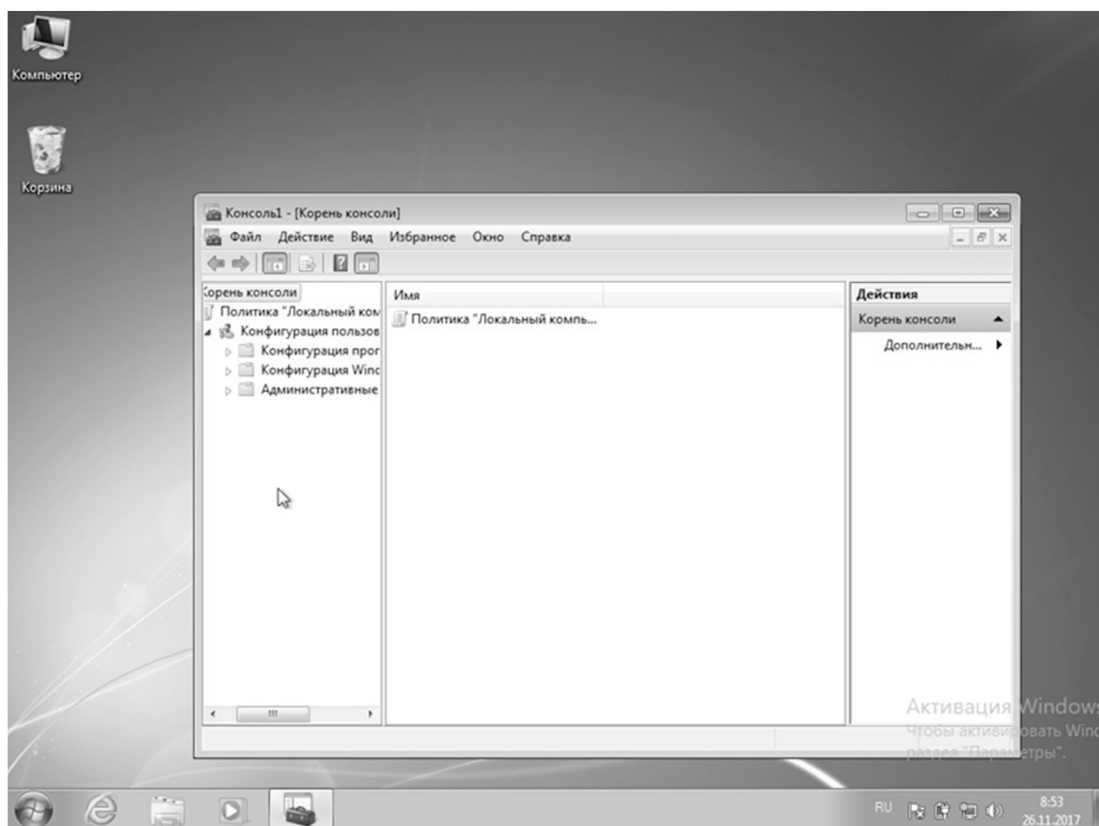


Рис. 1. Консоль управления ОС Windows 7

Используя административную учетную запись настроить локальные политики безопасности. Для примера рассмотрим задачу, связанную с отключением настройки панелей инструментов браузера. Для этого в консоли управления необходимо пройти по дереву настройки (Конфигурации пользователя / Ад-

министративные шаблоны /Компоненты Windows / Internet Explorer /Панели инструментов), где откроется окно редактирования выбранной политики. В нем можно задать следующие команды: «не задано» (по умолчанию), «включить», «отключить». В конкретном случае необходимо выбрать «включить». Аналогичным образом выполняются другие поставленные задачи:

- отключение вкладки "Дополнительно" в системном браузере;
- отключение вкладки "Подключения" в системном браузере;
- удаление всех файлы из папки временных файлов интернета при закрытии браузера;
- запрет записи на usb любые накопители;
- запрет записи на компакт-диски и dvd-диски;
- отключение автозаполнения для форм;
- отключение изменения параметров домашней страницы;
- отключение изменения параметров прокси.

7. Контрольные вопросы:

1. Что такое политики безопасности с точки зрения ОС Windows (основные понятия и определения)?
2. Основные требования к возможности работы с политиками безопасности.
3. Возможно ли ограничение административных записей через политики безопасности?
4. Какова приоритетность между доменными и локальными политиками?
5. Если у двух групп в которые входит конкретный пользователь реализована разная приоритезация на
6. один и тот же объект политики, какой итоговый будет приоритет? Почему?

Время на выполнение лабораторной работы – 3 часа.

Образовательная организация, авторы, эл. почта: Самарский национальный исследовательский университет им. академика С.П. Королева, Михаил Евгеньевич, burlakov@ssau.ru

Образовательная программа: 10.05.01 Компьютерная безопасность.

Дисциплина: Модели безопасности компьютерных систем.

Лабораторная работа. **Настройка и конфигурирование локальных политик безопасности** **операционной системы Linux**

1. Учебные цели:

Отработать навыки по настройке и работе с локальными политиками в операционной системы Linux на примере ОС Ubuntu 18.04 (64 bit).

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь работать с локальными политиками в пользовательской среде операционной системы Linux на примере ОС Ubuntu 18.04 (64 bit).

3. Перечень материально-технического обеспечения Лабораторное оборудование и программное обеспечение:

- компьютер с установленным гипервизором второго уровня (например, Oracle VM Virtual Box);
- установочный образ операционной системы Ubuntu 18.04 (64 bit).

4. Задание на исследование

Используя административную учетную выполнить ряд действий, связанных со служебными командами:

- chmod;
- chown;
- chgrp;
- newgrp;
- groups.

5. Краткие теоретические сведения

Перед началом выполнения лабораторных работ вводятся основные понятия и определения служебных команд Linux.

Команда `chmod` – инструмент для повышения безопасности операционной системы, который позволяет назначать права доступа к файлам или каталогам. Эта команда имеет опции:

- `R` – рекурсивное изменение прав доступа для каталогов и их содержимого
- `f` – не выдавать сообщения об ошибке для файлов, чьи права не могут быть изменены.
- `v` – подробно описывать действие или отсутствие действия для каждого файла.

Назначать права доступа на файлы или каталоги при помощи команды `chmod` можно двумя способами – при помощи символического и абсолютных режимов.

Абсолютный режим – представление прав доступа для конкретного файла из набора трёх восьмеричных чисел. Символьный режим – это представление прав доступа для конкретного файла из набора трёх трёхбуквенных значений вида «`gwx`». Более подробное описание представлено на Рис. 1

Команда `chown` предназначена для изменения владельца файла или каталога. Вызов выглядит следующим образом: `chown "новый владелец" "имя файла"`. Для смены не только владельца, но и группы следует указывать следующую последовательность: `chown "новый владелец":"новая группа" "имя файла"`. Для смены группы следует указывать предыдущего владельца.

Для смены владельца (группы) сразу на нескольких файлах/каталогах, вместо имени файла нужно указывать подходящий "шаблон", например, `"*"` (выполнить операцию для всех файлов в текущей директории).

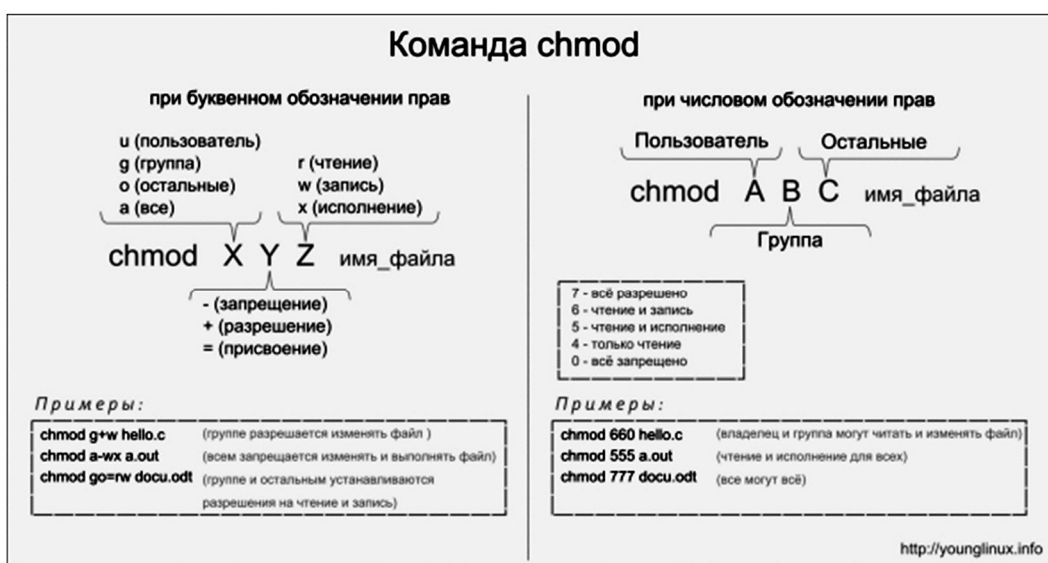


Рисунок 1. Символьный и абсолютный режим

Если необходимо, чтобы аналогичная операция была проделана не только в текущей директории, но и во всех "нижележащих" поддиректориях, следует применять ключ `-R` (recursively).

Например, команда `chown -R vasia:users *` заменит владельца на `vasia`, а группу на `users` для всех файлов и поддиректорий, находящихся в текущей директории и "ниже", то есть в самих поддиректориях.

Команда `chgrp` очень похожа на предыдущую только в качестве первого, аргумента ей нужно указать название новой группы для файла (или файлов). `chgrp "новая группа" "имя файла"`

Дополнительно, все что было сказано о команде `chown` относительно выполнения ее над несколькими файлами, также относится и к команде `chgrp`.

Целью выполнения данной работы является исследование аспектов безопасности в ОС Linux.

6. Порядок выполнения лабораторной работы (этапы)

1. Установить ОС Ubuntu 18.04 (64 bit) на хостовую операционную систему и убедиться в корректности запуска через прохождение процесса аутентификации административной записи.
2. Завести на установленной операционной системе неадминистративную учетную запись с логином соответствующему вашему имени и фамилии. Установить пароль на учетную запись (используя команду `pwd`).
3. Создать в домашнем каталоге файл с произвольным содержимым с идентифицирующими элементами исполнителя (например, ФИО).
4. Отработать навыки управления правами доступа с помощью команды `chmod` используя буквенные ключи, а также абсолютную запись.
5. Убедиться в возможности / невозможности чтения / изменения / исполнения файла при различных значениях атрибутов доступа (с применением команды `chmod` и различных символических ключей доступа, например, `000` или `400`). Также, в символическом режиме провести работу и с группами.

6. Создать подкаталог в домашнем каталоге. Изменяя режим доступа к каталогу, убедиться в возможности (невозможности) просмотра / удаления / добавления / переименования файлов в нём.
7. От имени другого пользователя создать пробные файлы и каталоги. Проверить работоспособность прав доступа для членов группы.

7. Контрольные вопросы:

1. Что такое политики безопасности с точки зрения ОС Linux (основные понятия и определения)?
2. Поясните основные команды по разграничению прав доступа в ОС Linux и их назначение.
3. Возможно ли ограничение административных записей через политики безопасности?
4. Какова приоритетность между доменными и локальными политиками в ОС Linux?

Время на выполнение лабораторной работы – 3 часа.

Образовательная организация, авторы, эл. почта: Самарский национальный исследовательский университет им. академика С.П. Королева, Бурлаков Михаил Евгеньевич, burlakov@ssau.ru

Образовательная программа: 10.05.01 Компьютерная безопасность.

Дисциплина: Модели безопасности компьютерных систем.

Лабораторная работа. **Исследование и ознакомление с функционалом ПО для сканирования портов** **и исследования безопасности локальных и глобальных вычислительных сетей** **на примере NMap**

1. Учебные цели:

Отработать навыки по работе со специализированным программным обеспечением, предназначенным для сканирования портов и исследования безопасности локальных и глобальных вычислительных сетей на примере ПО NMap.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь работать со специализированным программным обеспечением, предназначенным для сканирования портов и исследования безопасности локальных и глобальных вычислительных сетей на примере ПО NMap.

3. Перечень материально-технического обеспечения Лабораторное оборудование и программное обеспечение:

- компьютер с установленным гипервизором второго уровня (например, Oracle VM Virtual Box), с активным сетевым интерфейсом функционирующем на уровне не ниже локальной вычислительной сети без наличия систем обнаружения(предотвращения) вторжений на всех хабах до исследуемых хостов/ либо эмулятор локальной вычислительной сети с аналогичными требованиями.
- установочный образ операционной системы Kali Linux x64.
- установленное ПО NMap.

4. Задание на исследование

Используя поднятое окружение с установленным ПО NMap исследовать следующие аспекты сетевой безопасности локальных/глобальных вычислительных сетей:

- исследовать вопросы связанные с основами сканирования собственных и удаленных портов;
- исследовать механизмы обнаружения удаленных хостов;
- рассмотреть вопросы, связанные с определением портов и порядка их сканирования;
- освоить различные приемы и методики сканирования портов;
- исследовать вопросы управления временем и производительностью сканирования;
- рассмотреть проблематику обхода брандмауэров и систем обнаружения (IDS) и предотвращения (IPS) вторжений;
- рассмотреть возможность определения удаленной ОС;
- рассмотреть возможность обнаружения служб и их версий на удаленном хосте.

5. Краткие теоретические сведения

Перед началом выполнения лабораторных работ вводятся основные понятия и определения для работы со специализированным ПО NMap.

Утилита NMap предназначена для сканирования сетей с любым количеством объектов, определения состояния объектов сканируемой сети, а также портов и соответствующих им служб. Для этого в NMap заложено большое количество различных методов сканирования, среди которых можно выделить:

- UDP connect();
- TCP connect();
- TCP SYN (полуоткрытое);
- FTP proxu (прорыв через ftp);
- Reverse-ident;
- ICMP (ping);
- FIN – сканирование;
- ACK – сканирование;
- Xmas tree – сканирование;
- SYN – сканирование;
- NULL – сканирование.

Утилита NMap также поддерживает большой набор дополнительных возможностей, а именно:

- определение операционной системы удаленного хоста с использованием TCP/IP fingerprint;
- «невидимое» сканирование;
- динамическое вычисление времени задержки и повтор передачи пакетов;
- параллельное сканирование;
- определение неактивных хостов методом параллельного ping – опроса;
- сканирование с использованием ложных хостов;
- определение наличия пакетных фильтров;
- прямое (без использования portmapper) RPC – сканирование;
- сканирование с использованием IP – фрагментации;
- произвольное указание IP – адресов и номеров портов сканируемых сетей.

Результатом работы программы является список отсканированных портов удаленной машины с указанием номера и состояния порта, типа используемого протокола, а также названия службы, закрепленной за этим портом. Порт характеризуется тремя возможными состояниями «открыт», «фильтруемый» и «не фильтруемый»:

- открыт (open) – удаленная машина прослушивает данный порт;
- фильтруемый (filtered) – межсетевой экран, пакетный фильтр или другое устройство блокирует доступ к этому порту и NMap не смог определить его состояние;
- «Не фильтруемый» (closed) – по результатам сканирования NMap воспринял данный порт как закрытый, при этом средства защиты не помешали NMap определить его состояние. Это состояние NMap определяет в любом случае, даже если большинство сканируемых портов хоста фильтруются.

В зависимости от указанных опций, NMap также может определить следующие характеристики сканируемого хоста:

- операционная система хоста;
- метод генерации TCP ISN;
- имя пользователя владельца процесса, зарезервавшего сканируемый порт;
- символьные имена, соответствующие сканируемым IP – адресам и т.д.

В NMap выделяют следующие опции при выборе метода сканирования:

- -sT TCP Connect();
- -sS TCP SYN;
- -sF FIN – сканирование;
- -sX Xmas Tree – сканирование;
- -sN NULL – сканирование;
- -sP Ping – сканирование;
- -sV Определение версий;
- -sU UDP – сканирование;
- -sO Сканирование протоколов IP;
- -sI <zombie_хост [: порт]> – Сканирование «вхолостую»;
- -sA ACK – сканирование;
- -sW TCP Window;
- -sRRPC – сканирование;
- -b <ftp relay host> – «Прорыв через FTP». В качестве аргумента передается URL ftp-сервера, используемого в качестве «доверенного» (имя_пользователя:пароль@сервер:порт).

6. Порядок выполнения лабораторной работы (этапы)

1. Ознакомится со всеми служебными ключами, помогающими реализовать разного рода механизмы сканирования у ПО NMAP.
2. Применяя ACK сканирование определить защищены ли сканируемый хост межсетевым экраном или просто пакетным фильтром, блокирующим входящие SYN – пакеты.

3. Применяя TCP Windows сканирование проверить значение поля Initial Window TCP – пакета и установить возможность фильтрации данных на сканируемом хосте для конкретного порта.
4. Применяя Uriel Maimon сканирование с использованием FIN/ACK запросов получить подтверждение RST – пакет, который согласно спецификации RFC 793 даст точное значение открытости порта.
5. Применяя методику TCP/IP fingerprint сканирования обнаружить версию и тип ОС на удаленном хосте.
6. Применяя технику Idlescan с помощью поднятой виртуальной машины ввести в заблуждение систему IDS и получить характеристики открытости портов с удаленного хоста.
7. Разобрать методику сканирования IP протоколов, а также обнаружения служб и их версий на удаленных хостах.
8. Исследовать флаги, связанные с управлением временем и производительностью при реализации разных методик сканирования удаленных хостов.

7. Контрольные вопросы:

1. Для чего нужно ПО NMap?
2. Всегда ли NMap корректно трактует наличие на удаленном хосте средств IDS? Если нет, то почему?
3. Возможно ли полностью защитить удаленных хост от сканирования?
4. Дайте общие рекомендации для защиты удаленного хоста, а также методов для введение в заблуждение злоумышленника, осуществляющего сканирование защищаемого узла.

Время на выполнение лабораторной работы – 5 часов.

Образовательная организация, авторы, эл. почта: Самарский национальный исследовательский университет им. академика С.П. Королева, Михаил Евгеньевич, burlakov@ssau.ru

СПЕЦИАЛИТЕТ 10.05.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Дисциплина: Защита информации в компьютерных сетях

Образовательная программа: 10.05.02 Информационная безопасность телекоммуникационных систем, 10.03.01 Информационная безопасность.

Дисциплина: Защита информации в компьютерных сетях.

Лабораторная работа.

Обнаружение уязвимостей с помощью сканера безопасности Nessus

1. Учебные цели:

Получить теоретические и практические знания о методике обнаружения уязвимостей сетевых узлов при помощи сканера безопасности.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Знать основные механизмы и способы обнаружения уязвимостей, владеть навыками по устранению обнаруженных уязвимостей и работе со сканером безопасности Nessus.

3. Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение: Компьютерная лаборатория с ЛВС, среда для запуска виртуальных машин на базе VMware, образ виртуальной машины под управлением ОС Windows, сканер безопасности Nessus.

4. Задание на исследование:

- изучить теоретический материал по работе со сканером безопасности Nessus;
- выполнить задания по обнаружению уязвимостей сетевых узлов ЛВС лаборатории с помощью сканера безопасности Nessus.

5. Краткие теоретические сведения:

Под понятием уязвимость понимают слабость в системе защиты, которая дает возможность реализовать ту или иную угрозу. Под угрозой понимают совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности и конфиденциальности информации, хранящейся, обрабатываемой и проходящей через сетевую компьютерную систему. Уязвимости могут являться как следствием ошибочного администрирования компьютерной системы, так и следствием ошибок, допущенных при реализации механизмов безопасности разработчиком ПО.

Как правило, выделяют следующие группы уязвимостей:

- слабые и неустойчивые пароли;
- ошибки при конфигурировании систем безопасности ОС;
- отсутствие актуальных обновлений ОС;
- уязвимость к атакам из внешних сетей;
- бэкдоры и трояны и т.д.

Сканеры безопасности осуществляют поиск уязвимостей, за счет автоматизации операций по оценке защищенности систем. Сканеры безопасности могут определять уязвимости как по различным косвенным признакам (пассивное сканирование), например, проверке заголовков сервисов и их версий, так и путем имитации атаки (активное сканирование), т.е. применяя т.н. эксплойты. Большинство сканеров по результатам сканирования могут давать рекомендации по устранению данных уязвимостей.

Не стоит забывать важные моменты касательно сканеров безопасности. Они не могут обнаружить уязвимости 0-day. Как и антивирусные программные продукты, их базы должны обновляться каждый день, чтобы быть эффективными.

Сканер безопасности Nessus это мультиплатформенный инструмент, разработанный для сетевых администраторов, и позволяющий проверять, независимо от операционной системы, используемой на компьютере, наличие любых «дыр» в безопасности, которые могут присутствовать в локальной сети или на персональном компьютере. Nessus позволяет оперативно обнаруживать информационные ресурсы, проверять правильность конфигураций, формировать профили безопасности, а также управлять применением исправлений. Это достигается путем выявления наличия ряда уже известных уязвимостей, которые входят в состав обширной базы данных плагинов программы.

Основные возможности Nessus:

- Оперативное и точное обнаружение информационных ресурсов.
- Проверка соответствия требованиям FFIEC, FISMA и др.
- Проверка систем управления сетью.
- Проверка наличия конфиденциальной информацией, включая ПДн.
- Сканирование на наличие уязвимостей сетевых устройств, хостов, операционных систем БД и веб-приложений.
- Обнаружение нарушений безопасности (вирусы, бэкдоры, ботнеты и т.д.).
- Обнаружение локальных уязвимостей.

Интерфейс пользователя (ИП) Nessus представляет собой веб-интерфейс сканера Nessus, который состоит из простого HTTP-сервера и веб-клиента, не требующего установки программного обеспечения, кроме установки сервера Nessus. Для запуска графического интерфейса пользователя Nessus на панели навигации любого браузера необходимо ввести адрес <https://localhost:8834/>. Примечание: адрес localhost вводится только в случае входа в клиентскую часть на стороне сервера. При удаленном входе, из сегмента ЛВС, необходимо вместо localhost указать IP-адрес сервера.

После авторизации открывается главный экран пользователя с меню для выполнения сканирования. Фрагмент главного экрана представлен на рисунке 1.

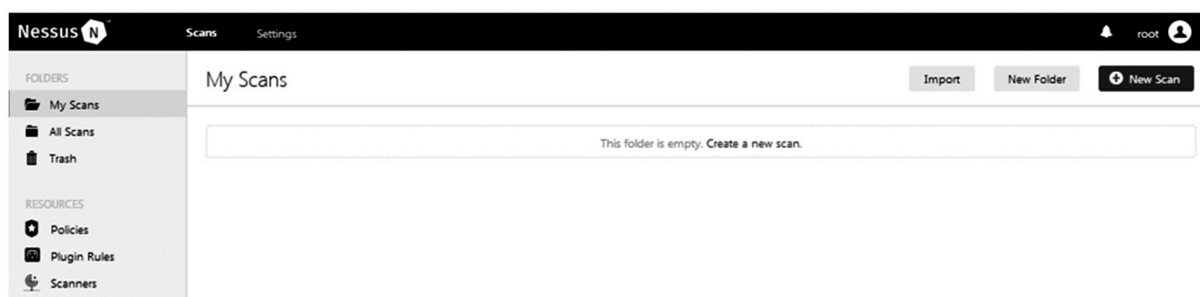


Рис. 1. Фрагмент главного экрана пользователя

Для перехода в режим сканирования перейдите в меню «Scans» и нажмите «New scan» – вы перейдете в окно выбора типа сканирования (см. рис. 2).

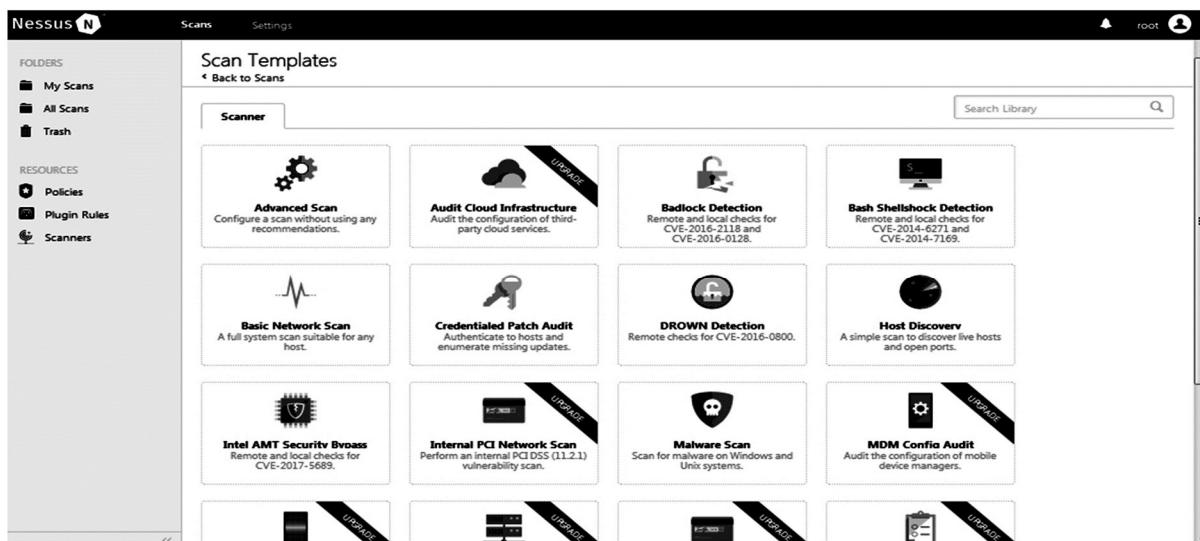


Рис. 2. Окно экрана выбора шаблона сканирования

В основе политик сканирования в Nessus положены различные шаблоны проверок, используемые для различных частных и общих задач. Наиболее часто используемые политики: Web Application Tests Policy – политика сканирования веб-приложений на наличие уязвимостей, Basic Network Scan Policy – сканирование внешних или внутренних хостов на наличие уязвимостей. Нажав по кнопке «Basic Network Scan» откроется страница настроек сессии сканирования (см. рис. 3), где нужно указать название данной сессии, её описание и диапазон сканирования.

В поле «Targets» необходимо указать узлы, которые будем сканировать. Можно указать как отдельные адреса, так и всю подсеть IP адресов 192.168.1.0/24. После настройки всех параметров нажима-

ем "Save". Для запуска процесса сканирования необходимо нажать кнопку "Launch" в открывшемся списке созданных сессий сканирования (см. рис. 4).

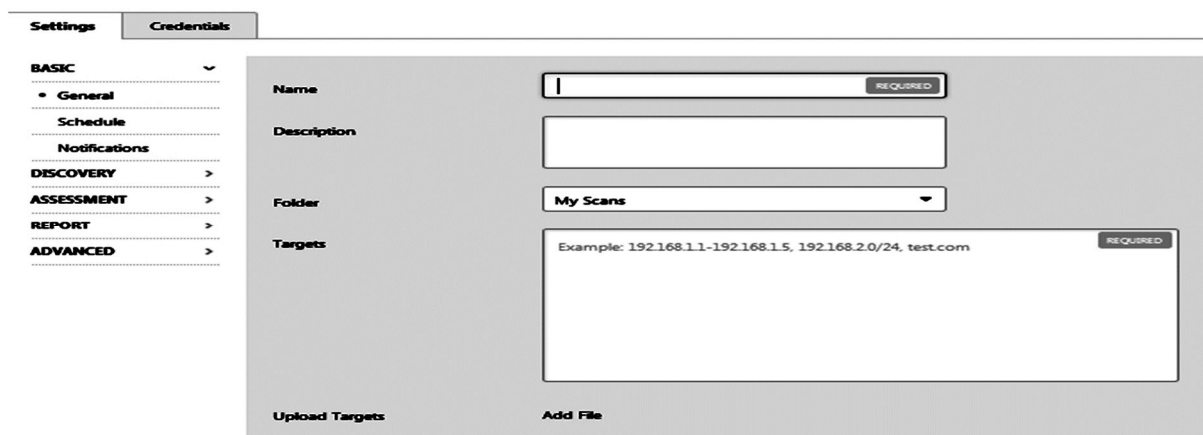


Рис. 3. Окно создания сессии сканирования

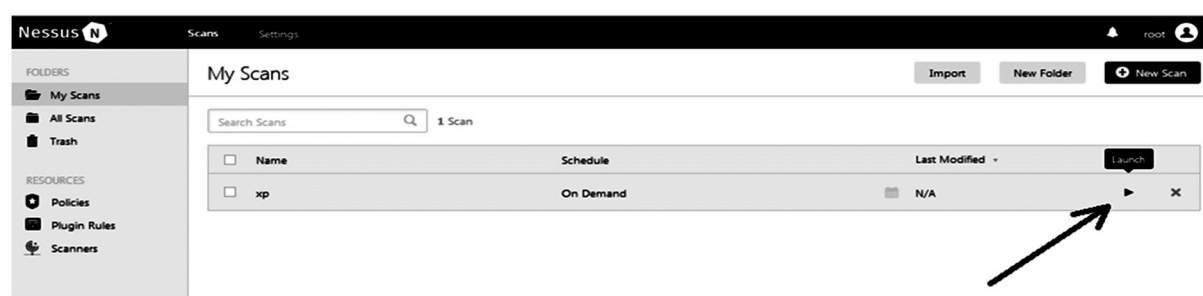


Рис. 4. Список сессий сканирования


Процесс сканирования обозначается анимацией значка  в третьей колонке списка «My Scans». Нажав по данной задаче сканирования можно перейти в окно отображающей информацию о текущем статусе сканирования и найденных на данный момент уязвимостях. Пример окна статуса сканирования сетевого узла на базе ОС Windows XP представлен на рисунке 5.



Рис. 5. Фрагмент окна статуса сканирования

По результатам сканирования мы получаем список с IP адресами и связанные с ними риски. Риски имеют цветовую кодировку. Для просмотра уязвимостей, обнаруженных в сети нажимаем "vulnerabilities" в верхнем меню.

На рисунке 6 показан фрагмент окна обнаруженных уязвимостей. Если кликнуть по конкретной уязвимости, то мы получим более детальную информацию. Важно отметить, что помимо описания уязвимости, в отчете присутствует также и способ ее исправления и закрытия (раздел Solution в описании уязвимости). Более подробное описание работы сканера можно найти на сайте производителя: https://docs.tenable.com/nessus/6_11/Content/GettingStarted.htm или в файле «DOCS\Nessus_6_11.pdf».

Sev	Name	Family	Count
CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities ...	Windows	1
MEDIUM	SMB Signing Disabled	Misc.	1
INFO	Nessus SYN scanner	Port scanners	9

Рис. 6. Фрагмент окна обнаруженных уязвимостей

6. Порядок выполнения лабораторной работы (этапы)

В качестве целей для сканирования необходимо использовать только специально подготовленные для выполнения данной лабораторной работы образы виртуальных машин “winxp”, “win2000” и “win2003”. Учетные записи для запуска образов необходимо запросить у преподавателя.

- С помощью Nessus просканируйте:
 - вашу виртуальную машину;
 - ваш физический ПЭВМ;
 - виртуальную машину, определенную преподавателем.
- Изучите отчеты, сгенерированные Nessus. Внести в отчет по лабораторной работе информацию о найденных проблемах и уязвимостях
- Изучите рекомендации сканера по закрытию найденных уязвимостей;
- Закройте наиболее критические уязвимости любым доступным способом, не нарушающим функционирование сетевого узла.

7. Контрольные вопросы:

- Что называется уязвимостью?
- Какие причины возникновения уязвимостей вы знаете?
- Какие признаки уязвимостей используются сканерами?
- Назовите основные возможности сканера Nessus.
- Назовите наиболее часто используемые политики сканирования в сканере Nessus.
- Предоставляет ли сканер Nessus информацию об устранении уязвимостей?

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ», доцент кафедры СИБ Ахметвалеев А.М., AMAkhmetvaleev@kai.ru

Дисциплина: Оптические телекоммуникационные системы и сети

Образовательная программа: 10.05.02 Информационная безопасность телекоммуникационных систем, Разработка защищённых телекоммуникационных систем.

Дисциплина: Оптические телекоммуникационные системы и сети.

Лабораторная работа.

Экспериментальное выявление НСД к ВОЛС за счёт контроля мощности сигналов в линии связи

1. Учебные цели:

Изучение принципов контроля несанкционированного доступа (НСД) к волоконно-оптической линии связи (ВОЛС) за счёт использования контроля мощности сигналов в линии связи, получение практических навыков работы волоконно-оптическим контрольно-измерительным оборудованием.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь:

- работать с современной элементной базой аппаратуры оптических телекоммуникационных систем и сетей; обоснованно выбирать архитектурные решения по построению оптических телекоммуникационных сетей и систем, в том числе средства и методы обеспечения защиты информации.

Владеть:

- навыками использования современной измерительной аппаратуры при проведении измерений в оптических системах связи, навыками рационального выбора средств и методов защиты оптических телекоммуникационных сетей и систем.

3. Перечень материально-технического обеспечения:

Модули преобразования интерфейсов (медиаконвертеры) P-Link AFS100-25, многофункциональная модульная тест-система мощности Yokogawa AQ2200, имитаторы ВОЛС (нормализующая катушка длиной 4 км, участок оголённого волокна 100 м), имитатор НСД к ВОЛС в виде прищепки FOD-5503, волоконно-оптический ответвитель 90/10 %, волоконно-оптический микроскоп Westover FM C-400, персональные компьютеры, осциллограф LeCroy WaveSurfer 104 Xs, программируемый генератор импульсов Tabor 8500, вольтметр универсальный В7-78/1, сетевой кабель «витая пара», соединительные оптические шнуры и соединительные оптические розетки

4. Задание на исследование

В лабораторной работе два персональных компьютера соединены между собой в локальную сеть с помощью преобразователей интерфейсов (медная витая пара – оптическое волокно). Между данными компьютерами поддерживается и контролируется наличие связи с помощью команды ping (утилита для проверки соединений в сетях на основе TCP/IP).

К ВОЛС, представляющей собой катушку волокна длиной 4 км и имитатор НСД в виде участка оголённого волокна (100 м) с возможностью подключения к его середине волоконно-оптического ответвителя-прищепки FOD-5503, на одном из концов подключён ответвитель, выводящий 10 % мощности излучения на контрольное оборудование.

Контроль мощности осуществляется с помощью модуля AQ2200-211 модульной тест-системы Yokogawa AQ2202. Аналоговый выход модуля, напряжение на котором пропорционально измеряемому уровню мощности, подключён к программируемому генератору импульсов Tabor 8500 (служит для формирования сигнала тревоги) и осциллографу LeCroy WaveSurfer 104 Xs.

Попытка НСД к ВОЛС будет приводить к внесению потерь в линию связи. Причём без контрольной аппаратуры это может быть не замечено легальными пользователями (связь между компьютерами не прервётся). Но при этом контрольное оборудование может зафиксировать даже незначительные изменения мощности в линии связи с выдачей сигнала тревоги.

5. Краткие теоретические сведения

Сущность демонстрируемого метода использования контроля мощности для выявления несанкционированного доступа к ВОЛС заключается в следующем.

Часть сигнала, передаваемого в ВОЛС от передающего оптического модуля к приёмному оптическому модулю, ответвляется с помощью волоконно-оптического ответвителя и направляется к оптическому измерителю мощности. Данный метод используется для того, чтобы отследить изменение уровня мощности и сравнить его с некоторым ожидаемым пороговым значением либо набором пороговых зна-

чений уровней. Несанкционированное воздействие на волокно, например, с целью получения доступа к передаваемому сигналу, как правило, вызывает внесение дополнительных потерь в линию связи и падение уровня мощности оптического сигнала на приёмном оптическом модуле.

6. Порядок выполнения лабораторной работы:

Схема проведения эксперимента показана на рисунке 1.

1. Проверить чистоту всех оптических разъёмов с помощью микроскопа Westover FM C-400, при необходимости провести очистку.
2. Убедиться, что компьютер 10.10.131.91 подключен к локальной сети.
3. Подключить порт RJ-45 медиаконвертера P-Link AFS100-25A к локальной сети.
4. Подключить оптический порт медиаконвертера P-Link AFS100-25A к имитатору ВОЛС (катушка волокна длиной 4 км).
5. Второй конец имитатора ВОЛС (катушка волокна длиной 4 км) подключить имитатору НСД (оголённое волокно длиной 100 м с возможностью установки прищепки FOD-5503).
6. Второй конец имитатора НСД (оголённое волокно длиной около 100 м с возможностью установки прищепки FOD-5503) подключить к входу ответвителя.
7. Выходной порт ответвителя, на который отводится 90 % мощности излучения, подключить к оптическому порту второго медиаконвертера P-Link AFS100-25B.
8. Подключить порт RJ-45 второго медиаконвертера P-Link AFS100-25B к компьютеру 10.10.131.92.
9. Подключить к медиаконвертерам источники питающего напряжения.
10. По световым индикаторам медиаконвертеров убедиться в наличии связи между ними, а также в обеспечении связи между соединяемыми сегментами локальной сети.
11. Выполнить на компьютере 10.10.131.92 команду «ping –t 10.10.131.91», тем самым запустим постоянную проверку связи между данными компьютера. Убедиться, что отклик от компьютера 10.10.131.91 имеется и время отклика незначительно.
12. Выходной порт ответвителя, на который отводится 10 % мощности излучения, подключить к входу измерителя мощности AQ2200-211 модульной тест-системы Yokogawa AQ2202.
13. Включить на измерителе мощности AQ2200-211 режим фиксации максимальных и минимальных значений измеряемой мощности.
14. В течение не менее 1 минуты провести измерения. Зафиксировать максимальное и минимальное значения измеряемой мощности, разницу между ними, рассчитать среднее значение мощности при отсутствии НСД.
15. Включить на измерителе мощности AQ2200-211 режим использования аналогового выхода. Установить линейный режим работы аналогового выхода.
16. В качестве опорного (максимального) значения мощности сигнала в линии задать значение, на 2...3 дБ превышающее рассчитанное ранее среднее значение мощности в линии при отсутствии НСД.
17. Аналоговый выход модуля AQ2200-211 подключить к осциллографу LeCroy WaveSurfer 104 Xs.
18. Настроить осциллограф для устойчивого отображения сигнала (который прямо пропорционален мощности оптического излучения в линии связи).
19. С помощью встроенных средств осциллографа зафиксировать среднее значение напряжения на аналоговом выходе модуля измерителя мощности AQ2200-211 при отсутствии НСД.
20. Подключить к оголенному волокну прищепку FOD-5503, тем самым осуществляя несанкционированный доступ к ВОЛС.
21. С помощью измерителя мощности и осциллографа убедиться в уменьшении уровня сигнала в линии.
22. С помощью наблюдения за выводом ранее запущенной команды «ping –t 10.10.131.91» убедиться в наличии устойчивой связи между компьютерами. Сделать вывод о невлинии осуществлённого НСД на связь между легальными пользователями (и тем самым о невозможности обнаружить факт НСД без использования контрольной аппаратуры).
23. Включить на измерителе мощности AQ2200-211 режим фиксации максимальных и минимальных значений измеряемой мощности.
24. В течение не менее 1 минуты провести измерения. Зафиксировать максимальное и минимальное значения измеряемой мощности, разницу между ними, рассчитать среднее значение мощности при наличии НСД.
25. С помощью встроенных средств осциллографа зафиксировать среднее значение напряжения на аналоговом выходе модуля измерителя мощности AQ2200-211 при наличии НСД.
26. Сравнить значения мощностей в контролируемой линии связи при отсутствии и наличии НСД к ВОЛС.
27. Сравнить значения напряжений на аналоговом выходе измерителя мощности AQ2200-211 при отсутствии и наличии НСД к ВОЛС.
28. Подключить аналоговый выход измерителя мощности к управляющему входу TRIG INPUT программируемого генератора Tabor 8500.

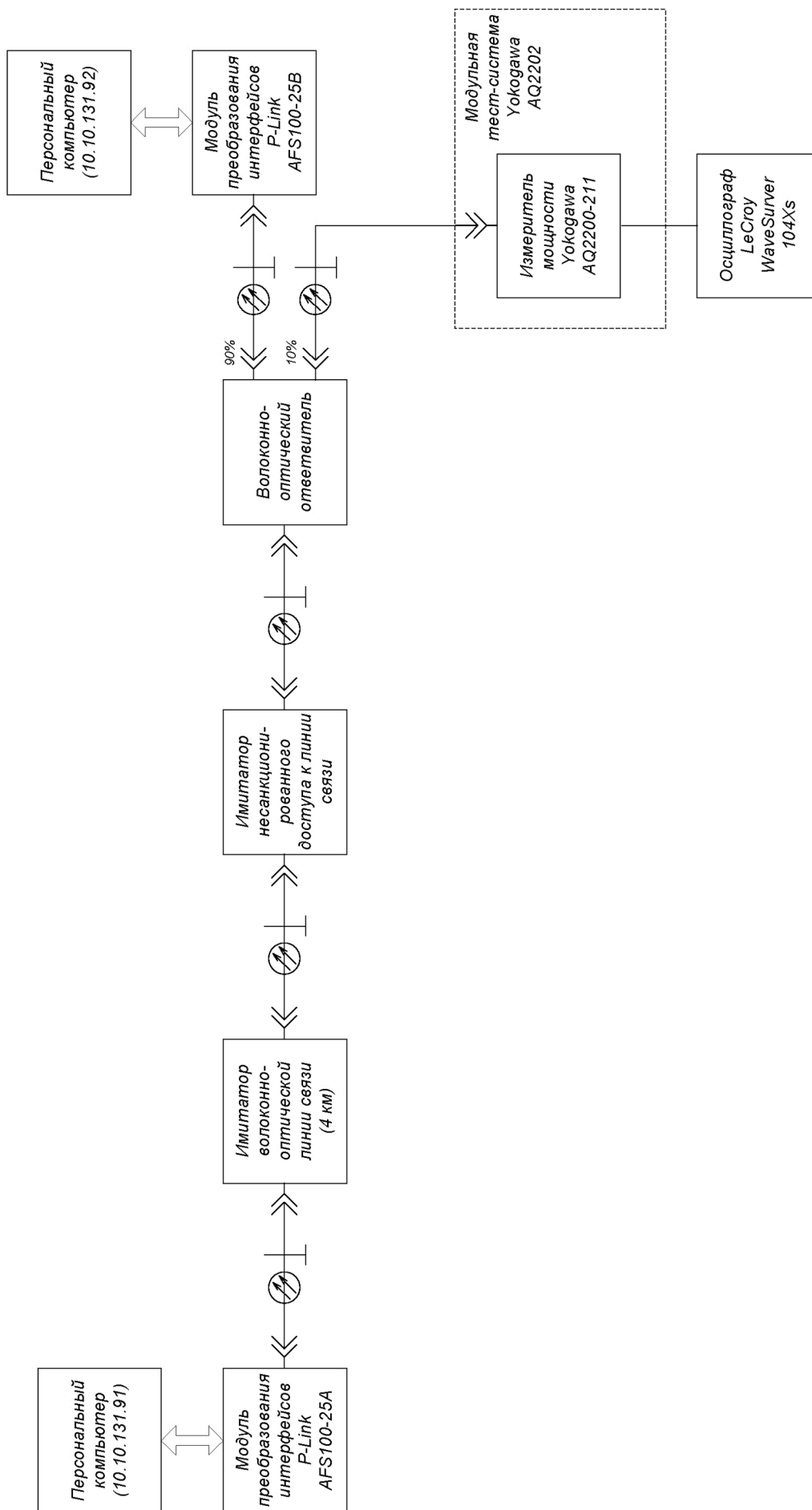


Рисунок 1. Схема проведения экспериментальных исследований

29. Настроить порог срабатывания управляющего триггера программируемого генератора Tabor 8500 таким образом, чтобы при подключении к линии связи ответителя прищепки происходил запуск генерации (формирование импульса, означающего наличие тревоги при контроле несанкционированного доступа к ВОЛС).
30. Сделать выводы о возможности выявления НСД с помощью измерителя мощности AQ2200-211 модульной тест-системы Yokogawa AQ2202.

7. Контрольные вопросы:

1. Поясните схему проведения экспериментальных испытаний.
2. Поясните назначение используемого оборудования.
3. Поясните назначение основных конструктивных элементов волоконно-оптического ответителя-прищепки FOD 5503.
4. Почему при работе с волоконно-оптическим ответителем-прищепкой FOD 5503 потери в ответвленном канале на длине волны 1550 нм превышают эти же потери на длине волны 1310 нм в 2..3 раза (на 3..5 дБ)?
5. Поясните итоговые результаты работы (скриншот экрана осциллографа с моментом срабатывания системы контроля и формирования сигнала тревоги).
6. Поясните, каким образом (за счёт каких преобразований) в экспериментальных испытаниях уровень мощности оптического сигнала визуализировался на экране осциллографа?
7. Поясните настройки генератора Tabor8500, используемого в ключевой схеме формирования сигнала тревоги.
8. Поясните, за счёт чего возможен контроль уровня мощности при передаче цифровых сигналов (то есть в ситуации, когда в линии связи постоянно "случайным" образом чередуются высокий и низкий логический уровень цифрового сигнала).
9. Сравните способы контроля НСД к ВОЛС за счёт измерения мощности передаваемого сигнала и за счёт использования контрольных сигналов. В чём их сравнительные преимущества и недостатки?
10. Сравните способы контроля НСД к ВОЛС за счёт контроля средней мощности и за счёт контроля спектра передаваемых сигналов. В чём их сравнительные преимущества и недостатки?

Время на выполнение лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, кафедра информационной безопасности телекоммуникационных систем, к.т.н., доцент Горбунов Александр Валерьевич, avgorbunov@sfedu.ru

Образовательная программа: 10.05.02 Информационная безопасность телекоммуникационных систем, Разработка защищённых телекоммуникационных систем.

Дисциплина: Оптические телекоммуникационные системы и сети.

Лабораторная работа. **Экспериментальное выявление НСД к ВОЛС** **с использованием метода анализа спектра**

1. Учебные цели:

Изучение принципов контроля несанкционированного доступа (НСД) к волоконно-оптической линии связи (ВОЛС) за счёт использования анализа спектра передаваемого сигнала, получение практических навыков работы волоконно-оптическим контрольно-измерительным оборудованием.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь:

- работать с современной элементной базой аппаратуры оптических телекоммуникационных систем и сетей; обоснованно выбирать архитектурные решения по построению оптических телекоммуникационных сетей и систем, в том числе средства и методы обеспечения защиты информации.

Владеть:

- навыками использования современной измерительной аппаратуры при проведении измерений в оптических системах связи, навыками рационального выбора средств и методов защиты оптических телекоммуникационных сетей и систем.

3. Перечень материально-технического обеспечения:

Модули преобразования интерфейсов (медиаконвертеры) TP-Link TR-965D, оптический спектроанализатор Yokogawa AQ6370, многофункциональная модульная тест-системы Yokogawa AQ2202, волоконно-оптический ответвитель-прищепка FOD-5503, оптический соединительный шнур с участком оголённого до полимерной оболочки (250 мкм) волокна, катушки волокна длиной 2 и 4 км, ответвители 50/50 %, ответвитель 90/10 %, оптический циркулятор, оптический переключатель, оптический EDFA-усилитель, волоконно-оптическая система передачи Proflex, волоконно-оптический микроскоп Westover FM C-400, два персональных компьютера, сетевой кабель «витая пара», соединительные оптические шнуры и соединительные оптические розетки.

4. Задание на исследование

В лабораторной работе два персональных компьютера соединены между собой в локальную сеть с помощью преобразователей интерфейсов (медная витая пара – оптическое волокно). Между данными компьютерами поддерживается и контролируется наличие связи с помощью команды ping (утилита для проверки соединений в сетях на основе TCP/IP).

К линии связи, представляющей собой катушку волокна длиной 4 км и имитатор НСД в виде участка оголённого волокна (100 м) с возможностью подключения к его середине волоконно-оптического ответвителя-прищепки FOD-5503, на одном из концов подключён ответвитель, выводящий 10 % мощности излучения на контрольное оборудование.

Контроль средней мощности осуществляется с помощью модуля AQ2200-211 модульной тест-системы Yokogawa AQ2202. Контроль спектра излучения осуществляется с помощью спектроанализатора Yokogawa AQ6370. Подключение того или иного измерительного прибора к линии связи осуществляется с помощью волоконно-оптического переключателя.

При имитации компенсационного НСД к ВОЛС сигнал выводится из линии связи с помощью ответвителя прищепки FOD-5503. Выход ответвителя-прищепки подключён к одному из портов циркулятора, назначение которого заключается в разделении встречных потоков выводимого информационного оптического сигнала и вводимого компенсирующего излучения. Для демонстрации характерных особенностей спектра излучения на выходе оптического усилителя компенсирующее излучение представляет собой усиленный с помощью EDFA-усилителя сигнал полупроводникового лазера. Атенюатор необходим для точной подстройки мощности компенсирующего излучения

Попытка НСД к ВОЛС будет приводить к внесению потерь в линию связи. Причём без контрольной аппаратуры это может быть не замечено легальными пользователями (связь между компьютерами не прервётся). Но при этом контрольное оборудование может зафиксировать даже незначительные изменения мощности в линии связи с выдачей сигнала тревоги.

5. Краткие теоретические сведения

Сущность демонстрируемого метода использования контроля мощности для выявления несанкционированного доступа к ВОЛС заключается в следующем.

Часть сигнала, передаваемого в ВОЛС от передающего оптического модуля к приёмному оптическому модулю, ответвляется с помощью волоконно-оптического ответвителя и направляется к оптическому измерителю мощности. Данный метод используется для того, чтобы отследить изменение уровня мощности и сравнить его с некоторым ожидаемым пороговым значением либо набором пороговых значений уровней. Несанкционированное воздействие на волокно, например, с целью получения доступа к передаваемому сигналу, как правило, вызывает внесение дополнительных потерь в линию связи и падение уровня мощности оптического сигнала на приёмном оптическом модуле.

6. Порядок выполнения лабораторной работы:

Внимание! До получения специальных указаний от преподавателя запрещается включать оптический усилитель, так как мощность на его выходе представляет опасность для человека и большинства используемого оборудования.

Схема проведения эксперимента показана на рисунке 1.

1. Проверить чистоту всех оптических разъемов с помощью микроскопа Westover FM C-400, при необходимости провести очистку коннекторов.
2. Убедиться, что компьютер 10.10.131.91 подключён к локальной сети.
3. Подключить порт RJ-45 медиаконвертера TP-Link TR-965DA к локальной сети.
4. Подключить оптический порт медиаконвертера TP-Link TR-965DA к имитатору ВОЛС (катушка волокна длиной 4 км).
5. Второй конец имитатора ВОЛС (катушка волокна длиной 4 км) подключить к имитатору НСД (оголённое волокно длиной 100 м с возможностью установки прищепки FOD-5503).
6. Второй конец имитатора НСД (оголённое волокно длиной 100 м с возможностью установки прищепки FOD-5503) подключить к входу ответвителя 90/10 %.
7. Выходной порт ответвителя, на который отводится 90 % мощности излучения, подключить к оптическому порту второго медиаконвертера TP-LINK TR-965DB.

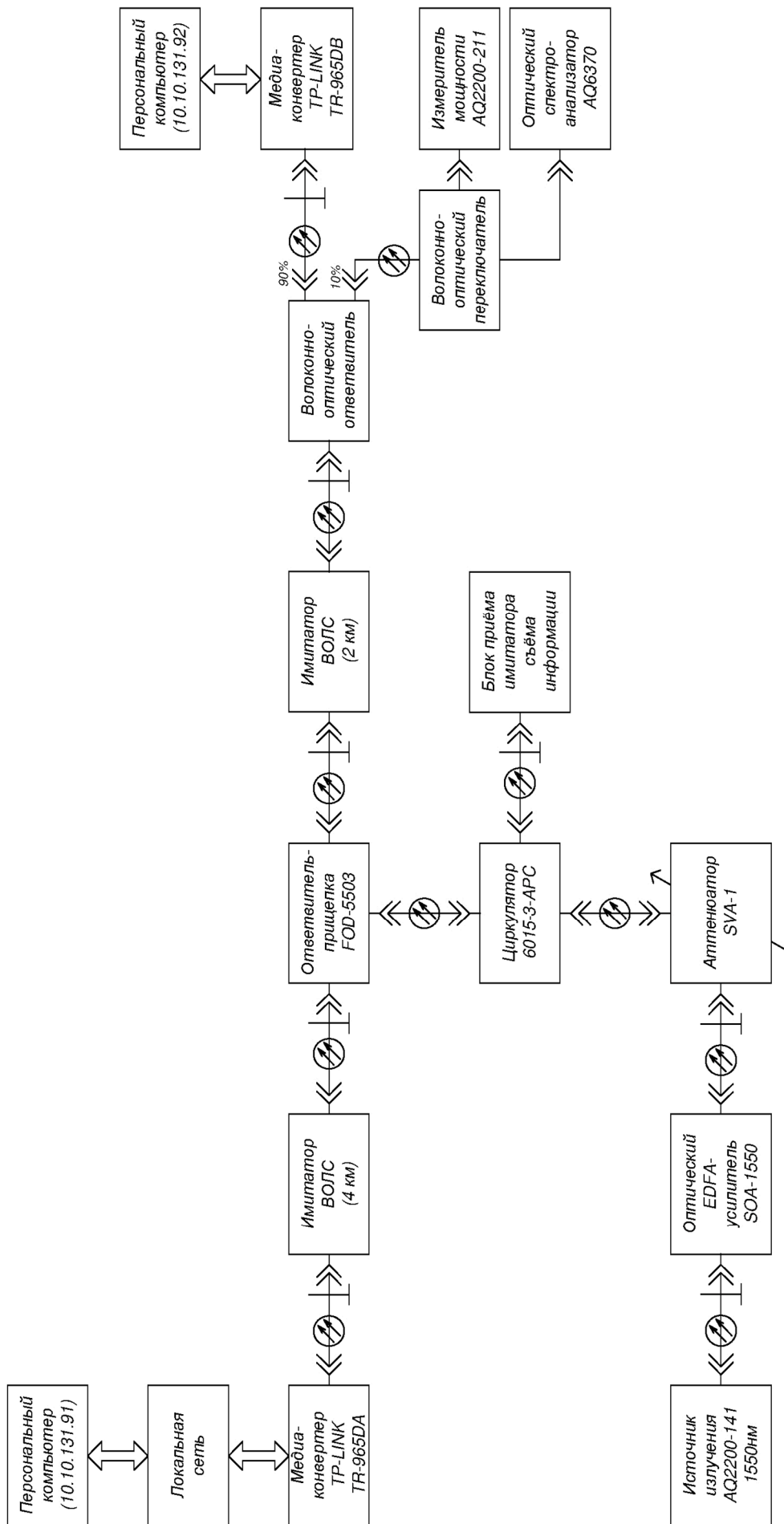


Рис. 1. Схема проведения экспериментальных исследований

8. Подключить порт RJ-45 второго медиаконвертера TP-LINK TR-965DB к компьютеру 10.10.131.92.
9. Подключить к медиаконвертерам источники питающего напряжения.
10. По световым индикаторам медиаконвертеров убедиться в наличии связи между ними, а также в обеспечении связи между соединяемыми сегментами локальной сети.
11. Выполнить на компьютере 10.10.131.92 команду «ping –t 10.10.131.91», тем самым запустив постоянную проверку связи между данными компьютера. Убедиться, что отклик от компьютера 10.10.131.91 имеется, и время отклика незначительно.
12. Выходной порт ответвителя, на который отводится 10 % мощности излучения, с помощью оптического переключателя подключить к входу измерителя мощности AQ2200-211 модульной тест-системы Yokogawa AQ2202.
13. Измерить и зафиксировать мощность излучения в линии без имитации съема.
14. Отключить от второго выхода ответвителя измеритель мощности Yokogawa AQ2202 и подключить к ответвителю спектроанализатор Yokogawa AQ6370.
15. Снять спектрограмму излучения. Сохранить полученную спектрограмму как первую трассу спектроанализатора.
16. Подключить к оголенному волокну прищепку FOD-5503, тем самым осуществляя несанкционированный доступ к ВОЛС.
17. С помощью измерителя мощности убедиться в уменьшении уровня сигнала в линии.
18. С помощью наблюдения за выводом ранее запущенной команды «ping –t 10.10.131.91» убедиться в наличии устойчивой связи между компьютерами. Сделать вывод о невлинии осуществлённого НСД на связь между легальными пользователями (и тем самым о невозможности обнаружить факт НСД без использования контрольной аппаратуры).
19. Выходной порт ответвителя, на который отводится 10 % мощности излучения, с помощью оптического переключателя подключить к входу измерителя мощности AQ2200-211 модульной тест-системы Yokogawa AQ2202.
20. Измерить и зафиксировать мощность излучения в линии при наличии имитации съема.
21. Отключить от второго выхода ответвителя измеритель мощности Yokogawa AQ2202 и подключить к нему Yokogawa AQ6370.
22. Снять, проанализировать и сохранить спектрограмму излучения при наличии имитации съема.
23. Вход оптического переключателя подключить к неподключенному выходу циркулятора.
24. Повторить измерения в пп. 19–22 для выводимого из линии сигнала при осуществлении НСД.
25. Повторно подключить вход оптического переключателя к второму (10 %) выходу оптического ответвителя в соответствии со схемой, приведённой на Рис. 6.1.
26. Установить на аттенуаторе максимальное затухание.
27. Включить дополнительный лазерный модуль, используемый в качестве источника компенсирующего излучения, и оптический усилитель.
28. Выходной порт ответвителя, на который отводится 10 % мощности излучения, с помощью оптического переключателя подключить к входу измерителя мощности AQ2200-211 модульной тест-системы Yokogawa AQ2202.
29. С помощью аттенуатора добиться того, чтобы мощность излучения, полученная в п. 13, совпала с мощностью излучения, регистрируемой при имитации НСД.
30. Измерить и зафиксировать мощность излучения в линии при наличии имитации съема.
31. С помощью наблюдения за выводом ранее запущенной команды «ping –t 10.10.131.91» убедиться в наличии устойчивой связи между компьютерами. Сделать вывод о невлинии осуществлённого компенсационного НСД на связь между легальными пользователями (и тем самым о невозможности обнаружить факт НСД с контролем только мощности излучения).
32. Отключить от второго выхода ответвителя измеритель мощности Yokogawa AQ2202 и подключить к нему спектроанализатор Yokogawa AQ6370.
33. Снять спектрограмму излучения в линии связи с НСД и сохранить её как вторую трассу спектроанализатора.
34. С помощью встроенных средств спектроанализатора проанализировать обе полученные трассы, провести сравнение полученных результатов.
35. Выключить используемое оборудование.
36. Сделать выводы о возможностях применения спектроанализаторов для выявления компенсационного НСД к ВОЛС.

7. Контрольные вопросы:

1. Поясните схему проведения эксперимента по контролю компенсационного несанкционированного доступа (НСД) к волоконно-оптической линии связи (ВОЛС) за счёт анализа спектра сигнала в линии связи.
2. В чём заключается принцип организации компенсационного метода съёма сигнала с ВОЛС?

3. За счёт автоматического анализа каких параметров спектрограммы сигнала в ВОЛС можно легко выявить компенсационный НДС при сильно различающихся параметрах двух лазеров (основного и компенсирующего)?
4. За счёт автоматического анализа каких параметров спектрограммы сигнала в ВОЛС можно легко выявить компенсационный НДС при несильно различающихся параметрах двух лазеров (основного и компенсирующего)?
5. За счёт автоматического анализа каких параметров спектрограммы сигнала в ВОЛС можно легко выявить компенсационный НДС при использовании EDFA-усилителя в канале компенсации?
6. Каким образом необходимо модифицировать схему эксперимента, чтобы в качестве компенсирующего излучения использовать выводимое из ВОЛС излучение?
7. Укажите и поясните направления распространения всех сигналов на схеме выявления несанкционированного доступа к ВОЛС при компенсационном методе съёма и использовании EDFA-усилителя в канале компенсации.
8. Поясните форму спектрограммы сигнала на выходе системы контроля при осуществлении компенсационного НДС с EDFA-усилителем в канале компенсации (на примере результатов выполнения лабораторной работы).
9. Назовите и поясните преимущества метода контроля спектра сигнала в ВОЛС при выявлении НДС перед другими методами (контроль мощности, рефлектометрический контроль).
10. Назовите и поясните недостатки метода контроля спектра сигнала в ВОЛС при выявлении НДС перед другими методами (контроль мощности, рефлектометрический контроль).

Время на выполнение лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, кафедра информационной безопасности телекоммуникационных система, к.т.н., доцент Горбунов Александр Валерьевич, avgorbunov@sfnedu.ru

Дисциплина: Проектирование защищенных телекоммуникационных систем

Образовательная программа: 10.05.02 Информационная безопасность телекоммуникационных систем.

Дисциплина: Проектирование защищенных телекоммуникационных систем.

Лабораторная работа.

Методы и технологии организации централизованных, многопользовательских защищенных систем информационного взаимодействия

1. Учебные цели:

Изучить и освоить принципы и технологии организации многоуровневого защищенного клиент-серверного взаимодействия, защищенной точки входа в централизованную систему, защищенного обмена протокольной информацией в клиент-серверной многопользовательской системе, а также централизованного информационного взаимодействия в многопользовательской среде посредством информационных сообщений (messaging); овладеть навыками декомпозиции сложных программных комплексов телекоммуникационных систем (ТКС) при их проектировании, выделения наиболее уязвимых компонентов ТКС и потоков информационного взаимодействия.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь обосновать выбор конкурентно-способных вариантов проектных решений по обеспечению информационной безопасности; владеть навыками применения системных методов и средств обеспечения безопасности информационного взаимодействия.

3. Перечень материально-технического обеспечения:

Учебно-исследовательский стенд (УИС) «SQLNetRemoting» в составе сервера баз данных, Web сервера и сервера приложений, динамически размещаемых в локальной сети лаборатории, и доступного множества клиентских ПК с установленным клиентским программным обеспечением.

4. Задание на исследование:

Изучить структуру УИС, технологию установки и настройки его компонентов и выполнить тестовые операции:

- запросы к серверу баз данных;
- организацию локального мессенджера.

5. Краткие теоретические сведения

Клиент-серверный принцип организации информационного взаимодействия, являющийся частным случаем систем централизованного управления, хорошо известен и незаменим, по крайней мере, в двух ситуациях:

- в многопользовательской среде, когда необходимо организовать совместную информационную деятельность, контролировать использование общего ресурса, или документировать результаты взаимодействия, и т.д.;
- для организации защищенного доступа к удаленному ресурсу, размещенному на сервере.

Особое внимание в лабораторной работе уделено решению проблем безопасного развертывания и эксплуатации клиентских и серверных компонентов УИС. Проблема заключается в том, что взаимодействие этих компонентов обеспечивается путем создания партнерских прокси-объектов на соответствующих сторонах взаимодействия. Разумеется, при этом раскрывается их структура и нарушается безопасная эксплуатация. В проекте проверена надежность оригинального метода применения интерфейсных образов в качестве прокси-объектов. Совместно с целенаправленным применением метода сокрытия реализующих членов классов внутри открытых членов-оболочек эти приемы обеспечивают наиболее высокий уровень безопасности взаимодействия компонентов.

Эффективное взаимодействие клиентских и серверных компонентов так или иначе связано с синхронизацией, под которой в программном пространстве чаще всего понимается причинно-следственная связь событий.

Наиболее распространенной является взаимная синхронизация, основанная на генерации программных событий на обеих сторонах информационного взаимодействия. Взаимная синхронизация обеспечивает наиболее точное информационное взаимодействие, однако проектировать, развертывать и сопровождать такие системы нелегко. Кроме того, взаимная синхронизация требует симметричного двунаправленного канала передачи данных.

Серверная синхронизация означает генерацию программных событий на стороне сервера. Чаще всего она необходима при длительной обработке клиентских запросов и (или) в многопользовательской системе,

где задержка реакции сервера порождается очередью запросов на обслуживание. Принципиальное отличие этого типа синхронизации от предыдущего заключается в том, что она не требует симметричного двунаправленного канала. Такой тип синхронизации не может обеспечить равноправного (симметричного) информационного взаимодействия. С позиции безопасности, однако, этот тип синхронизации более выгоден, так как обратный канал существует (теоретически) только на время отправки клиенту ответа на его запрос.

Клиентская синхронизация означает генерацию программных событий на стороне клиента. Такая организация информационного взаимодействия необходима при построении централизованной системы, в которой выделенный сервер используется, например, для контроля и аудита всех или определенных действий клиентов. Принципиальное отличие этого типа синхронизации от взаимной синхронизации заключается в том, что здесь не ожидается реакции сервера, а, следовательно, не требуется симметричный двунаправленный канал. Более того, в некоторых случаях может оказаться достаточным применение однонаправленного канала. Разумеется, клиентская синхронизация, как и серверная, не может обеспечить равноправного (симметричного) информационного взаимодействия.

Данный УИС обладает расширенной функциональностью и имеет несколько вариантов применения, реализуя защищенный доступ к удаленному ресурсу сервера баз данных и организуя многопользовательскую среду для совместной информационной деятельности, вследствие чего использует все три метода синхронизации.

На рисунке 1 приведены все основные компоненты УИС и связи между ними в виде UML-диаграммы взаимодействия.

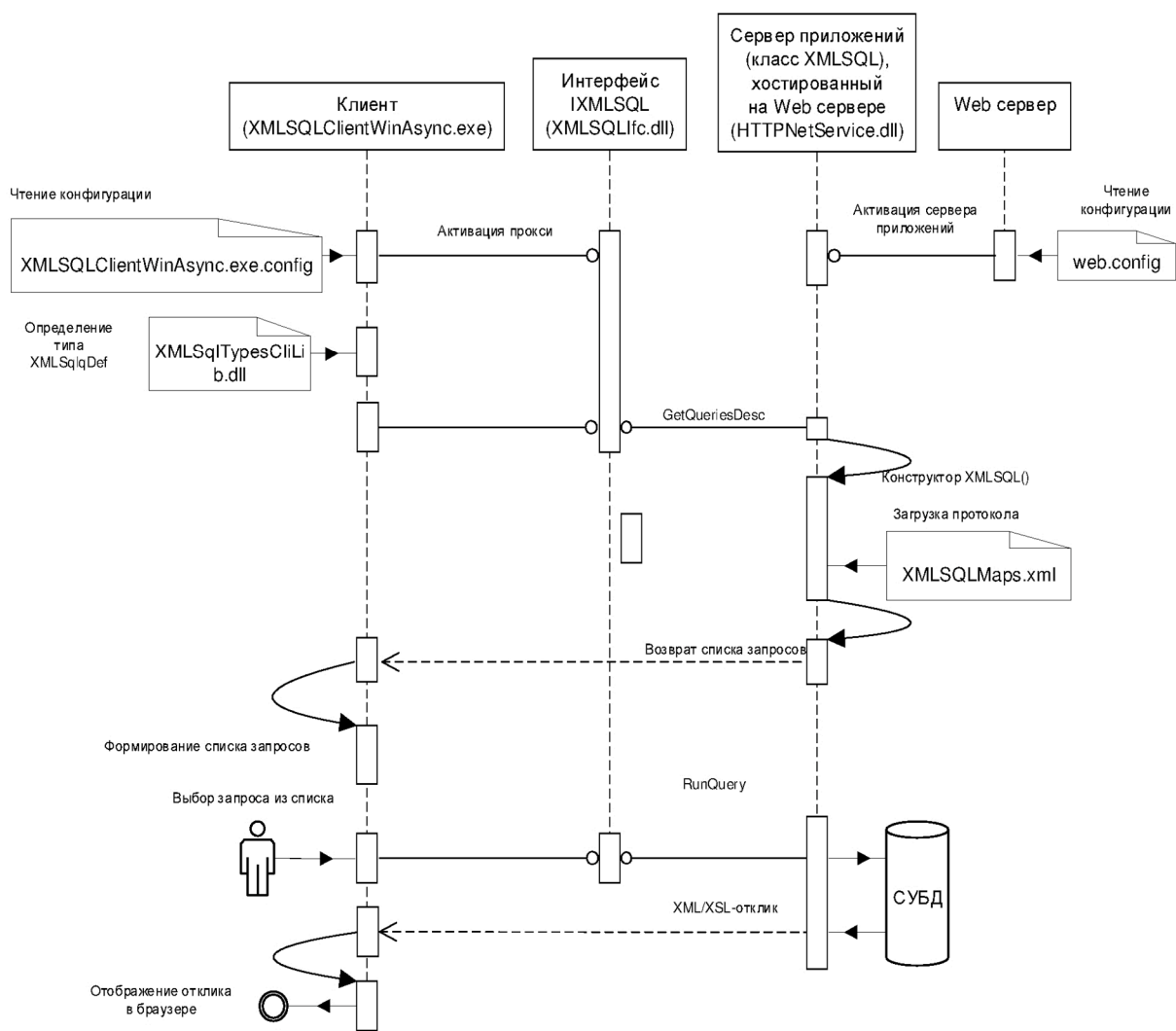


Рис. 1. Диаграмма взаимодействия компонентов УИС

На диаграмме представлены 3 ключевых объекта:

- клиент NetRemoting;
- сервер приложений в виде библиотеки классов HTTPNetService.dll, работающий (хостированный) в среде Web сервера;
- интерфейс IXMLSQL.

Режим работы и функциональность УИС обеспечивается внешними по отношению к нему Web сервером и сервером баз данных. Первый из них является хостом и точкой входа для сервера приложений, а второй обеспечивает его функциональность. При старте Web сервера автоматически из файла web.config читается конфигурация сервера приложений, определяющая все главные его настройки, в том числе, размещение сервера баз данных и параметры соединения с ним. Пример файла web.config приведен на рисунке 2.

```
<configuration>
  <appSettings>
    <add key="SQLServer" value="INSPIRON17R" />
    <add key="Provider" value="SQLOLEDB" />
    <add key="Database" value="NewServerTest" />
    <add key="PWD" value="xxx" />
    <add key="Debug" value="True" />
    <add key="FileFilter" value="*.*" />
    <add key="ActivityFolder" value="Talkers" />
    <add key="MaxUsers" value="5" />
    <add key="FSListen" value="False" />
    <add key="UseActivitiesFile" value="False" />
  </appSettings>
  <system.runtime.remoting>
    <application>
      <service>
        <activated type="XMLSQLServer.XMLSQL, HTTPNetService" />
      </service>
      <channels>
        <channel ref="http">
          <serverProviders>
            <formatter ref="binary" typeFilterLevel="Full" />
          </serverProviders>
          <clientProviders>
            <formatter ref="binary" />
          </clientProviders>
        </channel>
      </channels>
    </application>
    <customErrors mode="off"/>
  </system.runtime.remoting>
</configuration>
```

Рис. 2. Пример конфигурационного файла web.config

Устойчивость работы компонентов УИС обеспечивается реализацией асинхронного режима клиент-серверного взаимодействия. Дополнительная гибкость информационного взаимодействия поддерживается настройкой типа активации – клиентского или серверного, а также выбором транспорта (ТСР, HTTP). Полная функциональность УИС обеспечивается выбором «симметричного» транспорта, поддерживающего взаимную синхронизацию.

Интерфейсная часть проекта изолирует функциональное описание от реализации методов открытых классов сервера.

Конкретная конфигурация клиентского приложения задается в виде двух XML-файлов конфигурации: ClientWinApp.exe.config и XMLSQLClientWinAsync.exe.config, примеры которых приведены на рисунках 3 и 4 соответственно.

```
<configuration>
  <appSettings>
    <add key="Protocol" value="http" />
    <add key="ActivateType" value="client" />
    <add key="User" value="asus_1" />
  </appSettings>
</configuration>
```

Рис. 3. Пример конфигурационного файла ClientWinApp.exe.config

```

<configuration>
  <system.runtime.remoting>
    <application>
      <client url="http://inspiron17r/HTTPNetService">
        <activated type="XMLSQL, HTTPNetService"/>
      </client>
    <channels>
      <channel ref="http" useDefaultCredentials="true" port="0">
        <clientProviders>
          <formatter ref="binary" />
        </clientProviders>
        <serverProviders>
          <formatter ref="binary" typeFilterLevel="Full" />
        </serverProviders>
      </channel>
    </channels>
  </application>
</system.runtime.remoting>
</configuration>

```

Рис. 4. Пример конфигурационного файла XMLSQLClientWinAsync.exe.config

Высокоуровневый протокол взаимодействия хранится на стороне сервера в виде файла XMLSQLMaps.xml. Безопасность использования высокоуровневого протокола поверх сети обеспечивается его разделением на клиентскую и серверные части, каждая из которых владеет только своей функциональностью: клиентская часть отображает регламентированные запросы к серверу в понятном для пользователя виде, передавая по сети при этом их закодированные идентификаторы, которые сервером отображаются на SQL запросы к серверу баз данных. При выборе нужного запроса к серверу вызывается открытый метод сервера RunQuery, конкретная реализация которого скрыта внутри серверного компонента (см. рис. 1). Пример файла высокоуровневого протокола приведен на рисунке 5.

```

<?xml version="1.0" standalone="yes"?>
<NewDataSet>
  <xs:schema id="NewDataSet" xmlns="" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata">
  <xs:element name="NewDataSet" msdata:IsDataSet="true" msdata:Locale="ru-RU">
    <xs:complexType>
      <xs:choice maxOccurs="unbounded">
        <xs:element name="XMLSQLqMaps">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="id" type="xs:int" />
              <xs:element name="desc" type="xs:string" minOccurs="0" />
              <xs:element name="query" type="xs:string" minOccurs="0" />
              <xs:element name="rFile" type="xs:string" minOccurs="0" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:choice>
    </xs:complexType>
  </xs:element>
</xs:schema>
<XMLSQLqMaps>
  <id>0</id>
  <desc>Get all Users, Passwords</desc>
  <query>select Name, Password from Users</query>
  <rFile>r_Users_1</rFile>
</XMLSQLqMaps>
<XMLSQLqMaps>
  <id>1</id>
  <desc>Get active users</desc>
  <query>select Name from Users where discharged=0</query>
  <rFile>r_Users_2</rFile>
</XMLSQLqMaps>
<XMLSQLqMaps>

```



```

<id>2</id>
<desc>Get Users with Passwords</desc>
<query>select Name, Password from Users where Password is not null</query>
<rFile>r_Users_3</rFile>
</XMLSQLqMaps>
<XMLSQLqMaps>
<id>3</id>
<desc>Get User Works</desc>
<query>select UserName, SysUser, HostName, IP, MAC, ProgramName, discharged from Users INNER
JOIN UsersWork ON User_ID = UserID
</query>
<rFile>r_UWorks_1</rFile>
</XMLSQLqMaps>
</NewDataSet>

```

Рис. 5. Пример файла высокоуровневого протокола XMLSQLMaps.xml

6. Порядок выполнения работы:

- изучение структуры УИС (состав и размещение компонентов программного комплекса) – физическое расположение компонентов УИС;
- изучение структуры, содержание и методы редактирования конфигурационных файлов клиентского и серверных компонентов – логическое размещение компонентов УИС;
- изменение структуры УИС путем изменения физического и логического расположения сервера баз данных и (или) Web сервера, сервера приложений;
- выполнение тестовых запросов к серверу баз данных;
- организация локального мессенджера и выполнение сеансов совместного взаимодействия в режиме конференции;
- объяснение и исправление ошибок конфигурирования УИС при их возникновении (настройка системы сложна, поэтому ошибки, как правило, возникают) с использованием log-файла на сервере;
- выявить наиболее уязвимые элементы, компоненты УИС и процессы в информационном взаимодействии;
- обосновать применение и пояснить параметры настройки средств и мер обеспечения безопасности информационного взаимодействия;

7. Контрольные вопросы:

1. Проблемы создания безопасного и надежного ПО.
2. Цели анализа системы при проектировании.
3. Роль декомпозиции системы в процессе оптимизации структуры системы.
4. Способы и средства повышения защищенности систем при их проектировании и оценка их эффективности.
5. Цели управления в информационных системах (ИС)
6. Цели замкнутого управления в ИС.
7. Цели разомкнутого управления в ИС.
8. Цели отложенного управления в ИС.
9. Характеристика централизованного управления системой.
10. Характеристика децентрализованного управления системой.
11. Характеристика и особенности иерархических систем управления.
12. UML-схемы, диаграммы и их роль в проектировании компонентов ИС
13. Способы управления режимами, состоянием и поведением ИС.
14. Способы синхронизации в клиент-серверных системах.
15. Методы эффективного программирования.
16. Структура учебно-исследовательского стенда.
17. Характеристика методов, приемов, технологий организации безопасного информационного взаимодействия на примере УИС.

Время выполнения лабораторной работы – 8 часов.

Образовательная организация, авторы, электронная почта: Московский авиационный институт (национальный исследовательский университет), проф., д.т.н. Михайлов Владимир Юрьевич, mrb402@mai.ru.

Дисциплина: Сети и системы передачи информации

Образовательная программа: 10.05.02 Информационная безопасность телекоммуникационных систем, Защита информации в системах связи и управления.

Дисциплина: Сети и системы передачи информации, Технологии пакетной коммутации.

Лабораторная работа.

Конфигурирование интерфейсов маршрутизаторов

1. Учебные цели:

- Приобрести знания об адресации интерфейсов маршрутизаторов.
- Отработать навыки конфигурирования интерфейсов маршрутизаторов.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

- Уметь конфигурировать адреса интерфейсов
- Владеть навыками конфигурирования и проверки интерфейсов реальных устройств и виртуальных устройств симулятора Packet Tracer.

3. Перечень материально-технического обеспечения:

Компьютерный класс, лаборатория сетей пакетной коммутации.

Лабораторное оборудование и программное обеспечение: Маршрутизаторы Cisco 2811, коммутаторы Catalyst 2600, компьютеры, симулятор Packet Tracer.

4. Задание на исследование








Конфигурирование интерфейсов маршрутизаторов

5. Краткие теоретические сведения

Изложены в литературе:

1. Технологии пакетной коммутации : учебник / Н.Н. Васин. – М. : ИНГУИТ, 2017. С. 41–45; 194–200.
2. Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для вузов / К.Е. Самуйлов, И.А. Шалимов, Н.Н. Васин, В.В. Василевский, Д.С. Кулябов, А.В. Королькова. – М. : Юрайт, 2016. С. 135–145.

6. Порядок выполнения лабораторной работы

1. Запустите программу **Packet Tracer** (рис. 1.1)
2. Сформируйте схему сети передачи (рис. 1.2), для чего добавьте в рабочую область маршрутизатор 2811 (меню  в левом нижнем углу), 2 коммутатора 2960 (меню ) , 4 конечных узла (меню ).
3. Согласно схеме Рис. 1.2 соединить порт FastEthernet 0/0 маршрутизатора со свободным портом FastEthernet коммутатора. Аналогично соединить порт FastEthernet 0/1 с коммутатором. Меню соединений представлено символом . Для соединений использовать прямой кабель (**Straight Through**), представленный сплошной черной линией .
4. Соединить прямым кабелем порты FastEthernet компьютеров с коммутаторами (рис. 1.2).
5. При необходимости удалить какое-либо устройство «кликните» на правой панели значок  , наведите его на удаляемый элемент и «кликните». Значок  отменяет функционирование удаления.
6. Посмотрите и запишите в отчет начальную конфигурацию маршрутизатора, для чего наведите на него курсор.
7. Конфигурацию конечных узлов посмотрите по команде ipconfig в командной строке, для чего «кликните» компьютер. При этом появляется окно (рис. 1.3). Из верхнего меню выберите «рабочий стол» – (Desktop). При этом появляется окно (рис. 1.4). Выберите режим командной строки (Command Prompt). Выполните команду ipconfig (рис. 1.5). Результат запишите в отчет.
8. Сконфигурируйте адреса конечных узлов в сети 1: 192.168.1.11/24; 192.168.1.12/24; и в сети 2: 192.168.2.21/24; 192.168.2.22/24. Для этого, выбрав компьютер, в режиме Desktop (рис. 1.4) выберите режим IP Configuration (левое верхнее окно рис. 1.4). При этом всплывает окно (рис. 1.6). (Не забудьте про шлюз! – Default Gateway). Аналогично – на всех компьютерах.

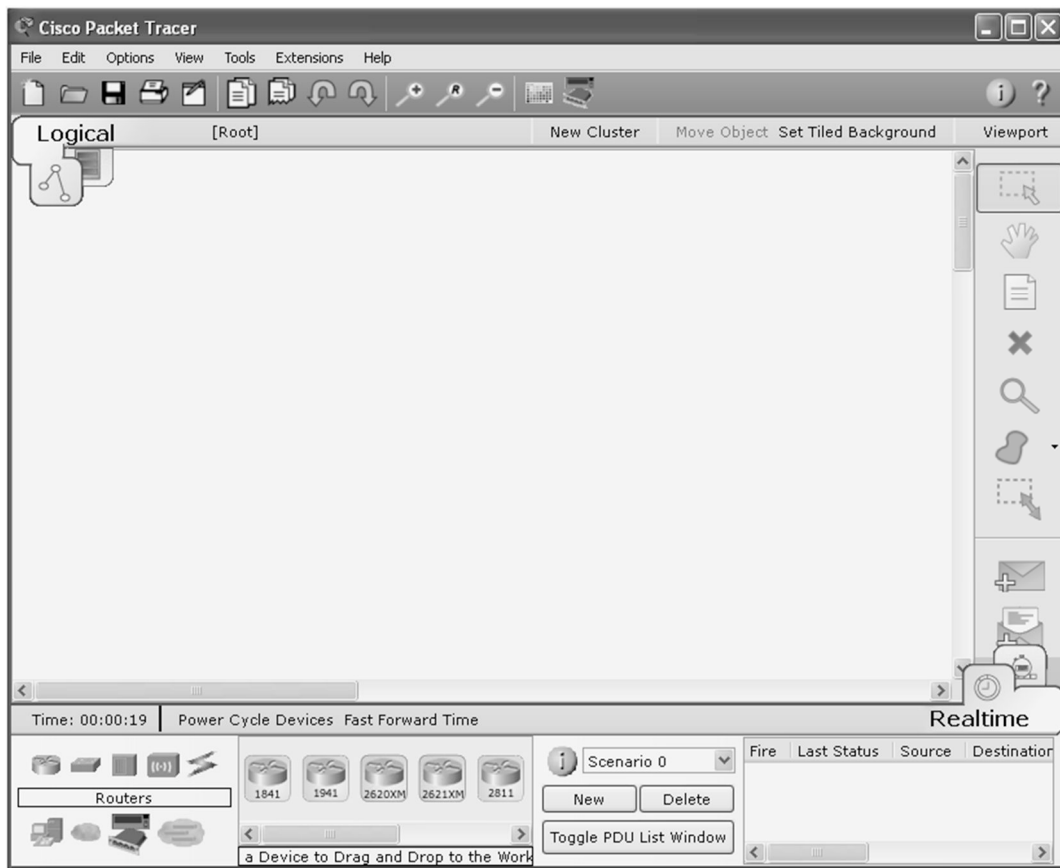


Рис. 1.1.

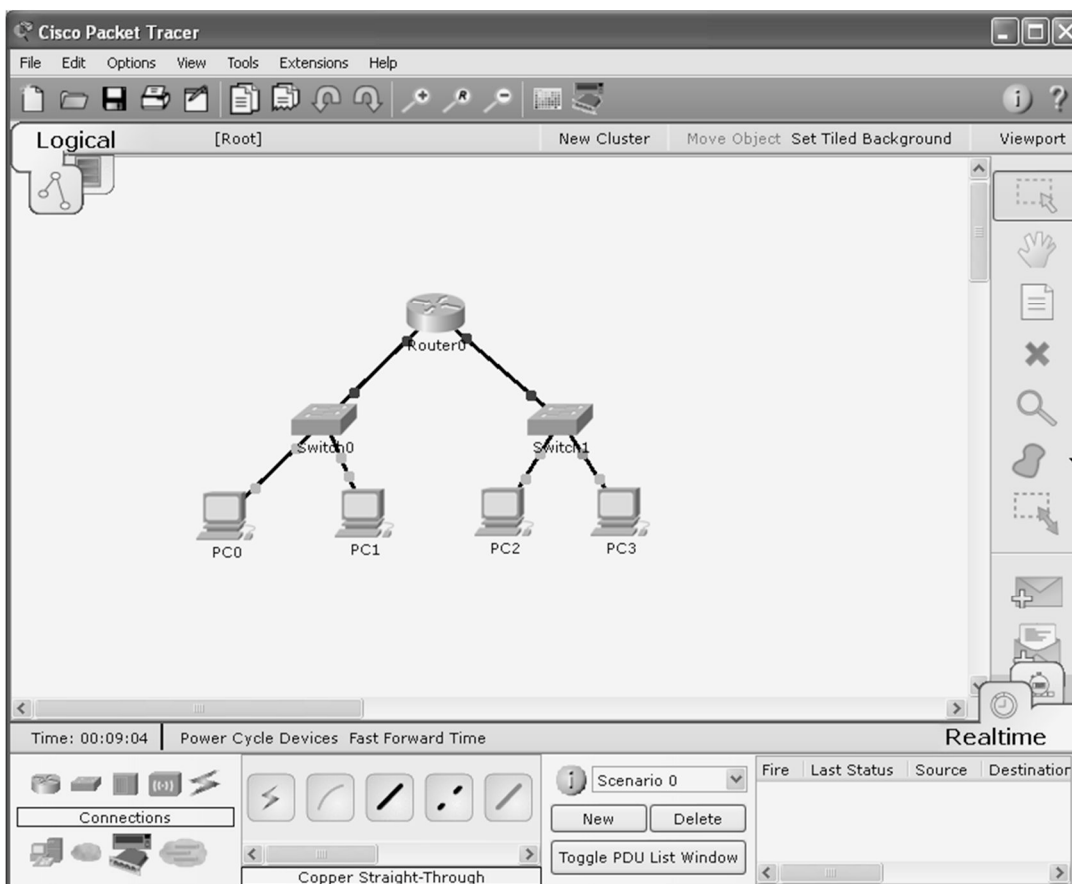


Рис. 1.2.

