МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ

Декан факультета энергетики и систем управления

_____ / А.В. Бурковский /

_____ 16.02 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность и защита информации»

Направление подготовки 27.03.04 Управление в технических системах

Профиль Управление и информатика в технических системах

Квалификация выпускника бакалавр

Нормативный период обучения 4 года

Форма обучения очная

Год начала подготовки 2023

Автор программы _____ И.В. Зубарев

Заведующий кафедрой Электропривода, автоматики и управления в технических системах _____ В.Л. Бурковский

Руководитель ОПОП _____ Ю.В. Мурзинов

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

ознакомление студентов с основами комплексного подхода к обеспечению информационной безопасности (ИБ) автоматизированных систем (АС), проблемами защиты информации и подходами к их решению, а так же способам и приёмам защиты информации криптографическими средствами.

1.2. Задачи освоения дисциплины

приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности (ИБ) автоматизированных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность и защита информации» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационная безопасность и защита информации» направлен на формирование следующих компетенций:

ПК-2 - Способен осуществлять разработку методического обеспечения автоматизированных систем управления производством, планирование предварительных испытаний автоматизированных систем.

ПК-5 - Способен к разработке отдельных разделов проекта на различных стадиях проектирования автоматизированных систем управления технологическими процессами

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-2	знать основные методы управления информационной безопасностью
	Уметь пользоваться моделями безопасности КС при управлении доступом и информационными потоками
	Владеть навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности

ПК-5	Знать требования информационной безопасности при эксплуатации автоматизированной системы
	Уметь оценивать информационные риски в автоматизированных системах и разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;
	Владеть методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность и защита информации» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		2
Аудиторные занятия (всего)	72	72
В том числе:		
Лекции	18	18
Практические занятия (ПЗ)	18	18
Лабораторные работы (ЛР)	36	36
Самостоятельная работа	108	108
Курсовая работа	+	+
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 180 5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	Лаб. зан.	СРС	Всего, час
1	Понятие "информационная безопасность"	• ознакомиться с основными подходами к определению понятия "информационная безопасность". • изучить составляющие информационной безопасности и их характеристику. • ознакомиться с нормативно-правовыми основами информационной безопасности в РФ, нормативными документами и ответственностью за нарушения информационной безопасности.	2	2	4	12	20
2	Угрозы информационной безопасности. Виды угроз. Сетевые атаки.	• Изучить виды угроз и их характеристики • изучить классы удаленных угроз распределенным вычислительным сетям.	2	2	4	12	20

3	Классификация средств защиты информации. Многоуровневая защита информации. Подходы к обеспечению безопасности автоматизированных систем	Средства защиты информации принято делить на нормативные (неформальные) и технические (формальные). нормативные(законодательные), административные(организационные) и морально-этические средства Физические средства защиты информации Аппаратный средства защиты информации Программные средства защиты информации DLP-системы, SIEM-системы, Математический (криптографический), Многоуровневая защита информации	2	2	4	12	20
4	Введение в криптографию. История развития. Основные понятия и определения. Архитектура криптографических систем защиты информации.	основными понятиями криптографии, изучить основы криптографических методов защиты информации, дается историческая справка об основных этапах развития криптографии как науки. структуру криптосистем, методы шифрования и способы управления криптосистемами.	2	2	4	12	20
5	Информационная Безопасность в Отраслях. Политика безопасности организации. И Б на предприятии: с чего начать. Корпоративная информационная безопасность	принцип правового обеспечения. Принцип глобализации принципу экономической целесообразности Принцип гибкости систем принцип не секретности. принцип разнообразия Принцип простоты управления Информационная безопасность предприятий Аудит Этапы внедрения системы безопасности Организационные меры Режим коммерческой тайны Технические меры	2	2	4	12	20
6	Безопасность Информационных Систем. Архитектура безопасности информационных систем. Разработка, механизмы обеспечения.	Составляющие информационной безопасности Построение системы ИБ Технические средства защиты Понятие архитектуры безопасности ИС и ее задачи Методы построения идеальной архитектуры Стратегия Разработка систем информационной безопасности Новые идеи и технологии Механизмы обеспечения ИБ ИС	2	2	4	12	20
7	DLP-СИСТЕМЫ	Что такое DLP и как они работают «Побочные» задачи DLP Классификация DLP-систем Мировой рынок DLP Перспективы и тенденции С чего начать выбор DLP-системы Хостовые DLP Сетевые DLP Внедрение и настройка DLP-системы	2	2	4	12	20
8	Информационная безопасность вычислительных сетей.	Особенности обеспечения информационной безопасности в компьютерных сетях. и специфику средств защиты компьютерных сетей. Сетевые модели передачи данных. теоретические основы построения компьютерных сетей; протоколы передачи данных. Понятие протокола передачи данных. Принципы организации обмена данными в вычислительных сетях. Транспортный протокол TCP и модель TCP/IP.структуру модели открытых систем OSI/ISO и назначение ее уровней. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO. Характеристика уровней модели OSI/ISO.	2	2	4	12	20
9	Классификация удаленных угроз в вычислительных сетях. Принципы защиты, механизмы защиты КС.	Классы удаленных угроз и их характеристика Типовые удаленные атаки и их характеристика Причины успешной реализации удаленных угроз в вычислительных сетях Принципы защиты распределенных вычислительных сетей Межсетевое экранирование Технология виртуальных частных сетей (VPN)	2	2	4	12	20
		Итого	**18**	**18**	**36**	**108**	**180**

5.2 Перечень лабораторных работ

Лабораторная работа 1 Простые числа.
Лабораторная работа 2 Взаимно простые числа
Лабораторная работа 3 Модульная арифметика
Лабораторная работа 4 Шифр Цезаря
Лабораторная работа 5 Парольная защита
Лабораторная работа 6 Обмен ключами по Диффи-Хелману
Лабораторная работа 7 Шифр RSA
Лабораторная работа 8 Реализация в среде Excel алгоритма RSA шифрования с открытым ключом.
Лабораторная работа 9 Решение в локальной сети задачи аутентификация пользователей.

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовой работы в 2 семестре для очной формы обучения.

Тема курсовой работы может иметь как научный (разработка и исследования основных и вспомогательных алгоритмов криптографии, разработка средств и протоколов защищенной передачи информации по сети, разработка средств сокрытия информации и т.д.), так и прикладной (разработку информационных систем с подсистемами защиты информации, анализ прикладных решений на их устойчивость к атакам).

Примерная тематика курсовой работы: «Реализация и изучение бинарного алгоритма Евклида. Сравнение с классическим алгоритмом Евклида.»

