МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

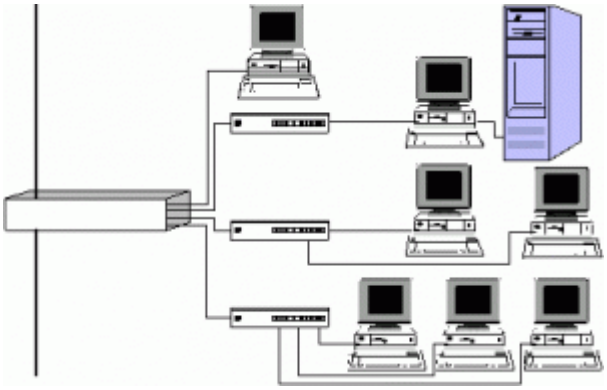
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Воронежский государственный технический университет»

Кафедра автоматизированных и вычислительных систем

ТЕХНОЛОГИИ ПРОГРАММНОЙ ЗАЩИТЫ ДАННЫХ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению лабораторных работ
по дисциплине «Технологии защиты Web-контента»
для студентов направления 38.03.05 «Бизнес-информатика»
(профиль «Информационные системы в бизнесе»)
очной и заочной форм обучения



Воронеж 2022

УДК 681.3.06(07)
ББК 32.973

Составители:
канд. техн. наук Т. И. Сергеева,
канд. техн. наук М. Ю. Сергеев,
асс. М.А. Белых

Технологии программной защиты данных: методические указания к выполнению лабораторных работ по дисциплине «Технологии защиты Web-контента» для студентов направления 38.03.05 «Бизнес-информатика» (профиль «Информационные системы в бизнесе») очной и заочной форм обучения / ФГБОУ ВО «Воронежский государственный технический университет»; сост.: Т. И. Сергеева, М. Ю. Сергеев. Воронеж: Изд-во ВГТУ, 2022. 32 с.

Цель методических указаний - освоение программных средств защиты веб-приложений, выработка умений и навыков настройки программных средств для защиты данных.

Методические указания содержат теоретические сведения и практические задания для выполнения лабораторных работ.

Предназначены для проведения лабораторных работ по дисциплине «Технологии защиты Web-контента» для студентов 4 и 5 курсов очной и заочной форм обучения.

Методические указания подготовлены в электронном виде и содержатся в файле TZWK_LR.pdf.

Ил. 15. Табл. 9. Библиогр.: 5 назв.

УДК 681.3.06(07)
ББК 32.973

Рецензент – В. В. Сафронов, канд. техн. наук, доцент кафедры автоматизированных и вычислительных систем ВГТУ

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

1. ЛАБОРАТОРНАЯ РАБОТА № 1
РАЗРАБОТКА ПРЕЗЕНТАЦИИ ПО ТЕМЕ «ОБЗОР ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ»
1.1. Общие сведения

Цель работы – ознакомление с основными направлениями защиты веб-приложений и с используемыми программными средствами защиты.

Существуют следующие технологии защиты веб-приложений:

- блокировка атак;
- сигнатурный анализ;
- поведенческий и репутационный анализ
- формирование эталонной (позитивной) модели безопасности (машинное обучение);
- защита идентификаторов сессий;
- специальные механизмы защиты (не сигнатурные);
- формирование правил пользователя (пользовательские правила);
- применение специализированных программных средств Firewall.

Средства защиты веб-приложений применяют на этапе разработки и на этапе эксплуатации.

На этапе разработки — это различные инструменты тестирования безопасности.

На этапе эксплуатации веб-приложений применяют следующие средства защиты:

- системы предотвращения вторжений, межсетевые экраны следующего поколения (Next Generation Firewall, сокращенно NGFW);
- средства фильтрации трафика прикладного уровня, специально ориентированные на веб-приложения (Web Application Firewall, сокращенно — WAF).

WAF может быть реализован как облачный сервис, агент на веб-сервере или специализированное железное или виртуальное устройство.

Применение Web Application Firewall традиционно считается наиболее эффективным подходом к защите веб-ресурсов.

Наиболее простые способы защиты веб-контента следующие:

- проверка сайта на уязвимости;
- использование защищенных протоколов передачи данных;
- применение программного обеспечения, включающего функции защиты данных.

Проверка сайта на уязвимость может осуществляться с помощью бесплатных инструментов-приложений:

- OpenVAS сканирует локальные сети на уязвимости;
- OWASP Xenotix XSS Exploit Framework проверяет сайт на XSS-уязвимость, – возможность внедрения в веб-страницу вредоносного кода, по-

хищающего данные аккаунтов пользователей и иную информацию. Код внедряется через уязвимости на сервере или устройстве пользователя;

- Approof от Positive Technologies изучает конфигурацию веб-приложения и находит лишний или вредоносный код.

Вторым по популярности способом защитить данные пользователя после идентификации является применение защищенного протокола передачи данных HTTPS. Hyper Text Transfer Protocol Secure защищает информацию о пользователе веб-приложения при помощи шифрования трафика. Он обеспечивает сохранение конфиденциальности и целостности информации, не допуская утечку или подмену данных.

Необходимо также регулярно обновлять используемое программное обеспечение.

1.2. Задания для лабораторной работы № 1

Задание

Разработать презентацию по предложенной теме.

Презентация должна описать:

- основные угрозы информационной безопасности в сети Интернет;
- основные направления защиты веб-приложений;
- средства защиты веб-приложений;
- обзор программных продуктов из группы Web Application Firewall (WAF);
- выбрать программный продукт для обзора из списка: PT Application Firewall (Positive Technologies), Wallarm, Barracuda Web Application Firewall, Citrix NetScaler AppFirewall, F5 BIG-IP Application Security Manager;
- принципы работы WAF;
- Российский рынок WAF.

Презентация должна содержать иллюстративный материал.

Вариант текста для оформления презентации необходимо получить у преподавателя.

Отчет

Отчет – это разработанная презентация.

2. ЛАБОРАТОРНАЯ РАБОТА № 2 НАСТРОЙКА ЗОН БЕЗОПАСНОСТИ СРЕДСТВАМИ ОПЕРАЦИОННЫХ СИСТЕМ

2.1. Общие сведения

Цель работы – изучение основных направлений настройки операционных систем и браузеров для обеспечения информационной безопасности.

Web-обозреватель делит Интернет на зоны, чтобы можно было назначить требуемый уровень защиты каждому веб-узлу. Перед просмотром и загрузкой веб-сайтов будет проверяться соответствие сайта заданной зоне безопасности.

Имеется четыре категории зон.

Местная зона безопасности. Содержит любые адреса узлов, расположенных в сети организации. По умолчанию для этой зоны установлен средний уровень защиты.

Зона надежных узлов. К ней относят узлы, которым доверяют и с которых загружают информацию и программы без опасения повреждения собственных данных на компьютере. По умолчанию для этой зоны защита отсутствует.

Зона ограниченных узлов. К ней относят узлы, которым не доверяют и считают небезопасным загружать с них информацию или запускать программы. По умолчанию для этой зоны назначают высокий уровень защиты.

Зона Интернета. К этой зоне относится все, что не имеет отношения к конкретному компьютеру или внутренней сети организации. По умолчанию для этой зоны назначен средний уровень защиты.

Для каждой зоны можно изменить и настроить уровень защиты.

Настройка браузера Internet Explorer для безопасного использования ресурсов Web-серверов реализуется через Панель управления, Свойства обозревателя.

Вкладка «Общие» позволяет настроить домашнюю страницу, осуществить настройки параметров поиска, настроить вкладки для отображения веб-страниц.

Вкладка «Содержание» настраивает контроль за разрешенным для просмотра веб-содержимым, ограничения доступа к информации, получаемой из Интернета, сертификаты для шифрования подключений и удостоверения личности, определяют каналы и веб-фрагменты предоставления содержимого веб-узлов.

Вкладка «Безопасность» позволяет выбрать зону для настройки ее параметров безопасности, установить уровень безопасности для этой зоны, включить защищенный режим работы.

Вкладка «Подключения» обеспечивает настройки прокси-сервера и параметров локальной сети.

Вкладка «Программы» определяет программу обзора по умолчанию, настройки веб-обозревателя, программы поддержки служб Интернета.

Вкладка «Конфиденциальность» позволяет определить уровень безопасности для зон Интернет.

2.2. Задания для лабораторной работы № 2

Задание

Выполнить следующие действия:

- осуществить настройку уровня защиты для зоны безопасности Интернет;

- осуществить настройку уровня защиты для зоны ограниченных узлов;

- добавить web-узел в список зоны с ограничением доступа;
- осуществить ограничение доступа к информации, получаемой из Интернета;
- запретить посещение нежелательных web-страниц, не имеющих оценок;
- оформить отчет.

Отчет

Отчет должен содержать:
- титульный лист;
- задание;
- инструкции по выполнению предложенных заданий;
- скриншоты окон настройки параметров по каждому заданию.