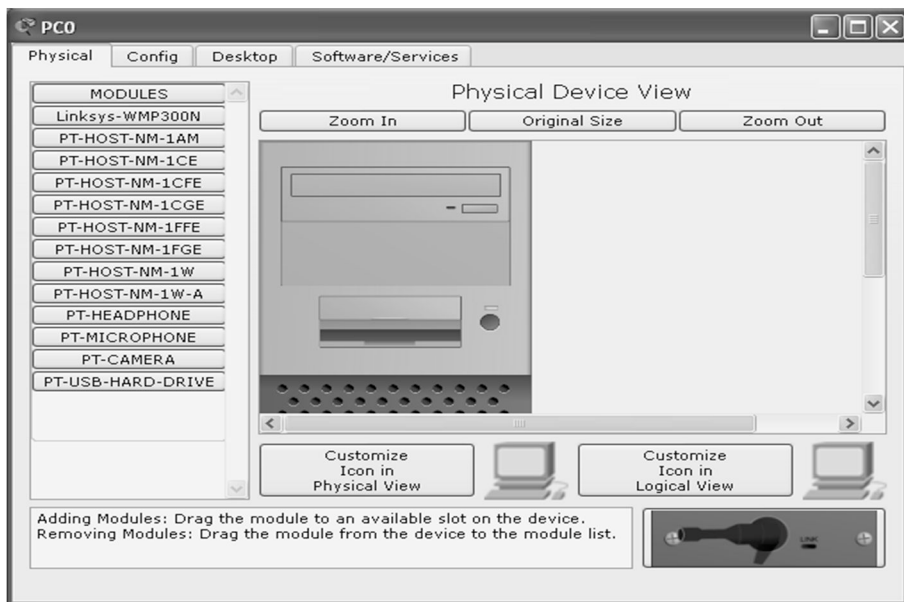


Рис. 1.3.

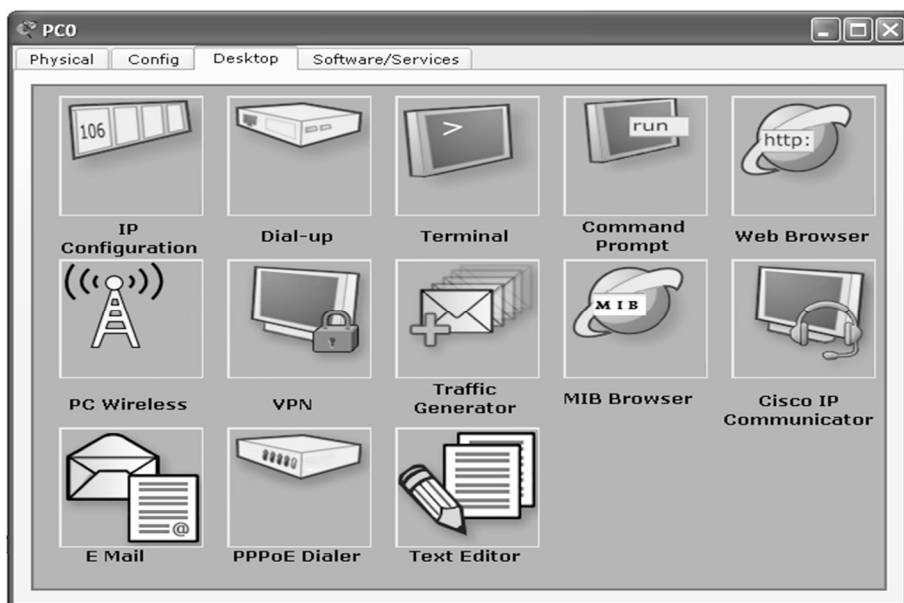


Рис. 1.4.

```

Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection: (default port)
Link-local IPv6 Address.....: FE80::250:FFF:FE37:AAA1
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

PC>

```

Рис. 1.5.

9. Вновь проверьте конфигурации всех конечных устройств (ipconfig). Запишите в отчет. Прокомментируйте изменения.
10. Войдите в режим конфигурирования маршрутизатора, для чего нужно «кликните» маршрутизатор и в верхней строке выберите режим конфигурирования с консоли CLI (рис. 1.7).

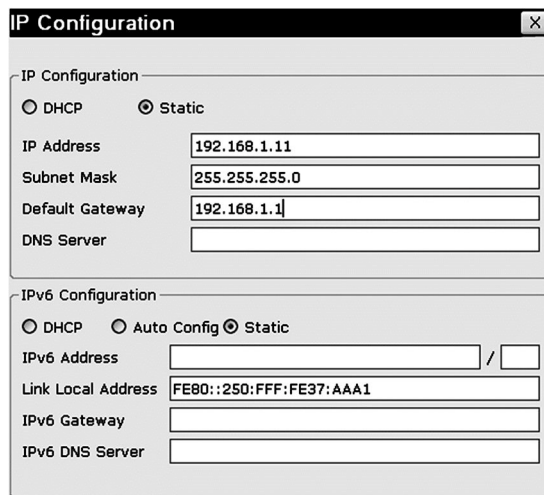


Рис. 1.6.

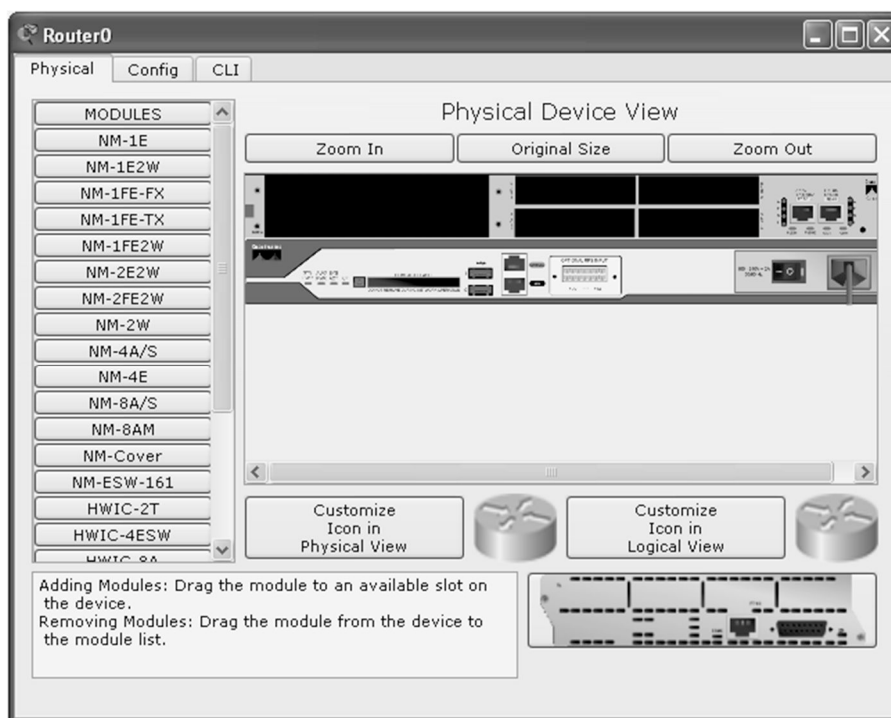


Рис. 1.7.

11. После начальной загрузки маршрутизатора операционная система предложит продолжить конфигурирование в диалоговом режиме (Continue with configuration dialog? [yes/no]:). От диалогового режима следует отказаться, набрав на клавиатуре **no** или **n** (на английском языке), и произвести «ввод» дважды (рис. 1.8). При этом маршрутизатор переходит в пользовательский режим конфигурирования со следующим приглашением:

```
Router>
```

12. Из пользовательского режима можно перейти в привилегированный, набрав команду:

```
Router>enable
Router#
```

13. Из привилегированного режима следует посмотреть текущую конфигурацию маршрутизатора (running configuration) по команде

```
Router#show running-config
или сокращенно
Router#sh run
```

14. Для дальнейшего конфигурирования перевести маршрутизатор в режим глобальной конфигурации по команде configure terminal или сокращенно

```
Router#conf t
Router(config)#
```

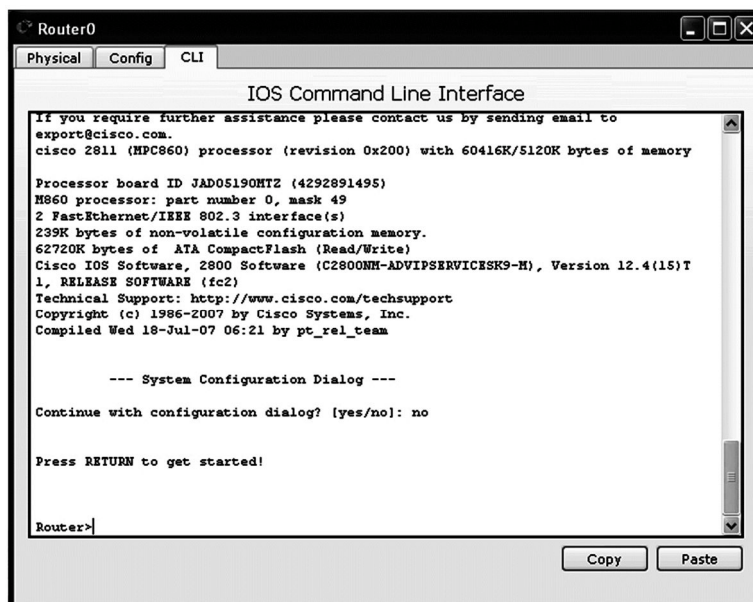


Рис. 1.8.

15. Следующая команда задает имя маршрутизатора:

```
Router(config)#hostname R-A
R-A(config)#
```

Обратите внимание, что команды вступают в действие сразу после ввода.

Сконфигурируйте интерфейсы F0/0, F0/1 маршрутизатора. Используйте адреса F0/0 – 192.168.1.1/24; F0/1 – 192.168.2.1/24. Например:

```
R-A(config)#interface fastethernet 0/0
```

При этом маршрутизатор переходит в режим детального (специфического) конфигурирования с приглашением R-A(config-if)#

```
R-A(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
R-A(config-if)#no shutdown
```

Команда interface fastethernet 0/0 может быть записана в сокращенной форме int f0/0, а команда ip address 192.168.1.1 255.255.255.0 – в виде ip add 192.168.1.1 255.255.255.0.

Аналогично выполнить конфигурацию для F0/1.

16. Посмотрите и запишите в отчет текущую конфигурацию маршрутизатора по команде:

```
R-A#show running-config
```

или сокращенно R-A#sh run

Переход из режима детального конфигурирования в привилегированный режим производится по команде str z или последовательно ввести две команды exit.

Прокомментируйте изменения в текущей конфигурации.

17. Выполните команду show ip interface brief в привилегированном режиме. Какая информация получена? Запишите в отчет.

18. Выполните команду show interfaces. Прокомментируйте результат.

19. Выполните команду ipconfig на своем компьютере. Прокомментируйте результат.

20. Проверьте работоспособность сети, используя команды ping, traceroute, для чего выполните команды ping, tracert, tracertout поочередно со всех устройств на все оставшиеся. Команда tracert выполняется с конечных узлов, команда traceroute – из маршрутизатора. Изучите параметры, отображаемые указанными командами. Результаты прокомментируйте.

21. Выполните команду ping 127.0.0.1. Что проверяется по этой команде? Объясните результат.

22. По команде show ip route посмотрите сети, к которым имеются маршруты. Запишите в отчет.

23. Измените имя маршрутизатора. Посмотрите конфигурацию маршрутизатора по команде sh run.

24. Не сохраняя текущую конфигурацию, введите команду reload из привилегированного режима. Посмотрите конфигурацию. Объясните что произошло.

25. В ряде случаев требуется удалить конфигурацию startup-config, что реализуется по команде: Router_A#erase startup-config. Команду нужно использовать с осторожностью!!!

7. Контрольные вопросы:

1. Каков начальный режим конфигурирования при работе через интерфейс командной строки CLI?
2. Какие режимы конфигурирования используются в маршрутизаторах и коммутаторах, какие параметры задаются в каждом из них?

3. Какие символы можно использовать в именах устройств?
4. В каких случаях выполняется команда перезагрузки reload?
5. По какой команде проводится сохранение текущей конфигурации? Где оно сохраняется?
6. Как удалить стартовую конфигурацию?
7. Какие команды используются для конфигурирования адресной информации маршрутизатора?
8. В каком состоянии по умолчанию находятся интерфейсы маршрутизатора? Как их включить?
9. Что такое шлюз по умолчанию? Как его сконфигурировать?
10. По каким командам можно посмотреть адресную информацию компьютера?
11. Что проверяется по команде ping 127.0.0.1?

Время на выполнение лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: ПГУТИ, д.т.н., профессор Васин Н.Н., e-mail: vasin@psati.ru, тел. (846) 332-08-05

Образовательная программа: 10.05.02 Информационная безопасность телекоммуникационных систем, Защита информации в системах связи и управления.

Дисциплина: Сети и системы передачи информации, Технологии пакетной коммутации.

Лабораторная работа. **Конфигурирование паролей маршрутизаторов**

1. Учебные цели:

- Приобрести знания об организации безопасности маршрутизаторов.
- Отработать навыки конфигурирования паролей маршрутизаторов.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

- Уметь конфигурировать пароли, знать возможности восстановления утраченных паролей
- Владеть навыками конфигурирования и проверки работоспособности реальных и виртуальных устройств симулятора.

3. Перечень материально-технического обеспечения:

Компьютерный класс, лаборатория сетей пакетной коммутации.

Лабораторное оборудование и программное обеспечение: Маршрутизаторы Cisco 2811, коммутаторы Catalyst 2600, компьютеры, симулятор Packet Tracer.

4. Задание на исследование



Конфигурирование паролей маршрутизаторов

5. Краткие теоретические сведения

1. Технологии пакетной коммутации : учебник / Н.Н. Васин. – М. : ИНТУИТ, 2017. С. 34–41.
2. Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для вузов / К.Е. Самуйлов, И.А. Шалимов, Н.Н. Васин, В.В. Василевский, Д.С. Кулябов, А.В. Королькова. – М. : Юрайт, 2016. С. 216–218.

6. Порядок выполнения лабораторной работы

Схема сети лабораторной работы приведена на рисунке 2.1, адреса – в таблице 2.1. Схема может быть реализована в Packet Tracer или на реальном оборудовании. Для связи маршрутизаторов между собой необходимо использовать последовательные (Serial) соединения S1/1, S1/2.

У маршрутизаторов 2811 последовательные (Serial) порты не установлены. Для их установки необходимо «кликнуть» маршрутизатор и выбрать Physical из верхней строки меню (рис. 2.2). Выключить () маршрутизатор. Из левой колонки меню вставить в левую пустую нишу разъема NM-4A/S (рис. 2.2), включить маршрутизатор. Соединить интерфейс S1/1 маршрутизатора А (соединение DCE – ) с интерфейсом S1/2 маршрутизатора В.

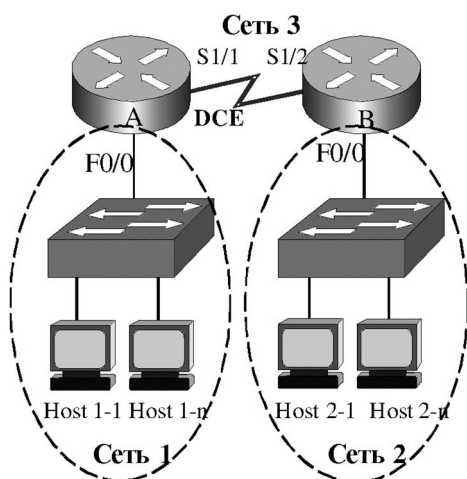


Рис. 2.1. Схема сети

Таблица 2.1 – Адреса сетей и интерфейсов маршрутизаторов

	IP-адрес сети	Интерфейсы	IP-адрес интерфейса
Сеть 1	192.168.10.0/24	F0/0	192.168.10.1
Сеть 2	192.168.20.0/24	F0/0	192.168.20.1
Сеть 3	200.30.30.0/24	S1/1	200.30.30.11
		S1/2	200.30.30.12

1. Сконфигурировать имена маршрутизаторов (R-A, R-B) и адреса Fast Ethernet интерфейсов маршрутизаторов согласно табл. 2.1. Конфигурирование интерфейсов рассмотрено в предыдущей лабораторной работе № 1.

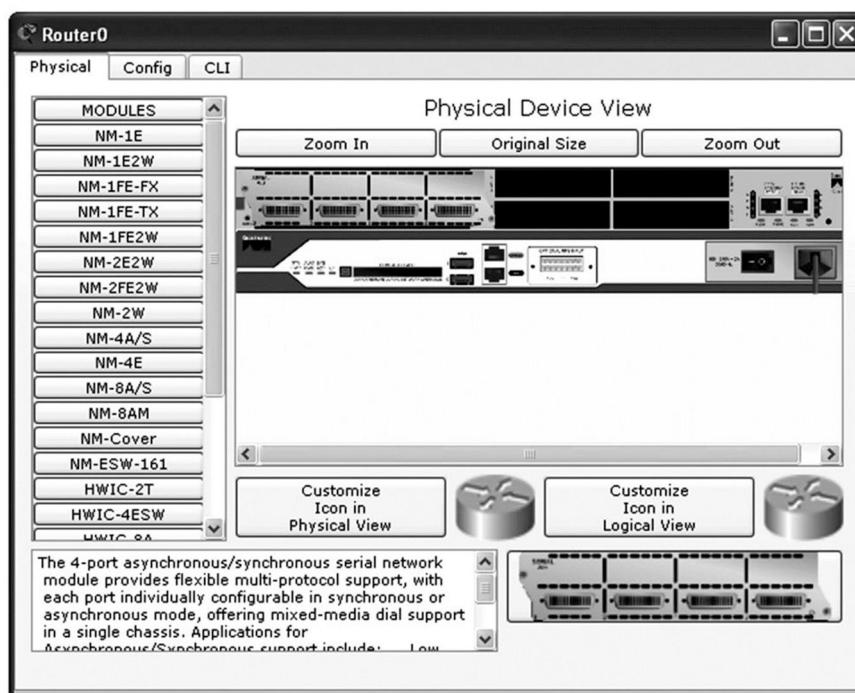


Рис. 2.2.

2. Сконфигурировать последовательные (serial) интерфейсы

```
R-A(config)#int s1/1
R-A(config-if)#ip add 200.30.30.11 255.255.255.0
R-A(config-if)#no shut
```

Для того чтобы интерфейс S1/1 стал устройством DCE необходимо выполнить команду
R-A(config-if)#clock rate 64000

- Значение 64000 задает скорость передачи данных по соединению.
Аналогично конфигурируется интерфейс S1/2, только он остается устройством DTE, поэтому команда clock rate не нужна.
3. Сконфигурировать адреса конечных узлов сети
Host 1-1 – 192.168.10.11, Host 1-n – 192.168.10.18, Host 2-1 – 192.168.20.21,
Host 2-n – 192.168.20.29, и соответствующие шлюзы по умолчанию.
Конфигурирование проводится также, как в лабораторной работе № 1.
 4. На маршрутизаторах А и В сконфигурировать протокол маршрутизации RIP. Конфигурирование протоколов маршрутизации рассматривается во второй части настоящего курса. Поэтому в данной лабораторной работе выполняется следующая последовательность команд без объяснения подробностей.
Router>enable
Router#conf t
Router(config)#hostname R-A
R-A(config)#router rip
R-A(config-router)# network 192.168.10.0
R-A(config-router)# network 200.30.30.0
По команде network – дается описание непосредственно присоединенных к маршрутизатору сетей. Аналогично конфигурируется маршрутизатор В.
 5. По командам ping, show run, show ip route проверить работоспособность сети, при необходимости отладить конфигурацию.
 6. По команде sh ip route посмотреть таблицы маршрутизации А и В.
 7. Установка пароля на консольный вход
На маршрутизаторе А сконфигурировать имя и пароль консольного порта:
Router(config)#hostname R-A
R-A(config)#line console 0
R-A(config-line)#password cis-1
R-A(config-line)#login
Проверить работоспособность пароля, для чего используя команды exit выйти из режима конфигурирования и вновь войти.
Что при этом происходит? Сравнить с маршрутизатором В, где пароль не установлен.
 8. Защита входа в привилегированный режим
На маршрутизаторе А сконфигурировать два пароля:
R-A(config)#enable password cis-2
R-A(config)#enable secret cis-3
Проверить работоспособность паролей, для чего используя команду exit выйти в пользовательский режим и вновь войти в привилегированный.
Какой пароль позволяет войти в привилегированный режим? Почему?
Посмотреть текущую конфигурацию (sh run). Прокомментировать информацию об установленных паролях. В какой форме представлены пароли?
 9. Удаленный доступ
На маршрутизаторе В сконфигурировать имя:
Router(config)#hostname R-B
R-B(config)#
По команде telnet реализовать удаленный доступ в маршрутизатор А:
R-B#telnet 192.168.10.1
Что при этом происходит? Почему?
 10. Защита удаленного доступа
На маршрутизаторе А сконфигурировать пароль на виртуальные линии:
R-A(config)#line vty 0 4
R-A(config-line)#password cis-4
R-A(config-line)#login
По команде telnet реализовать удаленный доступ с маршрутизатора В в маршрутизатор А:
R-B#telnet 192.168.10.1
Что при этом происходит? Почему?
В режиме удаленного доступа изменить имя маршрутизатора А на R_A. Завершить удаленный доступ. Проверить, что имя изменено.
 11. Реализовать удаленный доступ в маршрутизатор А с конечного узла Host 2-n.
Внести изменения в конфигурацию маршрутизатора А, используя команду:
R_A(config)#service password-encryption
Проверить текущую конфигурацию. Прокомментировать информацию об установленных паролях. В какой форме представлены пароли?
Выйти из режима удаленного доступа.
На маршрутизаторе А отменить команду service password-encryption. Прокомментировать текущую конфигурацию.

12. Сохранить текущую конфигурацию!!!
R-A#copy run start
13. Восстановление утерянного пароля
Если пользователь позабыл пароль, то пароль enable password можно восстановить, а пароль enable secret можно заменить новым. Это реализуется только при физическом доступе к маршрутизатору через консольный порт (console). При загрузке маршрутизатора необходимо обойти проверку паролей за счет изменения значения конфигурационного регистра.
14. Проверить значение конфигурационного регистра по команде:
R-A#show version...
Configuration register is 0x2102
15. Выключить и вновь включить маршрутизатор
В течение 1 минуты, когда производится проверка (тестирование) аппаратных средств маршрутизатора, нажать клавишу Ctrl+Break на клавиатуре. При этом маршрутизатор переходит в режим rommon 1>
16. Ввести команду
rommon 1>confreg 0x2142,
которая позволяет при загрузке конфигурационного файла обойти проверку паролей.
17. Следующая команда
rommon 2>reset
запустит процесс перезагрузки, который завершится вопросом:
Continue with configuration dialog? [yes/no]:
на который нужно ответить отрицательно – no.
Маршрутизатор готов к переконфигурированию!
Проверить текущую конфигурацию! Прокомментировать ее.
Router>enable
Router#show run
18. Для сохранения прежней конфигурации, хранящейся в памяти NVRAM, выполнить команду:
Router#copy start run...
R-A#
19. Проверить текущую конфигурацию!
R-A#show run
20. Внести необходимые изменения в текущую конфигурацию. Изменить пароли, запомнить их!
21. Вернуть прежнее значение конфигурационного регистра
R-A(config)#config-register 0x2102
22. Сохранить текущий конфигурационный файл
R-A#copy run start

7. Контрольные вопросы:

1. В чем заключается особенность конфигурирования последовательных интерфейсов?
2. Что задает команда clock rate?
3. Какие интерфейсы и режимы можно защищать паролями?
4. Какой пароль является более строгим enable password или enable secret?
5. Почему для удаленного доступа необходимо задавать имя устройства и пароль на вход через виртуальные линии?
6. Для чего используется команда service password-encryption?
7. Что происходит с ранее установленными паролями при отмене команды service password-encryption?
8. Почему при вводе команды no service password-encryption пароли остаются криптографированными?
9. Каково стандартное значение конфигурационного регистра? По какой команде можно его посмотреть?
10. Можно ли восстановить пароль enable secret?

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: ПГУТИ, д.т.н., профессор Васин Н.Н., e-mail: vasin@psati.ru, тел. (846) 332-08-05

Образовательная программа: 10.05.02 Информационная безопасность телекоммуникационных систем, Защита информации в системах связи и управления.

Дисциплина: Сети и системы передачи информации, Технологии пакетной коммутации.

Лабораторная работа. Формирование подсетей

1. Учебные цели:

Приобрести знания о формировании подсетей. Оработать навыки конфигурирования подсетей.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь конфигурировать адреса подсетей, владеть навыками конфигурирования и проверки работоспособности реальных и виртуальных устройств симулятора.

3. Перечень материально-технического обеспечения:

Компьютерный класс, лаборатория сетей пакетной коммутации.

Лабораторное оборудование и программное обеспечение: Маршрутизаторы Cisco 2811, коммутаторы Catalyst 2600, компьютеры, симулятор Packet Tracer.

4. Задание на исследование

Конфигурирование подсетей с использованием Packet Tracer

5. Краткие теоретические сведения

1. Технологии пакетной коммутации : Учебник / Н.Н. Васин. – М. : ИНТУИТ, 2017. С. 155–167.
2. Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для вузов / К.Е. Самуйлов, И.А. Шалимов, Н.Н. Васин, В.В. Василевский, Д.С. Кулябов, А.В. Королькова. – М. : Юрайт, 2016. С. 143–145.

5. Порядок выполнения лабораторной работы

1. С использованием Packet Tracer сформировать сеть на маршрутизаторе 2811 согласно рисунку 3.1. Поскольку маршрутизатор 2811 имеет только два интерфейса Fast Ethernet, то следует добавить еще 2 (F1/0, F1/1), установив слот NM-2FE2W в режиме Physical. Перед установкой маршрутизатор нужно выключить, после установки – включить. Зарисовать схему в отчет.

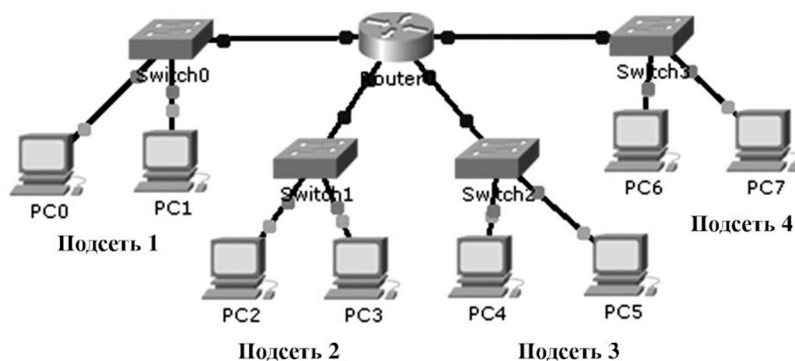


Рис. 3.1.

2. Распределить выделенное администратору адресное пространство 192.168.1.128/25 так, чтобы в Подсети 1 было 50 компьютеров, в Подсети 2 – 25 компьютеров, в Подсети 3 – должно быть максимально возможное количество компьютеров при значении маски 255.255.255.240, в Подсети 4 – должно быть максимально возможное количество компьютеров при значении префикса /29.
3. Пронумеровать на схеме в отчете адреса интерфейсов, первого и последнего компьютера в каждой подсети. Укажите адрес широковещательной рассылки в каждой подсети, запишите его в отчете.
4. Сконфигурировать все представленные на схеме Рис. 3.1 компьютеры в соответствии с требованиями п. 2. (Не забудьте шлюз по умолчанию!).
5. Проверить функционирование сети, выполнив команду ping с каждого компьютера на все остальные и на шлюз по умолчанию. Сделать вывод, записать в отчет.
6. Сконфигурировать интерфейсы маршрутизатора
7. Проверить результат по командам show running-config, show ip route. Основную информацию распечаток записать в отчет.

8. Повторить п.5.Объяснить произошедшие изменения.
9. Посчитайте, сколько неиспользованных адресов в каждой подсети.
10. Сколько всего неиспользованных адресов из выделенного адресного пространства? Как можно использовать эти адреса?

7. Контрольные вопросы:

1. Для чего производится деление сети на подсети?
2. Какое устройство производит деление сети на подсети?
3. Может ли деление сети на подсети может реализовать коммутатор?
4. Каким маскам соответствуют префиксы /20, /23, /26, /28, /30?
5. Сколько максимально подсетей может быть сформировано при использовании маски 255.255.255.224? Сколько максимально узлов в каждой?
6. В какую сеть входит узел 172.20.171.25/18? Каков широковещательный адрес в этой сети?
7. В какую сеть входит узел 172.20.171.25/20? Каков широковещательный адрес в этой сети?
8. Какую маску следует использовать для формирования 8-ми классов по 10-12 компьютеров в каждом?
9. Каковы будут адреса шлюза по умолчанию, первого и последнего компьютеров, широковещательной рассылки в сети 10.10.10.160/27?
10. Каковы будут адреса шлюза по умолчанию, первого и последнего компьютеров, широковещательной рассылки в сети 172.20.10.128/26?
11. Каков будет суммарный адрес группы подсетей 172.16.51.16/24, 172.16.51.17/24, ..., 172.16.51.23/24? Что позволяет радикально решить проблему дефицита IP-адресов?

Упражнения:

1. Рассчитайте максимальное количество узлов в подсетях 10.169.77.16/28; 172.18.190/27; 192.168.55.112/29.
2. Для выделенного диапазона адресов 172.16.10.0/24 сформируйте 10 подсетей по 8 – 14 компьютеров в каждой. Какова будет сетевая маска?
3. Для выделенного адреса 10.1.5.0/24 сформируйте 2 подсети по 50–60 компьютеров, 2 подсети по 25–30 компьютеров, 2 подсети по 10–12 компьютеров, 2 подсети по 5–6 компьютеров, остальные адреса использовать для адресации соединений «точка-точка».
4. Укажите агрегированный адрес группы из четырех подсетей: 172.16.16.0/24, 172.16.17.0/24, 172.16.18.0/24, 172.16.19.0/24.

Время на выполнение лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: ПГУТИ, д.т.н., профессор Васин Н.Н., e-mail: vasin@psati.ru, тел. (846) 332-08-05

Образовательная программа: 10.05.02 Информационная безопасность телекоммуникационных систем, Защита информации в системах связи и управления.

Дисциплина: Сети и системы передачи информации, Технологии пакетной коммутации.

Лабораторная работа. **Конфигурирование адресов IPv6**

1. Учебные цели:

- Приобрести знания об адресации IPv6.
- Отработать навыки конфигурирования адресов узлов и сетей IPv6.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

Уметь конфигурировать адреса IPv6, владеть навыками конфигурирования и проверки реальных устройств и виртуальных устройств симулятора Packet Tracer.

3. Перечень материально-технического обеспечения:

Компьютерный класс, лаборатория сетей пакетной коммутации.

Лабораторное оборудование и программное обеспечение: Маршрутизаторы Cisco 2811, коммутаторы Catalyst 2600, компьютеры, симулятор Packet Tracer.

4. Задание на исследование

Конфигурирование адресов узлов и сетей IP

5. Краткие теоретические сведения

1. Технологии пакетной коммутации : Учебник / Н.Н. Васин. – М. : ИНТУИТ, 2017. С. 137–149.
2. Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для вузов / К.Е. Самуйлов, И.А. Шалимов, Н.Н. Васин, В.В. Василевский, Д.С. Кулябов, А.В. Королькова. – М. : Юрайт, 2016. С. 145–149.

6. Порядок выполнения лабораторной работы

1. В среде Packet Tracer сформировать сеть (рис. 4.1), используя маршрутизатор 2911. Схему сети зарисовать в отчет.
2. Поскольку маршрутизатор 2911 не имеет последовательных (Serial) интерфейсов, то необходимо установить слот HWIC-2T. Установка слотов последовательных интерфейсов было рассмотрено в лаб. работе № 2.

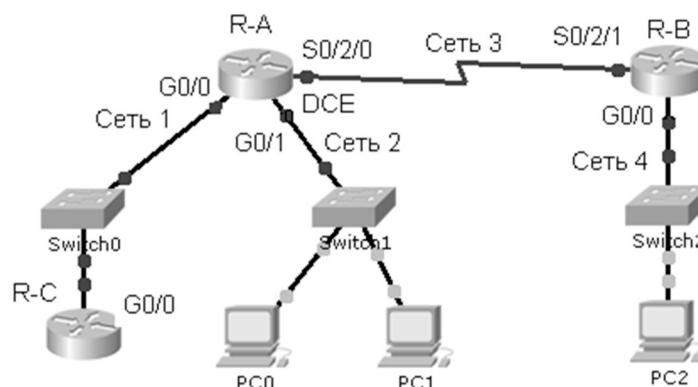


Рис. 4.1.Схема сети

3. Задать префикс глобальной маршрутизации 2001:db8:a/48, сети 1, 2, 3, 4.
4. На схеме сети записать все адреса интерфейсов и компьютеров.
5. Сконфигурировать интерфейсы маршрутизаторов, например R-B:
R-B(config)#int g0/0
R-Bconfig-if#ipv6 add 2001:db8:a:4::1/64
R-Bconfig-if#no shut
R-B(config-if)#int s0/02/1
R-B(config-if)#ipv6 add 2001:db8:a:3::1/64
R-B(config-if)#clock rate 64000
R-B(config-if)#no shut
6. Проверить конфигурацию по команде show run. Записать в отчет.
7. Аналогично сконфигурировать интерфейсы маршрутизаторов А и С.
8. Проверить конфигурацию по команде show run. Записать в отчет.
9. Выполнить команду sh ipv6 route на всех маршрутизаторах. Объяснить содержимое таблиц маршрутизации. Записать в отчет.
10. Сконфигурировать адреса компьютера PC2.
11. Проверить адресную информацию по командам ipv6config, ipconfig. Объяснить результаты и записать в отчет.
12. «Пропинговать» шлюз по умолчанию.
13. Из маршрутизатора «пропинговать» локальный и глобальный адреса компьютера. Прокомментировать результат.
14. Сконфигурировать адреса компьютера PC0.
15. Сконфигурировать адреса компьютера PC1.
16. Из маршрутизатора А прозвонить все доступные устройства. Результаты прокомментировать и записать в отчет.
17. Изменить локальные адреса интерфейсов маршрутизаторов А, В, С, по Вашему усмотрению, используя команду, например с адресом FE80::1 или любым другим: ipv6 add fe80::1 link-local в режиме конфигурирования интерфейсов.
18. После изменений выполнить команду sh ipv6 route на всех маршрутизаторах. Объяснить содержимое таблиц маршрутизации.
19. Записать в отчет.

7. Контрольные вопросы:

1. Что позволит радикально решить проблему дефицита IP-адресов?
2. Сколько двоичных разрядов содержат логические адреса в IPv6-сетях?
3. Как представлены адреса версии IPv6?
4. Какие типы индивидуальных адресов используются в IPv6-сетях?
5. Каковы три составляющих индивидуального глобального адреса?
6. Из какого диапазона назначаются локальные индивидуальные адреса канала? Для чего они нужны?
7. Какую команду необходимо использовать, чтобы маршрутизатор начал функционировать в режиме IPv6?
8. Для чего необходим протокол ICMPv6? Какие сообщения он передает?
9. Приведите пример адреса IPv6, зарезервированного для использования в документации и в учебных целях. Объясните назначение каждого блока.
10. Приведите пример адреса IPv6, идентификатор интерфейса которого создан с использованием механизма EUI-64.
11. В среде Packet Tracer смоделируйте нижеприведенную схему сети.

Время на выполнение лабораторной работы – 2 часа.

Образовательная организация, авторы, эл. почта: ПГУТИ, д.т.н., профессор Васин Н.Н., e-mail: vasin@psati.ru, тел. (846) 332-08-05

Образовательная программа: 10.05.02 Информационная безопасность телекоммуникационных систем, Защита информации в системах связи и управления.

Дисциплина: Сети и системы передачи информации, Технологии пакетной коммутации.

Лабораторная работа. **Конфигурирование статической маршрутизации**

1. Учебные цели:

- Приобрести знания о статической маршрутизации.
- Отработать навыки конфигурирования статических маршрутов.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

- Знать принципы статической маршрутизации.
- Владеть навыками конфигурирования статической маршрутизации и проверки реальных устройств и виртуальных устройств симулятора Packet Tracer.

3. Перечень материально-технического обеспечения:

Компьютерный класс, лаборатория сетей пакетной коммутации.

Лабораторное оборудование и программное обеспечение: Маршрутизаторы Cisco 2811, коммутаторы Catalyst 2600, компьютеры, симулятор Packet Tracer.

4. Задание на исследование

Конфигурирование статических маршрутов

5. Краткие теоретические сведения:

1. Технологии пакетной коммутации : Учебник / Н.Н. Васин. – М. : ИНТУИТ, 2017. С. 213–229.
2. Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для вузов / К.Е. Самуйлов, И.А. Шалимов, Н.Н. Васин, В.В. Василевский, Д.С. Кулябов, А.В. Королькова. – М. : Юрайт, 2016. С. 165–168.

6. Порядок выполнения лабораторной работы

1. С использованием Packet Tracer сформируйте схему сети лабораторной работы (рис. 5.1). Используйте маршрутизаторы серии 2911, коммутаторы – серии 2960. Установите в каждый маршрутизатор последовательные интерфейсы HWIC-2T (serial 0/3/0 и serial 0/3/1). Зарисуйте схему в отчет.
2. Сконфигурируйте имена всех маршрутизаторов, например:
Router(config)#hostname R-A
R-A(config)#

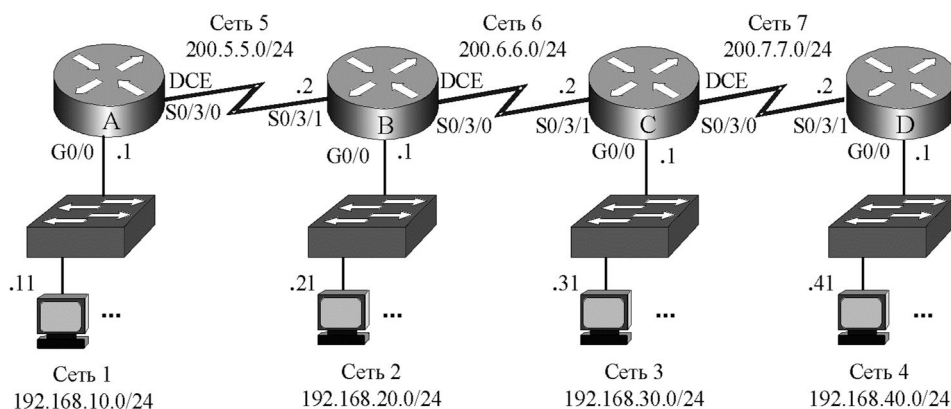


Рис. 5.1. Схема сети IPv4

3. Сконфигурируйте адреса всех задействованных интерфейсов маршрутизаторов в соответствии с заданными адресами схемы сети. Активируйте интерфейсы.
4. Проведите верификацию (проверку) конфигурации всех интерфейсов всех маршрутизаторов по командам `show ip route`, `show running-config`, `show ip interface brief`. Основные параметры запишите в отчет.
5. Каждому оконечному устройству (компьютеру) назначьте индивидуальный IP-адрес, сетевую маску и шлюз по умолчанию в соответствии со схемой сети (рис. 5.1).
6. Чтобы сконфигурировать статическую маршрутизацию администратор должен задать маршруты ко всем удаленным сетям назначения, которые прямо не присоединены к конфигурируемому маршрутизатору. Для конфигурирования статической маршрутизации используется команда `ip route`, которая содержит три параметра:
 - адрес сети назначения,
 - сетевую маску
 - адрес следующего перехода на пути к адресату (шлюз) или выходной интерфейс конфигурируемого маршрутизатора.
7. С использованием адреса следующего перехода сконфигурируйте статическую маршрутизацию на всех маршрутизаторах. Например, к маршрутизатору R-B (рис. 5.1) прямо присоединены три сети (сеть 2 – 192.168.20.0, сеть 5 – 200.5.5.0, сеть 6 – 200.6.6.0), поэтому нужно проложить маршруты к оставшимся четырем сетям (к сети 1 – 192.168.10.0, к сети 3 – 192.168.30.0, к сети 4 – 192.168.40.0, к сети 7 – 200.7.7.0):

```
R-B(config)#ip route 192.168.10.0 255.255.255.0 200.5.5.1
R-B(config)#ip route 192.168.30.0 255.255.255.0 200.6.6.2
R-B(config)#ip route 192.168.40.0 255.255.255.0 200.6.6.2
R-B(config)#ip route 200.7.7.0 255.255.255.0 200.6.6.2
```
8. Проведите верификацию (проверку) конфигурации всех маршрутизаторов по командам `show ip route`, `show running-config`. Сравните с результатами предыдущей проверки. Запишите в отчет таблицу маршрутизации. Результаты покажите преподавателю.
9. Прокомментируйте все строки таблиц маршрутизации всех маршрутизаторов. Объяснить все символы и параметры.
10. Проверьте работоспособность сети с использованием команд `ping` и `tracert`, выполняемых с конечных узлов. Результаты покажите преподавателю.
11. Проверьте работоспособность сети с использованием команд `ping` и `tracert`, выполняемых на маршрутизаторах. Результаты покажите преподавателю.
12. Конфигурирование статической маршрутизации по умолчанию
13. Удалите все статические маршруты на тупиковом маршрутизаторе R-A, например:

```
R-A(config)#no ip route 192.168.20.0 255.255.255.0 200.5.5.2
```
14. Проведите проверку конфигурации маршрутизатора R-A по командам `show ip route`, `show running-config`.
15. Сконфигурируйте статическую маршрутизацию по умолчанию

```
R-A(config)#ip route 0.0.0.0 0.0.0.0 200.5.5.2
```
16. Проведите проверку конфигурации маршрутизатора R-A по командам `show ip route`, `show running-config`. Результаты покажите преподавателю.
17. Проверьте работоспособность сети с использованием команд `ping` и `tracert`, выполняемых с конечных узлов. Результаты покажите преподавателю.
18. Конфигурирование статической маршрутизации с использованием выходного интерфейса
19. Удалите все статические маршруты на всех маршрутизаторах сети (рис. 1.1).

20. Проведите проверку конфигурации маршрутизаторов по команде `show ip route`.
21. Сконфигурируйте статическую маршрутизацию на всех маршрутизаторах с использованием выходного интерфейса. Например, на маршрутизаторе R-B:
- ```
R-B(config)#ip route 192.168.10.0 255.255.255.0 s0/3/1
R-B(config)#ip route 192.168.30.0 255.255.255.0 s0/3/0
R-B(config)#ip route 192.168.40.0 255.255.255.0 s0/3/0
R-B(config)#ip route 200.7.7.0 255.255.255.0 s0/3/0
```
22. Проведите проверку конфигурации всех маршрутизаторов по командам `show ip route`, `show running-config`.
- Запишите в отчет таблицу маршрутизации. Сравните с ранее записанной в отчет таблицей. Объясните, в чем преимущество этого способа маршрутизации.
- Какой метод маршрутизации используется в современных сетях?
- Конфигурирование статической маршрутизации в сетях IPv6
23. Сформируйте схему сети лабораторной работы (рис. 5.2). Используйте маршрутизаторы серии 2911, коммутаторы – серии 2960. Зарисуйте схему в отчет.

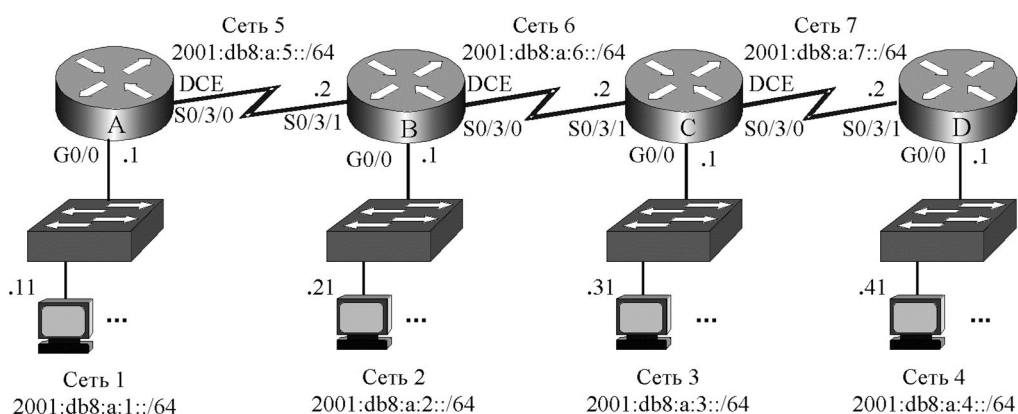


Рис. 5.2. Схема сети IPv6

24. Сконфигурируйте имена всех маршрутизаторов.
25. Сконфигурируйте адреса всех задействованных интерфейсов маршрутизаторов в соответствии с заданными адресами схемы сети. Активируйте интерфейсы.
26. Измените автоматически назначенные локальные адреса интерфейсов на более короткие, например:
- ```
Router(config-if)#ipv6 add fe80::1 link-local.
```
27. Проведите верификацию (проверку) конфигурации всех интерфейсов всех маршрутизаторов по командам `show ipv6 route`, `show running-config`, `show ipv6 interface brief`. Основные параметры запишите в отчет. Прокомментируйте записи распечаток.
- Результаты покажите преподавателю.
28. Для включения маршрутизации IPv6 на каждом маршрутизаторе выполните команду
- ```
Router(config)#ipv6 unicast-routing
```
29. Каждому оконечному устройству (компьютеру) назначьте индивидуальный IP-адрес, сетевую маску и шлюз по умолчанию в соответствии со схемой сети (рис. 5.2).
30. С использованием адреса следующего перехода сконфигурируйте статическую маршрутизацию на всех маршрутизаторах.
31. Проведите проверку конфигурации всех маршрутизаторов по командам `show ipv6 route`, `show running-config`. Запишите таблицу маршрутизации в отчет. Сравните с ранее записанной в отчет таблицей.
- Маршрутизация с использованием выходного интерфейса
32. Удалите все статические маршруты на всех маршрутизаторах сети.
33. Проведите проверку конфигурации маршрутизаторов по команде `show ipv6 route`.
34. Сконфигурируйте статическую маршрутизацию на всех маршрутизаторах с использованием выходного интерфейса.
35. Проведите проверку конфигурации всех маршрутизаторов по командам `show ipv6 route`, `show running-config`. Запишите таблицу маршрутизации в отчет. Сравните с ранее записанной в отчет таблицей.
- Маршрутизация по умолчанию
36. Удалите все статические маршруты на тупиковом маршрутизаторе R-A.
37. Проведите проверку конфигурации маршрутизатора R-A по командам `show ipv6 route`, `show running-config`.
38. Сконфигурируйте на R-A статическую маршрутизацию по умолчанию



39. Проведите проверку конфигурации маршрутизатора R-A по командам `show ipv6 route`, `show running-config`. Запишите в отчет таблицу маршрутизации.
40. Результаты покажите преподавателю.
41. Проверьте работоспособность сети с использованием команд `ping` и `tracert`, выполняемых с конечных узлов. Результаты покажите преподавателю.

#### **7. Контрольные вопросы:**

1. Кто создает статическую маршрутизацию?
2. Какие команды используются для создания статической маршрутизации?
3. Каков формат команды конфигурирования статической маршрутизации?
4. Каков формат команды конфигурирования статической маршрутизации с использованием выходного интерфейса?
5. Каков формат команды конфигурирования статической маршрутизации по умолчанию?
6. Каким символом помечаются непосредственно присоединенные к маршрутизатору сети?
7. Каким символом помечаются маршруты, созданные администратором?
8. По какой команде можно посмотреть таблицу маршрутизации?
9. Какие команды используются для проверки и отладки конфигурации?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** ПГУТИ, д.т.н., профессор Васин Н.Н., e-mail: vasin@psati.ru, тел. (846) 332-08-05

---

**Образовательная программа:** 10.05.02 Информационная безопасность телекоммуникационных систем, Защита информации в системах связи и управления.

**Дисциплина:** Сети и системы передачи информации, Технологии пакетной коммутации.

### **Лабораторная работа.** **Конфигурирование динамической маршрутизации**

#### **1. Учебные цели:**

- Приобрести знания о динамической маршрутизации.
- Отработать навыки конфигурирования динамической маршрутизации.

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- Знать характеристики протоколов маршрутизации RIP, EIGRP.
- Владеть навыками конфигурирования протоколов RIP, EIGRP и проверки реальных устройств и виртуальных устройств симулятора Packet Tracer.

#### **3. Перечень материально-технического обеспечения:**

Компьютерный класс, лаборатория сетей пакетной коммутации.

**Лабораторное оборудование и программное обеспечение:** Маршрутизаторы Cisco 2811, коммутаторы Catalyst 2600, компьютеры, симулятор Packet Tracer.

#### **4. Задание на исследование**

Конфигурирование динамической маршрутизации

#### **5. Краткие теоретические сведения**

1. Технологии пакетной коммутации : учебник / Н.Н. Васин. – М. : ИНТУИТ, 2017. С. 230–260.
2. Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для вузов / К.Е. Самуйлов, И.А. Шалимов, Н.Н. Васин, В.В. Василевский, Д.С. Кулябов, А.В. Королькова. – М. : Юрайт, 2016. С. 168–176.

#### **6. Порядок выполнения лабораторной работы**

1. С использованием Packet Tracer сформируйте схему сети лабораторной работы (рис. 6.1). Используйте маршрутизаторы серии 2911, коммутаторы – серии 2960. Зарисуйте схему в отчет.

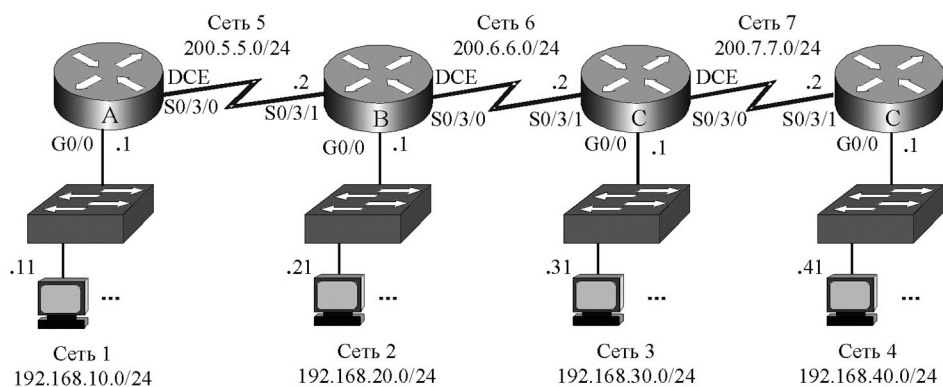


Рис. 6.1. Схема сети

2. Сконфигурируйте имена всех маршрутизаторов, например:  

```
Router(config)#hostname R-A
R-A(config)#
```
3. Сконфигурируйте адреса всех задействованных в схеме интерфейсов маршрутизаторов в соответствии с заданными адресами сети. Активируйте интерфейсы.
4. Проведите верификацию (проверку) конфигурации всех интерфейсов всех маршрутизаторов по командам `show ip route`, `show running-config`, `show ip interface brief`. Основные параметры запишите в отчет. Результаты покажите преподавателю.
5. Каждому оконечному устройству (компьютеру) назначьте индивидуальный IP-адрес, сетевую маску и шлюз по умолчанию в соответствии со схемой сети Рис. 6.1.
6. Чтобы сконфигурировать динамическую маршрутизацию необходимо задать протокол (`router rip`) и формальное описание прямо присоединенных сетей (`network`).  
 Например, для маршрутизатора R-B последовательность команд будет следующая:  

```
R-B(config)#router rip
R-B(config-router)#network 192.168.20.0
R-B(config-router)#network 200.5.5.0
R-B(config-router)#network 200.6.6.0
```

 Описание прямо присоединенных сетей проводится в режиме детального (специфического) конфигурирования.
7. Сконфигурируйте протокол RIP на остальных маршрутизаторах  
 Проведите верификацию (проверку) конфигурации всех маршрутизаторов по командам `show ip route`, `show running-config`. Запишите в отчет таблицу маршрутизации. Сравните с результатами предыдущей проверки.  
 Результаты покажите преподавателю.  
 Объясните, как формируется метрика.
8. Проверьте работоспособность сети с использованием команд `ping` и `tracert`, выполняемых с конечных узлов. Результаты покажите преподавателю.
9. Проверьте работоспособность сети с использованием команд `ping` и `tracert`, выполняемых на маршрутизаторах. Результаты покажите преподавателю.

#### Конфигурирование протокола RIP2

10. Сформируйте схему сети лабораторной работы (рис. 6.2). Используйте маршрутизаторы серии 2911, коммутаторы – серии 2960. Зарисуйте схему.

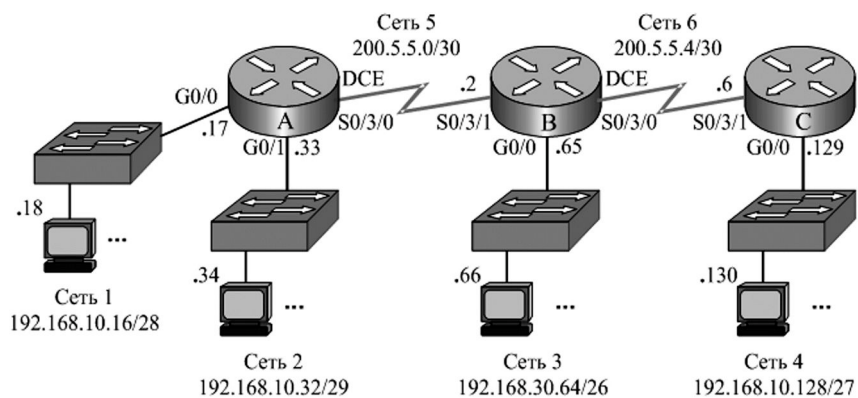


Рис. 6.2. Схема сети лабораторной работы

11. Сконфигурируйте имена маршрутизаторов, адреса всех задействованных в схеме интерфейсов в соответствии с заданными адресами сети Рис. 6.2.
12. Проведите верификацию конфигурации всех маршрутизаторов по командам `show ip route`, `show running-config`, `show ip interface brief`. Основные параметры запишите в отчет.
13. Каждому оконечному устройству (компьютеру) назначьте индивидуальный IP-адрес, сетевую маску и шлюз по умолчанию в соответствии со схемой сети Рис. 6.2.
14. Проведите верификацию конфигурации всех маршрутизаторов по командам `show ip route`, `show running-config`, `show ip interface brief`. Основные параметры запишите в отчет.
15. Каждому оконечному устройству (компьютеру) назначьте индивидуальный IP-адрес, сетевую маску и шлюз по умолчанию в соответствии со схемой сети Рис. 6.2.
16. Сконфигурируйте протокол RIP на всех маршрутизаторах.  
Проведите верификацию (проверку) конфигурации всех маршрутизаторов по командам `show ip route`, `show running-config`. Запишите в отчет таблицы маршрутизации.  
Проверьте работоспособность сети с использованием команд `ping`. Результаты объясните преподавателю.  
На всех маршрутизаторах измените протокол маршрутизации на RIP2, и отмените автоматическое суммирование маршрутов, например:
 

```
R-B(config)#router rip
R-B(config-router)#version 2
R-B(config-router)#network 192.168.30.64
R-B(config-router)#network 200.5.5.0
R-B(config-router)#network 200.5.5.4
R-B(config-router)#no auto-summary
```
17. Проведите верификацию конфигурации всех маршрутизаторов по командам `show ip route`, `show running-config`. Прокомментируйте и запишите в отчет основные параметры.
18. Проверьте работоспособность сети с использованием команд `ping`, выполняемых с конечных узлов и маршрутизаторов. Результаты объясните преподавателю.

### Конфигурирование протокола EIGRP

19. Для изучения протокола EIGRP используется схема сети Рис. 6.2.
20. На всех маршрутизаторах отмените протокол маршрутизации RIP2. Проведите верификацию конфигурации всех маршрутизаторов по командам `show ip route`, `show running-config`, `show ip interface brief`.
21. На всех маршрутизаторах сконфигурируйте протокол маршрутизации EIGRP и отмените автоматическое суммирование маршрутов, например:
 

```
R-B(config)#router eigrp 20
R-B(config-router)#network 192.168.30.64 0.0.0.63
R-B(config-router)#network 200.5.5.0 0.0.0.3
R-B(config-router)#network 200.5.5.4 0.0.0.3
R-B(config-router)#no auto-summary
```
22. Объясните, что означают числа 20, 0.0.0.63, 0.0.0.3.
23. Проведите верификацию конфигурации всех маршрутизаторов по командам `show ip route`, `show running-config`. Прокомментируйте и запишите в отчет основные параметры конфигурации.
24. Проверьте работоспособность сети с использованием команд `ping`. Результаты объясните преподавателю.

### 7. Контрольные вопросы:

1. Как формируется динамическая маршрутизация?
2. Какие команды используются для создания статической маршрутизации?
3. Каков формат команды конфигурирования статической маршрутизации?
4. Каков формат команды конфигурирования статической маршрутизации с использованием выходного интерфейса?
5. Каков формат команды конфигурирования статической маршрутизации по умолчанию?
6. Каким символом помечаются непосредственно присоединенные к маршрутизатору сети?
7. Каким символом помечаются маршруты, созданные администратором?
8. Каким символом помечаются маршруты, созданные протоколом RIP?
9. Каков формат команды конфигурирования протокола RIP?
10. По какой команде можно посмотреть таблицу маршрутизации?
11. Какие команды используются для проверки и отладки конфигурации?
12. В чем преимущество RIP2 по сравнению с RIP?
13. Какие протоколы передают, и какие не передают в своих обновлениях значения маски подсетей?
14. Каков период передачи обновлений протокола RIP, RIP2?
15. Каков период передачи пакетов Hello протокола EIGRP?
16. Какие адреса используются протоколами RIP, RIP2, EIGRP при обмене маршрутной информацией?

17. Какие таблицы создает протокол EIGRP?
18. Когда протокол EIGRP производит обмен маршрутной информацией?
19. Какая таблица содержит полную информацию о топологии сети?
20. Какие параметры учитывает метрика протокола EIGRP?
21. Какие параметры метрики протокола EIGRP учитываются по умолчанию?
22. Каковы достоинства и недостатки авто-суммирования?
23. Каков формат команд конфигурирования протокола EIGRP?
24. Какую информацию содержат таблицы топологии?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** ПГУТИ, д.т.н., профессор Васин Н.Н., e-mail: vasin@psati.ru, тел. (846) 332-08-05

---

**Образовательная программа:** 10.05.02 Информационная безопасность телекоммуникационных систем, Защита информации в системах связи и управления.

**Дисциплина:** Сети и системы передачи информации, Технологии пакетной коммутации.

### **Лабораторная работа.** **Конфигурирование протокола OSPF**

#### **1. Учебные цели:**

Приобрести знания о протоколе OSPF. Отработать навыки конфигурирования динамической маршрутизации OSPF.

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

Знать характеристики протокола маршрутизации OSPF. Владеть навыками конфигурирования протокола OSPF и проверки реальных устройств и виртуальных устройств симулятора Packet Tracer.

#### **3. Перечень материально-технического обеспечения:**

Компьютерный класс, лаборатория сетей пакетной коммутации.

**Лабораторное оборудование и программное обеспечение:** Маршрутизаторы Cisco 2811, коммутаторы Catalyst 2600, компьютеры, симулятор Packet Tracer.

#### **4. Задание на исследование**

Конфигурирования динамической маршрутизации OSPF.

#### **5. Краткие теоретические сведения**

1. Технологии пакетной коммутации : учебник / Н.Н. Васин. – М. : ИНГУИТ, 2017. С. 263–283.
2. Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для вузов / К.Е. Самуйлов, И.А. Шалимов, Н.Н. Васин, В.В. Василевский, Д.С. Кулябов, А.В. Королькова. – М. : Юрайт, 2016. С. 175–182.

#### **6. Порядок выполнения лабораторной работы**

1. С использованием Packet Tracer или реального оборудования создайте схему сети лабораторной работы (рис. 8.1). Используйте маршрутизаторы серии 2911, коммутаторы – серии 2960. Зарисуйте схему в отчет.
2. Сконфигурируйте имена всех маршрутизаторов и адреса интерфейсов в соответствии с заданными адресами схемы сети. Активируйте интерфейсы.
3. Каждому оконечному устройству (компьютеру) назначьте индивидуальный IP-адрес, сетевую маску и шлюз по умолчанию в соответствии со схемой сети (рис. 8.1).
4. На всех маршрутизаторах сконфигурируйте динамическую маршрутизацию с использованием протокола RIP.
5. Проведите верификацию всех маршрутизаторов по командам **show ip route**, **show running-config**, **show ip interface brief**. Основные параметры запишите в отчет.

Проверьте работоспособность сети с использованием команд **ping** и **tracert**. Результаты покажите преподавателю.

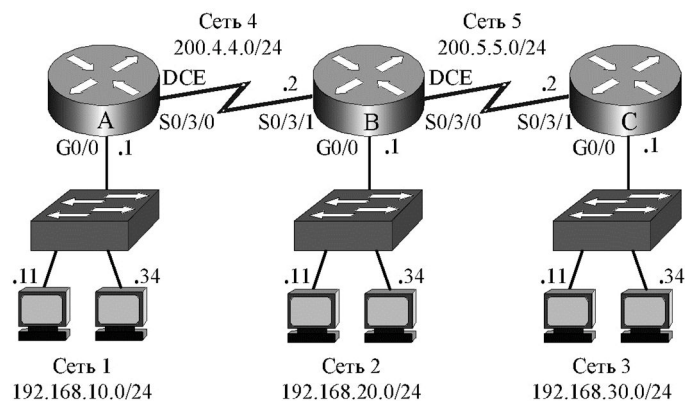


Рис. 8.1. Схема сети

### Задание 1.

Сконфигурируйте список доступа, чтобы узлы Сети 1 были доступны только узлу с адресом 192.168.20.11 Сети 2, а все остальные узлы Сети 2 и Сети 3 не имели бы доступа в Сеть 1. Список доступа следует установить на интерфейс F0/0 маршрутизатора R-A. Номер списка доступа (10) выбирается из диапазона 1 – 99. Создание и установка списка доступа производится по командам:

```
R-A(config)#access-list 10 permit 192.168.20.11
```

```
R-A(config)#int f0/0
```

```
R-A(config-if)#ip access-group 10 out
```

Проверить работоспособность списка доступа. Результаты прокомментировать преподавателю.

Удалить список.

### Задание 2.

Узлы Сети 1 должны быть доступны всем узлам Сети 2 и одному узлу Сети 3 с адресом 192.168.30.11, остальные узлы Сети 3 не должны иметь доступа. Список доступа установить на интерфейс F0/0 Router\_A.

В списке доступа необходимо использовать инверсную маску (Wildcard mask). Нулевые значения инверсной маски означают требование обработки соответствующих разрядов адреса, а единичные значения – игнорирование соответствующих разрядов адреса при функционировании списка доступа. Таким образом, маска 0.0.0.0 предписывает анализ и обработку всех разрядов адреса, т.е. в этом случае будет обрабатываться адрес каждого узла. Маска 0.0.0.255 показывает, что обрабатываться будет только сетевая часть адреса. Некоторые версии операционных систем IOS маршрутизаторов требуют в обязательном порядке использование масок WildCard при задании адресов узлов и сетей, либо расширения host при задании адресов узлов. Записи 192.168.30.11 0.0.0.0 полностью соответствует другой вариант – host 192.168.30.11, который также предписывает обрабатывать адрес только одного узла.

```
R-A(config)#access-list 11 permit 192.168.30.11 0.0.0.0
```

```
R-A(config)#access-list 11 permit 192.168.20.0 0.0.0.255
```

```
R-A(config)#int f0/0
```

```
R-A(config-if)#ip access-group 11 out
```

Проверить работоспособность списка доступа!

Удалить список.

### Задание 3.

В Сети Рис. 8.1 необходимо установить список доступа, который:

- блокирует рабочей станции 192.168.20.11 Сети 2 доступ в Сеть 1;
- блокирует рабочей станции 192.168.30.34 Сети 3 доступ в Сеть 1;

Для этого создается список доступа:

```
R-A(config)#access-list 12 deny host 192.168.20.11
```

```
R-A(config)#access-list 12 deny host 192.168.30.34
```

```
R-A(config)#access-list 12 permit any
```

```
R-A(config)#int f0/0
```

```
R-A(config-if)#ip access-group 12 out
```

Если бы отсутствовала третья строка списка доступа, то ни одна станция из других сетей не могла бы попасть в Сеть 1, поскольку в конце каждого списка неявно присутствует команда deny any – запретить все остальное.

Проверить работоспособность списка доступа! Удалить список.

#### Задание 4.

Используя исходные данные Задания 3, сформируйте список доступа в виде именованного (имя ACL):

```
R-A(config)#ip access-list standard ACL
R-A(config)#deny host 192.168.20.11
R-A(config)#deny host 192.168.30.24
R-A(config)#permit any
R-A(config)#int f0/0
R-A(config-if)#ip access-group ACL out
Проверить работоспособность списка доступа! Удалить список.
```

#### Задание 5.

На маршрутизаторе А (рис. 8.1) необходимо установить расширенный список доступа, который:

- блокирует рабочим станциям Сети 2 доступ в Сеть1 по telnet;
- разрешает рабочим станциям Сети 2 доступ в Сеть1 по другим протоколам, например, по команде ping протокола ICMP.

Предварительно сконфигурируйте пароли на маршрутизаторе А:

```
Router_A(config)#line vty 0 15
Router_A(config-line)#password cisco-1
Router_A(config-line)#login
Router_A(config)#enable secret cisco-2
```

Выполнить удаленный доступ на маршрутизатор R-A с конечного узла 192.168.20.11:

```
PC>telnet 192.168.10.1
```

...

Password:

```
R-A>ena
```

Password: (ввести пароль)

```
R-A#conf t
```

Измените конфигурацию маршрутизатора, например, измените имя:

```
R-A(config)#hostname Router_A
```

```
Router_A(config)#
```

Выполните команду:

```
PC>ping 192.168.10.1
```

Прокомментируйте результаты выполнения команд telnet и ping!

Сформируйте список доступа, блокирующий рабочим станциям Сети 2 доступ в Сеть1 по telnet и разрешающий доступ в Сеть1 по команде ping.:

```
Router_A(config)#access-list 102 deny tcp 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 eq 23
```

```
Router_A(config)#access-list 102 permit ip any any
```

```
Router_A(config)#int s0/3/0
```

```
Router_A(config-if)#ip access-group 102 in
```

Выполните удаленный доступ к маршрутизатору А (адрес 192.168.10.1) с конечного узла 192.168.20.11.

```
PC>telnet 192.168.10.1
```

```
Выполните команду PC>ping 192.168.10.1
```

Прокомментируйте результаты выполнения команд telnet и ping!

#### Списки доступа IPv6

Сформируйте схему сети лабораторной работы (рис. 7.3). Используйте маршрутизаторы серии 2911, коммутаторы – серии 2960. Зарисуйте схему.

Сконфигурируйте интерфейсы всех маршрутизаторов.

Сконфигурируйте протокол OSPFv3 на всех маршрутизаторах, например

```
R-A(config)#ipv6 unicast-routing
```

```
R-A(config)#ipv6 router ospf 1
```

```
R-A(config-rtr)#router-id 1.1.1.1
```

```
R-A(config-rtr)#int g0/0
```

```
R-A(config-if)#ipv6 ospf 1 area 0
```

```
R-A(config-if)#int s0/3/0
```

```
R-A(config-if)#ipv6 ospf 1 area 0
```

Проверьте результат конфигурирования, используя команды **show run**, **show ipv6 route**, **ping**. Результат прокомментируйте преподавателю!

### **Задание 6.**

Сформируйте список доступа IPv6, который запрещал бы всем узлам сети 2001:db8:a:3::/64 доступ в сеть 2001:db8:a:1::/64, все остальное разрешить. Список установить на интерфейсе s0/3/0 R-A.

```
R-A(config)#ipv6 access-list ACL
R-A(config-ipv6-acl)#deny ipv6 2001:db8:a:3::/64 any
R-A(config-ipv6-acl)#permit ipv6 any any
R-A(config-ipv6-acl)#int s0/3/0
R-A(config-if)#ipv6 traffic-filter ACL in
```

Проверьте результат конфигурирования, используя команды show run, show ipv6 route, show ipv6 int, show access-lists.

Проверьте функционирование списка ACL по командам ping.

Результат прокомментировать преподавателю!

### **7. Контрольные вопросы:**

1. Какую информацию содержит пакет OSPF при обновлениях?
2. Каков период передачи пакетов Hello протокола OSPF? Какие адреса при этом используются?
3. Какая таблица строится на основе обмена пакетами Hello?
4. Когда протокол OSPF производит обмен маршрутной информацией?
5. Какая база данных содержит полную информацию о топологии сети?
6. Какие параметры учитывает метрика протокола OSPF?
7. Каков формат команд конфигурирования протокола OSPF2?
8. Что позволит радикально решить проблему дефицита IP-адресов?
9. Сколько двоичных разрядов содержат логические адреса в IPv6-сетях?
10. Как представлены адреса версии IPv6?
11. Какие типы индивидуальных адресов используются в IPv6-сетях?
12. Каковы три составляющих индивидуального глобального адреса?
13. Из какого диапазона назначаются локальные индивидуальные адреса канала? Для чего они нужны?
14. Какую команду необходимо использовать, чтобы маршрутизатор начал функционировать в режиме IPv6?
15. Каков формат команд конфигурирования протокола OSPF3?
16. В чем различие конфигурирования OSPF2 и OSPF3?
17. Для чего необходим протокол ICMP? Какие сообщения он передает?
18. Приведите пример адреса IPv6, зарезервированного для использования в документации и в учебных целях. Объясните назначение каждого блока.
19. Приведите пример адреса IPv6, идентификатор интерфейса которого создан с использованием механизма EUI-64.

**Время на выполнение лабораторной работы – 2 часа.**

**Образовательная организация, авторы, эл. почта:** ПГУТИ, д.т.н., профессор Васин Н.Н., e-mail: vasin@psati.ru, тел. (846) 332-08-05

---

**Образовательная программа:** 10.05.02 Информационная безопасность телекоммуникационных систем, Защита информации в системах связи и управления.

**Дисциплина:** Сети и системы передачи информации, Технологии пакетной коммутации.

### **Лабораторная работа.** **Конфигурирование списков доступа**

#### **1. Учебные цели:**

Приобрести знания о защите сетевых устройств с помощью списков доступа. Отработать навыки конфигурирования списков доступа.

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

Знать о функционировании списков доступа для обеспечения информационной безопасности сетевых устройств, владеть навыками конфигурирования списков доступа и проверки их работоспособности на реальных устройствах и виртуальных устройств симулятора Packet Tracer.

### 3. Перечень материально-технического обеспечения:

Компьютерный класс, лаборатория сетей пакетной коммутации.

**Лабораторное оборудование и программное обеспечение:** Маршрутизаторы Cisco 2811, коммутаторы Catalyst 2600, компьютеры, симулятор Packet Tracer.

### 4. Задание на исследование

Конфигурирование списков доступа

### 5. Краткие теоретические сведения:

1. Технологии пакетной коммутации : учебник / Н.Н. Васин. – М. : ИНТУИТ, 2017. С. 288–300.
2. Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для вузов / К.Е. Самуйлов, И.А. Шалимов, Н.Н. Васин, В.В. Василевский, Д.С. Кулябов, А.В. Королькова. – М. : Юрайт, 2016. С. 220–228.

### 6. Порядок выполнения лабораторной работы (этапы)

1. С использованием Packet Tracer или реального оборудования создайте схему сети лабораторной работы (рис. 8.1). Используйте маршрутизаторы серии 2911, коммутаторы – серии 2960. Зарисуйте схему в отчет.
2. Сконфигурируйте имена всех маршрутизаторов и адреса интерфейсов в соответствии с заданными адресами схемы сети. Активируйте интерфейсы.
3. Каждому оконечному устройству (компьютеру) назначьте индивидуальный IP-адрес, сетевую маску и шлюз по умолчанию в соответствии со схемой сети (рис. 8.1).
4. На всех маршрутизаторах сконфигурируйте динамическую маршрутизацию с использованием протокола RIP.
5. Проведите верификацию всех маршрутизаторов по командам **show ip route**, **show running-config**, **show ip interface brief**. Основные параметры запишите в отчет.
6. Проверьте работоспособность сети с использованием команд **ping** и **tracert**. Результаты покажите преподавателю.

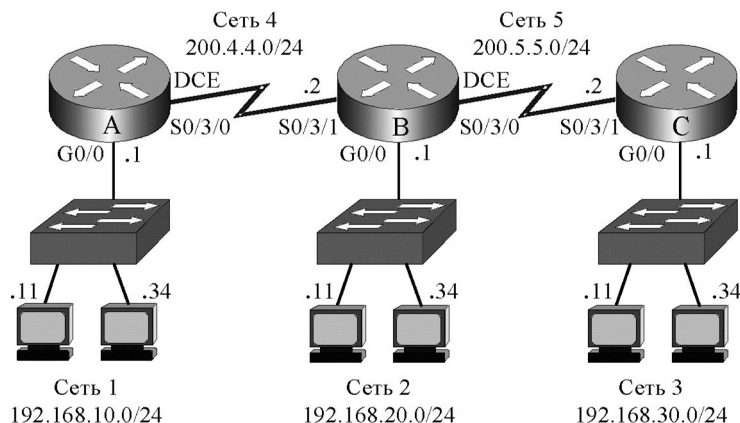


Рис. 8.1. Схема сети

#### Задание 1.

Сконфигурируйте список доступа, чтобы узлы Сети 1 были доступны только узлу с адресом 192.168.20.11 Сети 2, а все остальные узлы Сети 2 и Сети 3 не имели бы доступа в Сеть 1. Список доступа следует установить на интерфейс F0/0 маршрутизатора R-A. Номер списка доступа (10) выбирается из диапазона 1 – 99. Создание и установка списка доступа производится по командам:

```
R-A(config)#access-list 10 permit 192.168.20.11
```

```
R-A(config)#int f0/0
```

```
R-A(config-if)#ip access-group 10 out
```

Проверить работоспособность списка доступа. Результаты прокомментировать преподавателю.

Удалить список.

#### Задание 2.

Узлы Сети 1 должны быть доступны всем узлам Сети 2 и одному узлу Сети 3 с адресом 192.168.30.11, остальные узлы Сети 3 не должны иметь доступа. Список доступа установить на интерфейс F0/0 Router\_A.



В списке доступа необходимо использовать инверсную маску (Wildcard mask). Нулевые значения инверсной маски означают требование обработки соответствующих разрядов адреса, а единичные значения – игнорирование соответствующих разрядов адреса при функционировании списка доступа. Таким образом, маска **0.0.0.0** предписывает анализ и обработку всех разрядов адреса, т.е. в этом случае будет обрабатываться адрес каждого узла. Маска **0.0.0.255** показывает, что обрабатываться будет только сетевая часть адреса. Некоторые версии операционных систем IOS маршрутизаторов требуют в обязательном порядке использование масок WildCard при задании адресов узлов и сетей, либо расширения **host** при задании адресов узлов. Записи **192.168.30.11 0.0.0.0** полностью соответствует другой вариант – **host 192.168.30.11**, который также предписывает обрабатывать адрес только одного узла.

```
R-A(config)#access-list 11 permit 192.168.30.11 0.0.0.0
R-A(config)#access-list 11 permit 192.168.20.0 0.0.0.255
R-A(config)#int f0/0
R-A(config-if)#ip access-group 11 out
Проверить работоспособность списка доступа!
Удалить список.
```

**Задание 3.** В Сети Рис. 8.1 необходимо установить список доступа, который:

- блокирует рабочей станции 192.168.20.11 Сети 2 доступ в Сеть 1;
- блокирует рабочей станции 192.168.30.34 Сети 3 доступ в Сеть 1;

Для этого создается список доступа:

```
R-A(config)#access-list 12 deny host 192.168.20.11
R-A(config)#access-list 12 deny host 192.168.30.24
R-A(config)#access-list 12 permit any
R-A(config)#int f0/0
R-A(config-if)#ip access-group 12 out
```

Если бы отсутствовала третья строка списка доступа, то ни одна станция из других сетей не могла бы попасть в Сеть 1, поскольку в конце каждого списка неявно присутствует команда **deny any** – запретить все остальное.

**Проверить работоспособность списка доступа!** Удалить список.

**Задание 4.** Используя исходные данные **Задания 3**, сформируйте список доступа в виде именованного (имя ACL):

```
R-A(config)#ip access-list standard ACL
R-A(config)#deny host 192.168.20.11
R-A(config)#deny host 192.168.30.24
R-A(config)#permit any
R-A(config)#int f0/0
R-A(config-if)#ip access-group ACL out
```

**Проверить работоспособность списка доступа!** Удалить список.

**Задание 5.**

На маршрутизаторе А (рис. 8.1) необходимо установить расширенный список доступа, который:

- блокирует рабочим станциям Сети 2 доступ в Сеть 1 по **telnet**;
- разрешает рабочим станциям Сети 2 доступ в Сеть 1 по другим протоколам, например, по команде **ping** протокола ICMP.

Предварительно сконфигурируйте пароли на маршрутизаторе А:

```
Router_A(config)#line vty 0 15
Router_A(config-line)#password cisco-1
Router_A(config-line)#login
Router_A(config)#enable secret cisco-2
```

Выполнить удаленный доступ на маршрутизатор R-A с конечного узла 192.168.20.11:

```
PC>telnet 192.168.10.1
```

...

```
Password:
```

```
R-A>ena
```

```
Password: (ввести пароль)
```

```
R-A#conf t
```

Измените конфигурацию маршрутизатора, например, измените имя:

```
R-A(config)#hostname Router_A
```

```
Router_A(config)#
```

Выполните команду:

```
PC>ping 192.168.10.1
```

### **Прокомментируйте результаты выполнения команд telnet и ping!**

Сформируйте список доступа, блокирующий рабочим станциям Сети 2 доступ в Сеть1 по **telnet** и разрешающий доступ в Сеть1 по команде **ping**:

```
Router_A(config)#access-list 102 deny tcp 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 eq 23
```

```
Router_A(config)#access-list 102 permit ip any any
```

```
Router_A(config)#int s0/3/0
```

```
Router_A(config-if)#ip access-group 102 in
```

Выполните удаленный доступ к маршрутизатору А (адрес 192.168.10.1) с конечного узла 192.168.20.11.

```
PC>telnet 192.168.10.1
```

```
Выполните команду PC>ping 192.168.10.1
```

### **Прокомментируйте результаты выполнения команд telnet и ping!**

### **Списки доступа IPv6**

Сформируйте схему сети лабораторной работы (рис. 7.3). Используйте маршрутизаторы серии 2911, коммутаторы – серии 2960. Зарисуйте схему.

Сконфигурируйте интерфейсы всех маршрутизаторов.

Сконфигурируйте протокол OSPFv3 на всех маршрутизаторах, например

```
R-A(config)#ipv6 unicast-routing
```

```
R-A(config)#ipv6 router ospf 1
```

```
R-A(config-rtr)#router-id 1.1.1.1
```

```
R-A(config-rtr)#int g0/0
```

```
R-A(config-if)#ipv6 ospf 1 area 0
```

```
R-A(config-if)#int s0/3/0
```

```
R-A(config-if)#ipv6 ospf 1 area 0
```

Проверьте результат конфигурирования, используя команды **show run**, **show ipv6 route**, **ping**. Результат прокомментируйте преподавателю!

### **Задание 6.**

Сформируйте список доступа IPv6, который запрещал бы всем узлам сети 2001:db8:a:3::/64 доступ в сеть 2001:db8:a:1::/64, все остальное разрешить. Список установить на интерфейсе s0/3/0 R-A.

```
R-A(config)#ipv6 access-list ACL
```

```
R-A(config-ipv6-acl)#deny ipv6 2001:db8:a:3::/64 any
```

```
R-A(config-ipv6-acl)#permit ipv6 any any
```

```
R-A(config-ipv6-acl)#int s0/3/0
```

```
R-A(config-if)#ipv6 traffic-filter ACL in
```

Проверьте результат конфигурирования, используя команды **show run**, **show ipv6 route**, **show ipv6 int**, **show access-lists**.

Проверьте функционирование списка ACL по командам **ping**.

**Результат прокомментируйте преподавателю!**

### **7. Контрольные вопросы:**

1. Для чего используются списки доступа?
2. На основании чего формируется запрет или разрешение сетевого трафика через интерфейс маршрутизатора?
3. Какие параметры пакета могут анализироваться в списке доступа?
4. Где устанавливаются списки доступа?
5. Что анализируют стандартные списки доступа?
6. Что анализируют расширенные списки доступа?
7. Какое условие имеется неявно в конце любого списка доступа?
8. Для чего нужны идентификационные номера списков доступа?
9. Каков формат команды создания стандартного списка доступа?
10. Каков формат команды создания расширенного списка доступа?
11. Каков формат команды привязки списка к интерфейсу?
12. Какие достоинства имеют именованные списки доступа?
13. Каков формат команды создания списка доступа IPv6? Каковы особенности конфигурирования списков доступа IPv6?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** ПГУТИ, д.т.н., профессор Васин Н.Н., e-mail: vasin@psati.ru, тел. (846) 332-08-05

**Образовательная программа:** 10.05.02 Информационная безопасность телекоммуникационных систем, Защита информации в системах связи и управления.

**Дисциплина:** Сети и системы передачи информации, Технологии пакетной коммутации.

### **Лабораторная работа.** **Конфигурирование безопасности коммутатора**

**1. Учебные цели:**

Приобрести знания об организации безопасности коммутаторов. Отработать навыки конфигурирования портов коммутаторов.

**2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

Знать принципы функционирования коммутаторов, таблицы коммутации (MAC-адресов), и обеспечения информационной безопасности коммутаторов, владеть навыками конфигурирования и проверки реальных устройств и виртуальных устройств симулятора Packet Tracer.

**3. Перечень материально-технического обеспечения:**

Компьютерный класс, лаборатория сетей пакетной коммутации.

**Лабораторное оборудование и программное обеспечение:** Маршрутизаторы Cisco 2811, коммутаторы Catalyst 2600, компьютеры, симулятор Packet Tracer.

**4. Задание на исследование**

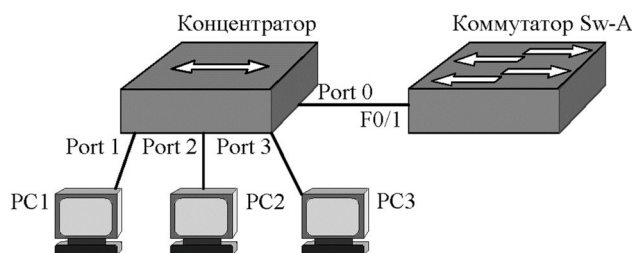
Конфигурирование портов коммутаторов

**5. Краткие теоретические сведения**

1. Технологии пакетной коммутации : учебник / Н.Н. Васин. – М. : ИНГУИТ, 2017. С. 304–335.
2. Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для вузов / К.Е. Самуйлов, И.А. Шалимов, Н.Н. Васин, В.В. Василевский, Д.С. Кулябов, А.В. Королькова. – М. : Юрайт, 2016. С. 228–232.

**6. Порядок выполнения лабораторной работы (этапы)**

Лабораторная работа выполняется для сети (рис. 9.1), адреса – в табл. 9.1.



**Рис. 9.1. Схема сети**

**Таблица 9.1 – Адреса сетей и интерфейсов маршрутизаторов**

| Устройство |          | Адрес      | Маска         | Шлюз       |
|------------|----------|------------|---------------|------------|
| PC1        | NIC      | 10.1.10.21 | 255.255.255.0 | 10.1.10.11 |
| PC2        | NIC      | 10.1.10.22 | 255.255.255.0 | 10.1.10.11 |
| PC3        | NIC      | 10.1.10.23 | 255.255.255.0 | 10.1.10.11 |
| S1         | Vlan 101 | 10.1.10.11 | 255.255.255.0 | 10.1.10.1  |

1. Собрать схему сети (рис. 9.1).
2. Сконфигурировать адресную информацию на компьютерах PC1, PC2, PC3 согласно таблице 9.1.
3. Выполнить последовательность команд:

```
Switch>enable
Switch#show run
Switch#show start
Switch#show vlan brief
```

```
Switch#show int vlan 1
Switch#show ip int vlan 1
Switch#show int f0/1
```

Обратить внимание на состояние устройств и интерфейсов (включен – **up** или выключен **down**), их IP-адреса и MAC-адреса, к каким виртуальным сетям **vlan** приписаны порты коммутатора.

4. Сконфигурировать имя коммутатора и пароли на нем:

```
Switch(config)#hostname Sw-A
Sw-A(config)#line console 0
Sw-A(config-line)#password cisco-1
Sw-A(config-line)#login
Sw-A(config-line)#line vty 0 15
Sw-A(config-line)#password cisco-2
Sw-A(config-line)#login
Sw-A(config-line)#exit
Sw-A(config)#enable secret cisco-3
```

5. Используя команды exit, вернуться в пользовательский режим. Затем вновь войти в привилегированный режим. Объяснить действие паролей. Проверить пароли по команде sh run. Какие пароли представлены в открытой форме, а какие криптографированы? Как зашифровать пароли на консольной и виртуальных линиях?

Выполнить шифрование всех паролей. Произвести проверку!

6. Сконфигурировать IP-адрес на коммутаторе для управления с удаленного устройства. По умолчанию управляющей является виртуальная локальная сеть vlan 1, на которую и выполняют атаки хакеры. Поэтому в качестве управляющей рекомендуется использовать виртуальную сеть с другим номером, например vlan 101, на интерфейс которой устанавливается адрес шлюза по умолчанию (10.1.10.11) компьютеров PC1, PC2, PC3.

```
Sw-A(config)#vlan 101
Sw-A(config-vlan)#exit
Sw-A(config)#int vlan 101
Sw-A(config-if)#ip add 10.1.10.11 255.255.255.0
Sw-A(config-if)#no shutdown
```

7. Выполнить команды верификации:

```
Sw-A#sh vlan brief
Sw-A#sh int vlan 101
```

Прокомментировать полученные результаты.

8. Приписать порт f0/1 к vlan 101:

```
Sw-A(config)#int f0/1
Sw-A(config-if)#switchport access vlan 101
```

9. Установить шлюз по умолчанию:

```
Sw-A(config)#ip default-gateway 10.1.10.1
```

10. Выполнить команды верификации:

```
Sw-A#sh run
Sw-A#sh vlan brief
Sw-A#sh int vlan 101
Sw-A#sh mac-address-table
```

Прокомментировать полученные результаты.