Задачи, решаемые при выполнении курсовой работы:

- проанализировать информационные источники по теме курсовой работы;
- изучить бинарный алгоритм Евклида и привести пример;
- сравнить бинарный алгоритм с классическим;
- проанализировать проделанную работу.

Курсовая работа включает в себя обязательную разработку программного продукта за исключением случаев, когда тема предполагает серьезные научные исследование, проведение математических доказательств, предложение и обоснование новых методик применения средств защиты информации.

Курсовая работа включат в себя графическую часть и расчетно-пояснительную записку.

1. Реализация на компьютере и исследование эффективности процедуры факторизации натуральных чисел (разложения на простые множители) ро-методом Полларда. Разложение специальных чисел вида .

2. Реализация на компьютере и исследование эффективности факторизации натуральных чисел (p-1) - методом Полларда. Разложение чисел вида .

3. Программирование системы шифрования на эллиптических кривых.

4. Реализация на компьютере генерации простых чисел на основе метода Миллера-Рабина. Построение простых чисел, удовлетворяющих требованиям RSA.

5. Реализация на компьютере и исследование эффективности арифметических операций на эллиптических кривых.

6. Реализация на компьютере и исследование эффективности факторизации натуральных чисел методом Шенкса непрерывных дробей и сравнение с ро-методом Полларда.

7. Реализация на компьютере метода факторизации на эллиптических кривых. Исследование его эффективности. Разложение чисел специального вида.

8. Сравнительное изучение и реализация на компьютере алгоритма вычисления дискретного логарифма в конечных полях.

9. Программирование процедуры факторизации на основе метода квадратичных форм.

10. Реализация на компьютере алгоритма Шенкса-Тоннелли извлечения квадратного корня в конечных полях.

11. Изучение и реализация на компьютере метода вычисления составных псевдопростых чисел для различных баз.

12. Реализация и исследование теста простоты BPSW.

13. Изучение преобразования Тейта и его использования в криптографии.

14. Разработка автоматизированной системы оценки реккурентных алгоритмов на основе производящих функций.

15. Реализация и изучение бинарного алгоритма Евклида. Сравнение с классическим алгоритмом Евклида.

16. Реализация и изучение k-арного алгоритма Евклида. Сравнение с классическим алгоритмом Евклида.

17. Изучение числовых рядов Дирихле и использование для оценки алгоритмов.

18. Исследование эффективности реализации операции модульной арифметики на многоядерных видеопроцессорах (система программирования CUDA).

19. Реализация метода Ленстры процедуры факторизации на эллиптических кривых с использованием кривых Монтгомери.

20. Реализация и исследования преобразований Вейля. MOV-атака на системы шифрования на эллиптических кривых.

21. Реализация на компьютере метода факторизации на эллиптических кривых с использованием кривых Эдварда.

22. Реализация алгоритма построения слепой и короткой подписи на основе преобразования Тейта.

23. Реализация на компьютере метода факторизации на эллиптических кривых с использованием кривых Эдварда. Сравнение эффективности метода с простой процедурой факторизации.

24. Исследование атак типа DDos на web-приложения и способов защиты от них.

25. Исследование атак типа SQL-инъекции на web-приложения и способов защиты от них.

26. Исследование криптоустойчивости шифров.

27. Создание средств аутентификации пользователя по его биометрическим данным.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-2	знать основные методы управления информационной безопасностью	Знание основных методов управления информационной безопасностью	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь пользоваться моделями безопасности КС при управлении доступом и информационными потоками	Умение разрабатывать модели угроз и нарушителей в автоматизированных системах, разрабатывать структуру системы обеспечения безопасности автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности	Владение навыками администрирования информационной инфраструктуры автоматизированной системы и ее безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-5	знать требования информационной безопасности при эксплуатации	знание основных принципов организации технического, программного и информационного обеспечения	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	автоматизированной системы	эксплуатации защищѐнных автоматизированной системы		
	уметь оценивать информационные риски в автоматизированных системах и разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Умение оценивать информационные риски в автоматизированных системах и разрабатывать модели угроз и модели нарушителя информа ционной безопасности автома тизированной системы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	Владение механизмом реализации типовых удаленных атак и их характеристик классифицировать типовые удаленные атаки по совокупности признаков	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 2 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**зачтено**	**не зачтено**
ПК-2	знать основные методы управления информационной безопасностью	Тест	Выполнение теста на 90- 100%	В тесте менее 70% правильных ответов
	уметь пользоваться моделями безопасности КС при управлении доступом и информационными потоками	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Задачи не решены
	владеть навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Задачи не решены
ПК-5	знать требования информационной безопасности при эксплуатации автоматизированной системы	Тест	Выполнение теста на 90- 100%	В тесте менее 70% правильных ответов
	уметь оценивать информационные риски в автоматизированных системах и разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Задачи не решены
	владеть методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Что понимается под информационной безопасностью?

a) Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий…
b) Программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия.
c) Оба варианта верны.

2. Что такое защита информации?

a) Небольшая программа для выполнения определенной задачи.
b) Процесс разработки структуры базы данных в соответствии с требованиями пользователей.
c) Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

3. От чего зависит компьютерная безопасность?

a) От компьютеров.
b) От поддерживающей инфраструктуры
c) Оба варианта верны.

4. Что из перечисленного является основой информационной безопасности?

a) Доступность информации.
b) Защита информации.
c) Нет правильного ответа.

5. Где применяются средства контроля динамической целостности?

a) Анализ потока сообщений для выявления некорректных.
b) Контроль правильности передачи сообщений.
c) Подтверждение отдельных сообщений.
d) Все ответы верны.

6. Какое основное положение важнейших законодательных актов РФ в области информационной безопасности и защиты информации?

a) Закон РФ "Об информации, информатизации и защите информации".

b) Конституция РФ.
c) Уголовный кодекс РФ.
d) Нет правильного ответа.

7. Что относится к государственной тайне?

a) Защищаемые государством сведения в области его военной, внешнеполитической и др. деятельности.
b) Реквизиты, свидетельствующие о степени секретности сведений.
c) Материальные объекты, в том числе физические поля, в которых сведения находят свое отображение в виде символов.

8. Что такое конфиденциальность?

a) Это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.
b) Гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.
c) Гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

9. Главная проблема, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки?

a) Доступность информации.
b) Целостность информации.
c) Информационная безопасность.

10. Основными документами в направлении ответственности субъектов за нарушения в сфере информационной безопасности являются:

a) Уголовный кодекс Российской Федерации.
b) Кодекс Российской Федерации об административных правонарушениях.
c) Оба варианта верны.
d) Нет правильного ответа.