3. ЛАБОРАТОРНАЯ РАБОТА № 3 НАСТРОЙКА БЕЗОПАСНОСТИ ПОЧТОВОЙ СЛУЖБЫ

3.1. Общие сведения

Цель работы – изучение способов настройки безопасности почтовой службы.

Основные протоколы передачи почты обычно не осуществляют надежной аутентификации, что позволяет легко создать письма с фальшивыми адресами. Ни один из этих протоколов не использует криптографию, которая могла бы гарантировать конфиденциальность электронных писем.

Заголовки и содержимое электронной почты передаются в чистом виде. В результате содержимое сообщения может быть прочитано или изменено в процессе передачи его по интернету. Заголовок может быть модифицирован, чтобы скрыть или изменить отправителя или перенаправить сообщение.

Существует также такой вид угрозы как почтовая бомба. Почтовая бомба – это атака с помощью электронной почты. Атакуемая система переполняется письмами до тех пор, пока не выйдет из строя.

Возможны также нежелательные отправители писем.

Типовые действия по защите электронной почты:
- определение почтового адреса нежелательного отправителя;
- установка фильтров для анализа содержания входящей почты;
- установка фильтра на темы писем входящей почты;
- определение правил обработки входящих писем с целью анализа недопустимых слов;
- блокировка сообщений с определенным адресом.

Чтобы определить **адрес нежелательного отправителя электронной почты** выполняют следующие действия:
- запустить почтового клиента MS Outlook Express,
- выбрать папку Входящие,
- выделить сообщение, вызвать контекстное меню, выбрать Свойства, вкладка Подробности,

- изучить заголовок письма.

В заголовке письма записывается весь путь его прохождения через цепь почтовых серверов. В самом последнем абзаце, начинающимся словом Received, находится адрес первого сервера, на который отправлено письмо.

Установка фильтров для анализа содержания входящей почты осуществляется следующим образом:

- запустить почтового клиента MS Outlook Express,
- Сервис, Правила для сообщений, Почта,
- в окне «Выбрать условие для данного правила» установить флажок «Искать сообщения, содержащие заданные слова»,
- в окне «Выберите действия для данного правила» установить флажок Удалить,
- в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова».

В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить. В этом же окне щелкнуть по кнопке Параметры, в открывшемся окне «Условия для правила» активировать переключатель «Имеются указанные слова» и щелкнуть по кнопке ОК, ОК.

Установка фильтра для анализа темы писем входящей почты реализуется следующим образом:

- запустить почтового клиента MS Outlook Express,
- Сервис, Правила для сообщений, Почта,
- в окне «Выбрать условие для данного правила» установить флажок «Искать сообщения, содержащие заданные слова в поле «Тема»,
- в окне «Выберите действия для данного правила» установить нужный флажок,
- в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова».

В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить. В этом же окне щелкнуть по кнопке Параметры, в открывшемся окне «Условия для правила» активировать переключатель «Имеются указанные слова» и щелкнуть по кнопке ОК, ОК.

Создание правил обработки входящих почтовых сообщений, согласно которому сообщения, включающие определенные слова, удаляются выполняют следующим образом:

- запустить почтового клиента MS Outlook Express,
- Сервис, Правила для сообщений, Почта,
- в окне «Выбрать условие для данного правила» установить флажок «Искать сообщения, содержащие заданные слова»,
- в окне «Выберите действия для данного правила» установить флажок Удалить, в списке «Описание правила» щелкнуть по ссылке «содержащие заданные слова».

В раскрывшемся окне «Ввод ключевых слов» ввести ключевые слова и щелкнуть по кнопке Добавить. В этом же окне щелкнуть по кнопке Параметры, в открывшемся окне «Условия для правила» активировать переключатель «Имеются указанные слова» и щелкнуть по кнопке ОК, ОК.

Блокировку сообщений с определенным адресов выполняют следующим образом:

- запустить почтового клиента MS Outlook Express,
- Сервис, Правила для сообщений, Список блокируемых отправителей,
- во вкладке «Заблокированные отправители» в окне «Правила для сообщений» щелкнуть по кнопке «Добавить»,
- в окне «Добавить отправителя» ввести адрес электронной почты, который надо заблокировать и установить флажок «Почтовые сообщения», ОК.

3.2. Первое задание для лабораторной работы № 3

Задание

Выполнить следующие действия:

- определить адрес отправителя электронной службы с помощью почтового клиента MS Outlook Express;
- установить фильтр на анализ содержания входящей почты для удаления сообщения;
- установить фильтр на тему входящей почты;
- создать правило обработки входящих почтовых сообщений, согласно которому сообщения, включающие определенные слова, удаляются;
- заблокировать сообщения, получаемые от отправителя с определенным адресом;
- оформить отчет.

Отчет

Отчет должен содержать:

- титульный лист;
- задание;
- инструкции по выполнению предложенных заданий;
- скриншоты окон настройки параметров по каждому заданию.

3.3. Защита e-mail от спама через настройки фильтра в Яндекс.Почте

Для перехода в настройки фильтра входящих сообщений щелкают по ссылке с названием **«Настроить»** в левом меню сайта Яндекс.Почты, а затем переходят во вкладку «**Правила обработки почты»**. Окно настроек приведено на рис. 1.

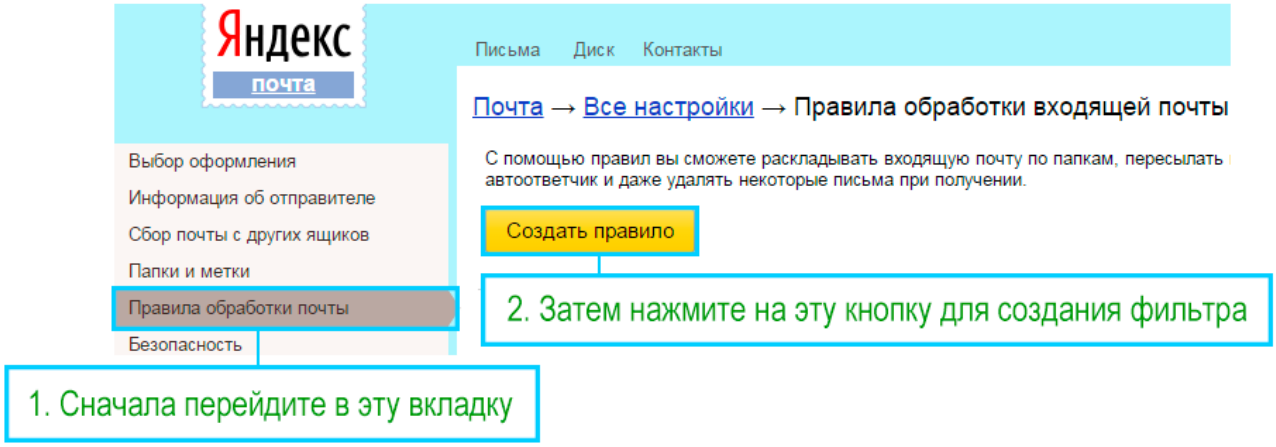


Рис. 1. Окно настроек фильтра

Затем нажимают кнопку **“Создать правило”.**

Создание фильтра от спама преполагает реализацию ряда действий.

1. Сначала необходимо задать условие определения соответствующих писем (рис. 2).

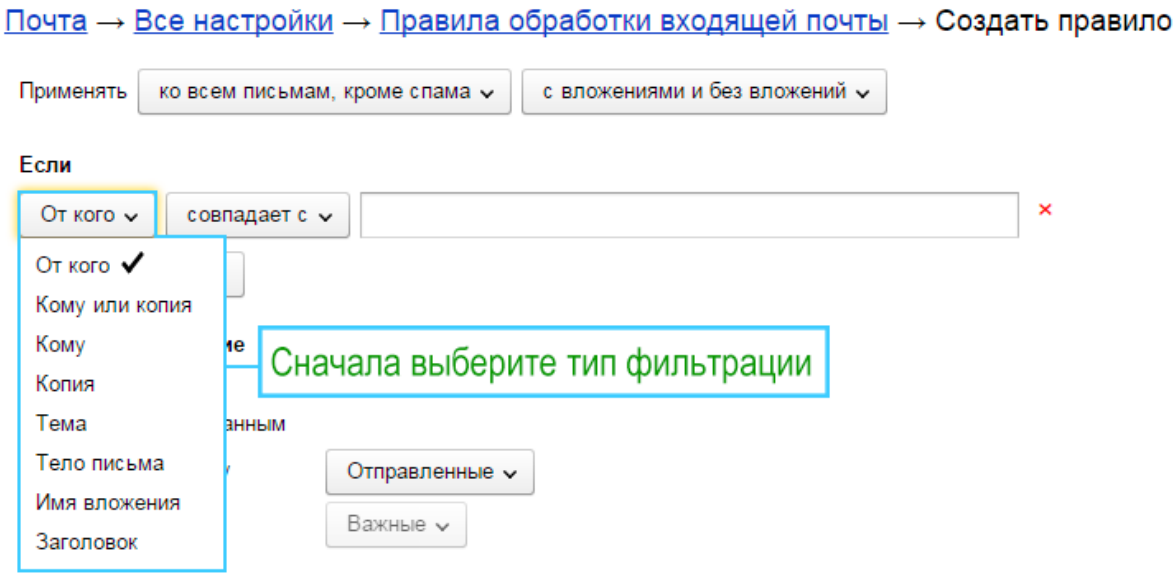


Рис. 2. Выбор типа фильтрации

Яндекс предлагает несколько вариантов сортировки писем: по отправителю, названию темы, заголовку, части содержания сообщения.