11. С компьютера PC1 выполнить удаленный доступ к коммутатору:

```
PC1>telnet 10.1.10.11
```

12. С компьютера PC1 в режиме удаленного доступа произвести изменение конфигурации коммутатора, например, изменить имя коммутатора на S1.

13. Завершить сеанс удаленного доступа, используя команды exit.

14. Убедиться в изменении конфигурации коммутатора, войдя в режим конфигурирования коммутатора CLI.

15. Выполнить команду:

```
S1#show mac-address-table
```

Команду повторить через 5 минут. Объяснить полученный результат.

16. Определить физические адреса сетевых карт компьютеров по команде ipconfig /all для компьютеров PC1, PC2 и PC3. Записать MAC-адреса.

17. Сконфигурировать статическую запись в таблице маршрутизации, приписав MAC-адрес компьютера PC1 к порту Fa0/1 коммутатора:

```
S1(config)#mac-address-table static Mac-адрес vlan 101 interface fastethernet 0/1
```

Проверить таблицу коммутации.

18. Удалить статическую запись из таблицы коммутации. Проверить таблицу коммутации.

Конфигурирование безопасности порта коммутатора

19. Сконфигурировать безопасность порта f0/1:
 

```
S1(config)#int f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
Задать количество безопасных адресов, равное 1:
S1(config-if)#switchport port-security maximum 1
Установить режим безопасных адресов sticky:
S1(config-if)#switchport port-security mac-address sticky
Установить режим реагирования на нарушение безопасности shutdown:
S1(config-if)#switchport port-security violation shutdown
```
20. Проверить текущую конфигурацию и таблицу коммутации по командам show running-configuration и show mac-address-table. Прокомментировать полученные результаты.
21. Выполнить команду ping 10.1.10.11 с компьютера PC1. Вновь проверить таблицу коммутации и прокомментировать полученный результат.
22. Выполнить команду ping 10.1.10.11 с компьютера PC2. Порт коммутатора должен выключиться.
23. Выполнить команду show port-security int f0/1 и прокомментировать полученный результат.
24. Включить порт f0/1 коммутатора. После того, как загорится зеленый индикатор, выполнить команду ping 10.1.10.11 с компьютера PC1.
25. Выполнить команду show port-security int f0/1.
26. Увеличить количество безопасных адресов до 2:
 

```
S1(config-if)#switchport port-security maximum 2
```
27. Выполнить команду ping 10.1.10.11 с компьютеров PC1, PC2.
28. Выполнить команды show mac-address-table и show port-security int f0/1 и прокомментировать полученный результат.
29. Выполнить команду ping 10.1.10.11 с компьютера PC3. Прокомментировать результат.

### Конфигурирование протокола SSH на коммутаторе.

Для того чтобы сконфигурировать SSH на коммутаторе (рис. 9.2) необходимо выполнить ряд команд.

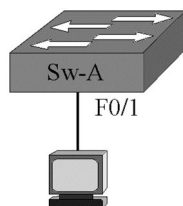


Рис. 9.2. Конфигурирование SSH на коммутаторе

Предварительно нужно задать имя коммутатора, например:

```
Switch(config)#hostname Sw-A
```

В режиме глобального конфигурирования требуется задать имя домену, где функционирует SSH, например **class**:

```
Sw-A(config)#ip domain-name class
```

Протокол SSH автоматически включается при создании пары ключей RSA, при этом требуется указать длину модуля в диапазоне от 360 до 2048. В приведенном примере задана длина 1024:

```
Sw-A(config)#crypto key generate rsa
```

```
The name for the keys will be: S-A.class
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys.
```

Choosing a key modulus greater than 512 may take a few minutes.

```
How many bits in the modulus [512]: 1024
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Для аутентификации пользователя задают его имя (например, vas) и пароль (например, cis1):

```
Sw-A(config)#username vas secret cis1
```

```
*?? ?10:4:3:608: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Сообщение говорит о том, что используется версия 1.99. В настоящее время предпочтительной является версия 2, которую необходимо задать.

Настройку SSH на виртуальных линиях реализует следующая последовательность команд:

```
Sw-A(config)#line vty 0 4
```

```
Sw-A(config-line)#transport input ssh
```

```
Sw-A(config-line)#login local
```

```
Sw-A(config-line)#exit
Sw-A(config)#ip ssh version 2
```

Если ранее на виртуальном интерфейсе (SVI) не была установлена конфигурация управления коммутатором, то сделайте это, например:

```
Sw-A(config)#int vlan 101
Sw-A(config-if)#ip add 192.168.10.11 255.255.255.0
Sw-A(config-if)#no shut
Sw-A(config-if)#exit
Sw-A(config)#ip default-gateway 192.168.10.1
```

Кроме того, необходимо сформировать виртуальную локальную сеть vlan 101 и к ней приписать физический интерфейс, например interface f0/19, к которому подключен персональный компьютер:

```
Sw-A(config)#vlan 101
Sw-A(config-vlan)#
%LINK-5-CHANGED: Interface Vlan101, changed state to up
Sw-A(config-vlan)#int f0/1
Sw-A(config-if)#switchport access vlan 101
Sw-A(config-if)#
```

Проверка возможности удаленного доступа по SSH с персонального компьютера (рис. 6.3) производится по команде:

```
PC>ssh -l vas 192.168.10.11
Open
Password:
Sw-A>
```

При этом протокол Telnet не работает. Ввод команды transport input all на линиях vty разрешает функционирование как SSH, так и Telnet.

**Время на выполнение лабораторной работы – 2 часа.**

**Образовательная организация, авторы, эл. почта:** ПГУТИ, д.т.н., профессор Васин Н.Н., e-mail: vasin@psati.ru, тел. (846) 332-08-05

---

**Образовательная программа:** 10.05.02 Информационная безопасность телекоммуникационных систем, Защита информации в системах связи и управления.

**Дисциплина:** Сети и системы передачи информации, Технологии пакетной коммутации.

### **Лабораторная работа.** **Конфигурирование виртуальных локальных сетей**

#### **1. Учебные цели:**

Приобрести знания о виртуальных локальных сетях VLAN. Отработать навыки конфигурирования коммутаторов по формированию VLAN.

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

Знать принципы функционирования VLAN, владеть навыками конфигурирования VLAN и проверки работы реальных коммутаторов и виртуальных устройств симулятора Packet Tracer.

#### **3. Перечень материально-технического обеспечения:**

Компьютерный класс, лаборатория сетей пакетной коммутации.

**Лабораторное оборудование и программное обеспечение:** Маршрутизаторы Cisco 2811, коммутаторы Catalyst 2600, компьютеры, симулятор Packet Tracer.

#### **4. Задание на исследование**

Конфигурирование коммутаторов по формированию VLAN.

#### **5. Краткие теоретические сведения**

1. Технологии пакетной коммутации : учебник / Н.Н. Васин. – М. : ИНГУИТ, 2017. С. 336–362.

- Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для вузов / К.Е. Самуйлов, И.А. Шалимов, Н.Н. Васин, В.В. Василевский, Д.С. Кулябов, А.В. Королькова. – М. : Юрайт, 2016. С. 332–348.

## 6. Порядок выполнения лабораторной работы

**Статическое конфигурирование** виртуальных сетей сводится к назначению портов коммутатора на каждую виртуальную локальную сеть VLAN, через использование командной строки CLI.

- Создать схему лабораторной работы, включающую три виртуальных локальных сети (рис. 10.1) на коммутаторе Sw\_A, подключив PC0 к порту f0/1, PC1 – к порту f0/2, PC2 – к порту f0/3, PC3 – к порту f0/4, PC4 – к порту f0/5, PC5 – к порту f0/6:
- Согласно схеме (рис. 10.1 и табл. 10.1) сконфигурировать на конечных узлах (персональных компьютерах PC0 – PC5) IP-адреса, маски и шлюзы по умолчанию.

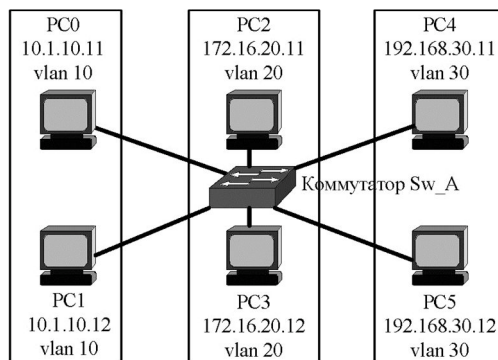


Рис. 10.1. Виртуальные локальные сети

Таблица 10.1 – Конфигурация конечных узлов виртуальных локальных сетей

| VLAN №  | Узел | Адрес узла    | Маска         | Шлюз         |
|---------|------|---------------|---------------|--------------|
| Vlan 10 | PC0  | 10.1.10.11    | 255.255.255.0 | 10.1.10.1    |
|         | PC1  | 10.1.10.12    |               |              |
| Vlan 20 | PC2  | 172.16.20.11  | 255.255.255.0 | 172.16.20.1  |
|         | PC3  | 172.16.20.12  |               |              |
| Vlan 30 | PC4  | 192.168.30.11 | 255.255.255.0 | 192.168.30.1 |
|         | PC5  | 192.168.30.12 |               |              |

Таким образом, каждая виртуальная локальная сеть имеет свой IP-адрес.

- По команде **sh vlan brief** посмотреть состояние виртуальных сетей и интерфейсов коммутатора. Прокомментировать результат.
- Сконфигурировать на коммутаторе три виртуальных локальных сети:
 

```
Sw-A(config)#vlan 10
Sw-A(config-vlan)#vlan 20
Sw-A(config-vlan)#vlan 30
```
- По команде **sh vlan brief** проанализировать изменения конфигурации.
- Назначить виртуальные сети на определенные интерфейсы (приписать интерфейсы к созданным виртуальным сетям), используя пару команд **switchport mode access**, **switchport access vlan №.** Ниже приведен пример указанных операций для сети (рис. 10.1).

```
Sw-A(config)#int f0/1
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switchport access vlan 10
Sw-A(config-if)#int f0/2
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switchport access vlan 10
Sw-A(config-if)#int f0/3
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switchport access vlan 20
Sw-A(config-if)#int f0/4
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switchport access vlan 20
Sw-A(config-if)#int f0/5
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switchport access vlan 30
Sw-A(config-if)#int f0/6
Sw-A(config-if)#switchport mode access
Sw-A(config-if)#switchport access vlan 30
```

7. Произвести верификацию полученной конфигурации с помощью команды **show vlan brief**. Прокомментировать результат.
8. Скопировать конфигурационный файл в энергонезависимую память коммутатора по команде:  
Sw-A #copy running-config startup-config
9. Для отмены неверного назначения виртуальной сети на интерфейс, например, ошибочное назначение виртуальной сети vlan 20 на интерфейс F0/2, используется команда:  
Sw-A(config)#**int f0/2**  
Sw-A(config-if)#**no switchport access vlan**  
Также можно просто приписать интерфейс f0/2 к другой виртуальной сети, например, к vlan 10:  
Sw-A(config)#**int f0/2**  
Sw-A(config-if)#**switchport mode access**  
Sw-A(config-if)#**switch access vlan 10**
10. Проверка работоспособности сети производится по командам ping, (tracert). Проверить соединение PC0 с PC1 и другими компьютерами:  
PC0>**ping 10.1.10.12**  
PC0>**ping 172.16.20.12**  
PC0>**ping 192.168.30.12**
11. Если к сети присоединить дополнительный узел PC6, адрес которого 192.168.30.101 (рис. 10.2), т.е. адрес его сети совпадает с адресом сети vlan 30, но узел PC6 не приписан ни к одной из виртуальных сетей, то он не сможет реализовать соединения с узлами существующих виртуальных сетей. **Проверить! Результат показать преподавателю.**

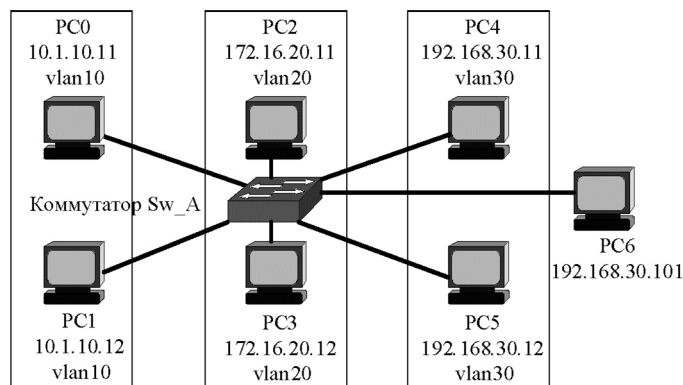


Рис. 10.2. Функционирование виртуальных локальных сетей

### Формирование виртуальных локальных сетей на нескольких коммутаторах

12. Собрать схему сети (рис. 10.3).

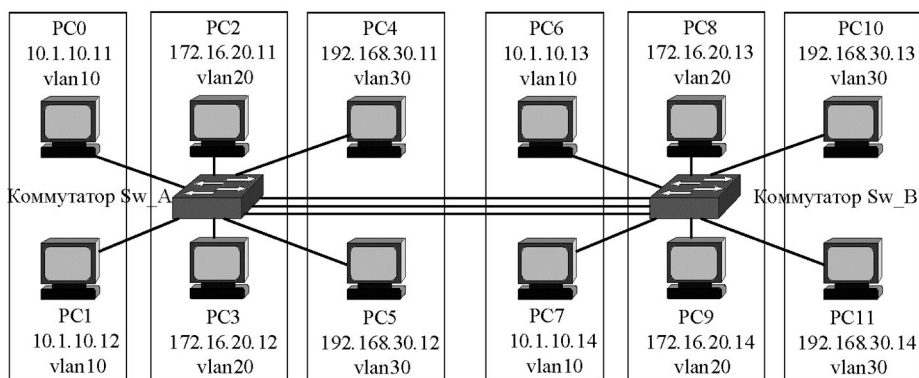


Рис. 10.3. VLAN на двух коммутаторах

Согласно схеме Рис. 10.3 сконфигурировать на конечных узлах (персональных компьютерах PC6–PC11) IP-адреса, маски и шлюзы по умолчанию. Приписать интерфейсы второго коммутатора Sw\_B к vlan 10, vlan 20, vlan 30. Приписать интерфейсы, соединяющие коммутаторы между собой, например f0/7, f0/8, f0/9, к vlan 10, vlan 20, vlan 30.

13. Проверить работоспособность сети. По команде **ping** проверить соединение PC0 с PC1 и другими компьютерами:  
PC0>**ping 10.1.10.12**  
PC0>**ping 10.1.10.13**  
PC0>**ping 10.1.10.14**



```
PC0>ping 172.16.20.12
PC0>ping 192.168.30.12
Объяснить результаты!
```

#### Маршрутизация между виртуальными локальными сетями

14. Поскольку каждая виртуальная локальная сеть представляет собой широковещательный домен, т.е. сеть со своим IP-адресом, то для связи между сетями необходима маршрутизация Уровня 3. Поэтому к коммутатору необходимо присоединить маршрутизатор (рис. 10.4).

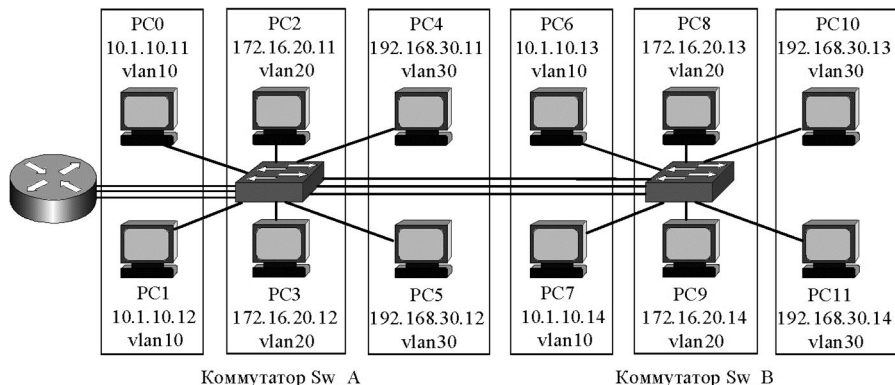


Рис. 10.4. Связь между сетями через маршрутизатор

15. Для соединения с маршрутизатором в схеме дополнительно задействованы три интерфейса коммутатора Sw\_A: F0/11, F0/12, F0/13. При этом порт F0/11 приписан к сети vlan 10, порт F0/12 – к vlan 20, порт F0/13 – к vlan 30.

```
Sw_A(config)#int f0/11
Sw_A(config-if)#switchport access vlan 10
Sw_A(config-if)#int f0/12
Sw_A(config-if)#switchport access vlan 20
Sw_A(config-if)#int f0/13
Sw_A(config-if)#switchport access vlan 30
```

16. На маршрутизаторе серии 2811 установите дополнительные интерфейсы локальных сетей, например, NM-2FE2W. Таким образом, на маршрутизаторе будут функционировать 4 интерфейса локальных сетей: F0/0, F0/1, F1/0, F1/1.

17. На маршрутизаторе используются три интерфейса F0/0, F0/1, F1/0 (по числу виртуальных сетей), которые сконфигурированы следующим образом:

```
Router>ena
Router#conf t
Router(config)#int f0/0
Router(config-if)#ip add 10.1.10.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int f0/1
Router(config-if)#ip add 172.16.20.1 255.255.255.0
Router(config-if)#no shut
Router(config)#int f1/0
Router(config-if)#ip add 192.168.30.1 255.255.255.0
Router(config-if)#no shut
```

18. По команде **sh ip route** посмотреть таблицу маршрутизации:

```
Router#sh ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B – BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, ia – IS-IS inter area
* – candidate default, U – per-user static route, o – ODR
P – periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 1 subnets
C 10.1.10.0 is directly connected, FastEthernet0/0
172.16.0.0/24 is subnetted, 1 subnets
C 172.16.20.0 is directly connected, FastEthernet0/1
C 192.168.30.0/24 is directly connected, FastEthernet1/0
```

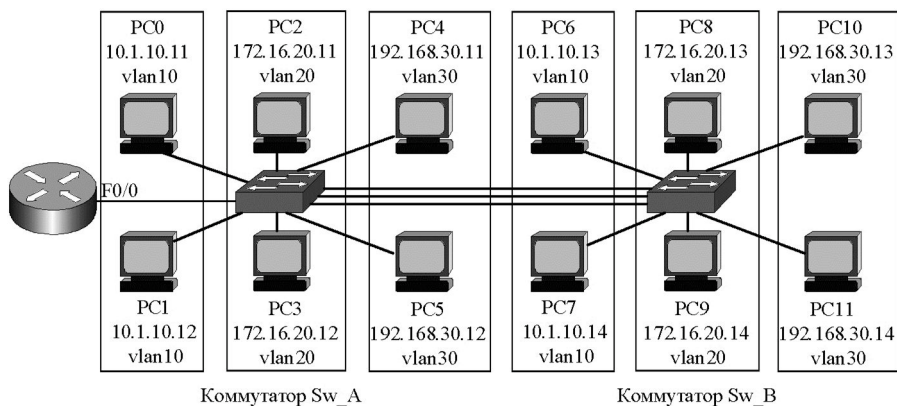
Из таблицы маршрутизации следует, что все три сети (10.1.10.0, 172.16.20.0, 192.168.30.0) являются непосредственно присоединенными и, следовательно, могут обеспечивать маршрутизацию между сетями. «Прозвонка» с узла 10.1.10.11 узлов сетей 172.16.20.0, 192.168.30.0 должна дать положительный результат.

19. Проверить работоспособность сети. По команде **ping** проверить соединение PC0 со всеми другими компьютерами сети. **Результат показать преподавателю.**

Недостатком такого метода организации межсетевых соединений является необходимость использования дополнительных интерфейсов коммутатора и маршрутизатора, число которых равно количеству виртуальных сетей. От этого недостатка свободно **транковое** соединение, когда совокупность физических каналов между двумя устройствами может быть заменена одним агрегированным каналом, включающим несколько логических соединений.

### Конфигурирование транковых соединений

20. Собрать схему сети (рис. 10.5). При транковом соединении коммутатора и маршрутизатора три физических канала между ними (рис. 10.4) заменяются одним агрегированным каналом (рис. 10.5).



**Рис. 10.5. Транковое соединение коммутатора и маршрутизатора**

Для создания транкового соединения на коммутаторе задействован интерфейс F0/10, а на маршрутизаторе – F0/0.

21. Конфигурирование коммутатора будет следующим:

```
Sw_A>ena
Sw_A#conf t
Sw_A(config)#vlan 10
Sw_A(config-vlan)#vlan 20
Sw_A(config-vlan)#vlan 30
Sw_A(config-vlan)#int f0/1
Sw_A(config-if)#switchport mode access
Sw_A(config-if)#switchport access vlan 10
Sw_A(config-if)#int f0/4
Sw_A(config-if)#switchport access vlan 10
Sw_A(config-if)#int f0/2
Sw_A(config-if)#switchport access vlan 20
Sw_A(config-if)#int f0/5
Sw_A(config-if)#switchport access vlan 20
Sw_A(config-if)#int f0/3
Sw_A(config-if)#switchport access vlan 30
Sw_A(config-if)#int f0/6
Sw_A(config-if)#switchport access vlan 30
Sw_A(config-if)#int f0/10
Sw_A(config-if)#switchport mode trunk
Sw_A(config-if)#^Z
```

22. По команде **sh int f0/10 switchport** можно посмотреть состояние интерфейса:

```
Sw_A#sh int f0/10 switchport
Name: Fa0/10
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
```

```

Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
...
Sw_A#

```

Из распечатки следует, что порт F0/10 находится в режиме Trunk.

23. Конфигурирование маршрутизатора сводится к тому, что на его интерфейсе F0/0 формируются субинтерфейсы F0/0.10, F0/0.20, F0/0.30. На указанных субинтерфейсах конфигурируется протокол Dot 1q для виртуальных сетей 10, 20, 30. Последовательность команд необходимо завершить включением интерфейса **no shut**.

```

Router>ena
Router#conf t
Router(config-if)#int f0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip add 10.1.10.1 255.255.255.0
Router(config-subif)#int f0/0.20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip add 172.16.20.1 255.255.255.0
Router(config-subif)#int f0/0.30
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip add 192.168.30.1 255.255.255.0
Router(config-subif)#int f0/0
Router(config-if)#no shut

```

24. Результат конфигурирования проверяется по команде **sh ip route**:

```

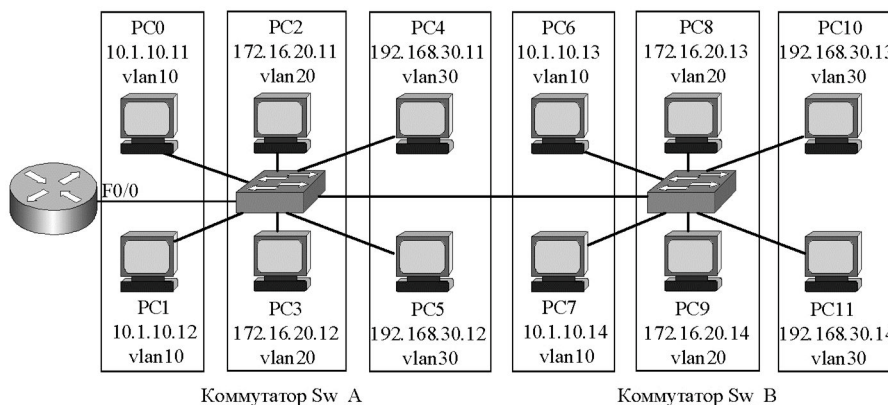
Router#sh ip route
...
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 1 subnets
C 10.1.10.0 is directly connected, FastEthernet0/0.10
172.16.0.0/24 is subnetted, 1 subnets
C 172.16.20.0 is directly connected, FastEthernet0/0.20
C 192.168.30.0/24 is directly connected, FastEthernet0/0.30
Router#

```

Из таблицы маршрутизации следует, что сети 10.1.10.0, 172.16.20.0, 192.168.30.0 являются непосредственно присоединенными. Поэтому маршрутизатор способен обеспечить маршрутизацию между сетями.

25. Проверить работоспособность сети. По команде **ping** проверить соединение всех компьютеров сети между собой. **Результат показать преподавателю.**

26. Сформировать транковое соединение между коммутаторами (рис. 10.6)



**Рис. 10.6.** Транковое соединение коммутаторов

27. Проверить работоспособность сети. По команде **ping** проверить соединение всех компьютеров сети между собой. **Результат показать преподавателю.**

**Время на выполнение лабораторной работы – 2 часа.**

**Образовательная организация, авторы, эл. почта:** ПГУТИ, д.т.н., профессор Васин Н.Н., e-mail: vasin@psati.ru, тел. (846) 332-08-05

**Образовательная программа:** 10.05.02 Информационная безопасность телекоммуникационных систем, Защита информации в системах связи и управления.

**Дисциплина:** Сети и системы передачи информации, Технологии пакетной коммутации.

### **Лабораторная работа.** **Конфигурирование сети на реальном оборудовании**

#### **1. Учебные цели:**

Приобрести знания о функционировании сети пакетной коммутации. Отработать навыки конфигурирования маршрутизаторов и коммутаторов.

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

Знать принципы функционирования сетей пакетной коммутации, владеть навыками конфигурирования и проверки работы реальных маршрутизаторов и коммутаторов.

#### **3. Перечень материально-технического обеспечения:**

Компьютерный класс, лаборатория сетей пакетной коммутации.

**Лабораторное оборудование и программное обеспечение:** Маршрутизаторы Cisco 2811, коммутаторы Catalyst 2600, компьютеры.

#### **4. Задание на исследование**

Конфигурирование маршрутизаторов и коммутаторов.

#### **5. Краткие теоретические сведения:**

1. Технологии пакетной коммутации : учебник / Н.Н. Васин. – М. : ИНТУИТ, 2017. 408 с.
2. Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для вузов / К.Е. Самуйлов, И.А. Шалимов, Н.Н. Васин, В.В. Василевский, Д.С. Кулябов, А.В. Королькова. – М. : Юрайт, 2016. 363 с.

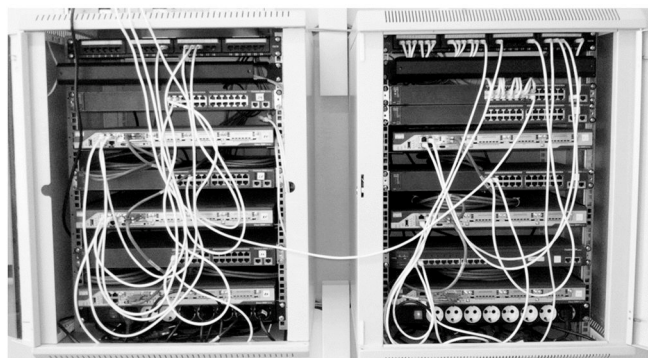
#### **6. Порядок выполнения лабораторной работы (этапы)**

Оборудование лаборатории «Технологии пакетной коммутации» включает 6 маршрутизаторов 2800 фирмы Cisco, 6 коммутаторов 2960 фирмы Catalyst, размещенных в двух телекоммуникационных шкафах (рис. 11.1).

Кроме того, оборудование включает 12 компьютеров, шесть из которых используются для подключения к консольным портам маршрутизаторов с целью их конфигурирования, а 6 – подключены к коммутаторам для создания сети (рис. 11.2). Схему сети зарисовать в отчет.

#### **Выполнение работы:**

1. Убедиться, что консольные кабели (плоские голубого цвета) компьютеров № 12, № 10, № 8, № 6, № 4, № 2 подсоединены к СОМ-портам и выведены на соответствующий разъем (помечен символом С).
2. С помощью «патч-кордов» соединить последовательные интерфейсы СОМ1 компьютеров № 12, № 10, № 8, № 6, № 4, № 2 с консольными портами маршрутизаторов согласно схеме (рис. 11.1).
3. На компьютерах, подключенных к консольным портам маршрутизаторов, запустить программу Nureg Terminal (PuTTY, Tera Term) и установить требуемые параметры.
4. Сконфигурировать адресную информацию на интерфейсах маршрутизаторов. Адреса предлагает преподаватель или студенты.



**Рис. 11.1.** Оборудование лаборатории

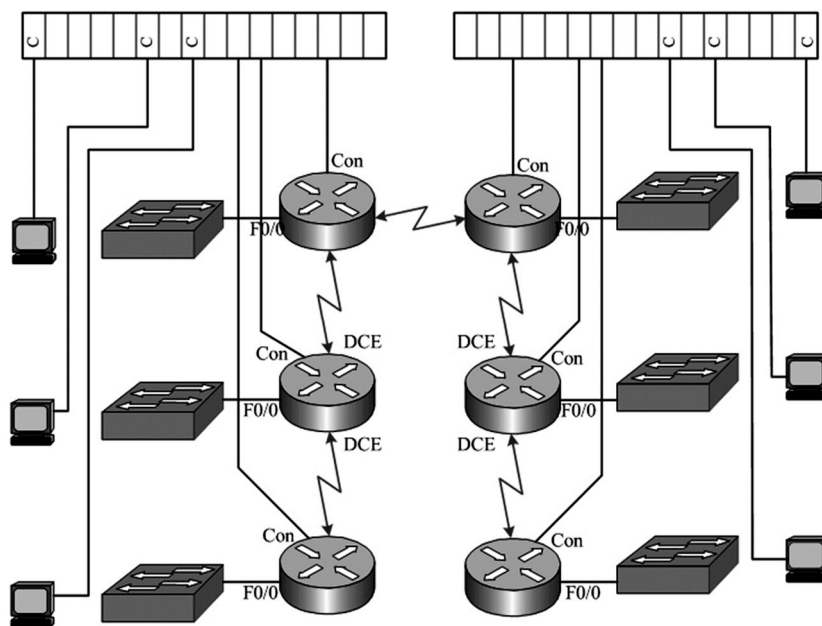


Рис. 11.2. Схема сети

5. Сконфигурировать один из протоколов маршрутизации (RIP2, EIGRP, OSPF) по согласованию с преподавателем.
6. Провести отладку и проверку работоспособности сети, выполнив команды: **ping, show run, show ip route**. Результаты занести в отчет.

**Время на выполнение лабораторной работы – 2 часа.**

**Образовательная организация, авторы, эл. почта:** ПГУТИ, д.т.н., профессор Васин Н.Н., e-mail: vasin@psati.ru, тел. (846) 332-08-05

## **Дисциплина: Техническая защита информации**

**Образовательная программа:** 10.05.02 Информационная безопасность телекоммуникационных систем, 10.03.01 Информационная безопасность.

**Дисциплина:** Техническая защита информации.

### **Лабораторная работа.**

#### **Защита информации от утечки по радиоканалу**

##### **1. Учебные цели:**

Приобретение теоретических знаний о способах защиты информации от утечки по радиоканалу, получение практических навыков поиска и локализации средств несанкционированного съема акустической информации на примере универсального программно-аппаратного комплекса обнаружения средств негласного съема информации (ПО «Филин ультра» и профессиональный сканирующий радиоприемник AR 5000A).

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

Знать общую методологию оценки возможностей средств технической разведки в отношении к системам связи, управления и объектам информатизации. Знать общую методологию применения наиболее эффективных методов и средств для закрытия возможных каналов перехвата акустической речевой информации. Уметь применять методы и средства для обнаружения возможных каналов перехвата акустической речевой информации. Владеть навыками поиска и локализации средств несанкционированного съема акустической информации

##### **3. Перечень материально-технического обеспечения**

**Лабораторное оборудование и программное обеспечение:** Компьютерная лаборатория, специализированное ПО «Филин ультра» и профессиональный сканирующий радиоприемник AR 5000A.

##### **4. Задание на исследование:**

- изучить теоретический материал методики работы с программно-аппаратным комплексом обнаружения средств негласного съема информации, на примере ПО «Филин ультра» и профессиональный сканирующий радиоприемник AR 5000A;
- выполнить задания поиска и локализации закладного устройства.

##### **5. Краткие теоретические сведения:**

Управляющая программа «ФИЛИН» (Filin) предназначена для создания на ее основе программно-аппаратных комплексов поиска и локализации средств несанкционированного съема информации, передающих информацию по радиоканалу или по проводным линиям, а также с целью анализа их характеристик, сбора, обработки и представления статистических данных о радиосигналах.

В данной лабораторной работе в качестве аппаратного средства будет использоваться профессиональный сканирующий радиоприемник AR 5000A.

В качестве тестового сигнала активного теста используется wave файл. Wave файл может быть любого типа, записанный в режиме 11 кГц 8 бит (в том числе записанный Вами с помощью стандартных средств Windows – например, с помощью фонографа).

##### **6. Порядок выполнения лабораторной работы (этапы)**

Для начала работы необходимо запустить управляющую программу «Филин»

###### **1.1. Настройка программы**

1.1.1. Открываем пункт меню "Установки", который позволяет выбрать оборудование, с которым будет работать программа. При его выборе на экран выводится окно установки параметров аппаратуры (рис. 1).

###### **1.1.2. Выбираем подпункт меню "Выбор аппаратуры"**

1.1.3. На странице «Устройства» в группе "Приемник" необходимо выбрать сканирующий приемник, который будет использоваться, выбираем сканирующий приемника и блока преобразования спектра. В группе "Приемник" необходимо выбрать сканирующий приемник AR 5000A, который будет использоваться для получения картины панорам и работы с аудиоданными и фонограммами принимаемых сигналов.

1.1.4. Если БПА не используется в группе "Блок панорамного анализа" необходимо выбрать пункт "Не используется", в этом случае картина панорамы радиочастотного спектра и демодулированный аудиосигнал получают с помощью сканирующего приемника (рис. 1).



Рис. 1. Выбор аппаратуры

## 1.2. Поиск закладного устройства:

1.2.1. Для начала выполнения поиска закладок необходимо открыть подпункт меню "Установки текущей задачи", который позволяет выбрать задачу, которую будет выполнять программа и настроить параметры выбранной задачи (рис. 2).

1.2.2. В левой части окна выбирается текущая задача: «поиск закладок»;

1.2.3. В левой части окна выбирается метод поиска, в зависимости от коммутатора (рис. 3).

В правой части окна отображаются параметры решаемой задачи, параметры поиска;

1.2.4. Для того чтобы определить, какие тесты будут использоваться при автоматическом сканировании, необходимо с помощью мышки поставить галочку в окошке выбора соответствующего теста (рис. 2). Выбираем вид теста, лучше всего применять несколько тестов для проверки, так как комплексное использование тестов позволяет добиться гораздо большей вероятности обнаружения при меньшей вероятности ложной тревоги.

1.2.5. Далее выбираем «цифровой тест» для настройки параметров работы цифровых тестов (рис. 4).

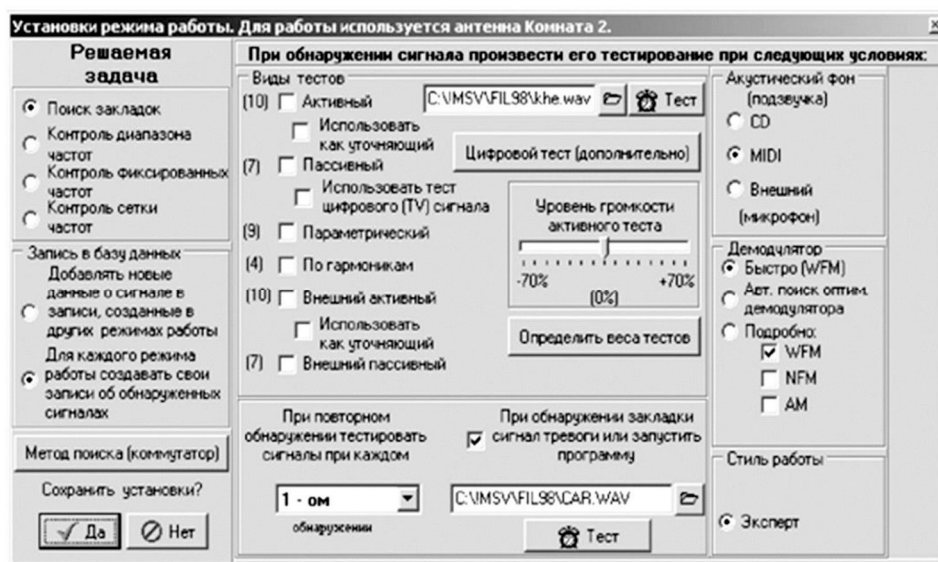


Рис. 2. Установки режима работы

1.2.6. Для каждого из тестов в раскрывающемся окне необходимо выбрать, при каких демодуляторах проводить тестирование, отдельно для тестов телевизионного сигнала и теста цифровых сигналов (рис. 2, рис. 3).

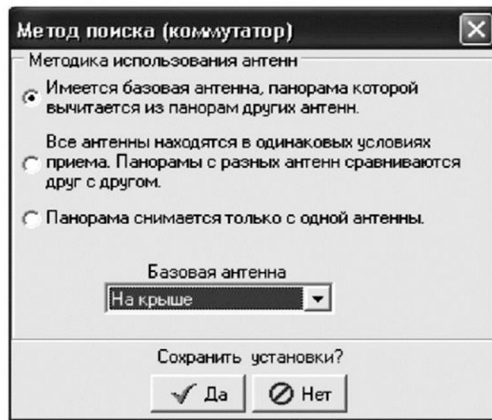


Рис. 3. Методика поиска

1.2.7. По завершению все действий сохраняем установки.

1.2.8. Выбираем midi для акустического фона (рис. 2).

1.2.9. В поле ввода, расположенной на панели управления, задаем диапазон сканирования.

1.2.10. Сканирование (в порядке приоритетов) начинается с:

- текущего положения курсора, если он находится на отображаемом участке панорамы;
- места последней остановки работы автоматического сканирования;
- начала диапазона при первом запуске или после изменения диапазона сканирования

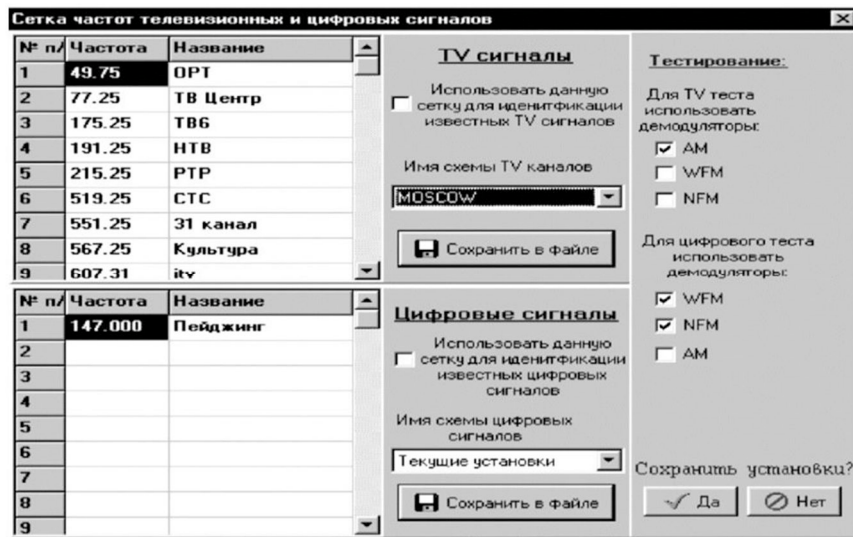


Рис. 4. Сетка частот телевизионных и цифровых

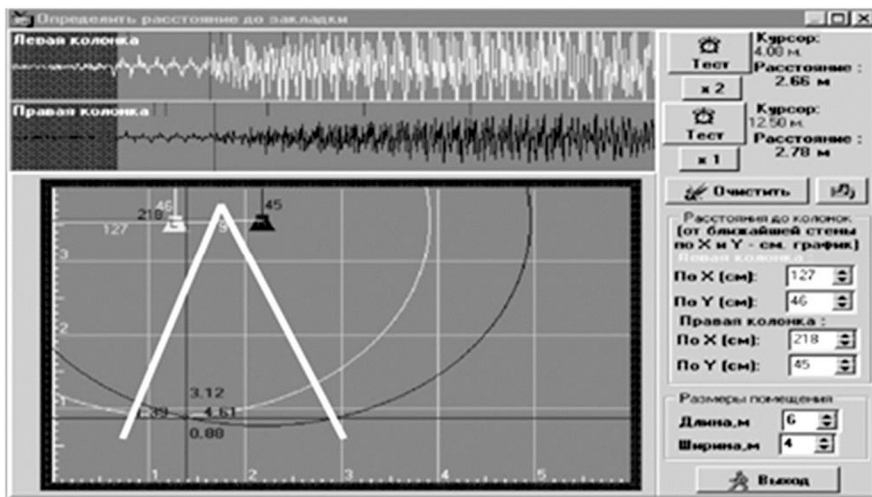


Рис. 5. Определение расстояние до закладки



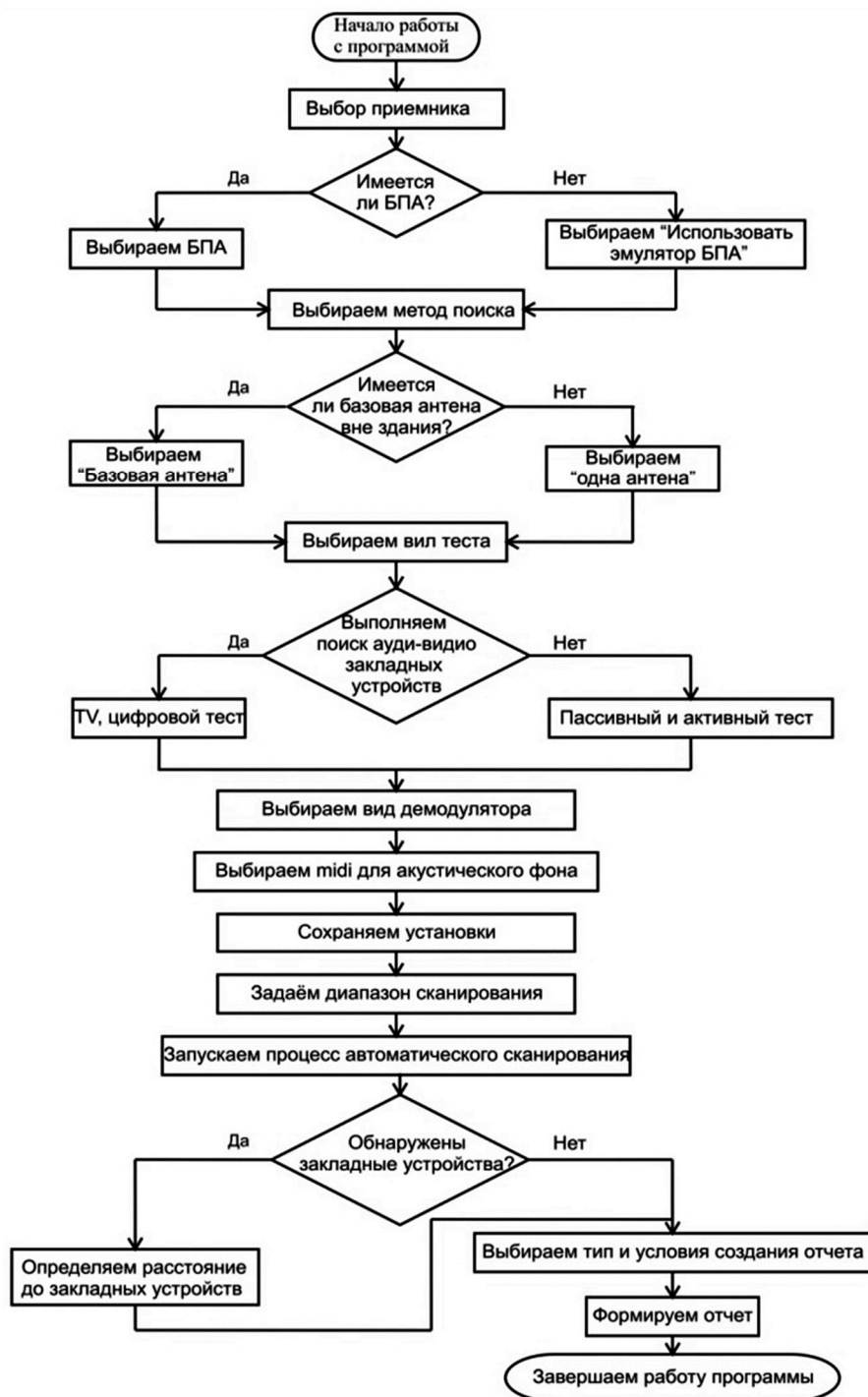


Рис. 6. Блок-схема выполнения задания лабораторной работы

### 1.3. Локализация закладного устройства:

#### 1.3.1. В пункте меню «Сервис» выбираем подпункт меню "Определить расстояние".

Данный пункт меню предназначен для определения расстояния до радиозакладки и доступен только в режиме "Поиск закладок" (рис. 4).

Данное окно логически разбито на две части: окно диаграммы откликов на тестовый акустический сигнал и окно с планом помещения, в котором отображается положение акустических колонок и отображается потенциальное местоположение обнаруженной радиозакладки.

1.3.2. Кнопки «Тест» предназначены для подачи импульсов акустического зондирования. Диаграмма отклика на поданный акустический сигнал позволяет визуально оценить временную зависимость изменения характера модуляции принимаемого радиосигнала с момента подачи акустического теста, приведенной к расстоянию от акустического излучателя (колонок). Красный маркер на графике отклика означает начало изменения характера модуляции и, соответственно, обозначает расстояние до источника радиосигнала.

1.4. Составление отчета:

1.4.1. В пункте меню "Сервис" выбираем подпункт меню "Отчетный документ".

1.4.2. В этом окне необходимо выбрать тип создаваемого отчета и условия создания отчета (рис. 7).

1.4.3. Формируем отчет.

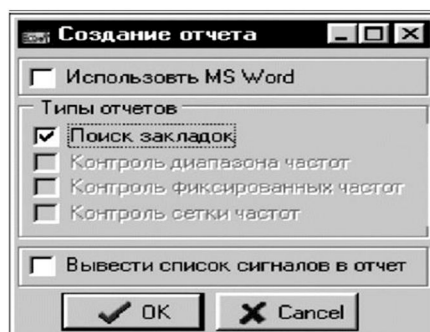


Рис. 7. Создание отчета

## 7. Контрольные вопросы:

1. Основные функции выполняемые программно-аппаратным комплексом (AR 5000 и Филин)?
2. Назовите способы получения панорам, реализованных в программно-аппаратном комплексе (AR 5000 и ПО Филин)?
3. Суть метода поиска радиозакладок основанного на разности панорам?
4. Недостатки и ограничения метода, при котором антенны находятся в контролируемых помещениях?
5. Виды демодуляторов и их использование в программно-аппаратном комплексе (AR 5000 и ПО Филин)?
6. Назовите основные характеристики, которыми обладает профессиональный сканирующий радиоприемник AR 5000A?
7. Активный тест, для чего используется и принцип работы?
8. Цель использования пассивного теста, его принцип работы
9. Вероятность пропуска радиозакладки при использовании активного пассивного тестов?
10. Для чего необходим акустический фон (подзвучка)?
11. Способ используемый в программно-аппаратном комплексе для определения расстояния до закладного подслушивающего устройства.
12. Какие закладные подслушивающие устройства невозможно локализовать?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** Федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ» (КНИТУ-КАИ), И.В.Аникин, Г.С.Корнилов, gskornilov@kai.ru

---

**Образовательная программа:** 10.05.02 Информационная безопасность телекоммуникационных систем, 10.03.01 Информационная безопасность.

**Дисциплина:** Техническая защита информации.

## Лабораторная работа.

### Защита информации от утечки по акустическому каналу

#### 1. Учебные цели:

Отработать навыки оценки звуко- и виброизоляции помещения, калибровки и настройки аппаратно-программного комплекса виброакустической защиты VNK-012GL.

#### 2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

- Знать общий подход к оценке возможностей средств технической разведки в отношении к системам связи, управления и объектам информатизации.
- Уметь применять методы и средства оценки звуко- и виброизоляции помещения.
- Владеть навыками применения средств оценки звуко- и виброизоляции помещения.

### 3. Перечень материально-технического обеспечения

**Лабораторное оборудование и программное обеспечение:** Компьютерная лаборатория, аппаратно-программный комплекс виброакустических измерений VNK–012GL и ПО "Форманта".

#### 4. Задание на исследование:

- изучить теоретический материал методики работы с аппаратно-программным комплексом виброакустической защиты VNK–012GL;
- выполнить задания по оценке звуко- и виброизоляции помещения с помощью с аппаратно-программного комплекса виброакустической защиты VNK–012GL и программное обеспечение "Форманта".

#### 5. Краткие теоретические сведения:

Аппаратно-программный комплекс виброакустической защиты VNK–012GL предназначен для проведения специальных акустических и виброакустических измерений по выявлению и оценке эффективности каналов утечки речевой информации из проверяемых помещений, а также для настройки и определения эффективности систем активной виброакустической защиты.

Комплекс имеет следующие основные режимы работы:

- оценка эффективности каналов утечки речевой информации по следующим критериям:
- отношение сигнал/помеха;
- индекс артикуляции словесная разборчивость речи;
- настройка активных систем защиты речевой информации:
- оценка звукоизоляции;
- оценка виброизоляции.

Состав средств аппаратно-программного комплекса виброакустической защиты VNK–012GL

- Персональный компьютер с установленным программным обеспечением.
- Шумомер АТТ-9000.
- Акустический излучатель SI-3100.
- Предварительный усилитель AA-012GL.
- Комплект приемных датчиков (микрофон М-1, акселерометр AS-4).
- Комплект соединительных кабелей и приспособлений.


(Полные теоретические сведения можно получить из конспекта лекции).

#### 6. Порядок выполнения лабораторной работы (этапы)

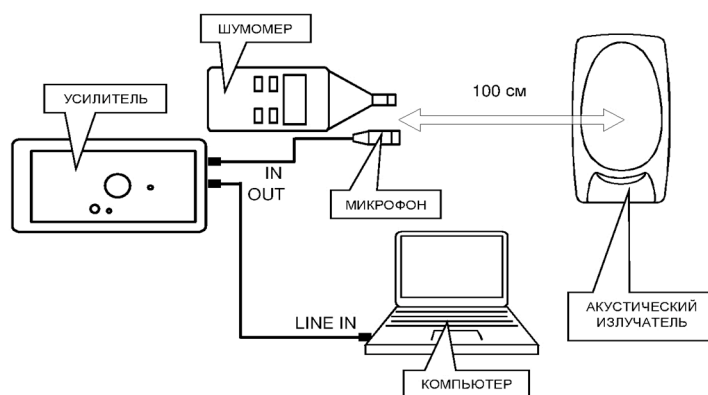
1. Изучить теоретический материал методики работы с аппаратно-программным комплексом виброакустической защиты VNK–012GL.

2. Провести калибровку аппаратно-программного комплекса виброакустической защиты VNK–012GL.

Для входа в режим калибровки необходимо запустить программу "Форманта" и выбрать пункт "Калибровка" в основном меню. Калибровка изделия производится в следующей последовательности:

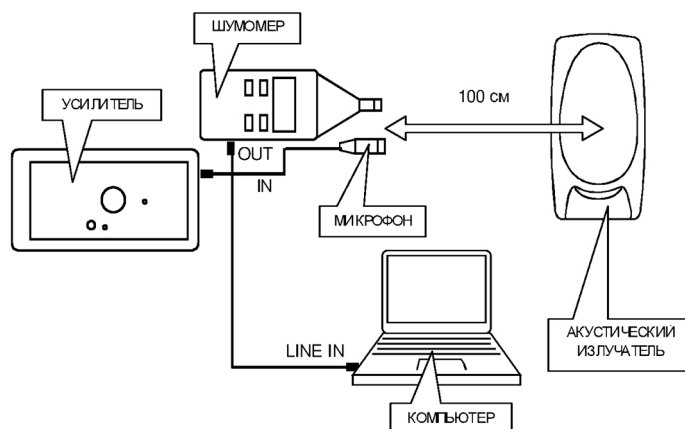
- 2.1. После запуска режима "Калибровка", вместе с текстовым окном откроется панель воспроизведения микшера Windows. На этой панели установите флажок "Выключить" для линейного и микрофонного входов.
- 2.2. Перейдите к панели записи микшера, выбрав следующие органы управления:  
ПАРАМЕТРЫ;  
СВОЙСТВА;  
ЗАПИСЬ;  
ОК.
- 2.3. Выберите на панели записи "ЛИНЕЙНЫЙ ВХОД" установите флажок "ВЫБРАТЬ".
- 2.4. Установите на выбранном входе ненулевой уровень с помощью движка.
- 2.5. Закройте панель микшера.
- 2.6. Нажмите клавишу "Далее". Откроется окно анализатора спектра.
- 2.7. В окне анализатора спектра нажмите кнопку  "УСТАНОВКИ" либо клавишу F3.
- 2.8. На панели "УСТАНОВКИ" под заголовком "Зв.карта" откройте верхний выпадающий список и выберите в нем пункт, относящийся к регулировке записи.
- 2.9. Откройте следующий выпадающий список и выберите пункт, соответствующий используемому входу звуковой карты ("ЛИНЕЙНЫЙ").
- 2.10. Откройте выпадающий список "КОРРЕКЦИЯ" и выберите режим "FLAT".
- 2.11. Введите в поле "СРЕДНЕЕ" количество отсчетов уровня, подвергающихся скользящему усреднению при нажатии клавиши F6.
- 2.12. Закройте панель "УСТАНОВКИ".
- 2.13. Движок регулятора уровня сигнала установите в ненулевое положение.
- 2.14. Закройте окно анализатора спектра.

- 2.15. Соберите измерительную схему, согласно рисунка 1.
- 2.16. Установите органы управления в следующие положения.  
На акустическом излучателе SI-3100:  
переключатель "дБ" – "90";  
выключатель "POWER" – "OFF";  
регулятор "Гц" – "СТАРТ".  
На шумомере:  
переключатель "POWER" – "OFF";  
переключатель "DB" – "50-100";  
переключатель "WEIGHTING" – "C";  
переключатель "RESPONSE" – "S".
- 2.17. Поместите акустический излучатель в центре проверяемого помещения на высоте приблизительно 1,5 м от пола. Расстояние от ограждающих конструкций и предметов интерьера помещения должно быть не менее одного метра.
- 2.18. Подключите выход "OUT" усилителя к входному разъему звуковой карты компьютера. Для подключения используйте кабель из комплекта изделия.
- 2.19. Установите микрофон шумомера на расстоянии  $(100 \pm 3)$  см от акустического излучателя по оси излучения.
- 2.20. Присоедините измерительный микрофон к микрофону шумомера.



**Рис. 1.** Схема калибровки (первое измерение)

- 2.21. На усилителе переключатель "LEVEL" переведите в положение "0 дБ".
- 2.22. Включите питание усилителя.
- 2.23. Включите шумомер и акустический излучатель.
- 2.24. С помощью органов управления акустического излучателя установите интегральное значение уровня звукового давления равное  $(94 \pm 1)$  дБ. Уровень контролируйте по шумомеру.
- 2.25. В окне программы "Форманта" нажмите кнопку "Далее". Откроется окно анализатора спектра.
- 2.26. В окне анализатора спектра регулятором "УРОВЕНЬ СИГНАЛА", расположенном в нижнем правом углу, установите уровень сигнала примерно 80 % от максимального.
- 2.27. Проведите измерение, нажав кнопку "ОК" в окне анализатора спектра.
- 2.28. Не выключая акустического излучателя, отключите усилитель от входного разъема звуковой карты и подключите вместо него шумомер (см. рис. 2).



**Рис. 2.** Схема калибровки (второе измерение)

- 2.29. В окне программы "Форманта" нажмите кнопку "Далее". Откроется окно анализатора спектра.
- 2.30. Проведите измерение, нажав кнопку "ОК" в окне анализатора спектра.
- 2.31. Выключите акустический излучатель, шумомер и усилитель.
- 2.32. В окне программы "Форманта" нажмите кнопку "Готово".

Операция калибровки завершена. После проведения калибровки положения органов управления на акустическом излучателе и микшере Windows не изменять.

### 3. Провести оценку звукоизоляции проверяемого помещения

- 3.1. Введите исходные данные для проверяемого помещения:  
 Название объекта;  
 Название проверяемого помещения;  
 Название соседнего помещения.
- 3.2. Выберите вид частотного анализа (октавный) и верхнюю границу частотного диапазона (5.6 кГц).
- 3.3. Нажмите кнопку "Далее".
- 3.4. Соберите измерительную установку согласно схеме (рис. 3).

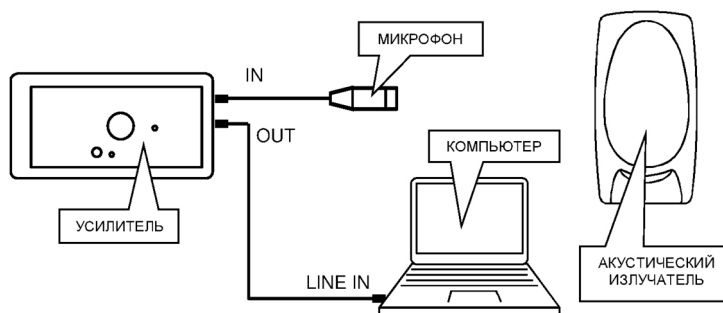


Рис. 3. Схема измерений при оценке звукоизоляции

- 3.5. Установите органы регулировки в следующие положения:  
 на акустическом излучателе:  
 переключатель "дБ" – "90";  
 выключатель "POWER" – "OFF".  
 на предварительном усилителе – переключатель "LEVEL" – "0".
  - 3.6. Разместите акустический излучатель в центре проверяемого помещения на высоте приблизительно 1,5 м от пола. Расстояние от ограждающих конструкций и предметов интерьера помещения должно быть не менее одного метра.
  - 3.7. Установите микрофон измерительного комплекса в контрольной точке внутри основного помещения на расстоянии не менее 1,5 метров от ограждающих конструкций и предметов интерьера помещения.
  - 3.8. Включите акустический излучатель и усилитель.
  - 3.9. Установите на усилителе максимально возможный уровень усиления путем перевода переключателя "LEVEL" по часовой стрелке до момента загорания светодиода "OVERLOAD" и возвращения его на одну позицию назад.
  - 3.10. Нажмите кнопку "Далее". Откроется окно анализатора спектра.
  - 3.11. Введите показания переключателя "LEVEL" в поле ввода, расположенного в окне "дБ" анализатора спектра.
  - 3.12. Не ранее, чем через 5–6 секунд завершите измерение, нажав кнопку "ОК" в окне анализатора спектра. При этом автоматически производится измерение усредненных значений уровня.
  - 3.13. Выключите акустический излучатель.
  - 3.14. После завершения измерения на экране появится таблица "Уровни акустического сигнала". В таблице отражены:  
 – название объекта и основного помещения;  
 – номер контрольной точки КТ №...;  
 – значения уровней сигнала в контрольных точках основного помещения  $L_{1i}$  в частотных полосах;  
 – усредненные по точкам значения уровней сигнала в основном помещении  $L_{1,cp,i}$  в частотных полосах.
- При необходимости удаления данных какой-либо контрольной точки необходимо выделить соответствующий столбец нажатием правой кнопки мыши и подтвердить удаление столбца. Измерения в соответствующей контрольной точке можно провести повторно, используя режим "Переход к новой точке", при этом номер контрольной точки следует ввести вручную.
- 3.15. При необходимости продолжения измерений в основном помещении в следующей контрольной точке нажмите кнопку "Переход к новой точке" и повторите п.п. 3.7–3.12.

- 3.16. Для проведения измерений в соседнем помещении нажмите кнопку "В соседнее помещение". В открывшемся окне введите или подтвердите название соседнего (по отношению к основному) помещения, в котором будут проводиться дальнейшие измерения.
- 3.17. Перейдите в соседнее помещение.
- 3.18. Установите микрофон измерительного комплекса в контрольную точку соседнего помещения.
- 3.19. Установите на усилителе максимально возможный уровень усиления путем перевода переключателя "LEVEL" по часовой стрелке до момента загорания светодиода "OVERLOAD" и возвращения его на одну позицию назад.
- 3.20. Нажмите кнопку "Далее". Откроется окно анализатора спектра.
- 3.21. Введите показания переключателя "LEVEL" в поле ввода, расположенного в окне "дБ" анализатора спектра.
- 3.22. Не ранее, чем через 5–6 сек завершите измерение, нажав кнопку "ОК" в окне анализатора спектра.
- 3.23. Не изменяя положения микрофона в выбранной контрольной точке соседнего помещения, включите акустический излучатель в основном помещении.
- 3.24. Установите на усилителе максимально возможный уровень усиления путем перевода переключателя "LEVEL" по часовой стрелке до момента загорания светодиода "OVERLOAD" и возвращения его на одну позицию назад.
- 3.25. Нажмите кнопку "Далее". Откроется окно анализатора спектра.
- 3.26. Не ранее чем через 5–6 сек завершите измерение, нажав кнопку "ОК" в окне анализатора спектра.
- 3.27. После измерения на экране появится таблица "Значение звукоизоляции между помещениями ...". В таблице отражены:
  - название основного и соседнего помещений;
  - номер контрольной точки КТ № ...;
  - усредненные значения уровней сигнала в основном помещении  $L_{1,cp,i}$  в частотных полосах;
  - уровень акустических помех в данной контрольной точке  $L_{шп}$  в частотных полосах;
  - значения уровней сигнала в контрольных точках соседнего помещения  $L_{2i}$  в частотных полосах;
  - разность усредненных значений уровней сигнала в основном помещении и уровня сигнала в контрольной точке данного соседнего помещения  $L_{1,cp,i} - L_{2i}$ .
 Вычисление уровней сигнала в контрольной точке  $L_{2i}$  в каждой частотной полосе осуществляется с учетом уровней фона  $L_{шп}$ . При условии  $L_{2i} - L_{шп} \leq 0$  дБ рассчитанные значения помечаются звездочкой, а значения уровней сигнала принимаются равными:  $L_{2i} = 10$  дБ.
- 3.28. Нажмите клавишу "Далее". На экране появится меню:
  - Продолжить измерения в следующей контрольной точке текущего соседнего помещения.
  - Перейти в новое соседнее помещение (для текущего основного).
  - Закончить измерения.
- 3.29. Для перехода в основное меню или при проведении измерений в новом основном помещении воспользуйтесь командой "Закончить измерения".
- 3.30. По результатам проведения оценки звукоизоляции помещения составить отчет в виде таблицы. Полученный отчет прикладывается к отчету о выполнении лабораторной работы.

## 7. Контрольные вопросы:

1. Что входит в состав комплекса виброакустической защиты VNK-012GL?
2. Основные функции, выполняемые аппаратно-программным комплексом виброакустической защиты VNK-012GL.
3. Какие параметры фиксируются при измерениях?
4. Какие параметры используются для оценки эффективности утечки информационного речевого сигнала?
5. Что собой представляет акустический излучатель SI-3100 и для чего он предназначен?
6. Что такое предварительный усилитель AA-012GL и его функция?
7. Для чего используется шумомер АТТ-9000?
8. Что входит в состав комплекта приемных датчиков и их функции?
9. Перечислите основные этапы режима калибровки.
10. Что позволяет делать режим оценки виброизоляции?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** Федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ» (КНИТУ-КАИ), И.В.Аникин, Г.С. Корнилов, gskornilov@kai.ru

**Образовательная программа:** 10.05.02. Информационная безопасность телекоммуникационных систем / Системы подвижной цифровой защищенной связи; 10.03.01. Информационная безопасность / Комплексная защита объектов информатизации.

**Дисциплина:** Техническая защита информации.

### **Лабораторная работа.**

#### **Поиск радиозакладных устройств в контролируемом помещении**

##### **1. Учебные цели:**

Теоретическое изучение технических характеристик и функциональных возможностей приемника «Скорпион» и функционального генератора «Импульс-2» для обнаружения и подавления устройств скрытого съема информации в сетях связи; выработать практические навыки для использования данных приборов при проведении поисковых работ.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- Уметь определять возможные каналы утечки информации в помещении
- Владеть навыками развертывания стандартных технических средств защиты

##### **3. Перечень материально-технического обеспечения**

**Лабораторное оборудование и программное обеспечение:** широкополосный приемник «Скорпион 3.5», функциональный генератор «Импульс-2».

##### **4. Задание на исследование**

- Ознакомиться с инструкцией к приемнику и имитатору, с руководствами по их эксплуатации.
- Выполнить сканирование по частоте в рабочем диапазоне приемника.
- Исследовать режимы работы приемника, оценить чувствительность и точность измерения.
- Использовать в качестве радиозакладки прибор «Импульс-2».
- Осуществить поиск радиозакладки в контролируемом помещении.
- Сформировать прицельную помеху для нейтрализации радиозакладки.

##### **5. Краткие теоретические сведения**

Изучаются по ссылкам:

1. Скоростной поисковый приёмник «СКОРПИОН 3.5» [Электронный ресурс]. Режим доступа : <http://www.bnti.ru/des.asp?itm=5298&tbl=04.01.01.04>.
2. Методы поиска радиозакладных устройств [Электронный ресурс]. Режим доступа : <http://project-mega.narod.ru/system/raznoe/zakladka.htm>

##### **6. Порядок выполнения лабораторной работы (этапы)**

Скоростной поисковый приемник радиосигналов «Скорпион» является портативным средством радиотехнического контроля. Он предназначен для автоматического обнаружения сигналов, излучаемых нелегальными передатчиками, и подавления каналов их приема. Подавление осуществляется путем постановки на выявленной частоте прицельной помехи.

Генератор «Импульс-2» используется для имитации работы средств съема и передачи информации. Он необходим для проверки работоспособности поисковых приборов, при проведении поисковых мероприятий, для оценки защищенности помещений и для подготовки специалистов-операторов поисковой техники. Прибор воспроизводит физические процессы, сопровождающие утечку информации по различным каналам, и позволяет провести их объективную оценку.

Внешний вид приборов показан на рисунке 1.



**Рис. 1.** Внешний вид приборов («Скорпион» – слева, «Импульс-2» – справа)

Основные технические характеристики приемника:

- Диапазон принимаемых частот – 30 МГц – 2 ГГц.
- Чувствительность – 50 мкВ – 1 мВ.
- Полоса пропускания на промежуточной частоте – 200 кГц.
- Точность измерения частоты – 10 кГц.
- Количество запоминаемых обнаруженных сигналов – 256.
- Количество исключаемых каналов приема – 4850.
- Мощность прицельной помехи в диапазоне 30 – 1000 МГц не менее 50 мВт.

Генератор «Импульс-2» обеспечивает работу в следующих режимах:

Акустический канал:

- имитация микрофонного эффекта электронного оборудования;
- оценка прохождения звуковых сигналов по вентиляционным каналам, сквозным щелям, трещинам и нарушениям уплотнителей, по структуре ограждающих конструкций и инженерных коммуникаций;
- озвучивание помещений для идентификации средств подслушивания;
- имитация работы средств передачи акустических сигналов в проводных коммуникациях.

Проводной канал (обесточенные линии, сеть переменного тока, абонентские телефонные линии и т. п.):

- имитация работы средств передачи сигналов в проводных коммуникациях;
- имитация работы устройств, использующих процесс навязывания.

Канал инфракрасного излучения:

- имитация работы устройств, использующих в качестве канала передачи ИК-диапазон.

Радиоканал:

- имитация излучения радиочастотных средств подслушивания;
- имитация работы переизлучателей частоты с модуляцией акустическим колебанием.

Подготовить прибор к работе:

Включите питание прибора, повернув регулятор громкости до появления характерного щелчка выключателя. На ЖКИ отобразится тестовая надпись «Скорпион» с указанием версии используемой программы, а радиоприёмник будет настроен на радиостанцию «Радио Мария» на частоте 102,9 МГц. Регулятором громкости установите уровень выходного сигнала устройства (если сигнала нет, вращением ручки «Порог» добиться его появления).

В левом верхнем углу ЖКИ отображается значок Y или YY, обозначающий количество приемных антенн. Для изменения – выключите питание ручкой регулятора громкости, нажмите одновременно кнопки «Режим» и «Поиск», снова включите прибор, отпустите кнопки и после появления на экране надписи – ПРИЕМНЫХ АНТЕНН: 1 или 2 – выберите нужный режим работы, который сохраняется при выключении питания.

К пункту 4.2. В режиме работы с одной антенной осуществить сканирование в рабочем диапазоне приёмника:

Нажмите кнопку «ПОИСК» (правая открытая)

○ □ □ ■  
Сброс Режим Память Поиск

На экране появится надпись:

ИСКЛЮЧЕНО: ...

ОБНАРУЖЕНО: ...

Через 2 секунды появится первое, также называемое предварительным, меню из 4 режимов, появляющихся на ЖКИ друг за другом слева направо.

○ ■ □ □  
Стирание памяти Сканирование Набор частоты Установка порога

Активизация каждого режима осуществляется путём нажатия соответствующей кнопки, на которую указывает стрелка на ЖКИ.

Примечание: при пониженном напряжении питания на экране на 2 секунды появляется надпись: «Батареи разряжены».

Повторить предыдущий пункт для режима работы с двумя антеннами (выбор двух антенн описан в пункте 1).

Установите порог обнаружения разности уровней в пределах 0...7 делений шкалы, что соответствует примерно 0...20 дБ (это осуществляется регулятором «ПОРОГ») и нажмите кнопку «Поиск». Установленный порог сохраняется при выключении питания. Минимальное значение порога обнаружения зависит от уровня электромагнитных излучений в месте работы, длины и типа используемой антенны. Вернитесь в режим работы с одной антенной.



Примечание: при работе с двумя приемными антеннами случае остановка производится при превышении разницы уровней сигналов запрограммированного порога или при отсутствии обнаружения на второй антенне.

К пункту 4.3. В режиме работы с одной антенной осуществить АВТОЗАПИСЬ и АВТОИСКЛЮЧЕНИЕ в рабочем диапазоне частот. Проконтролировать наличие ОБНАРУЖЕННЫХ, ИСКЛЮЧЕННЫХ каналов в выбранном ранее буфере.

Нажмите кнопку «Режим» в предварительном меню. На экране появится меню режимов сканирования, в котором для АВТОЗАПИСИ нажмите:

#### **АВТОЗАПИСЬ**

После входа в режим выберите диапазон сканирования – «У» – установленный диапазон частот (30...2000 МГц). После появления надписи РАБОТА С БУФЕРОМ выберите рабочий буфер памяти.

РАБОТА С БУФЕРОМ

**a b**

Для осуществления АВТОИСКЛЮЧЕНИЯ нажмите кнопку режим и затем:

•

#### **АВТОИСКЛЮЧЕНИЕ**

Появление надписи: «НЕ ИСКЛЮЧАЕТСЯ» свидетельствует о заполнении банка памяти.

Просмотр обнаруженных и исключенных каналов производится из предварительного меню нажатием кнопки «Поиск» и выбора режима ПРОСМОТР. Для выбора буфера памяти нажмите кнопку под соответствующим обозначением.

Очистите содержимое буферов, которые использовали. Для этого нажмите кнопку «Сброс» и осуществите стирание в каждом использованном буфере памяти.

Программирование произвольно выбранного участка диапазона.

Нажмите кнопку «Режим» → «АВТОЗАПИСЬ» → диапазон сканирования «П» программируемый участок диапазона. Также следует выбрать рабочий буфер памяти. Провести сканирование этого участка.

Повторить задание с двумя участками (запрограммировать и просканировать). В этом случае следует выбрать диапазон сканирования «ПП» – два программируемых участка диапазона.

Очистите содержимое буферов, которые были использованы.

К пункту 4.4. Подготовить прибор «Импульс-2» к работе. Включение его производится нажатием на клавишу Enter. Через некоторое время на экране появится меню, в котором необходимо задать параметры радиозакладки.

Осуществить сканирование при выключенных в аудитории сотовых телефонах. Установить порог чувствительности (см. выше пункт 4.3). Нажмите кнопку «Режим» → ПОИСК и выберите диапазон сканирования GD– диапазон стандартов GSM и DECT.

Осуществить сканирование при включенных в аудитории сотовых телефонах, но находящихся в спокойном режиме (методика аналогична).

Осуществить сканирование, когда один из сотовых телефонов находится в режиме вызова (методика аналогична). Сделать выводы.

К пункту 4.5. Установить на приборе «Импульс-2» параметры имитируемой закладки. Осуществить настройку на несущую частоту на приёмнике «СКОРПИОН». Возможны два варианта.

Автонастройка на данную частоту (см. выше пункт 3.3). Набор нужной частоты вручную.

В приёмнике предусмотрена возможность набора частоты настройки, для чего следует перейти в режим «Набор частоты». Для этого нажмите кнопку «ПОИСК» → «Режим» → «Набор частоты»

Сброс    Режим    Память    Поиск

Стирание памяти

Режим Набор частоты Установка порога и с помощью кнопки «ПОИСК» последовательно произведите набор цифр во всех разрядах, начиная со старшего. Настройки производятся после фиксации младшего разряда. Для повтора настройки нажмите кнопку «ПОИСК». Для выхода в меню нажмите кнопку «СБРОС».

К пункту 4.6. Установить на приемнике «Скорпион» вторую антенну и сформировать прицельную помеху для подавления радиозакладки. Осуществить блокирование выбранного радиодиапазона с помощью трехкратного нажатия кнопки «Режим», что приводит к переходу в режим ПЕРЕДАЧА. Изменить радиус блокирования радиодиапазона.

**7. Контрольные вопросы:**

1. Перечислить и охарактеризовать виды контроля для проведения аттестации помещений.
2. Назвать и описать основные признаки радиозакладок.
3. Характерные особенности широкополосного приемника «Скорпион»?
4. Какие частоты используют современные радиозакладки?
5. Перечислить конструктивные особенности закладных устройств.
6. Какие еще приемники можно применять при аттестации помещений?
7. Охарактеризовать режимы работы прибора «Импульс-2».

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** ФГБОУ ВО «Вятский государственный университет», составители Корепанов Александр Гаврилович, alkor47@yandex.ru, Трубин Игорь Сергеевич, i\_trubin@mail.ru

**СПЕЦИАЛИТЕТ 10.05.03**  
**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**  
**АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

**Дисциплина: Безопасность систем баз данных**

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем.

**Дисциплина:** Безопасность систем баз данных.

**Лабораторная работа.**

**Преобразование паролей для хранения их в приложении в преобразованном виде**

**1. Учебные цели:**

- Отработать вопросы создания подпрограмм преобразования (шифрования) паролей и включения их в динамически компокуемую библиотеку (DLL).
- Освоить применение паролей для защиты приложений от несанкционированного использования.

**2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- Уметь использовать возможности современных систем программирования для решения задач защиты баз данных и приложений для работы с данными.
- Владеть средствами языка программирования по разработке подпрограмм, помещаемых в динамически компокуемые библиотеки (DDL) приложений, использующих эти подпрограммы.

**3. Перечень материально-технического обеспечения**

Сеть персональных ЭВМ.

**4. Задание на исследование**

Разработать в среде Delphi процедуру или функцию, обеспечивающую преобразование пароля для работы приложения с целью хранения его в коде приложения в преобразованном виде. Виды преобразования приведены в табл. 1 (30 вариантов, для примера оставлен один вариант).

Включить разработанную подпрограмму в динамически подключаемую библиотеку (DDL).

Разработать приложение, использующее разработанную DDL. Работа с приложением должна обеспечиваться только при вводе правильного пароля. При вводе неправильного пароля должно выдаваться соответствующее сообщение.

**Таблица 1** – Виды преобразования пароля

| Вариант | Преобразование                                                                    |
|---------|-----------------------------------------------------------------------------------|
| 1       | Преобразование символов пароля с помощью операции Исключающее ИЛИ.<br>Ключ – ХЪЖЖ |

**5. Краткие теоретические сведения**

**5.1. Операции и стандартные подпрограммы для работы со строками**

Для выполнения первой части задания лабораторной работы следует использовать операции и стандартные функции для работы со строками.

Над строками определены операции присваивания «:=», конкатенации (сцепления) «+» и операции отношения (сравнения) «=», «<>», «>», «<», «>=», «<=».

В Delphi для работы со строками предусмотрены различные функции и процедуры, основные из них представлены в таблицах 2 и 3 соответственно.

**Таблица 2** – Стандартные функции для работы со строками

| Обращение               | Назначение                                          |
|-------------------------|-----------------------------------------------------|
| AnsiLowerCase(S)        | Все заглавные буквы строки S заменяются на строчные |
| AnsiUpperCase(S)        | Все строчные буквы строки S заменяются на заглавные |
| Concat(S1, S2, ..., Sn) | Сцепление строк S1, S2, ..., Sn                     |

|                     |                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------|
| Copy(S, Ind, N)     | Выделение из строки S подстроки длиной N символов, начиная с позиции Ind                    |
| Length(S)           | Определение текущей длины строки S                                                          |
| LowerCase(S)        | Все заглавные латинские буквы строки S заменяются на строчные                               |
| Pos(Substr, S)      | Определение номера позиции строки S, с которой начинается первое вхождение подстроки Substr |
| StringOfChar(Ch, N) | Создает строку, состоящую из N раз повторенного символа ch.                                 |
| UpperCase(S)        | Все строчные латинские буквы строки S заменяются на заглавные                               |

**Таблица 3** – Стандартные процедуры работы со строками

| Обращение          | Назначение                                                                                                                                                                                                                                                                                                                        |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delete(S, Ind, N)  | Удаление N символов из строки S, начиная с позиции Ind                                                                                                                                                                                                                                                                            |
| Insert(S1, S, Ind) | Вставка строки S1 в строку S, начиная с позиции Ind                                                                                                                                                                                                                                                                               |
| Str(X, S)          | Преобразование числового значения X в строку S. При задании числа X можно указывать формат X:m:n:<br>m – определяет общую ширину поля, выделенного под соответствующее символьное представление числа X;<br>n – количество символов в дробной части (этот параметр имеет смысл только в том случае, когда X – вещественное число) |

## 5.2. Создание и применение динамически компокуемых библиотек

Процедуры, функции, классы программиста можно объединить в один или несколько программных модулей, оформить их в виде динамически компокуемой библиотеки (Dynamic Link Library – DLL), а затем использовать *подпрограммы* библиотеки в *различных* приложениях, существенно экономя время их разработки.

Динамически компокуемая библиотека представляет собой исполняемый модуль Windows с расширением DLL, код и ресурсы которого могут использоваться различными приложениями и другими динамическими библиотеками.

Загрузка DLL-библиотеки в оперативную память осуществляется операционной системой Windows автономно от программ, поэтому одну и ту же библиотеку могут использовать несколько приложений.

Динамические библиотеки процедур и функций, разработанные в Delphi или в других системах программирования, загружаются в память лишь при необходимости. Они могут выгружаться из памяти, если потребность в них в данный момент отсутствует, но имеется необходимость использования других библиотек. В освободившуюся память могут загружаться другие библиотеки и приложения.

Динамически компокуемые библиотеки являются средством разработки приложений с использованием нескольких языков программирования.

**Структура DLL-библиотеки.** В общем случае исходный код для динамически компокуемой библиотеки имеет следующую структуру:

```

library <имя библиотеки>; {Желательно, чтобы имя библиотеки
совпадало с именем файла, в котором хранится библиотека}
uses
ShareMem, {Модуль ShareMem должен быть первым модулем,
указанным в операторе uses как в библиотеке, так
и в приложении, использующем эту библиотеку}
SysUtils, {Обеспечивает обработку исключительных ситуаций}
Classes, {Модуль содержит объявления основных классов
объектов, используемых в Delphi}
<имя модуля 1> in '<имя файла 1>.pas', {Модуль пользователя}
...
<имя модуля k> in '<имя файла k>.pas'; {Модуль пользователя}

exports
<имя подпрограммы 1> index <значение индекса 1>,
<имя подпрограммы 2> index <значение индекса 2>

```

```

name <имя подпрограммы 2 для экспорта>,
...
<имя подпрограммы i> index <значение индекса i >
<имя подпрограммы i для экспорта> resident,
<имя подпрограммы i+1> index <значение индекса i+1>,
...
<имя подпрограммы n> <значение индекса n >;

begin
end.

```

Модули, входящие в состав библиотеки, оформляются по обычным правилам, но при этом в интерфейсной части модуля к объявлению каждой подпрограммы, которая будет экспортироваться (использоваться приложениями), через символ «;» добавляется зарезервированное слово StdCall, например, function Ravn(a, b: real): real; stdcall;

Объявление процедур и функций с зарезервированным словом StdCall означает, что их предполагается вызывать из других приложений, в том числе, написанных на других языках программирования.

Раздел Exports включает в себя те процедуры и функции, которые должны экспортироваться DLL-библиотекой в другие приложения.

В теле динамической библиотеки могут быть объявлены типы, константы, переменные, процедуры, функции, классы и другие элементы, но экспортировать библиотека может только процедуры и функции.

**Создание DLL-библиотеки.** Создание DLL-библиотеки оформляется как проект специального вида и включает в себя два основных этапа:

1) собственно создание проекта, результатом компиляции которого будет динамическая библиотека, т.е. файл с расширением DLL;

2) формирование в составе проекта программных модулей, содержащих необходимые интерфейсные и реализационные части для подпрограмм библиотеки.

Все файлы проекта целесообразно хранить в отдельной папке, специально созданной для этой цели.

Для создания проекта необходимо выполнить следующие действия:

1) выбрать команду File|New|Other. В открывшемся окне диалога New Items на вкладке New выбрать значок с надписью DLL Wizard и нажать кнопку ОК. В результате Delphi создаст заготовку проекта для DLL-библиотеки вида:

```

library Project1;
uses SysUtils, Classes;
begin end.

```

2) указать в разделе Uses на первом месте модуль ShareMem, а в конце раздела надо перечислить имена модулей пользователя, которые должны быть созданы на следующем этапе;

3) включить в заготовку проекта после раздела Uses раздел Exports, в котором перечислить имена процедур и функций для экспорта. Как было отмечено выше, для подпрограмм можно указывать в явном виде значения индексов и имена для экспорта, являющиеся, по сути, псевдонимами, назначение которых обычно заключается в замене длинных имен подпрограмм более короткими при использовании в приложениях.

В инициализирующей части можно задать любые действия, которые будут выполнены при загрузке DLL-библиотеки в оперативную память;

4) сохранить проект в рабочей папке под каким-либо именем (файл с расширением DPR), при этом имя файла автоматически присвоится имени библиотеки.

Для создания в составе проекта программных модулей, содержащих подпрограммы будущей библиотеки, необходимо выполнить следующие действия:

1) выбрать команду File|New|Unit. В результате Delphi создаст заготовку для модуля;

2) включить в интерфейсную часть заготовки модуля объявления, а в реализационную часть – тексты процедур и функций, не забывая ставить зарезервированное слово stdcall после объявления каждой подпрограммы;

3) сохранить модуль в рабочей папке под именем, которое было указано в разделе Uses файла проекта библиотеки, при этом имя файла автоматически присвоится имени модуля;

4) повторить пункты 1–3 для других модулей.

После компиляции проекта в рабочей папке будет создан двоичный файл DLL-библиотеки с именем, под которым был сохранен проект, и расширением DLL.

Чтобы приложение могло найти библиотеку, ее надо переместить из места создания в папку приложения (менее желательный вариант) или в одну из системных папок, например C:\WINNT; C:\WINNT\System32; C:\WINNT\system; C:\Program Files\Borland\Delphi7\Bin; C:\Program Files\ Borland\Delphi7\Projects;

**Использование DLL-библиотеки.** Для обеспечения доступа какого-либо приложения к процедурам и функциям динамически подключаемой библиотеки в нем необходимо определить операцию импорта подпрограмм из библиотеки одним из двух способов:

- 1) с помощью директивы компилятора `external` (статический импорт);
- 2) вручную с использованием функций `LoadLibrary` и `GetProcAddress` (динамический импорт).

Наиболее удобным является статический импорт. В этом случае в разделе описаний исходного текста программы необходимо *объявить* процедуры и функции как внешние по отношению к приложению с указанием имени динамически вызываемой библиотеки:

```
procedure <имя процедуры> (список параметров с указанием их типов); stdcall; external 'имя_библиотеки.DLL' ;
```

```
function <имя функции> (список параметров с указанием их типов): <тип результата>; stdcall; external 'имя_библиотеки.DLL' ;
```

После этого процедуры и функции можно использовать так, как будто они описаны в самой программе.

## 6. Порядок выполнения лабораторной работы

1. Сначала создается проект приложения, в котором осуществляется прямое и обратное преобразования пароля, при этом операции преобразования оформляются как подпрограммы.
2. Подпрограмма прямого преобразования включается в динамически компоновемую библиотеку.
3. Создается приложение с минимальным набором функций, которое требует для работы ввода пароля.
4. Эталон пароля хранится в приложении в преобразованном виде. Вводимый пользователем пароль преобразуется подпрограммой из DLL. Сравнение введенного и эталонного паролей выполняется в преобразованном виде.

## 7. Контрольные вопросы

1. В чем суть шифрования с симметричным ключом?
2. Как можно защитить данные в базе данных от использования похитителями?

**Время на выполнение лабораторной работы – 2 часа.**

**Образовательная организация, авторы, эл. почта:** ВУНЦ ВВС «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж), Афанасьевский Леонид Борисович, [afleonid@yandex](mailto:afleonid@yandex); Будников Сергей Алексеевич, [buser@bk.ru](mailto:buser@bk.ru); Горин Александр Николаевич, [algorin.algoral@mail.ru](mailto:algorin.algoral@mail.ru)

## Дисциплина: Криптографические методы защиты информации

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, 10.03.01 Информационная безопасность.

**Дисциплина:** Криптографические методы защиты информации.

### **Лабораторная работа.**

#### **Частотные характеристики открытого текста**

##### **1. Учебные цели:**

Изучение основных частотных характеристик открытых текстов, позволяющих восстанавливать закодированные тексты на естественном языке и отличать их от зашифрованных.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- Уметь различать криптографические преобразования.
- Владеть стандартными навыками первичного криптографического анализа текстов.

##### **3. Перечень материально-технического обеспечения:**

- персональный компьютер,
- программа S1144 (распространяется свободно).

##### **4. Задание на исследование:**

Заданы фрагменты текстов на одном естественном языке. Текст содержит только буквы одного алфавита и знак «пробел». Для кодирования каждого фрагмента используется свой знаковый код. Размер фрагмента не менее 4000 знаков. Пример начала фрагмента:

ИdЦZRdПгПлы-  
ЦАvjcdцыПdRdvnЦdПRdПmzldRыПZsЦnvvZДлдXdПИЗCгncсПzdlцnRzdПИлнБылRZПsZZцгыцсгА  
MUdCПnЦZблдаыRRZyПRdПlnsПZsqdRZгncцПdRdvnЦdцZлПsИыццld.....  
.....