7.2.2 Примерный перечень заданий для решения стандартных задач

Задача 1. Алгоритмы нахождения простых чисел.

Составить программу, которая будет проверять, является ли введенное число простым. Самый простой путь решения этой задачи - проверить, имеет

ли данное число n (n > 2) делители в интервале [2; n-1]. Если делители есть, число n - составное, если - нет, то - простое. При реализации алгоритма разумно делать проверку на четность введенного числа, поскольку все четные числа делятся на 2 и являются составными числами, то, очевидно, что нет необходимости искать делители для этих чисел. Ввести логическую переменную flag, в программе выступаете в роли "флаговой" переменной и повышает наглядность программы, так, если flag = true, то n -простое число; если у числа n есть делители, то "флаг выключается" с помощью оператора присваивания flag:=false, таким образом, если flag = false, то n - составное число.

Пример реализации на VB6.

```
For j = 3 To N - 1 Step 2
                    k = m Mod j
                If k = 0 And j <> m Then
                        flag = False
                        Form1.BackColor = RGB(256, 0, 0)
                        Text1.FontSize = 16
                       Text1.Text = "Число составное"
                        Exit For
             ElseIf k = 0 And j = m Then
                       flag = True
                       Form1.BackColor = RGB(0, 256, 0)
                       Text1.FontSize = 16
                       Text1.Text = "Введено простое число"
                       Exit For
              End If
 Next j
              MsgBox " k=   " & Str(r) & "   " & "j =   " & Str(j)
              MsgBox "Работа программы завершена"

            End
```

Задача 2. Нахождение простых чисел в заданном интервале. Составить программу, которая напечатает все простые числа в заданном интервале [2, m], для m>3 и подсчитает их количество. Для реализации данного алгоритма необходимо проверить каждое число, находящееся в данном интервале, - простое оно или нет. Однако для этого машине пришлось бы потратить много времени. подумать, каким образом можно оптимизировать алгоритм, описанный в задаче

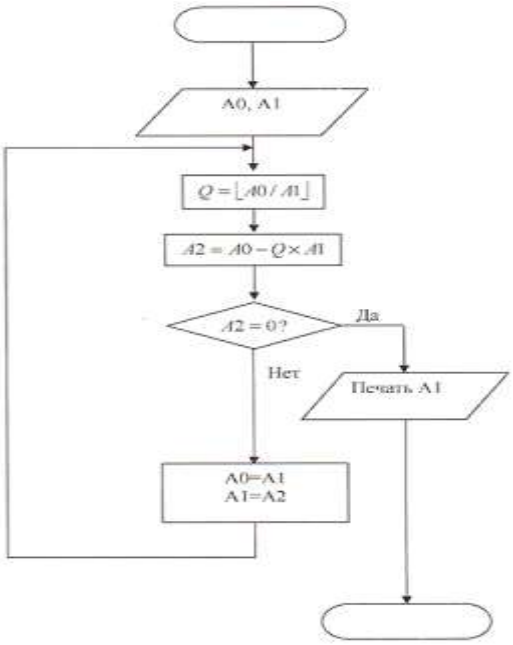
1. При реализации решения выполнять следующие действия:
рассматривать только нечетные числа;

1. прерывать работу цикла, реализующего поиск делителей числа, при нахождении первого же делителя с помощью процедуры Break

(Exit), которая реализует немедленный выход из цикла и передает управление оператору, стоящему сразу за оператором цикла.

2. Счетчик чисел будет находиться в переменной k. Когда очередное простое число найдено, увеличивать k на 1, Простые числа выводятся по 10 в строке, как только значение счетчика становится кратным 10, курсор переводится на новую строку.

Реализовать алгоритм задачи 2 с выводом простых чисел в выходной файл по 10 в строке.



Алгоритм Евклида

НОД(a,n)=1

Одним из способов вычислить наибольший общий делитель двух чисел является **алгоритм Эвклида.** Эвклид описал этот алгоритм в своей книге, *Элементы,* написанной в 300 году до нашей эры. Он не изобрел его. Историки считают, что этот алгоритм лет на 200 старше. Это самый древний нетривиальный алгоритм, который дошел до наших дней, и он все еще хорош. Кнут описал алгоритм и его современные модификации у на языке С:

```
/* возвращает НОД(gcd) x и y*/
 int gcd (int x, int y)
 {
    int g;
    if (x < 0)
          x = -x;
    if (y < 0)
          y = -y;
    if (x + y == 0
ERROR;
    g=y;
```

```
        While (x>0){
                q=x;
                x=y % x;
                y=q;
                }
return q;
}
```

Задача 3. Докажите, что числа 84 и 275 являются взаимно простыми.

Очевидно, что данные числа не являются простыми, поэтому мы не можем сразу говорить о взаимной простоте чисел 84 и 275, и нам придется вычислять НОД. Используем алгоритм Евклида для нахождения НОД: 275=84·3+23,84=23·3+15, 23=15·1+8, 15=8·1+7, 8=7·1+1, 7=7·1, следовательно, НОД(84, 275)=1. Этим доказано, что числа 84 и 275 взаимно простые.

Определение взаимно простых чисел можно расширить для трех и большего количества чисел.

Определение.

Целые числа a1, a2, …, ak, k>2 называются взаимно простыми, если наиболь-ший общий делитель этих чисел равен единице.

Из озвученного определения следует, что если некоторый набор целых чисел имеет положительный общий делитель, отличный от единицы, то данные целые числа не являются взаимно простыми.

Приведем примеры. Три целых числа −99, 17 и −27 являются взаимно про-стыми. Любая совокупность простых чисел составляет набор взаимно простых чисел, к примеру, 2, 3, 11, 19, 151, 293 и 677 – взаимно простые числа. А че-тыре числа 12,−9, 900 и −72 не являются взаимно простыми, так как они име-ют положительный общий делитель 3, отличный от 1. Числа 17, 85 и 187 тоже не взаимно простые, так как каждое из них делится на 17.

Задача 4. Докажите, что числа −14, 105, −2 107 и −91 не являются взаимно простыми

Чтобы доказать, что данные числа не взаимно простые, можно найти их НОД и убедиться, что он не равен единице. Так и поступим.

Так как делители целых отрицательных чисел совпадают с делителями соответ-ствующих противоположных чисел, то НОД(−14, 105, 2 107, −91)=НОД(14, 105, 2 107, 91). Обратившись к материалу статьи нахождение наибольшего общего делителя трех и большего количества чисел, выясняем, что НОД(14, 105, 2 107, 91)=7. Следовательно, наибольший общий делитель исходных чи-сел равен семи, поэтому эти числа не являются взаимно простыми.