2. Задание писем для фильтрации (рис. 3).

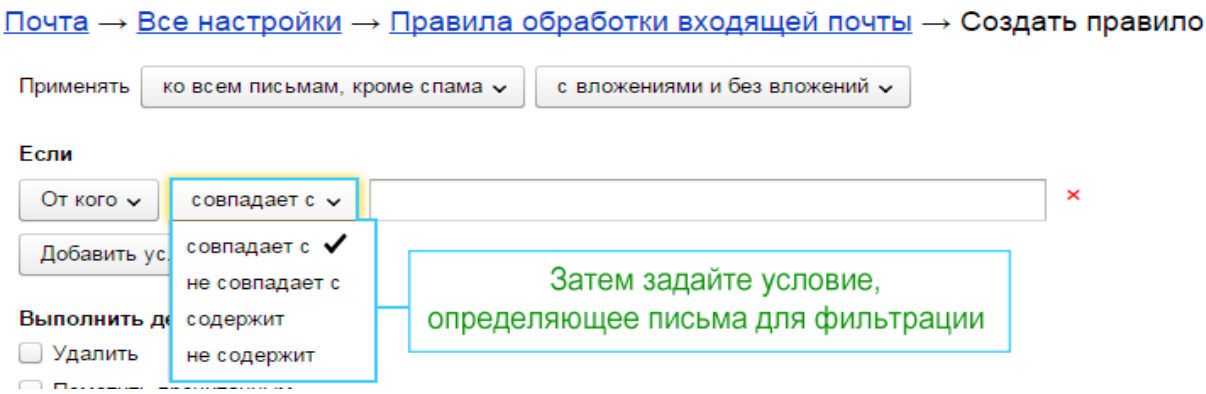


Рис. 3. Окно задания писем для фильтрации

Во втором поле выбирают условие фильтрации: **содержит/не содержит текст (или его часть)**, указанный в третьем поле.

3. Задание условия фильтрации (рис. 4).

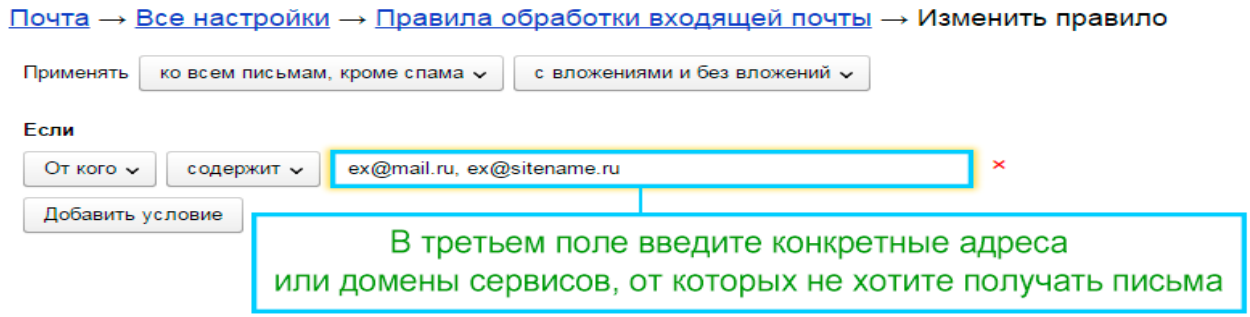


Рис. 4. Окно задания условий фильтрации

Например, если необходимо отфильтровать сообщения от определённого адреса, то в первом поле выбирают «**От кого»**, затем во втором поле выбирают критерий «**Содержит»**, а в третьем поле вводят адреса или домены сервисов, от которых не хотят получать письма.

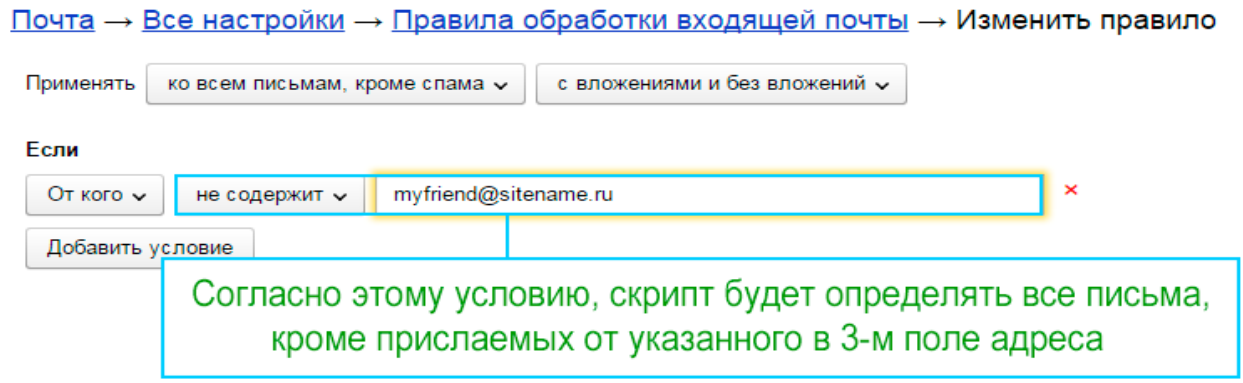


Рис. 5. Пример задания условия

3. Создание нескольких условий фильтрации

Для создания нескольких условий фильтрации щелкают по кнопке «**Добавить условие»**, создают его, а затем выбирают критерий, согласно которому будут фильтроваться сообщения – если выполняются оба условия или хотя бы одно из них (рис. 6). Затем выбирают действия, которые совершит робот сервиса после определения писем, удовлетворяющих заданному условию фильтрации. В примере отмечена опция перемещения этих писем в папку со спамом.

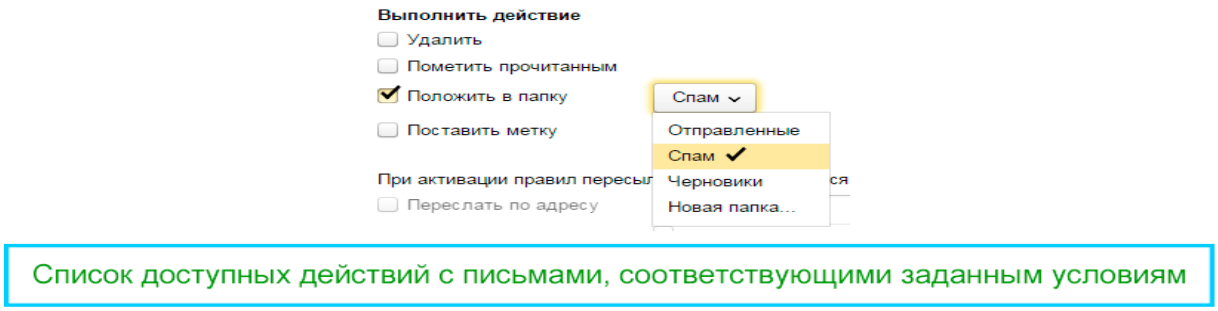


Рис. 6. Задание дополнительных условий фильтрации

4. Сохранение настроек фильтра

Для сохранения настроек фильтра нажимают кнопку «**Создать правило».** Окно сохранения установленных настроек фильтра приведено на рис. 7.

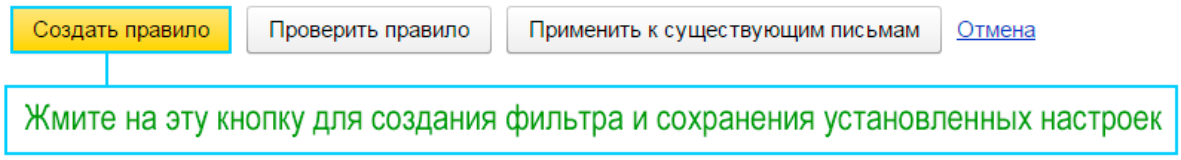


Рис. 7. Сохранение установленных настроек

5. Редактирование или удаление фильтра

Чтобы отредактировать настройки созданного правила, переходят в раздел «**Правила обработки почты»,** в котором осуществляют редактирование, удаление, включение/отключение фильтров (рис. 8).