Необходимо:

1. Выбрать один фрагмент текста из файла «Варианты к Л1 КМ» в соответствии с порядковым номером студента в групповом журнале.
2. Определить язык исходного сообщения – русский или английский и среднюю длину слова.
3. Восстановить исходный текст на языке сообщения.
4. Письменно ответить на контрольный вопрос; номер вопроса выбрать в соответствии с порядковым номером студента в групповом журнале по модулю общего числа вопросов.

##### **5. Краткие теоретические сведения**

Шифром называется совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемое ключом и алгоритмом преобразования. Такие преобразования называются криптографическими. Ключ – это конкретное секретное состояние некоторых параметров криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма. Криптографические преобразования имеют две цели: обеспечить сокрытие смысла сообщения от лиц, не имеющих ключа; обеспечить обнаружение искажения исходной информации.

Установим различие между тремя способами преобразования информации: кодированием, шифрованием, тайнописью. Кодирование устанавливает взаимоднозначное соответствие между сигналом, несущим информацию о реальном физическом объекте, и его кодом. Следовательно, каждый раз, когда повторяется исходный объект, повторяется и его код. Закодированное сообщение полностью сохраняет семантику и свойства исходного сообщения. Шифрование устанавливает многозначное соответствие между объектом и его (шифро-) кодами, которое становится однозначным только при наличии ключа. Одному и тому же исходному объекту при шифровании соответствуют разные (шифро-) коды. Тайнопись – это невозпроизводимость части или всей информации при использовании стандартного для неё способа отображения. Например, если предполагается, что текст воспроизводится в лучах отраженного белого цвета, то не будут воспроизводиться сообщения, нанесённые термочернилами, краска, проявляющаяся в особых частях спектра, и т.д. Будем говорить, что шифрование вырождается в кодирование, если между кодами открытого текста и шифротекста существует взаимоднозначное соответствие. Будем говорить, что кодирование вырождается в копирование, если кодируемый объект и его код совпадают.

Будем в качестве объекта применения шифров рассматривать только тексты. Текст состоит из знаков, которые разделяются на знаки алфавита языка сообщения (называемые обычно буквами) и вспо-

могательные – пробел, цифры, знаки пунктуации и т.д. Термин знак, используемый и самостоятельно, является основой и других терминов – буква, символ, код, понимаемых в разных дисциплинах по-разному. В криптографии используют смешанную терминологию, в зависимости от однозначности понимания термина в каждом конкретном случае.

Алфавит  $A$  любого языка представляет собой множество упорядоченных кодов символов, обозначающих буквы этого языка. Буквы языка однозначно связаны с их порядковым номером в исходном алфавите, но могут быть представлены разными – в том числе неизвестными – знаками, и в то же время одинаковые знаки в разных текстах могут обозначать одну и ту же, но возможно неизвестную букву. Будем далее под символом понимать букву языка, код которой (значение) в исходном алфавите нам может быть заранее неизвестен.

Отсюда следует, что буква языка имеет значение, и это значение – порядковый номер (код) буквы в исходном алфавите. В текстах эта буква может быть представлена не одним, но разными знаками: заглавные и строчные буквы, прописные и печатные и т.д. Возможно даже, что буква имеет «размер», и представлена не одним, а некоторой последовательностью знаков. Будем для упрощения считать, что все буквы алфавита представлены одним одиночным знаком каждая. Тогда мощность алфавита языка  $N_A$  соответствует количеству букв алфавита и представляет начальную числовую характеристику для текстов на данном языке. Будем так же считать, что в текстах используется только один вспомогательный символ – пробел.

Математически это означает, что все слова текста представляют собой разделенные пробелом числа в  $N_A$  – ричной системе счисления, определяемой алфавитом  $A$ .

Первое, что можно определить по тексту  $T$  – это множество используемых в нем знаков  $AT$  и мощность этого множества  $N_{AT}$ , объем текста  $N_T$  как общее количество используемых в нем символов. Полагая, что на множестве  $AT$  существует некоторое упорядочение, можно говорить об алфавите текста  $AT$ . Сопоставляя значение  $N_{AT}$  с известными значениями мощности алфавитов различных языков, при определенных условиях можно сделать предположение о принадлежности  $T$  к конкретному языку. Для более точного определения языка текста можно использовать так называемый индекс совпадения. Он показывает вероятность того, что две случайно выбранные из текста буквы совпадают. Другие характеристики, которые можно получить из текста – это число повторений сочетаний знаков в тексте – так называемых  $(k)$ -грамм. В общем случае это сочетание  $(k)$  элементов: знаков, слов, предложений и т.д. Но мы будем использовать термин  $(k)$ -граммы только для знаков и символов. Тогда (1) –граммы (униграммы) – это число повторений одиночных символов текста, (2) – граммы (называемые биграммами) – число повторений сочетаний пар символов, (3) –граммы (триграммы) – число повторений трехсимвольных цепочек и т.д. Обычно их называют частотными характеристиками, т.к. их легко привести к частотной форме.

Число повторений сочетаний знаков используется в различных методах частотного анализа текстов. Так, простое сопоставление числа повторений одиночных символов текста с известными эталонными значениями вероятности появления символов в текстах на некотором языке, которое легко осуществить методом упорядочивания, может дать начальное приближение при решении задачи восстановления простой замены букв. Однако погрешность такого приближения достигает 0.7 по символам даже при объемах текста свыше 350000 символов. То есть можно считать, что мы никогда не получим более 30 – 40 % % правильных букв при таком приближении. Более точную информацию о тексте можно получить, рассматривая частотные характеристики более высокого порядка, например, символьные биграммы.

Пусть, например, для русскоязычного текста, представленного в простой замене символов, у нас есть таблица биграмм, симметрично упорядоченная по числу появления символов в тексте. На основании этой таблицы при достаточном объеме текста можно идентифицировать следующие буквы текста (рис. 1–2).

1. Если разность сумм по строке первых 7 значений и остальных меньше нуля, то данный символ, скорее всего – гласный.

2. Первые 4 символа таблицы, для которых суммарное количество не нулевых биграмм по строке и столбцу больше, чем для других символов, представляют символы (О, Е, А, И).

3. Результат (2) сопоставляется с (1) для проверки, и символы, выделенные по критерию (2), переносятся (в случае необходимости) в начало таблицы с сохранением исходного взаимного упорядочения.

4. По столбцам таблицы выделяются первые два символа, для которых сумма первых 4-х значений по столбцу равна нулю – это символы (Б, Ы) или наоборот.

5. Начиная с 5-го символа, в таблице выделяется подматрица размером 10×10. Максимальное значение в этой подматрице определяет биграмму (и соответственно символы) (СТ).

6. Для выделенных ранее символов (О, Е, А, И) максимальное значение (значения) в строке будут появляться, скорее всего, для символа (О). Возможно, это значение будет идентифицировать биграмму (ОВ), возможно – (ОР).

7. Максимальное значение в столбце ранее идентифицированного символа (Б) (без учета ранее идентифицированного символа «Т»), скорее всего, указывает биграмму (ЛБ) – то есть символ (Л).

8. Среди всех диагональных значений наибольшее, скорее всего, указывает на биграмму (НН) – символ (Н).



4      7 – линия Δ      14 (Ы,Б)?      (Л)?

(О,Е,А,И)?      (СТ)?      (Н)? (ОВ,ОР)?

|   |    |    |    |    |    |    |    |     |    |    |    |    |    |    |    |    |    |    |    |   |    |    |    |    |    |    |    |   |    |   |   |   |
|---|----|----|----|----|----|----|----|-----|----|----|----|----|----|----|----|----|----|----|----|---|----|----|----|----|----|----|----|---|----|---|---|---|
|   | ж  | к  | й  | х  | у  | м  | л  | я   | а  | ц  | о  | р  | л  | с  | ч  | ш  | н  | г  | ц  | н | б  | д  | т  | г  | з  | р  | ы  | е |    |   |   |   |
| ж | 40 | 19 | 38 | 7  | 34 | 39 | 47 | 15  | 3  | 21 | 22 | 40 | 22 | 32 | 11 | 0  | 66 | 27 | 8  | 0 | 8  | 18 | 16 | 21 | 4  | 6  | 8  | 4 | 8  | 2 | 7 |   |
| к | 9  | 8  | 5  | 2  | 45 | 57 | 24 | 122 | 32 | 55 | 15 | 50 | 0  | 3  | 0  | 6  | 12 | 6  | 0  | 3 | 12 | 0  | 4  | 1  | 3  | 2  | 17 | 3 | 10 | 1 |   |   |
| й | 11 | 14 | 10 | 6  | 73 | 60 | 84 | 88  | 14 | 32 | 9  | 25 | 0  | 2  | 0  | 25 | 23 | 4  | 0  | 1 | 15 | 6  | 0  | 13 | 0  | 8  | 1  | 3 | 1  |   |   |   |
| х | 6  | 4  | 24 | 3  | 37 | 34 | 75 | 14  | 31 | 30 | 20 | 24 | 21 | 5  | 1  | 0  | 5  | 17 | 2  | 0 | 2  | 25 | 8  | 5  | 9  | 10 | 18 | 1 | 20 | 5 | 0 |   |
| у | 77 | 73 | 65 | 46 | 2  | 43 | 11 | 39  | 17 | 5  | 1  | 13 | 5  | 2  | 3  | 26 | 2  | 3  | 13 | 3 | 0  | 1  | 0  | 1  | 1  | 0  | 0  | 0 | 0  | 0 | 0 |   |
| м | 24 | 22 | 65 | 17 | 72 | 18 | 1  | 7   | 10 | 25 | 22 | 26 | 3  | 37 | 2  | 5  | 1  | 1  | 2  | 2 | 2  | 8  | 0  | 0  | 4  | 0  | 0  | 0 | 0  | 0 | 0 | 0 |
| л | 94 | 62 | 31 | 35 | 39 | 1  | 1  | 1   | 0  | 4  | 0  | 15 | 19 | 37 | 9  | 1  | 8  | 1  | 0  | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 4  | 1 | 0  | 0 | 0 |   |
| я | 46 | 81 | 54 | 84 | 35 | 0  | 6  | 1   | 0  | 2  | 3  | 1  | 0  | 19 | 3  | 0  | 10 | 0  | 1  | 0 | 1  | 0  | 1  | 0  | 1  | 2  | 0  | 4 | 0  | 5 | 0 |   |
| а | 27 | 26 | 31 | 78 | 17 | 27 | 9  | 3   | 10 | 9  | 16 | 5  | 3  | 2  | 1  | 24 | 0  | 2  | 4  | 0 | 1  | 0  | 2  | 1  | 0  | 0  | 0  | 0 | 0  | 0 | 0 |   |
| ц | 7  | 89 | 20 | 28 | 2  | 10 | 4  | 68  | 0  | 7  | 1  | 11 | 0  | 0  | 0  | 2  | 0  | 0  | 6  | 6 | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0 | 0 |   |
| о | 36 | 21 | 31 | 19 | 3  | 1  | 10 | 0   | 0  | 3  | 0  | 0  | 1  | 42 | 0  | 5  | 0  | 1  | 43 | 0 | 0  | 0  | 0  | 2  | 15 | 0  | 0  | 0 | 3  | 0 | 0 |   |
| р | 27 | 35 | 8  | 49 | 1  | 5  | 0  | 16  | 8  | 1  | 16 | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0 | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0 | 3  | 5 | 1 |   |
| л | 30 | 20 | 29 | 25 | 2  | 7  | 3  | 1   | 5  | 20 | 1  | 4  | 2  | 0  | 2  | 6  | 2  | 0  | 7  | 0 | 0  | 0  | 1  | 2  | 0  | 2  | 0  | 0 | 1  | 0 | 3 |   |
| с | 8  | 6  | 9  | 3  | 8  | 13 | 10 | 5   | 8  | 17 | 0  | 2  | 9  | 0  | 11 | 0  | 1  | 8  | 5  | 2 | 0  | 1  | 1  | 7  | 5  | 2  | 0  | 0 | 0  | 0 | 0 |   |
| ч | 6  | 28 | 20 | 24 | 0  | 2  | 5  | 1   | 1  | 5  | 24 | 5  | 7  | 2  | 4  | 1  | 0  | 0  | 3  | 0 | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0 | 0  | 0 | 0 |   |
| в | 7  | 2  | 19 | 2  | 15 | 5  | 2  | 0   | 12 | 13 | 4  | 3  | 13 | 0  | 4  | 0  | 0  | 1  | 0  | 0 | 1  | 6  | 16 | 5  | 0  | 1  | 0  | 0 | 0  | 0 | 0 |   |
| ш | 37 | 3  | 8  | 25 | 1  | 23 | 0  | 32  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 2  | 0  | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0 | 0 |   |
| н | 8  | 32 | 1  | 46 | 1  | 0  | 5  | 8   | 6  | 1  | 1  | 2  | 7  | 1  | 4  | 1  | 0  | 1  | 4  | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0 | 0 | 0 |
| г | 3  | 4  | 11 | 2  | 11 | 17 | 2  | 10  | 4  | 19 | 2  | 2  | 0  | 3  | 0  | 1  | 0  | 0  | 0  | 0 | 0  | 0  | 2  | 9  | 0  | 1  | 1  | 0 | 8  | 1 |   |   |
| з | 3  | 4  | 2  | 0  | 2  | 9  | 12 | 2   | 3  | 4  | 0  | 3  | 0  | 0  | 1  | 0  | 4  | 25 | 0  | 0 | 2  | 0  | 0  | 6  | 1  | 0  | 0  | 3 | 0  | 1 |   |   |
| р | 0  | 16 | 21 | 1  | 0  | 0  | 4  | 6   | 0  | 6  | 2  | 1  | 1  | 2  | 0  | 5  | 0  | 12 | 0  | 0 | 0  | 1  | 0  | 0  | 0  | 7  | 0  | 0 | 0  | 0 |   |   |
| ц | 6  | 2  | 5  | 0  | 1  | 7  | 3  | 2   | 3  | 5  | 24 | 4  | 1  | 0  | 0  | 0  | 2  | 6  | 1  | 0 | 2  | 0  | 0  | 0  | 0  | 0  | 1  | 0 | 0  | 0 |   |   |
| н | 6  | 9  | 1  | 10 | 1  | 3  | 1  | 6   | 7  | 13 | 0  | 2  | 0  | 0  | 0  | 3  | 0  | 2  | 0  | 1 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0 | 0 |   |
| б | 14 | 1  | 30 | 7  | 4  | 0  | 5  | 1   | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0 | 0 |   |
| д | 1  | 0  | 0  | 0  | 25 | 4  | 0  | 1   | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0 | 1  | 0  | 0  | 14 | 0  | 0  | 6  | 0 | 0  | 0 | 0 |   |
| т | 32 | 0  | 6  | 7  | 0  | 0  | 2  | 0   | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0 | 0 |   |
| г | 28 | 0  | 11 | 5  | 0  | 0  | 0  | 0   | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0 | 0 |   |
| з | 6  | 20 | 0  | 6  | 1  | 0  | 0  | 3   | 0  | 0  | 0  | 1  | 0  | 0  | 3  | 0  | 0  | 3  | 0  | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0 | 0 |   |
| р | 28 | 0  | 8  | 0  | 0  | 4  | 0  | 0   | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0 | 0 |   |
| о | 7  | 0  | 19 | 7  | 0  | 0  | 3  | 0   | 0  | 0  | 0  | 1  | 0  | 0  | 2  | 0  | 0  | 0  | 0  | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0 | 0 |   |
| е | 0  | 0  | 0  | 0  | 2  | 0  | 0  | 1   | 0  | 0  | 0  | 2  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0  | 0 | 0 |   |

Рис. 1

Таблица биграмм

|          |          |            |  |             |  |            |  |            |            |                                |  |          |
|----------|----------|------------|--|-------------|--|------------|--|------------|------------|--------------------------------|--|----------|
| <b>D</b> |          | $s_1$      |  | $s_{31}$    |  | $\Sigma^1$ |  | $K_1$      | $K_2^T$    | $\Sigma^3$                     |  | $\Delta$ |
| $d_1$    | $s_1$    | $b_{1,1}$  |  | $b_{1,31}$  |  | $m_1^1$    |  | $k_1^1$    | $k_1^2$    | $r_1 = k_1^1 + k_1^2$          |  |          |
| ...      | ...      | ...        |  | ...         |  | ...        |  | ...        | ...        | ...                            |  |          |
| $d_{31}$ | $s_{31}$ | $b_{31,1}$ |  | $b_{31,31}$ |  | $m_{31}^1$ |  | $k_{31}^1$ | $k_{31}^2$ | $r_{31} = k_{31}^1 + k_{31}^2$ |  |          |

|            |         |     |            |  |
|------------|---------|-----|------------|--|
| $\Sigma^2$ | $m_1^2$ | ... | $m_{31}^2$ |  |
|------------|---------|-----|------------|--|

|                      |         |     |            |  |
|----------------------|---------|-----|------------|--|
| <b>K<sub>2</sub></b> | $k_1^2$ | ... | $k_{31}^2$ |  |
|----------------------|---------|-----|------------|--|

специальная вставка:  
значения+транспонировать

Рис. 2

Пояснения к обозначениям рисунка 2.

$$d_i = b_{i,i}, \quad b_{i,i} = 0$$

$$m_i^1 = \sum_{j=1}^{31} b_{i,j}, \quad m_i^2 = \sum_{j=1}^{31} b_{j,i}$$

$$k_i^1 = \text{счётесли}(b_{i,j} > 0, j = \overline{1,31}), \quad k_i^2 = \text{счётесли}(b_{j,i} > 0, j = \overline{1,31})$$

$$\Delta_i = \sum_{j=1}^7 b_{i,j} - \sum_{j=8}^{31} b_{i,j}$$

Оценки (1) – (8) следует получать, предварительно обнулив значения диагональных биграмм в таблице и выделив их в отдельный вектор **D** (рис. 2). Все расчеты несложно проделать с помощью любого табличного процессора, в частности MS Excel, рекомендуемая начальная форма таблиц в котором предложена на Рис. 2. Использование частотных характеристик биграмм дает более точную, чем одиночные символы, но все же приближенную информацию о тексте. Для дальнейшего повышения точности анализа текста необходимо использовать частотные характеристики все более высоких порядков, в том числе частотные словари языков.

### 6. Порядок выполнения лабораторной работы (этапы)

1. Работа выполняется на основе частотного анализа заданного текста в соответствии с краткими теоретическими сведениями и другими доступными источниками. Термины «символ», «знак», «код» и «буква» в работе используются как эквивалентные. Для выполнения задания необходимо использовать программу s1144 и возможности пакетов Excel и Word. Программа s1144 подсчитывает повторы знаков и биграмм текста, помещенного в файл input.txt, индекс совпадения, а также производит замену знаков текста в соответствии с таблицей, помещенной в файл tab.txt. Замена производится по правилу: наиболее часто встречающийся знак в тексте заменяется на 1-й знак из таблицы, следующий по встречаемости – на 2-й и т.д. Если таблица пуста, то замен нет. Если знаков в таблице меньше, чем в

- тексте, то заменяются только они. При необходимости индивидуальной настройки программу s1144.cpp следует внести в Visual Studio и сформировать исполняемый модуль в своей рабочей папке.
- По условию задачи имеем текст достаточного объема, в котором используются все буквы алфавита, и только 2 возможных языка, заметно различающихся количеством букв алфавита. В этом случае начальное предположение о типе языка исходного сообщения для закодированного текста можно сделать на основе мощности множества используемых знаков. Это простой, но слабый критерий, нуждающийся в подтверждении. Для этого можно определить индекс совпадения и сравнить полученное значение с табличными значениями для русского и английского языков (0,0576 и 0,0662 соответственно). Определите значения индекса совпадения (с помощью программы s1144) для 4-х объемов своего текста: 100 % текста, 50 %, 25 % и <10 %. Результаты сведите в таблицу. С вопросом о языке сообщения непосредственно связан и вопрос о том, закодирован текст или зашифрован. Поясните, почему индекс совпадения не дает на него однозначного ответа.  
Количество слов в лабораторных фрагментах текста определяется количеством используемых в них исходно пробелов плюс единица (поясните почему). На основании этого определите формулу для подсчета средней длины слова и ее значение для заданного варианта.
  - Когда язык сообщения определен, можно приступить к восстановлению сообщения. Основные сложности, возникающие здесь, обычно связаны с недостаточным объемом текста, а также с тем, что вероятности появления некоторых букв совпадают. Объем текста, предложенный в задании (не менее 4000 знаков), достаточен для решения задачи. Для повышения эффективности работы рекомендуется использование биграмм в сочетании с логическим подбором перестановок. В последнем случае необходимо перенести таблицу биграмм, сформированную программой s1144 в MS Excel (используя вкладку ДАННЫЕ – инструмент ТЕКСТ ПО СТОЛБЦАМ), и организовать ее обработку в соответствии с рекомендациями, приведенными в кратких теоретических сведениях.  
Восстановление текста – неформальный процесс, реализуемый методом проб и ошибок. Программа s1144 поддерживает этот метод следующим образом. При каждом запуске, называемом сеансом, она позволяет пошагово переставлять (менять местами) неограниченное количество пар символов текущего алфавита закодированного текста относительно исходного алфавита файла tab.txt. Все шаги (перестановки) запоминаются только для текущего сеанса и сохраняются в файле output.txt. Если необходимо восстановить поиск решения с какого-то промежуточного шага, то алфавит в файле tab.txt следует переупорядочить в соответствии с упорядочением требуемого шага и первоначальной упорядоченностью алфавита закодированного текста по частоте. Для сохранения промежуточных данных после каждого сеанса использования программы s1144 необходимо переименовывать файл output.txt. Окончательно восстановленный текст и есть доказательство правильности всех предположений, сделанных на этапах 6.2 и 6.3.
  - Оформление результатов. Все необходимые для отчета данные переносятся в него из протоколов программы s1144 и дополняются комментариями.
  - Содержание отчета. Титульный лист, цель работы и задание. Текст фрагмента. Объем текста. Количество символов алфавита. Количество слов в тексте. Средняя длина слова. Таблица частот. Таблица индексов совпадений. Пошаговая таблица кодировок, примененных для заданного текста. Восстановленный текст. Контрольный вопрос и ответ на него.

## 7. Контрольные вопросы

1. Дайте определение шифра, ключа.
2. Чем шифрование отличается от кодирования?
3. Что такое тайнопись?
4. Для чего применяются шифры?
5. Что такое алфавит?
6. Какое значение имеет буква?
7. Что такое  $(k)$ -граммы?
8. Что такое индекс совпадения и как он вычисляется?
9. Как в закодированном тексте выделить с помощью биграмм:  
Буквы (О, Е, А, И);  
Буквы (Ь, Ы)  
Буквы (С, Т);  
Букву (Л);  
Букву (Н);  
Буквы (О, В).

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** Новосибирский государственный технический университет, кафедра защиты информации, к.ф.-м.н., доцент кафедры Котов Юрий Алексеевич, kotov@corp.nstu.ru.

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, 10.03.01 Информационная безопасность.

**Дисциплина:** Криптографические методы защиты информации.

### **Лабораторная работа.** **Шифры с открытым ключом. RSA**

#### **1. Учебные цели:**

Изучение шифров с открытым ключом на примере шифра RSA.

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- Уметь различать криптографические преобразования с симметричным и открытым ключом.
- Владеть стандартными навыками использования шифров с открытым ключом.

#### **3. Перечень материально-технического обеспечения:**

- персональный компьютер,
- программа 1\_3.exe (распространяется свободно).

#### **4. Задание на исследование:**

- Реализовать обмен ключами и шифротекстами в системе с открытым ключом.
- Зашифровать текст на закрытом ключе, полученный шифротекст повторно зашифровать на открытом ключе.
- Установить ограничение для ключа  $< 100$  и зашифровать и расшифровать текст.
- Письменно ответить на контрольный вопрос; номер вопроса выбрать в соответствии с порядковым номером студента в групповом журнале по модулю общего числа вопросов.

#### **5. Краткие теоретические сведения**

Появление систем шифрования с открытым ключом в конце 70-х годов 20 века обусловлено дороговизной традиционных систем секретной связи, построенных на основе симметричных шифров. Они используют для шифрования и расшифрования один и тот же ключ. Следовательно, организация такой связи предполагает предварительное распространение ключа по закрытому каналу связи между абонентами системы, что при массовом использовании шифрования и современных требованиях к смене ключей приводит на практике к барьеру сверхзатрат. Системы с открытым ключом используют 2 ключа: один для шифрования («общедоступный», «открытый»), другой («секретный», «закрытый») – для расшифрования информации, причем знание первого из них не дает никакой возможности узнать второй. Основой такой связи становится обмен открытыми ключами, а закрытый канал «исчезает» внутри абонентов вместе с секретными ключами. Несколько непривычно, так как «шифровки» пишут «только тебе», и, не имея открытого ключа другого пользователя, послать ему шифросообщение невозможно. Нельзя его и расшифровать, хотя вы только что сами его и зашифровали. Итак, шифруем «на чужом», а расшифровываем «на своем» ключе.

В основу таких методов положен принцип, предложенный К.Шенноном. Он предложил строить шифр таким образом, чтобы его раскрытие было эквивалентно решению математической задачи, превосходящей возможности современных ЭВМ. Иными словами, использовать при формировании шифров известную в теории алгоритмов проблему вычислительной неразрешимости. Тогда ключевым становится понятие «современных ЭВМ», в то время как метод решения (алгоритм, алгоритмическая разрешимость) объявляется известным. Наряду с принципом О.Керкгофса о несекретности алгоритма шифрования принцип вычислительной неразрешимости К.Шеннона образует основу построения современных алгоритмов шифрования.

Один из шифров с открытым ключом разработан в США начале 80-х годов 20 века и назван по первым буквам фамилий авторов (Rivest, Shamir, Adleman). Основан на задаче дискретной факторизации, т.е. на трудности разложения целого числа на простые сомножители. Напомним, что простыми называются числа, которые делятся только на единицу и на самих себя. Взаимно простыми называются числа, не имеющие общих делителей кроме единицы.

Протокол метода RSA заключается в следующем.

1. Выбираются два больших простых числа  $p$  и  $q$  и определяется  $N=p \cdot q$ .

Число  $N$  считается общеизвестным (открытым), числа  $p$  и  $q$  хранятся в секрете.

2. Пусть  $M=(p-1) \cdot (q-1)$ . Выбирается большое случайное целое число  $d$ , которое должно быть взаимно простым с числом  $M$ .

3. Определяется число  $e$  из условия  $(e \cdot d) \bmod M = 1$ .

4. Пусть  $(N, e)$  – открытый ключ,  $d$  – закрытый (секретный) ключ.

5. Пусть  $S$  – числовая форма шифруемых данных. Тогда для шифрования данных необходимо выполнить преобразование  $SS = S^d \bmod N$ , а для расшифрования:  $S = SS^e \bmod N$ .

6. Для корректной работы алгоритма необходимо выполнение условия  $1 < S < N$ .

Повсеместно в литературе относительно ключей RSA указывается, что  $N$  и « $e$ » используются как открытый ключ, а « $d$ » – как закрытый ключ. В то же время нет никаких математических и иных ограничений на выбор в качестве открытого ключа числа  $d$ , а закрытого – числа  $e$ . Ключ ( $e$  или  $d$ ) становится открытым только в момент своего опубликования, и в тот же момент второе число из пары ( $e$ ,  $d$ ) становится секретным ключом. Действительно,  $SS = SS^e \bmod N = S^{de} \bmod N = S^{ed} \bmod N$ . Т.е. можно шифровать и на ключе  $e$ , а расшифровывать – на  $d$ .

Алгоритм RSA – числовой, работает только с числами, причем формулируется обычно в десятичной системе. В то же время шифруются, как правило, символьные сообщения. Известно, что между символьной и числовой кодировками можно установить, причем не единственным образом, взаимно однозначное соответствие, то есть преобразовать любой текст в числовую форму и обратно. Перед шифрованием открытый текст разбивается на блоки одинаковой длины (алгоритм не требует этого, блочность связана с реализацией), и каждый блок представляется в числовой кодировке  $S$ . Нетрудно понять из условия п.б, что чем ближе  $N$  к максимально представимому в данной реализации числу, тем больше вариантов сообщений можно будет зашифровать с помощью алгоритма RSA.

Каждый блок текста шифруется одним и тем же ключом, и он может показаться «коротким» со всеми вытекающими отсюда последствиями. Однако стойкость шифров с открытым ключом определяется по-иному, чем стойкость шифров с симметричным ключом, и при наличии не менее 300 десятичных знаков о длине ключа можно не беспокоиться. Однако можно указать на условие, при котором шифрование с открытым ключом вырождается в кодирование. Если шифровать методом RSA каждый знак текста, то получим взаимно однозначное соответствие между кодами знаков исходного сообщения и кодами знаков шифротекста, то есть простую замену.

## 6. Порядок выполнения лабораторной работы (этапы)

1. Используемый для выполнения лабораторной работы программный комплекс «1\_3» имеет оконный интерфейс, в верхнем меню которого следует выбрать кнопку *Лаб2*. Для выполнения работы следует открыть два рабочих окна, в каждом из них сгенерировать ключи «хозяев» и затем обменяться ими.

Для этого в правой части окна имеются 3 поля: верхнее «Ключи» – для генерации ключей «хозяев», среднее «Пользователи» – для управления базой ключей, и нижнее – для ввода ключей «гостей» и изменения ранее введенных в базу ключей (как «гостей», так и «хозяев»).

Первоначально следует очистить базу, используя поле «Пользователи» и кнопки «-» или *Clear* слева. Затем в нижнем поле ввести свой уникальный идентификатор и кнопкой «+» поля «Пользователи» добавить его в базу.

На следующем шаге в поле «Ключи» сгенерировать  $N$ , нажав кнопку *Генератор*, и выбрать  $d$  из выпадающего списка (одновременно установится  $e$ ). Нажать кнопку *В\_базу*, после чего оба ключа будут сохранены для введенного ранее идентификатора, причем открытые ключи одновременно появятся и в нижнем поле. Оба ключа имеются только у «хозяина», им может быть только один и первый по порядку идентификатор в базе пользователей.

После этого необходимо обменяться ключами, используя нижнее поле, в которое вводится идентификатор пользователя из другого окна, его открытые ключи « $e$ » и « $N$ » (можно копировать), которые затем нажатием кнопки «+» в поле «Пользователи» добавляются в базу ключей.

Проверить правильность ввода ключей можно переключением идентификаторов пользователей в поле «Пользователи», сравнивая появляющиеся в нижнем поле открытые ключи с теми, которые установлены для «хозяев» в верхнем поле «Ключи».

После генерации ключей и обмена ими можно приступить непосредственно к шифрованию.

Входная и выходная информация представляется в трех эквивалентных формах:

- 1) символьной,
- 2) десятичных кодов символов, разделенных пробелами,
- 3) десятичных кодов двухбайтовых блоков, разделенных пробелами.

Входная информация вводится в любом из трех верхних полей в объеме не более 20 символов. Ввод подтверждается кнопкой *OK* справа от поля, при ее нажатии введенная информация одновременно отображается в оставшихся двух полях.

Выходная информация выводится в три нижних поля, аналогично входной. Передать ее на вход можно из любого поля, нажав кнопку *OT* справа от него, и затем подтвердив ввод нажатием *OK* в том же поле на входе. Рекомендуется во всех случаях передавать на вход числовую информацию из поля «Блоки 2 байта» (или «Блоки 1 байт», когда это необходимо).

После выбора абонента в поле «Пользователи» шифрование входной информации осуществляется нажатием кнопки *Зашифровать*. Если абонент находится в другом окне, следует скопировать полученные коды блоков шифротекста, используя стандартные средства операционной системы, и затем вста-

вить их в соответствующую входную строчку другого окна, подтвердив ввод нажатием кнопки *OK*. Затем нажать кнопку *Расшифровать* в появившемся окне для секретного ключа нажать кнопку *OK*. Если ключи настроены правильно и условия алгоритма не нарушены, на выходе появиться расшифрованный текст. Обмен зашифрованными сообщениями необходимо произвести в обе стороны.

2. Оформление результатов. Все необходимые для отчета данные переносятся в него из протоколов программы 1\_3.exe и дополняются комментариями.

3. Содержание отчета. Титульный лист, цель работы и задание. Текст фрагмента. Ключи и результат шифрования каждого этапа. Контрольный вопрос и ответ на него.

#### **7. Контрольные вопросы.**

1. В чем заключается отличие систем шифрования с открытым ключом от симметричных криптосистем.
2. Сформулируйте принцип Шеннона разработки криптографических алгоритмов.
3. Сформулируйте задачи: а) дискретной факторизации; в) дискретного логарифмирования.
4. Опишите способ установления взаимоднозначного соответствия между тестом и числом, используемый в 1\_3.exe.
5. Какая задача положена в основу метода RSA.
6. Как формируются ключи в методе RSA, какой из них называется открытым, а какой – закрытым.
7. Как осуществляется шифрование (расшифрование) в методе RSA.
8. Какое условие должно выполняться, чтобы шифрование осуществлялось корректно.
9. Является ли число  $e$ , удовлетворяющее условию  $ed=1(\text{mod } M)$  единственным.
10. Какие числа называются простыми.
11. У пользователей «А» и «В» по три ключа у каждого: своя пара и открытый ключ другой стороны. На каком из трех ключей они должны шифровать сообщения друг другу.
12. Вы зашифровали сообщение  $M$  для пользователя «В», используя RSA, и утратили  $M$ . Остался лишь шифротекст. Сможете ли Вы восстановить  $M$ .
13. Укажите условие, при котором метод RSA вырождается в систему кодирования.
14. Какие числа называются взаимопростыми.

**Время на выполнение лабораторной работы – 2 часа.**

**Образовательная организация, авторы, эл. почта:** Новосибирский государственный технический университет, кафедра защиты информации, к.ф.-м.н., доцент кафедры Котов Юрий Алексеевич, kotov@corp.nstu.ru

---

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, Обеспечение информационной безопасности распределенных информационных систем.

**Дисциплина:** Криптографические методы защиты информации.

### **Лабораторная работа.** **Шифр Цезаря. Частотный криптоанализ**

#### **1. Учебные цели:**

Ознакомиться с одноалфавитными шифрами подстановки. Получить практические навыки проведения криптоанализа для одноалфавитных шифров подстановки

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- I уровень: Уметь реализовывать криптографические алгоритмы. Владеть навыками использования вычислительной техники для решения задач криптографии.
- II уровень: Уметь реализовывать и взламывать криптографические алгоритмы. Владеть навыками использования вычислительной техники для решения задач криптографии и криптоанализа.

#### **3. Перечень материально-технического обеспечения**

**Лабораторное оборудование и программное обеспечение:** Microsoft Visual Studio 2017.

#### **4. Задание на исследование**

Программно реализовать шифр Цезаря с заданными характеристиками.

| Вариант | Алфавит                                               | Ключ                           |
|---------|-------------------------------------------------------|--------------------------------|
| 1       | Цифры                                                 | Вводится в диапазоне [0;10]    |
| 2       | Большие буквы английского алфавита                    | Вводится в диапазоне [11;20]   |
| 3       | Большие буквы русского алфавита                       | Вводится в диапазоне [21;30]   |
| 4       | Знаки препинания и спецсимволы                        | Вводится в диапазоне [31;40]   |
| 5       | Цифры, знаки препинания и спецсимволы                 | Вводится в диапазоне [41;50]   |
| 6       | Большие буквы русского и английского алфавитов        | Вводится в диапазоне [51;60]   |
| 7       | Большие и маленькие буквы английского алфавита        | Вводится в диапазоне [61;70]   |
| 8       | Большие и маленькие буквы русского алфавита           | Вводится в диапазоне [71;80]   |
| 9       | Цифры и большие буквы английского алфавита            | Вводится в диапазоне [-10;0]   |
| 10      | Цифры и большие буквы русского алфавита               | Вводится в диапазоне [-20;-11] |
| 11      | Знаки препинания и большие буквы английского алфавита | Вводится в диапазоне [-30;-21] |
| 12      | Знаки препинания и большие буквы русского алфавита    | Вводится в диапазоне [-40;-31] |
| 13      | Спецсимволы и большие буквы английского алфавита      | Вводится в диапазоне [-50;-41] |

Программно реализовать частотный криптоанализ для шифротекстов, зашифрованных шифром Цезаря.

## 5. Краткие теоретические сведения

Шифр подстановки – это метод шифрования, в котором элементы исходного открытого текста заменяются элементами зашифрованного текста в соответствии с некоторым правилом. Элементами текста могут быть отдельные символы, пары символов, тройки символов, комбинирование этих случаев и так далее.

Различают четыре типа шифра подстановки:

1. Одноалфавитный шифр подстановки (шифр простой замены) – шифр, при котором каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита.
2. Однозвучный шифр подстановки похож на одноалфавитный за исключением того, что символ открытого текста может быть заменен одним из нескольких возможных символов.
3. Полиграммный шифр подстановки заменяет не один символ, а целую группу.
4. Полиалфавитный шифр подстановки состоит из нескольких шифров простой замены. Каждый символ открытого текста заменяется с использованием одного конкретного шифра.

### Шифры простой замены

Шифр простой замены (простой подстановочный шифр, моноалфавитный шифр) – это класс методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифротекста. Само шифрование заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которой она генерируется.

Примеры шифров простой замены:

#### Атбаш

Атбаш – это шифр простой замены, использованный для еврейского алфавита и получивший отсюда своё название.

Правило шифрования состоит в замене  $i$ -й буквы алфавита буквой с номером  $n - i + 1$ , где  $n$  – это число букв в алфавите.

Шифр Атбаш для английского алфавита имеет вид:

Исходный алфавит: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Алфавит замены: Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

#### Шифр Цезаря

При шифровании каждая буква заменяется другой, отстоящей от нее в алфавите на фиксированное число позиций (рис. 1).

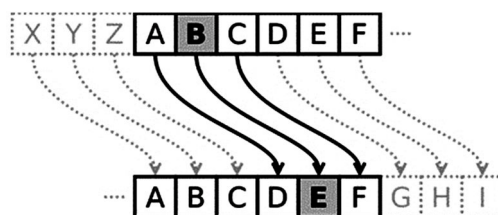


Рис. 1. Схема работы шифра Цезаря

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

$$y=(x+k) \bmod n$$

$$x=(y-k+n) \bmod n$$

где  $x$  – это символ открытого текста;  $y$  – символ зашифрованного текста;  $n$  – мощность алфавита;  $k$  – ключ.

Таким образом, шифр Цезаря является множеством, содержащим  $n$  подстановок.

#### *Пример*

Шифрование с использованием ключа  $k = 3$  открытого текста «Съешь же ещё этих мягких французских булок, да выпей чаю».

Исходный алфавит: А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Зашифрованный алфавит: Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В

Зашифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой зашифрованного алфавита. Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее. Зашифрованный текст имеет вид: «Фэзыя йз зы ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм ьгб».

#### **Шифр с использованием кодового слова**

Шифр с использованием кодового слова является одним из самых простых как в реализации, так и в расшифровывании. Идея заключается в том, что выбирается кодовое слово, которое пишется впереди, затем выписываются остальные буквы алфавита в своем порядке.

Шифр с использованием кодового слова WORD.

Исходный алфавит: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Алфавит замены: W O R D A B C E F G H I J K L M N P Q S T U V X Y Z

Можно использовать слово с повторяющимися буквами в качестве кодового слова, но только в том случае, если уберём из кодового слова лишние буквы, иначе это приведёт к неоднозначности расшифровки, то есть двум различным буквам исходного алфавита будет соответствовать одна и та же буква зашифрованного текста.

#### **Метод записи зашифрованных текстов**

По традиции, зашифрованный текст пишут блоками (другое название «группы») по 5 символов, не учитывая пунктуацию и пробелы. Это помогает избежать ошибок при передаче зашифрованного сообщения и позволяет скрыть границы слов в исходном тексте.

#### **Криптоанализ**

Выделяют 3 основных метода криптоанализа:

1. Атака на основе шифротекста;
2. Атака на основе открытых текстов;
3. Атака на основе подобранного открытого текста.

Рассмотрим криптостойкость шифров подстановки относительно данных методов.

#### *Атаки на основе шифротекста*

Моноалфавитные шифры легко вскрываются с использованием методов частотного анализа.

Криптоанализ однозвучных шифров подстановки осуществляется подсчетом частот появления пар и троек символов.

Для дешифровки полиалфавитных шифров применяется метод Касиски.

Полиграммный шифр Хилла может быть взломан при вычислении частот последовательностей символов.

#### *Атаки на основе открытых текстов*

При наличии открытого текста достаточной длины взлом моноалфавитных и однозвучных шифров является тривиальным.

Для быстрого взлома полиалфавитных шифров длина открытого текста должна превышать длину ключа.

#### *Атаки на основе подобранного открытого текста*

К атаке на основе выбранного открытого текста уязвимы все шифры подстановки.

Стандартный шифр Хилла, составленный из  $n$  линейных уравнений, может быть взломан по выбранному открытому тексту при перехвате криптоаналитиком  $n^2$  пар символов сообщения и шифротекста.

#### **Частотный криптоанализ**

Это один из методов криптоанализа, основывающийся на предположении о существовании не-тривиального статистического распределения отдельных символов и их последовательностей как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования.

Частотный анализ предполагает, что частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка. При этом, в случае моноалфавитного шифрования, если в шифротексте будет символ с аналогичной вероятностью появления, то можно предположить, что он и является указанной зашифрованной буквой. Аналогичные рассуждения применяются к биграммам (двубуквенным последовательностям), триграммам и т.д. в случае полиалфавитных шифров.

Утверждается, что вероятность появления отдельных букв, а также их порядок в словах и фразах естественного языка подчиняются статистическим закономерностям: например, пара стоящих рядом букв «ся» в русском языке более вероятна, чем «цы», а «оь» в русском языке не встречается вовсе. Анализируя достаточно длинный текст, зашифрованный методом замены, можно по частотам появления символов произвести обратную замену и восстановить исходный текст.

Важными характеристиками текста являются повторяемость букв (количество различных букв в каждом языке ограничено), пар букв, то есть  $m$  ( $m$ -грамм), сочетаемость букв друг с другом, чередование гласных и согласных, и некоторые другие особенности. Эти характеристики являются достаточно устойчивыми.

Идея состоит в подсчёте чисел вхождений каждой  $n^m$  возможных  $m$ -грамм в достаточно длинных открытых текстах  $T=t_1t_2\dots t_l$ , составленных из букв алфавита  $\{a_1, a_2, \dots, a_n\}$ . При этом просматриваются подряд идущие  $m$ -граммы текста:

$$t_1t_2\dots t_m, t_2t_3\dots t_{m+1}, \dots, t_{l-m+1}t_{l-m+2}\dots t_l.$$

Если  $L(a_{i_1}a_{i_2}\dots a_{i_m})$  – число появлений  $m$ -граммы  $a_{i_1}a_{i_2}\dots a_{i_m}$  в тексте  $T$ , а  $L$  – общее число подсчитанных  $m$ -грамм, то при достаточно больших  $L$  частоты  $L(a_{i_1}a_{i_2}\dots a_{i_m})/L$ , для данной  $m$ -граммы мало отличаются друг от друга в различных текстах.

В силу этого, относительную частоту считают приближением вероятности  $P(a_{i_1}a_{i_2}\dots a_{i_m})$  появления данной  $m$ -граммы в случайно выбранном тексте (такой подход принят при статистическом определении вероятности).

В общем случае частоту букв в процентном выражении можно определить следующим образом: подсчитывается, сколько раз она встречается в шифротексте, затем полученное число делится на общее число символов шифротекста; для выражения в процентах, полученный результат умножается на 100.

Частотность существенно зависит, однако, не только от длины текста, но и от его характера. Например, в техническом тексте обычно редкая буква Ф может появляться гораздо чаще. Поэтому для надёжного определения средней частоты букв желательно иметь набор различных текстов.

## 6. Порядок выполнения лабораторной работы

1. Изучить теоретический материал, представленный в лабораторной работе.
2. Оформить отчет о выполнении лабораторной работы письменно ответив на контрольные вопросы в тетради.
3. Программно реализовать шифр Цезаря и частотный криптоанализ для шифротекстов, зашифрованных шифром Цезаря с заданными характеристиками (согласно варианту лабораторной работы).

## 7. Контрольные вопросы:

1. Дайте определение шифру подстановки.
2. Опишите типы шифра подстановки.
3. Опишите шифр простой замены.
4. Опишите шифр Атбаш.
5. Опишите шифр Цезаря.
6. Опишите шифр с использованием кодового слова.
7. Опишите метод записи зашифрованных текстов.
8. Перечислите основные методы криптоанализа.
9. Опишите криптостойкость шифров подстановки.
10. Дайте определение частотному криптоанализу.
11. Опишите частотный криптоанализ.

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** ФГАОУ ВО «Волгоградский государственный университет», к.т.н., доцент кафедры информационной безопасности Никишова А.В., ассистент кафедры информационной безопасности Омельченко Т.А., nikishova.arina@volsu.ru



## Дисциплина: Криптографические протоколы

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, Защищенные информационные системы управления.

**Дисциплина:** Криптографические протоколы.

### Лабораторная работа.

#### Настройка средств криптографической защиты сетевого трафика стандартного протокола IPsec в операционной системе MS Windows

##### 1. Учебные цели:

Изучить возможности настройки средств криптографической защиты сетевого трафика стандартного протокола IPsec в операционной системе MS Windows, а также отработать навыки выполнения работ по установке, настройке, обслуживанию программных, программно-аппаратных (в том числе криптографических), технических средств защиты информации и контроля эффективности защиты информации.

##### 2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

###### Уметь:

- выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

###### Владеть:

- навыками выполнения работ по установке, настройке, обслуживанию программных, программно-аппаратных (в том числе криптографических), технических средств защиты информации и контроля эффективности защиты информации.

##### 3. Перечень материально-технического обеспечения:

- Специализированные классы учебного корпуса К 9: № 205, 215, 403.
- **Технические средства обучения:** мультимедийный проектор, ноутбук, экран для проекции, презентации отдельных лекций, практических занятий.
- **Лабораторное оборудование и программное обеспечение:**
  - krypt.exe;
  - Криптопротоколы.exe.

##### 4. Задание на исследование

**Цель:** научиться управлять защитой сетевого трафика с помощью средств стандартного протокола IPsec операционной системы Microsoft Windows 2008.

**Задание:** настроить протокол IPsec, согласно указанным параметрам.

##### 5. Краткие теоретические сведения

IPsec (сокращение от IP Security) – определенный IETF стандарт достоверной/конфиденциальной передачи данных по сетям IP. Чаще всего IPsec используется для создания VPN (Virtual Private Network).

IPsec является неотъемлемой частью IPv6 – Интернет-протокола следующего поколения, и расширением существующие версии Интернет-протокола IPv4. IPsec определен в RFC с 2401 по 2412.

Практически все механизмы сетевой безопасности могут быть реализованы на третьем уровне эталонной модели ISO/OSI в соответствии с рисунком 1. Кроме того, IP-уровень можно считать оптимальным для размещения защитных средств, поскольку при этом достигается удачный компромисс между защищенностью, эффективностью функционирования и прозрачностью для приложений.

| Уровни TCP/IP          | Уровни ISO/OSI                                    |
|------------------------|---------------------------------------------------|
| 4. Прикладных программ | 7. Прикладных программ<br>6. Представление данных |
| 3. Транспортный        | 5. Сеансовый<br>4. Транспортный                   |
| 2. Межсетевой          | 3. Сетевой                                        |
| 1. Доступа к сети      | 2. Канальный<br>1. Физический                     |

Рис. 1. Модель OSI/ISO



Определен стандартный набор алгоритмов по умолчанию для обеспечения интероперабельности. Использование этих алгоритмов совместно с защитой трафика на основе IPSec и протоколами управления ключа позволяет обеспечить высокую степень криптографической безопасности.

Алгоритмическая независимость протоколов имеет и оборотную сторону, состоящую в необходимости предварительного согласования набора применяемых алгоритмов и их параметров, поддерживаемых общающимися сторонами. Иными словами, стороны должны выработать общий контекст безопасности (Security Association, SA) и затем использовать такие его элементы, как алгоритмы и их ключи. SA подробно рассматривается далее. За формирование контекстов безопасности в IPSec отвечает особое семейство протоколов ISAKMP, которое рассматривается также в отдельном разделе.

Безопасность, обеспечиваемая IPSec, зависит от многих факторов операционного окружения, в котором IPSec выполняется. Например, от безопасности ОС, источника случайных чисел, плохих протоколов управления системой.

#### Размещение и функционирование IPSec

IPSec выполняется на хосте или шлюзе безопасности, обеспечивая защиту IP-трафика. Термин <шлюз безопасности> используется для обозначения промежуточной системы, которая реализует IPSec-протоколы. Защита основана на требованиях, определенных в Базе Данных Политики Безопасности (Security Policy Database- SPD), определяемой и поддерживаемой системным администратором. Пакеты обрабатываются одним из трех способов на основании соответствия информации заголовка IP или транспортного уровня записям в SPD. Каждый пакет либо отбрасывается сервисом безопасности IPSec, либо пропускается без изменения, либо обрабатывается сервисом IPSec на основе применения определенной политики.

IPSec обеспечивает сервисы безопасности на IP-уровне, выбирая нужные протоколы безопасности, определяя алгоритмы, используемые сервисами, и предоставляя все криптографические ключи требуемым сервисам. IPSec может использоваться для защиты одного или нескольких <путей> между парой хостов, между парой шлюзов безопасности или между шлюзом безопасности и хостом.

IPSec использует два протокола для обеспечения безопасности трафика – Authentication Header (AH) и Encapsulating Security Payload (ESP). Хотя бы один из этих сервисов должен быть задействован при использовании ESP.

Эти протоколы могут применяться как по отдельности, так и в комбинации с друг другом для обеспечения необходимого набора сервисов безопасности в IPv4 и IPv6. Каждый протокол поддерживает два режима использования: режим транспорта и режим туннелирования. В транспортном режиме протоколы обеспечивают защиту главным образом для протоколов более высокого уровня; в режиме туннелирования протоколы применяются для скрытия IP-заголовков исходных пакетов. Разница между двумя режимами рассматривается дальше.

IPSec позволяет системному администратору управлять детализацией, с которой предоставляется сервис безопасности. Например, можно создать единственный зашифрованный туннель между двумя безопасными шлюзами, или для каждого TCP соединения может быть создан зашифрованный туннель между парой хостов. IPSec позволяет указывать следующие параметры:

- а) какие сервисы используются, и в какой комбинации;
- б) необходимый уровень детализации применяемой защиты;
- в) алгоритмы, используемые для обеспечения безопасности на основе криптографии;

Существует несколько способов реализации IPSec на хосте или в соединении с роутером или firewall (для создания безопасного шлюза). Несколько общих примеров:

а) интеграция IPSec в конкретную реализацию IP, что требует доступа к исходному коду IP и применимо как к хостам, так и к шлюзам безопасности;

б) bump-in-the-stack (BITS) реализации, где IPSec действует <внизу> существующей реализации стека протоколов IP, между обычным IP и локальными сетевыми драйверами; доступа к исходному коду стека IP в данном контексте не требуется, что делает такой подход пригодным для встраивания в существующие системы, и реализации на хостах;

в) использование внешнего криптопроцессора (обычно в военных и в некоторых коммерческих системах), как правило, это является Bump-in-the-stack (BITS) реализацией, используется как на хостах, так и на шлюзах, обычно BITS-устройства являются IP-адресуемыми.

#### Транспортный режим работы

В этом варианте механизмы безопасности применяются только для протоколов, начиная с транспортного (TCP) уровня и выше, оставляя данные самого сетевого уровня (заголовок IP) без дополнительной защиты. Места размещения дополнительной информации, вставляемой протоколами в пакет, представлены в соответствии с рисунком 3.

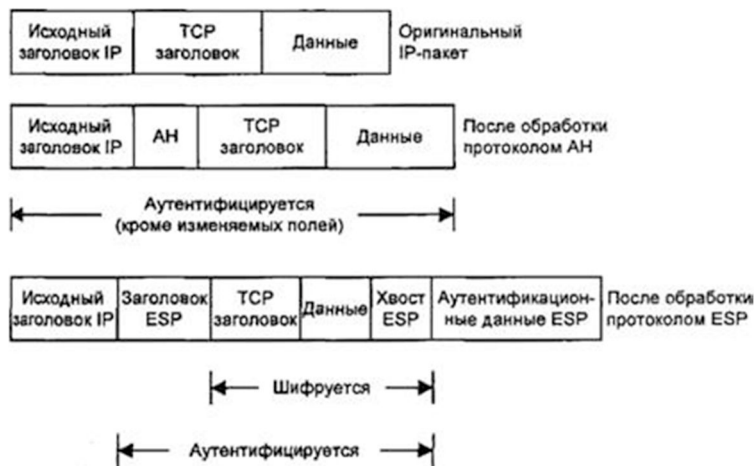


Рис. 3. Транспортный режим

### Туннельный режим работы

Этот режим интересен тем, что обеспечивает защиту также и данных сетевого уровня путем добавления нового IP-заголовка. После определения ассоциаций безопасности (например, между двумя шлюзами) истинные адреса хостов отправления и назначения (и другие служебные поля) полностью защищаются от модификаций для AH или вообще скрываются для ESP, а в новый заголовок выставляются адреса и другие данные для шлюзов (отправления/получения). В соответствии с рисунком 4 видны преимущества и недостатки обоих протоколов. ESP обеспечивает сокрытие данных, но не полную аутентификацию всего пакета. AH полностью аутентифицирует, но не скрывает данные. В этом причина того, что для обеспечения высокого уровня безопасности, применение протоколов совмещается.

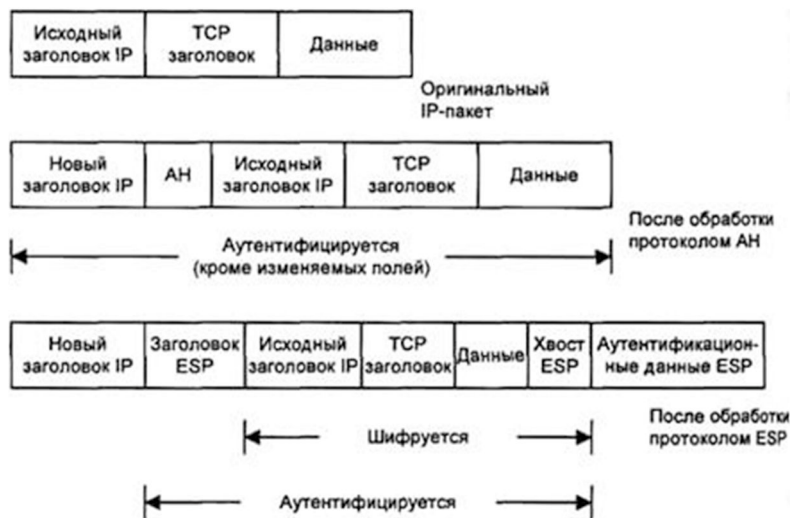


Рис. 4. Туннельный режим

### 6. Выполнение задания:

1. Для управления политикой безопасности IPsec с консоли управления Microsoft, выполните следующие действия.
2. Нажмите кнопку Пуск, выберите команду «Выполнить», введите MMC и нажмите кнопку ОК.
3. В меню консоль выбрать команду «Добавить» или «удалить оснастку» и нажать кнопку «Добавить».
4. Выбрать «Управление безопасностью IP-безопасности» и нажать «Добавить».
5. Выбрать Домен с Active Directory, политикой которого будем управлять и нажать «Готово».
6. Выбрать сервер безопасности – Secure Server (Require Server).
7. Указать общие настройки.
8. Указать используемые методы шифрования данных.
9. Определить правила и фильтры IPsec.
10. Выбрать действие фильтра – требуется безопасность (Require Security).
11. Тип подключения – все сетевые подключения.
12. Методы и проверки подлинности оставить прежним, чтобы избежать конфликтов.
13. Разрешить связь по протоколу http: нажать «Добавить».
14. Запустить Мастер создания новых правил.

15. Не определять туннель
16. В открывшемся окне фильтров нажать Добавить
17. Создать список фильтров IP, нажав кнопку Добавить.
18. Указать описание и нажали кнопку Далее.
19. В адресе источника пакетов указать свой IP адрес
20. В адресе назначения указали любой IP адрес (чтобы мы могли отправлять сообщения кому угодно).
21. Указали номер порта, используемый для протокола (для http – 80, для https – 443).
22. Завершим работу мастера, нажав кнопку Готово.
23. Проверить, что правило появилось в фильтре.
24. Разрешить (permit) передачу данных этому протоколу.
25. Перенастроить данное правило по заданию: подготовьте internet explorer для безопасной работы по порту 8080.

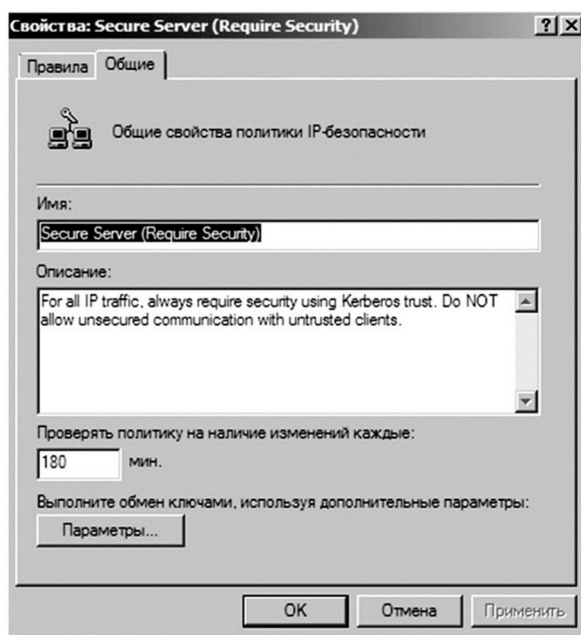


Рис. 5. Общие настройки Secure Server

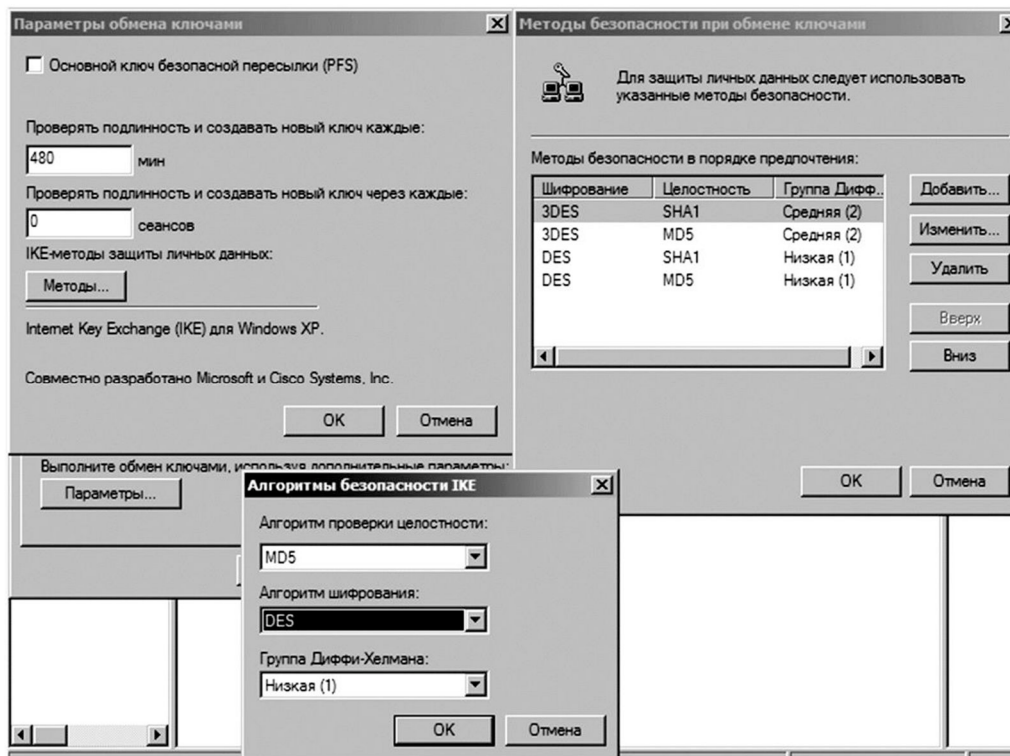


Рис. 6. Методы безопасности при обмене ключами

**Вывод:** В результате работы научились настраивать протокол IPsec стандартными средствами операционной среды MServer 2008.

**7. Контрольные вопросы:**

1. Перечислите возможности, предоставляемые IPsec:
2. Преимущества и недостатки IPsec.
3. Конкуренты IPsec
4. Типичные применения IPsec

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** КубГТУ, Осипенко Л.П., Osipenko\_l\_p@mail.ru

---

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, Защищенные информационные системы управления.

**Дисциплина:** Криптографические протоколы.

**Лабораторная работа.**  
**Протоколы с нулевым разглашением**

**1. Учебные цели:**

Изучить возможности криптографических протоколов, а также отработать навыки выполнения работ по установке, настройке, обслуживанию программных, программно-аппаратных (в том числе криптографических), технических средств защиты информации и контроля эффективности защиты информации.

**2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

**Уметь:**

- выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

**Владеть:**

- навыками выполнения работ по установке, настройке, обслуживанию программных, программно-аппаратных (в том числе криптографических), технических средств защиты информации и контроля эффективности защиты информации.

**3. Перечень материально-технического обеспечения:**

- **Специализированные классы** учебного корпуса К9: № 205, 215, 403.
- **Технические средства обучения:** мультимедийный проектор, ноутбук, экран для проекции, презентации отдельных лекций, практических занятий.
- **Лабораторное оборудование и программное обеспечение:**
  - Протокол Гиллу-Кискатра
  - Протокол Фиата-Шамира
  - Протокол Шнорра
  - Криптопротоколы.exe.

**4. Задание на исследование**

**Цель:** Изучить протоколы реализуются по двум схемам шифрования – RSA (протокол Фиата-Шамира и Гиллу-Кискатра) и Эль-Гамала (протокол Шнорра)

**5. Краткие теоретические сведения**

Доказательство с нулевым разглашением (информации) (англ. Zero-knowledge proof) – интерактивный вероятностный протокол, который позволяет доказать, что доказываемое утверждение верно, и Доказывающий знает это доказательство, в то же время, не предоставляя никакой информации о самом доказательстве данного утверждения. Протокол должен обладать тремя свойствами:

- **Полнота:** если утверждение действительно верно, то Доказывающий убедит в этом Проверяющего с любой наперед заданной точностью;

• **Корректность:** если утверждение неверно, то любой, даже «нечестный», Доказывающий не сможет убедить Проверяющего за исключением пренебрежимо малой вероятности;

• **Нулевое разглашение:** если утверждение верно, то любой, даже «нечестный», Проверяющий не узнает ничего кроме самого факта, что утверждение верно.

В данной лабораторной работе рассматриваются два протокола с нулевым разглашением: протокол Фиата-Шамира и протокол Шнорра.

### Примеры протоколов с нулевым разглашением

Протокол Фиата-Шамира – один из наиболее известных протоколов доказательства с нулевым разглашением, основанный на проблеме извлечения квадратного корня по модулю большого составного  $n$ .

Предварительный этап:

1. Доверенный центр  $T$  выбирает и публикует модуль схемы – число  $n$ , являющееся произведением двух больших простых чисел  $p$  и  $q$ .

2. Пользователь выбирает секретное  $S$  из интервала  $(1, n-1)$ , взаимно простое с  $n$ . Затем вычисляется открытый ключ  $V = s^2 \pmod{n}$ . Значение  $V$  регистрируется доверенным центром в качестве открытого ключа пользователя, а число  $S$  является его закрытым ключом.

Рабочий этап:

1.  $A$  выбирает случайно  $r$  из интервала  $(1, n-1)$  и отправляет  $B$  значение  $x = r^2 \pmod{n}$ .

2.  $B$  случайно выбирает бит  $e$  (0 или 1) и отправляет его  $A$ .

3.  $A$  вычисляет  $y = r * v^e \pmod{n}$  и отправляет его обратно к  $B$ .

Сторона  $B$  проверяет равенство  $y^2 = x * v^e \pmod{n}$ . Если оно верно, раунд считается завершенным корректно и осуществляется переход к следующему раунду. В противном случае доказательство не принимается.

Таким образом протокол состоит из этапа подготовки (достаточно осуществить один раз для каждого пользователя) и этапа доказательства, состоящего из  $t$  раундов.

В каждом раунде пользователь, не обладающий знанием секрета может угадать.

### Протокол Гиллу-Кискатра

Протокол Гиллу-Кискатра является расширением протокола Фиата-Шамира  $M$  в сравнении с ним имеет меньшее число сообщений, которыми необходимо поменаться сторонам,  $M$  более низкие требования к памяти, используемой для хранения секретов пользователей.

Предварительный этап:

1. Доверенный центр  $T$  выбирает и публикует модуль схемы – число  $n$ , являющееся произведением двух больших простых чисел  $p$  и  $q$ .

2.  $T$  определяет и делает доступным для всех пользователей  $v$ , где  $v$  – открытая экспонента ( $v > 2, \text{НОД}(v, \varphi(n)) = 1$ ),  $s$  – закрытая экспонента ( $s = v^{-1} \pmod{\varphi(n)}$ ).

3. Каждый участник  $A$  получает уникальный идентификатор, на основании которого по известной функции  $f$  вычисляется значение  $J_A = f(I_A)$ .

4.  $T$  возвращает участнику  $A$  секретное значение  $S_A = J_A^{-s} \pmod{n}$ .

Рабочий этап:

1. Участник  $A$  выбирает случайное секретное число  $r$  ( $0 < r < n$ ), вычисляет  $x = r^v \pmod{n}$  и отправляет  $B$  пару чисел  $(I_A, x)$ .

2.  $B$  генерирует случайное целое число  $e$  ( $0 < e < (n+1)$ ) и отправляет его участнику  $A$ .

3.  $A$  вычисляет и передаёт  $B$   $y = r * S_A^e \pmod{n}$ .

4.  $B$  получает  $y$ , из  $I_A$ , используя функцию  $f$  получает  $J_A = f(I_A)$ , вычисляет  $z = J_A^e * y^v \pmod{n}$  и принимает доказательство участника  $A$ , если  $z=x$  и  $z!=x$ .

### Протокол Шнорра

Протокол Шнорра – протокол доказательства с нулевым разглашением, стойкость которого базируется на проблеме дискретного логарифмирования.

Этап 1: Выбор параметров протокола

1. Выбирается два простых числа  $p$  и  $q$ , причём  $q|(p-1)$ .

2. Выбирается число  $t$  ( $2^t < q$ ), являющееся параметром безопасности.

3. Выбирается элемент  $g$ , лежащий в пределах  $(1, p-1)$  и имеющий порядок  $q$ .

4. Каждая сторона протокола получает копию системных параметров  $(g, p, q)$ , а также открытый ключ доверенного центра  $T$ , который позволяет проверить подпись сообщения  $m$ .

Ответ с вероятностью  $1/2$ . Для  $t$  раундов таким образом вероятность обмана составит  $2^{-t}$ .

Этап 2: Выработка параметров пользователя

1. Каждая сторона протокола  $A$  получает уникальный идентификатор  $I_A$ .

2. Сторона  $A$  выбирает приватный ключ  $a$  (лежащий в пределах  $(1, q-1)$ ) и вычисляет  $v = g^{-a} \pmod{p}$ .

3. Сторона  $A$  передаёт  $v$  доверенному центру  $T$  и получает сертификат  $certA = (I_A, v, S_r(I_A, v))$ , который связывает  $v$  и  $I_A$ .

### Этап 3: Доказательство

1. Доказывающая сторона А случайным образом выбирает число  $r$  ( $0 < r < q$ ), вычисляет  $x = g^r \pmod{p}$  и отправляет проверяющей стороне В ( $cert_A, x$ ).

2. Сторона В делает вывод об аутентичности открытого ключа  $v$  доказывающей стороны А путём проверки подписи доверенного центра, после чего отправляет А случайное ранее не использовавшееся число  $e$ ,  $1 \leq e \leq 2^t$ .

3. Сторона А проверяет  $1 \leq e \leq 2^t$  и передаёт В  $y = ae + r \pmod{q}$ .

4. В вычисляет  $z = g^y * v^e \pmod{p}$  и принимает доказательство, если  $z=x$ .

## 6. Задания

### Реализация протокола Фиата-Шаира

Целью данного задания является реализация протокола доказательства с нулевым разглашением Фиата-Шаира. В интерфейсе приложения должны быть наглядно представлены:

- исходные данные протокола (модули, ключи, секретные данные и т.п.);
- данные, передаваемые по сети каждой из сторон;
- проверки, выполняемые каждым из участников.

Процесс взаимодействия между сторонами протокола может быть реализован как с применением сетевых технологий, так и при помощи буферных переменных. Также необходимо выделить каждый из этапов протоколов для того, чтобы его можно было отделить от остальных.

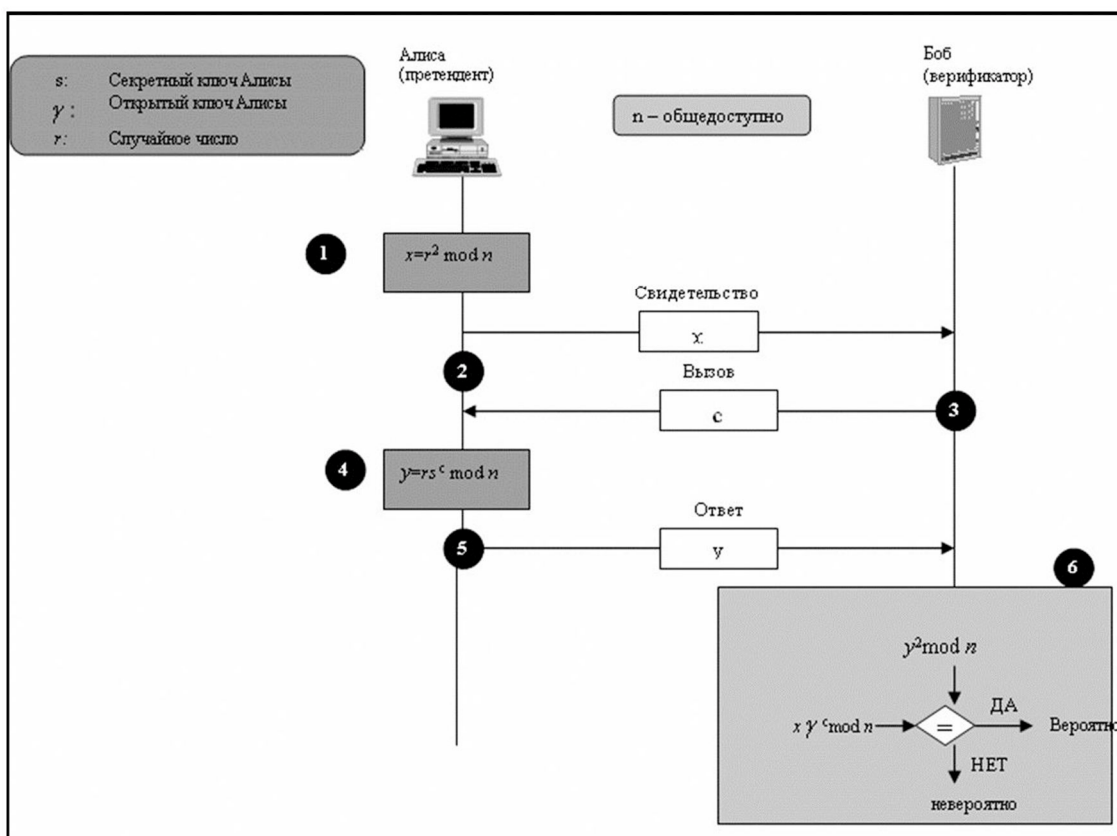


Рис. 1. Протокол Фиата-Шаира

### Реализация протокола Гиллу-Кискатра

Используя исходный код, полученный в процессе выполнения задания, необходимо создать реализацию протокола Гиллу-Кискатра, являющего модификацией протокола Фиата-Шаира. В интерфейсе приложения должны быть наглядно представлены:

- исходные данные протокола (модули, ключи, секретные данные и т.п.);
- данные, передаваемые по сети каждой из сторон;
- проверки, выполняемые каждым из участников.

Процесс взаимодействия между сторонами протокола может быть реализован как с применением сетевых технологий, так и при помощи буферных переменных. Также необходимо выделить каждый из этапов протоколов для того, чтобы его можно было отделить от остальных.



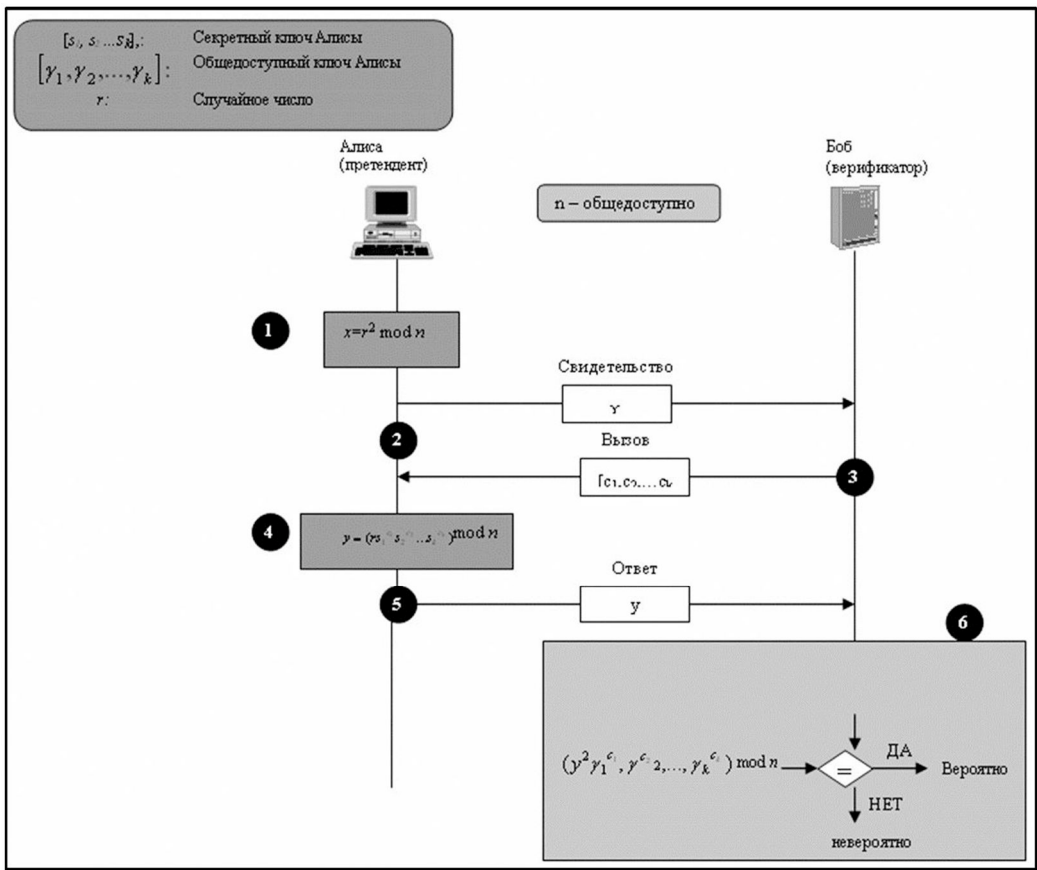


Рис. 2. Протокол Фейге-Фиата-Шамира

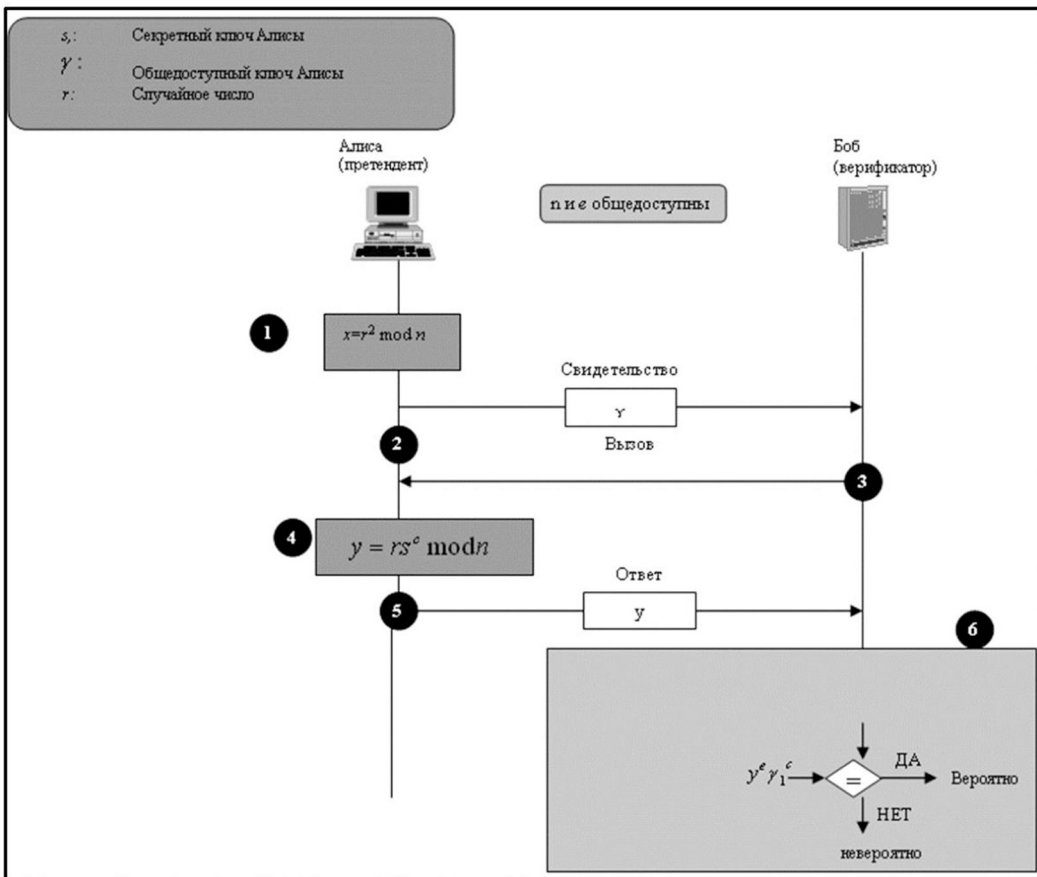


Рис. 3. Протокол Гиллу-Кискатра

## Реализация протокола Шнорра

Целью данного задания является реализация протокола доказательства с нулевым разглашением Шнорра. В интерфейсе приложения должны быть наглядно представлены:

- исходные данные протокола (модули, ключи, секретные данные и т.п.);
- данные, передаваемые по сети каждой из сторон;
- проверки, выполняемые каждым из участников.

Процесс взаимодействия между сторонами протокола может быть реализован как с применением сетевых технологий, так и при помощи буферных переменных. Также необходимо выделить каждый из этапов протоколов для того, чтобы его можно было отделить от остальных.

Задание:

1. Реализуйте протокол Фиата-Шамира и объясните принцип его работы.
2. Реализуйте протокол Гиллу-Кискатра и объясните принцип его работы.
3. Реализуйте протокол Шнорра и объясните принцип его работы.

## Практическая часть:

1. Реализуем протокол Фиата-Шамира на языке программирования высокого уровня C#:

```
C:\Users\gogol_o1k5xs\source\repos\Протокол Фиата-Шамира\Протокол Фиата-Шамира\bin\Debug\Протокол Фиата-Шамира.exe
Предварительный этап
УЦ выбирает p и q, публикует n - модуль системы:
p = 517545121
q = 277370837
n = p*q =143551923397036277
Выберите S (в диапазоне от 1 до n-1): 142621946
Открытый ключ: v=s^2 mod n =142621946 ^ 2 mod 143551923397036277 = 20341019480826916
Закрытый ключ: s = 142621946
Рабочий этап:
Выберите случайное значение из диапазона (1, n-1). r = 649614619
Отправляем другой стороне: x = r^2 mod n = 649614619 ^ 2 mod 143551923397036277 = 134895306424442607
Другая сторона выбирает бит (0 или 1) отсылает значение первой стороне:
e = 1
Первая сторона вычисляет и отправляет значение: y=r*v^e mod n
649614619 * 20341019480826916 ^ 1 mod 143551923397036277 = 134317827038555905
Другая сторона проверяет y^2=x*v^2e mod n
134317827038555905 ^ 2 = 11973255080666640
134895306424442607 * 20341019480826916 ^ 2 mod 143551923397036277 = 11973255080666640
Значения совпали!!!
```

Рис. 4. Протокол Фиата-Шамира

2. Реализуем протокол Гиллу-Кискатра на языке программирования высокого уровня C#:

```
C:\Users\gogol_o1k5xs\source\repos\Протокол Гиллу-Кискатра\Протокол Гиллу-Кискатра\bin\Debug\Протокол Гиллу-Кискатра.exe
Предварительный этап
УЦ выбирает p и q, публикует n - модуль системы:
p = 1018190389
q = 695182259
n = p*q =707827894717108751
phi(n)=(p-1)*(q-1) = 707827893003736104
Выберите v (в диапазоне от 1 до n-1): 2410621062
Выберите другое число v (в диапазоне от 1 до n-1): 712575410614901
Закрытая экспонента: s=v^-1 mod phi(n) =712575410614901 ^ -1 mod 707827893003736104 = 118678087372280813
Открытая экспонента: v = 712575410614901
Выберите номер идентификации A: Ia = 742107218013
Функция (I^2 +1) = 460853926716387624
460853926716387624 ^ - 118678087372280813 mod 707827894717108751 = 675387037552940472
УЦ выдаёт A секретное значение: sa = 675387037552940472
Рабочий этап:
Сторона A выбирает случайное значение из диапазона (1, n-1). r = 46106106180617
Сторона A вычисляет: x = r^v mod n = 46106106180617 ^ 712575410614901 mod 707827894717108751 = 474773805839668481
И отправляет B пару чисел: (Ia,x): (I = 742107218013, x = 474773805839668481)
Сторона B выбирает случайное число и отсылает значение стороне A:
e = 436178176109719
Сторона A вычисляет и отправляет значение: y=r*sa^e mod n
46106106180617 * 675387037552940472 ^ 436178176109719 mod 707827894717108751 = 347191807095003367
Действия стороны B:
Из Ia получаем Ja = 460853926716387624
460853926716387624 ^ 436178176109719 mod 707827894717108751 * 347191807095003367 ^ 712575410614901 mod 707827894717108751 = 474773805839668481
Сторона B проверяет z=x
Значения совпали Идентификация прошла успешно!!!
```

Рис. 5. Протокол Гиллу-Кискатра

### 3. Реализуем протокол Шнорра на языке программирования высокого уровня C#:

```
C:\Users\gogol_o1k5x\source\repos\Протокол Шнорра\Протокол Шнорра\bin\Debug\Протокол Шнорра.exe
Этап 1: Выбор параметров протокола
Простое число: p = 264702527
Делитель числа p: q = 3626062
Параметр безопасности: t = 20
Порождающий элемент на q по p: g = 104909933
Публикация (p,q,g)

Этап 2: Выработка параметров пользователя
Введите идентификатор стороны A: Ia = 1467476471
Введите секретный ключ стороны A: a = 714071671
Сторона A вычисляет v=g^-a mod p
104909933 ^ -714071671 mod 264702527 = 145220824
Сторона A передает v УЦ и получает сертификат, связывающий v и Ia

Этап 3: Доказательство
Сторона A выбирает число r = 3641718601
Вычисляет x=g^r mod p
104909933 ^ 3641718601 mod 264702527 = 227810515
Сторона A отправляет сертификат и x стороне B
Сторона B делает вывод об аутентичности открытого ключа v доказывающей стороны A путём проверки подписи доверенного центра,
после чего отправляет A случайное ранее не использовавшееся число
e = 3196798371103
Сторона A проверяет e и вычисляет u=ae+r mod q
714071671 * 3196798371103 + 3641718601 mod 3626062 = 2056060
И посылает это значение B
B вычисляет z=g^u*v^e mod p
104909933 ^ 2056060 * 145220824 ^ 3196798371103 mod 264702527 = 227810515
Идентификация прошла успешно!!!
```

Рис. 6. Протокол Шнорра

#### Вывод:

Протоколы реализуются по двум схемам шифрования – RSA (протокол Фиата-Шамира и Гиллу-Кискатра) и Эль-Гамала (протокол Шнорра), соответственно, и атаки на эти протоколы используются аналогичные этим видам шифрования.

#### 7. Контрольные вопросы:

1. Сравнить протоколы.
2. Указать области применения.

Время на выполнение лабораторной работы – 4 часа.

Образовательная организация, авторы, эл. почта: КубГТУ, Осипенко Л.П., Osipenko\_l\_p@mail.ru

---

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, Защищенные информационные системы управления.

Дисциплина: Криптографические протоколы.

### **Лабораторная работа.** **Протоколы удаленной аутентификации**

#### 1. Учебные цели:

Изучить возможности протоколов удаленной аутентификации, а также отработать навыки выполнения работ по установке, настройке, обслуживанию программных, программно-аппаратных (в том числе криптографических), технических средств защиты информации и контроля эффективности защиты информации.

#### 2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

##### Уметь:

- выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

## **Владеть:**

- навыками выполнения работ по установке, настройке, обслуживанию программных, программно-аппаратных (в том числе криптографических), технических средств защиты информации и контроля эффективности защиты информации.

## **3. Перечень материально-технического обеспечения:**

- **Специализированные классы** учебного корпуса К 9: № 205, 215, 403.
- **Технические средства обучения:** мультимедийный проектор, ноутбук, экран для проекции, презентации отдельных лекций, практических занятий.
- **Лабораторное оборудование и программное обеспечение:**
  - krypt.exe;
  - Криптопротоколы.exe;
  - SHAP.exe;
  - S/KEY.exe.

## **4. Задание на исследование**

**Цель:** научиться управлять защитой сетевого трафика с помощью средств стандартного протокола IPsec операционной системы Microsoft Windows 2008.