Задача 5. Найти результат следующих операций:

a. 27 mod 5

b. 36 mod 12
c. –18 mod 14
d. –7 mod 10

Мы ищем вычет r. Мы можем разделить a на n и найти q и r. Далее можно иг-норировать q и сохранить r.

а. Разделим 27 на 5 - результат: r = 2. Это означает, что 27 mod 5 = 2.

б. Разделим 36 на 12 — результат: r = 0. Это означает, что 36 mod 12 = 0.

в. Разделим (–18) на 14 — результат: r = –4. Однако мы должны прибавить модуль (14), чтобы сделать остаток неотрицательным. Мы имеем r = –4 + 14 = 10. Это означает, что –18 mod 14 = 10.

г. Разделим (–7) на 10 — результат: r = –7. После добавления модуля –7 мы имеем r = 3. Это означает, что –7 mod 10 = 3.

Задача 6. Выполните следующие операции (поступающие от Zn):

a. Сложение 17 и 27 в Z_{14}
b. Вычитание 43 из 12 в Z_{13}
c. Умножение 123 на -10 в Z_{19}

Ниже показаны два шага для каждой операции:

(17 + 27) mod 14 -> (44) mod 14 = 2
(12 – 43) mod 13 -> (–31) mod 13 = 8
((123) x (–10)) mod 19 -> (–1230) mod 19 = 5

Задача 7. определить время перебора всех паролей, состоящих из 6 цифр:

Алфавит составляют цифры n=10.

Длина пароля 6 символов k=6.

Таким образом, получаем количество вариантов: C=nk= 106

Примем скорость перебора s=10 паролей в секунду. Получаем время перебора всех

паролей t= C/s=105 секунд 1667 минут 28 часов 1,2 дня.

Примем, что после каждого из m=3 неправильно введенных паролей идет пауза в v=5 секунд. Получаем время перебора всех паролей

T=t*5/3=1667 *5/3 2778 минут≈ 46 часов 1,9 дня.

Титог = t+T= 1,2+1,9 = 3,1 дня

Задача 8. Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет:

Длина пароля рассчитывается: k=logn C= lg C.

Определим количество вариантов C= t * s=10лет*10 паролей в сек. =

10*10*365*24*60*60 =3,15* 109вариантов.

Таким образом, получаем длину пароля: k=lg (3,15*109) = 9,5

Очевидно, что длина пароля должна быть не менее 10 символов.

Задача 9. Вычислить $c = 5^{13} \bmod 19$.

Переведем степень e=13 в двоичный вид. Для этого заполним следующую таблицу:

e div 2	13	6	3	1
e mod 2	1	0	1	1

Таблица 1. Перевод десятичного числа e к двоичному представлению.

Искомое двоичное разложение числа *e* будет во второй строке таблицы , записанное в обратном порядке справа налево.

Далее, составим таблицу вычисления c, заполняя следующую таблицу:

e	1	1	0	1
c	5	11	7	1 0

Таблица 2. Возведение a=5 в степень e=13 по модулю 19.

В первой строке запишем цифры двоичное разложения числа 13. В первую ячейку второй строки поместим основание *a*=5. Далее каждое следующее значение *c* будем вычислять по формуле:

$$c_{i+1} = \begin{cases} c_i^{\,2} \cdot a \bmod N, \text{ если } e_{i+1} = 1 \\ c_i^{\,2} \bmod N, \text{ если } e_{i+1} = 0 \end{cases}$$

Например,

$$c_2 = 5^2 \cdot 5 \bmod 19 = 125 \bmod 19 = 11$$
$$c_3 = 11^2 \bmod 19 = 121 \bmod 19 = 7$$
$$c_4 = 7^2 \cdot 5 \bmod 19 = 245 \bmod 19 = 17$$

Приведем код на Паскале вычисления функции возведения в степень:

```
Function Rise(A,B,N:Integer):Integer;
var
B2:array[1..20] of byte;
i,C,L:integer;
Begin
      C:=B; i := 1;
   While C > 0   do
   Begin
      B2[i]:= C Mod 2;
      C:= C div 2;
      i:= i + 1;
   End;
   L:= i - 1;
   i:= 1;
   D:= A;
   While i <L do
```

```
    Begin
        D:= (D * D) Mod N;
        If B2[L-i]= 1 Then D:=(D * A) Mod N;
        i := i + 1;
    End;
    Rise := D;
End;
```

Задача 10. Тест Миллера Рабина

Пусть T – произвольное число. Представим T–1 в виде N–1=2s·t, где t – нечет-но. Будем говорить, что число a отвергает число T, если выполнено одно из двух условий:

а) T делится на a,

б) и для всех целых k, .

Если найдется число a, отвергающее T, то T является составным. Тест Миллера выполняется следующим образом:

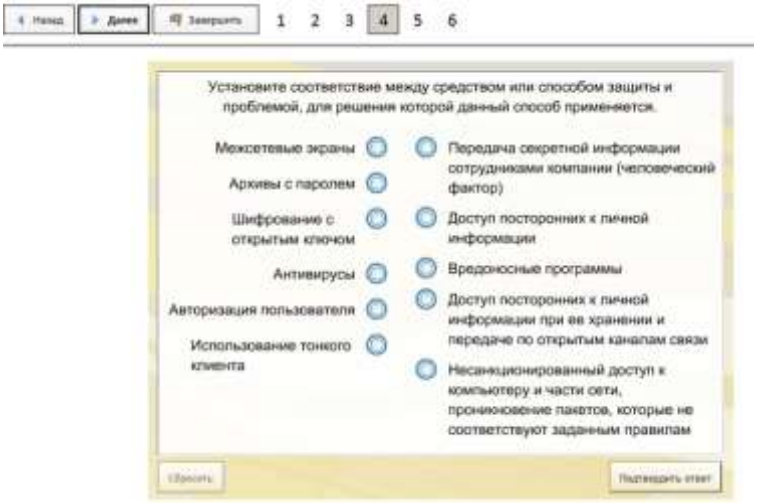
1. Выбираем случайное число a, 1 < a < T, и проверим, что T не делится на a нацело,
2. Проверим далее, что или найдется k, , такое, что

Если какое-то из условий 1 и 2 не будет выполнено, то число T – составное, иначе, ответ не известен. Повторим процедуру с новым a.