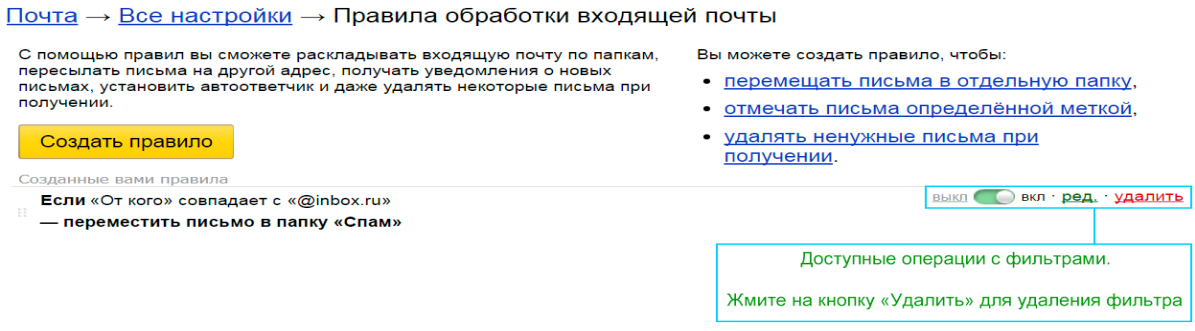


Рис. 8. Окно редактирования фильтров

3.4. Второе задание для лабораторной работы № 3

Задание

Осуществить настройку фильтров в Яндекс.Почте.

- задать разные типы фильтрации (три примера);
- задать разные условия выбора писем для фильтрации;
- задать конкретные адреса или домены сервисов, письма которых не будут приниматься;
- определить действия с неугодными письмами;
- сохранить произведенные настройки;
- продемонстрировать преподавателю выполненные настройки;
- оформить отчет;
- удалить настроенные фильтры.

Отчет

Отчет должен содержать:

- титульный лист;
- задание;
- инструкции по выполнению предложенных заданий;
- скриншоты окон настройки фильтров.

4. ЛАБОРАТОРНАЯ РАБОТА № 4
АНТИВИРУСНЫЕ ПРОГРАММЫ

4.1. Общие методические указания по выполнению лабораторной работы № 4

Цель работы – проведение профилактических антивирусных мероприятий.

Основными видами компьютерных вирусов являются загрузочные, файловые, загрузочно-файловые и полиморфные вирусы.

Для обнаружения, удаления компьютерных вирусов и защиты от них разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы.

Различают следующие виды антивирусных программ:

- программы-детекторы;
- программы-доктора;
- программы-ревизоры;
- программы-фильтры;
- программы–вакцины.

В настоящее время существует большое количество различных программных средств борьбы с компьютерными вирусами. Это программы Aidtest, DrWeb, Adinf, а также антивирус Касперского.

Антивирус Касперского использует все современные типы антивирусной защиты: антивирусные сканеры, мониторы, поведенческие блокираторы и ревизоры изменений. Он поддерживает все самые популярные операционные системы, почтовые шлюзы, межсетевые экраны, web-серверы и контролирует все возможные пути проникновения вирусов на компьютер пользователя, включая Интернет, электронную почту, мобильные носители информации и т.д.

Знакомство с антивирусной программой Касперского можно осуществить на сайте http://www.viruslist.com/viruslist.asp.

В разделе «Методы обнаружения и удаления компьютерных вирусов» можно изучить тему «Методика использования антивирусных программ».

Программа Kaspersky Anti-Virus Control Center содержит четыре закладки.

Закладка «Задачи» служит для управления задачами проверки на наличие вирусов, просмотра статистики их работы и уведомлений.

Закладка «Компоненты» предназначена для управления компонентами пакета Антивирус Касперского и создания новых задач сканирования.

Закладка «Параметры» предназначена для настройки параметров работы программы.

На закладке «Карантин» представлено содержимое локального карантина со списком файлов, отправленных на карантин.

Программа Kaspersky Anti-Virus Scanner работает с четырьмя категориями.

Категория «Объекты» позволяет задать область сканирования, подлежащие сканированию объекты, правила обработки инфицированных объектов.

Категория «Параметры» позволяет задать общие настройки.

Категория «Настройки» задает специальные настройки программы.

Категория «Статистика» позволяет просматривать результаты работы программы в таблице.

Для сканирования отмеченных в окне объектов на наличие вирусов выбирают в меню «Сканирование» команду «Начать сканирование».

Щелкнув по категории «Статистика», просматривают результаты сканирования на наличие вирусов.

Для просмотра подробного отчета о результатах сканирования щелкают кнопку «Показать отчет» в панели инструментов.

Для запуска обновления антивирусных баз выбирают в меню «Сервис» пункт «Обновить антивирусные базы».

Для изменения настройки сканера щелкают на ярлыке категории «Настройка». После этого в правой части окна откроется список опций настройки, которые можно включать/выключать.

Для изменения параметров щелкают на ярлыке категории «Параметры» и в правой части окна задают параметры записи результатов сканирования в файл, настройки переименования зараженных файлов и уровень приоритета сканирования.

В антивирусный пакет программ Касперского входит антивирусная программа-ревизор диска KAV Inspector.

Данная программа сохраняет основные данные о диске компьютера в таблице, содержащей образы Master-Boot и Boot-секторов, список номеров сбойных кластеров, схему дерева каталогов и информацию обо всех контролируемых файлах. Программа проверяет диски на наличие изменений содержимого файлов и каталогов.

Для запуска KAV Inspector используют меню программ. Для создания таблицы с данными выбирают в меню «Таблицы» команду «Создать таблицы для дисков». После этого будут созданы таблицы для дисков, чтобы в последующем проверять диски на наличие изменений содержимого файлов и каталогов.

В случае обнаружения изменений нужно запускать программу Kaspersky Anti-Virus Scanner для поиска компьютерных вирусов.

4.2. Задания для лабораторной работы № 4

Задание

Выполнить следующие действия:

- с помощью программы Kaspersky Anti-Virus Control Center создайте новую задачу сканирования диска на вирусы; запустите созданную задачу на выполнение;
- с помощью программы Kaspersky Anti-Virus Scanner осуществите сканирование на наличие вирусов выбранной папки,
- реализуйте просмотр результатов сканирования с использованием категории «Статистика»;
- получите подробный отчет о результатах сканирования;
- осуществите обновление антивирусных программ из Интернета;
- осуществите изменение настроек сканера;
- выполните изменение параметров записи результатов сканирования в файл;
- выполните настройки переименования зараженных файлов и измените уровень приоритета сканирования;
- создайте таблицу, содержащую основные данные о диске компьютера.

Отчет

Отчет должен содержать:

- титульный лист;
- задание;
- инструкции по выполнению предложенных заданий;
- скриншоты окон настройки параметров по каждому заданию.

5. ЛАБОРАТОРНАЯ РАБОТА № 5
ШИФРОВАНИЕ ЭЛЕКТРОННЫХ СООБЩЕНИЙ С ПРИМЕНЕНИЕМ ПРОГРАММЫ PGP

5.1. Общие методические указания по выполнению лабораторной работы № 5

Цель работы – изучение технологии защиты электронных сообщений с помощью программы специального назначения (программы PGP).

Pretty Good Privacy (PGP) – это гибридная криптосистема, объединяющая принципы симметричной (с одним ключом) и асимметричной (с двумя ключами) криптосистем**.**

В асимметричной криптосистеме могут использоваться следующие алгоритмы:

- RSA (назван в честь авторов Рона Ривеста, Ади Шамира и Леонарда Адлмана);

- DH / DSA (назван по имени авторов (Diffie – Hellman), предложивших концепцию метода, и по наименованию алгоритма (Digital Signature Algorithm); алгоритм предложен Дэвидом Кравицом; этот алгоритм может иметь другое обозначение DH / DSS (Digital Signature Standart)).

В PGP исходное сообщение вначале сжимается. Сжатие сокращает время модемной передачи и экономит дисковое пространство, а также снижает избыточность данных, повышая криптографическую стойкость сообщения.

Затем в PGP создается одноразовый симметричный ключ, применяемый только для одной операции. Этот сеансовый ключ представляет собой псевдослучайное число. С помощью сеансового ключа сжатое сообщение зашифровывается в шифротекст.

На следующем шаге зашифровывается сам сеансовый ключ, но уже открытым ключом получателя. Зашифрованный сеансовый ключ прикрепляется к шифротексту и передается вместе с ним получателю.

Расшифрование происходит в обратном порядке:

- закрытый ключ получателя используется для расшифрования сеансового ключа;

- сеансовый ключ применяется для восстановлении исходного сообщения.

Ключи в PGP хранятся в зашифрованном виде в двух файлах на жестком диске:

- файл для открытых ключей (pabring.prk);

- файл для закрытых ключей (secring.srk).

Эти файлы называются связками (keyrings) и хранятся чаще всего в папке PGP.

В связку открытых ключей будут добавляться открытые ключи будущих корреспондентов, а в связке закрытых ключей всегда хранятся закрытые ключи владельца компьютера.