**Задание:** настроить протокол IPsec, согласно указанным параметрам.

## **5. Краткие теоретические сведения**

### **Понятие аутентификации**

**Аутентификация** – процесс проверки подлинности идентификатора, предъявляемого пользователем.

Учитывая степень доверия и политику безопасности систем, проводимая проверка подлинности может быть односторонней или взаимной. Обычно она проводится с помощью криптографических способов:

- Односторонняя – серверу или веб-приложению достаточно убедиться в подлинности клиента, который инициирует соединение.
- Двусторонняя (взаимная) – для такого сценария каждый из участников должен убедиться в подлинности своего собеседника.

Любая система аутентификации представляет собой совокупность элементов, выполняющих ту или иную роль в реализуемом ей сценарии. К таким элементам относятся:

- **Субъект аутентификации** – лицо, проходящее процедуру аутентификации;
- **Характеристика субъекта (фактор)** – отличительная черта, характеризующая субъект;
- **Владелец системы аутентификации** – лицо, несущее ответственность и контролирующее работу системы;
- **Механизм аутентификации** – принцип, по которому осуществляется проверка подлинности предоставленного субъектом фактора;
- **Механизм предоставления прав** – механизм, обеспечивающий авторизацию, то есть предоставление тех или иных прав, приписанных данному субъекту, прошедшему проверку подлинности;

В общем случае процедуру аутентификации можно представить следующим образом:

- 1) субъект инициирует процедуру аутентификации;
- 2) субъект предъявляет один или несколько факторов аутентификации;
- 3) на основании механизма аутентификации принимается решение о подлинности субъекта;
- 4) в случае положительного решения, субъект наделяется правами доступа, присвоенными для него хозяином системы;

В качестве фактора аутентификации выступает то или иное свойство, являющееся отличительным для данного субъекта. К факторам аутентификации относят:

- знание («пользователь знает») – тайные сведения, которыми обладает субъект аутентификации;
- обладание («пользователь имеет») – устройство аутентификации (смарт-карта, eToken);
- существование («пользователь существует») – биометрические данные;

### **Удаленная аутентификация**

Под удаленной аутентификацией понимается осуществление процедуры аутентификации с использованием каналов связи. Основными проблемами данного процесса являются:

- Обеспечение подлинности канала связи.
- Защита механизма аутентификации пользователя от атак методом повтором (получение злоумышленником информации, передаваемой в процессе аутентификации подлинного клиента не должно позволить злоумышленнику пройти последующие процедуры аутентификации).

Основными методами обеспечения подлинности канала являются метод запрос-ответ и механизм меток времени.

Метод "запрос-ответ" основан на использование некоторой случайной информации (запрос, Challenge), передаваемой пользователю В от пользователя А в случае, если пользователь А хочет проверить подлинность пользователя В. Схему этого метода можно представить в следующем виде:

1. Алиса генерирует случайное число, называемое запросом (Challenge).
2. Боб, получив запрос, прикрепляет к нему свои аутентификационные данные и подвергает его криптографическому преобразованию, а затем отправляет ответ (Response) Алисе.
3. Алиса, получив ответ, проверяет его, повторяя описанные выше операции на своей стороне, и на основании данной проверки принимает решение о подлинности сеанса связи.

Стойкость данной системы основана на том, что злоумышленник не знает секретной информации, принадлежащей Бобу – следовательно он не сможет подделать корректный ответ на полученный запрос.

Метод "меток времени" заключается в том, что в каждое пересылаемое сообщение добавляется специальная информация, называемая меткой времени (Time Stamp), которая описывает точное время отправки данного сообщения. Это позволяет каждому субъекту определить, насколько старо пришедшее сообщение и отбросить его в случае, если появится сомнение в его подлинности.

### Протоколы, используемые при удаленной аутентификации

**Password Access Protocol (PAP).** Самым простым и эффективным протоколом удаленной аутентификации является протокол доступа по паролю (Password Access Protocol, PAP).

Суть протокола заключается в аутентификации пользователя на сервере путем передачи последнему пары "логин-пароль", представляющей из себя идентификатор и информацию, известную лишь подлинному пользователю.

Основной проблемой данного протокола является то, что информация передается в открытом виде, а значит данный протокол неустойчив к атакам типа Sniffing.

Злоумышленник, обладающий доступом к открытому каналу связи и средствами перехвата пакетов может с легкостью получить пароль, что позволит ему пройти аутентификацию от лица другого пользователя.

Для повышения безопасности пароли могут передаваться не в открытом виде, а в виде хэшей, однако данная модификация не способна повысить стойкость к атакам типа Sniffing, так как злоумышленник может перехватить и хэш пароля.

### Протокол CHAP

Протокол CHAP (Challenge-Handshake Authentication Protocol) – протокол удаленной аутентификации, основанный на методе "запрос-ответ"

Протокол нашел применение в технологиях RADIUS (Remote Authentication Dial In User Service) и EAP (Extensible Authentication Protocol). В самом простом случае (односторонняя аутентификация) протокол в точности повторяет схему метода "запрос-ответ":

1. Алиса генерирует случайное число N и отправляет его Бобу.
2. Боб, получив из запроса N, добавляет к нему свой пароль P и осуществляет вычисление дайджеста  $H_1 = \text{Hash}(N, P)$ . Полученный результат отправляется Алисе.
3. Алиса повторяет процедуры, выполненную Бобом на прошлом шаге и вычисляет значение дайджеста  $H_2 = \text{Hash}(N, P_1)$  от P1, которое хранится у Алисы в качестве пароля Боба. Если H1 совпадает с H2, пользователь считается аутентифицированным.

Существует модификация протокола, позволяющая проводить взаимную аутентификацию сторон. При этом производится следующая последовательность действий:

1. Алиса генерирует случайное число N1 и отправляет его Бобу вместе с запросом на аутентификацию (A);
2. Боб, получив запрос, генерирует собственное случайное число N2, которое вместе с  $\text{Hash}(N_1, P_b)$  отправляется Алисе;
3. Алиса проверяет подлинность сообщения, содержащего ее зашифрованное случайное число и пароль Боба, а затем генерирует дайджест  $\text{Hash}(N_2, P_A)$  и отправляет его Бобу;
4. Боб проверяет подлинность сообщения, полученного от Алисы и содержащего его зашифрованное случайное число.

### Протокол использования одноразовых ключей S/KEY

Протокол S/KEY основан на независимом формировании клиентом и сервером последовательности одноразовых паролей, построенной на общем секрете K. В основе протокола лежит Метод Лампорта (Lamport's Hash Chain Method)

Пусть K – секретный пароль, известный как серверу, так и подлинному клиенту.

$$\begin{aligned} P_1 &= H(K) \\ P_2 &= H(P_1) = H(H(K)) \\ &\dots \\ P_N &= H(P_{N-1}) = H(H(\dots H(H(P_1)))) \end{aligned}$$

Клиент вычисляет последовательность одноразовых ключей  $Y$  следующим образом:

Сервер, независимо от пользователя может сгенерировать точно такую же последовательность, что позволяет использовать ее для проверки одноразовых паролей. После генерации паролей изначальный секрет  $K$  отбрасывается, сервер устанавливает  $P_N$  в качестве первоначального пароля пользователя и  $I$  в качестве текущего номера транзакции.

Процесс аутентификации выглядит следующим образом:

1. Пользователь запрашивает аутентификацию у сервера;
2. Сервер сообщает пользователю текущий номер транзакции  $I$ ;
3. Пользователь передает серверу пароль с индексом  $N-I$ ;
4. Сервер применяет хеш-функцию  $H$  к полученному паролю от пользователя и сверяет его со значением пароля, хранящимся на сервере.
5. В случае, если пароли совпадают, пользователь считается аутентифицированным, сервер увеличивает текущий номер транзакции на единицу и перезаписывает хранимый пароль пользователя паролем, полученным при аутентификации.

К недостаткам этого протокола можно отнести тот факт, что после исчерпания конечного множества одноразовых паролей мы не должны использовать его повторно, так как злоумышленник мог перехватить всю последовательность целиком. Это значит, что необходим механизм модификации исходных данных для процесса генерации последовательностей.

Чаще всего используют подход, основанный на передаче перед формированием последовательности одноразовых ключей случайного числа  $R$  от сервера к клиенту. Это случайное число, наряду с секретным паролем  $K$  ложится в основу пары  $K||R$ , которая используется в качестве базы для генерации последовательности. После исчерпания одноразовых паролей для числа  $R$ , сервер передает клиенту новое случайное число и процесс повторяется.

## 6. Задания

### Реализация протоколов PAP/CHAP

Целью данного задания является реализация базовых протоколов аутентификации PAP/CHAP в виде приложения. В интерфейсе приложения должны быть наглядно представлены:

- исходные данные протокола (модули, ключи, секретные данные и т.п.);
- данные, передаваемые по сети каждой из сторон;
- проверки, выполняемые каждым из участников.

Процесс взаимодействия между сторонами протокола может быть реализован как с применением сетевых технологий, так и при помощи буферных переменных. Также необходимо выделить каждый из этапов протоколов для того, чтобы его можно было отделить от остальных.

Задание состоит из двух этапов. На первом этапе Вы осуществляете реализацию протокола PAP и одностороннего протокола CHAP. После того, как Вы получите работающее приложение, Вам необходимо расширить его функциональность и обеспечить поддержку двухстороннего протокола CHAP. Для генерации секретных параметров рекомендуется использовать криптографически стойкие генераторы случайных чисел, а в качестве хеш-функции использовать алгоритм SHA1.

### Реализация протокола S/KEY

Целью данного задания является реализация протокола аутентификации S/KEY в виде приложения. В интерфейсе приложения должны быть наглядно представлены:

- исходные данные протокола (модули, ключи, секретные данные и т.п.);
- данные, передаваемые по сети каждой из сторон;
- проверки, выполняемые каждым из участников.

Процесс взаимодействия между сторонами протокола может быть реализован как с применением сетевых технологий, так и при помощи буферных переменных. Также необходимо выделить каждый из этапов протоколов для того, чтобы его можно было отделить от остальных.

Необходимо обеспечить доступ ко всем паролям, сгенерированным в процессе инициализации протокола (например, вынести в отдельное окно). Для генерации секретных параметров рекомендуется использовать криптографически стойкие генераторы случайных чисел, а в качестве хеш-функции использовать алгоритм SHA1.

### Задание:

1. Реализуйте протокол PAP/CHAP.
2. Реализуйте протокол S/KEY.

Практическая часть:

1. Реализуем протокол PAP/CHAP на языке программирования высокого уровня C#:

```
C:\Users\gogol_of1k5xs\Desktop\КГП\30-09-2017\лп2\CHAP.exe
Алиса вводит случайное число и отправляет его Бобу: 36710701
Введите пароль Алисы (в числовой форме): 36710701
Боб выбирает случайное число: 36761718
Введите пароль Боба (в числовой форме): 16147168637
Боб вычисляет хеш: $H1=N1 \text{ xor } P_b$
36710701 xor 16147168637 = 16110457936
Боб посылает Алисе N2 и H1
Алиса проверяет подлинность сообщения (при известном пароле боба)
Алиса подтверждает аутентификацию
Алиса вычисляет хеш: $H2=N2 \text{ xor } P_a$
36761718 xor 36710701 = 55643
Алиса посылает Бобу H2
Боб проверяет подлинность по своему числу и известному паролю Алисы
Боб подтверждает аутентификацию
```

Рис. 1. Реализация протокола PAP/CHAP

2. Реализуем протокол S/KEY на языке программирования высокого уровня C#:

```
C:\Users\gogol_of1k5xs\Desktop\КГП\30-09-2017\лп2\SKey.exe
Подготовительный этап:
Введите секретный ключ: 16796179161
Введите начальное заполнение: 67
Введите количество паролей: 5
Пароль №1 = 2111634408410663858
Пароль №2 = 9518296932267444103
Пароль №3 = 4204310340229474674
Пароль №4 = 9385316946007406215
Пароль №5 = 6290493632020626290
Обмен ключами
Введите ключ №5 = 6290493632020626290
Успешно!!!
Введите ключ №4 = 9385316946007406215
Успешно!!!
Введите ключ №3 = 1
Вы не прошли авторизацию(
Введите ключ №2 = 2
Вы не прошли авторизацию(
Введите ключ №1 = 3
Вы не прошли авторизацию(
Количество одноразовых ключей исчерпано(((
Повторите действие программы
```

Рис. 2. Реализация протокола S/KEY

**Вывод:** Аутентификация по протоколу CHAP благодаря своей простоте применяется в системе сотового оператора для связи с клиента с провайдером, для обеспечения интернет-услуг. Система одноразовых паролей требует надёжного способа вычисления хеша и невозможности проведения вычислений в обратную сторону, для чего применяются операции сложения по модулю 2, возведение в степень по модулю. Одноразовые пароли должны быть доставлены в место назначения необозначенным способом, за которые уже не отвечают криптографические протоколы.

#### 7. Контрольные вопросы:

1. Сравнить протоколы аутентификации.
2. Указать области применения.

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** КубГТУ, Осипенко Л.П., Osipenko\_l\_p@mail.ru

**Образовательная программа:** 10.05.03 – Информационная безопасность автоматизированных систем, Защищенные информационные системы управления.

**Дисциплина:** Криптографические протоколы.

### **Лабораторная работа.**

#### **Цифровая подпись на основе алгоритмов RSA и Эль-Гамала**

##### **1. Учебные цели:**

Изучить возможности алгоритмов цифровой подписи: RSA и Эль-Гамала.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

###### **Уметь:**

- выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

###### **Владеть:**

- навыками выполнения работ по установке, настройке, обслуживанию программных, программно-аппаратных (в том числе криптографических), технических средств защиты информации и контроля эффективности защиты информации.

##### **3. Перечень материально-технического обеспечения:**

- **Специализированные классы** учебного корпуса, расположенного на ул. Красной 91: № 205, 215, 403.
- **Технические средства обучения:** мультимедийный проектор, ноутбук, экран для проекции, презентации отдельных лекций, практических занятий.
- **Лабораторное оборудование и программное обеспечение:**
  - krypt.exe;
  - «Программа для генерации и проверки параметров ассиметричных шифров RSA и Эль-Гамала «Generaing\_parameters\_of\_RSA\_and\_ElGamal»;
  - «Программа для ЭВМ «Программа для шифрования и вычисления цифровой подписи по типу RSA «Cipher\_RSA»;
  - «Программа для шифрования и вычисления цифровой подписи по типу Эль-Гамала «Cipher\_of\_ElGamal».;
  - Криптопротоколы.exe.

##### **4. Задание на исследование**

В данной лабораторной работе требуется освоить работу алгоритмов RSA и Эль-Гамала. Для этого необходимо выполнить следующее (каждый студент индивидуально выполняет задание и оформляет отчет).

- Выполнить на бумаге расчет шифрования и расшифрования первых букв из собственных инициалов (фамилии, имени, отчества).
- Программно реализовать (для чисел размерностью в машинное слово) оба алгоритма в виде программы на любом из следующих языков программирования: C#, C++. Текст программы должен содержать комментарии к каждой строке кода.
- Оформить отчет о выполненной работе, с приведением расчета из пункта 1, листингов программ и двух-трех тестов (как в первом пункте задания).
- Выполнить сдачу работы руководителю лабораторного занятия (при этом существует возможность задания дополнительных вопросов).

Все вычисления проводить для своих данных (ФИО)

##### **5. Краткие теоретические сведения**

**Алгоритм RSA** предложили в 1978 г. три автора: Райвест (Rivest), Шамир (Shamir) и Адлеман (Adleman). Алгоритм получил свое название по первым буквам фамилий его авторов. RSA стал первым полноценным алгоритмом с открытым ключом, который может работать как в режиме шифрования данных, так и в режиме электронной цифровой подписи. Системы с открытым ключом позволяют исключить явную передачу по открытым каналам секретных постоянных данных – паролей и секретных ключей для шифрования.

Надежность алгоритма основывается на трудности факторизации больших чисел и трудности вычисления дискретных логарифмов.

Пусть выбираются случайные большие простые числа  $P$  и  $Q$ , равной длины, которые являются секретом. Данные числа образуют модуль  $N$ , используемый для нормирования результатов:  $N = P \cdot Q$ .



Открытый ключ  $K_o$  выбирают случайным образом так, чтобы выполнялись условия:

$$1 < K_o \leq \varphi(N),$$

$$\text{НОД}(K_o, \varphi(N)) = 1 \text{ (числа } K_o \text{ и } \varphi(N) \text{ взаимнопросты),}$$

$$\varphi(N) = (P-1)(Q-1),$$

где  $\varphi(N)$  – функция Эйлера. Функция Эйлера  $\varphi(N)$  указывает количество положительных целых чисел в интервале от 1 до  $N$ , которые взаимнопросты с  $N$ . Второе условие означает, что открытый ключ  $K_o$  и  $\varphi(N)$  должны быть взаимно простыми (использование алгоритма Евклида).

Далее, используя расширенный алгоритм Евклида, вычисляется секретный ключ  $K_c$  как обратный элемент к  $K_o$ , такой, что

$$K_c * K_o \equiv 1 \pmod{\varphi(N)} \text{ или } K_c = K_o^{-1} \pmod{(P-1)(Q-1)}.$$

Символ  $\equiv$  обозначает сравнимость левой и правой частей уравнения. Два целых числа  $a$  и  $b$  сравнимы по модулю  $n$ , если  $(a - b)$  делится на  $n$ , то есть

$$a \equiv b \pmod{n} \text{ или } a - b = n * t, \text{ } t - \text{положительное целое число.}$$

Открытый ключ  $K_o$  используют для шифрования данных, а секретный ключ  $K_c$  – для расшифрования.

Открытый текст  $M$  перед шифрованием разбивается на блоки чисел, сравнимые с модулем  $N$ .

Преобразование шифрования определяет зашифрованный текст  $C$  через пару (открытый ключ  $K_o$ , сообщение  $M$ ) в соответствии со следующей формулой (возведение в степень с нормированием результата с помощью схемы Горнера):

$$C = M^{K_o} \pmod{N}.$$

Задача расшифрования криптограммы  $C$  решается с использованием пары (секретный ключ  $K_c$ , криптограмма  $C$ ) по формуле:

$$M = C^{K_c} \pmod{N}.$$

Процесс расшифрования можно записать как  $D(E(M)) = M$  ( $D$  – операция расшифрования,  $E$  – операция шифрования).

Формулу  $K_c * K_o \equiv 1 \pmod{\varphi(N)}$ , используя определение операции сравнения, можно переписать в следующем виде:  $K_c * K_o = 1 + \varphi(N) * t$ . Тогда  $D(E(M)) = (M^{K_o})^{K_c} \pmod{N} = M^{K_o * K_c} \pmod{N} = M^{1 + \varphi(N) * t} \pmod{N}$ . При  $t = 0$   $D(E(M)) = M \pmod{N}$ .

В криптосистеме RSA открытый ключ  $K_o$ , секретный ключ  $K_c$ , сообщение  $M$  и криптограмма  $C$  принадлежат множеству положительных целых чисел  $[0; N-1]$ , где  $N$  – модуль. Данное множество с операциями сложения и умножения по модулю  $N$ , с существованием обратного и единичного элементов, образует арифметику поля по модулю  $N$ .

Открытыми элементами являются элементы  $K_o$ , модуль  $N$  и шифротекст  $C$ . А закрытыми – секретный ключ  $K_c$ , простые числа  $P$  и  $Q$ , и открытый текст  $M$ .

### Особенности алгоритма RSA

Чтобы алгоритм RSA имел практическую ценность, необходимо иметь возможность без существенных затрат генерировать большие простые числа, уметь оперативно вычислять значения ключей  $K_c$  и  $K_o$ .

Для нахождения чисел  $P$  и  $Q$  из  $N$  для злоумышленника встает задача разложения числа  $N$  на множители. Для получения открытого текста  $M$  из закрытого текста  $C$ , без знания секретного ключа  $K_c$ , возникает проблема нахождения дискретного логарифма. Обе эти задачи имеют вычислительную экспоненциальную сложность.

Аппаратная реализация RSA примерно в 1000 раз медленнее аппаратной реализации симметричного алгоритма DES. А программная реализация – в 100 раз медленнее программной реализации DES. То есть, из-за большого числа вычислений, асимметричная криптосистема RSA работает медленнее симметричных криптосистем.

Предлагаются следующие оценки длин ключей для ассиметричных алгоритмов, с учетом прогресса развития вычислительной техники (рис. 1).

### Алгоритм вычисления обратного элемента для небольших чисел

Для упрощения ручного счета обратный элемент для числа в модулярной арифметике можно находить по следующему алгоритму, вместо расширенного алгоритма Евклида. Для чисел, сравнимых с размерностью машинного слова, можно вычислять обратный элемент итеративно с помощью следующего алгоритма.

Если числа  $a$  и  $n$  взаимнопросты ( $\text{НОД}(a, n) = 1$ ), то выражение  $a * a^{-1} \equiv 1 \pmod{n}$  можно записать в виде  $a * a^{-1} - 1 = n * t$ ,  $t$  – положительное целое число из множества  $[0, +\infty)$ . Числа  $a$  и  $n$  заданы, неизвестны  $t$  и  $a^{-1}$ . Тогда нужно найти такое  $t$ , при котором  $a^{-1}$  будет удовлетворять условию обратного элемента:  $a * a^{-1} \equiv 1 \pmod{n}$ . Перепишем выражение  $a * a^{-1} - 1 = n * t$  как  $a^{-1} = \frac{1 + nt}{a}$ .

Описание алгоритма RSA. Предлагается реализовать данный алгоритм для чисел размерностью в машинное слово (до  $2^{32}$ ), задавая в качестве исходного открытого текста буквы русского алфавита, и выбирая модуль, соизмеримый с размером алфавита (если модуль будет меньше, то результат расшифровки будет отличаться от исходного открытого текста). Опишем шаги алгоритма.

1. Если  $\text{НОД}(a, n) \neq 1$  (алгоритм Евклида), то выход. Обратный элемент не существует.
2. Для любого  $t \in [0, +\infty)$  вычисляем действия.

2.a. Если значение выражения  $\frac{1+nt}{a}$  не является натуральным числом, то переход к пункту 2.

Иначе это выражение задает обратный элемент:  $a^{-1} = \frac{1+nt}{a}$ , выход.

Данный алгоритм будет конечным тогда, когда выполняется условие взаимной простоты двух чисел  $a$  и  $n$  (условие существования обратного элемента).

**Механизм использования алгоритма RSA**

Пусть пользователь А хочет передать пользователю В сообщение в зашифрованном виде, используя криптосистему RSA. Пользователь А выступает в роли отправителя сообщения, а пользователь В – в роли получателя. Элементы криптосистемы RSA должен формировать получатель сообщения – пользователь В. Рассмотрим последовательность действий пользователя В и пользователя А.

**Действия пользователя В**

1. Пользователь В выбирает два произвольных больших простых числа  $P$  и  $Q$ .
2. Пользователь В вычисляет значение модуля  $N = P * Q$ .
3. Пользователь В вычисляет функцию Эйлера:  $\varphi(N) = (P-1)(Q-1)$ , и выбирает случайным образом значение открытого ключа  $K_o$  с учетом выполнения условий:

$$1 < K_o \leq \varphi(N),$$

$\text{НОД}(K_o, \varphi(N)) = 1$  (алгоритм Евклида).

4. Пользователь В вычисляет значение секретного ключа  $K_c$ , используя расширенный алгоритм Евклида при решении сравнения:

$$K_c = K_o^{-1} \text{ mod } \varphi(N).$$

5. Пользователь В пересылает пользователю А пару чисел  $(N, K_o)$  по незащищенному каналу.

**Действия пользователя А, передающего пользователю В сообщение М.**

6. Пользователь А разбивает исходный открытый текст  $M$  на блоки, каждый из которых может быть представлен в виде последовательности чисел  $M_i = 0, 1, \dots, n-1$ .

7. Пользователь А шифрует текст, представленный в виде последовательности чисел  $M_i$  по формуле  $C_i = M_i^{K_o} \text{ mod } N$  (схема Горнера) и отправляет криптограмму  $C_1, C_2, \dots, C_i \dots$  пользователю В.

**Действия пользователя В**

8. Пользователь В расшифровывает принятую криптограмму  $C_1, C_2, \dots, C_i \dots$  используя секретный ключ  $K_c$ , по формуле  $M_i = C_i^{K_c} \text{ mod } N$ .

В результате будет получена последовательность чисел  $M_i$ , которые представляют собой исходное сообщение  $M$ .

### **Шифрование по схеме Эль-Гамала**

Схема Эль-Гамала, предложенная в 1985 г., используется для шифрования и для цифровых подписей. Безопасность схемы Эль-Гамала обусловлена сложностью вычисления дискретных логарифмов в конечном поле. В реальных схемах шифрования используется в качестве модуля  $P$  простое число размерностью в [512; 1024] бит.

Выберем большое простое число  $P$  и два больших целых числа  $G$  и  $X$ , меньших  $P$ :  $G < P, X < P$ . Выберем случайное целое число  $K$ , удовлетворяющее условиям:

$$1 < K < P-1,$$

$$\text{НОД}(K, P-1)=1 \text{ (взаимно простые)}.$$

Числа  $P$  и  $G$  являются открытой информацией, а  $X$  и  $K$  – секретные.

Далее вычислим открытый ключ  $Y = G^X \text{ mod } P$ .

Для передачи сообщения  $M$  вычисляем два числа, образующих шифротекст:

$$a = G^K \text{ mod } P$$

$$b = Y^K M \text{ mod } P.$$

В результате шифротекст по длине в 2 раза больше открытого текста  $M$ .

Возведем уравнение для  $a$  в степень  $x$ :  $a^x = G^{xk} \text{ mod } P$ .

Изменим выражение  $b$ : так как  $Y = G^X \text{ mod } P$ , то  $b = Y^K M \text{ mod } P = (G^X)^k M \text{ mod } P = G^{xk} M \text{ mod } P$ . Так как  $a^x = G^{xk} \text{ mod } P$ , то  $b = G^{xk} M \text{ mod } P = a^x M \text{ mod } P$ . Тогда восстановим открытый текст  $M$ :

$$M = b / a^x \text{ mod } P.$$

Для нахождения  $M$  нужно решить сложное сравнение  $b = a^x M \pmod P$  или  $a^x M/b = 1 \pmod P$ .  
 Для решения сложного сравнения вида  $a^x \equiv b \pmod n$  применим метод замены:  $z = x/b$ . Тогда  $a^z \equiv 1 \pmod n$ , где  $z$  является обратным элементом для  $a$ . Число  $z$  определяется с помощью расширенного алгоритма Евклида.

Тогда из  $z = x/b \Rightarrow x = z*b \pmod n$ .

Применим данную схему для нахождения открытого текста  $M$  в  $a^x M = b \pmod P$ . Обозначим за  $z$  выражение  $z = M/b$ , которое будет обратным элементом для  $a^x$  по модулю  $P$ :  $a^x z \equiv 1 \pmod P$ . Тогда  $M = z*b \pmod P = a^{-x}*b \pmod P$ .

### Механизм использования схемы Эль-Гамала

Предлагается реализовать данный алгоритм для чисел размерностью в машинное слово (до 32 бит –  $2^{32}$  комбинаций), задавая в качестве исходного открытого текста буквы русского алфавита, и выбирая модуль, соизмеримый с размером алфавита (если модуль будет меньше, то результат расшифровки будет отличаться от исходного открытого текста).

Пусть пользователь  $A$  собирается передать пользователю  $B$  сообщение в зашифрованном виде, используя схему Эль-Гамала. Пользователь  $A$  выступает в роли отправителя сообщения, а пользователь  $B$  – в роли получателя. Элементы схемы Эль-Гамала должен формировать получатель сообщения – пользователь  $B$ . Рассмотрим последовательность действий пользователя  $B$  и пользователя  $A$ .

Действия пользователя  $B$

1. Выбирает произвольное большое простое числа  $P$ .
2. Выбирает случайное  $G$ ,  $G < P$  и секретный ключ  $X$ ,  $X < P$ .
3. Вычисляется открытый ключ  $Y = G^X \pmod P$ .
4. Стороне  $A$  передаются числа  $G$ ,  $P$  и  $Y$ .

Действия пользователя  $A$ , передающего пользователю  $B$  сообщение  $M$ .

5. Пользователь  $A$  разбирает исходный открытый текст  $M$  на блоки, каждый из которых может быть представлен в виде последовательности чисел  $M_i = 0, 1, \dots, n-1$ .
6. Случайно выбирается  $K$ , удовлетворяющее условиям

$$1 < K < P-1 \text{ и } \text{НОД}(K, P-1)=1.$$

7. Вычисляется первая часть шифротекста:  $a = G^K \pmod P$ .

8. Пользователь  $A$  шифрует текст, представленный в виде последовательности чисел  $b_i$  по формуле  $b_i = Y^K M_i \pmod P$  (схема Горнера) и отправляет криптограмму  $(a, b_1, b_2, \dots, b_n, \dots)$  пользователю  $B$ .

Действия пользователя  $B$

9. Находит обратный элемент для  $a^x$  по модулю  $P$ .

10. Расшифровывает  $M_i = b_i * a^{-x} \pmod P$ ,  $A^{-x} = 0^{P-x} - 1$ .

В результате будет получена последовательность чисел  $M_i$ , которые представляют собой исходное сообщение  $M$ .

Результаты работы программ:

1. Шифрование по схеме Эль-Гамала

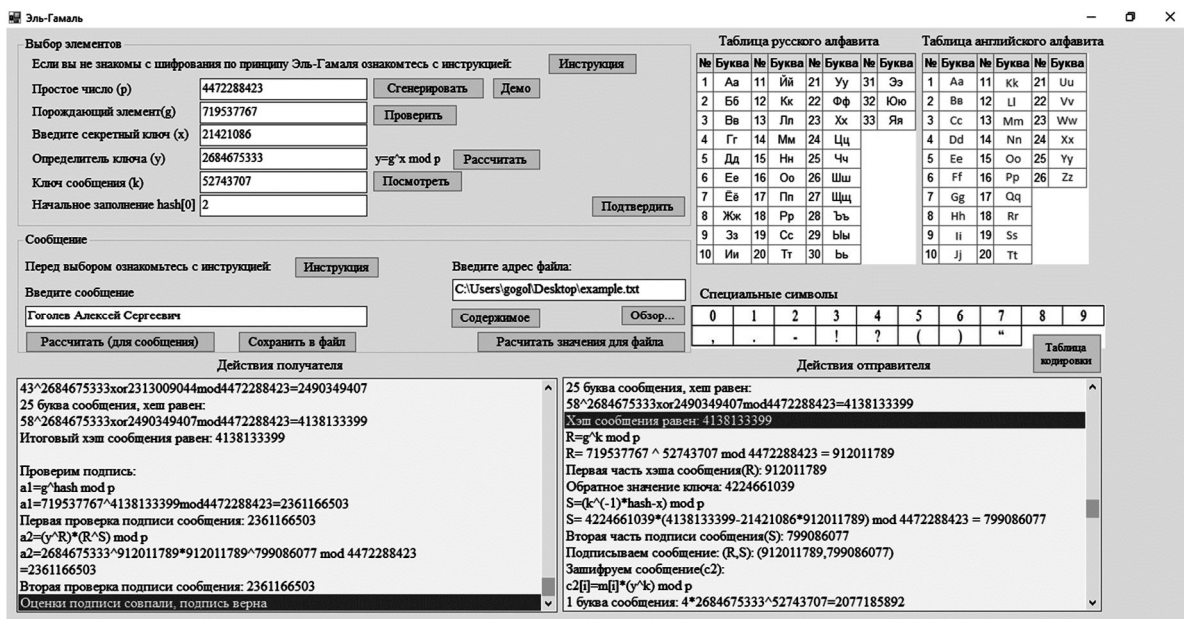


Рис. 1. Шифрование по схеме Эль-Гамала

## 2. Шифрование по типу RSA

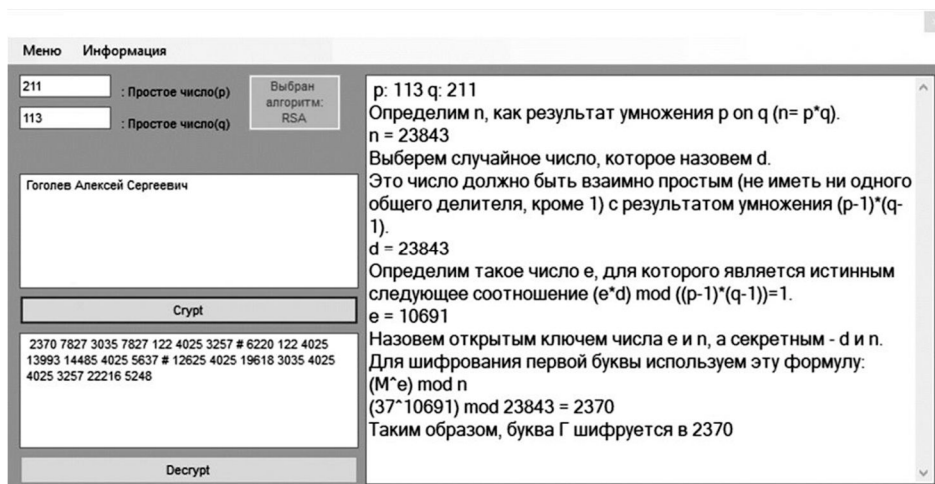


Рис. 2. Шифрование по типу RSA

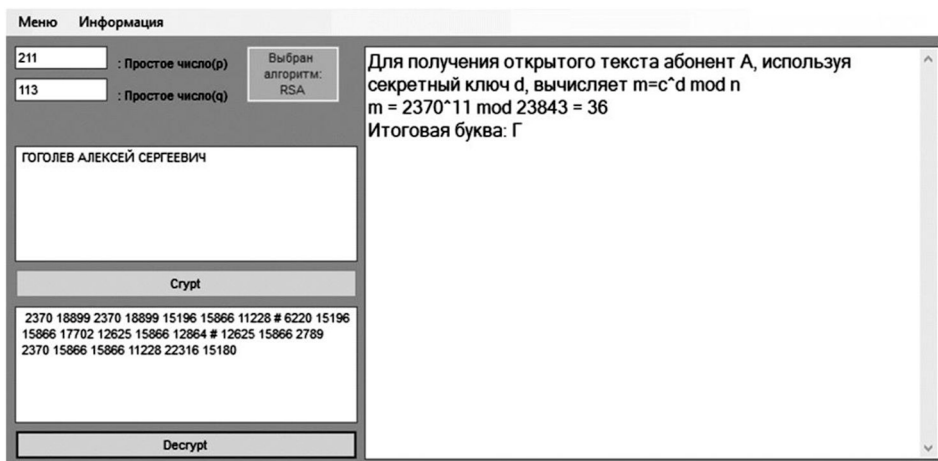


Рис. 3. Шифрование по типу RSA

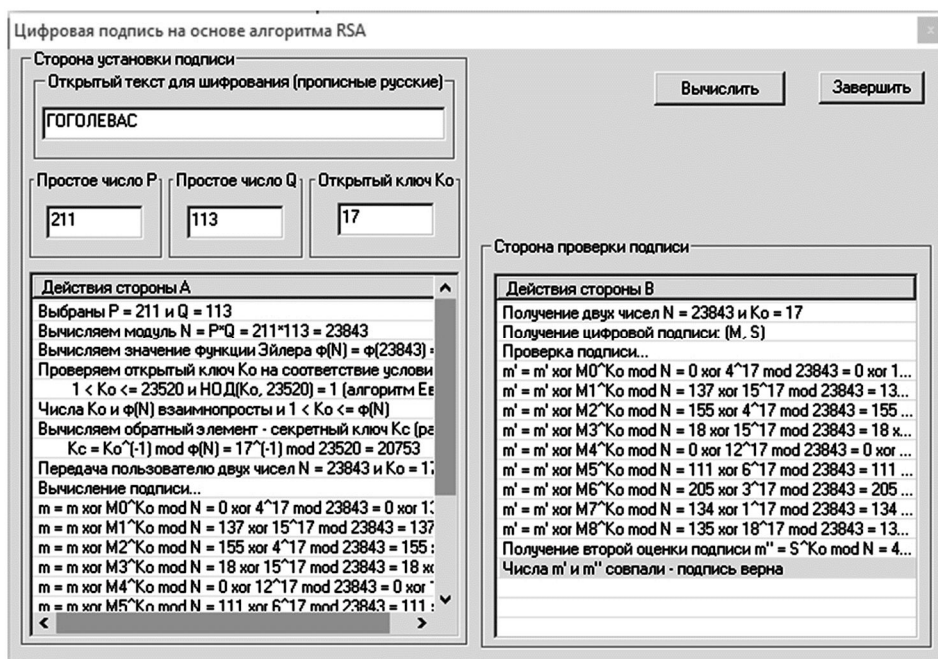


Рис. 4. Шифрование по типу RSA

**Выводы:**

Были изучены два алгоритма цифровой подписи: RSA и Эль-Гамала

Схема цифровой подписи Эль Гамала имеет ряд преимуществ по сравнению со схемой цифровой подписи RSA:

1. При заданном уровне стойкости алгоритма цифровой подписи целые числа, участвующие в вычислениях, имеют запись на 25 % короче, что уменьшает сложность вычислений почти в два раза и позволяет заметно сократить объем используемой памяти.
2. При выборе модуля  $P$  достаточно проверить, что это число является простым и что у числа  $(P-1)$  имеется большой простой множитель (т.е. всего два достаточно просто проверяемых условия).
3. Процедура формирования подписи по схеме Эль Гамала не позволяет вычислять цифровые подписи под новыми сообщениями без знания секретного ключа (как в RSA).

Однако алгоритм цифровой подписи Эль Гамала имеет и некоторые недостатки по сравнению со схемой подписи RSA. В частности, длина цифровой подписи получается в 1,5 раза больше, что, в свою очередь, увеличивает время ее вычисления.

**7. Контрольные вопросы:**

1. В чем преимущество RSA над DSA?
2. Что такое электронная подпись?
3. Какие виды электронной подписи существуют?
4. Что такое ключ электронной подписи?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** КубГТУ, Осипенко Л.П., Osipenko\_l\_p@mail.ru

## **Дисциплина: Обеспечение доверия к информационной безопасности автоматизированных систем**

**Образовательная программа:** 10.05.03 – Информационная безопасность автоматизированных систем («Защищенные автоматизированные системы управления»)

**Дисциплина:** «Обеспечение доверия к информационной безопасности автоматизированных систем».

### **Лабораторная работа.**

#### **Законодательный уровень обеспечения доверия к информационной безопасности автоматизированной системы предприятия**

##### **1. Учебные цели:**

- Изучить законодательный уровень обеспечения доверия к информационной безопасности автоматизированных систем.
- Отработать навыки построения модели системы информационной безопасности предприятия в среде моделирования ERWin.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

###### **Уметь:**

- анализировать и оценивать применимость законодательных актов Российской Федерации и международного права к вопросам обеспечения доверия системам безопасности в пределах учебных задач;
- использовать информационно-коммуникационные технологии в профессиональной деятельности в рамках учебных задач;
- разрабатывать компоненты проектной и технической документации с использованием графических языков спецификаций пределах учебных задач.

###### **Владеть:**

- навыками работы с методическими и нормативными материалами, технической документацией;
- методологией проектных работ;
- способностью создавать и исследовать модели автоматизированных систем;
- способностью проводить анализ защищенности автоматизированных систем.

##### **3. Перечень материально-технического обеспечения**

- **Лабораторное оборудование и программное обеспечение:**
  - Специализированные классы учебного корпуса, оснащенные средствами вычислительной техники.
  - Инструменты анализа и проектирования фирмы PLATINUM technology.
  - BPWin и ERWin.
  - Правовые справочно-поисковая система «Гарант».

##### **4. Задание на исследование**

Изучить законодательные акты, ответить на вопросы.

###### **Задание № 1**

Проведите анализ специальных понятий: «социальная информация», «документальная информация», «правовая информация», «научная информация» и приведите примеры информации, которая может быть отнесена к данным понятиям.

###### **Задание № 2**

Определите, к какому виду информации в зависимости от порядка ее предоставления или распространения относится информация в конкретных ситуациях:

а) юридическое лицо заключило с таможенным представителем договор представлять свои интересы при оформлении таможенной декларации и помещении товаров под определённую таможенную процедуру при перемещении товаров через таможенную границу Таможенного союза, и предоставил ему информацию о себе, товаре и его назначении;

б) государственный фонд данных государственного экологического мониторинга (государственного мониторинга окружающей среды) включает в себя:

- информацию, содержащуюся в базах данных подсистем единой системы государственного экологического мониторинга (государственного мониторинга окружающей среды);
- результаты производственного контроля в области охраны окружающей среды и государственного экологического надзора;
- данные государственного учета объектов, оказывающих негативное воздействие на окружающую среду.

в) при принятии бюджета на 2017 год и плановый период на 2018–2019 годы Комитет Государственной Думы по бюджетному планированию рассмотрел источник доходов и размеры финансирования на обеспечения обороноспособности страны с подробным указанием всех статей расходов.

#### Задание № 3

Для выбранной организации провести анализ уровня доверия к информационной безопасности автоматизированной системы (автоматизированная система дипломного проекта или другая по желанию).

#### Задание № 4

Познакомиться со средой моделирования ERWin. Реализовать модель системы в среде моделирования.

Лабораторные работы построены таким образом, что для выполнения последующего задания необходимо иметь результат выполнения предыдущего, поэтому следует сохранять модель, полученную в конце каждой лабораторной работы.

## 5. Краткие теоретические сведения

Организация и функционирование системы безопасности должны осуществляться на основе следующих принципов:

**Комплексность.** Предполагает обеспечение безопасности персонала, материальных и финансовых ресурсов, информации от всех возможных угроз всеми доступными законными средствами и методами, в течение всего жизненного цикла и во всех режимах функционирования, а также способностью системы к развитию и совершенствованию в процессе функционирования.

**Надежность.** Различные зоны безопасности должны быть одинаково надежными с точки зрения вероятности реализации угрозы.

**Своевременность.** Способность системы носить упреждающий характер на основе анализа и прогнозирования угроз безопасности и разработке эффективных мер противодействия им.

**Непрерывность.** Отсутствие перерывов в действии систем безопасности, вызванных ремонтом, заменой, профилактикой и т.д.

**Законность.** Разработка систем безопасности на основе существующего законодательства.

**Разумная достаточность.** Установление приемлемого уровня безопасности, при котором вероятность и размер возможного ущерба будут сочетаться с предельно допустимыми затратами на разработку и функционирование системы безопасности.

**Централизация управления.** Самостоятельное функционирование системы безопасности по единым организационным, функциональным и методологическим принципам.

**Компетентность.** Система безопасности должна создаваться и управляться лицами, имеющими профессиональную подготовку, достаточную для корректной оценки обстановки и адекватного принятия решения, в том числе в условиях повышенного риска.

Для поддержания законности, правовые акты общего назначения, затрагивающие вопросы информационной безопасности, необходимые к изучению:

- Конституция Российской Федерации, принятая 12 декабря 1993 года.
- Гражданский кодекс Российской Федерации (редакцию от 15 мая 2001 года).
- Уголовный кодекс РФ (редакция от 14 марта 2002 года) Глава 28.
- Закон РФ от 21.07.1993 N 5485-1 (ред. от 29.07.2018) "О государственной тайне"
- Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ.
- Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ.
- Федеральный закон "О банках и банковской деятельности" от 02.12.1990 N 395-1.
- Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ.
- Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ.
- Trusted Network Interpretation. National Computer Security Center. -- NCSC-TG-005 , 1987 (интерпретация "Оранжевой книги" для сетевых конфигураций).
- Государственные стандарты, указы, пояснения к законам и технические регламенты ведомств.

Установление доверия безопасности, согласно "Общим критериям", основывается на активном исследовании объекта оценки.

Анализ системы безопасности предприятия содержит следующие шаги:

- Характеристика предприятия.
- Анализ действующей системы информационной безопасности предприятия.
- Выявление угроз информационной безопасности на предприятии.
- Анализ рисков.
- Мероприятия по улучшению системы информационной безопасности организации.
- Эффективность предложенных мероприятий.

После анализа системы необходимо разработать ее модель средством моделирования, которое представляет собой программный продукт автоматизации разработки схемы базы данных и определения необходимых ограничений целостности.

Огромным преимуществом ERwin является графический пользовательский интерфейс, базируемый на операционной системе Windows со встроенным инструментом для работы с ER-диаграммами (сущность-связь).

Информация о настройках программной среды и методов работы представлена в курсе «моделирование информационных систем».

## **6. Порядок выполнения лабораторной работы (этапы)**

1. Ознакомиться с требованиями законодательства Российской Федерации в области информационной безопасности автоматизированных систем, со стандартами и спецификациями в области информационной безопасности.
2. Проанализировать существующую систему информационной безопасности с конкретной организации (по вариантам),
3. В результате обследования учебного предприятия необходимо выделить сущности. Проектирование начинается с составления контекстной диаграммы для определения сущностей и связей между ними, так как на этой стадии еще точно неизвестны атрибуты конкретных сущностей и ограничения целостности. Описать каждую сущность: детальное описание сущностей помогает лучше разобраться в процессе функционирования модели. Создать инфологическую модель системы безопасности. Представленная модель оформляется с помощью языка ER-диаграмм. Стержневые сущности изображаются прямоугольниками, ассоциативные – шестиугольниками, характеристические – трапециями, а атрибуты – овалами.

В программе представлено четыре основных уровня отображения модели: полный логический, контекстный, с ключами, с описанием сущностей. После создания модели сущностей перейти к определению первичных и внешних ключей. Завершающим этапом необходимо определить остальные атрибуты сущностей, не вошедших в описательный модуль. В результате выполнения лабораторной работы получим отображение модели на полном логическом уровне.

4. Ответить на контрольные вопросы (контроль знаний) в форме «брейн ринга» при разделении на команды или индивидуально по вариантам.

## **7. Контрольные вопросы:**

### **Вариант 1**

1. Уровень безопасности C, согласно "Оранжевой книге", характеризуется:
  - произвольным управлением доступом
  - принудительным управлением доступом
  - верифицируемой безопасностью
2. Согласно рекомендациям X.800, аутентификация может быть реализована на:
  - сетевом уровне
  - транспортном уровне
  - прикладном уровне
3. Уголовный кодекс РФ не предусматривает наказания за:
  - неправомерный доступ к компьютерной информации
  - создание, использование и распространение вредоносных программ
  - массовую рассылку незапрошенной рекламной информации
4. Согласно Закону "О персональных данных", персональные данные – это:
  - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность
  - данные, хранящиеся в персональном компьютере
  - данные, находящиеся в чьей-либо персональной собственности
5. Согласно Закону "О лицензировании отдельных видов деятельности", лицензия – это:
  - специальное разрешение на осуществление конкретного вида деятельности
  - удостоверение, подтверждающее высокое качество изделия
  - документ, гарантирующий безопасность программного продукта
6. В законопроекте "О совершенствовании информационной безопасности" (США, 2001 год) особое внимание обращено на:
  - системы электронной коммерции
  - инфраструктуру для электронных цифровых подписей
  - средства электронной аутентификации
7. "Общие критерии" содержат следующие виды требований:
  - функциональные



- доверия безопасности
- экономической целесообразности

## Вариант 2

1. Уровень безопасности В, согласно "Оранжевой книге" характеризуется:
  - произвольным управлением доступом
  - принудительным управлением доступом
  - верифицируемой безопасностью
2. Согласно рекомендациям X.800, целостность с восстановлением может быть реализована на:
  - сетевом уровне
  - транспортном уровне
  - прикладном уровне
3. Уголовный кодекс РФ не предусматривает наказания за:
  - увлечение компьютерными играми в рабочее время
  - неправомерный доступ к компьютерной информации
  - нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
4. Согласно Закону "Об информации, информационных технологиях и защите информации", конфиденциальная информация – это:
  - информация с грифом "секретно"
  - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации
  - информация, доступ к которой ограничивается сертифицированными техническими средствами
5. Действие Закона "О лицензировании отдельных видов деятельности" не распространяется на:
  - деятельность по технической защите конфиденциальной информации
  - образовательную деятельность в области защиты информации
  - предоставление услуг в области шифрования информации
6. В следующих странах сохранилось жесткое государственное регулирование разработки и распространения криптосредств на внутреннем рынке:
  - Китай
  - Россия
  - Франция
7. В число классов функциональных требований "Общих критериев" входят:
  - анонимность
  - приватность
  - связь

### Отчет по лабораторной работе должен содержать:

1. Тему и цель лабораторной работы;
2. Вариант задания на лабораторную работу;
3. Результаты построения модели;
4. Выводы.

**Время на выполнение лабораторной работы – 6 часов.**

**Образовательная организация, авторы, эл. почта:** Кубанский государственный технологический университет, Власенко А.В., Корх И.А., aia2004@inbox.ru

## **Дисциплина: Программно-аппаратные средства защиты информации**

Образовательная программа: **10.05.03 Информационная безопасность автоматизированных систем, 10.03.01 Информационная безопасность**

Дисциплина: **Программно-аппаратные средства защиты информации**

### **Лабораторная работа.**

#### **DallasLock 8.0-C. Механизм дискреционного управления доступом.**

##### **Подсистема регистрации и учёта**

#### **1. Учебные цели:**

- Получить теоретические знания и навыки настройки дискреционного доступа, изучить функциональные возможности и настроить средство защиты информации от несанкционированного доступа (СЗИ от НСД) «DallasLock 8.0-C».

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- Знать структуру и составные модули, возможности работы СЗИ от НСД «DallasLock 8.0-C»,
- Владеть навыками настройки средства защиты и анализа журналов.

#### **3. Перечень материально-технического обеспечения**

- **Лабораторное оборудование и программное обеспечение:**
  - Лаборатория программно-аппаратных средств защиты информации.
  - Персональные компьютеры (ПК) с установленной операционной системой (ОС) Windows 7 Professional.
  - Программа виртуализации VMware Workstation Player.
  - Виртуальная машина Windows 7 Professional.
  - СЗИ от НСД «Dallas Lock 8.0-C».

#### **4. Задание на исследование**

- Изучение теоретических сведений.
- Установка системы защиты в автономном режиме.
- Создание и настройка учетных записей пользователей.
- Настройка прав доступа к каталогам (папкам) в соответствии с матрицей доступа.
- Настройка прав доступа к файлам в соответствии с матрицей доступа.
- Настройка замкнутой программной среды для пользователей.
- Настройка параметров аудита информации, анализ журналов аудита.

#### **5. Краткие теоретические сведения**

Система защиты информации от несанкционированного доступа Dallas Lock 8.0-C предназначена для предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных правил и норм и обладателями информации с нарушением установленных правил разграничения доступа к защищаемым ресурсам. Также осуществляется контроль за потоками информации, которые поступают в автоматизированную систему и выходят за пределы системы, таким образом обеспечивается защита информации в автоматизированной системе посредством её фильтрации.

Система защиты Dallas Lock 8.0-C является программным комплексом средств защиты информации в операционных системах семейства Windows и Linux с возможностью использования аппаратной идентификации пользователей и устройств.

Система защиты информации Dallas Lock 8.0-C используется в проектах по защите информации автоматизированных систем, система позволяет настроить их в соответствии требованиям безопасности информации.

Система защиты предназначена для использования на серверах (файловых, контроллерах домена и терминального доступа), портативных компьютерах (ноутбуках), персональных компьютерах. Может быть установлено на автономные персональные компьютеры, на компьютеры в составе локально-вычислительной сети (ЛВС), также под управлением контроллера домена.

Dallas Lock 8.0-C обеспечивает защиту информации от несанкционированного доступа на компьютер в сетях такие входы как локальный, сетевой и терминальный входы. Также средство защиты обеспечивает мандатное и дискреционное разграничение полномочий пользователей по доступу к файловой системе (ФС), устройствам, процессам и прочим ресурсам. Разграничения распространяются на все типы пользователей.

В СЗИ от НСД Dallas Lock 8.0-C реализовано ведение электронных журналов, в которых фиксируются действия пользователей:

- журнал входов. В журнал заносятся все входы (или попытки входов с указанием причины отказа) и выходы пользователей персонального компьютера, включая локальные, сетевые, на другие ПК, в том числе терминальные входы и входы для удаленного администрирования;
- журнал управления учетными записями. В журнал заносятся все события, связанные с созданием или удалением учетных записей пользователей, изменением их параметров;
- журнал ресурсов. В журнал заносятся события доступа к объектам ФС, программно-аппаратной среды, веткам реестра и к устройствам, для которых назначен аудит;
- журнал печати. В журнал заносятся все события, связанные с распечаткой документов на локальных или сетевых принтерах;
- журнал управления политиками. В журнал заносятся все события, связанные с изменением конфигурации СЗИ от НСД. Также в этот журнал заносятся события запуска/завершения модулей администрирования Dallas Lock 8.0-C;
- журнал процессов. Заносятся события запуска и завершения процессов в ОС;
- журнал пакетов межсетевого экрана (МЭ). В журнал заносятся все события, связанные с передачей пакетов данных в соответствии с заданными правилами в обоих направлениях через сетевые адаптеры компьютера;
- журнал соединений МЭ. В журнал заносятся сведения об истории сетевых соединений, устанавливаемых процессами (приложениями) в соответствии с заданными правилами;
- журнал событий ОС. В журнал заносятся сведения о событиях безопасности, генерируемых операционной системой и прикладным ПО;
- журнал трафика. В журнал заносятся события, связанные с проходящим сетевым трафиком через контролируемые сетевые интерфейсы;
- журнал контроля приложений. В журнал заносятся сведения об активности приложений, при вызове ими функций, связанных с безопасностью ОС. Для облегчения работы с журналами есть возможность фильтрации, архивации, группировки по заданному набору полей и экспорта записей журналов в различные форматы.

## 6. Порядок выполнения лабораторной работы (этапы)

### 1. Установка

- Запустить приложение DallasLock8.0C.msi
- Для защиты от нелегального использования продукта необходимо ввести номер лицензии Dallas Lock 8.0 и код технической поддержки.
- Оставить пустыми поля «Ввести компьютер в домен безопасности», выбрать стандартную конфигурацию.
- Проконтролировать, что установка компонентов (подсистем) прошла без ошибок и перезагрузить компьютер.

### 2. Создание и настройка учетных записей пользователей.

- Во вкладке «Учётные записи» создать пользователей User1 и User2. Задать им пароли не менее 6 буквенно-цифровых символов.
- Включить параметр: «Запретить работу при нарушенной целостности».

### 3. Настроить права доступа к каталогам (папкам) в соответствии с матрицей доступа, указанной в таблице 1.

**Таблица 1** – Права доступа на каталоги для пользователей

| Каталог: D:\Documents\PDocs  |              |               |
|------------------------------|--------------|---------------|
|                              | Пользователь | Права доступа |
|                              | User1        | RWX           |
|                              | User2        | RWX           |
| Каталог: D:\Documents\SDocs  |              |               |
|                              | Пользователь | Права доступа |
|                              | User1        | R--           |
|                              | User2        | RWX           |
| Каталог: D:\Documents\SSDocs |              |               |
|                              | Пользователь | Права доступа |
|                              | User1        | -WX           |
|                              | User2        | ---           |

R – чтение; W – запись, удаление, создание; X – выполнение.

- Создать папки PDocs, SDocs, SSDocs в каталоге Documents на диске D.
- В контекстном меню каталога выбрать «DL8.0:Права доступа...», затем выбрать вкладку «Дискреционный доступ».
- Чтобы назначить определенные дискреционные права для определенных пользователей необходимо при помощи кнопок «Пользователь», «Группы», «Все», «Удалить» выбрать определенные учетные записи пользователей или групп.
- Для выбранных пользователей необходимо задать набор разрешений/запретов, который будет определять права по доступу (обзор папки, изменение содержимого, удаление вложенных объектов, выполнение вложенных объектов, чтение разрешений, запись разрешений) к данному объекту.
- Для того, чтобы настроить аудит доступа к каталогу перейдем во вкладку «аудит доступа», далее нужно отметить флажком параметр «аудит включен», в зависимости от того, успешное или неудачное событие нужно зарегистрировать, выставить флажок в полях «Успех» или «Отказ» для операции, далее необходимо применить параметры
- Выполнить вход под пользователями User1 и User2, выполнить проверку настройки дискреционного доступа.

Результаты действий

#### 4. Настройка прав доступа к файлам в соответствии с матрицей доступа.

**Таблица 2** – Права доступа на файлы для пользователей

| Файл: C:\Windows\notepad.exe                        |              |               |
|-----------------------------------------------------|--------------|---------------|
|                                                     | Пользователь | Права доступа |
|                                                     | User1        | R-X           |
|                                                     | User2        | RWX           |
| C:\Program Files\Windows NT\Accessories\wordpad.exe |              |               |
|                                                     | Пользователь | Права доступа |
|                                                     | User1        | R--           |
|                                                     | User2        | ---           |

R – чтение; W – запись, удаление; X – выполнение.

- В контекстном меню файлов выбрать «DL8.0:Права доступа...», затем выбрать вкладку «Дискреционный доступ».
  - Чтобы назначить определенные дискреционные права для определенных пользователей необходимо при помощи кнопок «Пользователь», «Группы», «Все», «Удалить» выбрать определенные учетные записи пользователей или групп.
  - Для выбранных пользователей необходимо задать набор разрешений/запретов, который будет определять права по доступу (чтение, запись, удаление, выполнение, чтение разрешений, запись разрешений) к данному объекту.
  - Для того, чтобы настроить аудит доступа к каталогу перейдем во вкладку «аудит доступа», далее нужно отметить флажком параметр «аудит включен», в зависимости от того, успешное или неудачное событие нужно зарегистрировать, выставить флажок в полях «Успех» или «Отказ» для операции, далее необходимо применить параметры
  - Выполнить вход под пользователями User1 и User2, выполнить проверку настройки дискреционного доступа.
  - Результаты действий просмотреть в журнале ресурсов, журнале входов, журнале процессов. Проанализировать информацию, указанную в журналах аудита.
- #### 5. Настройка замкнутой программной среды для пользователей.
- Создать группу ZPS (Пользователи замкнутой программной среды).
  - Добавить в группу ZPS пользователей User1 и User2.
  - Во вкладке «Контроль ресурсов» выбрать меню «Глобальные», перейти к настройке параметра «Параметры ФС по умолчанию». Выбрать вкладку «Дискреционный доступ», для группы ZPS выбрать параметр «запретить» для «выполнение вложенных объектов», остальные права оставить без изменений (пустыми).
  - Каталогом C:\Windows, C:\ProgramFiles, C:\ProgramFiles (x86) задать права дискреционного доступа для группы ZPS «Только чтение».
  - Выполнить вход под пользователями User1 и User2, выполнить проверку настройки замкнутой программной среды.

#### 7. Контрольные вопросы:

1. Из каких подсистем состоит СЗИ от НСД Dallas Lock 8.0 С?
2. В чём заключается дискреционный принцип разграничения доступа?
3. Как реализован механизм дискреционный управления доступом?

4. Перечислите типы объектов и субъектов дискреционного доступа?
5. Механизм определения прав доступа пользователя?
6. Какие типы событий позволяет журналировать СЗИ от НСД?
7. Что такое «Замкнутая программная среда»?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** Новосибирский государственный технический университет, кафедра защиты информации, к.т.н., доцент Зырянов Сергей Алексеевич, ассистент Грищенко Лев Аркадьевич, l.grishhenko@corp.nstu.ru.

---

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, Обеспечение информационной безопасности распределенных информационных систем.

**Дисциплина:** Программно-аппаратные средства обеспечения информационной безопасности.

### **Лабораторная работа.**

#### **Определение качества детектирования вирусов средствами защиты компьютера от вредоносного программного обеспечения**

##### **1. Учебные цели:**

Определение степени защиты, обеспечиваемой антивирусным программным обеспечением. Получение навыков работы с антивирусными сканерами.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

###### **Уметь:**

- применять средства и системы защиты информационно-технологических ресурсов автоматизированной системы;

###### **Владеть:**

- методикой применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы.

##### **3. Лабораторное оборудование и программное обеспечение:**

- ПК (ЦПУ -1,2 ГГц, ОЗУ – 2048 Мб, HDD500Гб) ОС Windows, Kaspersky Removal Tools, антивирусный пакет «Антивирус Касперского», Dr.Web CureIT.

##### **4. Задание на исследование:**

- Используя тестовую антивирусную запись произвести исследование качества детектирования вирусов средствами защиты компьютера от вредоносного программного обеспечения

##### **5. Краткие теоретические сведения**

Компьютерный вирус – это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или FAT-таблицу, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает также, как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющихся в компьютере дисках. Но некоторые виды файлов вирус может "заразить". Это означает, что вирус может "внедриться" в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу.

Методы защиты от компьютерных вирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов.

Имеются две основные разновидности этих средств:

- копирование информации – создание копий файлов и системных областей дисков;
- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. Такая комбинация называется сигнатурой. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны".

Таким образом, из того, что программа не опознается детекторами как зараженная, не следует, что она здорова – в ней могут сидеть какой-нибудь новый вирус или слегка модифицированная версия старого вируса, неизвестные программам-детекторам.

Программы-ревизоры имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Многие программы-ревизоры являются довольно "интеллектуальными" – они могут отличать изменения в файлах, вызванные, например, переходом к новой версии программы, от изменений, вносимых вирусом, и не поднимают ложной тревоги. Дело в том, что вирусы обычно изменяют файлы весьма специфическим образом и производят одинаковые изменения в разных программных файлах. Понятно, что в нормальной ситуации такие изменения практически никогда не встречаются, поэтому программа-ревизор, зафиксировав факт таких изменений, может с уверенностью сообщить, что они вызваны именно вирусом.

Программы-фильтры, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не регистрируют подозрительные действия, а проверяют вызываемые на выполнение программы, на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны – они позволяют обнаружить многие вирусы на самой ранней стадии.

Программы-вакцины, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, "эшелонированная" оборона. Рассмотрим структуру этой обороны.

Средствам разведки в "обороне" от вирусов соответствуют программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

На переднем крае обороны находятся программы-фильтры. Эти программы могут первыми сообщить о работе вируса и предотвратить заражение программ и дисков.

Второй эшелон обороны составляют программы-ревизоры, программы-доктора и доктора-ревизоры.

Самый глубокий эшелон обороны – это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные. В "стратегическом резерве" находятся архивные копии информации. Это позволяет восстановить информацию при её повреждении.

Итак, одним из основных методов борьбы с вирусами является своевременная профилактика их появления и распространения. Только комплексные профилактические меры защиты обеспечивают защиту от возможной потери информации. В комплекс таких мер входят:

1. Регулярное архивирование информации (создание резервных копий важных файлов и системных областей винчестера).
2. Использование только лицензионных дистрибутивных копий программных продуктов.
3. Систематическая проверка компьютера на наличие вирусов. Компьютер должен быть оснащен эффективным регулярно используемым и постоянно обновляемым пакетом антивирусных программ. Для обеспечения большей безопасности следует применять параллельно несколько антивирусных программ.
4. Осуществление входного контроля нового программного обеспечения, поступивших дискет. При переносе на компьютер файлов в архивированном виде после распаковки их также необходимо проверять.
5. При работе на других компьютерах всегда нужно защищать свои дискеты от записи в тех случаях, когда на них не планируется запись информации.
6. При поиске вирусов следует использовать заведомо чистую операционную систему, загруженную с дискеты.
7. При работе в сети необходимо использовать антивирусные программы для входного контроля всех файлов, получаемых из компьютерных сетей. Никогда не следует запускать непроверенные файлы, полученные по компьютерным сетям.

Распространенные антивирусные программы:

1. Kaspersky Internet Security. Основное достоинство – это комплексный подход к защите информации на компьютере пользователя. Продукт обеспечивает защиту от всех видов угроз, которые существуют на сегодняшний момент в мире, и, что самое важное, – от еще неизвестных угроз.
2. DrWeb. Главной особенностью "Лечебной паутины" является наличие эвристического анализатора, который подключается ключом /S. Баланса между скоростью и качеством можно добиться, указав ключу уровень эвристического анализа: 0 – минимальный, 1 – оптимальный, 2 – максимальный; при этом, естественно, скорость уменьшается пропорционально увеличению качества. К тому же Dr.Web позволяет тестировать файлы, вакцинированные CPAV, а также упакованные LZEXE, PKLITE, DIET. Для этого следует указать ключ /U (при этом распаковка файлов будет произведена на текущем устройстве) или /U диск: (где диск: – устройство, на котором будет производиться распаковка), если дискета, с которой запущен Doctor Web защищена от записи.
3. NAV (Symantec). По качеству детектирования вирусов – достаточно средняя программа. Вызывает ложные срабатывания. По остальным пунктам замечаний не имеет. Удобный пользовательский интерфейс, большое количество дополнительных функций, версии под все популярные платформы.

Из-за недостаточно качественного детектирования вирусов пользователи NAV часто попадают в ситуацию, когда для обнаружения и лечения вируса им приходится обращаться к антивирусным продуктам других фирм.

Активность и правильность настройки антивирусной программы можно проверить с помощью тестового вируса, имеющего запись, например,

DELE-X50!P % @AP[4PZX54(P^)^7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*.

Возможно использование модификаций проверочного вируса посредством добавления специальных ключей.

При условии правильной работы антивирусного сканера вирус будет опознан.

**Таблица 1**

| Модификации тестового "вируса"                    |                                                                                            |
|---------------------------------------------------|--------------------------------------------------------------------------------------------|
| Префикс                                           | Тип объекта                                                                                |
| Префикс отсутствует, стандартный тестовый "вирус" | Зараженный. При попытке лечения объекта возникает ошибка; объект удаляется.                |
| CORR-                                             | Поврежденный.                                                                              |
| SUSP-                                             | Возможно, заражен вирусом (код неизвестного вируса).                                       |
| WARN-                                             | Заражен модификацией вируса (модифицированный код известного вируса).                      |
| ERRO-                                             | Не проверенный из-за сбоя.                                                                 |
| CURE-                                             | Зараженный. Объект подвергается лечению, при этом текст тела "вируса" изменяется на CURED. |
| DELE-                                             | Зараженный. Объект автоматически удаляется.                                                |

## 6. Порядок выполнения лабораторной работы

1. Откройте блокнот и введите:

DELE-X50!P % @AP[4PZX54(P^)^7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*.

Сохраните запись в файл с именем, например, eicar\_dele.com. просканируйте систему антивирусным сканером Kaspersky на предмет выявления вирусной программы.

2. Последовательно создайте несколько модификаций, добавляя новые префиксы таким образом, чтобы были последовательно использованы все допустимые дополнения к данной записи.

3. Создайте каталог на диске и сохраните в нем созданные вами тестовые аналоги "вирусов".

4. Последовательно произведите проверку вашего компьютера или каталога, где хранятся созданные вами "вирусы" сканерами Kaspersky, DrWeb, AVZ. При проверке, по мере обнаружения зараженных объектов, на экран будут выведены диалоги с информацией об объекте и запросом действия на их обработку. Таким образом, выбирая различные варианты действий в диалогах, появляющихся в процессе проверки, вы сможете проверить реакцию антивируса при обнаружении объектов различных типов.

5. Определите причину различий в результатах работы предоставленных антивирусных программ, и заполните отчет.

#### **Содержание отчета:**

1. Название и цель лабораторной работы;
2. Указать, какие модификации были опознаны антивирусными сканерами
3. Указать действия произведенные сканерами при обнаружении проверочного вируса и его модификаций.

#### **7. Контрольные вопросы:**

1. Что называется компьютерным вирусом?
2. Какая программа называется "зараженной"?
3. Что происходит, когда зараженная программа начинает работу?
4. Каковы признаки заражения вирусом?
5. Каковы последствия заражения компьютерным вирусом?
6. По каким признакам классифицируются компьютерные вирусы?
7. Как классифицируются вирусы по среде обитания?
8. На какие виды можно подразделить программы защиты от компьютерных вирусов?
9. Как действуют программы-детекторы?
10. Что называется сигнатурой?
11. Всегда ли детектор распознает зараженную программу?
12. Каков принцип действия программ-ревизоров, программ-фильтров.

**Время на выполнение лабораторной работы – 2 часа.**

**Образовательная организация, авторы, эл. почта:** Новосибирский государственный технический университет, кафедра защиты информации, к.т.н., доцент Зырянов Сергей Алексеевич, ассистент Грищенко Лев Аркадьевич, l.grishhenko@corp.nstu.ru

---

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, Обеспечение информационной безопасности распределенных информационных систем.

**Дисциплина:** Программно-аппаратные средства обеспечения информационной безопасности.

### **Лабораторная работа.**

#### **Определение жизненного цикла вредоносных программ**

##### **1. Учебные цели:**

- Реконструкция жизненного компьютерного вируса с целью разработки мер противодействия его вредоносной деятельности и последующего удаления.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

###### **Уметь:**

- применять средства и системы защиты информационно-технологических ресурсов автоматизированной системы;

###### **Владеть:**

- методикой применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы.



### 3. Лабораторное оборудование и программное обеспечение:

- ПК (ЦПУ-1,2 ГГц, ОЗУ- 2048 Мб, HDD500Гб) ОС Windows, MS Office, Браузер.

### 4. Задание на исследование:

- Определение типов представленных ниже вирусов, произвести поэтапный разбор их жизненного цикла, реконструировать жизненный цикл выбранного вируса с целью разработки мер противодействия его вредоносной деятельности и последующего удаления.

### 5. Краткие теоретические сведения

Компьютерные вирусы обладают следующими свойствами:

- способность к самодублированию;
- способность к ассоциированию с другими процессами и объектами операционной среды;
- способность к скрытию признаков своего присутствия и вредоносной деятельности в программной среде.

Проявление наличия вируса в работе операционной системе(ОС):

- некоторые программы перестают работать или начинают работать неправильно;
- на экран выводятся посторонние сообщения, символы и т.д.;
- работа на компьютере существенно замедляется;
- некоторые файлы оказываются испорченными и т.д.
- операционная система не загружается;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти и т.п.

Вирусы можно классифицировать по следующим признакам:

- по алгоритму работы:
- компаньон-вирусы;
- вирусы-"черви";
- паразитические;
- студенческие;
- вирусы-невидимки;
- полиморфные.
- по среде обитания вируса:
- файловые;
- загрузочные;
- специальные;
- сетевые;
- макровирусы.
- по способу заражения среды обитания:
- резидентный;
- нерезидентный.
- по деструктивным возможностям:
- безвредные (шутки);
- опасные (повреждают ПО);
- очень опасные (повреждают ПК).

Наиболее сложно определить классификационную принадлежность вирусов типа Троян (тройная программа, троянская программа). Они отличаются отсутствием механизма дублирования.

Виды троянских программ:

1. Клавиатурный шпион (Trojan-SPY) – троянская программа, постоянно находящиеся в памяти и сохраняющая все данные, поступающие от клавиатуры, с целью последующей передачи этих данных злоумышленнику.
2. Похититель паролей (Trojan-PSW) – троянская программа, также предназначенная для получения паролей, но не использующая слежение за клавиатурой.
3. Утилита удаленного управления (Backdoor) – троянская программа, обеспечивающая полный удаленный контроль над компьютером пользователя.
4. Анонимный smtp-сервера и прокси (Trojan-Proxy) – троянская программа, выполняющая функции почтовых серверов или прокси и использующаяся в первом случае для спам-рассылок, а во втором для заметания следов хакерами
5. Модификатор настроек браузера (Trojan-Clicker) – троянская программа, меняющая стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, для организации несанкционированных обращений к Интернет-ресурсам
6. Инсталлятор вредоносных программ (Trojan-Dropper) – троянская программа, скрыто устанавливающая другие программы.

7. Загрузчик вредоносных программ (Trojan Downloader) – троянская программа, предназначенная для загрузки на компьютер новых версий вредоносных программ.
8. Уведомители об успешной атаке (Trojan-Notifier) – троянские программы данного типа предназначены для сообщения своему командному серверу данных о зараженном компьютере
9. "Бомбы" в архивах (ARCBomb) – троянские программы, представляющие собой архивы, специально оформленные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать.
10. Логические бомбы – троянские программы, которые при определенных условиях реализуют заданный порядок действий.

Жизненный цикл вирусов включает в себя две основные стадии – хранение (латентная фаза) и исполнение.

В ходе латентной фазы вирус не активен, не может контролировать работу операционной системы, и просто хранится на диске совместно с объектом, в который он внедрен.

Переход от латентной фазы к исполнению вируса осуществляется по некоторому активизирующему событию (открытие файла, наступление определенной даты и т.д.).

Фаза исполнения вируса, как правило, состоит из следующих этапов.

1. Загрузка вируса в память.
2. Поиск «жертвы».
3. Заражение «жертвы» (инфицирование).
4. Выполнение деструктивных функций.
5. Передача управления программе-носителю вируса.

Как правило, загрузка вируса в память осуществляется ОС одновременно с загрузкой исполняемого объекта, в который внедрен вирус.

По способу поиска «жертвы» вирусы можно разделить на два класса.

- вирусы, осуществляющие «активный» поиск с использованием функций ОС;
- вирусы, осуществляющие «пассивный поиск» с помощью механизмов расстановки «ловушек» для программных файлов (так часто поступают макровирусы).

Инфицирование объектов компьютерной системы осуществляется различными способами в зависимости от типа вируса. В простейшем случае этап заражения жертвы сводится к самокопированию кода вируса в выбранный в качестве жертвы объект (файл, загрузочный сектор, псевдосбойные сектора и т.д.).

Полиморфные вирусы

Помимо простого копирования кода вируса в заражаемый объект на этом этапе могут использоваться более сложные алгоритмы, обеспечивающие защиту вируса на стадии хранения (шифрование, «мутации» кода и т.п.). Модификация предполагает, что часть кода вируса, относящаяся к расшифровщику, модифицируется так, чтобы возникли различия с оригиналом, но результаты работы остались неизменными. Наиболее распространенными приемами модификации кода являются следующие:

- изменение порядка независимых инструкций;
- замена некоторых инструкций на эквивалентные по результату работы;
- замена используемых в инструкциях регистров на другие;
- внедрение случайным образом зашумляющих инструкций.

По характеру выполнения деструктивных функций вирусы делят на «безвредные», «неопасные», «опасные» и «очень опасные».

В «безвредных» вирусах реализована только функция самодублирования.

«Неопасные» вирусы – это вирусы, присутствие которых в системе связано с различными эффектами, но которые не наносят вред программам и данным.

«Опасные» вирусы могут стать причиной сбоя системы. «Очень опасные» вирусы приводят непосредственно к разрушению программ и данных.

Процесс размножения вирусов может быть условно разделен на несколько стадий:

- активация вируса;
- поиск объектов для заражения;
- подготовка вирусных копий;
- внедрение вирусных копий.

Существуют разновидности жизненных циклов вирусов в соответствии с их особенностями построения и функционирования.

Жизненный цикл червей можно разделить на определенные стадии:

- проникновение в систему;
- активация;
- поиск "жертв";
- подготовка копий;
- распространение копий.

У троянских программ вследствие отсутствия функций размножения и распространения, их жизненный цикл меньше чем у вирусов – всего три стадии:

- проникновение на компьютер;
- активация;
- выполнение заложенных функций.

Удаление вируса, как правило, прерывает выполнение его жизненного цикла. Поэтому, чтобы определить методику удаления нужно определить последовательность выполнения всех действий вируса на всех этапах его работы.

Рассмотрим вирус W32.Explet.A@mm.

Когда он загружается, то производит следующие действия:

- 1) Создает mutex по имени "Expletus", который позволяет только одному ему загружаться.
- 2) Копирует файл %Windir %\system32\upn.exe.
- 3) Добавляет в системный реестр:  
"NvClipRsv"="<path to the worm>"HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- 4) Восстанавливает папку KaZaA  
"DIDir0" HKEY\_CURRENT\_USER\Software\Kazaa\Transfer
- 5) Копирует след. файлы в папки с доступом:  
AVP5.xcrack.exe  
hx00def.exe  
ICQBomber.exe  
InternetOptimizer1.05b.exe  
Shrek\_2.exe  
UnNukeit9xNTICQ04noimageCrk.exe  
YahooDBMails.exe
- 6) Копирует по сети во все доступные папки:  
hx00def.exe  
ICQBomber.exe  
InternetOptimizer1.05b.exe  
Shrek\_2.exe  
UnNukeit9xNTICQ04noimageCrk.exe  
YahooDBMails.exe
- 7) Перезаписывает файл хостов file %Windir %\system32\drivers\etc\hosts  
127.0.0.1 downloads-us1.kaspersky-labs.com  
127.0.0.1 downloads1.kaspersky-labs.com  
127.0.0.1 downloads4.kaspersky-labs.com  
127.0.0.1 downloads2.kaspersky-labs.com  
127.0.0.1 downloads-eu1.kaspersky-labs.com
- 8) Пытается размножиться через уязвимость LSASS и DCOM порты 135 и 445
- 9) Ищет случайный TCP порт. Если связь установлена, это может послать себя отдаленному компьютеру.
- 10) Восстанавливает адрес электронной почты от файлов с .htm.html.php.tbb, и .txt расширениями {продлениями}, на всех установленных дисках от C до Y.  
Червь избегает адресов электронной почты, основанных на адресе фильтрации

Удаление:

1. Необходимо отменить восстановление Системы, (Windows Me/XP).
2. Необходимо обновить антивирусную базу.
3. Перезапускаем компьютер в Безопасном режиме или VGA режиме.
4. Запускаем сканирование и удаляем все файлы, обнаруженные как W32.Explet.A@mm.
5. Удаляем всё лишнее в системном реестре
6. Удаляем лишнее в файле хоста

## 6. Порядок выполнения лабораторной работы

Этап 1. Определение жизненного цикла вируса (ЖЦ) Win32.Gpcode.ak:

- Определить тип вируса Win32.Gpcode.ak по представленной спецификации.
- Реконструировать его жизненный цикл таким образом, чтобы каждому этапу ЖЦ, свойственного данному вирусу, была приведена его конкретная реализация.
- Определите методы его удаления.

Спецификация вируса Win32.Gpcode.ak.

Платформа: Win32

Вредоносная программа, шифрующая файлы пользователя на зараженном компьютере. Является приложением Windows (PE EXE-файл), имеет размер 8030 байт.

Деструктивная активность.

После запуска вирус создает в памяти компьютера уникальный идентификатор (mutex) `_G_P_C_`, для идентификации своего присутствия в системе.

Далее, вирус приступает к последовательному обходу всех логических дисков и поиску на них файлов для шифрования. Вирус шифрует все найденные пользовательские файлы со следующими расширениями: 7z, abk, abd, acad, arh, arj, ace, arx, asm, bz, bz2, bak, bcb, c, cc, cdb, cdw, cdr, cer, cgi, chm, cnt, cpp, css, csv, db, db1, db2, db3, db4, dba, dbb, dbc, dbd, dbe, dbf, dbt, dbm, dbo, dbq, dbx, Djvu, doc, dok, dpr, dwg, dxf, ebd, eml, eni, ert, fax, flb, frm, frt, frx, fig, gtd, gz, gzip, gfa, gfr, gfd, h, inc, igs, iges, jar, jad, Java, jpg, jpeg, Jfif, jpe, js, jsp, hpp, htm, html, key, kwm, Ldif, lst, lsp, lzh, lzw, ldr, man, mdb, mht, mmf, mns, mnb, mnu, mo, msb, msg, mxl, old, p12, pak, pas, pdf, pem, pfx, php, php3, php4, pl, prf, pgr, prx, pst, pw, pwa, pwl, pwm, pm3, pm4, pm5, pm6, rar, rnr, rnd, rtf, Safe, sar, sig, sql, tar, tbb, tbc, tdf, tgz, txt, uue, vb, vcf, wab, xls, xml.

Для шифрования файлов вирус использует встроенные в операционную систему Windows криптоалгоритмы (Microsoft Enhanced Cryptographic Provider v1.0). Файлы шифруются при помощи алгоритма RC4. Ключ шифрования затем шифруется открытым ключом RSA (длиной 1024 бит), содержащимся в теле вируса.

Алгоритм RSA основан на разделении ключей шифрования на секретный и открытый. Принцип шифрования при помощи RSA гласит: для того, чтобы зашифровать сообщение достаточно иметь один лишь открытый ключ. Расшифровать зашифрованное сообщение можно только располагая секретным ключом.

Вирус создает зашифрованную копию файла, имеющую оригинальное имя файла и расширение к которому добавляется `_CRYPT`. Пример:

- первоначальный файл: WaterLilles.jpg
- зашифрованный файл: WaterLilles.jpg.\_CRYPT

Затем первоначальный файл удаляется.

В каждый каталог, файлы которого были зашифрованы, вредоносная программа помещает файл `<!_READ_ME!.txt>` следующего содержания:

```
Your files are encrypted with RSA-1024 algorithm.
To recovery your files you need to buy our decryptor.
To buy decrypting tool contact us at: [censored]@yahoo.com
=== BEGIN ===
[key] === END ===
```

Файлы, находящиеся в каталоге Program Files шифрованию не подвергаются. Также вирус не шифрует файлы: имеющие атрибуты «системный» и «скрытый»; имеющие размер меньше 10 байт; имеющие размер больше 734003200

В ходе своей работы вирус не регистрирует себя в системном реестре.

По окончании работы вирус создает VBS-файл, который удаляет основное тело вируса с компьютера и выводит на экран MessageBox – сообщение об удалении тела вируса

Этап 2. Определение жизненного цикла вируса Backdoor.Win32.Landis.b:

- Определить тип вируса Backdoor.Win32.Landis.b по представленной спецификации.
- Реконструировать его жизненный цикл таким образом, чтобы каждому этапу ЖЦ, свойственного данному вирусу, была приведена его конкретная реализация.
- Определите методы его удаления.

Спецификация вируса Backdoor.Win32.Landis.b.

Backdoor.Win32.Landis.b («Лаборатория Касперского») также известен как: W32/Generic.worm!p2p (McAfee), W32.Chod.D (Symantec), BackDoor.Generic.1066 (Doctor Web), Worm.MytoB.GH (ClamAV), Trj/MultidroppeR.ARF (Panda), троянская программная программа, предоставляющая злоумышленнику удаленный доступ к зараженной машине.

Управляется через IRC. Представляет собой Windows PE-EXE файл. Имеет размер около 113 КБ. При инсталляции бэкдор создает папку со случайным именем в системном каталоге Windows и копирует себя в эту папку с именем `csrss.exe`.