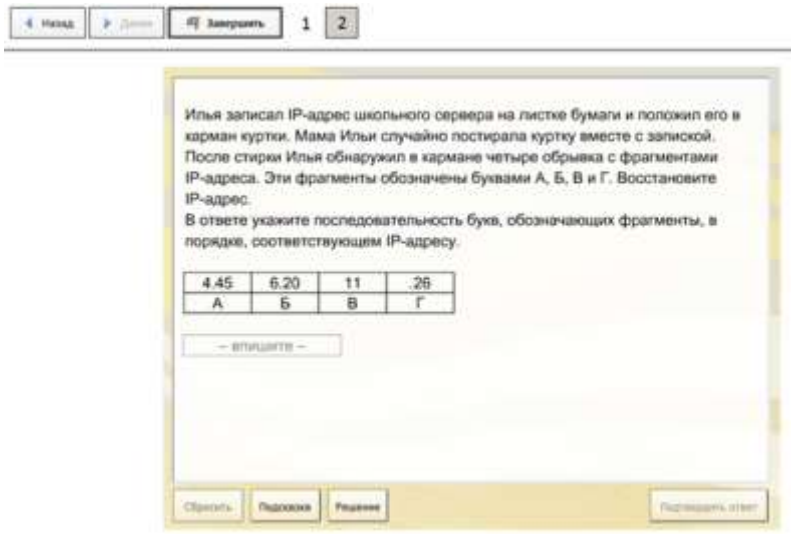
После k циклов вероятность того, что T – составное, меньше 4-k, т.е. убывает очень быстро.

7.2.3 Примерный перечень заданий для решения прикладных задач

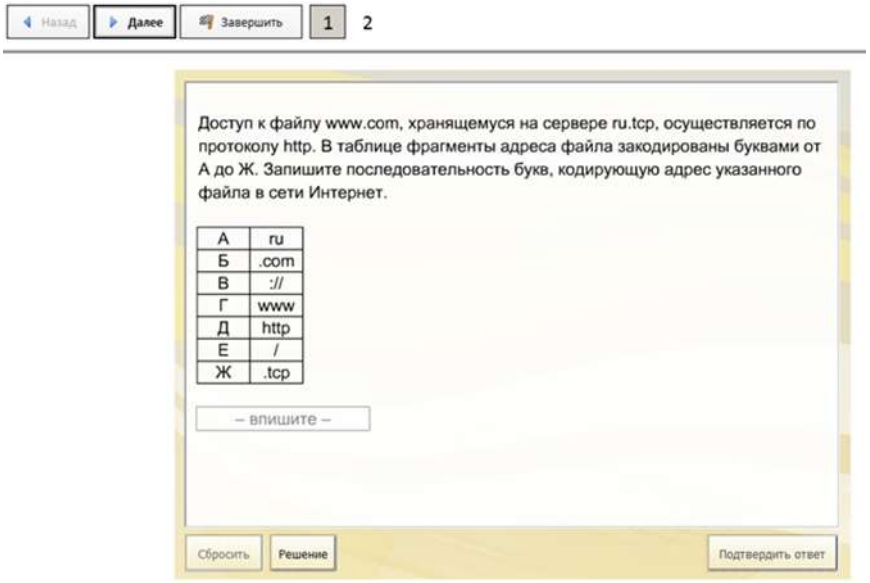
1.



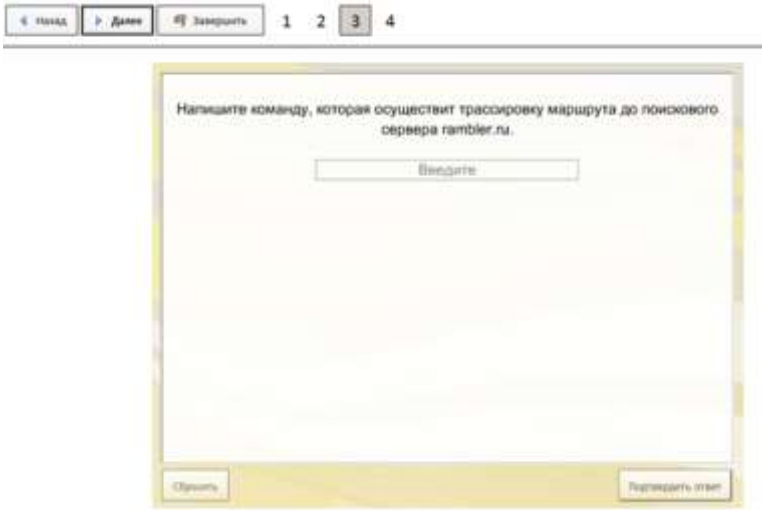
2


Назад
Далее
Завершить
1
2
Илья записал IP-адрес школьного сервера на листке бумаги и положил его в карман куртки. Мама Ильи случайно постирала куртку вместе с запиской. После стирки Илья обнаружил в кармане четыре обрывка с фрагментами IP-адреса. Эти фрагменты обозначены буквами А, Б, В и Г. Восстановите IP-адрес.
В ответе укажите последовательность букв, обозначающих фрагменты, в порядке, соответствующем IP-адресу.
4.45 | 6.20 | 11 | .26
А | Б | В | Г
– впишите –
Сбросить
Подсказка
Решение
Подтвердить ответ

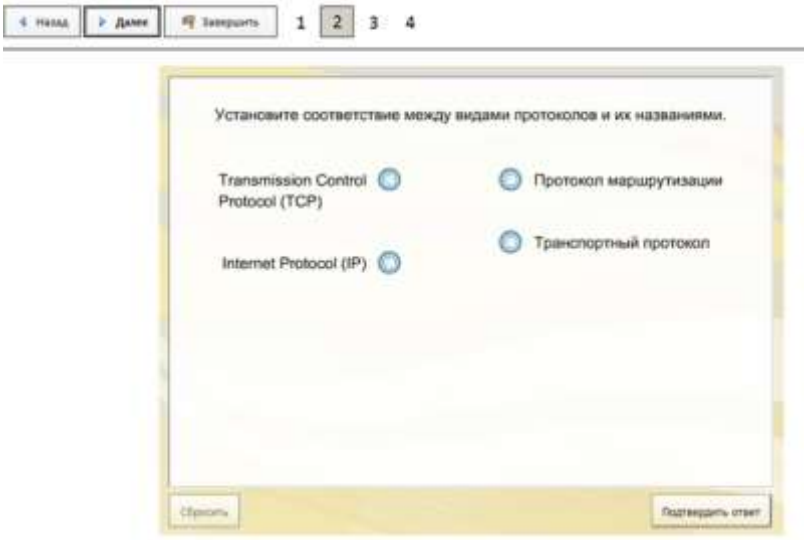
3


Назад
Далее
Завершить
1
2
Доступ к файлу www.com, хранящемуся на сервере ru.tcp, осуществляется по протоколу http. В таблице фрагменты адреса файла закодированы буквами от А до Ж. Запишите последовательность букв, кодирующую адрес указанного файла в сети Интернет.
А | ru
Б | .com
В | ://
Г | www
Д | http
Е | /
Ж | .tcp
– впишите –
Сбросить
Решение
Подтвердить ответ