Потеря (удаление) связки закрытых ключей приводит к невозможности расшифрования сообщений, зашифрованных корреспондентами с помощью соответствующих открытых ключей. Поэтому полезно создание резервных копий этой связки.

5.2. Технология применения криптосистемы PGP для шифрования и расшифрования сообщений

5.2.1. Генерация ключей

Генерация ключей. Генерирование новой ключевой пары осуществляется следующим образом.

Щелкают на иконке Замок на панели задач и выбирают пункт меню PGPkeys; при этом открывается окно PGPkeys; если программу используют первый раз, то окно пустое.

В окне PGPkeys щелкают на панели инструментов по иконке Ключик (Generate new keypair); при этом открывается окно мастера генерации ключа.

Нажимают кнопку Expert, чтобы перейти к заданию расширенных параметров создаваемого ключа. На экране появится окно с предложением назначить параметры ключевой пары:

- поле Full name (полное имя) – поле для ввода имени, которое будет представлять Вас вашим корреспондентам;
- поле E-mail address (адрес электронной почты) – поле для ввода адреса, указание которого позволит корреспондентам находить на связке открытых ключей те, которые принадлежат вам;
- параметры Key type (тип ключа), Key size (размер ключа) лучше не изменять;
- параметр Key Expiration (истечение срока ключа) может иметь установленное по умолчанию значение Never (никогда), либо принимать значение даты, с которой ключевая пара не сможет применяться для новых криптографических операций;
- кнопка More Information (подробная информация) обеспечивает вывод на экран разделов документации с пояснением назначения указанных в окне параметров;
- кнопка Далее обеспечивает переход в следующее окно, в котором вводится ключевая фраза; ключевая фраза должна содержать не менее 8 символов (желательно не буквенных); ключевую фразу (пароль, ключ) необходимо хранить в тайне; ключевая фраза вводится дважды в поля Passphrase и Confirmation; если введенные ключевые фразы совпадут, то на экране появится окно с сообщением об успешном завершении процесса генерации ключевой пары;
- кнопка Далее; на экране появится окно завершения работы мастера генерации ключевой пары;

- кнопка Готово; на экране снова появится окно PGPkeys, которое раньше было пустым; теперь в окне представлены сведения о сгенерированной ключевой паре.

Окно PGPkeys может отображать следующие параметры ключей:

- Keys (ключи) содержит имя пользователя и его e-mail-адрес, введенные при генерации; параметр может сопровождаться пиктограммами (например, золотой ключ и человечек обозначают пару «открытый ключ / закрытый ключ» типа Diffie-Hellman / DSS; серый ключ и человечек – пару «открытый ключ / закрытый ключ» типа RSA; конверт обозначает просто имя и электронный адрес владельца ключа; желтый конверт используют для обозначения ключа типа DH / DSS; карандаш с синей стрелкой обозначает экспортируемую с ключом подпись и т.д.);

- Validity (достоверность); применительно к чужим ключам обозначает степень убежденности в том, что данный открытый ключ действительно принадлежит предполагаемому владельцу; зависит от состава подписей; ключ, не имеющий подписей, считается частично достоверным; параметр сопровождает пиктограмма (серый кружок обозначает недостоверные или частично достоверные ключи; зеленый кружок обозначает достоверные открытые ключи и т.д.);

- Size (размер); для DH / DSS: 2048 бит – ключ шифрования, 1024 бит – ключ подписания;

- Trust (уровень доверия); с помощью шкалы отображается указанный пользователем уровень доверия владельцу данного ключа как заверителю чужих открытых ключей;

- ADK (наличие дополнительных ключей расшифрования);

- Description (описание); краткое описание объекта в колонке Keys: тип и состояние ключа, тип удостоверения, вид подписи и т.д.

Итак, в окне PGPkeys после генерации ключевой пары отображаются:

- сгенерированная пользователем асимметричная пара «открытый / закрытый ключ» типа DH / DSS;

- имя простого сертификата PGP;

- экспортируемая со связки подпись.

Полученная пара ключей одновременно является основной. Основная пара (основной ключ), или ключ по умолчанию, используется криптосистемой PGP при шифровании и расшифровании сообщений, а также при подписании отправляемых сообщений. В окне PGP основной ключ выделен жирным шрифтом.

Если ключевых пар несколько, то для выбора основного ключа поступают следующим образом:

- в окне PGP надо выделить ключ, который станет основным;

- выбрать пункт меню Keys, затем Set as Default Key.

Имя ключа станет жирным.

PGP автоматически направит открытый ключ в файл pubring.pkr, а закрытый ключ – в файл secring.skr.

После генерации ключевой пары необходимо сделать несколько резервных копий. Дополнительно закрытый ключ рекомендуется хранить на флешке.

5.2.2. Экспортирование и импортирование открытых ключей

Экспортирование открытых ключей. Чтобы сохранить свой открытый ключ в виде отдельного файла (**экспорт ключа**) необходимо:

- в окне PGPkeys выделить ключ, который надо экспортировать;
- выбрать пункты меню Keys, Export; на экране появится окно Export Key to File, в котором необходимо указать место хранения экспортируемого ключа;
- в окне Папка необходимо указать каталог хранения экспортируемого ключа, в окне Имя файла – имя и расширение файла. По умолчанию PGP предлагает для файла расширение asc, что соответствует текстовой форме представления открытого ключа (вариантами расширения могут быть pkr, pubkr);
- опция Include 6.0 Extensions включается при необходимости экспортирования вместе с ключом фото (в этом случае сам ключ будет несовместим с версиями PGP ниже 6.0);
- опция Include Private Keys активируется при необходимости включения в файл и закрытого ключа; полученный при этом файл не подлежит передаче и используется только пользователем;
- нажать клавишу Сохранить.

Сохранение ключа можно осуществить и другими способами. При необходимости копирования открытого ключа со связки в любой текстовый файл или сообщение необходимо:

- в окне PGPkeys выделить ключ, который намечено экспортировать;
- выбрать пункты меню Edit, Copy.

Текст ключа представляет собой набор символов, ограниченный фразами ----- BEGIN --- END ----.

Этот текст находится в буфере обмена, откуда его можно вставить в сообщение командами Edit, Paste или комбинацией клавиш Strl+V.

Для того, чтобы осуществить **импорт ключа** (**добавить в связку ключ, полученный от корреспондента в виде файла**), необходимо:

- в окне PGPkeys выбрать пункты меню Keys, Import; на экране появится окно Select File Containing Key для указания папки хранения принятого файла с ключом (или ключами, если корреспондент прислал файл с несколькими открытыми ключами);
- в строке Папка указать директорию размещения принятого файла с открытым ключом корреспондента;
- в строке Тип файла указать расширение принятого файла (вариантами расширения могут быть: txt, asc, pkr, pubkr);
- в появившемся списке выделить принятый файл с ключом корреспондента и нажать кнопку Открыть. На экране появится окно Select Keys с параметрами ключа (ключей);

- выделить строку с ключом (или строки с ключами, если их в файле несколько) и нажать кнопку Import. Ключ будет присоединен к списку в окне PGPkeys.

Если открытый ключ вставлен в сообщение, полученное от корреспондента, то для добавления его на связку необходимо:

- в полученном сообщении выделить блок, начиная с заголовка

----BEGIN PGP PUBLIC KEY BLOCK----

и заканчивая строкой

----END PGP PUBLIC KEY BLOCK----

и скопировать выделенный текст в буфер обмена (например, нажать Ctrl+C);

- в окне PGPkeys выбрать пункты меню Edit, Paste. На экране появится окно Select Keys с параметрами ключа;

- выделить строку с ключом и нажать кнопку Import. Ключ будет присоединен к списку в окне PGPkeys.

5.2.3. Зашифрование и расшифрование сообщений через буфер обмена

Для подготовки зашифрованного сообщения, предназначенного для передачи по электронной почте, в криптосистеме PGP применяются два способа:

- подготовка зашифрованного сообщения через **буфер обмена**;
- подготовка зашифрованного сообщения **из файла**.

Для **подготовки зашифрованного сообщения** в криптосистеме PGP через **буфер обмена** необходимо:

- текст сообщения скопировать в буфер обмена (Ctrl+C или Правка, Копировать);

- щелкнуть по изображению замочка (PGPtray) на панели задач и в появившемся меню выбрать Clipboard, Engrypt (зашифровать). На экране появится окно Key Selection Dialog со списком сертификатов доступных открытых ключей;

- указать вариант зашифрования, выбрав опцию внизу слева.

Вариант 1. **Secure Viewer** (Безопасный зритель) – если необходимо отправить получателю сообщение, которое и после расшифрования его закрытым ключом не может быть прочитано, пока не будет выполнена процедура снятия дополнительной защиты.