Также в данной папке бекдор создает следующие файлы:

- `%System%\drtusi\csrss.dat`
- `%System%\drtusi\csrss.ini`

После чего оригинальный запускаемый файл удаляется. Бекдор создает ссылку на себя в каталоге автозагрузки: `%UserProfile%\Start Menu\Programs\Startup\csrss.lnk`

Затем регистрирует себя в ключах автозапуска системного реестра:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
[HKCU\Software\Microsoft\Windows\CurrentVersion\Run]
"csrss"="
```

Программа соединяется с различными серверами IRC и получает команды удаленного управления от «хозяина». Спектр доступных команд очень разнообразен и позволяет осуществлять полный контроль над системой, а также осуществлять атаки на другие компьютеры, скачивать файлы и т.д.

Помимо этого, вредоносная программа обладает следующей функциональностью:

- 1) распространение по команде злоумышленника по каналам MSN Messenger ссылки, призывающей пользователей скачать копию данного бекдора; при этом ссылка выглядит весьма безопасно: [http://www.vbulletin.com/\[removed\]](http://www.vbulletin.com/[removed]), – очень похоже на адрес авторитетного журнала антивирусной индустрии Virus Bulletin, и может вызвать заблуждение пользователей;
- 2) загрузка и запуск на зараженном компьютере различных файлов;
- 3) удаление файлов;
- 4) остановка различных активных процессов;
- 5) перезагрузка компьютера;
- 6) проведение DoS-атак;
- 7) отсылка злоумышленнику подробной информации о системе, в том числе вводимых с клавиатуры паролей и другой секретной информации;
- 8) выполнение на зараженном компьютере различных команд;
- 9) загрузка своих обновлений.

Бэкдор изменяет файл %System %\drivers\etc\hosts, дописывая в него нижеприведенный текст и, тем самым, блокируя обращения к данным сайтам:

```
127.0.0.1 avp.com
127.0.0.1 download.mcafee.com
127.0.0.1 kaspersky.com
127.0.0.1 zonelabs.com и т.д.
```

Landis.b выгружает из системы процессы, содержащие в именах следующие строки: bbeagle.exe, regedit.exe, winsys.exe, zapro.exe, zlclient.exe и т.п.

Этап 3. Определение жизненного цикла вируса W32.Zotob.A:

- Определить тип вируса W32.Zotob.A по представленной спецификации.
- Реконструировать его жизненный цикл таким образом, чтобы каждому этапу ЖЦ, свойственного данному вирусу, была приведена его конкретная реализация.
- Определите методы его удаления.

Спецификация вируса W32.Zotob.A.

W32.Zotob.A – вирус, эксплуатирующий уязвимость в Microsoft Windows Plug and Play сервисе, описанную в бюллетене безопасности MS05-039.

W32.Zotob.A не заражает компьютеры под управлением Windows 95/98/Me/NT4. Несмотря на это, они могут использоваться для заражения других уязвимых компьютеров.

При запуске вирус W32.Zotob.A выполняет следующие действия:

1. Создает следующий флаг для того, чтобы только одна копия червя выполнялась на скомпрометированном компьютере: B-O-T-Z-O-R.
2. Копирует себя как %System %\botzor.exe.
3. Добавляет значение: "WINDOWS SYSTEM" = "botzor.exe" в подключи реестра: HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices.
4. Изменяет значение: "Start" = "4" в ключе реестра: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess чтобы отключить Shared Access сервис в Windows 2000/XP.
5. Соединяется с IRC сервером на домене: по 8080 TCP порту. Что дает удаленный неавторизованный доступ.
6. Открывает FTP сервер по 33333 TCP порту.
7. Генерирует случайный IP адрес из текущего IP адреса. Червь оставляет первые два октета IP адреса системы и изменяет случайным образом последние два октета. Например, если IP адрес системы 192.168.0.1, червь попытается заразить IP адреса, начиная с 192.168.x.x.
8. Пытается распространиться на компьютеры со случайными IP адресами, открывая бекдор на 8888 TCP порту на удаленном компьютере. Червь пытается эксплуатировать уязвимость в Microsoft Windows Plug and Play сервисе, описанную в Microsoft Security Bulletin MS05-039
9. Копирует следующий файл в скомпрометированный компьютер и выполняет FTP скрипт, содержащийся в нем: %System %\2pac.txt.
10. Загружает и выполняет копию червя с предварительно созданного FTP сервера на зараженном компьютере: %System %\haha.exe.
11. Добавляет следующие записи в хост файл:  
Made By .... Greetz to good friend [REMOVED] in the next 24hours!!!  
127.0.0.1 www.symantec.com  
127.0.0.1 securityresponse.symantec.com  
127.0.0.1 symantec.com  
127.0.0.1 www.sophos.com  
127.0.0.1 sophos.com  
127.0.0.1 www.mcafee.com

Этап 4. Составьте отчет.

**Содержание отчета:**

1. Название и цель лабораторной работы;
2. Указание типа вируса с указанием его типологических особенностей
3. Реконструкция жизненного цикла вируса с указанием конкретной реализации действий вируса на каждом этапе ЖЦ.
4. Рекомендации по удалению вируса.

**7. Контрольные вопросы**

13. Что такое троянская программа?
14. По каким признакам классифицируются компьютерные вирусы?
15. Дайте определение понятию жизненный цикл вируса
16. Чем отличается жизненный цикл троянской программы и компьютерного «червя»?
17. Приведите классификацию компьютерных вирусов
18. Приведите классификацию троянской программы?

**Время на выполнение лабораторной работы – 2 часа.**

**Образовательная организация, авторы, эл. почта:** Федеральное государственное бюджетное образовательное учреждение высшего образования Калининградский государственный технический университет» Балтийская государственная академия рыбопромыслового флота, a.zhestovskiy@bk.ru

---

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, Обеспечение информационной безопасности распределенных информационных систем

**Дисциплина:** Программно-аппаратные средства обеспечения информационной безопасности

**Лабораторная работа.**

**DallasLock 8.0-С. Мандатное разграничение доступа.**

**Подсистема обеспечения целостности**

**1. Учебные цели:**

- Получить теоретические знания и навыки настройки мандатного разграничения доступа, подсистемы обеспечения целостности СЗИ от НСД доступа «DallasLock 8.0-С».

**2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- Знать принцип мандатного разграничения доступа, механизмы работы подсистемы обеспечения целостности средства защиты информации от несанкционированного доступа «DallasLock 8.0-С»,
- Владеть навыками настройки средства защиты.

**3. Перечень материально-технического обеспечения**

- **Лабораторное оборудование и программное обеспечение:**
  - Лаборатория программно-аппаратных средств защиты информации.
  - Персональные компьютеры (ПК) с установленной операционной системой (ОС) Windows 7 Professional.
  - Программа виртуализации VMware Workstation Player.
  - Виртуальная машина Windows 7 Professional.
  - СЗИ от НСД «Dallas Lock 8.0-С».

**4. Задание на исследование:**

- Изучение теоретических сведений.
- Редактирование уровней мандатного доступа.
- Настройка учетных записей пользователей.
- Настройка прав мандатного доступа к каталогам (папкам).
- Создание разделяемых папок.
- Настройка программ для работы в различных режимах доступа
- Настройка параметров контроля целостности.

- Тестирование функционала средства защиты
- Контроль целостности файлов средства защиты.

## 5. Краткие теоретические сведения

В DallasLock 8.0-С реализован мандатный принцип разграничения доступа (применяется полностью независимый от ОС механизм), при котором каждому пользователю и каждому защищаемому объекту присваивается уровень доступа (по умолчанию, все объекты имеют уровень 0 «открытые данные», но он может быть поднят до любого из семи доступных). Пользователь будет иметь доступ к объектам, уровень доступа которых не превышает его собственный.

Каждому объекту файловой системы и подключаемому несистемному устройству можно присвоить метку конфиденциальности. Метки конфиденциальности имеют номера от 0 до 7. Чем больше номер, тем выше уровень конфиденциальности. Если не указана никакая метка, то считается, что объект имеет метку 0 (ноль) – открытые данные. Если метку конфиденциальности присвоить папке (диску), то все объекты, находящиеся в данной папке (диске) будут иметь ту же метку, за исключением тех случаев, когда им явно присвоены другие метки конфиденциальности.

Для удобства работы, меткам конфиденциальности можно присваивать имена. По умолчанию первым пяти уровням конфиденциальности (от 0 до 4) присвоены следующие наименования: 0 (Открытые данные); 1 (Конфиденциальные данные); 2 (Персональные данные); 3 (Секретные данные); 4 (Сов. секретно).

Эти имена можно сменить на любые другие, на работу системы защиты это никак не повлияет. Для системы защиты имеет значение только номер.

Для каждого пользователя в профиле его учетной записи также устанавливается уровень конфиденциальности от 0 (нуля) до 7 (семи).

Пользователи, имеющие уровень конфиденциальности 0 (ноль), имеют доступ только к объектам ФС, имеющим метку конфиденциальности 0. Пользователи, имеющие уровень конфиденциальности 1 (один), имеют доступ только к объектам ФС, имеющим метки конфиденциальности 0 (ноль) и 1 (один). Имеющие уровень конфиденциальности 2 (два) – только к объектам с метками 0 (ноль), 1 (один), 2 (два). И так далее. Пользователи уровня 7 (семь) имеют доступ ко всем объектам.

При входе в операционную систему пользователь может выбрать уровень доступа, не превышающий установленный для него уровень мандатного доступа. Например, если пользователь имеет уровень мандатного доступа 5 (пять), то он может войти в систему с уровнями от 0 (нуля) до 5 (пяти). Если пользователь выберет уровень доступа, который превышает собственный уровень конфиденциальности, то система защиты выдаст сообщение об ошибке «Мандатный уровень указан неверно». Мандатный уровень доступа, с которым пользователь вошёл в систему называется «текущий уровень доступа». Также пользователь, не производя выход из системы, в процессе, работы может поднять свой текущий уровень конфиденциальности, но не выше своего максимально. Понизить же текущий уровень можно, только начав новый сеанс работы.

В системе защиты предусмотрен механизм, который позволяет предотвратить понижение уровня мандатного доступа. Механизм действует следующим образом:

- При входе в систему система защиты позволяет пользователю выбрать уровень мандатного доступа, который не превышает установленный для него уровень.
- Запись во все объекты (изменение файлов) производится только тогда, когда уровень мандатного доступа файла или каталога равен текущему уровню доступа пользователя, если же это условие не выполняется, то действие блокируется системой защиты (за исключением «разделяемых» папок).

Подсистема контроля целостности обеспечивает контроль целостности файловой системы, программно-аппаратной среды и реестра, периодическое тестирование СЗИ от НСД, наличие средств восстановления СЗИ от НСД, восстановление файлов и веток реестра в случае нарушения их целостности. При обнаружении нарушения целостности в системе DallasLock 8.0-С происходит следующее:

- Блокировка ПК (если у пользователя установлено соответствующее свойство).
- Вывод предупреждения.
- Занесение события в журнал.
- Отправка сообщения на Сервер безопасности (для ПК в Домене безопасности).

## 6. Порядок выполнения лабораторной работы (этапы):

### 1. Редактирование уровней мандатного доступа.

Перейти во вкладку «Параметры безопасности», далее выбрать меню «Уровни доступа», отредактировать уровни мандатного доступа. Удалить уровни №№ 3,4 с помощью переименования.

### 2. Настройка учетных записей пользователей.

Задать пользователям уровень мандатного доступа: User1-«Конфиденциальные данные», User2-«Персональные данные».

### 3. Настройка прав мандатного доступа к каталогам (папкам).

- Создать папки KD\_Docs и PD\_Docs в каталоге D:\Documents\, назначить им уровни доступа «Конфиденциальные данные» и «Персональные данные» соответственно.

- В контекстном меню каталогов (папок) выбрать «DL8.0: Права доступа...», затем выбрать вкладку «Мандатный доступ», установить флажок на параметр «Мандатный доступ включен», затем выбрать соответствующую классификационную метку мандатного доступа.
- Выполнить вход под пользователями User1 и User2, выполнить проверку настройки мандатного доступа.

#### 4. Создание разделяемых папок.

Для создания разделяемой папки следует в контекстном меню каталога выбрать «DL8.0: Права доступа...», выбрать вкладку «Мандатный доступ», установить флажок на параметр «Мандатный доступ включен», затем установить флажок «Папка является разделяемой».

Создать папку Razd\_Docs в каталоге D:\Documents\, сделать её разделяемой и проверить, выполнив вход в систему с учётной записью User2, используя различные уровни доступа.

#### 5. Настройка программ для работы в различных режимах доступа.

- Для настройки будет использоваться Microsoft Office Word Enterprise 2007, так как при работе пользователя User1 с программой выполняется сохранение временных файлов в следующие директории:

C:\Users\User1\AppData\Roaming\Microsoft  
 C:\Users\User1\AppData\Local\Temp  
 C:\Users\User1\AppData\Local\Microsoft\Windows\INetCache  
 C:\ProgramData\Microsoft\OFFICE\DATA  
 C:\Users\User1\AppData\Local\Microsoft\FORMS  
 C:\Users\User1\AppData\Local\Microsoft\Windows\Temporary Internet Files

- Для этих папок следует выполнить следующие действия: в контекстном меню каталога выбрать «DL8.0: Права доступа...», выбрать вкладку «Мандатный доступ», установить флажок на параметр «Мандатный доступ включен», затем установить флажок «Папка является разделяемой».
- Выполнить вход под пользователями User1 и User2 с максимальными уровнями доступа, запустить Microsoft Office Word Enterprise 2007, создать и отредактировать файл. При успешной настройке разделяемых папок ошибок об отказе доступа не будет. Иначе настройка будет производиться с помощью журнала процессов. Этот журнал позволяет просмотреть, к какому файловому ресурсу было отказано в доступе.

#### 6. Настройка параметров контроля целостности.

- Перейти во вкладку «Параметры безопасности», далее выбрать меню «Контроль целостности», задать значение «3 мин.» следующим параметрам:
  - периодический контроль ФС;
  - периодический контроль прогр. апп. среды;
  - периодический контроль реестра;
  - результаты контроля представить в отчёте по лабораторной работе.

#### 7. Тестирование функционала средства защиты.

- Открыть главное меню DallasLock 8.0-С.
- Выбрать «Тестирование функционала СЗИ...», нажать на кнопку «Запустить».
- Результаты тестирования представить в отчёте по лабораторной работе.

#### 8. Контроль целостности файлов средства защиты

- Перейти во вкладку «Контроль ресурсов», далее выбрать меню «Контроль целостности», в панели «Действия» выбрать кнопку «Проверить».
- В результате отобразятся контрольные суммы и расчетные контрольные суммы. При успешной проверки контрольные суммы совпадут.

#### 7. Контрольные вопросы:

1. В чём заключается мандатный принцип разграничения доступа?
2. Как реализован механизм мандатного управления доступом?
3. Может ли быть применим механизм мандатного управления доступом к устройствам?
4. Механизм, позволяющий предотвратить понижение уровня секретности данных?
5. Механизм определения прав доступа пользователя?
6. Для каких типов объектов файловой системы выполняется контроль целостности?
7. Что происходит при обнаружении нарушения целостности в системе?

**Время на выполнение лабораторной работы – 4 часа**

**Образовательная организация, авторы, эл. почта:** Новосибирский государственный технический университет, кафедра защиты информации, к.т.н., доцент Зырянов Сергей Алексеевич, ассистент Грищенко Лев Аркадьевич, l.grishhenko@corp.nstu.ru



**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем.

**Дисциплина:** Программно-аппаратные средства обеспечения информационной безопасности.

### **Лабораторная работа.**

#### **Система защиты информации от несанкционированного доступа DallasLock 8.0**

##### **1. Учебные цели:**

- Изучить возможности сертифицированной системы защиты информации накладного типа для автономных и сетевых АРМ. Отработать навыки реализации правил разграничения доступа пользователей к защищаемым информационным ресурсам.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

###### **Уметь:**

- настраивать механизмы идентификации и аутентификации пользователей в системе средствами DallasLock 8.0;
- настраивать управление доступом к компонентам информационной системы и информационным ресурсам;
- настраивать подсистему обеспечения целостности информационной системы и информации.

###### **Владеть навыками:**

- работы с устройствами хранения ключевой информации;
- работы с защитными механизмами операционной системы Windows;
- контроля защищенности информационных ресурсов.

##### **3. Перечень материально-технического обеспечения**

- **Лабораторное оборудование и программное обеспечение:** компьютерный класс с установленным программным обеспечением: серверная и клиентские компоненты DallasLock 8.0.

##### **4. Задание на исследование:**

Сформировать комплекс правил разграничения доступа пользователей к защищаемым информационным ресурсам средствами DallasLock 8.0 с использованием мандатной и дискреционной политик разграничения доступа.

##### **5. Краткие теоретические сведения**

DallasLock 8.0 – сертифицированная система защиты информации накладного типа для автономных и сетевых АРМ (применима для сложных сетевых инфраструктур).

Предназначена для защиты конфиденциальной информации (редакции «К» и «С»), в том числе содержащейся в автоматизированных системах (АС) до класса защищенности 1Г включительно, в государственных информационных системах (ГИС) до 1 класса защищенности включительно, в информационных системах персональных данных (ИСПДн) для обеспечения 1 уровня защищенности ПДн, в автоматизированных системах управления производственными и технологическими процессами (АСУ ТП) до 1 класса защищенности включительно, а также для защиты информации, содержащей сведения, составляющие государственную тайну (редакция «С») до уровня «совершенно секретно» включительно.

Использование СЗИ необходимо в соответствии с закрепленными в приказах и руководящих документах регулятора группами мер. Указанные группы мер должны быть реализованы в ИСПДн, в АСУ ТП, а также в автоматизированных системах классов 1Д и выше.

##### **6. Порядок выполнения лабораторной работы (этапы)**

###### **Подготовка к работе**

Для выполнения работы используются рабочие места WS27 и WS28 в ауд. 201а-3. На WS27 установлена только клиентская часть, на WS28 клиентская и серверная части системы DallasLock 8.0.

Перед тем, как приступить к работе следует изучить документ «RU.48957919.501410-02 92 – Руководство по эксплуатации» (далее – Руководство), который находится в соответствующем файле на рабочих местах WS27 и WS28, а также в общей папке локального сервера лаборатории.

Перед началом работы следует получить один аппаратный идентификатор EToken, который может использоваться на обоих рабочих местах.

###### **Этап 1. Настройка прав доступа к файлам**

1. Войти в систему под логином student с уровнем доступа «Сов.секретно» (пароль к этой учетной записи следует узнать у лаборанта).

*Примечание.* Пользователь student имеет права администратора в системе DallasLock. Поэтому создание новых пользователей и управление правами доступа следует выполнять из-под этой учетной записи.

Имя пользователя и уровень доступа отображаются в заголовке окна утилиты администратора DallasLock.

2. С помощью утилиты администратора DallasLock создать новых пользователей со следующими параметрами:

| № | Логин         | Полное имя      | Уровень доступа |
|---|---------------|-----------------|-----------------|
| 1 | Secret_Ivanov | Иванов В.А.     | Секретно        |
| 2 | Secret_Petrov | Петров П.В.     | Секретно        |
| 3 | Open_Ivanov   | Открытые данные | Открытые данные |

*Примечание.* Вместо Ivanov, Petrov следует указывать фамилии студентов, выполняющих работу.

3. Убедиться, что учетные записи созданы в системе и для них подготовлены системные папки. Для этого нужно войти под учёткой каждого пользователя, указав уровень доступа «Открытые данные».

*Примечание.* Дальнейшая работа с настройкой прав пользователей будет проводиться в отношении пользовательских папок, находящихся в папке c:\Users\. Следует проверить наличие папок Secret\_Ivanov, Secret\_Petrov и Open\_Ivanov.

4. Настроить доступ к папке Secret\_Petrov следующим образом:

- пользователь Secret\_Petrov имеет полный доступ ко всем вложенным папкам своей папки (которая также называется Secret\_Petrov);
- пользователь Secret\_Ivanov имеет полный доступ к папке «Мои документы» в Secret\_Petrov;
- пользователь Secret\_Ivanov имеет право просматривать файлы в папке «Мои видео» в Secret\_Petrov, но не имеет право создавать новые файлы и изменять существующие;

*Примечание.* При задании прав доступа средствами DallasLock следует также задать соответствующие права доступа в системных настройках безопасности для соответствующих папок.

5. Включить полный аудит папок Secret\_Ivanov и Secret\_Petrov.

6. Настроить двухфакторную аутентификацию пользователя Secret\_Ivanov по паролю и аппаратному идентификатору (токену).

*Указание.* Если данную работу одновременно выполняет две бригады и имеется только один аппаратный идентификатор, то этот пункт можно выполнить позже, по договоренности между бригадами.

### **Этап 2. Проверка прав настроек доступа к файлам**

7. Проверить полный доступ пользователя Secret\_Petrov ко всем вложенным папкам своей папки (которая также называется Secret\_Petrov).

Для этого следует зайти в систему под учёткой Secret\_Petrov и создать любые файлы в папках «Мои документы», «Мои видео» и т.п.

8. Проверить полный доступ пользователя Secret\_Ivanov к папке «Мои документы» в папке Secret\_Petrov.

Для этого следует зайти в систему под учёткой Secret\_Ivanov и создать любой файл в папке «Мои документы» в папке Secret\_Petrov.

9. Проверить доступ пользователя Secret\_Ivanov к папке «Мои видео» в Secret\_Petrov с правами только чтения.

Для этого следует зайти в систему под учёткой Secret\_Ivanov и попытаться создать любой файл в папке «Мои видео» в папке Secret\_Petrov. В этом действии должно быть отказано.

Выполнить попытку просмотра файла в папке «Мои видео». Это действие должно быть разрешено.

10. Проверить права доступа пользователя Open\_Ivanov. Для этого следует зайти в систему под учёткой Open\_Ivanov и попытаться открыть папки Secret\_Ivanov и Secret\_Petrov. В доступе должно быть отказано. Доступ к папке Open\_Ivanov должен быть разрешен.

11. Проверить работу двухфакторной аутентификации. Для этого нужно попытаться войти в систему под учёткой Secret\_Ivanov (к которой ранее был привязан аппаратный идентификатор). Во входе должно быть отказано.

12. Проверить правильность работы авторизации. Для этого нужно выполнить п.7, однако при входе в систему указать уровень доступа «Открытые данные». В доступе к файлам должно быть отказано.

### **Этап 3. Проверка подсистемы аудита**

13. Просмотреть журналы доступа и убедиться, что в них содержатся выполненные ранее действия по доступу к папкам Secret\_Ivanov и Secret\_Petrov.

14. Просмотреть журнал входов в систему и убедиться, что там содержится запись о неудачной попытке входа в систему пользователя Secret\_Ivanov без аппаратного идентификатора (при выполнении п.11).

#### **Этап 4. Управление отчуждаемыми накопителями**

15. Запретить использование USB-накопителей пользователю Secret\_Ivanov.

*Примечание.* Для этого и последующих действий следует включить режим аудита доступа.

16. Вставить USB-накопитель, зайти в систему под учетной записью Secret\_Ivanov и проверить, запрещён ли доступ к нему.

17. Убедиться, что в журнале аудита появилась соответствующая запись о попытке доступа.

18. Разрешить пользователю Secret\_Petrov использование одного определенного USB-накопителя. Доступ ко всем остальным должен быть запрещен.

*Примечание.* Для выполнения этого задания потребуется два любых USB-накопителя, можно использовать свои личные устройства. Если своих USB-накопителей нет, то необходимо получить их у лаборанта.

19. Убедиться, что из учетной записи Secret\_Petrov есть доступ только к одному, «разрешенному» USB-накопителю.

Требования к содержанию и оформлению отчета

В ходе выполнения задания следует заносить в отчет наиболее значимую информацию по каждому пункту.

#### **Отчет должен содержать следующие данные:**

- логины, полные имена и пароли созданных учётных записей;
- настройки прав дискреционного и мандатного доступа к защищаемым ресурсам;
- словесное описание действий, которые были сделаны для выполнения каждого пункта задания;
- скриншоты фрагментов экрана, где содержится пояснение или подтверждение выполненных действий.

#### **7. Контрольные вопросы:**

1. Какие учетные записи присутствуют в DallasLock по умолчанию?
2. Какие пользователи обладают правами для создания, удаления и изменения учетных записей пользователей?
3. Сколько уровней мандатного доступа предусмотрено в DallasLock? Какой уровень имеет наивысшие права?
4. Какие виды аудита папок имеются в DallasLock?
5. Какие параметры парольной политики доступны при создании/модификации учетной записи пользователя?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** Федеральное государственное автономное образовательное учреждение высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» (Самарский университет) Адрес: ул. Московское шоссе, д. 34, г. Самара, 443086, к.т.н. доцент Жмуров Д.Б., эл.почта – [ssau.fit.chief.ibas@gmail.com](mailto:ssau.fit.chief.ibas@gmail.com)

## Дисциплина: Системы радиомониторинга

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем.

**Дисциплина:** Системы радиомониторинга.

### **Лабораторная работа.**

#### **Исследование спектра генератора шума, на базе ГШ ГНОМ-3**

##### **1. Учебные цели:**

- Изучить возможности исследования спектра генератора шума, на базе ГШ ГНОМ-3. Отработать навыки оценки спектра излучения генератора шума Гном-3 по прикрытие объектов защиты от утечки за счет ПЭМИН

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

###### **Знать:**

- Основные формулы расчета спектра генератора шума, на базе ГШ ГНОМ-3.

###### **Уметь:**

- Проводить комплексный радиомониторинг при проведения контрольных испытаний.

###### **Владеть:**

- Навыками проведения работ при сертификации СЗИ.

##### **3. Перечень материально-технического обеспечения**

- **Лабораторное оборудование и программное обеспечение:** Генератор шума Гном-3, Персональная ЭВМ в составе.
- **Контрольно-измерительная аппаратура:** При проведении СИ использована следующая контрольно-измерительная аппаратура:
  - Селективный микровольтметр SMV-8,5, зав. № 91200406;
  - Анализатор спектра СК4 Белан;
  - Антенна АИ5-0, зав. № 177;

##### **4. Задание на исследование**

- собрать по заданной схеме лабораторную установку;
- произвести измерения спектральной плотности электромагнитного шума в диапазоне существования ПЭМИ;
- нарисовать график распределения обнаруженных опасных сигналов;
- сделать выводы.

##### **5. Краткие теоретические сведения**

В данной лабораторной работе рассмотрим то, что в принятой терминологии именуется аббревиатурой САЗ (системы или средства активной защиты). Разумеется, в применении к защите от утечки по техническому каналу за счёт ПЭМИН.

Как и следует из формулировки канала утечки, задача разбивается на две подзадачи, на защиту (а, следовательно, и на оценку эффективности) в свободном пространстве и в отходящих (или близко проходящих) линиях.

С точки зрения физики и теории радиотехники, задача защиты формулируется как обеспечение некоторого, заданного нормативными документами, отношения сигнал/шум. Причём под «сигналом» подразумевают пиковое значение энергии сигнала, а под «шумом» – среднеквадратичное значение помехового сигнала от САЗ. Всё это измеряется и вычисляется в некоторой, отдельно задаваемой, полосе частот. Суммирование сигналов производится в полосе 1/г. Именно в этой полосе, чаще всего, и рассчитывается требуемое отношение сигнал/помеха. Собственно, ничего хоть сколько-нибудь необычного в вычислении энергии сигнала нет. Либо нам удалось с помощью тест-режима заставить работать интересующие нас цепи, линии, узлы, блоки технического средства с постоянной тактовой частотой кодовых посылок. И тогда спектр ПЭМИН «с точки зрения» узкополосного приёмного устройства имеет линейчатый характер. Либо не удалось по причинам, изложенным ранее. И тогда спектр будет носить характер сплошного (обычно, некими зонами, полосами частот). В обоих случаях можно и нужно рассчитать энергию, «умещающуюся» в заданной полосе.

На верхнем спектре представлен «линейчатый» вариант, на нижнем – «сплошной», а на среднем – некий промежуточный и достаточно часто встречающийся вариант.

В числителе выражения (приведённого исключительно для «линейчатого» варианта спектра) суммируются энергии отдельных, измеренных в оговоренных условиях, частотных составляющих спектра ПЭМИН. Причём суммируются не сами измеренные величины (в мкВ/м), а их квадраты, что пропорционально энергии.

Несложно вспомнить закон Ома, формулы, связывающие напряжение, ток и мощность. Кроме того, выполняется нормировка по полосе частот. Деление на тактовую частоту каждой частотной составляющей переводит расчётную величину в спектральную плотность энергии (мощности) на единицу ширины полосы (на 1 кГц), а последующее умножение на  $1/\tau$  «собирает» мощность во всей полосе суммирования. То есть в результате математических действий мы получаем гипотетическую мощность сигнала в полосе суммирования.

Итак, осталось понять, что же делать со сплошным или «линейчато-сплошным» спектром «опасного сигнала». Ну, с «линейчатыми» его составляющими – понятно. А с участками сплошного спектра, – всё то же суммирование квадратов измерений полосой приёмника. При этом полосы пропускания «прижаты» друг к другу, то есть шаг перестройки приёмника равен ширине полосы пропускания. Если предписано проводить такую операцию для сигнала САЗ, то она столь же законна и для широкополосного сигнала ПЭМИН.

Таким образом, для сплошного или участков сплошного спектра поступаем как с сигналом САЗ, а с «линейчатыми» составляющими – как обычно. Затем общая сумма квадратов, как обычно, делится на тактовую частоту и домножается на  $1/\tau$ . Даже «модификация» расчётных выражений НМД, практически, не нужна, использовано только то, что в них и так есть.

Для «опасного сигнала» предписано измерять максимумы. И по размещению измерительной антенны и по её ориентации в пространстве (ориентации диполей и/или рамки). А сами «опасные сигналы» – просто все (в первом приближении).

А вот в отношении измерения сигнала САЗ – измерять в направлении от «объекта» к опасной точке. Возможно поступать следующим образом:

- Ориентировать антенну по минимуму сигнала САЗ.
- Ориентировать антенну так, как она была сориентирована при измерениях «опасного сигнала».

Оба подхода имеют свои «плюсы» и «минусы». Разброс результатов измерений уровней сигналов САЗ от ориентации антенны легко достигает десятка – другого дБ.

Рекомендуется для особо ответственных случаев распределять точки измерения так, чтобы результаты замеров сигналов в них (в любых двух смежных) отличались не более, чем на 3 дБ. Для менее ответственных случаев – на 6 дБ. Количество точек у Вас снизится в 10-М 00 раз, что нельзя не приветствовать. Сигнал (неважно, САЗ или ОС) в промежуточных точках легко восстанавливается обычной линейной интерполяцией (прямо по значениям в дБ). Возникающая при этом погрешность много меньше, чем погрешность наших измерений. Приведённый метод, по сути, есть рекомендованный метод приблизительного численного интегрирования методом «прямоугольников», так что и с методической стороны тут всё «чисто». Только не надо путать, где надо оперировать абсолютными значениями в размерности напряжённости поля, а где можно работать с относительными величинами в дБ.

Если мы измерили отношение сигнал/помеха в некой точке пространства (обычно вблизи защищаемого ТС), то в любой другой точке, на большем удалении, это отношение останется таким же. Утверждение верное, но не при любых исходных условиях. Давайте рассмотрим графики («закон затухания») ослабления сигнала с увеличением радиуса. Для классического случая, то есть хрестоматийного распространения волны над проводящей поверхностью в свободном пространстве. Если мы начнём учитывать влияния строительных конструкций, стен, проводящих линий, то на анализ нам понадобится очень много времени, и мощные вычислительные ресурсы.

Если «опасные сигналы» сосредоточены на вполне определённых частотах, то сигналы САЗ принципиально широкополосны, даже сверхширокополосны. Когда имеем дело с такими сигналами, то описанная выше картина «стоячих волн» немедленно исчезает. Несложно себе представить, что бесконечная сумма разных частот даст и бесконечную сумму стоячих волн, максимумы и минимумы которых придутся на разные участки линии. В результате – благодатная картина «псевдобегущей волны». Тем не менее измерять чисто практически проще токоизмерителем и уж точно безопаснее, особенно на линиях электропитания. Остаётся последний вопрос. Токоизмеритель измеряет ток вблизи линии (как и следует из названия). А по ряду причин нам бы нужно было иногда и напряжение...

Если результатом должно быть отношение сигнал/помеха, то «по току» или «по напряжению» совершенно безразлично, численно эти два отношения будут равны. Но если нам понадобилось именно напряжение (строго говоря модуль «Е» вектора волны вблизи линии), то без знания волнового сопротивления линии не обойтись. По сути всё тривиально, по закону Ома,  $E=I \cdot R$ . Откуда же взять это самое  $R$ ?

Можно измерить, значение частотнозависимо, по нему на многих частотах и аппаратура для таких измерений не самая простая, как и процедура измерений на ВЧ частотах. Есть рекомендация проще.

На частотах самых низких, до 100–150 кГц можно принимать сопротивление произвольной линии равным 150 ом, до 30 МГц – 75 ом, выше – порядка 50 ом (в наших экспериментах спало до 20-30 Ом).

Все расчёты, естественно, выполняются так же, как и для «эфира», если по условиям объекта ОС и сигнал САЗ поступают в разные участки линии, то необходимо измерение реального затухания отдельно, для этих сигналов. Механизм погонного затухания в транспортирующей системе (вблизи линии) более сложен, чем в пространстве. А в конкретной, проложенной на объекте, порою с многочисленными переходами из кабеля в кабель, ответвлениями и т.д. затухание вообще непредсказуемо.

Генератор шума Гном – 3 предназначен для защиты от утечки конфиденциальной информации, обусловленной паразитными электромагнитными излучениями и наводками ПЭВМ и других средств оргтехники.

**Технические характеристики:**

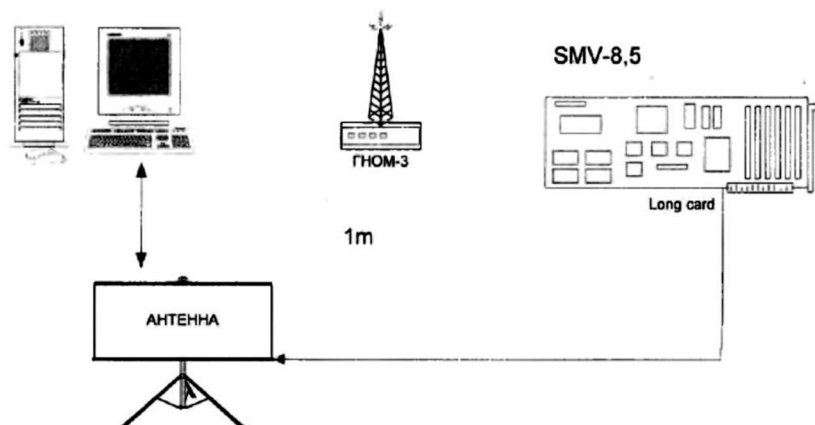
- Диапазон частот шумового сигнала: 10 кГц ... 1 ГГц.
- Антенны – рамочные, монтируемые в 3-х плоскостях.
- Уровень шумового сигнала на выходных разъемах генератора в диапазонах частот:
  - 10... 150 кГц (при полосе пропускания приемника 200 Гц): не менее 70 дБ;
  - 150 кГц...30 МГц (при полосе пропускания приемника 9 кГц): не менее 70 дБ;
  - 30...400 МГц (при полосе пропускания приемника 120 кГц): не менее 75 дБ;
  - 0,4...1 ГГц (при полосе пропускания приемника 120 кГц): не менее 70 дБ.
- Питание – 220 В, 50 Гц.

**6. Порядок выполнения лабораторной работы (этапы)**

СИ ОТСС проводятся в соответствии с действующей методикой Гостехкомиссии при Президенте РФ.

Значения опасных сигналов (ОС) измерялись и рассчитывались от устройств с последовательным кодированием информации (монитор, накопители на жёстком и гибком магнитных дисках, принтер, клавиатура).

Собираем лабораторную установку по схеме:



**Рис. 1.** Схема лабораторной установки

Исследуемые устройства компьютерной техники (ОТСС) включались в режиме обработки специального тест – сигнала с заранее известными параметрами передаваемых данных. Основные параметры ОС (FT, т., и др.) в цепях устройств выявлялись непосредственными измерениями в исследуемых цепях.

Измерения побочных электромагнитных излучений (ПЭМИ) монитора производятся при выводе на экран последовательности чёрных и белых элементов изображения (пикселей) в режиме «пиксел через пиксел».

Исследования производятся по электрической и магнитной компонентам поля на тактовой частоте ОС и кратных частотах.

Оценка эффективности САЗ производится путём измерения спектральной плотности электромагнитного шума в диапазоне существования ПЭМИ. Данные инструментального контроля эффективности САЗ приведены в таблице 1.

Измерения производятся в диапазоне частот 0.01 – 1000 МГц (для гармоник побочного электромагнитного излучения служебных и информационных сигналов и паразитных генераторов) на тактовой частоте ОС и кратных частотах.

**Результаты измерений и расчётов.**

Данные измерений и расчётов занести в таблицу

**Таблица 1**

| F<br>[МГц] | Uc<br>[дБ] | Ka<br>[дБ] | Uc+ Ka<br>[дБ] | Uc+ Ka<br>[мкВ] | Uш+Ka<br>[дБ] | Uш+Ka<br>[мкВ] | Отношение<br>С/Ш |
|------------|------------|------------|----------------|-----------------|---------------|----------------|------------------|
|            |            |            |                |                 |               |                |                  |
|            |            |            |                |                 |               |                |                  |
|            |            |            |                |                 |               |                |                  |

Отношение

$$C / Ш = \frac{E_c K_{c \text{ реиз}} \sqrt{\Delta F_{\text{пр}}}}{K_{\text{ш реал}} E_{\text{ш i}} K_c K_n K_k \sqrt{\Delta F}},$$

где  $E_c$  – уровень сигнала на частоте гармоники (мкВ);  $K_{\text{ереал}}$  – коэффициент реального затухания сигнала = 1;  $K_{\text{шреал}}$  – коэффициент реального затухания шума = 1;  $E_{\text{ш i}}$  – смотри график 2 приложения 1;  $K_c$  – коэффициент кодирования: для импульсных кодов = 1, для потенциальных =  $\sqrt{2}$ , для трехуровневых = 1/2;  $K_n$  – коэффициент разрядности = 1;  $K_k$  – коэффициент качества генератора шума, для ГШ Г ном – 3 = 0,8;  $\Delta F$  – частота повторения импульсов теста;  $\Delta F_{\text{пр}}$  – полоса пропускания приемника.

**Таблица 2** – Таблица коэффициента антенны

| F<br>[МГц] | Ка<br>[дБ] |
|------------|------------|
| 20         | 27,5       |
| 30         | 27,5       |
| 50         | 27,8       |
| 100        | 28,9       |
| 200        | 29,2       |
| 300        | 28,4       |
| 400        | 26,7       |
| 500        | 26,2       |
| 600        | 23,1       |
| 700        | 25,1       |
| 800        | 24,2       |
| 900        | 30,8       |
| 1000       | 29,3       |

В отчете нарисовать график распределения обнаруженных опасных сигналов.

#### 7. Контрольные вопросы:

1. Задача защиты информации. Сигнал. Шум. Полоса суммирования. Варианты спектров ПЭМИН.
2. Принципы расчета, различных видов спектра.
3. Измерение различных видов сигналов.
4. Три варианта взаимного размещения источника ОС («опасного сигнала») и сигнала САЗ.
5. Затухание сигнала и помехи в линиях.
6. Описание формирования наводок на линию при установившемся режиме «бегущей волны».
7. Особенности измерения наводок в линиях пробником и токосъемником.
8. Состав генератора шума Гном-3, его основные характеристики и вид создаваемой им помехи.

**Время на выполнение лабораторной работы** – 4 часа.

**Образовательная организация, авторы, эл. почта:** Волгоградский государственный университет, Умницын Юрий Петрович, Бахрачева Юлия Сагидуллоевна, infsec@volsu.ru

## **Дисциплина: Техническая защита информации**

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, 10.03.01 Информационная безопасность.

**Дисциплина:** Техническая защита информации.

### **Лабораторная работа.**

#### **Оценка защищенности информации от утечки по виброакустическим каналам**

##### **1. Учебные цели:**

- Изучение методов измерения акустических и вибрационных сигналов в задачах защиты информации, особенностей монтажа и настройки средств активной защиты.
- Освоение методики оценки защищенности речевой информации от утечки по виброакустическим каналам (разборчивость речи).

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- **Уметь** производить оценку защищенности речевой информации от утечки по виброакустическим каналам.
- **Владеть** навыками монтажа и настройки средств активной защиты для виброакустических каналов.

##### **3. Перечень материально-технического обеспечения:**

- ограждающие конструкции: окно, дверной проем;
- персональный компьютер;
- цифровой шумомер ZET 110;
- микрофон BC501;
- акселерометр BC111;
- генератор сигналов низкочастотный ГЗ-112;
- акустический излучатель с усилителем Dialog W-204;
- генератор шума VNG-012GL с излучателями VNT, VN-GL, AI-8;
- ПО Equa (для настройки параметров генератора шума VNG-012GL).

##### **4. Задание на исследование:**

Заданы ограждающие конструкции (окно, дверной проем), средство активной защиты (САЗ) с набором излучателей различного типа.

Необходимо:

- Произвести измерения для проведения оценки защищенности в заданных контрольных точках (КТ) без применения средств активной защиты.
- Рассчитать значение разборчивости речи в каждой КТ.
- Подключить выбранные излучатели средства активной защиты к соответствующим выходам генератора шума.
- Произвести первоначальную настройку генератора шума по рекомендации преподавателя.
- Повторить п. 1–2 с применением средств активной защиты.
- При необходимости изменить настройки генератора шума и повторить процедуру оценки защищенности.
- Оформить отчет, ответить на контрольные вопросы.

##### **5. Краткие теоретические сведения**

###### **5.1. Порядок и схемы проведения измерений для оценки разборчивости речи**

Измеряемые величины:

- Уровни тестового сигнала в каждой октавной полосе (250, 500, 1000, 2000, 4000 Гц.)  $L_{\text{тест}i}$
- Уровни шума (фонового, либо от САЗ) в каждой октавной полосе  $L_{\text{ш}i}$
- Уровни смеси сигнал+шум (при включенном генераторе тестового сигнала) в каждой октавной полосе  $L_{(\text{с+ш})i}$

Схемы проведения измерений:

1. Измерение уровней тестового сигнала в каждой октавной полосе производится согласно рисунка 1, после проведения измерений, регулировку уровня громкости на акустическом излучателе (усилителе) не изменять!
2. Измерение уровней шума и смеси сигнал+шум для виброакустического (оптикоэлектронного) канала утечки информации (КУИ) производится согласно рисунка 2.



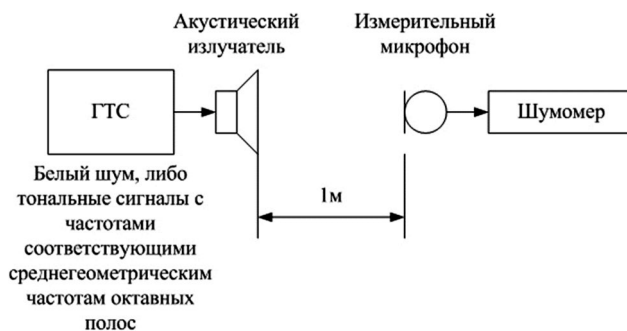


Рис. 1. Схема проведения измерения уровней тестового сигнала

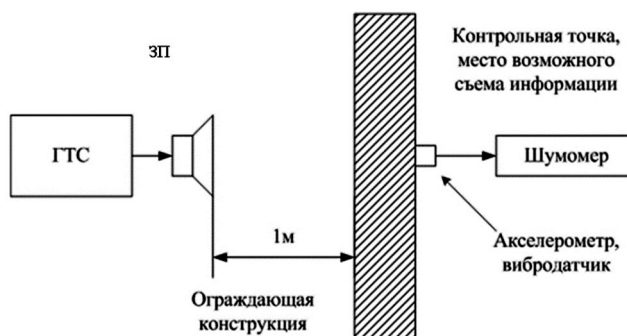


Рис. 2. Схема проведения измерения уровней шума и смеси сигнал + шум для виброакустического (оптикоэлектронного) канала утечки информации

1. Измерение уровней шума и смеси сигнал + шум для акустического КУИ производится согласно рисунка 3.



Рис. 3. Схема проведения измерения уровней шума и смеси сигнал + шум для акустического КУИ

Микрофон и акустический излучатель тестового сигнала располагаются на высоте 1,5 м от пола.

## 5.2. Методика расчета разборчивости речи

Исходные данные:

Результаты измерений  $L_{\text{тести}}$ ,  $L_{\text{ши}}$ ,  $L_{(c+\text{ш})i}$  в каждой октавной полосе (250, 500, 1000, 2000, 4000 Гц).

Порядок расчета показателя W:

1. Вычисляется разница между уровнем тестового сигнала и средним уровнем речи для каждой октавной полосы:  $\Delta L_i = L_{\text{тести}} - L_{\text{речи}}$

$L_{\text{речи}}$  – типовые интегральные уровни речи в октавных полосах для общего уровня 70 дБ (таблица 1).

2. Вычисляется уровень сигнала для каждой октавной полосы:

$$L_{ci} = 10 \cdot \log(10^{0,1 \cdot L_{(c+\text{ш})i}} - 10^{0,1 \cdot L_{\text{ши}}}).$$

Если в результате измерений  $L_{\text{ши}} \geq L_{(c+\text{ш})i}$  (ситуация возможна в случае, когда тестовый сигнал не различим на фоне шума), необходимо искусственно увеличить значение  $L_{(c+\text{ш})i}$ , чтобы оно превышало  $L_{\text{ши}}$  хотя бы на 0,1 дБ.

3. Вычисляются уровни ощущений для каждой октавной полосы:

$$Q_i = L_{ci} - L_{ши} - \Delta L_i - \Delta A_i$$

$\Delta A_i$  – формантное превышение (разница между спектром речи и спектром формант, таблица 1).

4. Вычисляется коэффициент восприятия для каждой октавной полосы:

$$p_i = \begin{cases} \frac{0.78 + 5.46 \cdot \exp[-4.3 \cdot 10^{-3} \cdot (27.3 - |Q_i|)^2]}{1 + 10^{0.1 \cdot |Q_i|}}, & \text{если } Q_i \leq 0; \\ 1 - \frac{0.78 + 5.46 \cdot \exp[-4.3 \cdot 10^{-3} \cdot (27.3 - |Q_i|)^2]}{1 + 10^{0.1 \cdot |Q_i|}}, & \text{если } Q_i > 0; \end{cases}$$

5. Вычисляется формантная разборчивость речи:

$$R = \sum_{i=1}^N p_i \cdot k_i$$

$N=5$  (пять октавных полос);  $k_i$  – вклад  $i$ -той октавной полосы в суммарную разборчивость (табличное значение см. ниже)

6. Осуществляется переход от формантной разборчивости к словесной:

$$W = \begin{cases} 1.54 \cdot R^{0.25} [1 - \exp(-11 \cdot R)], & \text{если } R < 0.15 \\ 1 - \exp\left(\frac{-11 \cdot R}{1 + 0.7 \cdot R}\right), & \text{если } R \geq 0.15 \end{cases}$$

**Таблица 1** – Характеристики октавных полос частотного диапазона речи

| Среднегеометрическая частота октавной полосы, Гц | Весовой коэффициент полосы $k_i$ | Значение параметра $\Delta A_i$ | Типовые интегральные уровни речи в октавных полосах для общего уровня 70 дБ |
|--------------------------------------------------|----------------------------------|---------------------------------|-----------------------------------------------------------------------------|
| 250                                              | 0.03                             | 18                              | 66                                                                          |
| 500                                              | 0.12                             | 14                              | 66                                                                          |
| 1000                                             | 0.20                             | 9                               | 61                                                                          |
| 2000                                             | 0.30                             | 6                               | 56                                                                          |
| 4000                                             | 0.26                             | 5                               | 53                                                                          |

### 5.3. Измерение акустических и вибрационных сигналов с применением шумомера ZET110

Измеряемые величины:

- $L$  – акустическое давление (дБ, относительно порога слышимости  $2 \cdot 10^{-5}$  Па);
- $V$  – виброускорение (дБ, относительно  $3 \cdot 10^{-4}$  м/с<sup>2</sup>).

Включить шумомер ZET110 (одновременное нажатие кнопок вверх и вправо). Включить ПК и запустить ПО ZETLab. Подключить шумомер кабелем USB-miniUSB (к портам на задней панели системного блока). Убедиться в том, что устройство подключено (Сервисное/Диспетчер устройств).

Измерение виброускорения

В качестве первичного преобразователя для измерения виброускорения выступает акселерометр BC111 (чувствительность 0,01 В/г). На шумомере необходимо указать тип первичного преобразователя, чтобы в процессе измерений автоматически учитывалась его чувствительность, а также тип. Для этого на шумомере переходим в меню выбора датчиков: Наст./Вход/Датчики. Выбираем BC111.

Также обращаем внимание на меню Наст./Вход/Диапазон. В данном меню осуществляется переключение поддиапазонов измеряемых значений 110/120/140 дБ. Установить первоначально 110 дБ, если в процессе измерений показания будут «зашкаливать», необходимо вручную переключиться на следующий поддиапазон. Диапазон 110 дБ используется для измерения слабых сигналов, 140 дБ используется для измерения мощных сигналов (по акустическому давлению 140 дБ это шум реактивного двигателя).

Подключить акселерометр ко входу шумомера. Закрепить акселерометр в контрольной точке (осуществляется преподавателем).

Измерение акустического давления

В качестве первичного преобразователя для измерения акустического давления выступает микрофон BC501 (чувствительность 63,5 мВ/Па). На шумомере необходимо указать тип первичного преобразователя, чтобы в процессе измерений автоматически учитывалась его чувствительность, а также тип.

Для этого на шумомере переходим в меню выбора датчиков: Наст./Вход/Датчики. Выбираем BC501. Также обращаем внимание на меню Наст./Вход/Диапазон (установить минимальный из возможных).

Подключить микрофон ко входу шумомера кабелем BNC-BNC. Разместить микрофон на штативе в выбранной контрольной точке.

Процесс проведения измерений (работа с ПО ZETLab)

В ПО ZETLab выбрать «Долеоктавный спектр» (меню анализ сигналов).

Зайти в параметры и установить 1/1 октавный режим, усреднение 2 сек, линейная АЧХ. Включить отображение среднего и минимального значения. При измерении шумов использовать минимальные значения, при измерении тест-сигнала и смеси сигнал+шум использовать средние значения.

Произвести измерения уровней виброускорения/акустического давления в октавных полосах со среднегеометрическими частотами: 250, 500, 1000, 2000, 4000 Гц. Измеряемое значение отображается над графиком при выборе «мышкой» необходимой октавной полосы.

## 6. Порядок выполнения лабораторной работы (этапы)

Оцениваемые ограждающие конструкции: элемент остекления окна (оптикоэлектронный/виброакустический канал) и дверь в смежное помещение (акустический канал).

В качестве источника маскирующей помехи будет использоваться система VNG-012GL, состоящая из генератора, вибро и акустоизлучателей.

В руководстве по эксплуатации VNG-012GL найти схему подключения излучателей.

1. Для элемента остекления будет использовано несколько схем средств защиты информации (СЗИ):

- а. Виброизлучатели VNT. Возможность регулировки уровня и спектра сигнала для данных излучателей отсутствует. Следовательно, защищенность будет достигаться подключением большего количества излучателей данного типа, до достижения нормы  $W$ .

Собрать схему СЗИ с использованием 1 излучателя VNT. Произвести измерения и расчет  $W$  в контрольных точках (КТ) 1-3. При значении  $W < 0,35$ , делается вывод о защищенности объекта. При невыполнении нормы необходимо увеличить количество используемых излучателей типа VNT и повторить процедуру оценки защищенности.

- б. Виброизлучатели VN-GL. Подключается один из излучателей. Данные излучатели отличаются от VNT своей мощностью и возможностью регулировки как по уровню, так и по спектру (1/1 и 1/3 октавный эквалайзер). Проверить подключение генератора шума к ПК по RS-232. Запустить на ПК ПО Equa (генератор шума должен быть включен). Выставить следующие настройки для канала, к которому подключен излучатель VN-GL:

Уровень: -10 дБ.

Выбрать октавный (1/1) эквалайзер

Задать следующие настройки эквалайзера:

250 500 1000 2000 4000 Гц

-3 0 3 6 9 дБ

Сохранить настройки в файл, закрыть программу, записать настройки в память генератора. После настройки произвести измерения и расчет  $W$ . При значении  $W < 0,35$ , делается вывод о защищенности объекта. При невыполнении нормы необходимо увеличить уровень шума в настройках ПО и повторить процедуру оценки защищенности.

- в. Дополнительное задание. постараться задать с помощью эквалайзера формантоподобную помеху (соотношение уровней в октавных полосах рассчитывается на основании  $L_{речи}$  и  $\Delta A_i$ )

2. Дверь в смежное помещение.

- а. Акустический излучатель AI-8 расположен над дверью в смежное помещение. Защищаемым считается помещение аудитории. Точка за дверью в смежное помещение считается потенциальной возможным местом утечки информации. Произвести подключение акустического излучателя (к соответствующим разъемам), в генераторе существует возможность изменения только уровня сигнала, без возможности изменения спектра. В ПО Equa осуществить следующие настройки для акустического канала (№ 5):

Уровень: -14 дБ

После настройки произвести измерения и расчет  $W$ . При значении  $W < 0,35$ , делается вывод о защищенности объекта. При невыполнении нормы необходимо увеличить уровень шума в настройках ПО и повторить процедуру оценки защищенности.

## 3. Содержание отчета

1. Титульный лист, цель работы и задание.
2. Перечень ограждающих конструкций
3. Перечень измерительного оборудования (модели, наименования).
4. Схемы расположения СЗИ и контрольных точек проведения измерений.
5. Перечень СЗИ (модели, наименования)
6. Схемы проведения измерений.
7. Результаты измерений и расчетов (без использования СЗИ и с использованием СЗИ).
8. Выводы о защищенности/незащищенности ограждающих конструкций.

## 7. Контрольные вопросы

1. Физические характеристики речи?
2. Методика оценки разборчивости речи?
3. Виды помех и их эффективность?

4. Порядок проведения измерений при оценке защищенности речевой информации от утечки по виброакустическим каналам?
5. Рекомендации по монтажу и настройке средств активной защиты?
6. Параметры измерительного оборудования для оценки защищенности речевой информации от утечки по виброакустическим каналам?
7. Выбор контрольных точек для проведения измерений?

**Время на выполнение и защиту лабораторной работы – 4 часа.**

**Образовательная организация, автор, эл. почта:** Новосибирский государственный технический университет, кафедра защиты информации, к.т.н., заведующий кафедрой Иванов Андрей Валерьевич, andrej.ivanov@corp.nstu.ru

---

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, 10.03.01 Информационная безопасность

**Дисциплина:** Техническая защита информации.

**Лабораторная работа.**  
**Оценка защищенности информации от утечки**  
**по каналам побочных электромагнитных излучений и наводок (ПЭМИН)**

**1. Учебные цели:**

- Изучение методов поиска и измерения сигналов побочных электромагнитных излучений и наводок.
- Освоение методики оценки защищенности конфиденциальной информации от утечки по каналам ПЭМИН.

**2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- Уметь производить оценку защищенности конфиденциальной информации от утечки по каналам ПЭМИН.
- Владеть навыками поиска и измерения сигналов ПЭМИН.

**3. Перечень материально-технического обеспечения:**

- Персональный компьютер (интерфейс монитора VGA)
- Анализатор спектра LIGNext1 NS-30A
- Антенна рамочная Н-30
- Антенна дипольная активная Е-30
- Антенна дипольная Е-3000
- Пробник напряжения П-400
- Цифровой осциллограф LeCroy Wavesurfer 62Xs
- Штатив для антенны.

**4. Задание на исследование:**

Дана автоматизированная система (персональный компьютер). Исследованию будет подвергаться видеотракт с интерфейсом VGA.

Необходимо:

- Установить тестовый режим работы для исследуемого интерфейса.
- Определить тактовую частоту сигналов (различными методами).
- Произвести поиск и измерение сигналов ПЭМИ.
- Произвести поиск и измерение сигналов наводок ПЭМИ в линии электропитания.
- Произвести расчеты показателей защищенности. Сделать выводы о защищенности объекта.

**5. Краткие теоретические сведения.**

Первостепенная задача при исследовании каждого технического средства (ТС) на предмет возможных ПЭМИ заключается в поиске информативных частот. Исследуемый частотный диапазон:

- при оценке ПЭМИ по электрической составляющей ЭМП от 10 кГц до 1 ГГц;
- при оценке ПЭМИ по магнитной составляющей ЭМП от 10 кГц до 30 МГц;
- при оценке наводок ПЭМИ от 10 кГц до 300 МГц.

Поиски и измерение частотных составляющих сигнала производится при работе исследуемого ТС в специальном тестовом режиме (режиме, когда исследуемый сигнал обладает максимальной энергией). Для реализации данных режимов используются специальными тестовыми программами.



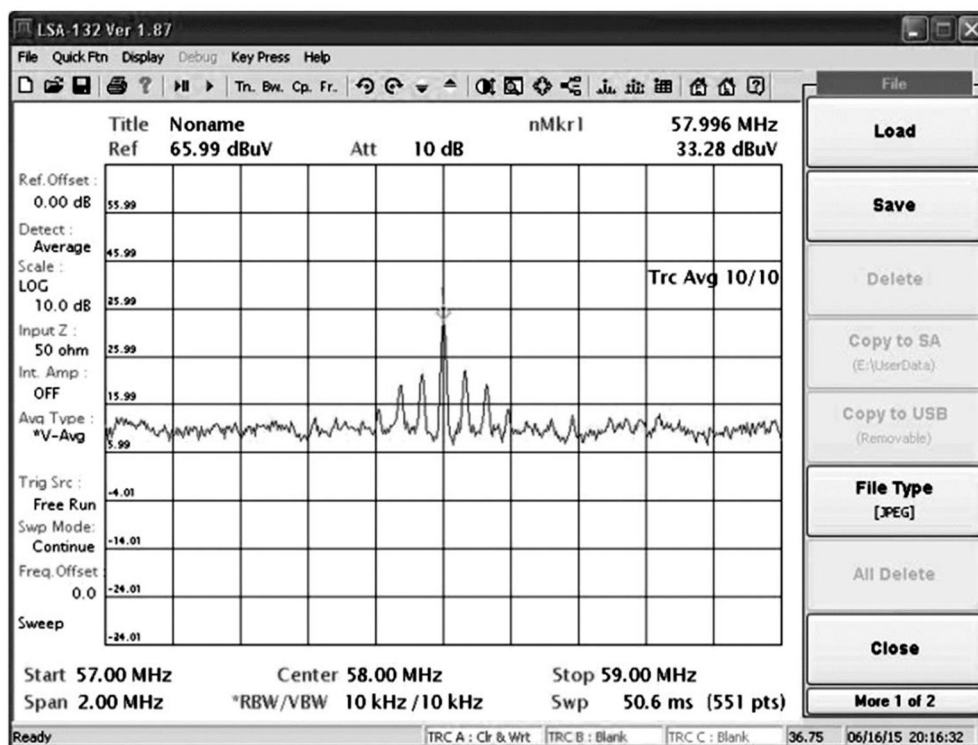


Рис. 2. Спектр сигнала VGA монитора, разрешение 1024x768, кадровая частота 60 Гц

## 6. Порядок выполнения лабораторной работы (этапы)

### 1. Оценка ПЭМИ:

1. Определить тактовую частоту сигнала сначала расчетным путем по формуле. Сверить полученные результаты с расчетом в тестовой программе. Зафиксировать полученные результаты в отчете.
2. Подключить осциллограф к отводам специально подготовленного кабеля VGA. К одному из цветов (R, G, B) и к «земле». Запустить тестовый режим на мониторе. Добиться на экране осциллографа четкой картинки с видео импульсом. «Пачки» импульсов следуют с частотой соответствующей кадровой частоте монитора, импульсы внутри (строчные импульсы) следуют с частотой исследуемого нами сигнала. Оценить частоту следования строчных импульсов. Зафиксировать полученные результаты в отчете. Сделать скриншот с экрана осциллографа с отображением кадрового импульса и курсоров, измеряющих частоту следования строчных импульсов. Добавить скриншот в отчет.
3. Отключить осциллограф, приступить к поиску сигнала анализатором спектра и проведению измерений. В зависимости от частоты исследуемого сигнала выбрать измерительную антенну. Измерительная антенна устанавливается на расстоянии 1 м от исследуемого ТС в направлении кратчайшего расстояния до границы КЗ (то есть места возможного съема информации).
4. Установить следующие настройки анализатора спектра: SPAN – 2 МГц; полоса пропускания RBW (Меню CPL) – 10 кГц (после обнаружения сигнала, при проведении измерений установить требуемое значение полосы пропускания 10 или 100 кГц, условия выбора см. выше); единицы измерения Unit (Меню Ampl) дБмкВ (на практике либо вручную, либо используя функционал анализатора спектра к измеренному значению добавляется калибровочный коэффициент первичного преобразователя: антенны, пробника напряжения, токосъемника и т.д., и конечная единица измерения напряженности ЭМП будет дБмкВ/м, калибровочные коэффициенты берутся из сертификата о калибровке).
5. Используя меню амплитуды (Ampl), изменяя значение аттенюатора (Ref. Level), устанавливать уровень ослабления таким чтобы спектр сигнала находился по середине или в верхней части дисплея.

Включить функцию усреднения и установить количество циклов = 10 (Average) меню Trace/More.

В меню частоты (Freq) установить центральную частоту, соответствующую определенной нами частоте сигнала.

Измерения производятся путем перестройки маркера (меню MRK), вращающая рукоятку перестройки. Для установки маркера на частотную составляющую с максимальной амплитудой, отображаемой на дисплее, можно воспользоваться кнопкой Peak.

6. Используя описанную выше методику (включение/отключение тестового режима) определить принадлежность данного сигнала к исследуемому ТС.

7. Для проведения расчетов по методике оценки защищенности (выдается преподавателем) необходимо зафиксировать уровни шума (выключенный тест) и смеси сигнал+шум (включенный тест), если разница между шумом и сигнал+шум меньше 3дБ, данную составляющую не учитываем.
8. Произвести расчет по предложенной методике и сравнить полученные радиусы с радиусом КЗ = 10м. Сделать выводы о защищенности и необходимости установки СЗИ.

## **2. Оценка наводок ПЭМИ**

1. Поиск и измерения сигналов производятся аналогичным образом.
2. Диапазон частот сокращается и составляет 10кГц-300МГц.
3. Вместо антенны подключается пробник напряжения и исследуются все токоведущие конструкции (линии, инженерные металлические коммуникации: отопление, вентиляция и т.д.), выходящие за пределы КЗ.
4. Измеряемая физическая величина – напряжение. Также необходимо учитывать калибровочные коэффициенты.
5. В рамках данной лабораторной работы исследуем линию электропитания.
6. Подключаем пробник напряжения П-400 к исследуемой линии, производим поиск и измерение сигналов на выявленных ранее частотах.
7. Для проведения расчетов по методике оценки защищенности (выдается преподавателем) необходимо зафиксировать уровни шума (выключенный тест) и смеси сигнал+шум (включенный тест), если разница между шумом и сигнал+шум меньше 3дБ, данную составляющую не учитываем.
8. Согласно методике, произвести оценку погонного затухания исследуемой линии на частотах сигналов ПЭМИН.
9. Рассчитать длину пробега  $R_i$ , которая сравнивается с пробегом линии до границы КЗ (10 метров), делаются выводы о защищенности.

## **3. Содержание отчета**

1. Титульный лист, цель работы и задание.
2. Перечень исследуемых ТС (с указанием моделей, интерфейсов и режима работы).
3. Перечень измерительного оборудования (модели, наименования).
4. Схема проведения измерений.
5. Скриншоты формы сигнала с осциллографа.
6. Скриншоты спектра одной из гармоник сигнала с полосой пропускания 10 кГц.
7. Результаты измерений и расчетов.
8. Выводы о защищенности/незащищенности ТС.

## **7. Контрольные вопросы**

1. Причины возникновения канала утечки информации за счет ПЭМИ и наводок?
2. Источники ПЭМИ в автоматизированной системе?
3. Диапазоны частот проведения оценки защищенности информации по каналам ПЭМИН по электрической и магнитным составляющим?
4. Способы определения тактовой частоты исследуемого ТС?
5. Принципы задания тестового режима работы ТС?
6. Выбор полосы пропускания анализатора спектра при проведении поиска и измерения сигналов?
7. Методика оценки защищенности от утечки по каналам ПЭМИ?
8. Методика оценки защищенности от утечки информации за счет наводок ПЭМИ?

**Время на выполнение и защиту лабораторной работы – 4 часа.**

**Образовательная организация, автор, эл. почта:** Новосибирский государственный технический университет, кафедра защиты информации, к.т.н., заведующий кафедрой Иванов Андрей Валерьевич, andrej.ivanov@corp.nstu.ru.

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, 10.03.01 Информационная безопасность.

**Дисциплина:** Техническая защита информации.

### **Лабораторная работа.** **Автономные средства радиомониторинга**

#### **1. Учебные цели:**

- Изучить основные демаскирующие признаки радиомикрофонов;
- Изучить особенности обнаружения демаскирующих признаков радиомикрофонов при помощи автономных средств радиомониторинга разного типа;
- Отработать навыки обнаружения радиомикрофонов при помощи автономных средств радиомониторинга разного типа.

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- Уметь идентифицировать обнаруженные сигналы.
- Уметь настраивать автономное оборудование радиомониторинга для работы в разных режимах.
- Владеть навыками идентификации обнаруженных сигналов.
- Владеть навыками локализации радиомикрофонов в помещении.

#### **3. Перечень материально-технического обеспечения**

- **Лабораторное оборудование и программное обеспечение:**
  - Корреляционный приемник «Оракул».
  - Индикатор поля-частотомер RFI-07.
  - Простейший индикатор поля Ловец-М.
  - Скоростной поисковый приемник «Скорпион».
  - Персональный компьютер с ПО SEL SP81 ORACLE.
  - Тестовое устройство.

#### **4. Задание на исследование:**

- Изучение видов индикации наличия сигнала от радиомикрофона при использовании простейшего индикатора поля;
- Изучение видов индикации наличия сигнала от радиомикрофона при использовании простейшего индикатора поля-частотомера;
- Изучение видов индикации наличия сигнала от радиомикрофона при использовании корреляционного приемника «Оракул»;
- Изучение видов индикации наличия сигнала от радиомикрофона при использовании скоростного поискового приемника «Скорпион».

#### **5. Краткие теоретические сведения**

Мониторинг – это процесс получения различного рода информации с использованием технических средств на участке ее прохождения по каналам связи. В случае радиомониторинга подразумеваются каналы радиосвязи, то есть радиочастоты или радиодиапазоны, используемые для передачи аналоговой информации или цифровой.

Радиомониторинг в основном, включает в себя деятельность по изучению радиообстановки, поиску, обнаружению и контролю различных каналов связи, радиомикрофонов и других источников радиоизлучений.

Важным достоинством радиомониторинга по сравнению с обычным (разовым) исследованием радиочастотного диапазона является непрерывность получения, достоверность и актуальность добываемых данных.

В процессе регулярного ведения радиомониторинга возможно решение следующих основных задач по обеспечению безопасности защищаемого объекта:

- Выявление излучений радиосредств несанкционированного съема информации, внедренных в помещения объекта, и их локализация.
- Контроль соблюдения дисциплины связи при использовании сотрудниками открытых каналов радиосвязи.
- Выявление информативных побочных излучений, возникающих при работе средств оргтехники, компьютеров и т.п.
- Оценка эффективности используемых на объекте технических средств защиты информации.



- Накопление данных по радиоэлектронной обстановке в зоне расположения объекта и обнаружение новых сигналов с их последующей идентификацией.

Для эффективного решения задач, обозначенных в процессе радиомониторинга, необходимо достаточно хорошо представлять организацию существующих систем радиосвязи, стандарты и способы передачи информации по каналам. Особенно это актуально в диапазонах УВЧ, ОВЧ, которые наиболее интересны для служб безопасности, поскольку именно в здесь работает большинство радиотехнических систем негласного съема информации, а также оперативных систем радиосвязи ведомственного и общего пользования.

Средства негласного съема акустической информации обеспечивают передачу воспринимаемых встроенным микрофоном разговоров или звуковых сигналов и шумов к злоумышленнику по радиоканалу.

Классифицировать радиопередающие устройства, передающие информацию по радиоканалу можно по нескольким критериям:

1. По используемому диапазону длин волн:

- HF(ВЧ) – диапазон (декаметровые волны).
- VHF(ОВЧ) – диапазон (метровые волны).
- UHF(УВЧ) – диапазон (дециметровые волны).
- SVF(GHz) – диапазон (сантиметровые волны).

2. По мощности излучения:

- Малой мощности (до 10 мВт).
- Средней мощности (от 10 до 100 мВт).
- Большой мощности (более 100 мВт).

3. По виду используемых сигналов:

- С простыми сигналами (AM, NFM, WFM – модуляция).
- Со сложными сигналами (шумоподобные, с псевдослучайной фазовой модуляцией (M-последовательность, код Рида – Мюллера и т.п.), с псевдослучайной перестройкой несущей частоты и др.).

4. По способу модуляции сигнала:

- С модуляцией несущей частоты.
- С модуляцией промежуточной частоты (двойная модуляция).

5. По способу стабилизации частоты:

- Нестабилизированные (“мягкий канал”).
- Со схематической стабилизацией частоты или с кварцевой стабилизацией частоты (“жесткий канал”).

Радиопередающие устройства могут быть выполнены в виде отдельного модуля обычно в форме параллелепипеда или закамуфлированы под предметы повседневного обихода: пепельницу, электронный калькулятор, электролампочку, зажигалку, наручные часы, авторучку, вазу, поясной ремень и т.п.

Питание их осуществляется от автономных источников питания (аккумуляторов, батарей), электросети переменного тока, телефонной сети, а также от источников питания радио – электронной аппаратуры, в которой они устанавливаются.

В зависимости от мощности излучения и типа источника питания время работы радиопередающего устройства составляет от нескольких часов до нескольких суток и даже месяцев. При электропитании от сети переменного тока или телефонной линии время работы не ограничено.

Большинство радиопередающих устройств с автономными источниками питания имеют мощность излучения до 10 мВт и дальность передачи информации до 100...200 м, однако встречаются и экземпляры с мощностью излучения в несколько десятков милливатт и дальностью передачи информации до 500...1000 м.

При использовании внешних источников питания (например, электросети или автомобильных аккумуляторов) мощность излучения может составлять более 100 мВт, что обеспечивает дальность передачи информации до нескольких километров.

Демаскирующие признаки автономных некамуфлированных радиопередающих устройств негласного съема информации включают:

- Радиоизлучение (как правило, источник излучения находится в ближней зоне) с модуляцией радиосигнала информационным сигналом.
- Наличие (как правило) небольшого отрезка провода (антенны), выходящего из корпуса закладки.
- Признаки внешнего вида – малогабаритный предмет (часто в форме параллелепипеда) неизвестного назначения;
- Одно или несколько отверстий малого диаметра в корпусе.
- Наличие автономных источников питания (например, аккумуляторных батарей).
- Наличие полупроводниковых элементов, выявляемых при облучении обследуемого устройства нелинейным радиолокатором.
- Наличие в устройстве проводников или других деталей, определяемых при просвечивании его рентгеновскими лучами.

Вследствие того, что при поиске радиопередающих устройств последние находятся в ближней зоне излучения и уровень сигналов о них, как правило, превышает уровень сигналов от других РЭС, у

большинства из них обнаруживаются побочные излучения и, в частности, излучения на второй и третьей гармониках, субгармониках и т.д.

Демаскирующие признаки полуактивных устройств несанкционированного съёма информации по радиоканалу:

- Облучение помещения направленным (зондирующим) мощным излучением (как правило, гармоническим);
- Наличие в помещении переизлученного зондирующего излучения с амплитудной или частотной модуляцией информационным акустическим сигналом.

Рассмотрев различные способы перехвата информации и передачи ее по радиоканалу, и оценив все многообразие устройств, предназначенных для такого рода целей, следует перейти к устройствам, предназначенным для их выявления, и методам использования подобной аппаратуры. К таковой относятся: индикаторы поля, интерсепторы, радиочастотомеры, сканирующие приемники, анализаторы спектра и комплексы радиоконтроля. Последние две позиции в данной работе не рассматриваются, так как им посвящена отдельная лабораторная работа.

## 6. Порядок выполнения лабораторной работы (этапы)

1. Ознакомиться с составом стенда. Изучить инструкции по эксплуатации входящих в состав стенда простейшего индикатора поля Ловец-М и индикатора поля-частотомера RFI-07.

2. Расположить тестовое устройство №1 (ТУ) с полностью выдвинутой вверх антенной в вертикальном положении на правом краю стола и включить (должен загореться красный светодиод, расположенный рядом с антенной). При помощи индикатора поля Ловец-М замерить наибольшие расстояния (антенну прибора не выдвигать для уменьшения чувствительности), на которых происходит срабатывание звуковой индикации прибора от сигнала ТУ при максимальном и минимальном положениях аттенюатора с учетом помеховой обстановки. Результаты измерения расстояний (ориентировочно в метрах и десятых долях) и положений порогов при обнаружении (в дБ) зафиксировать в отчёте.

3. При помощи индикатора поля-частотомера RFI-07 измерить частоту ТУ, зафиксировать результат для отчёта (с точностью до сотых долей МГц). При необходимости осуществить усреднение показаний прибора. Проверить наличие у прибора акустозавязки (активируется в меню прибора). Возникновение акустозавязки возможно при близком расположении микрофона ТУ и динамика частотомера. Протестировать по возможности режим акустозавязки преподавателю.

4. Включить корреляционный приемник «Оракул». Очистить от всех сигналов его банки памяти MEMORY и PASS. Расположив прибор на противоположном конце стола от ТУ (тестовое устройство выключено!), запустить режим поиска только непрерывных сигналов. После предварительного измерения (адаптационный цикл) включить прибор повторно в этот же режим и измерить время сканирования (в секундах). Положение прибора – вертикальное, неподвижное.

5. Зафиксировать общее количество сигналов, количество сигналов по каждому виду модуляции (определённому прибором автоматически), количество сигналов определённых как вещательные станции и как ТВ-передатчики, несущие звука или изображения с допустимой погрешностью прибора в 0,01 МГц), количество неопределённых и опасных сигналов, составить таблицу 1. К радиовещательным станциям относятся сигналы из диапазона 68-108 МГц и прослушиваемые как речевое сопровождение (голос диктора или музыки). Неопределёнными считать сигналы, не относящиеся к радиовещательным станциям и ТВ-передатчикам, а также не являющиеся очевидно опасными (требуется дополнительная идентификация одним из методов). Внести все радиовещательные станции и ТВ-передатчики в список PASS корреляционного приемника. Частоты всех опасных сигналов зафиксировать для отчета.

**Таблица 1** – Таблица результатов проведения радиомониторинга

| № измерения              | 1 | 2 |
|--------------------------|---|---|
| Время сканирования, сек. |   |   |
| Общее кол-во сигналов    |   |   |
| WFM                      |   |   |
| NFM                      |   |   |
| AM                       |   |   |
| PM                       |   |   |
| Кол-во радиостанций      |   |   |
| Кол-во ТВ-станций        |   |   |
| Кол-во неопред. сигналов |   |   |
| Кол-во опасных сигналов  |   |   |

Включить ТУ. И повторить пункт 4 (списки MEMORY и PASS не очищать!), замерив время сканирования. Заполнить продолжение таблицы 1.

Подключить корреляционный приемник «Оракул» к ПК с помощью кабеля, входящего в комплект, и запустить ПО SEL SP81 ORACLE (COM 1). Очистить его память MEMORY и PASS. Включить ТУ. Запустить режим поиска. Зафиксировать для отчёта полную таблицу обнаруженных сигналов, осуществив предварительно сортировку сигналов по уровню, расположив в верхней части наиболее мощные сигналы. Настроить приемник на сигнал ТУ. Просмотреть на экране осциллограммы одновременно демодулированного и акустического сигналов (режим включается с панели управления). Зафиксировать для отчёта осциллограмму, доказывающую корреляцию сигналов (совпадение изменений их амплитуд при появлении звуков в помещении).

Включить режим поиска сотовых телефонов. Убедившись в отсутствии сигналов, включить сотовый телефон на передачу (предварительно переключив его из 3G в EDGE), набрав номер своего знакомого или однокурсника. Телефон располагать на расстоянии около 100-150 см от устройства. Добившись нескольких показаний на оси времени с указанием амплитуды сигнала, поднести телефон на расстояние около 3-5 см к приемнику. Зафиксировать увеличение показаний отчетов на оси времени на экране компьютера для отчёта в виде скриншота.

Ознакомиться с поисковым скоростным приемником «Скорпион». Провести сканирование диапазона со включенным ТУ, зафиксировать показания частоты тестового устройства. Результат продемонстрировать преподавателю.

#### **7. Контрольные вопросы:**

1. Понятие мониторинга. Радиомониторинг?
2. Задачи радиомониторинга?
3. Условия проведения радиомониторинга?
4. Радиочастотный диапазон, его разделение?
5. Радиоканал как канал утечки информации?
6. Классификация по частоте, по мощности, по способу стабилизации?
7. Классификация по способу модуляции, по виду используемых сигналов, по способу питания?
8. Классификация по способу управления, по виду передаваемой информации, по способу исполнения?
9. Демаскирующие признаки скрытых радиопередатчиков?
10. Аппаратура, применяемая для радиомониторинга?
11. Принцип действия и основные типы индикаторов поля?
12. Классификация индикаторов поля?
13. Методика поиска при использовании индикаторов поля?
14. Интерсепторы и радиочастотомеры. Принцип работы?
15. Сканирующие приемники?
16. Корреляционный метод?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, автор, эл. почта:** Новосибирский государственный технический университет, кафедра защиты информации, старший преподаватель Теличко Евгений Анатольевич, эл. почта: telichko@corp.nstu.ru

---

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, Информационная безопасность автоматизированных систем на транспорте.

**Дисциплина:** Техническая защита информации.

#### **Лабораторная работа.**

#### **Освоение практических приёмов работы с системой "Шепот"**

##### **1. Учебные цели:**

- Ознакомиться с назначением, техническими характеристиками и составом оборудования системы «Шепот», принципом работы основных элементов системы «Шепот». Отработать навыки установки программного обеспечения «Шепот-Интерфейс», навыки калибровки микрофона и навыки работы с шумомером в ручном режиме.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- **Знать** способы и средства контроля эффективности защиты информации.
- **Уметь** использовать средства инструментального контроля показателей эффективности технической защиты информации.

### 3. Перечень материально-технического обеспечения:

- Компьютер, носитель с программным обеспечением «Шепот-интерфейс», HASP ключ, рабочая укладка, микрофон, калибратор, микрофонный кабель, USB кабель.

### 4. Задание на исследование:

- Провести развертывание и подготовку к работе системы «Шепот» в автоматическом и ручном режимах.

### 5. Краткие теоретические сведения

Назначение, технические характеристики и состав системы

Система оценки защищенности выделенных помещений по виброакустическому каналу «Шепот» предназначена для проведения специальных акустических и вибрационных измерений в выделенных помещениях с целью оценки их защищенности от утечки речевой информации по акустическому и вибрационному каналам. Система «Шепот» обеспечивает автоматические измерения уровня звукового давления в 5-ти октавных полосах с центральными частотами 250, 500, 1000, 2000 и 4000 Гц, автоматические измерения уровня виброускорения, возможность перехода на ручное управление аппаратурой системы, автоматизированный расчет показателей защищенности выделенных помещений по акустическому и виброакустическому каналу утечки речевой информации, возможность настройки системы защиты выделенных помещений объекта от утечки речевой информации по акустическому и виброакустическому каналу, формирование и ведение базы данных о месте и результатах выполненных измерений, составление отчета по результатам измерений в форме, отвечающей требованиям нормативной документации.

Основные технические характеристики:

- нижняя граница диапазона измерений звукового давления, не выше 24 дБ;
- верхняя граница диапазона измерений звукового давления, не ниже 132 дБ;
- абсолютная погрешность измерений виброускорения, не более  $\pm 0,7$  дБ;
- нижняя граница диапазона частот анализа в реальном времени, не выше 20 Гц;
- верхняя граница диапазона частот анализа, не ниже 7000 Гц;
- максимальное звуковое давление тест-сигнала в свободном пространстве на расстоянии 1 м от излучателя (интегральное, в полосе частот 175–5600 Гц) не менее 106 дБ;
- погрешность установки звукового давления калибратора, не более  $\pm 0,3$  дБ;
- мощность, потребляемая системой, не более 40 Вт.

Состав системы

Система поставляется в двух укладках – рабочей и транспортной.

В рабочей укладке смонтирована плата коммутатора, в ней также размещен шумомер, микрофоны, акселерометр, калибратор и соединительные кабели.

В транспортной укладке размещаются источник акустического сигнала «Шорох-2МИ», звуковая колонка, персональный компьютер, программное обеспечение управления системой «Шепот» и расчета параметров защищенности выделенных помещений по виброакустическому каналу «Шепот-Интерфейс» с ключом защиты Aladdin HASP, штативы, соединительные кабели.

Назначение основных компонентов системы

Генератор шума «Шорох-2МИ» предназначен для генерации электрического сигнала с возможностью регулировки его уровня на центральных октавных частотах 250, 500, 1000, 2000, 4000 Гц.

Акустический излучатель (звуковая колонка) предназначен для преобразования электрического сигнала в акустические колебания воздушной среды.

Микрофон предназначен для преобразования звукового давления в воздушной среде в электрический сигнал.

Акселерометр предназначен для преобразования виброускорений в твердых средах в электрический сигнал.

Шумомер предназначен для измерения уровня электрического сигнала от микрофонов или акселерометра и обработки результатов измерений.

Компьютер с соответствующим программным обеспечением предназначен для управления компонентами системы, ведения базы данных об исследуемых объектах и результатах измерений, выполнения необходимых расчетов и подготовки отчета.

Коммутатор управляемый смонтирован в рабочей укладке и предназначен для обеспечения управления отдельными компонентами системы «Шепот» по командам от компьютера.

К разъему «КАНАЛ 1» подключается микрофон, измеряющий уровень тестового сигнала. К разъему «КАНАЛ 2» подключается микрофон или акселерометр, измеряющий уровень информативного сигнала, фона и помехи. К разъему «УПРАВЛЕНИЕ» подключается генератор тестового сигнала «Шорох-2МИ». Разъем USB предназначен для подключения рабочей укладки к управляющему компьютеру.

Калибратор CAL-200 предназначен для калибровки шумомера. Калибратор создает звуковое давление 94 или 114 дБ на частоте 1000 Гц. На правой боковой стороне калибратора расположены кнопка ВКЛ и переключатель 94 дБ – 114 дБ. При нажатии на кнопку ВКЛ калибратор в течении 2-х минут создает заданное звуковое давление.

Высокоточный шумомер Larson&Davis Модель 824 является многоцелевым прибором для измерения уровня звука и спектрального анализа акустической обстановки. Упрощенная структурная схема шумомера изображена на рисунке 1.

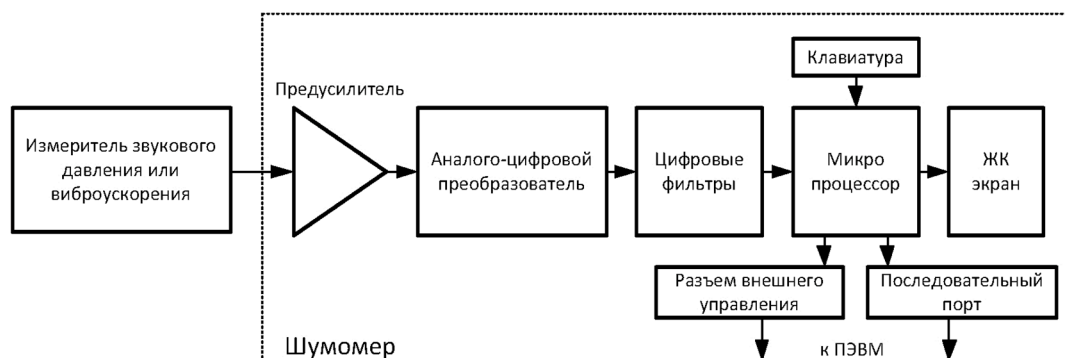


Рис. 1. Упрощенная структурная схема шумомера

### Принцип работы системы

Генератор тестового сигнала «Шорох-2МИ» по командам от компьютера формирует с помощью акустического излучателя (звуковой колонки) шумовой тест-сигнал в пяти октавных полосах, который принимается микрофоном 1.

Электрический сигнал от микрофона через управляемый коммутатор поступает в шумомер, где происходит измерение его уровня. Значения измеренных шумомером уровней информативного (тестового) сигнала в пяти октавных полосах записываются в базу данных компьютера. Длительность одного цикла измерения шумомера составляет 125 мс. Усредненные и минимальные значения измеренных сигналов записываются в базу данных компьютера (рис. 2).

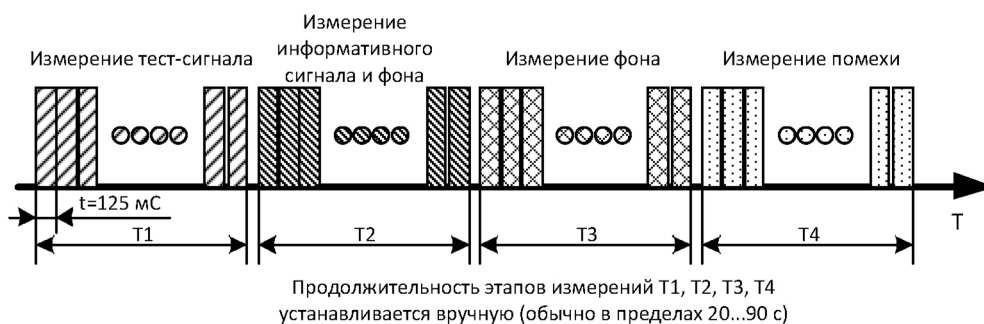


Рис. 2. Временная диаграмма последовательности циклов измерения

Во время второго этапа измерения в управляемом коммутаторе микрофон 1 отключается и включается микрофон 2, таким образом происходит измерение уровня информативного (тестового) сигнала и фона за ограждающей конструкцией аналогично измерению тест-сигнала.

На третьем этапе, по команде компьютера, излучение тест-сигнала прекращается и через микрофон 2 производится измерение уровня только акустического фона. Если проводится оценка эффективности помех, создаваемых средствами активной защиты (САЗ), то проводится четвертый этап измерения. При этом система предлагает включить САЗ после чего начинается измерение помехи и фона. При проведении виброакустических измерений система работает аналогично, только вместо микрофона 2 используется акселерометр.

### Калибровка системы «Шепот»

Для проведения калибровки микрофон должен быть подключен к шумомеру через коммутатор, а управление коммутатором осуществляется через компьютер.

Режим ручного управления системой «Шепот», кроме калибровки, может использоваться для проведения измерений в ручном режиме и для проверки работоспособности системы.

Включение и перевод системы в режим ручного управления осуществляется следующим образом:

Осуществляется сборка системы. Запустить программное обеспечение «Шепот-Интерфейс». Запуск программы «Шепот-Интерфейс» выполняется аналогично запуску любого приложению Windows щелчком левой кнопки мыши по позиции этой программы. Включить рабочую укладку и шумомер. (В некоторых версиях включение шумомера происходит при включении питания рабочей укладки).

Установить параметры соединения с шумомером. Для этого в главном окне кликнуть третью слева кнопку «Параметры соединения с шумомером и контрольной точки». В открывшемся окне «Начальные установки» в поле «Выбор шумомера» убедиться, что флаг выбора шумомера установлен на заданном шумомере.

Установить параметры соединения ПЭВМ и шумомера, для этого в поле «Соединение» в окне «Порт» указать номер COM-порта ПЭВМ, к которому подсоединен шумомер. Номер порта ПЭВМ, используемого для подключения шумомера, может быть введен с клавиатуры заглавными латинскими буквами. Уточнить номер порта можно в диспетчере устройств ПЭВМ. В окне «Скорость» из списка должно быть выбрано значение установленной на шумомере скорости передачи его данных. Рекомендованное значение скорости передачи данных для установки на шумомере и в окне «Скорость» - 19200 бит/с. Для вступления введенных в этом окне параметров в силу необходимо кликнуть на кнопке «Применить».

Уточнить/изменить скорость передачи данных шумомера. Для этого необходимо на шумомере нажать «Tolls/Communications/Bound» и выставить рекомендованное значение скорости передачи «19200». Убедиться, что флаг «ICP-питание» в окне «Начальные установки» установлен. При наличии этого флага производится программное включение встроенного источника ICP-питания измерительных датчиков системы «Шепот».

Ввести поверочные данные микрофонов и акселерометра. Для этого кликнуть на кнопке «Калибровка» в окне «Начальные установки», при этом появится окно ввода поверочных данных. Из поверочной таблицы занести данные в соответствующие окна, кликнуть на кнопках «Перевод дБ в мВ/Па», «Расчет поправки для акселерометра» и «ОК». Для вступления введенных в этом окне параметров в силу необходимо кликнуть на кнопке «Применить» в окне «Начальные установки». Микрофон 1 необходимо пометить и в дальнейшем использовать его только как МИКРОФОН 1. Ввод поверочных данных проводится однократно и должен быть повторен при замене микрофонов (акселерометра) или при замене компьютера (программного обеспечения).

Перейти в ручной режим работы. Для этого необходимо кликнуть на кнопке «Тест коммутатора» в главном рабочем окне. При этом появится окно «Тест коммутатора». Поле «Шепот» окна «Тест коммутатора» предназначено для управления системой «Шепот» в ручном режиме.

Кнопка «1 канал» – включает/выключает «Вход 1» рабочей укладки.

Кнопка «2 канал» – включает/выключает «Вход 2» рабочей укладки.

Кнопка «Сброс» служит для одновременного выключения подключенного канала («1 канала» или «2 канала») и «Генератора шума».

Установка флага «ICP-питание» в нижнем правом углу окна «Начальные установки» или окна «Тест коммутатора» включает источник ICP-питания измерительных датчиков рабочей укладки системы «Шепот». При наличии данного флага при открытии окна «Тест коммутатора» активируется полоса времени задержки. Необходимо выждать время, пока полоса полностью не заполнится. Данное время необходимо для накопления необходимого рабочего уровня заряда измерительных датчиков.

Нажать клавишу «TOOLS» (Инструментарий) на шумомере. При этом на экране шумомера появится одноименное меню. Управляющими клавишами необходимо перевести горизонтальный курсор на опцию «CALIBRATION» (Калибровка) и затем нажать клавишу «Вправо», чтобы войти в меню калибровки. Ввести микрофон в акустический калибратор. На калибраторе установить переключатель в положение «94 дБ». Убедиться, что уровень, создаваемый калибратором, соответствует значению опции «CAL LEVEL» (уровень калибратора). При необходимости это значение редактируется. Для этого курсор устанавливается на опцию «CAL LEVEL» и клавишей «ВПРАВО» шумомер переводится в режим редактирования. Управляющими клавишами устанавливаются нужные значения.

Перевести шумомер в режим «CHECK» (Контроль), включить калибратор и на шумомере и нажать клавишу «ОК». После проведения измерений прибор должен показать уровень звука «94 дБ». Если этого не произошло, то необходимо опять включить калибратор, затем клавишами выделить опцию «Change» (Изменить) калибровку. После нажатия клавиши «ОК» прибор перейдет в режим калибровки, в процессе которого он сначала проверяет, насколько стабилен уровень калибровочного сигнала, а затем автоматически настраивается так, чтобы измеряемое значение равнялось введенному калибровочному уровню 94 дБ.

На этом процесс калибровки заканчивается. Необходимо помнить, что калибровку необходимо проводить перед каждой серией измерений.

Работа системы в ручном режиме

Работу системы в ручном режиме рассмотрим на примере измерения уровней шума в помещении.

После нажатия клавиши «SETUP» (установка) на шумомере появится меню. Управляющими клавишами необходимо выбрать конфигурацию «SLM&RTA.SSA» и нажать «ОК». Чтобы провести пробное измерение, необходимо нажать клавишу «RUN/STOP». Когда прибор производит измерения, в правом верхнем углу экрана появляется фигурка бегущего человека. Это означает, что прибор производит измерения. Если нажать клавишу «RUN/STOP», то на экране в правом верхнем углу появится символ квадрата, показывающий, что измерение остановлено.

В режиме «SLM-RTA» на экран можно вывести различные окна просмотра результатов измерений. Для этого необходимо нажать клавишу «VIEW» и с помощью управляющих клавиш выделяется

пункт, например, «RTA» и нажимается клавиша «ОК». Окно «RTA» показывает спектр текущих уровней звукового давления в октавных или третьоктавных полосах частот. Используя управляющие клавиши можно изменить частоту курсора (частота курсора в герцах выводится в левом нижнем углу экрана). Уровень звукового давления на частоте курсора выводится в левом верхнем углу. Положение курсора отмечено на графике в виде незакрашенного столбика. За перемещением курсора можно следить как с помощью графика, так и с помощью числового значения в левом нижнем углу экрана.

#### **6. Порядок выполнения лабораторной работы (этапы)**

1. Собрать лабораторную установку.
2. Включить ПЭВМ, рабочую укладку, установить программное обеспечение, параметры соединения ПЭВМ с рабочей укладкой, запустить программное обеспечение и ознакомиться с основными элементами главного рабочего окна.
3. Ввести в ПЭВМ поправочные значения из поверочной таблицы микрофона.
4. Провести калибровку с микрофонным кабелем длиной 2 м, проверить калибровку, при этом убедиться, что калибровка не нарушена.
5. Проверить калибровку с микрофонным кабелем длиной 20м. Если калибровка окажется нарушенной, то объяснить причины.
6. Перевести шумомер в режим измерения (конфигурация SML-RTA.SSA). Провести измерения шума в помещении. Замерить средний и минимальный уровень шума. Определить на каких частотах в помещении существует максимальный уровень шума

#### **7. Контрольные вопросы:**

1. Зачем необходим ввод поправочных коэффициентов из поверочных таблиц?
2. Зачем необходимо калибровать систему перед проведением измерений?
3. Назначение основных клавиш шумомера?
4. Почему нельзя использовать шумомер в составе рабочей укладки для проведения измерений без применения ПЭВМ?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** Дальневосточный государственный университет путей сообщения, Рак Евгений Владимирович, pm@festu.khv.ru

---

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем.

**Дисциплина:** Техническая защита информации.

### **Лабораторная работа.**

#### **Исследование побочных электромагнитных излучений видеосигнала ПЭВМ**

##### **1. Учебные цели:**

- Обучение принципам проведения измерений побочных электромагнитных излучений (ПЭМИ) средств вычислительной техники по радиоэффиру; изучение причин возникновения и характеристик сигналов ПЭМИ в видеотракте и системном блоке компьютера.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

###### **Уметь:**

- проводить настройку оборудования для исследования ПЭМИ;
- проводить измерения ПЭМИ в указанных диапазонах частот.

###### **Иметь навыки:**

- работы с приемо-передающим оборудованием;
- настройки цифрового осциллографа для исследования характеристик радиосигналов
- работы с тестовым генератором радиосигнала

##### **3. Перечень материально-технического обеспечения**

- **Лабораторное оборудование и программное обеспечение:**
  - Анализатор спектра типа IFR2399C.
  - Антенна измерительная дипольная АИ5-0.
  - Антенна измерительная рамочная АИР3-2.
  - Устройство развязывающее УР-1
  - Тестовая программа «Monitor»

#### 4. Задание на исследование:

Исследовать характеристики побочных электромагнитных излучений видеосигнала ПЭВМ при различных вариантах сочетаний разрешений и частоты развертки.

#### 5. Краткие теоретические сведения

В случаях, когда технические средства применяются для обработки информации ограниченного доступа, наибольшую актуальность имеют вопросы, связанные с информативными побочными электромагнитными излучениями и наводками (ПЭМИН). Под ними понимают ПЭМИН, которые содержат сведения об обрабатываемой информации.

Характер ПЭМИ определяется назначением, схемными решениями, элементной базой, мощностью устройства, а также материалами, из которых изготовлен корпус, и его конструкцией. Излучение может происходить в широком диапазоне частот (от единиц герц до гигагерц), а дальность реального перехвата информации достигать сотен метров.

В персональном компьютере действует большое количество генераторов периодических сигналов, модулируемых информационными последовательностями данных. И большинство из них можно обнаружить в эфире или сети питания без использования высокочувствительных радиоприемников. Существуют программы, непосредственно использующие ПЭМИ для передачи хранимой в компьютере информации.

Согласно действующим нормативно-методическим документам (НМД), при проведении специальных исследований (СИ) требуется измерять информативные ПЭМИ, то есть такие излучения, создаваемые исследуемым техническим средством, которые содержат обрабатываемую данным техническим средством информацию. Такие излучения составляют лишь малую долю от всего спектра излучений технического средства. Все прочие излучения не должны фиксироваться при измерениях. Для того чтобы выделить информационные ПЭМИ, на исследуемом техническом средстве предусматривают специальные тестовые режимы его работы. Требования к тестам определяются в соответствующих ГОСТах и методиках.

Перехват ПЭМИ цепей, по которым передается видеосигнал, дает возможность восстановления большей части информации не восстанавливая при этом последовательности значений каждого разряда кода. Видеосигнал является периодическим сигналом, а сигнал, передаваемый от клавиатуры к системному блоку, – аperiodическим.

Периодический сигнал можно накапливать в приемнике что позволяет в дальнейшем проводить его обработку. Видеосигнал занимает широкую полосу частот, расположенную частично в высокочастотной части радиодиапазона.

Излучения цепей, по которым передаются сигналы от контроллера клавиатуры к порту вывода на материнской плате, находятся в низкочастотной области радиодиапазона. В этой части диапазона сосредоточены промышленные помехи, которые в значительной степени мешают приему информативных ПЭМИ. Кроме того с увеличением частоты сигнала увеличивается коэффициент полезного действия (КПД) антенны (излучающей цепи).

Таким образом, наибольшую опасность будут представлять информативные ПЭМИ, передающие видеосигнал от видеоадаптера к монитору. Знание взаимодействия и работы элементов и узлов исследуемых ТСС (в данном случае ПЭВМ) могут существенно оптимизировать защиту от утечки опасных сигналов по каналам ПЭМИ.

#### 6. Порядок выполнения лабораторной работы (этапы)

Подключить к анализатору спектра измерительную антенну АИ 5-0.

Включить в сеть электропитания сначала анализатор спектра, затем развязывающее устройство. Включить в сеть электропитания исследуемую ПЭВМ (пароль - @gji0kns).

Установить на исследуемой ПЭВМ заданное преподавателем разрешение экрана и частоту обновления изображения.

Вычислить по приведенной ниже формуле ориентировочное значение тактовой частоты видеосигнала:

$$F_{\Gamma} = A \cdot B \cdot \frac{F}{1,4}, [\text{МГц}] \quad (1)$$

где  $A$  – количество точек по горизонтали;  $B$  – количество точек по вертикали;  $F$  – частота обновления изображения, Гц.

Запустить тестовую программу для видеосигнала, для чего:

- найти на рабочем столе программу «Monitor» и запустить ее;
- выбрать опцию «Мигание статической засветки»;
- нажать клавишу «Дополнительно» и установить следующие параметры:
  - статическая засветка экрана – точка через точку;
  - цвет «темной» точки – черный;
  - цвет «светлой» точки – белый;



- количество линий в подкраске № 1 – 1;
- количество линий в подкраске № 2 – 1;
- время полной засветки экрана – 1000 мс;
- время подкраски № 1 – 1 мс;
- время подкраски № 2 – 1 мс;
- время полного гашения – 500 мс;
- время мигания статической засветки – 1000 мс;
- нажать клавишу «Применить»;
- нажать клавишу «Старт»;
- на экране будет чередование во времени полного гашения изображения черных и белых вертикальных полос;
- для остановки программы нажать клавишу «Esc»;
- настройка частоты середины экрана:
  - нажать клавишу «FREQ» на передней панели анализатора спектра;
  - с помощью клавиатуры ввести требуемое значение частоты в мегагерцах, вычисленное по формуле (1);
  - ввести размерность частоты с помощью клавиш, расположенных справа от экрана («МГц»);
- настроить полосу обзора:
  - нажать клавишу «SPAN» на передней панели анализатора спектра;
  - с помощью клавиатуры ввести требуемое значение частоты в мегагерцах, например – 2 МГц;
  - ввести размерность частоты с помощью клавиш, расположенных справа от экрана («МГц»);
- настроить полосу пропускания:
  - нажать клавишу «CLP» на передней панели анализатора спектра;
  - с помощью клавиатуры ввести требуемое значение частоты в килогерцах, например – 3 кГц;
  - ввести размерность частоты с помощью клавиш, расположенных справа от экрана RBW (F2) («кГц»);
- осуществить поиск и измерение уровня сигнала:
  - нажать клавишу «FREQ» на передней панели анализатора спектра и с помощью вращающегося колеса перестраивать анализатор спектра на несколько мегагерц выше и ниже расчетного значения частоты;
  - измерить уровень мощности найденного сигнала (в дБм) с помощью маркера путем нажатия клавиши «MKR» и установке маркера на отклик сигнала вращением колеса;
  - перевести найденное значение уровня мощности в напряжение

$$U_{[\text{дБмкВ}]} = 107 - P_{[\text{дБм}]}; \quad (2)$$

- рассчитать напряженность электрической составляющей электромагнитного поля

$$E_{[\text{дБмкВ/м}]} = U_{[\text{дБмкВ}]} + k_{A[\text{дБ/м}]} \quad (3)$$

Повторить поиск и измерение уровня сигнала на его высших гармониках (2F, 3F и т.д. до 2000 МГц). Результаты измерения свести в таблицу.

| Частота f, МГц                               | F <sub>T</sub> | 2F <sub>T</sub> | 3F <sub>T</sub> | 4F <sub>T</sub> | ... | ... | ... | F <sub>T</sub> |
|----------------------------------------------|----------------|-----------------|-----------------|-----------------|-----|-----|-----|----------------|
| Напряжение U, дБмкВ                          |                |                 |                 |                 |     |     |     |                |
| Коэффициент калибровки k <sub>A</sub> , дБ/м |                |                 |                 |                 |     |     |     |                |
| Напряженность поля E, дБмкВ/м                |                |                 |                 |                 |     |     |     |                |

Подключить к анализатору спектра измерительную антенну АИР 3-2.

Проделать указанные выше операции в диапазоне частот до 30 МГц. Рассчитать напряженность магнитной составляющей электромагнитного поля

$$\rho H_{[\text{дБмкВ/м}]} = U_{[\text{дБмкВ}]} + k_{A[\text{дБ/м}]} \quad (4)$$

Результаты измерения свести в таблицу:

| Частота f, МГц                               | F <sub>T</sub> | 2F <sub>T</sub> | 3F <sub>T</sub> | 4F <sub>T</sub> | ... | ... | ... | F <sub>T</sub> |
|----------------------------------------------|----------------|-----------------|-----------------|-----------------|-----|-----|-----|----------------|
| Напряжение U, дБмкВ                          |                |                 |                 |                 |     |     |     |                |
| Коэффициент калибровки k <sub>A</sub> , дБ/м |                |                 |                 |                 |     |     |     |                |
| Напряженность поля ρH, дБмкВ/м               |                |                 |                 |                 |     |     |     |                |

Отчет по выполненной работе должен содержать:

- описание лабораторной установки с приведением технических характеристик используемого оборудования;
- таблицы с результатами измерений в указанных диапазонах частот.

## 7. Контрольные вопросы

1. Что такое «побочные электромагнитные излучения»?
2. Какими цепями ПЭВМ создаются «информативные ПЭМИ»?

3. Какими цепями ПЭВМ создаются «неинформативные ПЭМИ»?
4. Какими цепями ПЭВМ создаются «безопасные информативные ПЭМИ»?
5. Для какой цели используются тестовые программы?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** Федеральное государственное автономное образовательное учреждение высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» (Самарский университет), ул. Московское шоссе, д. 34, г. Самара, 443086, д.т.н. профессор Сергеев В.В., старший преподаватель Дворянинов С.М., dwogyninowsm@mail.ru

## **Дисциплина: Технические средства охраны объектов**

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, 10.03.01 Информационная безопасность.

**Дисциплина:** Технические средства охраны объектов

### **Лабораторная работа.**

#### **Принципы построения и особенности применения современных систем охранно-пожарной сигнализации**

##### **1. Учебные цели:**

- Изучить конструкцию и принцип действия современных охранных и пожарных извещателей, приемно-контрольных панелей, оповещателей;
- Изучить правила соединения оборудования охранно-пожарной сигнализации;
- Отработать навыки размещения и соединения оборудования охранно-пожарной сигнализации для создания рабочей системы охранно-пожарной сигнализации.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- Уметь выбирать тип извещателя для обеспечения выбранного способа защиты.
- Уметь соединять оборудование охранно-пожарной сигнализации для создания рабочей системы охранно-пожарной сигнализации.
- Владеть навыками программирования приемно-контрольных панелей.

##### **3. Перечень материально-технического обеспечения**

- **Лабораторное оборудование и программное обеспечение:**
  - Приемно-контрольная панель «Гранит-4».
  - Приемно-контрольная панель NX-6.
  - Управляющая клавиатура NX-148.
  - Охранный инфракрасный извещатель «Астра».
  - Охранный инфракрасный извещатель «Рапид».
  - Охранный инфракрасный извещатель «Рефлекс».
  - Охранный магнито-контактный извещатель СМК.
  - Пожарный дымовой оптико-электронный извещатель ИП-212-4С.
  - Пожарный дымовой оптико-электронный извещатель ДИП-212-41-Н.
  - Пожарный дымовой оптико-электронный извещатель ИП-212-66.
  - Тепловые пожарные извещатели ИП-103-3-А2-1Н.
  - Звуковой оповещатель Маяк -12.
  - Демонстрационный стенд в составе:
    - Магнито-контактный извещатель ИО-102-14 (СМК).
    - Акустический извещатель ИО-329-3 (Арфа).
    - Акустический извещатель ИО-329-1 (Стекло).
    - Тепловой максимальный извещатель ИП-103-3-А2-1Н
    - Дымовой оптико-электронный извещатель ДИП-212-41-Н
    - Дымовой оптико-электронный извещатель ИП-212-66

##### **4. Задание на исследование**

На рисунке 1 показано размещение элементов лабораторного стенда.

Варианты параметров задания:

- Создание охранно-пожарной сигнализации на основе приемно-контрольной панели «Гранит-4».
- Создание охранно-пожарной сигнализации на основе приемно-контрольной панели NX-6.

##### **5. Краткие теоретические сведения**

На рисунке 2 приведена классификация датчиков, используемых в системах сигнализации. Необходимо отметить, что в большинстве каталогов и прайс-листах оборудования охранно-пожарной сигнализации датчики называются извещателями.

Пожарные датчики – предназначенные для предупреждения о возникновении пожара;

Охранные датчики – предназначенные для предупреждения о вторжении на охраняемый объект;

Совмещенные датчики – представляют собой охранный и пожарный датчик размещенные в одном корпусе. Такое конструктивное оформление датчика позволяет в некоторых случаях уменьшить трудозатраты на монтаж систем сигнализации. Так как принципиальных отличий от датчиков двух других групп они не имеют, более подробно они рассматриваться не будут.

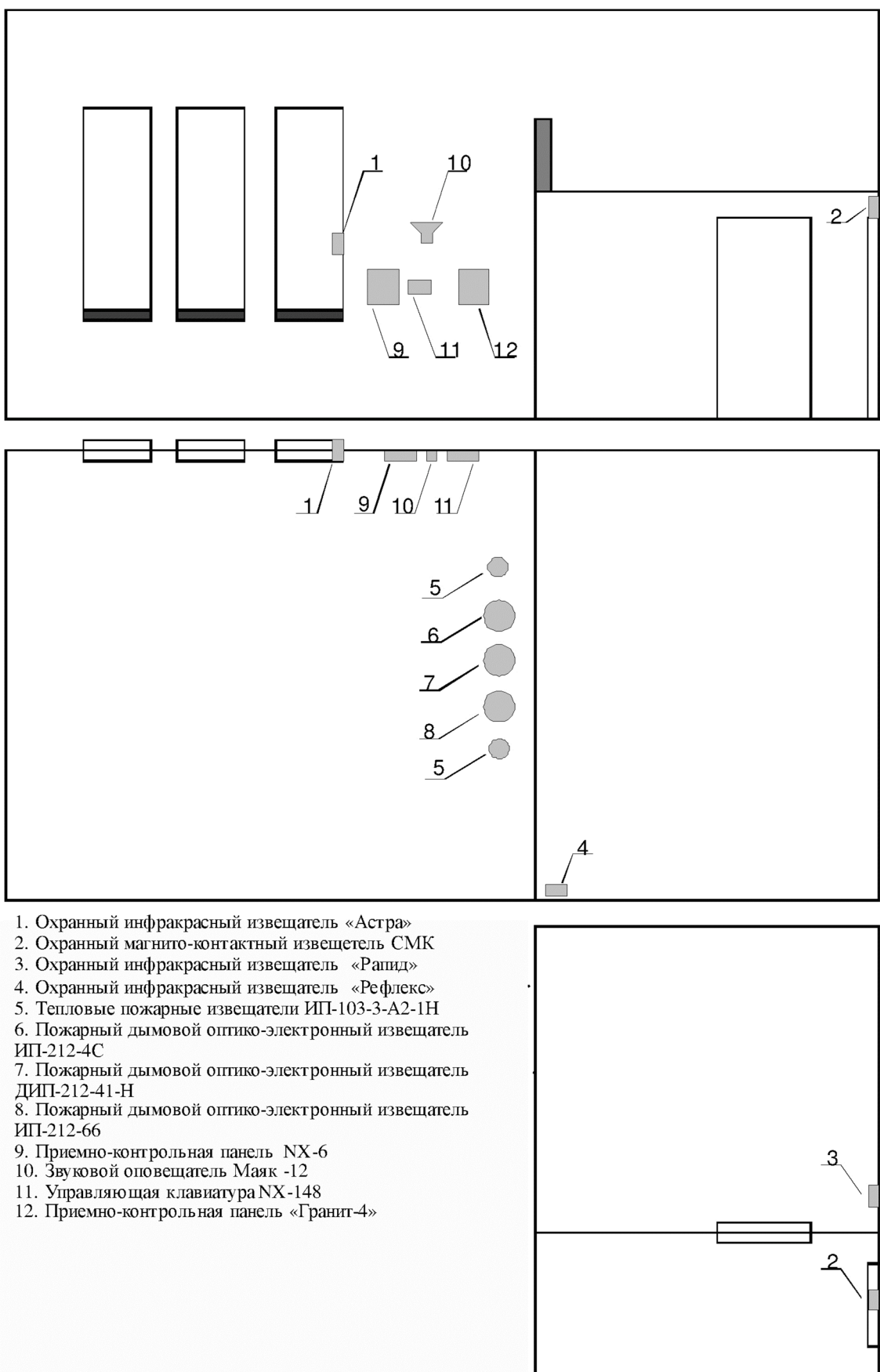


Рис. 1. Размещение элементов лабораторного стенда

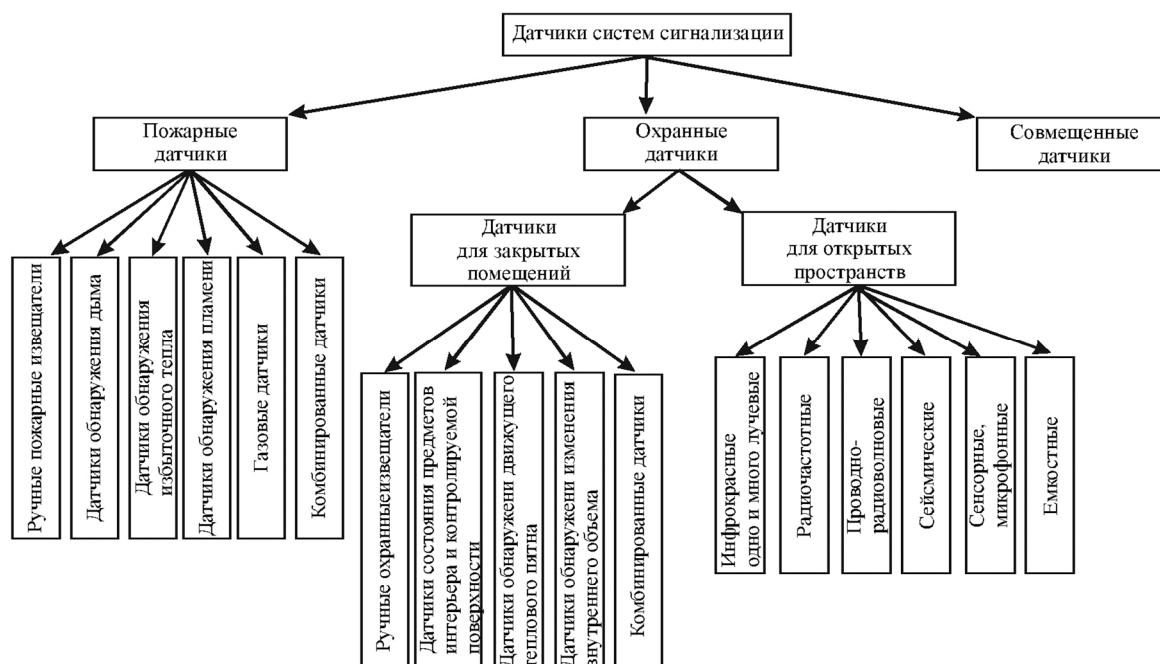


Рис. 2. Классификация датчиков систем сигнализации

В группу пожарных датчиков входят:

6. ручные пожарные извещатели – представляют собой механические устройства, имеющие в своем составе рычаги или кнопки, которые после их приведения в состояние тревоги могут быть возвращены в исходное состояние только при помощи специальных приспособлений;
7. датчики обнаружения дыма (дымовые датчики) – формируют сигнал тревоги при появлении в месте установки дыма с концентрацией выше определенного порога;
8. датчики обнаружения избыточного тепла (тепловые датчики) – формируют сигнал тревоги если в течении определенного времени температура в месте установки выше определенного порога или если в месте установки за короткий промежуток времени (несколько секунд) произошел резкий скачок температуры;
9. датчики обнаружения пламени – формируют сигнал тревоги, если в зоне действия датчика обнаружены признаки присутствия открытого огня;
10. газовые датчики – формируют сигнал тревоги при повышении в помещении концентрации газов, выделяющихся при горении, например, углекислого газа  $\text{CO}_2$ ;
11. комбинированные датчики – представляют собой установленные в одном корпусе два пожарных датчика реагирующих на разные физические факторы. Например, ИП212/101-2 производства фирмы SYSTEM SENSOR LTD совмещающий дымовой и тепловой датчики.

Датчики для закрытых помещений.

В зависимости от принципа действия охранные датчики для закрытых помещений бывают следующих типов:

- ручные охранные извещатели (называемые так же тревожными кнопками) – предназначены для передачи сигнала тревоги на пульт охраны сотрудниками охраняемого объекта. Конструктивно представляют собой кнопки без фиксации. В зависимости от расстояния до пульта охраны могут комплектоваться дополнительными устройствами передачи данных;
- датчики состояния предметов интерьера и контролируемой поверхности – предназначены для контроля за положением предметов интерьера (открыты или закрыты двери, окна) и за целостностью контролируемых поверхностей (разбитие стекла, разрушение двери);
- датчики обнаружения движущегося теплового пятна – сигнал тревоги формируется, если в зоне действия датчика появляется движущееся теплое пятно с размерами больше пороговых;
- датчики обнаружения изменения внутреннего объема – сигнал тревоги формируется при изменении внутреннего объема помещения. Например, при входе человека в помещение свободный объем уменьшится.
- комбинированные датчики – представляют собой установленные в одном корпусе два охранных датчика реагирующих на разные физические факторы.

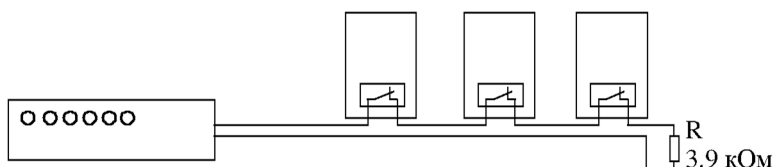
На рисунке 3 показаны способы организации связи между основными элементами систем охраны. Данная классификация упрощенная. В реальной системе охраны присутствуют, как правило, все способы организации связи. Как видно из названия для организации проводных соединений прокладываются кабели, а

для организации беспроводных соединений этого не требуется. Из всех возможных беспроводных каналов передачи информации в настоящее время используется только радиоканал.



**Рис. 3.** Способы организации связи между основными элементами системы сигнализации

Для обеспечения надежной работы систем сигнализации должен осуществляться контроль целостности канала передачи данных. При применении адресных датчиков это реализуется периодическим опросом состояния датчиков со стороны приемно-контрольной панели. При использовании неадресных датчиков в шлейф включают дополнительные элементы. При использовании датчиков, формирующих сигнал тревоги размыканием реле около самого удаленного датчика в шлейф включают резистор с сопротивлением в диапазоне 3.3–3.9 кОм (рис. 4).



**Рис. 4.** Пример соединения нескольких извещателей в один шлейф

В случае обрыва шлейфа будет формироваться сигнал тревоги, что приведет к необходимости осмотра помещений, подключенного к данному шлейфу. При этом существует вероятность обнаружения места повреждения или помещения будут находиться под более тщательным наблюдением до приезда сотрудников, обслуживающих сигнализацию. Если в результате каких-либо действий (случайных или намеренных) произойдет короткое замыкание шлейфа, то приемно-контрольная панель выдаст сигнал «Авария», что сигнализирует о прекращении нормальной работы датчиков, подключенных к шлейфу.

## 6. Порядок выполнения лабораторной работы (этапы)

### Вариант 1.

1. Основываясь на инструкции по эксплуатации приемно-контрольной панели «Гранит-4», определить, на работу с какой из тактик применения, настроена панель.
2. Присоединить к охранным извещателям кабели с соответствующими бирками. При соединении учитывать необходимость контроля целостности шлейфа. Для этого используются дополнительные элементы (резисторы).
3. Присоединить охранные извещатели к приемно-контрольной панели таким образом, чтобы реализовать следующий алгоритм охраны помещения:
  - при входе в помещение сирена должна срабатывать кратковременно, с возвратом в исходное положение. Это необходимо чтобы вошедший мог снять систему с режима охраны, если имеет такие полномочия;
  - оконный проем, верхняя площадка помещения и помещение под верхней площадкой охраняются при помощи одного шлейфа. При появлении движения в данных местах приемно-контрольная панель должна формировать акустический сигнал тревоги, если «Гранит-4» находится в режиме охраны;

Присоединить к приемно-контрольной панели пожарные датчики. Тип датчиков определяется преподавателем (тепловые или дымовые).

4. В соответствии с инструкцией по эксплуатации «Гранит-4», присоединить сирену.
5. Сориентировать охранные инфракрасные извещатели «Рapid» и «Рефлекс» таким образом, чтобы они обеспечивали максимальную эффективность охраны опасных направлений и минимальные ложные тревоги. Для датчика расположенного на верхней площадке («Рефлекс») опасным направлением являются перила, ограждающие площадку. При этом в зону действия датчика не должно попадать пространство, расположенное на нижнем уровне. Датчик расположенный под верхней площадкой («Рapid») необходимо сориентировать так, чтобы проход человека мимо дверного проема в это помещение не вызывал срабатывания. При ориентации датчиков необходимо следить за состоянием встроенного светодиода: он должен загораться при появлении движения в направлении и не быть активным если движение происходит в тех зонах, которые он не должен контролировать. Это наиболее удобно

делать при подключенных извещателях к приемно-контрольной панели, когда панель включена, но не находится в режиме охраны.

6. Включить приемно-контрольную панель в режим охраны и продемонстрировать работу системы сигнализации преподавателю.

### **Вариант 2.**

1. Подключить датчики к ПКП таким образом, чтобы реализовать следующую тактику работы системы сигнализации:

- зона 1 служит для контроля входной двери, при этом должен обеспечиваться временной интервал для выхода из помещения после постановки системы на охрану и временной интервал для снятия системы с охраны после входа в помещение. Временные интервалы необходимые для выхода и входа определить экспериментально;
- зона 2 обеспечивает круглосуточную охрану в зоне окна независимо от того находится система сигнализации в режиме охраны или нет;
- зона 3 обеспечивает мгновенное формирование сигнала тревоги при появлении движения в помещении под верхним этажом, если система сигнализации находится в режиме охраны. Движение вдоль прохода в данное помещение не должно вызывать срабатывание извещателя;
- зона 4. При появлении движения в верхнем помещении система должна формировать сигнал предупреждения, не включая основную сирену. В качестве сигнала предупреждения используется звук динамика клавиатуры;

- зона 5 обеспечивает пожарную безопасность.

2. Подключить сирену. Драйвер сирены ПКП должен работать в режиме «Выход постоянного тока». При постановке на охрану должен формироваться короткий звуковой сигнал сирены.

*Примечание:* при соединении внешних элементов системы сигнализации с ПКП необходимо устанавливать дополнительные резисторы в соответствии с инструкцией на ПКП.

3. Включить ПКП:

- войти в режим программирования текущей даты и времени. Установить время и дату.
- войти в режим программирования параметров ПКП и ввести данные, обеспечивающие выполнение тактики работы системы сигнализации, которая была описана выше. Характер реакции системы на срабатывания датчика 4 («Рефлекс») отсутствует среди заводских установок. Для реализации необходимого режима работы необходимо перепрограммировать одну из стандартных заводских установок, которая не используется в данной системе. Например, группа функций зон №7.

*Примечание:* при постановке на охрану и вход в режим программирования использовать коды, установленные по умолчанию (заводские установки). При этом вход в режим программирования даты и времени осуществляется при использовании кода постановки на охрану, а для входа в режим программирования основной код.

Продемонстрировать работу системы охраны.

### **7. Контрольные вопросы:**

1. Какие датчики входят в группу пожарных датчиков?
2. Описать какие бывают дымовые датчики, их конструкция и принцип действия?
3. Описать какие бывают тепловые датчики, их конструкция и принцип действия?
4. Принцип действия датчиков пламени. Объекты, на которых применение данных датчиков наиболее эффективно?
5. Принцип действия газовых датчиков?
6. Чем отличаются комбинированные датчики и их основное преимущество?
7. Какие датчики входят в группу охранных датчиков для закрытых помещений?
8. Какие функции выполняют датчики состояния предметов интерьера и контролируемой поверхности?
9. Структурная схема датчика разбития стекла. Какие параметры анализируются для принятия решения о формировании сигнала тревоги?
10. Где применяются датчики, контролирующие состояние дверей и стен. Их принципы действия?
11. Датчик обнаружения движущегося теплового пятна. Блок – схема и принцип действия?
12. Чем различаются между собой различные датчики обнаружения движущегося теплового пятна?
13. Датчики изменения внутреннего объема?
14. Классификация приемно-контрольных панелей?
15. Способы передачи информации между датчиками и приемно-контрольными панелями?
16. Как обеспечивается контроль целостности канала передачи данных для охранных и пожарных датчиков?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** Новосибирский государственный технический университет, кафедра защиты информации, старший преподаватель Быков Сергей Владимирович, к.т.н., доцент, декан АВТФ Рева Иван Леонидович, эл. почта: reva@corp.nstu.ru, s.bykov@corp.nstu.ru

## **Дисциплина: Управление средствами защиты информации**

**Образовательная программа:** 10.05.03. – Информационная безопасность автоматизированных систем, Информационная безопасность автоматизированных банковских систем.

**Дисциплина:** Управление средствами защиты информации.

### **Лабораторная работа.**

#### **Secret Net. Замкнутая программная среда. Контроль целостности**

##### **1. Учебные цели:**

Изучение и приобретение навыков настройки и управления обеспечением замкнутой программной среды и контролем целостности файлов.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- Умеет конфигурировать средства защиты информации систем управления базами данных.
- Умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах.

##### **3. Перечень материально-технического обеспечения:**

- Secret Net версии 7.2 и выше

##### **4. Задание на исследование**

- Прodelайте ход работы, выполните задания по варианту и зафиксируйте полученные результаты в отчете.
- Создайте замкнутую программную среду в «жестком режиме» для ресурса, заданного по варианту, для созданной учетной записи пользователя.
- Настройте контроль целостности для ресурса, заданного по варианту. Попробуйте подменить содержащийся в данной папке исполняемый файл другим файлом. Проверьте работу механизма контроля целостности.

##### **5. Краткие теоретические сведения**

Механизм контроля целостности (КЦ) предназначен для слежения за неизменностью содержимого ресурсов компьютера. Действие этого механизма основано на сравнении текущих значений контролируемых параметров проверяемых ресурсов и значений, принятых за эталон. Эталонные значения контролируемых параметров определяются или рассчитываются при настройке механизма. В процессе контроля при обнаружении несоответствия текущих и эталонных значений система оповещает администратора о нарушении целостности ресурсов и выполняет заданное при настройке действие, например, блокирует компьютер, на котором нарушение обнаружено.

Механизм замкнутой программной среды (ЗПС) предназначен для ограничения использования ПО на компьютере. Доступ разрешается только к тем программам, которые необходимы пользователям для работы. Для каждого пользователя определяется перечень ресурсов, в который входят разрешенные для запуска программы, библиотеки и сценарии. Попытки запуска других ресурсов блокируются, и в журнале безопасности регистрируются события несанкционированного доступа (НСД).

##### **6. Порядок выполнения лабораторной работы (этапы)**

Войдите под учетной записью Администратор. Для запуска программы необходимо выбрать следующую команду «Пуск \Все программы \Код Безопасности \SecretNet \Контроль программ и данных».

Перед тем как произвести построение фрагмента модели данных системой проводится анализ размещения программного обеспечения и данных на защищаемом компьютере, формируются требования к настройке контроля целостности и замкнутой программной среды, который включает в себя:

- сведения о защищаемом компьютере (установленное ПО, пользователи и их функциональные обязанности, задачи, решаемые пользователями в рамках бизнес-процессов);
- перечень ресурсов, подлежащих контролю целостности;
- перечень программ, с которыми разрешено работать разным группам пользователей;
- задачи (список задач и их краткое описание).

Для построения фрагментов модели данных в программе КЦ-ЗПС выбираем команду «Файл \ Новая модель данных». В ней предоставляется возможность детальной настройки параметров для формирования новой модели данных. Нажмите ОК для создания стандартной модели (для тех файлов, где появятся ошибки выберите вариант снять с контроля). В эту модель можно добавить файлы операционной системы и Secret Net



для контроля их целостности и создания ЗПС. Помимо стандартных задач, в модель можно добавить задачи, сформированные на основе ресурсов приложений. Добавление таких задач осуществляется с помощью параметра «Добавить другие задачи из списка». После успешного формирования модели данных в основном окне программы управления КЦ-ЗПС появится новая структура, включающая в себя субъект «Компьютер» с назначенными для него заданиями.

После того, как произойдет подготовка ресурсов для использования замкнутой программной среды, в левой части окна выберите категорию «Задания» и выберите в меню «Задания \Создать задание». На экране появится диалог выбора типа задания. Выбираем «Замкнутая программная среда» и нажимаем на кнопку «ОК». Затем введите имя задания и продолжите работу, нажав на кнопку «ОК».

После чего, новое задание будет отображаться в окне структуры.

Выделите созданное задание на ЗПС. Открыв правой кнопкой мыши контекстное меню выберите «Добавить задачи \группы-Новую группу по каталогу...». В окне выбора добавьте каталог «C:\Program Files \Movie Maker» и нажмите «ОК». На панели категорий выберите «Субъекты управления» и нажмите «Добавить в список». Введите имя выбираемого объекта «user» и нажмите «ОК».

Выделите добавленного пользователя. В меню выберите «XP-MSDN\user> Добавить задания> Существующие...», в открывшемся окне выберите «Новое задание на ЗПС» и нажмите «ОК». Теперь пользователь user выбранный каталог будет входить в ЗПС, а, следовательно, программы, находящиеся в каталоге будут разрешены к запуску. Для того, чтобы ЗПС функционировала необходимо включить «Жесткий режим». Для этого необходимо выполнить следующее:

- выбрать категорию «Субъекты управления» на панели категорий;
- выбрать в дополнительном окне структуры группу «XP-MSDN», вызовите контекстное меню и выберите команду «Свойства». В появившемся окне перейдите к вкладке «Режимы»;
- установите отметку в поле «Режим ЗПС включен» и удалите отметку в поле «Мягкий режим».

После проделанных действий замкнутая программная среда будет работать в «Жестком режиме». То есть будут разрешены для запуска только те программы, которые добавлены в задания на ЗПС. На учетную запись «Администратор» ЗПС не действует, так как в групповых политиках была задана данная привилегия.

Закройте программу, сохранив модель. Войдите под учетной записью «user». Попробуйте поработать в операционной системе, результаты зафиксируйте в отчете. Интерфейс Windows должен отображаться некорректно, так как не все файлы, нужные для корректной работы системы были добавлены в ЗПС. Для того чтобы это исправить необходимо обучить модель в «мягком» режиме.

Войдите под учетной записью «Администратор» и включите «мягкий» режим работы ЗПС (как в п. 11). Сохраните модель. Войдите под учетной записью user и запустите Movie Maker («C:\Program Files\Movie Maker\moviemk.exe»). Теперь все необходимые для корректной работы программы будут записаны в журнал Secret Net.

Войдите под учетной записью Администратор и добавьте в задание на ЗПС файлы из журнала Secret Net: под учетной записью Администратор откройте Контроль программ и данных, выберите Файл-Новая модель данных, задав режим ЗПС с добавлением группы ресурсов по журналу Secret Net. В этом случае Secret Net разрешит запускаться программам, записи о попытках запуска которых отмечены журналах Secret Net. Файлы без ЭЦП игнорировать. Далее включите жесткий режим ЗПС (как в п.11) и сохраните модель.

Войдите под учетной записью user. Запустите программу Windows Movie Maker и убедитесь в возможности ее запуска.

Запустите Windows Media Player («C:\Program Files\Windows Media Player\wmplayer.exe»). Попробуйте запустить другие программы. Результаты зафиксируйте в отчете.

#### Настройка контроля целостности

Контроль целостности настраивается для тех файлов, для которых критична их неизменность. Сюда могут входить исполняемые файлы и библиотеки операционной системы и другие важные файлы.

Войдите под учетной записью «Администратор». Запустите программу «Пуск \Все программы\Код Безопасности\Secret Net\Контроль программ и данных». Выберите категорию «Задания» и выберите в меню «Задания \Создать задание». На экране появится диалог выбора типа задания. Выбираем «Контроль целостности» и нажимаем на кнопку «ОК».

После того, как выбран тип «Контроль целостности», появится окно «Создание нового задания на КЦ». В данном окне задайте имя «Новое задание на КЦ». В методе контроля ресурсов выберите «Содержимое», а для параметра «Реакция на отказ» выставить значение «Заблокировать компьютер». Ниже приведены описания методов контроля и то, что будет проверяться.

#### Методы контроля:

- Содержимое. Проверяется целостность содержимого ресурсов.
- Атрибуты. Проверяются стандартные атрибуты, установленные для ресурсов.
- Права доступа. Проверяются категории конфиденциальности, установленные для ресурсов.
- Существование. Проверяется наличие ресурсов по заданному пути.

Перейдите к вкладке «Расписание». Во вкладке «Расписание» выберите поля «При загрузке ОС», «При входе». Также можно настроить по каким дням и месяцам будет выполняться контроль целостности. Для этого установите КЦ с июня по декабрь и с понедельника по воскресенье и нажмите кнопку «ОК».

Необходимо задать контроль целостности для данного компьютера. Для этого перейдите к вкладке «Субъекты управления», выберите «XP-MSDN» и вызовите контекстное меню и добавьте задание «Новое задание на КЦ». Перейдите к категории «Задания», вызовите контекстное меню нового задания на КЦ и добавьте ресурс по каталогу «D:\Документы». Произведите расчет эталонов для файлов, заданных на контроль целостности: В контекстном меню «Нового задания на КЦ» – Расчет эталонов (или Сервис – Эталоны – Расчет, если нужно рассчитать все эталоны). Установите галочку оставлять старые и нажмите ОК. Сохраните изменения, выбрав в меню «Файл» – «Сохранить». Зайдите под учетной записью «conf» и измените содержимое файла «Конф.txt» в папке «Документы» находящейся на диске «D:\». Попробуйте заново войти в систему под учетной записью «conf». Результаты зафиксируйте в отчете.

#### **7. Контрольные вопросы:**

1. Для чего предназначен механизм контроля подключения и изменения устройств?
2. Для каких устройств реализован механизм контроля подключения и изменения?
3. Для чего предназначен механизм контроля целостности (КЦ)?
4. Для чего предназначен механизм замкнутой программной среды?
5. Чем отличается «мягкий» режим ЗПС от «жесткого»?
6. Перечислите методы контроля целостности, используемые Secret Net.
7. Перечислите реакции на нарушение целостности файлов.
8. Для каких файлов следует настраивать контроль целостности?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** Томский государственный университет систем управления и радиоэлектроники (ТУСУР), Рахманенко Иван Андреевич, [ria@keva.tusur.ru](mailto:ria@keva.tusur.ru)

## **Дисциплина: Управление информационной безопасностью**

**Образовательная программа:** 10.05.03 – Информационная безопасность автоматизированных систем, Защищённые автоматизированные системы управления.

**Дисциплина:** Управление информационной безопасностью.

### **Лабораторная работа.**

#### **Исследование требований нормативных документов по защите информации к стойкости парольной защиты**

##### **1. Учебные цели:**

Изучить структуру, содержание и составить краткую характеристику нормативных документов ФСТЭК, представленных преподавателем. Изучить особенности построения требований к стойкости парольной защиты документа Методические рекомендации ФСТЭК «Меры защиты информации в государственных информационных системах».

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

###### **Уметь:**

- разрабатывать, реализовывать, оценивать и корректировать основные процессы управления информационной безопасностью.

###### **Владеть:**

- навыками разрабатывать предложения по совершенствованию процессов управления информационной безопасностью защищенных автоматизированных систем.

##### **3. Перечень материально-технического обеспечения**

**Лабораторное оборудование и программное обеспечение:** Персональные компьютеры (из расчета – один компьютер на одного человека) с полным пакетом офисных программ.

##### **4. Задание на исследование.**

1. Изучить структуру документа Методические рекомендации ФСТЭК к Приказу № 17 «Меры защиты информации в государственных информационных системах».
2. Изучить подробно раздел ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации. Требования к реализации ИАФ.4.
3. Из раздела Требование к усилению ИАФ.4 определить параметры систем аутентификации для расчета вероятности защиты информации и времени взлома парольной защиты ГИС классов 1,2,3, принятые в Методическом документе ФСТЭК от 11.02 .2014 г. при ручном и подборе и в автоматическом режиме. Составить таблицы зависимости вероятности защиты паролем от параметров – мощность алфавита (строки) и длина пароля (столбцы) – для четырех классов защиты.
4. Изучить теоретический материал по стойкости парольной аутентификации (формуле Андерсона).

##### **5. Краткие теоретические сведения.**

Система парольной аутентификации как неотъемлемая составляющая подсистемы управления доступом системы защиты информации (СЗИ) является частью "переднего края обороны" всей системы безопасности. Поэтому парольная система становится одним из первых объектов атаки при вторжении нарушителя в защищенную систему. Подсистема управления доступом СЗИ затрагивает следующие понятия:

Идентификатор доступа – уникальный признак субъекта или объекта доступа. Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов. Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Можно встретить и такие толкования терминов идентификатор и пароль пользователя:

Идентификатор – некоторое уникальное количество информации, позволяющее различать конкретных пользователей парольной системы (проводить их идентификацию). Идентификатор называют именем учетной записи пользователя.

Пароль – некоторое секретное количество информации, известное только пользователю и парольной системе, предъявляемое для прохождения процедуры аутентификации. Учетная запись – совокупность идентификатора и пароля пользователя. Одним из наиболее важных компонентов парольной системы является

база данных учетных записей (база данных системы защиты). Возможны следующие варианты хранения паролей в системе: в открытом виде; в виде хэш-значений; зашифрованными на некотором ключе.

Наибольший интерес представляют второй и третий способы, которые имеют ряд особенностей. Хэширование не обеспечивает защиту от подбора паролей по словарю в случае получения базы данных злоумышленником. При выборе алгоритма хэширования, который будет использован для вычисления хэш-значений паролей, необходимо гарантировать несовпадение хэш-значений, полученных на основе различных паролей пользователей. Кроме того, следует предусмотреть механизм, обеспечивающий уникальность хэш-значений в том случае, если два пользователя выбирают одинаковые пароли. Для этого при вычислении хэш-значения обычно используют некоторое количество "случайной" информации, например, выдаваемой генератором псевдослучайных чисел. При шифровании паролей особое значение имеет способ генерации и хранения ключа шифрования базы данных учетных записей.

Возможны следующие варианты: ключ генерируется программно и хранится в системе, обеспечивая возможность ее автоматической перезагрузки; ключ генерируется программно и хранится на внешнем носителе, с которого считывается при каждом запуске; ключ генерируется на основе выбранного администратором пароля, который вводится в систему при каждом запуске. Наиболее безопасное хранение паролей обеспечивается при их хэшировании и последующем шифровании полученных хэш-значений, т.е. при комбинации второго и третьего способов хранения паролей в системе.

Стойкость парольной системы определяется ее способностью противостоять атаке злоумышленника, завладевшего базой данных учетных записей и пытающегося восстановить пароли, и зависит от скорости "максимально быстрой" реализации используемого алгоритма хэширования.

Восстановление паролей заключается в вычислении хэш-значений по возможным паролям и сравнении их с имеющимися хэш-значениями паролей. Из базы данных учетных записей пароль может быть восстановлен различными способами: атакой по словарю, последовательным (полным) перебором и гибридом атаки по словарю и последовательного перебора.

Последовательный перебор всех возможных комбинаций (brute force) – грубая сила, решение "в лоб" – использует набор символов и вычисляет хэш-значение для каждого возможного пароля, составленного из этих символов. При использовании этого метода пароль всегда будет определен, если составляющие его символы присутствуют в выбранном наборе. Недостаток этого метода – большое количество времени, которое может потребоваться на определение пароля. Чем большее количество символов (букв разного регистра, цифр, спецсимволов) содержится в выбранном наборе, тем больше времени пройдет, пока перебор не закончится.

Повышение требований к паролю возникает из-за степени его важности. Примером "важного пароля" служит пароль, применяемый для работы в автоматизированных системах, обрабатывающих информацию ограниченного доступа (государственная тайна, конфиденциальная информация). Руководящие документы дают конкретные рекомендации по выбору пароля (но не расчету его стойкости).

Существуют методы количественной оценки стойкости парольных систем (формула Андерсона):

$$4,32 \times 10^4 \times (k) \frac{M}{P} \leq A^l,$$

где  $k$  – количество попыток подбора пароля в минуту;  $M$  – время действия пароля в месяцах;  $P$  – вероятность подбора пароля;  $A^l$  – мощность пространства паролей ( $A$  – мощность алфавита паролей,  $l$  – длина пароля).

Таким образом, наибольшее влияние на вероятность раскрытия пароля оказывает величина  $l$ . Другие составляющие данной формулы меньше оказывают влияние на величину  $P$ . Увеличение же длины пароля только на один символ значительно увеличивает требуемое злоумышленнику время для его раскрытия.

Параметры  $P$ ,  $V$ ,  $T$ ,  $A$  и  $l$  связаны между собой следующим соотношением:

$$P = \frac{V \times T}{A^l},$$

где  $P$  – вероятность подбора пароля в течение его срока действия (подбор осуществляется непрерывно в течение всего срока действия пароля);  $V$  – скорость подбора паролей (скорость обработки одной попытки регистрации проверяющей стороной либо скорость вычисления хэш-значения одного пробного пароля);  $T$  – срок действия пароля (задает промежуток времени, по истечении которого пароль должен быть сменен);  $A^l$  – мощность пространства паролей ( $A$  – мощность алфавита паролей,  $l$  – длина пароля).

В случае, когда неизвестна точная длина искомого пароля, максимальное время подбора пароля ( $T_{\max}$ ) будет вычисляться в соответствии со следующей формулой:

$$T_{\max} = \frac{A^l}{V}.$$

Требование к усилению аутентификации (ИАФ.4) по Методическому документу ФСТЭК для разных классов защиты должны быть следующими:

а) длина пароля не менее шести символов, алфавит пароля не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут, смена паролей не более чем через 180 дней;

б) длина пароля не менее шести символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут, смена паролей не более чем через 120 дней;

в) длина пароля не менее шести символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 8 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 10 до 30 минут, смена паролей не более чем через 90 дней;

г) длина пароля не менее восьми символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 4 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 15 до 60 минут, смена паролей не более чем через 60 дней;

## 6. Порядок выполнения лабораторной работы (этапы)

Этап 1. Рассчитать в таблице EXEL вероятности защиты информации для парольной защиты в государственных информационных системах (ГИС) классов 1,2,3, принятые в методическом документе ФСТЭК «Меры защиты информации в государственных информационных системах» от 11.02 .2014 г. при ручном подборе и в автоматическом режиме. Заполнить таблицу в отчете.

Этап 2. Рассчитать в таблице EXEL время, необходимое на гарантированный взлом защиты для паролей ГИС классов 1,2,3, принятые в методическом документе ФСТЭК.

**Таблица 1** – Время взлома пароля

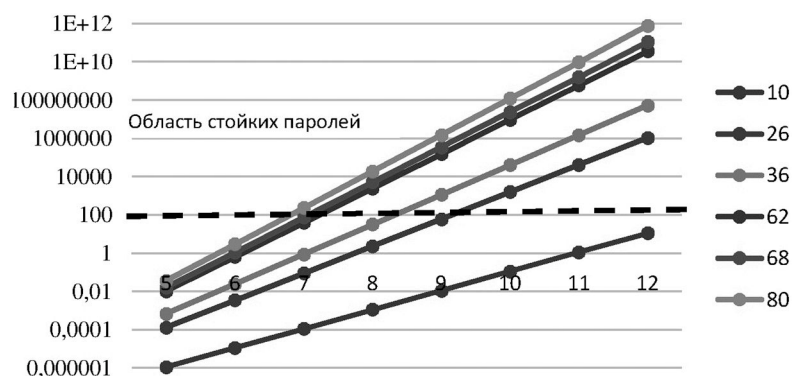
| Алфавит/длина                                     | 5<br>СИМВОЛОВ | 6<br>СИМВОЛОВ | .... | 12<br>СИМВОЛОВ |
|---------------------------------------------------|---------------|---------------|------|----------------|
| 10 (только цифры)                                 |               |               |      |                |
| 36 (латинские буквы одного регистра + цифры)      |               |               |      |                |
| 52 (латинский алфавит со смешанным регистром)     |               |               |      |                |
| 62 (латинский алфавит + цифры)                    |               |               |      |                |
| 68 (латинский алфавит + цифры + знаки препинания) |               |               |      |                |
| 80 (латинский алфавит + цифры + печатные символы) |               |               |      |                |

Этап 3. Определить теоретическую стойкость паролей от 5 до 12 символов при мощности алфавита в 10, 26, 36, 62, 68, 80 символов. Построить график зависимости времени взлома  $T_{max}$  от длины пароля для различных параметров пароля (мощности алфавита). Использовать для времени логарифмическую шкалу.

Пример: в таблице 2 отражены данные по максимальному времени взлома пароля для различных комбинаций длины пароля и мощности алфавита при условии средней квалификации нарушителя.

**Таблица 2** – Максимальное время взлома паролей для среднеквалифицированного нарушителя

| ЛА | 10          | 26       | 36       | 62       | 68       | 80       |
|----|-------------|----------|----------|----------|----------|----------|
| 5  | 1,15741E-06 | 0,000138 | 0,0007   | 0,010603 | 0,016828 | 0,037926 |
| 6  | 1,15741E-05 | 0,003575 | 0,025194 | 0,65741  | 1,1443   | 3,034074 |
| 7  | 0,000115741 | 0,092961 | 0,906993 | 40,75943 | 77,81237 | 242,7259 |
| 8  | 0,001157407 | 2,41698  | 32,65174 | 2527,085 | 5291,241 | 19418,07 |
| 9  | 0,011574074 | 62,84148 | 1175,462 | 156679,2 | 359804,4 | 1553446  |
| 10 | 0,115740741 | 1633,878 | 42316,65 | 9714113  | 24466699 | 1,24E+08 |
| 11 | 1,157407407 | 42480,84 | 1523399  | 6,02E+08 | 1,66E+09 | 9,94E+09 |
| 12 | 11,57407407 | 1104502  | 54842377 | 3,73E+10 | 1,13E+11 | 7,95E+11 |



**График 1** – Область стойких паролей для среднеквалифицированного нарушителя

Этап 4. Сделать выводы. Сравнить полученные теоретические результаты с цифрами, полученными из методического документа. Указать область стойких паролей. Представить отчет преподавателю.

Отчет должен содержать:

- Разработанные формулы в таблице EXEL и реализованные значения вероятности защиты информации для парольной защиты в ГИС классов 1,2,3.
- Графики зависимости времени взлома от длины пароля для различных параметров пароля. Указать на графике область стойких паролей.
- Выводы по результатам проверки стойкости ко взлому установленных парольных комбинаций пользователей и их соответствие установленным требованиям по безопасности в Методических рекомендациях ФСТЭК.

#### **7. Контрольные вопросы:**

1. Как компенсируются недостатки парольного способа аутентификации.
2. Перечислить параметры парольной аутентификации и требования к ним для разных классов информационных систем.
3. Какие значения вероятностей угроз «подбора пароля» приняты в нормативном документе ФСТЭК.
4. Какие значения параметра «время полного перебора пароля» приняты в нормативном документе ФСТЭК для разных классов защиты.

**Время на выполнение лабораторной работы** – 4 часа.

**Образовательная организация, авторы, эл. почта:** ФГБОУ ВПО «Кубанский государственный технологический университет», к.т.н., профессор В.Н. Хализев, ha53@mail.ru

## Дисциплина: Языки программирования

**Образовательная программа:** 10.05.03 Информационная безопасность автоматизированных систем, Информационная безопасность автоматизированных систем критически важных объектов

**Дисциплина:** Языки программирования

### **Лабораторная работа. Подготовка и решение на ЭВМ задач, реализуемых многомодульными структурами**

#### **1. Учебные цели:**

- Закрепить практические навыки разработки программ с использованием модулей.
- Овладеть приемами составления модулей.
- Уяснить применимость изученных средств при решении практических задач.
- Закрепить навыки работы в среде визуального программирования.

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- **Уметь** разрабатывать пользовательские модули и обращаться к ним в приложениях с использованием возможностей среды программирования.
- **Владеть** средствами языка программирования по разработке подпрограмм, объединению их в модули в среде визуального объектно-ориентированного программирования

#### **3. Перечень материально-технического обеспечения**

- Сеть персональных ЭВМ.

#### **4. Задание на исследование**

Разработать подпрограммы, обеспечивающие выполнение функций, приведенных в таблице 1, и оформить подпрограммы в виде модуля.

Разработать проект, использующий все подпрограммы разработанного модуля для проведения расчетов при произвольно выбранных исходных данных. Для разработки приложения использовать компонент «набор вкладок» (PageControl), он находится на вкладке Win32. Кнопки с рисунком –BitBtn, этот компонент находится на вкладке Additional и позволяет отображать на нем не только надпись, но и рисунок (пиктограмму). Компонент OleContainer предназначен для размещения, связанного или внедренного OLE-объекта (Object Linked or Embedding – связывание или внедрение объекта). Компонент находится на вкладке System. Компонент Image, этот компонент находится на вкладке Additional и служит для размещения на форме одного из трех поддерживаемых Delphi типов изображений: растровой картинки, пиктограммы или метафайла. Для изменения изображений использовать встроенный редактор изображений Image Editor, интерфейс которого практически идентичен стандартному редактору Paint.

Массивы заполнять с помощью датчика случайных чисел. Предлагается 30 вариантов. Пример реализации одного и з вариантов представлен ниже.

#### **5. Краткие теоретические сведения**

Структура модуля

Модуль имеет следующую структуру:

Unit имя;

interface

интерфейсная часть

implementation

реализационная часть

initialization

иницилирующая часть

finalization

завершающая часть

End.

#### **6. Порядок выполнения лабораторной работы**

Разработать подпрограммы, обеспечивающие выполнение следующих функций:

12. определение в матрице минимального и максимального элементов;
13. вычисление суммы и произведения отрицательных элементов одномерного массива;
14. вычисление значения функции  $y = \sum_{i=1}^n \frac{x}{i}$ ;
15. определение площади прямоугольного треугольника по его катетам.

Оформить подпрограммы в виде модуля. Разработать проект, использующий все подпрограммы разработанного модуля для проведения расчетов при произвольно выбранных исходных данных. Окно приложения оформляется в виде набора вкладок:

### Вкладка 1.

Обработчик события кнопки:

```

procedure TForm1.BitBtn1Click(Sender: TObject);
var i,j,n,m:integer; a:matr; s,s1:string; min,max:real;
begin
n:=strtoint(edit3.Text);
m:=strtoint(edit4.Text);
setlength(a,n,m);
randomize;
for i:=0 to n-1 do begin s:="";
for j:=0 to m-1 do begin a[i,j]:=random(20); str(a[i,j]:6:2,s1); s:=s+s1; end;
listbox1.Items.Add(s); end;
aminmax(a,n,m,min,max);
edit1.Text:=floattostr(min);
edit2.Text:=floattostr(max);
end;

```

### Вкладка 2.

Обработчик события «нажатие кнопки»:

```

procedure TForm1.BitBtn2Click(Sender: TObject);
var a:mas; i,n,k:integer; s,p:integer;
begin
n:=strtoint(edit5.text);
setlength(a,n);

```

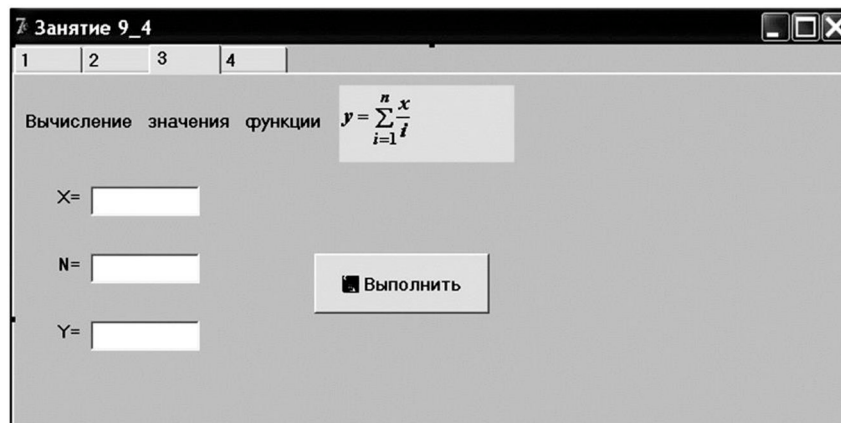


```

randomize;
for i:=0 to n-1 do begin
a[i]:=random(20)-5; listbox2.items.Add(inttostr(a[i]));
end;
otric(a,n,s,p,k);
if k=0 then label10.Caption:='отрицательных нет'
else begin
edit6.Text:=inttostr(s);
edit7.Text:=inttostr(p); end;
end;

```

### Вкладка 3.

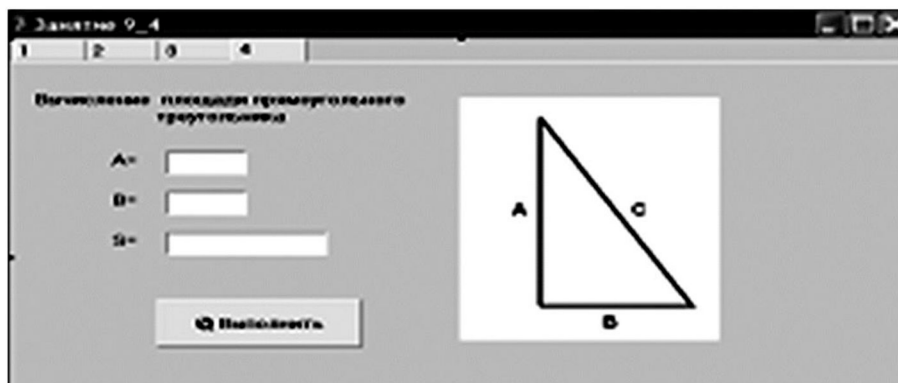


```

Обработчик события «нажатие кнопки»:
procedure TForm1.BitBtn3Click(Sender: TObject);
var x:real; n:integer;
begin
x:=strtofloat(edit8.Text);
n:=strtoint(edit9.Text);
edit10.Text:=floattostrf(sr(x,n),ffixed,8,3);
end;

```

### Вкладка 4.



```

Обработчик события «нажатие кнопки»:
procedure TForm1.BitBtn4Click(Sender: TObject);
var a,b:real;
begin
a:=strtofloat(edit11.Text); b:=strtofloat(edit12.Text);
edit13.Text:=floattostr(sptreyg(a,b));
end;

```

```

Модуль общего назначения
unit Unit2;
interface
type matr=array of array of real; mas=array of integer;
procedure aminmax (a:matr;n,m:integer; var min,max:real);
procedure otric (a:mas; n:integer; var sum, pros:integer; var k:integer);
function Sr(x:real; n:integer):real;
function sptreyg(a,b:real):real;
implementation