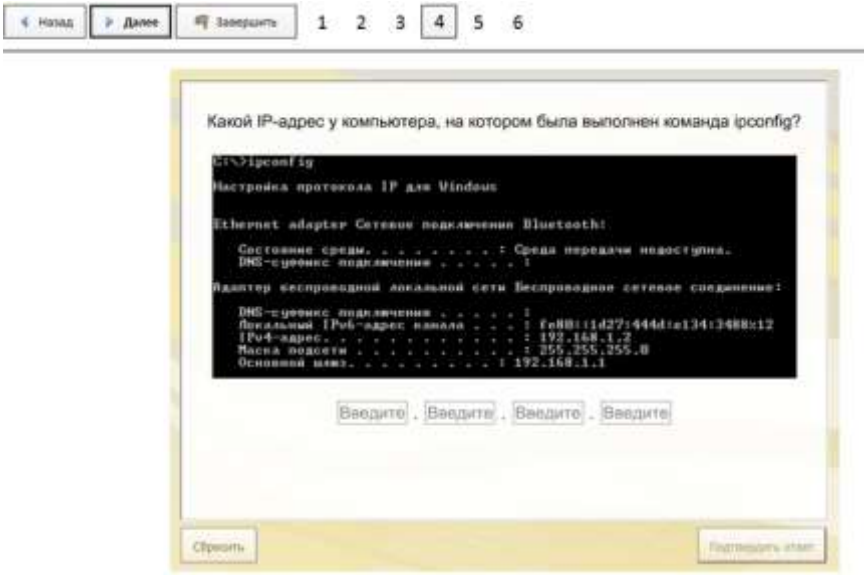
4


Назад
Далее
Завершить
1
2
3
4
Напишите команду, которая осуществит трассировку маршрута до поискового сервера rambler.ru.
Введите
Сбросить
Подтвердить ответ

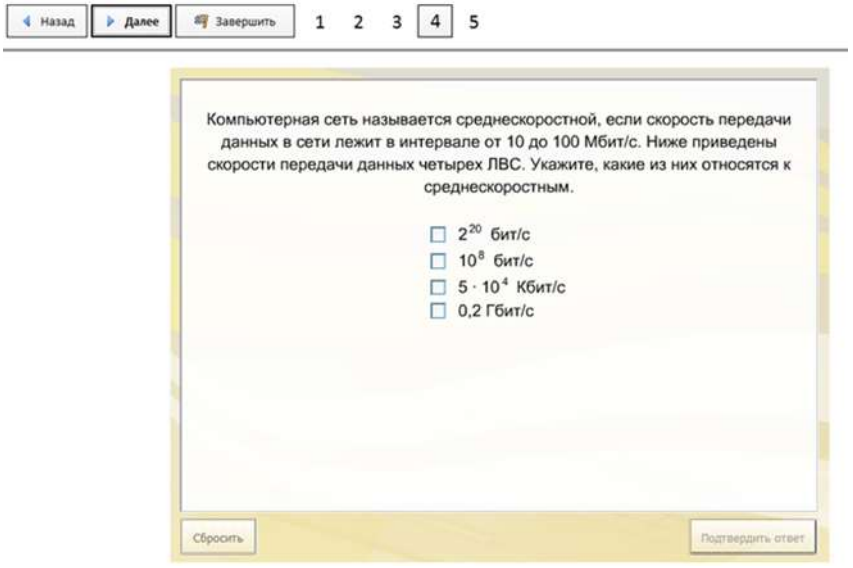
5


Назад
Далее
Завершить
1 2 3 4
Установите соответствие между видами протоколов и их названиями.
Transmission Control Protocol (TCP)
Internet Protocol (IP)
Протокол маршрутизации
Транспортный протокол
Сбросить
Подтвердить ответ

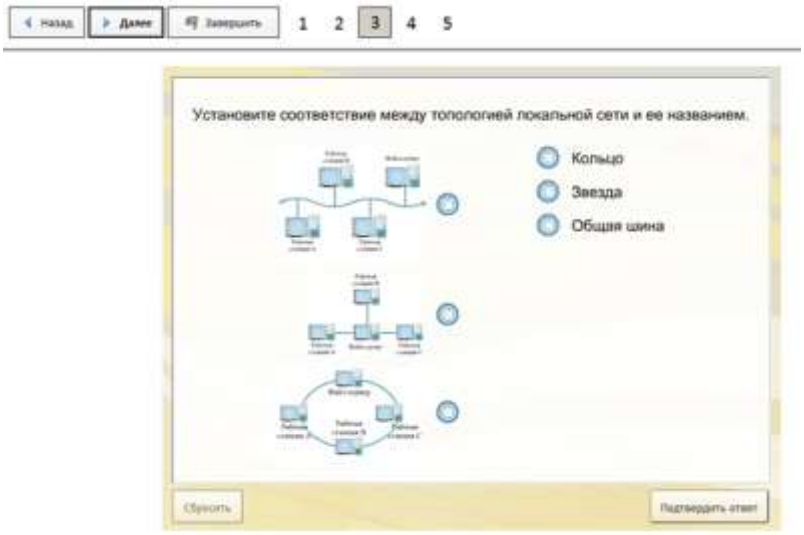
6


Назад
Далее
Завершить
1 2 3 4 5 6
Какой IP-адрес у компьютера, на котором была выполнен команда ipconfig?
C:\>ipconfig
Настройка протокола IP для Windows
Ethernet adapter Сетевое подключение Bluetooth:
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Адаптер беспроводной локальной сети Беспроводное сетевое соединение:
DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . : fe80::1d27:444d:e134:3488%12
IPv4-адрес. . . . . : 192.168.1.2
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : 192.168.1.1
Введите . Введите . Введите . Введите
Сбросить
Подтвердить ответ