Для зашифрования по первому варианту поступают следующим образом:

- в верхней части окна Drag users from this list to the Recipients list (Перенесите пользователя (его ключ) из этого списка в список получателя) дважды щелкнуть по ключу корреспондента. Ключ окажется в нижнем окне (Recipients – Получатели);

- щелкнуть по кнопке ОК, после чего в буфере обмена появится не открытый, а зашифрованный текст, который имеет вид:

-----BEGIN PGP MESSAGE-----

Version: PGP 7.0
Comment: sews
…
-----END PGP MESSAGE-----

Такой текст можно вставить из буфера обмена (через меню Правка, Вставить или Ctrl+V) в редактор используемой почтовой программы или в специально создаваемый файл для передачи. Фраза sews в шифротексте после слова Comment идентифицирует отправителя (если эта фраза вводилась в закладке General окна настройки PGP Options).

Для **расшифрования переданного получателю сообщения** необходимо:

- открыть текст в текущем окне;
- щелкнуть по изображению замочка (PGPtray) на панели задач и в появившемся меню выбрать пункт Current Window (или Clipboard, если получатель предварительно скопировал шифротекст в буфер обмена), а затем выбрать Decrypt & Verify (расшифровка и свертка). На экране появится окно с указанием на то, что сообщение зашифровано открытым ключом получателя и с предложением ввести свой закрытый ключ (пароль);
- щелкнуть по кнопке ОК, после чего на экране появится окно, напоминающее о том, что сообщение было зашифровано в варианте обеспечения безопасности просмотра и о необходимости соблюдения условий безопасности;
- щелкнуть по кнопке ОК, после чего на экране появится окно Secure Viewer, в котором сообщение останется нечитаемым до момента снятия «галочки» с опции Use TEMPEST Attack Prevention Fort в нижней области окна. После прочтения сообщения с соблюдением мер ограничения доступа достаточно восстановить «галочку», чтобы вновь сделать сообщение нечитаемым;
- закрыть окно Secure Viewer.

Вариант 2. **Conventional Encryption** (Обычное зашифрование) – если необходимо просто зашифровать и передать сообщение корреспонденту, который знает ключевую фразу. Другими словами, вариант реализован по схеме симметричного зашифрования и не связан с использованием асимметричных ключей сгенерированных ключевых пар.

Для зашифрования по этому варианту необходимо:

- после копирования сообщения в буфер и вызова в окне PGPtray пунктов меню Clipboard, Engrypt (зашифровать) в появившемся окне Key Selection Dialog выбрать опцию Conventional Encryption (поставить «галочку»);
- щелкнуть по кнопке ОК, после чего на экране появится окно с предложением ввести ключ для зашифрования сообщения, помещенного в буфер. Это может быть любой ключ, о котором заранее договорились отправитель и получатель;
- после ввода ключа щелкнуть по кнопке ОК, после чего в буфере обмена появится зашифрованный текст.

Этот текст можно отправлять получателю средствами почтовой программы, а можно записать в файл для последующей передачи.

Расшифрование принятого получателем сообщения осуществляется в следующем порядке:

- открыть текст в текущем окне;

- щелкнуть по изображению замочка (PGPtray) на панели задач и в появившемся меню выбрать пункты Current Window (или Clipboard, если получатель предварительно скопировал шифротекст в буфер обмена), затем пункт Decrypt & Verify (расшифровка и сверка);

- на экране появится окно с предложением ввести ключевое слово; необходимо ввести ключ и щелкнуть по кнопке ОК;

- если ключ введен правильно, на экране появится окно Text Viewer с расшифрованным сообщением.

Сохранить расшифрованное сообщение можно, записав его в буфер с помощью кнопки Copy to Clipboard (Ctrl+C), а затем переписать в файл.

Щелчок по кнопке ОК приведет к потере расшифрованного сообщения.

5.2.4. Зашифрование и расшифрование сообщений из файла

В PGP реализовано несколько вариантов зашифрования сообщения из файла.

Вариант 1. Для **шифрования сообщения из файла** необходимо:

- щелкнуть по изображению замочка (PGPtray) на панели задач и в появившемся меню выбрать пункт PGPtools. На экране появится набор пиктограмм;

- щелкнуть по пиктограмме Encrypt (конверт с замком – зашифровать); на экране появится окно Select File(s) to Encrypt (Выбор файла для зашифрования);

- выделить файл, подлежащий зашифрованию, и щелкнуть по кнопке Открыть; на экране появится окно PGPtray – Key Selection Dialog со списком сертификатов доступных открытых ключей; далее необходимо выделить ключ получателя и перенести его в окно (Recipients – Получатели);

- щелкнуть по кнопке ОК, после чего в папке, где хранится исходный файл, появится файл типа PGP Encrypted File с именем исходного файла, но с расширением .pgp. Этот файл можно отправлять получателю по электронной почте.

Для **расшифрования файла** необходимо выполнить следующие действия на стороне получателя:

- открыть папку с принятым файлом;

- правой кнопкой мыши щелкнуть по имени файла;

- в появившемся окне выбрать PGP, затем – Decrypt & Verify (Расшифровка и Сверка). На экране появится окно с указанием на то, что сообщение зашифровано открытым ключом получателя, и с предложением ввести свой закрытый ключ (пароль);

- после ввода ключа щелкнуть по кнопке ОК, после чего в папке с принятым файлом появится расшифрованный файл.

Расшифрование файла можно выполнить и **другим способом**:

- щелкнуть по изображению замочка на панели задач (PGPtray) и в появившемся меню выбрать пункт PGPtools;

- в появившейся панели пиктограмм щелкнуть по пиктограмме (Конверт с открытым замком – Decrypt / Verify (Расшифровка и Сверка). На экране появится окно Select File(s) to Decrypt / Verify (Выбор файла для расшифрования);

- выделить файл, подлежащий расшифрованию и щелкнуть по кнопке Открыть). На экране появится окно с предложением ввести свой закрытый ключ (пароль);

- после ввода ключа щелкнуть по кнопке ОК, после чего в папке с принятым файлом появится расшифрованный файл.

Вариант 2. Для **шифрования сообщения из файла** необходимо:

- вызвать на экран папку с файлом исходного сообщения и выделить этот файл;

- щелкнуть правой кнопкой мыши по строчке с выделенным файлом. В появившемся меню выбрать строчку PGP, Encrypt;

- на экране появится окно PGPshell – Key Selection Dialog со списком сертификатов доступных открытых ключей;

- не активировать опции в окне внизу слева, дважды щелкнуть по ключу предполагаемого корреспондента. Ключ переместится в окно Recipients – Получатели;

- щелкнуть по кнопке ОК, после чего в папке, где хранится исходный файл, появится файл типа PGP Encrypted File с именем исходного файла, но с расширением .pgp. Этот файл можно отправлять получателю по электронной почте.

Вариант 3. **Зашифрование сообщения в кодах ASCII**. Для зашифрования необходимо:

- вызвать на экран папку с файлом исходного сообщения и выделить этот файл;

- щелкнуть правой кнопкой мыши по строчке с выделенным файлом. В появившемся меню выбрать строчку PGP, Encrypt;

- на экране появится окно PGPshell – Key Selection Dialog со списком сертификатов доступных открытых ключей;

- активировать опцию (выставить «галочку») Text Output (Вывод текста) и дважды щелкнуть по ключу предполагаемого корреспондента. Ключ переместится в окно Recipients – Получатели;

- щелкнуть по кнопке ОК, после чего в папке, где хранится исходный файл, появится файл типа PGP Armored File с именем исходного файла, но с расширением .asc. Этот файл можно отправлять получателю по электронной почте.

Расшифрование выполняется по любому из способов, изложенных в варианте 1. Файл, зашифрованный по варианту 3, по объему больше почти на треть. Вариант 3 применяется только в том случае, если корреспондент заказывает именно такое представление.

Вариант 4. **Зашифрование по схеме симметричного зашифрования** и не связано с использованием асимметричных ключей сгенерированных ключевых пар.

Для зашифрования необходимо:

- вызвать на экран папку с файлом исходного сообщения и выделить этот файл;

- щелкнуть правой кнопкой мыши по строчке с выделенным файлом. В появившемся меню выбрать строчку PGP, Encrypt;

- на экране появится окно PGPshell – Key Selection Dialog со списком сертификатов доступных открытых ключей;

- поставить «галочку» в окне опции Conventional Encryption (Обычное зашифрование), после чего в текущем окне исчезнут доступные открытые ключи;

- щелкнуть по кнопке ОК, на экране появится окно PGPshell – Enter Passphrase с предложением дважды ввести оговоренный корреспондентами ключ;

- после ввода ключей и нажатия кнопки ОК в папке, где хранится исходный файл, появится файл типа PGP Encrypted File с именем исходного файла и расширением .pgp. Этот файл можно отправлять корреспонденту. Объем этого файла будет меньше, чем в других вариантах за счет применения другого алгоритма.