procedure aminmax (a:matr;n,m:integer; var min,max:real);
var i,j:integer;
begin
min:=a[0,0]; max:=a[0,0];
for i:=0 to n-1 do
for j:=0 to m-1 do
begin
if a[i,j]<min then min:=a[i,j]; if a[i,j]>max then max:=a[i,j];
end;
end;
procedure otric (a:mas; n:integer; var sum, pros:integer; var k:integer);
var i:integer;
begin
k:=0; sum:=0; pros:=1;
for i:=0 to n-1 do
if a[i]<0 then begin sum:=sum+a[i]; pros:=pros*a[i]; k:=k+1; end;
end;
function Sr(x:real; n:integer):real;
var i:integer;
begin
result:=0; for i:=1 to n do result:=result+x/i;
end;
function sptreyg(a,b:real):real;
begin result:=a*b/2; end;
end.

```

## 7. Контрольные вопросы

1. Какие виды модулей имеются в системе программирования Delphi?
2. Как подключить другие модули в пользовательском модуле?
3. Какие модули подключаются автоматически к любому приложению?
4. Какие особенности реализационной части модуля?
5. Для каких целей предназначена интерфейсная часть модуля?
6. Как в Delphi осуществляется связь между формами и создается многооконное приложение?

**Время на выполнение лабораторной работы – 2 часа.**

**Образовательная организация, авторы, эл. почта:** ВУНЦ ВВС «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж) Афанасьевский Леонид Борисович, afleonid@yandex; Будников Сергей Алексеевич, buser@bk.ru; Горин Александр Николаевич, algorin.algoral@mail.ru

**СПЕЦИАЛИТЕТ 10.05.04**  
**ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ**

**Дисциплина: Безопасность операционных систем**

**Образовательная программа:** 10.05.04 – Информационно-аналитические системы безопасности, Информационная безопасность финансовых и экономических структур

**Дисциплина:** Безопасность операционных систем

**Лабораторная работа.**  
**Разграничение доступа к устройствам**

**1. Учебные цели:**

Изучить возможности разграничения доступа к устройствам.

**2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

**Уметь:**

- контролировать доступ пользователей к дисководам, CD/DVD – приводам, другим сменным устройствам, адаптерам WiFi и Bluetooth, а также к USB, FireWire, инфракрасным, COM и LPT-портам.

**Владеть:**

- навыками проведения контроля доступ пользователей к дисководам, CD/DVD – приводам, другим сменным устройствам, адаптерам WiFi и Bluetooth, а также к USB, FireWire, инфракрасным, COM и LPT-портам.

**3. Перечень материально-технического обеспечения**

**Лабораторное оборудование и программное обеспечение:** Microsoft Windows 10, VirtualBox, DeviceLock Management Console.

**4. Задание на исследование**

Учётной записи «user» установите разрешения для устройств в соответствии с вариантом.

Пример варианта

| Съёмные устройства  | USB-порт           | WIFI             |
|---------------------|--------------------|------------------|
| Чтение и извлечение | Аудит всех событий | Доступ по будням |

**5. Краткие теоретические сведения:**

Контроль доступа может выполняться на двух уровнях: уровне интерфейса (порта) и уровне типа (съёмное устройство, принтеры, жёсткие диски и т.д.). Некоторые устройства проверяются на обоих уровнях, в то время как другие – только на одном: либо на уровне интерфейса (порта), либо на уровне типа.

**6. Порядок выполнения лабораторной работы**

Подключите консоль «DeviceLock Management Console» к управляемому компьютеру. Для этого в контекстном меню «Сервис DeviceLock» выберите «Подключиться...». Дополнительно включите настройку «Подключаться к локальному компьютеру при запуске» для автоматического подключения сервиса.

Перейдите во вкладку «Настройка сервиса – Администраторы DeviceLock». Добавьте в качестве администратора DeviceLock учётную запись «Администратор». В данной вкладке можно добавить и других пользователей с возможностью ограничения доступа к оснастке (полный доступ, изменение, только чтение). Пользователи, не внесённые в список, не будут иметь доступ к оснастке управления разграничением доступа к устройствам.

Когда пользователь пытается получить доступ к устройству, DeviceLock перехватывает запрос на уровне ядра ОС. В зависимости от типа устройства и интерфейса подключения (например, USB), DeviceLock проверяет права пользователя в соответствующем списке управления доступом (ACL). Если у пользователя отсутствуют права доступа к данному устройству, будет возвращено сообщение об ошибке – «доступ запрещён».

Перейдите в раздел «Устройства – Разрешения». Запретите доступ учётной записи «user» к приводу DVD/CD-ROM. Если на ПК установлено несколько CD/DVD- приводов, то можно воспользоваться белым листом устройств, для того чтобы выбрать определённый носитель.

Примечания:

- если пользователь входит в какую-либо группу и у этой группы стоит полный доступ к устройству, то режим только чтение не будет работать (это связано с тем, что разрешения суммируются);
- если учётную запись не добавить в разрешения, то доступ ей будет запрещён.

DeviceLock предоставляет возможность разграничения доступа к устройствам по дням недели и времени суток. Установите пользователю «user» полный доступ к съёмным устройствам в будние дни с 8:00 до 17:00 либо на время занятий (рис. 1).

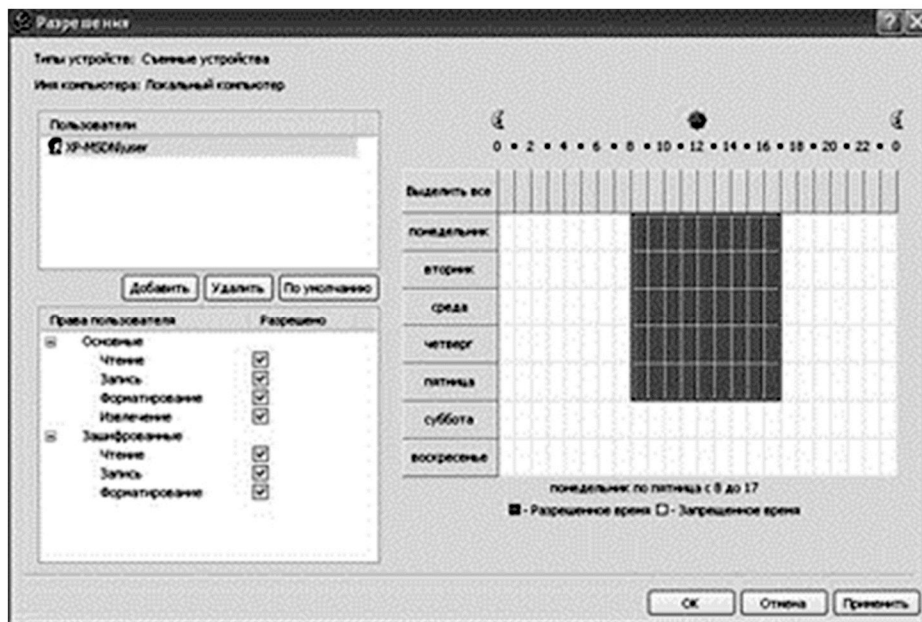


Рис. 1. Разграничения доступа к устройствам по дням недели и времени суток

Войдите под учётной записью «user». Подключите съёмный носитель и убедитесь, что доступ к нему разрешён.

Под учётной записью «Администратор» измените системное время на воскресенье.

В случае с USB-устройствами DeviceLock в первую очередь проверит разрешения на уровне интерфейса (USB-порта), открыт или нет доступ к USB-порту. Затем, поскольку «Windows» определяет USB-флэш как съёмное устройство, DeviceLock также проверит ограничения на уровне типа устройства (съёмное устройство). Под учётной записью «user» проверьте запрет доступа к съёмному носителю.

Так как разграничению доступа подвергаются все USB-устройства, возникает необходимость делать исключения для USB-устройств, разрешённых к использованию в организации.

Исключения можно указывать двумя способами:

- через «Настройки безопасности» (рис. 2);
- через «Белый список» на основе идентификации модели или конкретного экземпляра устройства.

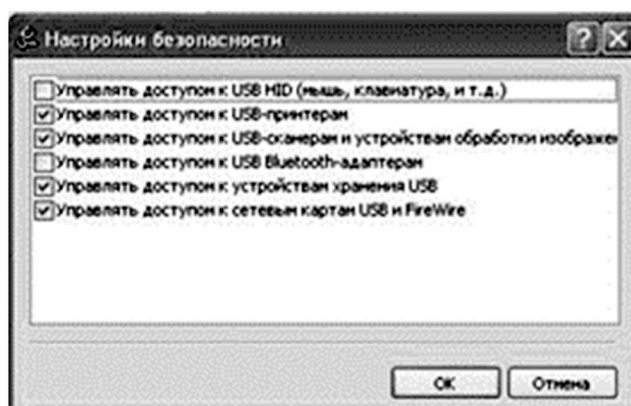


Рис. 2. Настройки безопасности

Если в «Настройках безопасности» включить настройки управления каким-либо классом устройств, то к устройствам этого класса применяется разграничение доступа. Если настройка отключена, то использовать устройства данного класса могут все пользователи.

При использовании белого списка есть два варианта идентификации устройств:

1. Device Model – описывает все устройства одной и той же модели. Каждое устройство идентифицируется по комбинации идентификатора производителя (VID) и продукта (PID).

Комбинация VID и PID описывает конкретную модель, но не конкретное устройство. Это значит, что все устройства данной модели данного производителя будут распознаны как одно устройство.

2. Unique Device – описывает конкретное уникальное устройство. Каждое устройство идентифицируется по комбинации идентификатора производителя (VID), продукта (PID) и серийного номера.

Устройство может быть добавлено в белый список как уникальное устройство только в том случае, если производитель присвоил ему серийный номер на этапе изготовления.

Кроме функции контроля доступа, DeviceLock позволяет осуществлять протоколирование и аудит использования устройств пользователями на локальном компьютере.

Чтобы включить протоколирование действий пользователя, необходимо установить соответствующие права аудита:

1. Чтение/запись – протоколируются попытки пользователя читать/записывать данные. Для типов устройств «Bluetooth, FireWire-порт, ИК-порт, Параллельный порт, последовательный порт, USB-порт и WiFi».

2. Печать – протоколируются попытки пользователя посылать документы на принтеры. Применимо только к типу «Принтер».

3. Выполнение – протоколируются попытки пользователя удаленно выполнить код на стороне устройства. Применимо только к типу «Windows Mobile».

4. Чтение/запись не файлов – протоколируются попытки пользователя читать/записывать не файловые объекты (календарь, контакты, задачи и т.п.). Применимо только к типам «Windows Mobile» и «Palm».

Существует возможность протолировать успешный доступ к устройствам и ошибки доступа:

1. «Аудит разрешений» – все попытки доступа, которые были разрешены DeviceLock, т.е. пользователю был предоставлен доступ к устройству.

2. «Аудит запретов» – все попытки доступа, которые были заблокированы DeviceLock, т.е. пользователю был запрещён доступ к устройству.

Перейдите в раздел «Устройства – Аудит и теневое копирование». Примените к съёмным устройствам аудит для пользователя «user» (рис. 3).

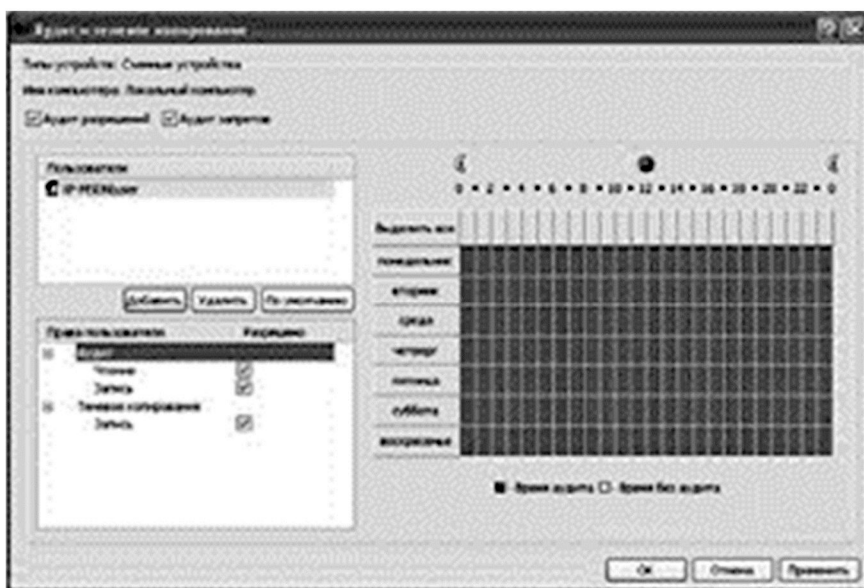


Рис. 3. Настройка аудита для съёмных устройств

Доступ к результатам аудита можно получить во вкладке «Просмотрщик журнала аудита». Журналы аудита могут храниться как в стандартных журналах ОС «Windows», так и в журналах DeviceLock. Перейдите во вкладку «Настройка сервиса – Аудит и теневое копирование» (рис. 4).

Опция – «Тип журнала аудита» устанавливает вид журнала и может принимать три значения:

- «Журнал событий» – данные аудита записываются только в стандартный журнал «Windows», хранящийся на локальном компьютере.
- «Журнал DeviceLock» – данные аудита записываются только в собственный защищённый журнал, отсылаемый на DeviceLock Enterprise Server для централизованного хранения.
- «Журнал событий и DeviceLock» – запись в оба журнала.

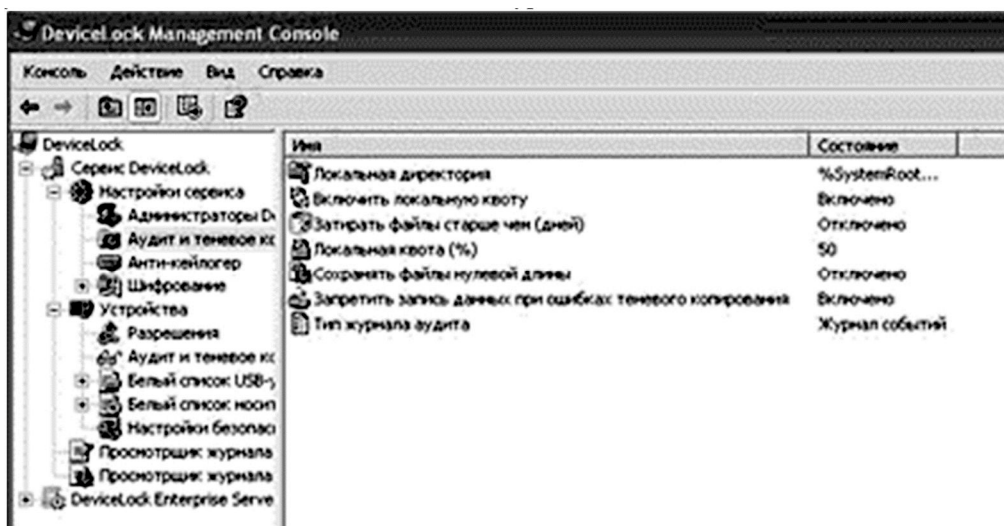


Рис. 4. Вкладка «Настройка сервиса – Аудит и теневое копирование»

Для того чтобы просмотреть журнал аудита через стандартный журнал «Windows», запустите консоль управления «Пуск – Выполнить – MMC». В ней добавьте оснастку «Просмотр событий». Вкладка «DeviceLock Log» предоставляет журнал аудита.

Теневое копирование позволяет сохранять копии всех файлов, которые пользователь копирует на съёмные носители или отправляет на печать. Сохранённые файлы могут быть в дальнейшем проанализированы на предмет наличия в них конфиденциальной информации.

Перейдите в раздел DeviceLock «Устройство – Аудит и теневое копирование». Включите для пользователя «user» теневое копирование файлов на съёмные устройства (рис. 5).

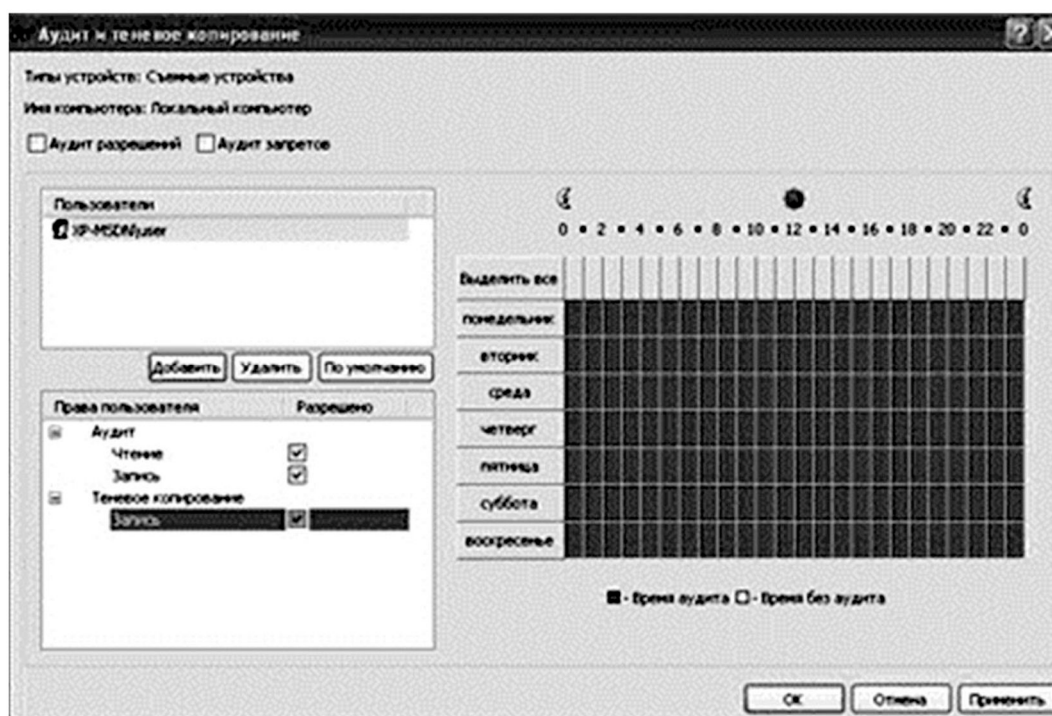


Рис. 5. Включение теневого копирования для съёмных устройств

Под учётной записью «user» подключите съёмное устройство и скопируйте на него текстовый или графический файл. Затем под учётной записью «Администратор» откройте раздел DeviceLock «Просмотрщик журнала теневого копирования» и откройте появившуюся в журнале запись. Это позволит увидеть содержимое файла, скопированного пользователем «user» на съёмное устройство.

## **7. Контрольные вопросы:**

1. Существует ли возможность разграничения доступа к управлению приложением DeviceLock?
2. В чём отличие уровня интерфейса от уровня типа устройств?
3. Какие функции разграничения доступа к ресурсам предоставляет DeviceLock?
4. Каким образом можно исключить классы USB-устройств (например, мыши, клавиатуры и т.п.) из механизма разграничения доступа?
5. Для чего используются белые списки?
6. К каким классам устройств могут быть созданы белые списки?
7. Какие варианты идентификации устройства применяются в белом списке?
8. Для чего используется база данных устройств?
9. Где могут храниться журналы аудита работы с устройствами?
10. Для чего используется теневое копирование файлов?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** Томский государственный университет систем управления и радиоэлектроники, Факультет безопасности, Конев Антон Александрович, kaa1@keva.tusur.ru

## **Дисциплина: Управление информационной безопасностью**

**Образовательная программа:** 10.05.04 – Информационно-аналитические системы безопасности, Информационная безопасность финансовых и экономических структур.

**Дисциплина:** Управление информационной безопасностью.

### **Лабораторная работа.**

#### **Оценка соответствия системы управления информационной безопасностью требованиям стандарта СТО БР ИББС 1.0**

##### **1. Учебные цели:**

Отработать навыки анализа рисков в автоматизированной системе управления рисками.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- Уметь осуществлять аудит, контроль, мониторинг безопасности банковских и других критических систем, инфраструктур и бизнес-процессов.
- Владеть навыками проведения аудита, контроля, мониторинга безопасности банковских и других критических систем, инфраструктур и бизнес-процессов.

##### **3. Перечень материально-технического обеспечения**

**Лабораторное оборудование и программное обеспечение:** Microsoft Windows 10, РискМенеджер-Инфо, VirtualBox.

##### **4. Задание на исследование**

Внесите данные в соответствии с описанием системы для варианта, установите логические связи, ответьте на вопросы из раздела «Политика безопасности» по собственному представлению, ознакомьтесь с предложенными контрмерами (примите необходимые), сформируйте отчет.

Пример варианта

Информационная система компании состоит из трех отделов: информационно-вычислительного центра, экономического отдела и бухгалтерии. Имеются два вида ресурсов: сервер и два компьютера. В компании одна сетевая группа. Компьютер экономического отдела, компьютер бухгалтерии и сервер объединены в сеть посредством сетевого коммутатора. На сервере хранится информация о ценовых предложениях для клиентов. Бухгалтерская информация хранится на компьютере бухгалтерии, информация о з/п хранится на компьютере экономического отдела. В системе всего три группы пользователей: системный администратор, экономисты, бухгалтеры. Выделены такие бизнес-процессы: внедрение изменений (для обработки информации о ценовых предложениях), подготовка и подписание договоров, начисление з/п. Системный администратор имеет доступ в Интернет и локальный доступ к информации о ценовых предложениях для клиентов со всеми правами доступа, экономисты имеют локальный доступ к информации о з/п с правами доступа «чтение» и «запись» и удаленный доступ с правом чтения к информации о ценовых предложениях для клиентов, бухгалтеры имеют локальный доступ к бухгалтерской информации с правом чтения и записи. Средства защиты укажите исходя из логических соображений (в реальной ситуации необходимо будет узнать об их наличии/отсутствии в рассматриваемой системе).

##### **5. Краткие теоретические сведения:**

Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» устанавливает требование регулярно проводить аудит информационной безопасности и самооценки информационной безопасности для всех организаций банковской системы на территории Российской Федерации. Стандарт Банка России СТО БР ИББС-1.2-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014» в свою очередь устанавливает способы определения степени выполнения требований, описанных в упомянутом выше стандарте.

##### **6. Порядок выполнения лабораторной работы**

На первом шаге необходимо создать модель. Для этого правым щелчком мыши на срезе структуры выбираем «Создать → Модель» (рис. 1).

На следующем шаге необходимо для созданного региона необходимо создать локальную среду. Правым щелчком мыши на регионе создаем локальную среду «Оценка банка по стандартам». Во



вновь созданной подсистеме правым щелчком мыши создаем объект. В окне свойств объекта указываем в качестве класса объекта «Оценка уровня обеспечения ИБ организации БС РФ в соответствии с требованиями СТО БР ИББС-1.0» (рис. 2).

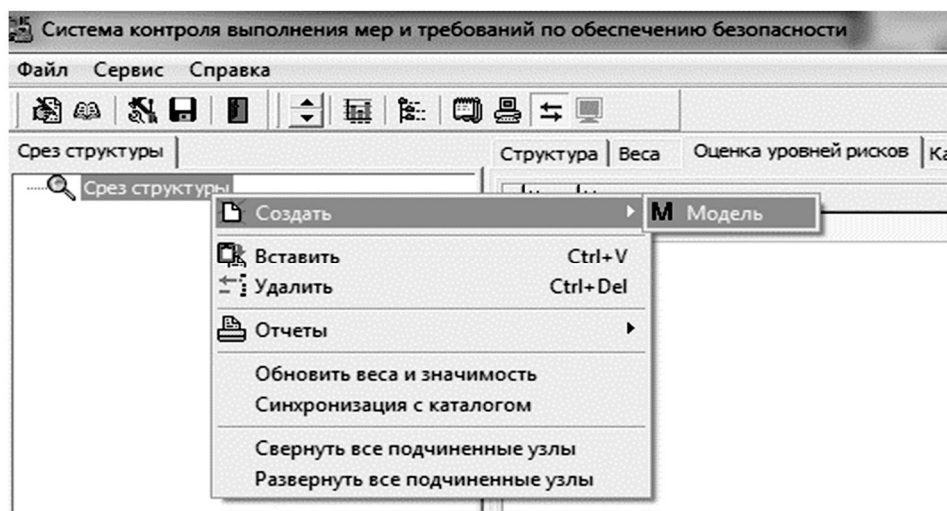


Рис. 1. Создание модели

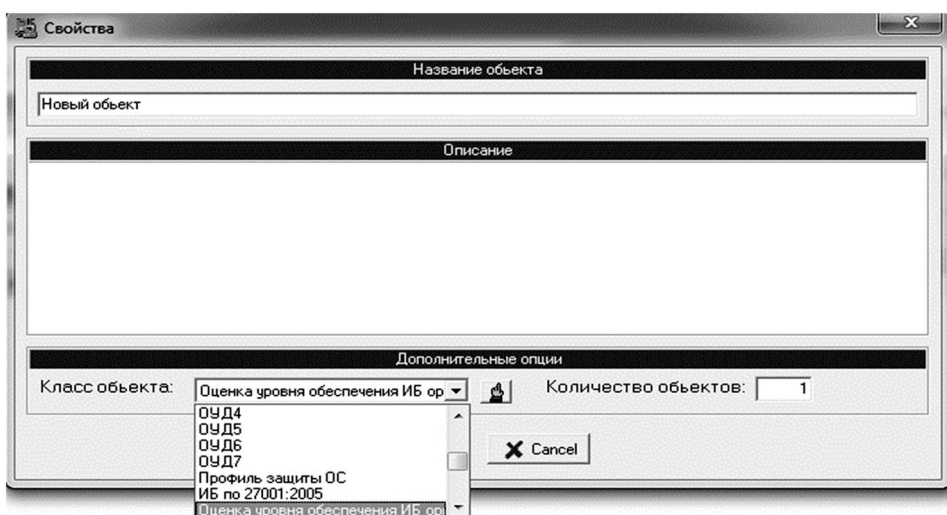


Рис. 2. Задание свойств объекта

После создания объекта нужно определить выполняемые требования по мерам защиты. Для этого необходимо перейти во вкладку «Выполнение мер и требований» (рис. 3) по объекту. Объект «Оценка уровня обеспечения ИБ организации БС РФ в соответствии с требованиями СТО БР ИББС-1.0» включает в себя 32 меры защиты для каждой из которых надо в окне требований по мере определить условия выполнения. По умолчанию все требования имеют значение «Да», с помощью двойного щелчка нужно сменить условие выполнения на «Нет».

Аналогично создайте локальную среду «Расчетный центр» и подсистему «Базовые сервисы безопасности». В созданную подсистему добавьте объект «Межсетевой экран – Профиль защиты для сред с низкими рисками нарушения безопасности».

Измените значения некоторых требований. Перечень требований со значением «Нет» представлены в таблице 1. В остальных требованиях оставить значение по умолчанию.

Создайте локальную среду «АИС», подсистему «АРМ» и объект «АРМ». Все значения требований по мере остаются по умолчанию.

Параметры задайте следующим образом:

- Регион: г.Томск;
- Локальная среда: Представительство;
- Подсистему: Базовые сервисы безопасности;
- Объект: Автоматизированная система.

Измените значения некоторых требований. Перечень требований со значением «Нет» представлены в таблице 2. В остальных требованиях оставить значение по умолчанию.

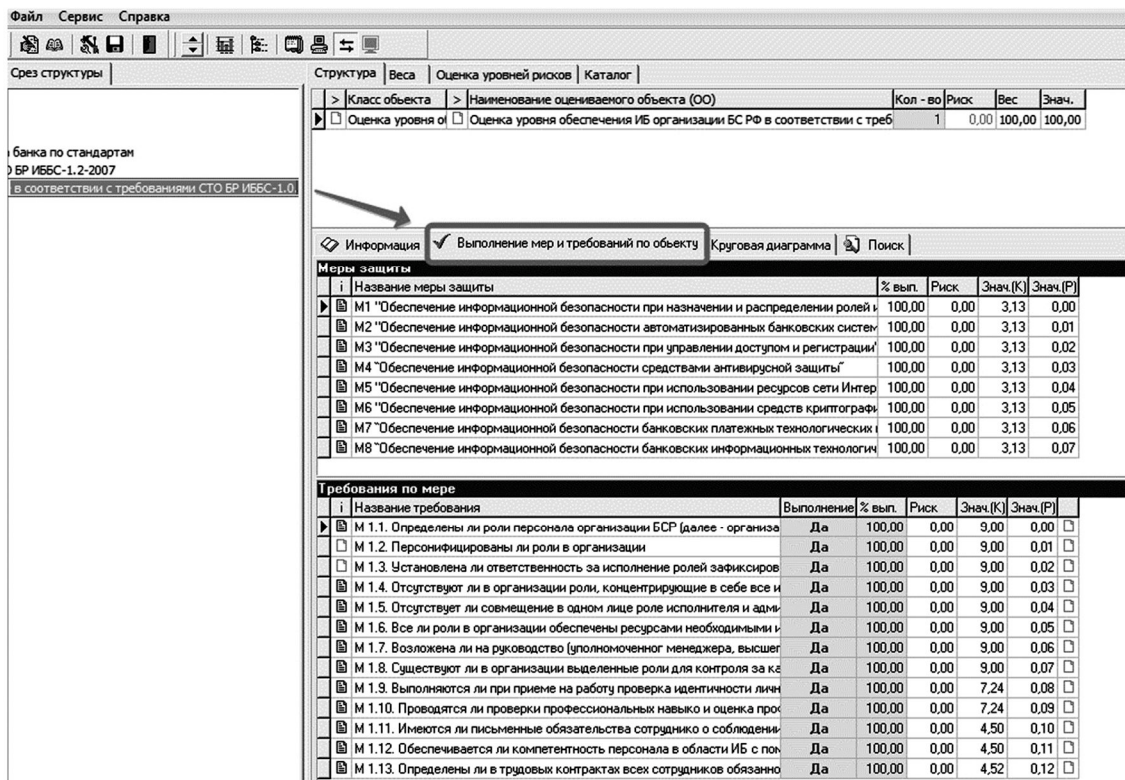


Рис. 3. Основное меню

Таблица 1 – Перечень мер

| Меры защиты                   | Требования по мере                                                                           |
|-------------------------------|----------------------------------------------------------------------------------------------|
| Аудит безопасности ПЗ МЭ НРНБ | КСБ должен предпринимать действия в случае, если обнаружено возможное нарушение безопасности |
|                               | КСБ должен выполнять заданные действия при обнаружении возможного нарушения безопасности     |

Таблица 2 – Перечень мер

| Меры защиты                                      | Требования по мере                                                                                                            |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Управление доступом к компьютерам                | Должно обеспечиваться ограничение времени подключения                                                                         |
|                                                  | Должно устанавливаться время простоя терминалов, после которого сеансы связи должны закрываться                               |
| Оперирование с носителями информации и их защита | Должны быть внедрены надежные и проверенные процедуры уничтожения компьютерных носителей информации, которые больше не нужны. |
| Обслуживание систем                              | Должен быть обеспечен постоянный контроль за окружающей средой                                                                |
|                                                  | Должны быть разработаны регламенты извещения о сбоях в работе систем и принятия соответствующих корректирующих действий       |

После окончания создания всех элементов срез структуры должен выглядеть следующим образом (рис. 4).

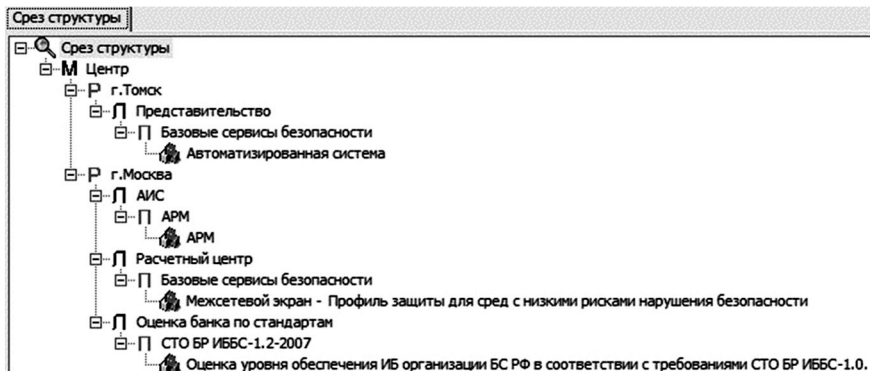


Рис. 4. Окно срез структуры

Во вкладке «Вес» (рис. 5) в графе г. Томск установите значение 80. Остальные значения оставьте без изменения.

| Регионы в активной модели |        |
|---------------------------|--------|
| Название региона          | Вес    |
| г.Москва                  | 100,00 |
| ▶г.Томск                  | 80,00  |

Рис. 5. Веса регионов в активной модели

После заполнения всей необходимой информации нужно запустить расчет рисков при помощи специальной кнопки (рис. 6).

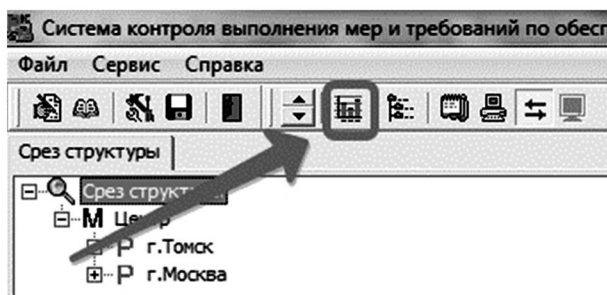


Рис. 6. Панель инструментов

Сохранение отчета происходит при нажатии правой кнопки мыши на соответствующем разделе (рис. 7).

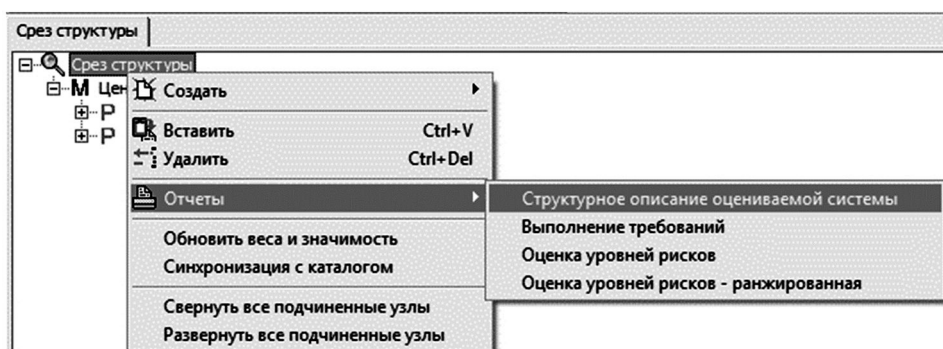


Рис. 7. Сохранение отчета

## 7. Контрольные вопросы:

1. Что представляет из себя система РискМенеджер-Инфо и для чего она предназначена?
2. Какое количество мер защиты содержит в себе «Оценка уровня обеспечения ИБ организации БС РФ в соответствии с требованиями СТО БР ИББС-1.0»?
3. Приведите несколько примеров названий мер защиты.
4. В каком формате выводятся результаты оценки объекта на предмет обеспечения требований из СТО БР ИББС-1.0?
5. Каким образом можно изменить значение веса региона в активной модели?
6. Что из себя представляет срез структуры?
7. Какие виды отчетов можно получить для среза структуры?
8. Какие типы экономического ущерба бывают? Каковы их последствия?
9. Приведите примеры средств защиты для ресурса.
10. Перечислите средства защиты информации.

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** Томский государственный университет систем управления и радиоэлектроники, Факультет безопасности, Конев Антон Александрович, kaa1@keva.tusur.ru

**Образовательная программа:** 10.05.04 – Информационно-аналитические системы безопасности, Информационная безопасность финансовых и экономических структур.

**Дисциплина:** Управление информационной безопасностью.

### **Лабораторная работа.** **Анализ и управление рисками информационной системы**

#### **1. Учебные цели:**

Отработать навыки анализа рисков информационной системы.

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

- **Уметь** анализировать модели информационных потоков
- **Владеть** анализа моделей информационных потоков с учетом зависимостей от исходных данных, а также того, какие данные интересуют пользователя на выходе.

#### **3. Перечень материально-технического обеспечения**

**Лабораторное оборудование и программное обеспечение:** Microsoft Windows 10, Digital Security Office Гриф, VirtualBox.

#### **4. Задание на исследование**

Постройте модель информационной системы, соответствующую описанию, предложенному в вариантах заданий, установите логические связи, ответьте на вопросы из раздела «Политика безопасности», ознакомьтесь с предложенными контрмерами (примите необходимые), сформируйте отчет.

#### **5. Краткие теоретические сведения.**

При работе с моделью информационных потоков в систему вносится полная информация обо всех ресурсах с ценной информацией, пользователях, имеющих доступ к этим ресурсам, видах и правах доступа. Заносятся данные обо всех средствах защиты каждого ресурса, сетевые взаимосвязи ресурсов, а также характеристики политики безопасности компании. В результате получается полная модель информационной системы с точки зрения информационной безопасности с учетом реального выполнения требований комплексной политики безопасности, что позволяет перейти к программному анализу введенных данных для получения комплексной оценки рисков и формирования итогового отчета.

#### **6. Порядок выполнения лабораторной работы**

В окне «Алгоритм анализа рисков» выберите пункт «Анализ модели информационных потоков», создайте новый проект.

Для начала работы необходимо иметь описание системы. Информационная система Компании состоит из одного отдела – бухгалтерии. Имеются сервер и рабочая станция, которые физически связаны между собой. На сервере хранятся два вида информации: бухгалтерский отчет и база клиентов; на рабочей станции. база данных наименований товаров с описанием. В компании есть три сотрудника: финансовый директор, главный бухгалтер, бухгалтер. К бухгалтерскому учету на сервере локальный доступ имеет главный бухгалтер, к базе клиентов удаленный доступ имеют бухгалтер (с рабочей станции через коммутатор) и финансовый директор. При чем финансовый директор имеет удаленный доступ через Интернет. К базе данных наименований товаров с описанием на рабочей станции локальный доступ имеет бухгалтер.

Для описания информационной системы существуют такие виды объектов, как отделы, сетевые группы, ресурсы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы (рис. 1).

Внесем входные данные. Так как, информационная система Компании состоит из одного отдела – бухгалтерии. В отделе имеется одна сетевая группа. Добавьте отдел «Бухгалтерия» и одноименную сетевую группу. Информационная система содержит два ресурса: сервер и рабочую станцию, которые физически связаны между собой (находятся в одной сетевой группе).

Добавьте ресурсы «Сервер» и «Рабочая станция», указав тип ресурса (сервер, рабочая станция, мобильный компьютер, твердая копия, веб-сервер), сетевую группу и отдел, к которым принадлежит ресурс.

На сервере хранятся два вида информации: бухгалтерский отчет и база клиентов; на рабочей станции – база данных наименований товаров с описанием. Добавьте эти три вида информации аналогичным образом.

Рассмотрим трех сотрудников, каждый из которых отнесем к отдельной группе пользователей. Создайте группы пользователей: главный бухгалтер, бухгалтер и финансовый директор. При чем для финансового директора укажите класс группы пользователей «Авторизованные пользователи из Интернет» (так как у него должен быть удаленный доступ к базе клиентов компании), а для бухгалтеров – «Пользователи».

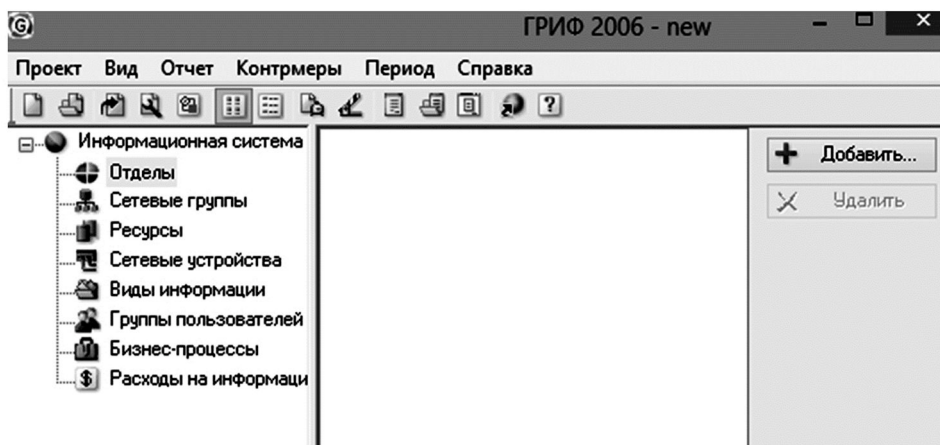


Рис. 1. Основное окно программы

В зависимости от выбора класса будут предложены средства защиты рабочего места группы пользователей. Средства защиты клиентского места групп авторизованных Интернет-пользователей (здесь – финансовый директор) оценить невозможно, т.к. неизвестно, откуда будут осуществлять доступ пользователи этой группы.

Для клиентского места бухгалтера укажите следующие средства защиты: контроль доступа в помещение, где расположен ресурс (дверь с замком, видео наблюдение); средства антивирусной защиты (антивирусный монитор); отсутствие возможности подключения внешних носителей; персональный межсетевой экран; система криптозащиты электронной почты. То же самое проделайте и для клиентского места главного бухгалтера, отметьте разрешение доступа в Интернет.

После добавления всех объектов в информационную систему, пользователю необходимо проставить связи, т.е. определить к каким отделам и сетевым группам относятся ресурсы, какая информация хранится на ресурсе и какие группы пользователей имеют к ней доступ. Также, пользователь системы указывает средства защиты ресурса и информации.

Для добавления к ресурсу «Сервер» двух видов информации (как указано выше) «Бухгалтерский отчет» и «База клиентов» необходимо в вкладке «Виды информации» кнопкой «Добавить» вызвать окно добавления вида информации, в котором в выпадающем меню выбрать требуемые пункты.

После выбора вида информации станет доступно поле «Ущерб по угрозам». Установите ущерб по угрозе «Конфиденциальность» – 100 у.е. в год, по угрозе «Целостность» – 100 у.е. в год, по угрозе «Доступность» – 1 у.е. в час для обоих видов информации. В случае, если единицы измерения ущерба по угрозам отличны от у.е., откройте справку, найдите каким образом выбрать другие единицы измерения.

Прделайте аналогичные действия для ресурса «Рабочая станция» (вид информации – «База данных наименований товаров»); ущерб по угрозам в точности такой же, как и у других видов).

Перейдите на вкладку «Группы пользователей» и укажите группы пользователей и их права на конкретный вид информации в соответствии с табл. 1.

Таблица 1 – Вид и права доступа групп пользователей к информации, наличие соединения через VPN, количество человек в группе

|                                              | Вид доступа | Права доступа            | Наличие VPN-соединения | Количество человек в группе |
|----------------------------------------------|-------------|--------------------------|------------------------|-----------------------------|
| Главный бухгалтер / бухгалтерский отчет      | локальный   | чтение, запись, удаление | нет                    | 1                           |
| Бухгалтер / база клиентов                    | удаленный   | чтение                   | есть                   | 1                           |
| Финансовый директор / база клиентов          | удаленный   | чтение, запись           | есть                   | 1                           |
| Бухгалтер / база данных наименований товаров | локальный   | чтение, запись, удаление | нет                    | 1                           |

Во вкладке «Каналы связи» укажите, что группа пользователей «бухгалтер» имеет доступ к ресурсу «Сервер» через сетевое устройство «Коммутатор».

Чтобы указать средства защиты ресурса, перейдите на вкладку «Средства защиты», нажмите кнопку «Изменить» и укажите для ресурса «Сервер» следующие пункты: контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком, специальный пропускной режим в помещении); отсутствие возможности подключения внешних носителей; межсетевой экран; обманная система; система антивирусной защиты на сервере; аппаратная система контроля целостности. Для ресурса «Ра-

бочая станция» задайте средства защиты из шаблона (необходимо задать: контроль доступа в помещение, где расположен ресурс (дверь с замком, видеонаблюдение); средства антивирусной защиты (антивирусный монитор); отсутствие возможности подключения внешних носителей; персональный межсетевой экран; система криптозащиты электронной почты). Для этого в окне выбора шаблона выберите группу пользователей «Бухгалтер».

В последней вкладке необходимо указать средства защиты для каждого вида информации. Для вида информации «Бухгалтерский учет» отметьте все средства защиты, кроме «Дополнительная программно-аппаратная система контроля доступа».

Так как модель «Информационных потоков» не может учесть организационные меры, связанные с поведением сотрудников организации, существует раздел «Политика безопасности» (рис. 2).

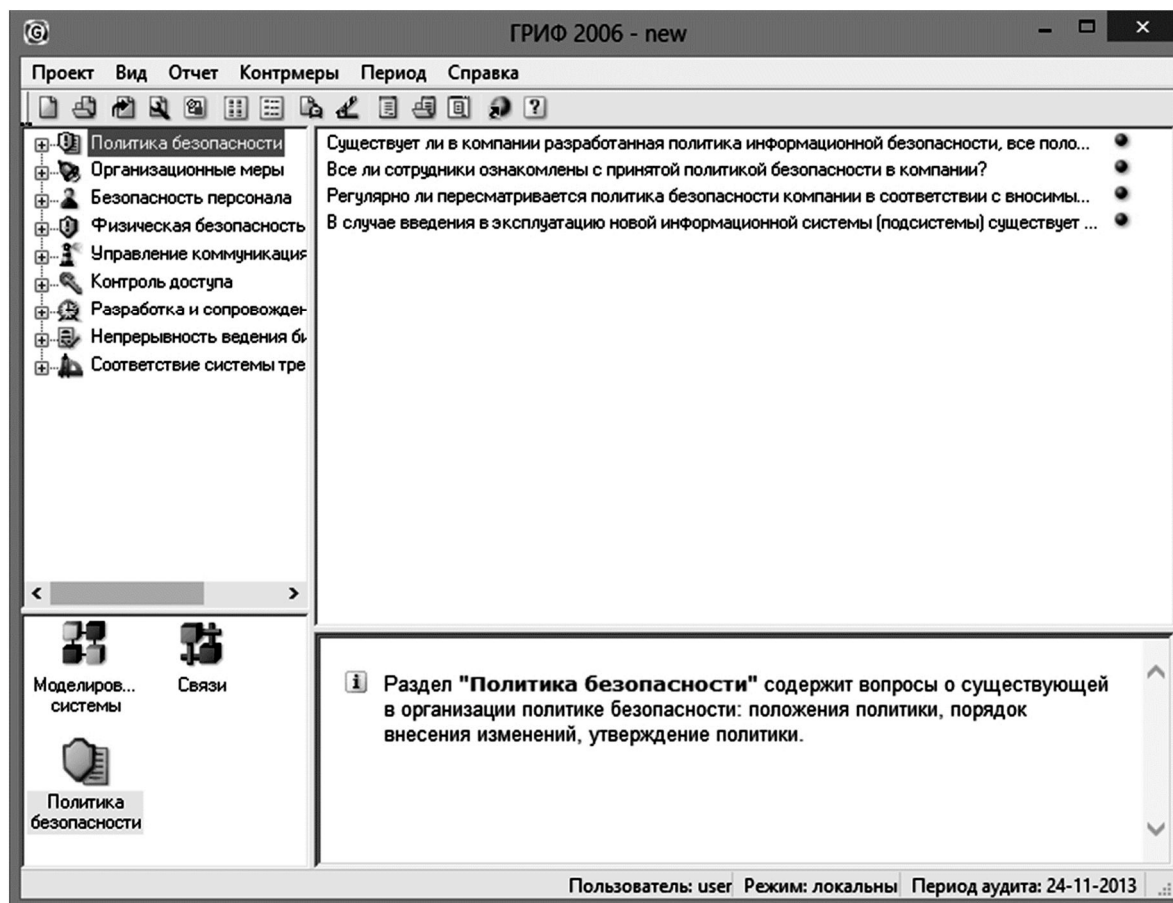


Рис. 2. Раздел «Политика безопасности»

В нем пользователю необходимо ответить на ряд вопросов. Ответы на вопросы влияют на веса средств защиты и изменяют риск реализации информационной безопасности.

После выполнения всех этапов, на выходе пользователь получает полную сформированную модель информационной системы с точки зрения информационной безопасности, что позволяет перейти к программному анализу введенных данных для комплексной оценки рисков, а также внедрению контрмер.

Для перехода в окно управления рисками, в главном меню выберите пункт «Контрмеры» и из выпадающего списка нажмите «Управление рисками» (рис. 3).

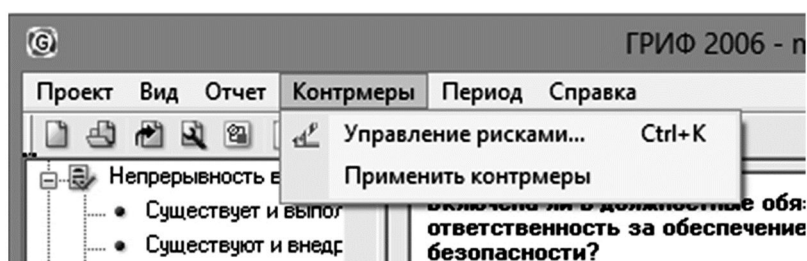


Рис. 3. Меню «Контрмеры»

После чего появится окно «Управление рисками», в нем содержится информация по каждому ресурсу системы, средствах защиты каждого ресурса отдельно, а также сведения о пользователях. В нижней части окна расположены регулятор уровня риска «Задание уровня риска» (по умолчанию он установлен в 0) и информация об эффективности контрмер для всей системы.

Регулятор уровня риска позволяет отфильтровать объекты системы по значимости, например, по умолчанию он установлен в 0.00 у.е., это означает что в поле «Объекты» будут показаны все объекты, уровень риска которых превышает данный порог. Передвинув регулятор вправо, определите какой уровень риска не превышает ресурс «Рабочая станция». В поле «Эффективность комплекса контрмер» показан суммарный риск всей системы.

Для внедрения контрмер выберите интересующий вас ресурс, в рамках ресурса будет показано, какие средства защиты не используются для защиты ресурса, какой вид информации использует данный ресурс и какие средства защиты еще не применены к данному виду информации, а также какая группа пользователей работает с данной информацией. Выберите одно из предложенных средств защиты, нажмите кнопку «Задать», откроется окно «Новая контрмера».

Внедрение контрмеры, напрямую снижает уровень риска реализации угроз, чем больше будет применено контрмер к системе, тем ниже будет показатель риска. Заданные контрмеры подсвечиваются оранжевым кругом, после применения контрмеры, она пропадет из списка, а риск информационной системы обновится.

Вы можете принять все контрмеры, или только некоторые, исходя из необходимости и возможности их внедрения в рассматриваемую вами конкретную систему.

Результатом работы системы ГРИФ является отчет, содержащий расчеты затрат компании на ИБ, на контрмеры, вероятности реализации рисков в общем и по отделам и другую информацию, представленную в виде обобщающих диаграмм, графиков и таблиц. Создайте отчет, для чего в главном меню системы гриф выберите пункт «Отчет» и нажмите «Создать отчет...». Появится окно конфигурации отчета, в нем пользователь выбирает, какая информация будет выведена в отчете и в каком виде (рис. 4). Ознакомьтесь с содержанием отчета.

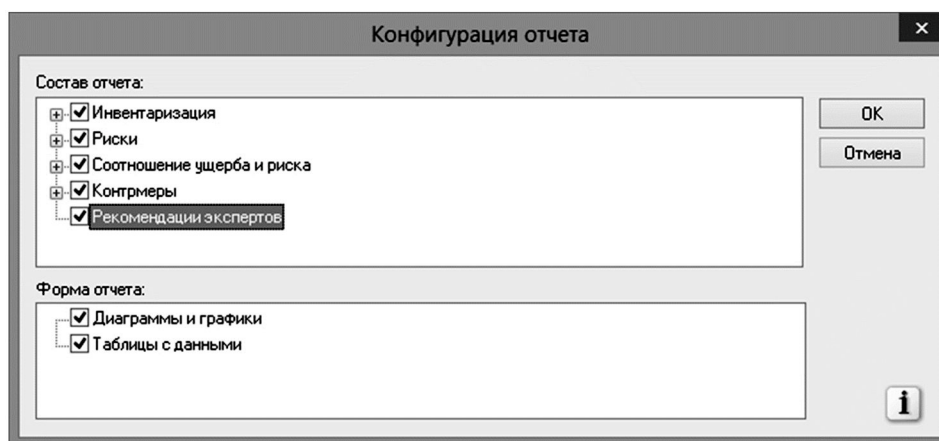


Рис. 4. Конфигурация отчета

#### 7. Контрольные вопросы:

1. Что представляет собой система ГРИФ и для чего она предназначена?
2. Что понимается под характеристиками группы пользователей?
3. Что такое эффективность средства защиты?
4. Приведите примеры ресурсов, используемых при построении модели информационных потоков в ГРИФ.
5. Что понимается под базовым временем простоя ресурсов?
6. С какой целью создан раздел контрмер?
7. Опишите пошагово работу с моделью информационных потоков.
8. Почему для класса группы авторизованных Интернет-пользователей система ГРИФ не предлагает никакие средства защиты рабочего места?
9. По каким угрозам оценивается ущерб в изученной системе?
10. Как повлияет на веса средств защиты ответ «Положения политики внедрены частично» на первый вопрос раздела о политике безопасности?

**Время на выполнение лабораторной работы – 4 часа.**

**Образовательная организация, авторы, эл. почта:** Томский государственный университет систем управления и радиоэлектроники, Факультет безопасности, Конев Антон Александрович, kaal@keva.tusur.ru

**СПЕЦИАЛИТЕТ 10.05.05**  
**БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**  
**В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ**

**Дисциплина: Техническая защита информации**

**Образовательные программы:** 10.03.01 Информационная безопасность (Комплексная защита объектов информатизации), 10.05.05 Безопасность информационных технологий в правоохранительной сфере («Компьютерная экспертиза при расследовании преступлений»).

**Дисциплина:** Техническая защита информации

**Лабораторная работа.**

**Способ контроля телефонной линии связи на наличие закладного устройства с применением анализатора проводных линий SEL SP-37 «Трал»**

**1. Учебные цели:**

Освоить навыки работы с аппаратурой контроля речевой информации в телефонных линиях.

**2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

**Уметь:**

- анализировать и оценивать угрозы информационной безопасности объекта;
- составлять структурные схемы образования комплексных каналов утечки информации;
- применять методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства.

**Владеть:**

- методами расчета и инструментального контроля показателей технической защиты информации;
- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

**3. Перечень материально-технического обеспечения**

- **Лабораторное оборудование и программное обеспечение:**
  - Персональный компьютер Intel Core i5-2400 Box 3.10.
  - Офисная аналоговая АТС фирмы Panasonic модель KX-TEM 824 RU.
  - Телефонные аппараты фирмы Panasonic модели KX-T7730 и KX-TS2350.
  - Имитатор закладного устройства (ИЗУ) в виде УКВ ЧМ передатчика в радиовещательном диапазоне частот.
  - Анализатор проводных линий SEL SP-37 «Трал».
  - Управляющая программа «Analizator», предназначенная для обмена данными с анализатором проводных линий, чтением архивов анализатора, чтения, представления и записи файлов телефонных линий и передачей сообщений с файлами телефонных линий по электронной почте.

**4. Задание на исследование**

Изучить возможности анализатора проводных линий SEL SP-37 «Трал» для проведения контроля телефонной линии связи на наличие закладного устройства.

**5. Краткие теоретические сведения**

Среди разнообразных электронных средств перехвата особое место занимает прослушивание телефонных разговоров, так как телефонная линия – это самый распространенный и самый небезопасный канал связи, а также доступ к нему часто требует минимальных затрат. Учитывая вышесказанное, при обеспечении защиты информации большое внимание уделяется способам и средствам контроля телефонных линий.

Телефонная связь – вид электросвязи, предназначенный для обмена информацией преимущественно путем разговора с использованием телефонных аппаратов. Через эту сеть можно передавать речь, цифровые данные, изображения, видео и другие виды информации.

Процесс телефонной передачи сообщения заключается в преобразовании звуковых колебаний речи в колебания (изменения) электрического тока, передачи его по проводным линиям и обратном преобразовании электрических колебаний в звуковые.

Кабель телефонной линии связи (ТФЛ) представляет собой совокупность нескольких проводников (жил), изолированных друг от друга и заключенных в общую оболочку. Проводники кабелей выполняются из мягкой меди, и каждая пара проводников имеет отличную от других цветовую окраску.



Современная АТС представляет собой программно-управляемую коммутационную систему способную работать с цифровыми сигналами. Это означает, что при вводе в АТС аналоговый сигнал, поступающий с абонентской линии, преобразуется в цифровую форму и в этой форме распространяется далее по телефонной сети, превращаясь снова в аналоговую форму при попадании в абонентскую линию другого абонента.

В представленной телефонной линии связи средствами, формирующими каналы утечки информации, могут быть подслушивающие устройства, устанавливаемые в помещениях и на телефонных линиях, а также автоматические устройства технической разведки, устанавливаемые в кабельных линиях связи.

Непосредственное подключение телефонных радиозакладок (ТФРЗ) к телефонной линии (ТФЛ), осуществляемое только при наличии гальванического контакта, можно подразделить на два вида (рисунок 1):

- ТФРЗ с последовательным подключением;
- ТФРЗ с параллельным подключением.

ТФРЗ этих двух видов включаются на передачу тогда, когда абонент снимет телефонную трубку (т.е. когда напряжение в ТФЛ упадет, а ток возрастет).

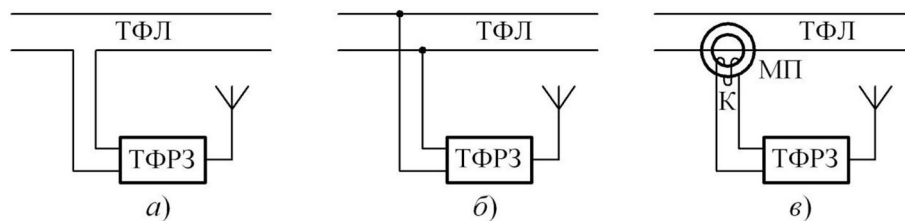


Рис. 1. Виды подключений ТФРЗ к ТФЛ

Закладные устройства с индуктивным подключением посредством магнитопровода с катушкой индуктивности слабо влияют на ТФЛ, а потому обнаружить их техническими средствами крайне затруднительно. Следует также отметить, что эти ТФРЗ не способны получать питание от линии связи и поэтому обычно снабжаются собственными автономными источниками питания.

Индуктивный съём информации с ТФЛ осуществляется следующим образом (рисунок 2 в). Два провода или две жилы ТФЛ отделяются одна от другой, и на одну из них одевается замкнутый магнитопровод индуктивного датчика ТФРЗ.

ТФРЗ, предназначенные для вышерассмотренных видов подключений, иногда могут быть закамouflированы под типовые элементы телефонной аппаратуры. Все эти виды подключений ТФРЗ к ТФЛ обеспечивают подслушивание за счет электромагнитных каналов утечки информации из линии.

При возникновении подозрений на утечку информации по телефонным линиям связи появляется необходимость решить задачу по обнаружению закладного устройства. Способы контроля телефонных линий основаны на том, что любое подключение к ним вызывает изменение электрических параметров линий: напряжения и тока в линии, значений емкости и индуктивности линии, активного и реактивного сопротивления. В зависимости от способа подключения подслушивающего устройства к телефонной линии (последовательного – в разрыв провода телефонного кабеля, параллельного или индуктивного) влияние подключаемого подслушивающего устройства может существенно отличаться. Так как закладное устройство использует энергию телефонной линии, величина отбора мощности закладкой из телефонной линии зависит от мощности передатчика закладки и его коэффициента полезного действия. Наилучшие возможности по выявлению этих отклонений обеспечиваются при опущенной трубке телефонного аппарата. Это обусловлено тем, что в этом состоянии в телефонную линию подается постоянное напряжение 48±60 В (для отечественных телефонных линий) и 25±36 В (для зарубежных АТС). При поднятии трубки в линию поступает от АТС дискретный сигнал, преобразуемый в телефонной трубке в длинный прерывистый тон, а напряжение в линии уменьшается до 10±15 В, т.е. происходит резкое изменение электрических параметров линии, существенно превышающие изменения из-за наличия закладных устройств.

При проверке проводных коммуникаций изначально проводится визуальный осмотр каждой линии, абонентских телефонов линии, распределительных коробок и т.п.

Если после проведения визуального осмотра в линии не найдено подключенных подслушивающих устройств, то проводится измерение параметров линии, а также поиск частот, на которых закладное устройство передает информацию в эфир. Если имеется возможность, то рекомендуется прохождение всей трассы эфирным нелинейным локатором.

Для выполнения контроля телефонной линии связи необходим прибор, который способен фиксировать следующие изменения в телефонной линии связи:

- постоянное напряжение в телефонной линии при поднятой трубке;
- постоянное напряжение в телефонной линии при положенной трубке;
- постоянный ток в телефонной линии при поднятой трубке.

Измерения проводятся несколько раз и измеренные значения могут отличаться на сотые значения, что является нормой для любого типа телефонных линий. Поэтому необходим расчет среднего зна-

чения напряжения (тока) в линии при поднятой ( $U_{up}$ ) и положенной ( $U_{down}$ ) трубках в соответствии с выражением:

$$U = \frac{a_1 + a_2 + \dots + a_n}{n},$$

где  $a$  – значение напряжение (тока) при измерении;  $n$  – количество проведенных измерений.

Для проведения эксперимента в настоящей лабораторной работе используется анализатор проводных линий SEL SP-37 «Трал», который предназначен для проверки проводных линий на наличие устройств несанкционированного съема информации. Анализатор «Трал» обеспечивает автоматическое измерение необходимых величин. По полученным данным с анализатора и оценивается возможность несанкционированного подключения к телефонной линии.

В данной работе в качестве ИЗУ используется устройство, схема которого представляется собой УКВ ЧМ передатчик в радиовещательном диапазоне частот. Питается оно от телефонной линии и имеет выходную мощность около 20 мВт.

Принципиальная схема ИЗУ представлена на рисунке 2.

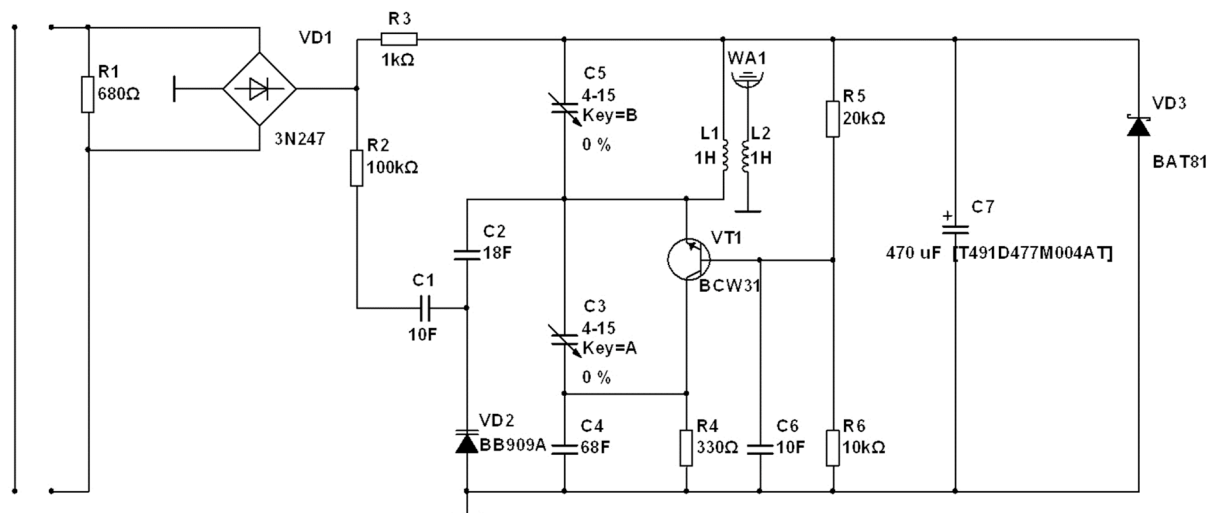


Рис. 2. Принципиальная схема УКВ ЧМ передатчика в радиовещательном диапазоне частот

Резистор R1 включается в разрыв одного из проводов телефонной сети. При снятии трубки телефонного аппарата в цепи появляется ток, который, в зависимости от типа аппарата и состояния линии, находится в пределах  $10 \div 35$  мА. Этот ток, протекая через резистор R1, вызывает на нем падение напряжения порядка от 4 до 25 В. Напряжение поступает на выпрямительную диодную сборку типа КЦ407, благодаря которой устройство может подключаться в линию без соблюдения полярности.

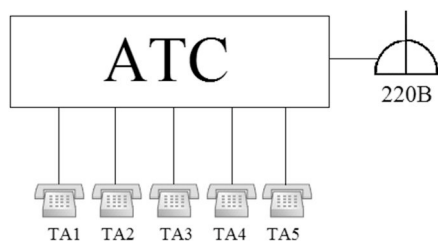
Высокочастотная часть схемы запитывается от параметрического стабилизатора, собранного на резисторе R3, стабилитроне VD3 типа КС191 и конденсаторе C7. Стабилизатор ограничивает излишек напряжения, поступающего с диодной сборки VD1. Задающий генератор выполнен на транзисторе VT1 типа КТ315. Частотная модуляция осуществляется путем изменения емкости варикапа VD2 типа KB109A. Модулирующее напряжение поступает из линии через последовательно включенные резистор R2 и конденсатор C1. Первый ограничивает уровень низкочастотного сигнала, второй – исключает проникновение постоянного напряжения линии в цепь модулятора.

Частотно-модулированный сигнал с катушки связи L2 поступает в антенну, в качестве которой используется отрезок монтажного провода длиной, равной четверти длины волны, на которой работает передатчик.

При настройке конденсаторы C3 и C5 подстраивают так, чтобы в нужном диапазоне (65÷200 МГц) передавался сигнал максимально возможной мощности. Дальность действия, собранного радиоретранслятора в зависимости от условий приема, составляет 30÷150 м.

## 6. Порядок выполнения лабораторной работы

1. Собрать экспериментальный стенд в соответствии со схемой, представленной на рисунке 1.
2. Провести инициализацию АТС с использованием значений по умолчанию в соответствии с инструкцией по эксплуатации офисной аналоговой АТС. Тип внешних линий определяется автоматически.
3. Задать собственный номер для каждого абонента. Номер строится по схеме «1\*», где «\*» – порядковый номер модульного разъема на АТС.
4. Проверить работоспособность системы, для чего необходимо осуществить вызовы между ТА, т.е. поднять трубку и ввести номер вызываемого абонента.



**Рис. 1. Схема экспериментального стенда**

Для быстрого набора номера имеется функция записи телефонного номера в память телефона. Чтобы осуществить запись номера необходимо перейти в режим программирования нажатием кнопки «PROGRAM» и выбрать ячейку, в которую требуется записать номер.

5. Подключить анализатор «Трал» к АТС через модульный разъем «LINE» на тыльной стороне анализатора к модульному разъему АТС (JACK 01 – JACK 24).
6. Подключить анализатор к электросети и включить его нажатием кнопки «POWER». Управление анализатором производится с использованием кнопок управления «А», «В», «С», «D» и валкодером.
7. Адаптировать анализатор «Трал» к той телефонной линии, к которой он подключен, для чего нужно перейти в режим «adapt», которой в автоматическом режиме установит требуемые параметры.
8. Для измерения тока и напряжения необходимо перейти в меню индикации «тето», которое находится в режиме адаптации, и нажать кнопку «В». В данном меню будут отображены текущие значения параметров телефонной линии.
9. Проверить каждую линию между АТС и абонентскими телефонными аппаратами.
10. Произвести не менее пяти измерений напряжения в линии при поднятой и опущенной трубке телефонного аппарата. Измерение тока производится только при поднятой трубке телефонного аппарата.
11. Рассчитать средние значения тока и напряжения при поднятой и опущенной трубке абонентского телефона. Данные занести в таблицы 1–2:

**Таблица 1 – Измеренные значения напряжения**

| Телефонный аппарат | Постоянное напряжение, В |       |       |       |       |          |
|--------------------|--------------------------|-------|-------|-------|-------|----------|
|                    | $U_1$                    | $U_2$ | $U_3$ | $U_4$ | $U_5$ | $U_{cp}$ |
| ТА 1               |                          |       |       |       |       |          |
| ТА 2               |                          |       |       |       |       |          |
| ТА 3               |                          |       |       |       |       |          |
| ТА 4               |                          |       |       |       |       |          |
| ТА 5               |                          |       |       |       |       |          |

**Таблица 2 – Измеренные значения тока**

| Телефонный аппарат | Ток, мА |       |       |       |       |          |
|--------------------|---------|-------|-------|-------|-------|----------|
|                    | $I_1$   | $I_2$ | $I_3$ | $I_4$ | $I_5$ | $I_{cp}$ |
| ТА 1               |         |       |       |       |       |          |
| ТА 2               |         |       |       |       |       |          |
| ТА 3               |         |       |       |       |       |          |
| ТА 4               |         |       |       |       |       |          |
| ТА 5               |         |       |       |       |       |          |

12. Сохранить полученные результатов измерения в память
13. Подключить анализатор «Трал» к компьютеру.
14. Запустить программу «Analizator».
15. Загрузить сохраненные значения тока и напряжения из памяти анализатора.
16. Перейти в раздел «Расчет» программы и построить графики на основе измеренных значений токов и напряжений для двух положений телефонной трубки: когда линия свободна или занята.
17. Подключить имитатор закладного устройства в виде УКВ ЧМ передатчика последовательно в разрыв одного из проводов телефонной линии в любом месте по всей длине кабеля между ТА1 ÷ ТА5 и АТС.
18. Провести измерения и расчеты согласно пунктам 8-11 и сравнить полученные данные. На основании проведенного анализа сформулировать вывод о наличии закладного устройства в телефонной линии.

## **7. Контрольные вопросы:**

1. Что такое телефонная линия связи?
2. Как могут быть сформированы каналы утечки информации по телефонной линии связи?
3. Поясните схемы подключения закладных устройств к телефонной линии связи.
4. На чем основаны способы контроля телефонных линий?
5. Поясните принцип действия анализатора проводных линий SEL SP-37 «Трал» при контроле телефонной линии связи.
6. По изменениям каких параметров телефонной линии связи можно судить о наличии закладного устройства?

**Время на выполнение лабораторной работы – 3 часа.**

**Образовательная организация, авторы, эл. почта:** Омский государственный технический университет, Данилова О.Т., olga.danlot@yandex.ru

---

**Образовательные программы:** 10.03.01 Информационная безопасность (Комплексная защита объектов информатизации), 10.05.05 Безопасность информационных технологий в правоохранительной сфере (Компьютерная экспертиза при расследовании преступлений).

**Дисциплина:** Техническая защита информации.

### **Лабораторная работа.**

#### **Расчет оценки защищенности помещения от утечки речевой информации по акустическому каналу**

#### **1. Учебные цели:**

Освоить метод оценки защищенности от утечки речевой информации по величине словесной разборчивости речи.

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

##### **Уметь:**

- анализировать и оценивать угрозы информационной безопасности объекта;
- составлять структурные схемы образования комплексных каналов утечки информации;
- применять методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства;
- анализировать исходные данные по аттестуемому объекту информатизации.

##### **Владеть:**

- методами расчета и инструментального контроля показателей технической защиты информации;
- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

#### **3. Перечень материально-технического обеспечения**

##### **Лабораторное оборудование и программное обеспечение:**

- Персональный компьютер Intel Core i5-2400 Box 3.10.
- Программа «Оценка разборчивости речи при прохождении звуковой волны через ограждающую конструкцию» (наименование исполняемого файла «Оценка.exe»). Программа реализована на языке C++ с использованием среды разработки Microsoft Visual Studio.

#### **4. Задание на исследование**

- Составить схему помещения с подробным описанием ограждающих конструкций.
- Выделить контрольные точки, для которых будет проводиться расчет оценки защищенности.
- Ознакомиться с алгоритмом программы расчета коэффициента разборчивости речи при прохождении акустического речевого сигнала через ограждающую конструкцию.
- Подготовить для проведения расчетов входные данные в соответствии с выбранной схемой исследуемого помещения.
- Провести вычисления в соответствии с пунктами раздела 6.

## 5. Краткие теоретические сведения

Оценка эффективности защиты помещения от утечек по речевому каналу утечки акустической информации включает в себя следующие этапы:

- составление схемы помещения и определение контрольных точек;
- расчет затухания звука при прохождении в воздухе до ограждающей конструкции и при прохождении через ограждающую конструкцию;
- определение значения разборчивости речи в определенной контрольной точке;
- оценка уровня защищенности помещения.

Для оценки защищенности каналов утечки информации используются два критерия: энергетический и смысловой.

Энергетическим показателем является распределение отношений «сигнал/шум», в октавных полосах частот в контрольных точках для нормированного энергетического спектра речевого сигнала.

Смысловым критерием является словесная разборчивость речи, т.е. относительное или процентное количество принятых специально тренированными слушателями (артикулянтами) слов из общего количества, переданных по тракту. На разборчивость речи в защищаемом помещении влияют характеристики: уровни речевого сигнала и шума; время реверберации; структура звуковых отражений.

В лабораторной работе используется метод оценки защищенности от утечки речевой информации по величине словесной разборчивости  $W$ . Суть этого метода заключается в следующем.

Энергетический спектр речи разбивается на  $N$  частотных полос, в общем случае произвольной ширины  $\Delta f = f_{Bi} - f_{Hi}$ , где  $f_{Bi}$  – верхнее значение частоты  $i$ -ой полосы;  $f_{Hi}$  – нижнее значение частоты  $i$ -ой полосы.

Для каждой  $i$ -ой частотной полосы инструментальными методами измеряются уровень сигнала  $L_{ci}$  (дБ) и уровень шума (помехи)  $L_{шиi}$  (дБ).

Далее для каждой  $i$ -ой частоты расчетным методом определяются:

- отношение «уровень речевого сигнала/уровень акустического шума (помехи):  $q_i = L_{ci} - L_{шиi}$ ;
- формантный параметр  $\Delta A_i$ , характеризующий энергетическую избыточность дискретной составляющей речевого сигнала в полосе, рассчитывается по формуле:

$$\Delta A_i(f_{срi}) = \begin{cases} \frac{200}{f^{0,43}} - 0,37, & \text{если } f \leq 1000 \text{ Гц,} \\ 1,37 - \frac{1000}{f^{0,69}}, & \text{если } f > 1000 \text{ Гц} \end{cases}$$

- весовой коэффициент полосы  $k_i$ , характеризующий вероятность наличия формант речи в данной полосе, по формуле:

$$k_i = k(f_{Bi}) - k(f_{Hi}),$$

где  $k(f_{Bi})$  и  $k(f_{Hi})$  – значения весового коэффициента для верхней  $f_{Bi}$  и нижней  $f_{Hi}$  граничных частот.

Значения весового коэффициента могут быть определены согласно выражению:

$$k(f) = \begin{cases} 2,57 \cdot 10^{-8} \cdot f^{2,4}, & \text{если } 100 < f \leq 400 \text{ Гц,} \\ 1 - 1,047 \cdot e^{-10^4 \cdot f^{1,18}}, & \text{если } 400 < f \leq 10000 \text{ Гц,} \end{cases}$$

- спектральный индекс артикуляции (понимаемости) речи  $R_i$ :

$$R_i = p_i \cdot k_i.$$

Значение коэффициента  $p_i$  вычисляется по формуле:

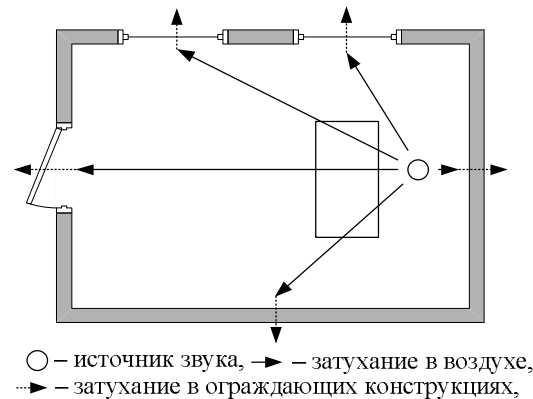
$$p_i = \begin{cases} \frac{0,78 + 5,46 \cdot e^{4,3 \cdot 10^{-3} \cdot (27,3 - |q_i - A_i|)^2}}{1 + 10^{0,1|q_i - A_i|}}, & \text{если } q_i \leq A_i \\ 1 - \frac{0,78 + 5,46 \cdot e^{4,3 \cdot 10^{-3} \cdot (27,3 - |q_i - A_i|)^2}}{1 + 10^{0,1|q_i - A_i|}}, & \text{если } q_i > A_i \end{cases}$$

Для общей частотной полосы спектра речевого сигнала следует определить:

- интегральный индекс артикуляции речи  $R = \sum_i R_i$ ;
- зависимость словесной разборчивости от интегрального индекса артикуляции речи:

$$W = \begin{cases} 1,54 \cdot R^{0,25} \cdot (1 - e^{-11 \cdot R}), & \text{если } R < 0,15 \\ 1 - e^{-\frac{11 \cdot R}{1 + 0,7 \cdot R}}, & \text{если } R \geq 0,15 \end{cases}$$

Для определения уровня звукового давления за пределами ограждающих поверхностей помещения необходимо провести расчет значений затухания звука в воздушной среде и в ограждающих конструкциях (рисунок 1).



**Рис. 1.** Схема типового помещения

Октавные уровни звукового давления  $L$  (Дб) в расчетных точках в помещениях с одним источником шума определяются по формуле:

$$L = L_p + 10 \lg \left( \frac{1}{S} \chi \Phi + \frac{4\Psi}{B} \right),$$

здесь  $L_p$  – октавный уровень звуковой мощности источника шума (человеческой речи)  $L_p$ ;  $S$  – площадь воображаемой поверхности правильной геометрической формы, окружающей источник шума по возможности равноудаленной от его поверхности и проходящей через расчетную точку,  $m^2$ ;  $\chi$  – коэффициент, учитывающий влияние ближнего акустического поля;  $\Phi$  – фактор направленности источника шума;  $\Psi$  – коэффициент, учитывающий изменение диффузности звукового поля в помещении;  $B$  – постоянная помещения.

Степень звукоизоляции ограждающей конструкции зависит от её конструкции и физических свойств материалов, из которых она изготовлена.

Степень звукоизоляции перегородки из однородного материала, в зависимости от веса её может быть определена как:

$$R = 13 \lg_{10} W + 14,$$

где  $W = \rho \cdot l$  – удельный вес перегородки ( $кг/м^2$ ).

Если перегородка состоит из нескольких слоев из различных материалов, то общий удельный вес можно рассчитать по формуле (в случае с небольшими различиями в удельной плотности):

$$W = \sum_{i=1}^n W_i .$$

Для выполнения заданий лабораторной работы используется программа расчета коэффициента разборчивости речи при прохождении акустического речевого сигнала через ограждающую конструкцию, разработанная на кафедре «Комплексная защита информации». Блок-схема программы включает в себя три основных блока:

- блок расчета затухания акустической волны в воздухе при прохождении от источника звука, до оцениваемой ограждающей конструкции;
- блок расчета индекса звукоизоляции ограждающей конструкции;
- блок расчета разборчивости речи.

Графическая схема алгоритма программы представлена на рисунке 2.

Входными параметрами для расчета являются:

- геометрические размеры помещения: длина ( $L$ ), ширина ( $D$ ), высота ( $H$ );
- расстояние от источника звука до ограждающей конструкции ( $r$ );
- толщина ограждающей конструкции;

- материал ограждающей конструкции;
- уровень акустического сигнала источника;
- уровень шумов в соседнем помещении.

Результатом расчета является значение коэффициента разборчивости речи, на основании которого формируется вывод об оценке защищенности исследуемого помещения.

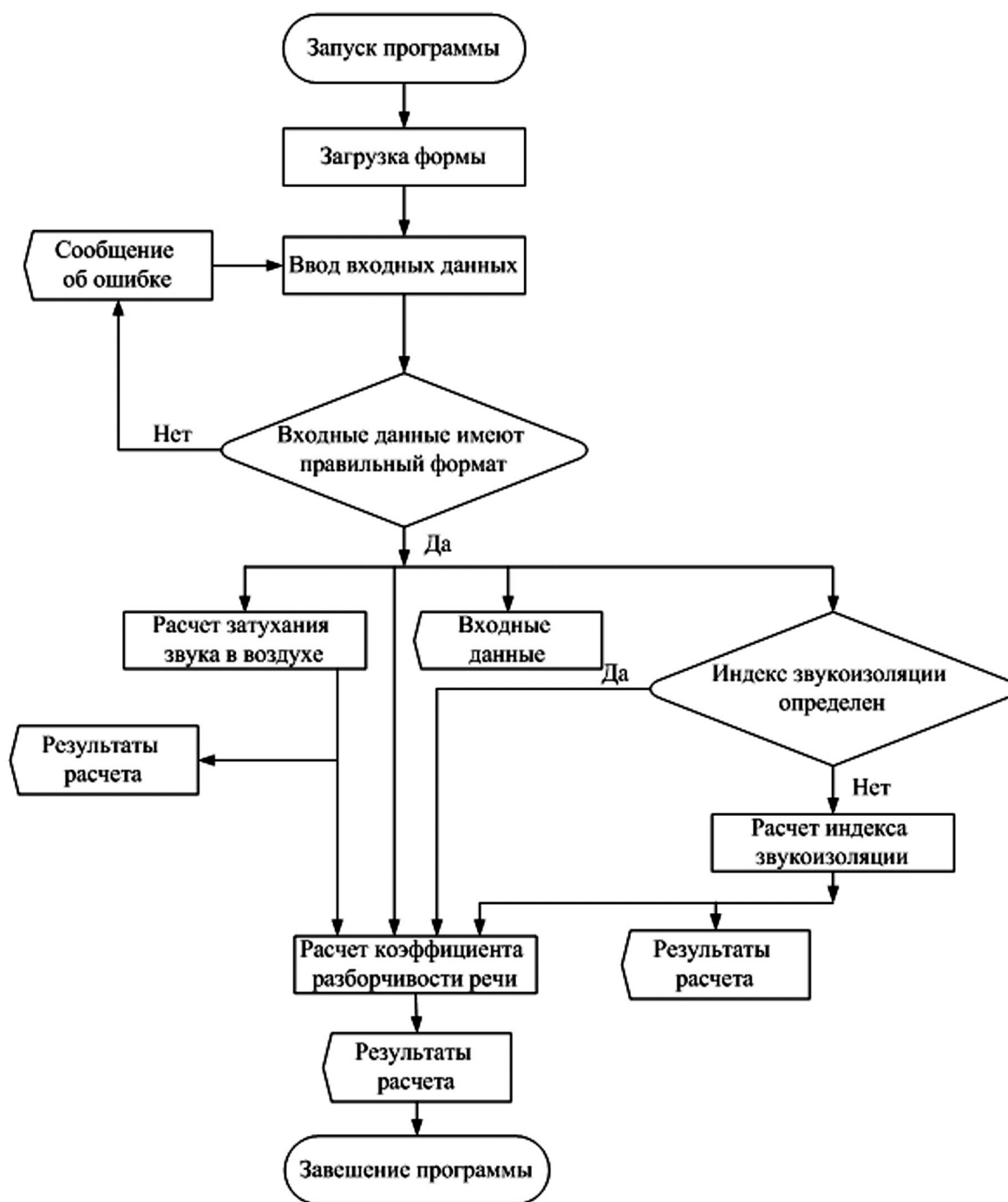


Рис. 2. Графическая схема алгоритма программы

## 6. Порядок выполнения лабораторной работы

1. Подготовить значения входных параметров для проведения расчетов в соответствии с планом защищаемого помещения: геометрические размеры помещения, расстояние от источника звука до контрольной точки, для которой производится оценка, свойства ограждающей конструкции.
2. Определить по согласованию с преподавателем местоположение контрольных точек для проведения расчетов.
3. Запустить приложение «Оценка.exe» (рис. 3)

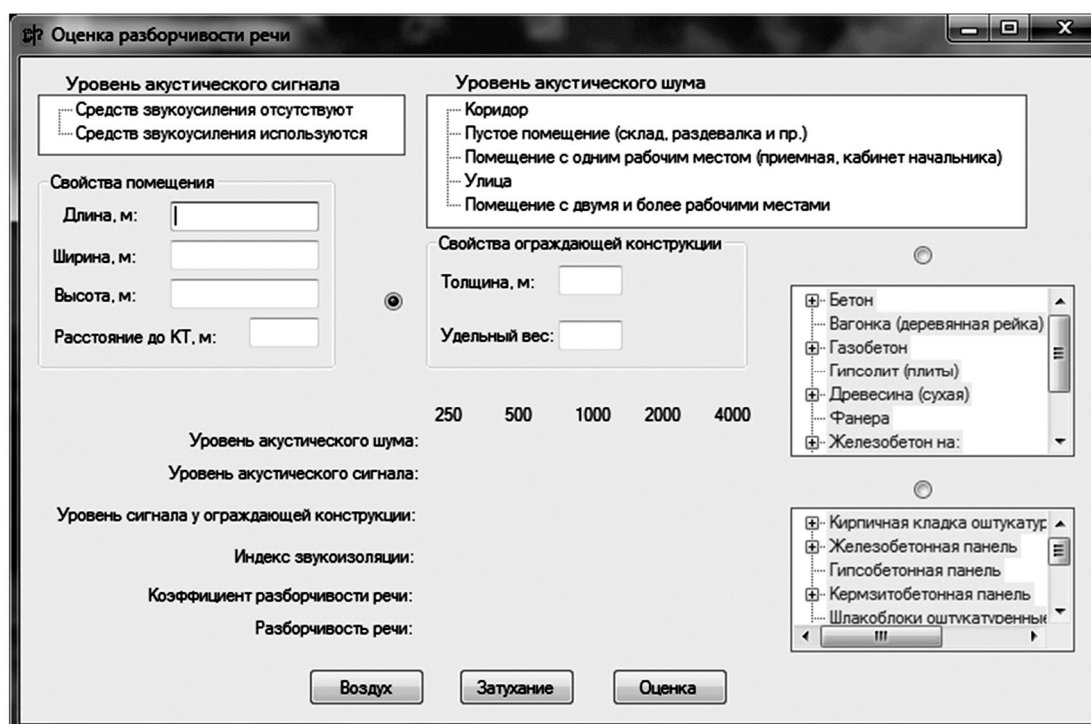


Рис. 3. Интерфейс программы расчета коэффициента разборчивости речи при прохождении акустического речевого сигнала через ограждающую конструкцию

4. Определить используются или нет в рассматриваемом помещении средства звукоусиления.
5. Для определения уровня акустического шума в смежном помещении, выбрать тип помещения.
6. Ввести значения геометрических размеров исследуемого помещения и расстояния от источника звука до контрольной точки, для которой производится оценка. Данные необходимо вводить без пробелов в формате «25,5», то есть, отделяя запятой целую часть от десятичной.
7. Ввести значения свойств ограждающей конструкции. В программе реализованы возможности ввода значений с клавиатуры или выбора из предлагаемого списка. Выбранному типу ограждающей конструкции сопоставляются значения индекса звукоизоляции для октавных полос.
8. Для проведения расчета значения затухания звука при прохождении от источника до ограждающей конструкции нажать кнопку «Воздух». Результаты расчета отобразятся в области вывода результатов.
9. Определить коэффициент разборчивости речи. Для определения коэффициента разборчивости речи необходимо нажать кнопку «Оценка». После нажатия в области отображения результатов появится значение коэффициента разборчивости и значение уровня разборчивости речи, оцениваемого по шкале: неудовлетворительная, приемлемая, хорошая и отличная. Область вывода всех полученных результатов приведена на рисунке 4.

|                                            | 250                      | 500   | 1000  | 2000  | 4000  |
|--------------------------------------------|--------------------------|-------|-------|-------|-------|
| Уровень акустического шума:                | 44                       | 43    | 39    | 36    | 32    |
| Уровень акустического сигнала:             | 66                       | 66    | 61    | 56    | 53    |
| Уровень сигнала у ограждающей конструкции: | 65,31                    | 65,24 | 60,12 | 54,95 | 51,73 |
| Индекс звукоизоляции:                      | 40                       | 42    | 48    | 54    | 60    |
| <b>Коэффициент разборчивости речи:</b>     | <b>0,439851526881044</b> |       |       |       |       |
| <b>Разборчивость речи:</b>                 | <b>Приемлемая</b>        |       |       |       |       |

рис. 4. Вид окна вывода результатов оценки защищенности

Примечание: в случае если ошибки при вводе данных, появляется сообщение «Повторите ввод». Оформить отчет по лабораторной работе с оценкой полученных результатов.



**7. Контрольные вопросы:**

1. Что называют каналом утечки речевой информации?
2. Дайте определение понятиям «интенсивность звука», «звуковое давление». Как взаимосвязаны данные величины?
3. Зачем вводится разбиение всего звукового диапазона на октавы?
4. Из каких этапов состоит порядок оценки эффективности защиты помещения от утечек по акустическому»
5. Поясните суть метода словесной разборчивости речи.
6. Что такое формантный параметр?
7. Как определяется зависимость словесной разборчивости от интегрального индекса артикуляции речи?

**Время на выполнение лабораторной работы – 1,5 часа.**

**Образовательная организация, авторы:** Омский государственный технический университет, Данилова О.Т., olga.danlot@yandex.ru

## СПЕЦИАЛИТЕТ 10.05.07 ПРОТИВОДЕЙСТВИЕ ТЕХНИЧЕСКИМ РАЗВЕДКАМ

**Дисциплина: Защита информации от несанкционированного доступа**

**Образовательная программа:** 10.05.07. Противодействие техническим разведкам.

**Дисциплина:** Защита информации от несанкционированного доступа.

### **Лабораторная работа.**

#### **Исследование эффективности работы сертифицированного механизма затирания информации на примере «Страж 3.0»**

##### **1. Учебные цели:**

Изучить принципы затирания и восстановления информации, снятия контрольных сумм, отработать навыки работы с программными средствами, осуществляющими эти процессы.

##### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

Уметь пользоваться специализированными программами, затирающими и восстанавливающими информацию, а также программами, предназначенными для снятия контрольных сумм. Понимать механизмы работы затирания и восстановления данных, снятия контрольных сумм.

##### **3. Перечень материально-технического обеспечения**

**Лабораторное оборудование и программное обеспечение:** ЭВМ с установленными на ней средствами защиты информации (СЗИ) «Страж 3.0» для затирания, «Recuva» для восстановления данных, «Terrier v3.0» для поиска информации на носителях по содержимому файла, «ФИКС-2.0.2» для получения контрольных сумм, флеш-накопитель.

##### **4. Задание на исследование**

Проверить работу механизма затирания по разным алгоритмам.

##### **5. Краткие теоретические сведения**

Все данные жёсткого диска сохраняются на кластерах – это небольшие «кусочки» информации ёмкостью от 1 байта до 4 мегабайт. Из кластеров строятся файлы. Первые биты каждого из них отмечаются нулём или единицей. Те электронные документы, в которых в атрибутах установлен «0», считаются как удалённые. По факту – они есть, но при первой же необходимости эта информация будет удалена, а на её место будет записана новая. Это делается для того, чтобы, во-первых, ускорить работу жёсткого диска. В противном случае процесс удаления файла занимал бы в десятки раз больше времени – он бы перезаписывался на пустой электронный документ (по времени это займёт столько же, сколько копирование данного файла в другую директорию этого же жёсткого диска), а во-вторых, такой алгоритм позволяет увеличить эксплуатационный ресурс жёсткого диска. Кластеры со временем повреждаются и при достижении критической отметки жёсткий диск может отказать.

Итого, даже после удаления файлов из корзины, данные остаются на жёстком диске (удалить их, используя программные средства, в принципе невозможно). Но при необходимости, на место этих файлов могут быть записаны новые данные, что повлечёт за собой частичную потерю удалённой информации, однако пока этого не произошло, такие файлы можно вернуть при помощи программы восстановления удалённых файлов с минимальным риском потери содержимого.

Чтобы безвозвратно удалить файл применяется затирание – многократное перезаписывание случайной информацией на те места диска, где хранился стираемый файл, чтобы исключить возможность его восстановления. Для этого используются специальные программы, использование которых и будет рассмотрено в данной лабораторной работе.

Для проверки соответствия восстановленного файла удалённому или затёртому сравнивают их контрольные суммы.

Контрольная сумма (хеш-сумма) – некоторое значение фиксированной длины, рассчитанное по набору данных путём применения определённого алгоритма – результат хеш-функции, используемой для вычисления контрольного кода – небольшого количества бит внутри большого блока данных, например, сетевого пакета или блока компьютерного файла. Значение контрольной суммы добавляется в конец блока данных непосредственно перед началом записи данных на какой-либо носитель информации или передачи по сети.

Так как при изменении исходного текста даже на один знак, полностью меняется результат хеш-функции, то впоследствии контрольная сумма проверяется для подтверждения целостности данных, быстрого сравнения двух наборов данных на неэквивалентность: с большой вероятностью различные наборы данных будут иметь разные контрольные суммы. Это может быть использовано, например, для обнаружения компьютерных вирусов.

Например, мы можем подать на вход 128-битной хеш-функции роман Льва Толстого в шестнадцатеричном виде или число 1. В результате на выходе мы в обоих случаях получим разные наборы псевдослучайных шестнадцатеричных цифр вида: «c4ca4238a0b923820dcc509a6f75849b».

В общем случае нет однозначного соответствия между исходными данными и хеш-кодом. Возвращаемые хеш-функцией значения менее разнообразны, чем значения входного массива. Случай, при котором хеш-функция преобразует несколько разных сообщений в одинаковые сводки, называется «коллизией». Вероятность возникновения коллизий довольно мала и используется для оценки качества хеш-функций.

Несмотря на своё название, контрольная сумма не обязательно вычисляется путём суммирования. Использование термина сумма связано с тем, что на заре цифровой связи при байтовых передачах информационными были 7 бит, а восьмой – контрольный – рассчитывался как младший разряд сложения информационных.

## **6. Порядок выполнения лабораторной работы (этапы)**

Начнём с программы восстановления удалённых файлов Recuva. Программа имеет простой графический интерфейс сходный с интерфейсом Windows. Перед началом работы создадим тестовый документ на Рабочем столе, например, с именем «СЕКРЕТНО.txt», напишем что-нибудь, например, «ВАЖНАЯ ИНФОРМАЦИЯ» и удалим его «мимо Корзины» (Shift + Delete), последовательность действий такая:

1. Запустить Recuva;
2. Next → Выбор типа файла, который требуется восстановить → Documents → Next → Выбор директории, в которой находился файл → In a specific location → Browse... → Рабочий стол → Next → Start;
3. Поставить галочку напротив файла с именем «СЕКРЕТНО.txt» → Recover... → Выбрать директории, в которую хотим сохранить восстановленный файл → Открыть файл и убедиться, что содержимое файла осталось тем же;
4. Теперь сделаем те же действия, но с включённым СЗИ.
5. Пуск → Страж NT → Настройки системы защиты → Гарантированная очистка всех удаляемых файлов → ОК;
6. Повторить пункты 1-3;
7. Сделать выводы о работе «Страж 3.0» и восстановителя Recuva.

Результат должен быть такой: При выключенном затирании Recuva успешно восстанавливает удалённый файл, при включённом затирании Recuva восстанавливает файл и его имя, но содержимое файла не отображается, текстовый редактор не может его открыть. СЗИ работает не совсем корректно.

Проведём аналогичную проверку работы на основе сравнения контрольных сумм. Для этого нам понадобится весь комплекс программ. На флеш-накопителе создадим уже известный текстовый файл. Примечание: стоит использовать флеш-накопитель малого объёма, так как скорость сканирования Terrier напрямую зависит от объёма. Страж выключен:

1. Запустить ФИКС → Выбрать алгоритм снятия контрольных сумм → Выбрать флеш-накопитель → Пуск → Посмотреть результат в папке \_#1 в директории ФИКС, файл .html → В колонке КС расположены контрольные суммы;
2. Удалить файл мимо Корзины с флеш накопителя;
3. Запустить Terrier → Выбрать объект сканирования, флеш-накопитель → Открыть окно подготовки поиска ключевых слов (Иконка лупы и окна) → Выбрать зелёный плюс → В строку данные ввести содержимое файла, «ВАЖНАЯ ИНФОРМАЦИЯ» → Начать поиск (при объёме 4 ГБ время поиска примерно 5 минут) → Отчёт → Выбрать место сохранения отчёта;
4. Восстановить файл с помощью Recuva;
5. С помощью ФИКС узнать контрольную сумму восстановленного файла;
6. Сделать выводы исходя из полученных результатов.

Результат должен быть такой: Контрольные суммы исходного файла и восстановленного должны быть разными. Теперь включить механизм затирания СЗИ и повторить п. 1-6. Сделать выводы. Результат: аналогично, контрольные суммы разные. Требования к отчёту:

7. Наличие контрольных сумм;
8. Скриншоты результатов поиска Terrier;
9. Текстовый отчёт результатов поиска Terrier;
10. Скриншоты процесса восстановления файлов с помощью программы Recuva;
11. Анализ полученных результатов.

Все полученные результаты желательно свести в таблицу для наглядности.

## **7. Контрольные вопросы**

1. Дайте определение затирания, обоснуйте его необходимость.
2. Основные принципы работы затирания.
3. Что такое контрольная сумма? Какую особенность контрольных сумм используют для индикации целостности переданного файла?
4. Могут ли два разных файла иметь одинаковую контрольную сумму? Объясните почему.
5. Что происходит при удалении файла в Корзину и из Корзины?
6. Почему хеш-сумма называется «суммой»?

**Время выполнения работы – 2 часа.**

**Образовательная организация:** МГТУ им. Н.Э. Баумана, кафедра ИУ10 «Защита информации», ассистент кафедры ИУ10 Холод Денис Александрович, dekhod@mail.ru.

## **Дисциплина: Информационно-телекоммуникационные системы**

**Образовательная программа:** 10.05.07 Противодействие техническим разведкам.

**Дисциплина:** Информационно-телекоммуникационные системы.

### **Лабораторная работа.** **Технологии виртуальных защищенных сетей VPN**

#### **1. Учебные цели:**

Изучить способы организации и настройки виртуальных частных сетей

#### **2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:**

##### **Уметь:**

- планировать мероприятия по защите информации в сети, исходя из известных угроз и финансовых возможностей предприятия.

##### **Владеть:**

- навыками работы с прикладными программными и аппаратными средствами защиты информации в компьютерных сетях.

#### **3. Перечень материально-технического обеспечения**

**Лабораторное оборудование и программное обеспечение:** Cisco Packet Tracer.

#### **4. Задание на исследование**

Организовать удаленное защищенное соединение между центральным офисом организации и филиалом посредством VPN туннеля

#### **5. Краткие теоретические сведения**

VPN – служит для организации доступа удаленных филиалов к центральному офису. Существует 3 основных способа доступа к локальным серверам:

1. **Static NAT** (пользователи филиала обращаются на “белый” публичный адрес роутера на определенный порт, они будут попадать на 1 из серверов);

2. **DMZ** (назначение серверам публичных адресов, т.е. вывести их в DMZ);

Минусы:

- Серверы становятся доступными из внешней сети абсолютно для всех (можно создать Access List, но это дополнительная трата временного ресурса).
- Необходимо, чтобы серверы оставались локальными и удаленный доступ к ним был только из локальной сети филиала, поэтому используем VPN:

3. **VPN** – способ организации локальной сети через публичное соединение, т.е. Интернет. При организации VPN между филиалами создаем логическое соединение (“туннель” между 2-мя офисами – “2 роутера соединены напрямую”). Таким образом, если пользователь филиала обращается к сети центрального офиса, то трафик логически соединяется в “туннель”, на самом деле, физически трафик идет через сеть Интернет. Данный трафик необходимо защищать.

При развертывании VPN используют различные протоколы защиты.

Например:

1. IPsec Site-to-Site VPN,

2. IPsec RA VPN, где

IPsec – набор протоколов для обеспечения защиты данных, Site-to-Site – объединение 2-ух сторон (подключение нескольких сетей), RA VPN (Remote Access) – удаленный доступ пользователей (подключение одного пользователя к корпоративной сети).

Процесс построения VPN соединения состоит из 2-ух этапов:

1. Две стороны по протоколу IKE договариваются о параметрах технического соединения, если они аутентифицируют друг друга, то поднимается защищенный ISAKMP Tunnel, по которому стороны будут договариваться об основном IPsec туннеле;

2. Две стороны договариваются о параметрах IPsec туннеля, после этого поднимается сам туннель, по которому будут идти уже пользовательские данные в зашифрованном виде.

#### **6. Порядок выполнения лабораторной работы (этапы)**

##### **1. Построение схемы сети**

Настроим схему из трех подсетей, двух внутренних (подсеть центрального офиса и подсеть филиала) и одну внешнюю, для связи удаленных участков сети. По внешней сети проложим vpn-туннель. Все сетевые устройства располагаются на логическом пространстве Cisco Packet Tracer, представленном на рисунке 1.

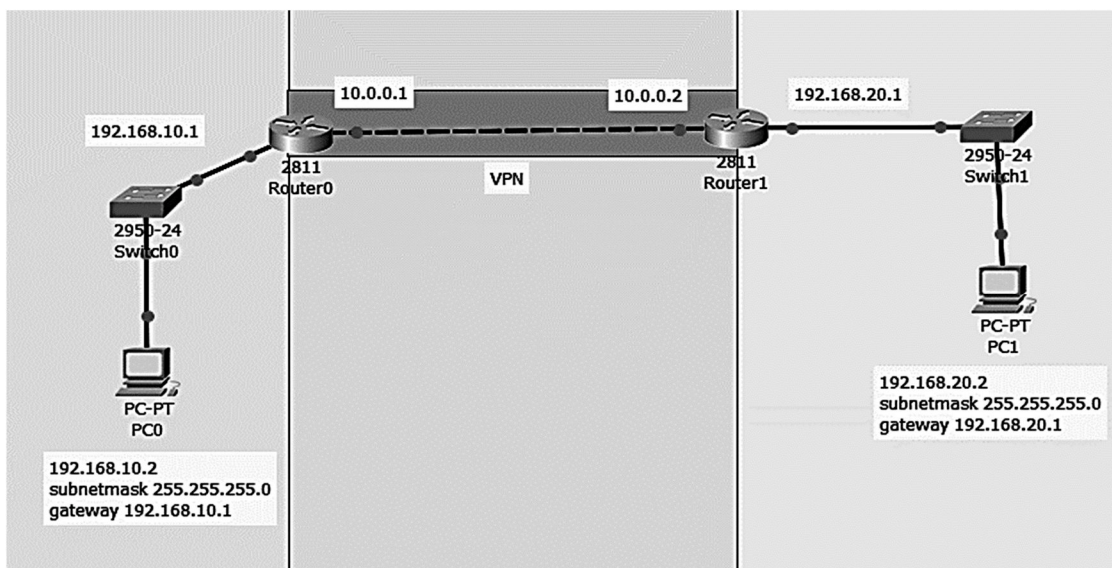


Рис. 1. Логическая схема компьютерной сети

## 2. Адресация всех узлов подсетей

Настроим компьютер подсети 192.168.10.0. Для каждого узла необходимо назначить IP адрес и маску, согласно своей подсети. У каждого узла в окне настройки выбрать вкладку Desktop и пункт IP Configuration, представленный на рисунке 2.

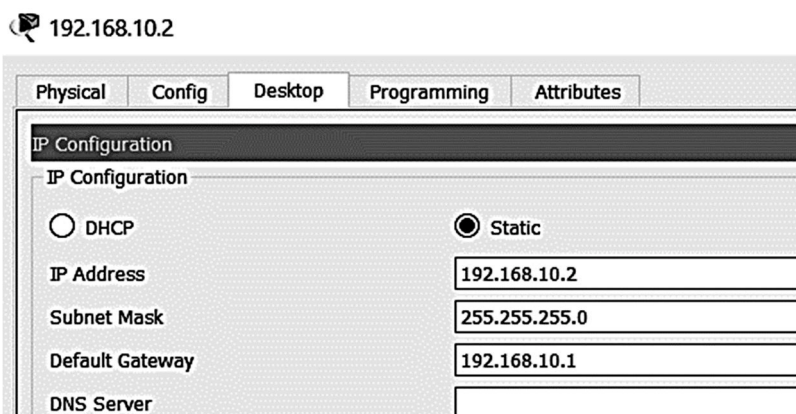


Рис. 2. Назначение IP адреса и маски для узла сети

В соответствующих пунктах прописать IP адрес узла, маску сети, IP адрес шлюза по умолчанию. Последовательность действий по назначению IP адресов необходимо повторить для всех узлов каждой подсети, таким образом, аналогично настраиваем компьютер подсети 192.168.20.0.

Согласно Рис. 1, необходимо задать IP адреса и роутерам, указав в интерфейсах адреса и маски подсети.

## 3. Настройка протокола маршрутизации

Настроим протокол RIP на Router0, посредством диалогового окна. Для этого:

1. Выбирается вкладка Config
2. Выбирается пункт RIP
3. Вводятся адреса подсетей, между которыми нужна связь
4. Нажимается кнопка Add.

Аналогичная настройка протокола маршрутизации RIP реализуется на Router1.

## 4. Настройка VPN.

При развертывании VPN туннеля необходимо решить следующие задачи:

5. Включение функций безопасности
6. Настройка параметров IPsec на Роутере 0
7. Настройка параметров IPsec на Роутере 1
8. Проверка работы VPN IPsec

Для этого на Router0, выбирается вкладка CLI и посредством ввода команд настраиваются следующие функции безопасности:

```
Router(config)#crypto isakmp policy 10
//выбираем политику шифрования
Router(config-isakmp)#authentication pre-share
//метод аутентификации пользователей pre-share
Router(config-isakmp)#hash sha
//алгоритм криптографического хеширования
Router(config-isakmp)#encryption aes 256
//алгоритм шифрования aes 256
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#exit
```

```
Router(config)#crypto isakmp key toor address 10.0.0.2
//настраиваем ключ аутентификации и задаем IP-адрес пира – IP-адрес внешнего интерфейса роутера на филиале – 10.0.0.2).
```

```
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
// TSET – имя, esp-aes – алгоритм шифрования, esp-sha-hmac – алгоритм хэширования
```

```
Router(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
//методы шифрования и аутентификации
```

```
Router(config)#access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
//определяется, какой трафик будет участвовать в vpn (трафик, который поступает из Центрального офиса из сети 192.168.10.0 в сеть 192.168.20.0 – филиала)
Router(config)#crypto map CMAP 10 ipsec-isakmp
//определяется карта шифрования
```

```
Router(config-crypto-map)#set peer 10.0.0.2
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#set transform-set TSET
Router(config-crypto-map)#exit
// указывается пир, т.е. IP-адрес внешнего интерфейса роутера филиала; указываются параметры IPsec туннеля и указывается, какой трафик необходимо шифровать (указывая Access List)
```

```
Router(config)#interface fa0/1
Router(config-if)#crypto map CMAP
Router(config-if)#do wr
// привязка криптокарты к интерфейсу (внешнему)
```

Для Router1 используется аналогичный алгоритм, заменив адрес 10.0.0.2 на адрес 10.0.0.1, а также последовательность адресов в access-list.

```
Router(config)#access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
```

Настроив VPN, необходимо, посредством команды ping, убедиться, что пакеты передаются и таким образом задать интересующий трафик.

Чтобы проверить работу VPN туннеля, т.е. наличие шифрования сообщений, необходимо в консоли одного из роутеров набрать команду:

```
Router#show crypto ipsec sa
```

В результате выполнения команды определяется количество инкапсулированных, зашифрованных, деинкапсулированных и дешифрованных пакетов. Так как это количество не равно 0, VPN работает, пакеты шифруются:

```
current_peer 10.0.0.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
```

**7. Контрольные вопросы:**

1. В чем суть организации VPN туннеля для локальной сети?
2. Этапы построения VPN соединения
3. Какие параметры необходимо указать при настройке ISAKMP?
4. Для чего используется AccessList?

**Время на выполнение лабораторной работы – 2 часа.**

**Образовательная организация, авторы, эл почта:** МГТУ им. Н. Э. Баумана, ИУ10, доцент Федорова Вероника Анатольевна, fedorovava@bmstu.ru





**МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ  
XXII ПЛЕНУМА ФУМО ВО ИБ**

**СБОРНИК МЕТОДИЧЕСКИХ УКАЗАНИЙ  
ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ  
ПО ДИСЦИПЛИНАМ БАКАЛАВРИАТА  
И СПЕЦИАЛИТЕТА  
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Авторская редакция

Технический редактор – А.С. Семенов  
Компьютерная верстка – И.И. Фоменко  
Дизайн обложки – М.Б. Жаренко

Подписано в печать 01.10.2018  
Бумага «Снегурочка»  
Печ. л. 19,6  
Усл. печ. л. 18,2  
Уч.-изд. л. 16,4

Формат 60×84 <sup>1</sup>/<sub>8</sub>  
Печать трафаретная  
Изд. № 967  
Тираж 130 экз.  
Заказ № 1951

ООО «Издательский Дом – Юг»  
350072, г. Краснодар, ул. Зиповская 9, литер «Г», оф. 41/3  
тел. +7(918) 41-50-571

e-mail: [id.yug2016@gmail.com](mailto:id.yug2016@gmail.com)

Сайт: <http://id-yug.com>