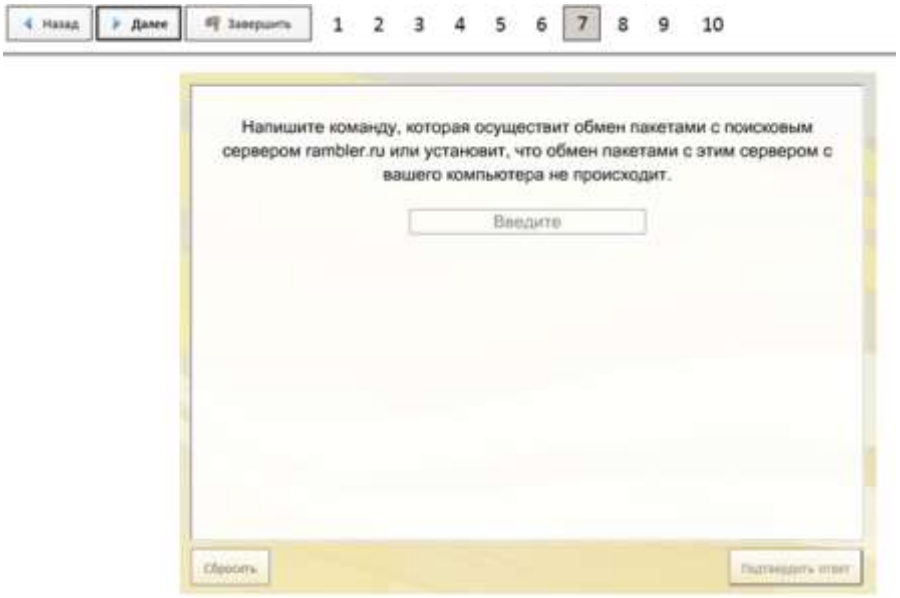
7


Назад
Далее
Завершить
1 2 3 4 5
Компьютерная сеть называется среднескоростной, если скорость передачи данных в сети лежит в интервале от 10 до 100 Мбит/с. Ниже приведены скорости передачи данных четырех ЛВС. Укажите, какие из них относятся к среднескоростным.
2^{20} бит/с
10^8 бит/с
$5 \cdot 10^4$ Кбит/с
0,2 Гбит/с
Сбросить
Подтвердить ответ

8



9



10

1.Получить у преподавателя вариант задания. Ознакомиться с описанием задания и при помощи пакета NetCracker собрать сеть с заданной топологией и спецификацией.

2. Задать сетевой трафик согласно заданию.

3. Вывести статистику в зависимости от варианта. Запустить модель и добиться устойчивой работы сети (без перегрузки). Показать результаты преподавателю.

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для подготовки к зачету

– В любой отрасли понятие «информационная безопасность» подразумевает:

- Самый популярный алгоритм шифрования для Систем открытого взаимодействия?
- Для защиты от вредоносного кода и хакерских атак нужно:
- Чем определяется уровень надежности применяемых криптографических преобразований:
- Что требуется для восстановления зашифрованного текста
- От чего зависит компьютерная безопасность?
- Алгоритм использующий симметричный ключ и алгоритм хэширования:
- Что должно стоять вместо знака «?»
- Кто такой инсайдер?
- Укажите какой из пунктов НЕ является принципом Керкхоффса
- Какой плюс хостовых DLP?
- Что понимается под информационной безопасностью?
- Стек протокола TCP/IP соответствует:
- TCP/IP – набор протоколов
- К какой группе утечек можно отнести утечку коммерческой тайны?
- Что НЕ является нарушением ИБ для отрасли торговли?
- Где применяются средства контроля динамической целостности?
- Бестселлер Дэна Брауна «Код да Винчи» пересыпан разнообразными шифрами и ключами. Каким из них НЕ пользуются герои романа?
- Основными документами в направлении ответственности субъектов за нарушения в сфере информационной безопасности являются:
- В любой отрасли базовый принцип информационной безопасности заключается:
- Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты?
- Когда в криптографии стало использоваться асимметричное шифрование?
- Утилита маскирующая вирус от антивирусной программы:
- Может ли заказчик системы выбирать компоненты системы?
- В чем заключается принцип «Лояльности» в ИБ?
- Что относится к государственной тайне?
- Типовая удаленная атака "отказ в обслуживании" соответствует рисунку
- Назовите нарушение динамической целостности данных:
- Что такое конфиденциальность?
- Кто такой инсайдер?
- Что в переводе с греческого языка означает слово «криптография»?
- Что в криптографии называют открытым текстом?
- Кодирование – это…
- Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое

фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?
- Выявите нарушение правил ИБ в промышленности (завод)
- Разработчик первого алгоритма с открытыми ключами:
- Архитектура безопасности информационных систем опирается на:
- Для решения каких задач может использоваться алгоритм Диффи-Хеллмана?
- К угрозам не относится:
- Под целостностью понимают (выберите продолжение)
- Архитектура безопасности информационных систем (ИС) зависит от:
- Настройка DLP. Классический подход означает…
- Есть ли уровни принципа «лояльности» в организациях? Если есть, то сколько?
- Алгоритм ГОСТ 28147-89 является
- Есть ли уровни политики безопасности организаций? Если есть, то сколько их всего?
- Какой аспект ИБ наиболее актуален для фармацевтической компании, занимающейся разработкой новых лекарств?
- Какие существуют методы реализации антивирусной защиты?
- Какой термин определяет защищенность информации, ресурсов от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений...

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет проводится с группой студентов, в аудитории для проведения лабораторных работ, на индивидуальных персональных компьютерах с привлечением программы компьютерного тестирования «Экзаменатор», которая содержит набор вопросов по изучаемой дисциплине, на которые необходимо ответить студенту. Программа «Экзаменатор» является клиент-серверным приложением. Предъявляемые вопросы выбираются из электронной базы данных и закрепляются за конкретным студентом. Предел длительности контроля - 40 мин. Предлагаемое количество вопросов - 65. Последовательность выборки вопросов – случайная. Оценка «Зачтено» ставится в случае, если студент правильно ответил на 46 вопросов. В случае не сдачи студентом электронного теста, по желанию студента в целях повышения оценки, проводится устный метод контроля, применяется индивидуальная форма, время проведения опроса 10 минут, ответы даются без использования справочной литературы и средств коммуникации, результат сообщается немедленно. Оценка «повышается» студенту, ответившему на два вопроса;

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Понятие "информационная безопасность"	ПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Угрозы информационной безопасности. Виды угроз. Сетевые атаки.	ПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Классификация средств защиты информации. Многоуровневая защита информации. Подходы к обеспечению безопасности автоматизированных систем	ПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Введение в криптографию. История развития. Основные понятия и определения. Архитектура криптографических систем защиты информации.	ПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Информационная Безопасность в Отраслях. Политика безопасности организации. И Б на предприятии: с чего начать. Корпоративная информационная безопасность	ПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Безопасность Информационных Систем. Архитектура безопасности информационных систем. Разработка, механизмы обеспечения.	ПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
	DLP-СИСТЕМЫ	ПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

	Информационная безопасность вычислительных сетей.	ПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
	Классификация удаленных угроз в вычислительных сетях. Принципы защиты, механизмы защиты КС.	ПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 40 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 40 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 40 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Основы управления информационной безопасностью :Учеб. пособие/ А. П. Курило. - М. : Горячая линия -Телеком, 2012. - 244 с. : ил . - (Вопросы управления информационной безопасностью. Кн. 1). – ISBN 978-5-9912-0271-8 : 300-00.