Для расшифрования зашифрованного данным способом файла необходимо:

- вызвать папку с принятым файлом и выделить файл;

- правой кнопкой мыши щелкнуть по имени файла;

- в появившемся окне выбрать PGP, затем Decrypt & Verify (Расшифровка и Сверка). На экране появится окно PGP Enter Passphrase с предложением ввести согласованный с отправителем ключ;

- если после ввода ключа и нажатия кнопки ОК на экране появится окно PGP Enter Passphrase, то это значит, что введен неверный ключ и ввод необходимо выполнить заново;

- если после ввода ключа и нажатия кнопки ОК на экран будет выведено окно Enter output filename с предложением определить имя и место хранения расшифрованного файла, то это значит, что файл расшифрован и его надо сохранить. Исходный файл при этом останется зашифрованным.

Вариант 5. Зашифрование по этому варианту выполняется при необходимости передать зашифрованное сообщение корреспонденту, у которого на компьютере **нет PGP**.

Для зашифрования необходимо:

- - вызвать на экран папку с файлом исходного сообщения и выделить этот файл;

- щелкнуть правой кнопкой мыши по строчке с выделенным файлом. В появившемся меню выбрать строчку PGP, Encrypt;

- на экране появится окно PGPshell – Key Selection Dialog со списком сертификатов доступных открытых ключей;

- поставить «галочку» в окне опции Self Decrypting Archive (Самораспаковывающийся архив), после чего программа сама проставит «галочку» в опции Conventional Encryption (Обычное зашифрование), а окно текущее окно изменится, исчезнут сертификаты открытых ключей;

- щелкнуть по кнопке ОК, после чего на экране появится окно PGPshell – Enter Passphrase с предложением дважды ввести оговоренный с корреспондентом ключ;

- после ввода ключей и нажатия кнопки ОК на экране появится окно Please confirm the file name of this SDA (Пожалуйста, подтвердите имя этого файла SDA);

- после уточнения имени и места хранения файла щелкнуть по кнопке Сохранить.

Сохраненный файл можно пересылать получателю.

Созданный файл является приложением с именем исходного файла и расширением .sda.exe. SDA – это аббревиатура самораспаковывающегося файла-приложения. Объем этого файла будет намного больше исходного, потому что исходный текст сообщения вставляется в исполняемый файл.

Для расшифрования файла с расширением .sda.exe, необходимо:

- открыть папку с принятым файлом и щелкнуть по имени файла. Файл запустится на выполнение и выведет на экран окно PGP Self Decrypting Archive – Enter Passphrase. Сообщение в окне о том, что файл зашифрован по технологии PGP, и выводится приглашение на веб-сайт для более детального изучения этой технологии. Внизу окна расположено окно для ввода ключа, которым по договоренности с получателем зашифровано сообщение;

- ввести ключ и щелкнуть по кнопке ОК, после чего в папку, где хранится файл-приложение, будет записано расшифрованное сообщение.

5.3. Задание для лабораторной работы № 5

Задание

1. Создать специальную папку для хранения результатов выполнения данной лабораторной работы.

2. Создать три сообщения (в текстовом редакторе Word или в другом редакторе) и сохранить их в файлах в папке «Открытые тексты».

3. Сгенерировать две ключевые пары (открытый и закрытый ключи).

4. Сохранить свои открытые ключи в виде отдельных файлов в папке «Открытые ключи». Передать соседу свои открытые ключи через диск X.

5. Получить от соседа два открытых ключа через диск X и добавить их в связку.

6. Зашифровать первое сообщение через буфер обмена и передать соседу через диск X.

7. Получить от соседа первое зашифрованное сообщение через диск X и расшифровать его через буфер обмена.

8. Зашифровать второе сообщение из файла и передать соседу через диск X.

9. Получить от соседа второе сообщение из файла через диск X и расшифровать его из файла.

10. Зашифровать и расшифровать третье сообщение по схеме симметричного зашифрования.

11. Зашифровать и расшифровать третье сообщение для корреспондента, у которого на компьютере **нет PGP.**

12. Оформить отчет.

Отчет

Отчет должен содержать:

- титульный лист;
- задание;
- описать выполненные действия для каждого пункта задания.

6. ЛАБОРАТОРНАЯ РАБОТА № 6 УСТАНОВКА И НАСТРОЙКА БЕСПЛАТНОГО FIREWALL

6.1. Общие методические указания по выполнению лабораторной работы № 6

Цель работы – познакомиться с основными настройками типичной программы firewall, используемой для защиты компьютера, выходящего в глобальную сеть.

В результате выполнения лабораторных работ студенты должны знать:

1) основные моменты процедуры установки firewall;
2) управление доступом к компьютеру по локальной сети через firewall;
3) просмотр протокола сетевой активности;
4) управление списком программ, обращающихся к сетевым ресурсам.

В качестве примера рассматривается бесплатная программа ZoneAlarm.

6.2. Задание к лабораторной работе № 4

Установка и настройка доступа по локальной сети.

1. Установить программу на одном из компьютеров учебного класса. При установке отказаться от регистрации и регулярного обновления через Интернет. В конце установки в окне настройки конфигурации установить следующие параметры и нажать **Finish** (рис. 9).

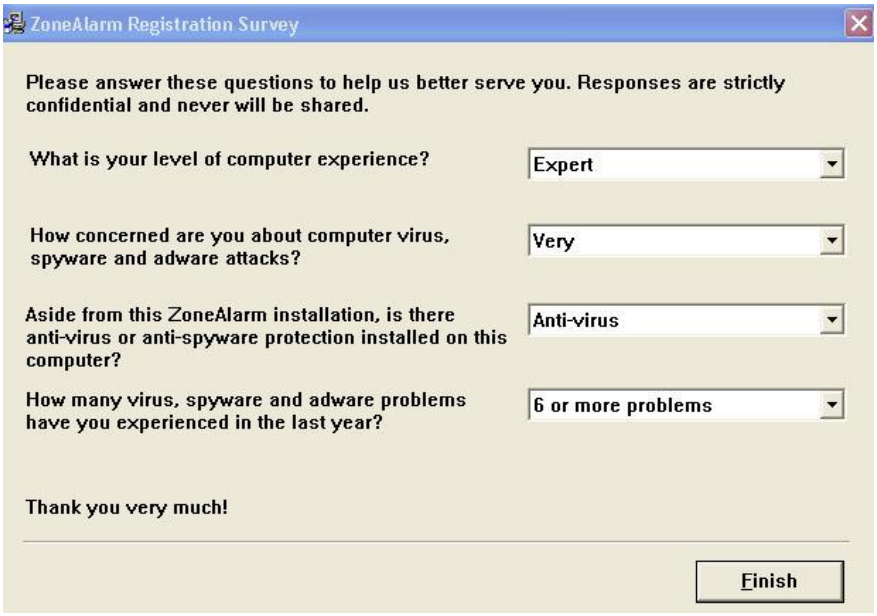


Рис. 9. Окно настройки конфигурации ZoneAlarm

2. В появившемся окне выбора варианта использования программы (бесплатный сокращенный вариант или полная 15-дневная версия) выбрать **Try ZoneAlarm Security Suite** и щелкнуть по данной опции мышью (рис.10).

Рис. 10. Окно выбора варианта использования программы ZoneAlarm

3. В следующих окнах указать параметры:
1) 1-е окно – **Maximum**;
2) 2-е окно – **Do not participate…**;
3) 3-е окно – **Manual**;
4) 4-е окно – **No – Disable Anti-virus Protection**;

5) 5-е окно – **Do not scan my computer**.

4. После завершения установки программы перезагрузить компьютер.

5. После перезагрузки запустить ZoneAlarm (**Пуск, Программы**…), если он сам не загрузится, и выбрать в появившемся окне **Continue Trial**. В следующем окне выбрать **Finish**. Откроется окно **ZoneAlarm Control Center** (рис.11).

Рис. 11. Окно ZoneAlarm Control Center

6. Во вкладке **Firewall** в закладке **Main** установить индикатор **Internet Zone Security** в положение **High**, индикатор **Trusted Zone Security** – **Medium**.

7. Зайти в командный режим Windows (**Пуск, Выполнить**…, набрать команду **cmd**) и набрать **ipconfig**, чтобы получить IP-адрес компьютера.

Аналогичную операцию проделать на соседнем компьютере, чтобы узнать его IP-адрес.

8. С соседнего компьютера пропинговать компьютер с установленным firewall (командный режим, команда **ping** <IP-адрес целевой машины>). Если все правильно, то пропинговать компьютер, защищенный firewall, не удастся.

9. На целевом компьютере в программе **ZoneAlarm** во вкладке **Firewall** перейти на закладку **Zones**. Щелкнуть мышью по кнопке **Add** и выбрать пункт **IP Address**. В открывшемся диалоговом окне ввести данные в **поля IP Address** (адрес соседнего компьютера) и **Description** (описание компьютера) (поле Zone установлено по умолчанию в значение **Trusted**) (рис.12). После ввода данных щелкнуть мышью по кнопке ОК, а во вкладке **Zones** – по кнопке **Apply**.

Рис. 12. Окно добавления IP-адреса компьютера в список разрешаемых адресов

10. Попробовать пропинговать целевой компьютер с соседнего компьютера. В данном случае операция пропингования осуществится. Также скопировать на/с целевого компьютера какие-либо файлы или каталоги.

Просмотр протокола сетевой активности.

11. Перейти во вкладку **Alerts & Logs** программы (рис. 13).

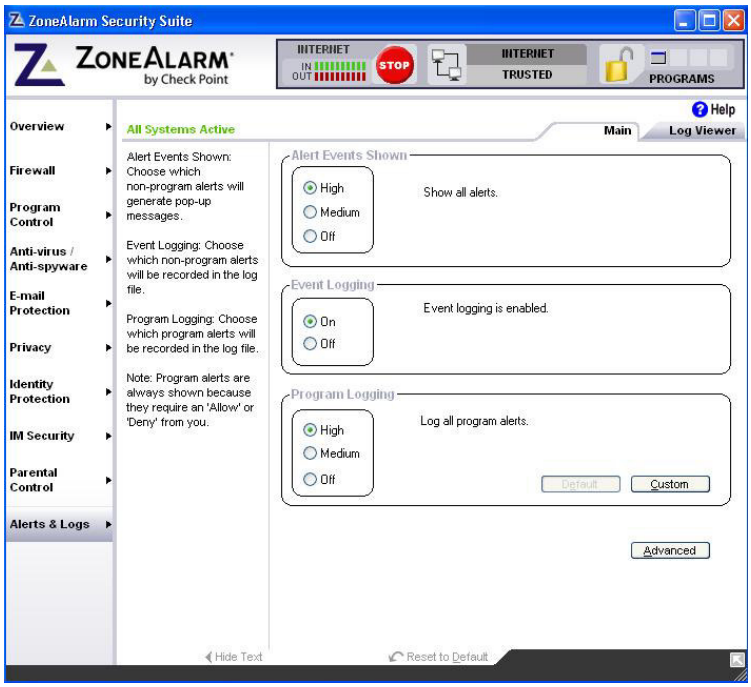


Рис. 13. Окно Alerts & Logs программы ZoneAlarm

В закладке **Main** поставить переключатель **Alert Events Shown** в положение **High**.

12. Перейти в закладку **Log Viewer** и посмотреть протокол. Должны быть отражены попытки доступа к целевому компьютеру по локальной сети / сети Интернет и доступа программ компьютера в локальную сеть / сеть Интернет (рис. 14).

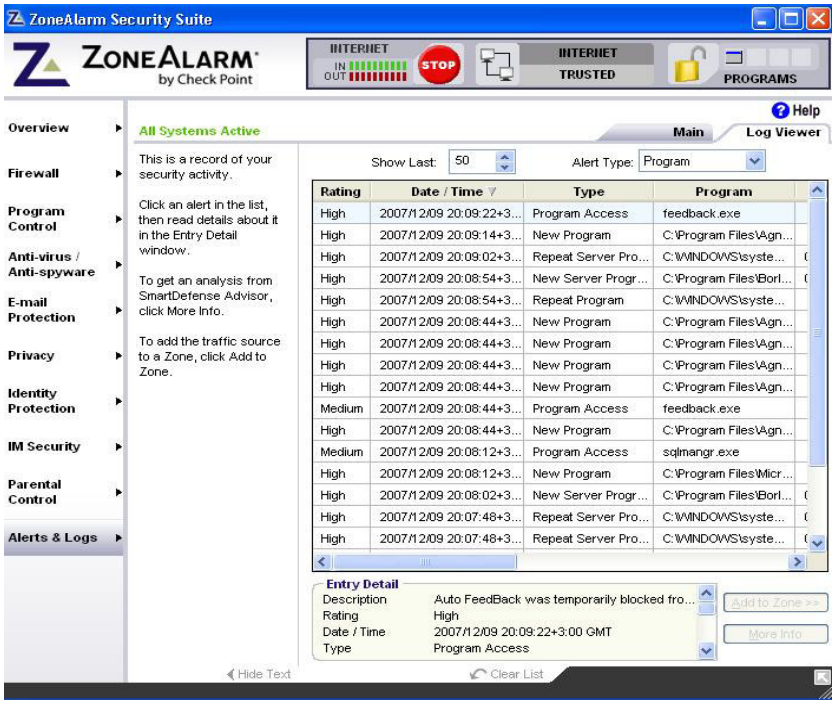


Рис. 14. Закладка **Log Viewer** вкладки **Alerts & Logs** программы

Чтобы отсортировать предупреждения по типу можно воспользоваться полем со списком **Alert Type** в верхней части окна программы.

Управление списком программ, обращающихся к сетевым ресурсам.

13. Перейти во вкладку **Program Control** программы. В закладке Main установить переключатель Program Control в положение **Maximum**, переключатель **Automatic Lock** в положение **Off**.

14. Перейти в закладку **Programs**. Там представлен список программ, имеющих доступ в Интернет (или к которым возможен доступ из Интернета). Столбец **Access** позволяет программам получать информацию из локальной/глобальной сети (**Trusted/Internet**), столбец **Server** позволяет обращение к программам из локальной/глобальной сети (**Trusted/Internet**) (рис. 15).

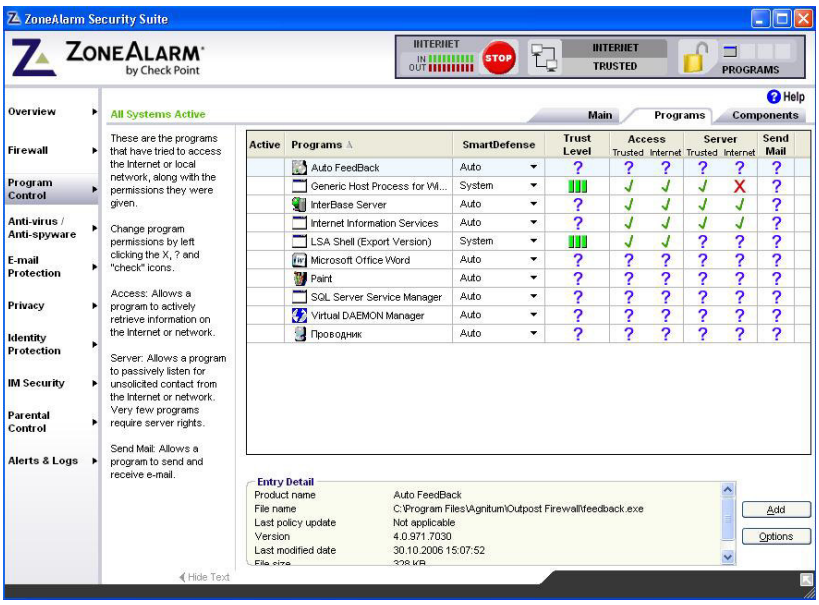


Рис. 15. Закладка **Programs** вкладки **Program Control** программы

15. В закладке **Programs** попробуйте поменять параметры доступа к программам (двойной щелчок мышью по нужным программам), добавить новые программы в список (щелчок правой кнопкой мыши по списку, пункт **Add Program…** контекстного меню).

16. Продемонстрировать преподавателю произведенные настройки и действия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Мельников В. П. Информационная безопасность : учебное пособие / под ред. С. А. Клейменова. - 8-е изд., испр. - М.: Академия, 2013.

2. Сергеева Т. И. Сергеев М.Ю. Методы и средства защиты компьютерной информации: учебное пособие/ Т. И. Сергеева, М. Ю. Сергеев – Воронеж: ВГТУ, 2011.

3. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 с.— Режим доступа: http://www.iprbookshop.ru/52182.html.— ЭБС «IPRbooks»

4. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 с.— Режим доступа: http://www.iprbookshop.ru/6991.html.— ЭБС «IPRbooks»

5. Семенов Ю.А. Процедуры, диагностики и безопасность в Интернет [Электронный ресурс]/ Семенов Ю.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 581 с.— Режим доступа: http://www.iprbookshop.ru/62827.html.— ЭБС «IPRbooks»

ОГЛАВЛЕНИЕ

ТЕХНОЛОГИИ ПРОГРАММНОЙ ЗАЩИТЫ ДАННЫХ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению лабораторных работ
по дисциплине «Технологии защиты Web-контента»
для студентов направления 38.03.05 «Бизнес-информатика»
(профиль «Информационные системы в бизнесе»)
очной и заочной форм обучения

Составители:
Сергеева Татьяна Ивановна
Сергеев Михаил Юрьевич
Белых Михаил Алексеевич

Компьютерный набор Т.И. Сергеевой

Подписано к изданию 26.01.2022.
Уч.-изд. л. 1,9.

ФГБОУ ВО «Воронежский государственный технический университет»
394026 Воронеж, Московский просп., 14