2. Комплексная система защиты информации на предприятии: учеб. пособие / В.Г. Грибунин, В.В. Чудовский. – М.: Издательский центр «Академия», 2009.-416 с.

3. Введение в информационную безопасность автоматизированных систем: учебное пособие/ В.В. Бондарев. – Москва: Издательство МГТУ им. Н.Э. Баумана, 2016. – 250 с.

4. Зубарев И.В., Методические указания к выполнению лабораторных работ по дисциплине «Информационная безопасность и защита информации» для студентов специальности 27.03.04 «Управление в технических системах» (профиль «Управление и информатика в технических системах»./ Зубарев И.В., Воронеж ГОУ ВПО ВГТУ 2018. 72 с.

5. Шилов А.К. Управление информационной безопасностью [Электронный ресурс]: учебное пособие/ Шилов А.К.— Электрон. текстовые данные.— Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018.— 120 с.— Режим доступа:
http://www.iprbookshop.ru/87643.html.— ЭБС «IPRbooks».

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Лицензионное программное обеспечение

Windows Server Standard 2016 R2- сетевая операционная система компании Microsoft. Учебная лицензия. Для академических организаций: Open License

Windows Professional 10 Single Upgrade MVL A Each Academic- операционная система компании Microsoft

Office Professional Plus 2013 Russian OLP NL Academic Edition -пакет офисных приложений компании Microsoft.

RAD Studio XE8 среда быстрой разработки приложений (RAD) фирмы Embarcadero Technologies, работающая под Windows. Разработка приложения для Windows на Delphi/Object Pascal и C++

Свободное ПО

LibreOffice — кроссплатформенный, свободно распространяемый офисный пакет с открытым исходным кодом

Firebird (FirebirdSQL) — кроссплатформенная реляционная система управления базами данных, работающая на macOS, Linux, Microsoft Windows

Oracle VM VirtualBox - программный продукт виртуализации для операционных систем Microsoft Windows, Linux, FreeBSD[7], macOS, Solaris/OpenSolaris, ReactOS, DOS и других. Принадлежит корпорациии Oracle.

Linux openSuse Leap 15.X- операционная система на базе ядра Linux, разработанная сообществом openSUSE Design System. Один дистрибутив объединяет в себе одновременно рабочую станцию и сервер.

NetCracker Professional V4.1-CASE-средство автоматизированного проектирования, моделирования и анализа компьютерных сетей

«Экзаменатор»- клиент-серверное приложение под ОС Windows, собственной разработки, для проведения экзаменов и тестирования студентов.

Отечественное ПО

Astra Linux Common Edition - операционная система на базе ядра Linux, разработанная АО «НПО РусБИТех».

Альт Рабочая станция К 9 - операционная система на базе ядра Linux, разработанная ООО «Базальт СПО»

«Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ»»

Модуль «Программный комплекс поиска текстовых заимствований в открытых источниках сети интернет «Антиплагиат-интернет»»

Модуль обеспечения поиска текстовых заимствований по коллекции диссертаций и авторефератов Российской государственной библиотеки (РГБ)

Модуль поиска текстовых заимствований по коллекции научной электронной библиотеки eLIBRARY.RU

Ресурс информационно-телекоммуникационной сети «Интернет»

http://www.edu.ru/
Образовательный портал ВГТУ

Информационная справочная система

http://window.edu.ru
https://wiki.cchgeu.ru/

Современные профессиональные базы данных

EEE Xplore

Электронная библиотека Институт инженеров по электротехнике и электронике (IEEE) и его партнеров в сфере издательской деятельности.

Адрес ресурса: https://ieeexplore.ieee.org/Xplore/home.jsp

SQL

Сайт, посвященный SQL, программированию, базам данных, разработке информационных систем

Адрес ресурса: https://www.sql.ru/

OpenNet

На сайте проекта OpenNet размещается информация о Unix системах и открытых технологиях для администраторов, программистов и пользователей

Адрес ресурса: http://www.opennet.ru/

Проглаб

Адрес ресурса: https://proglib.io

ХабрХабр

Адрес ресурса: https://habr.com/ru/

Microsoft Developer Network

Адрес ресурса: https://msdn.microsoft.com/ru-ru/

ACMQUEUE

Адрес ресурса: https://queue.acm.org/

The Register

На сайте публикуются актуальные новости из области компьютерных технологий; информация о программном обеспечении, сетях, безопасности; интересные видео, форумы и др.

Адрес ресурса: https://www.theregister.co.uk/

Driver.ru

Адрес ресурса: https://driver.ru/

Хакер

Адрес ресурса: https://xakep.ru/

Исходники.ru

На сайте размещается информация по программированию, администрированию и дизайну

Адрес ресурса: https://forum.sources.ru/

Инструменты разработчика Firefox

Адрес ресурса: https://developer.mozilla.org/ru/docs/Tools

Codewars

Адрес ресурса: https://www.codewars.com/

Uikit

Адрес ресурса: https://getuikit.com/

Dribbble

Адрес ресурса: https://dribbble.com/

Frontender Magazine

Адрес ресурса: https://frontender.info/

PR-CY

Адрес ресурса: https://pr-cy.ru/

1stWebDesigner

Адрес ресурса: https://1stwebdesigner.com/

Weng Vox

Адрес ресурса: https://medium.com/web-engineering-vox

NOUPE

Адрес ресурса: https://www.noupe.com/

Codrops

Адрес ресурса: https://tympanus.net/codrops/category/tutorials/

Bento

Адрес ресурса: https://bento.io/

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

9.1 **Специализированная лекционная аудитория**, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

9.2 **Дисплейный класс**, оснащенный компьютерными программами для проведения лабораторного практикума

9.3 **Натурные лекционные демонстрации**:

- Серверное оборудование (Системное ПО, ЭВМ)
- Активные сетевые устройства (коммутационные устройства, сетевые адаптеры).
- Сетевые комплектующие (кабели, коннекторы);
- Инструмент для монтажа и диагностики компьютерной сети.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Информационная безопасность и защита информации» читаются лекции, проводятся практические занятия и лабораторные работы, выполняется курсовая работа.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков работы алгоритмов нахождения простых чисел, созданию моделей безопасности информационных потоков, модели ролевого разграничения доступа, распространения прав доступа Take-Grant, модели решетки. Занятия проводятся путем решения конкретных задач в аудитории.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсовой работы изложена в учебно-методическом пособии. Выполнять этапы курсовой работы должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсовой работы, защитой курсовой работы.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по

	соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.