МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

27.12.2019 г.

протокол № 3

Зав. кафедрой Стариков Е.Н.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

15 января 2020 г.

протокол № 5

Председатель _____Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Информационная безопасность
Направление подготовки	02.03.03 Математическое обеспечение и администрирование информационных систем
Профиль	Разработка и администрирование информационных систем
Форма обучения	очная
Год набора	2020

Разработана:
Доцент,к.т.н.
Лаптева А.В.

Екатеринбург
2020 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем (уровень бакалавриата) (приказ Минобрнауки России от 23.08.2017г. №809)
ПС	

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

раскрытие сущности информационной безопасности и защиты информации, определение теоретических, методологических и организационных основ обеспечения безопасности информации, ознакомление с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к вариативной части учебного плана.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточный контроль	Часов				З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)		Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лабораторные		
Семестр 5					
Зачет	108	28	28	80	3

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Профессиональные компетенции (ПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
научно-исследовательский	
ПК-8 Способен проводить под научным руководством исследование на основе существующих методов в конкретной области профессиональной деятельности	ИД-1.ПК-8 Знать: основы научной работы, современные методы сбора и анализа полученного материала, способы аргументации; основные принципы защиты информации БД. Уметь: решать научные задачи в связи с поставленной целью и в соответствии с выбранной методикой. Иметь навыки: проведения научных исследований с использованием методов математического моделирования, а также решать задачи, связанные с выбором способов защиты информации БД.
производственно-технологический	

ПК-2 Способен разрабатывать и адаптировать прикладное программное обеспечение	ИД-1.ПК-2 Знать: языки объектно-ориентированного и функционального программирования; языки работы с базами данных; основы современных систем управления базами данных; теорию баз данных. Уметь: кодировать на языках программирования; разрабатывать структуру базы данных; разрабатывать интернет-приложения; разрабатывать сайты и мобильные приложения. Иметь навыки: разработки программного кода на языках объектно-ориентированного и функционального программирования.

Шифр и наименование компетенции	Индикаторы достижения компетенций
УК-8 Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	ИД-1.УК-8 Знать: основы безопасности жизнедеятельности, телефоны служб спасения. Уметь: оказать первую помощь в чрезвычайных ситуациях, создавать безопасные условия реализации профессиональной деятельности. Иметь практический опыт поддержания безопасных условий жизнедеятельности.

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 5		108					
Тема 1.	Основные понятия и анализ угроз информационной безопасности	6				6	
Тема 2.	Криптография и криптоанализ. Математика криптографии	10		4		6	
Тема 3.	Классическая криптография	6				6	
Тема 4.	Симметричные алгоритмы	10		4		6	
Тема 5.	Хэш-функции	10		4		6	
Тема 6.	Электронно-цифровая подпись	6				6	
Тема 7.	Асимметричные алгоритмы	10		4		6	
Тема 8.	Стеганография и стеганоанализ	10		4		6	
Тема 9.	Уязвимости программного	10		4		6	
Тема 10.	Компьютерные вирусы и методы их обнаружения	10		4		6	
Тема 11.	Разделение прав в операционных системах	6				6	
Тема 12.	Методы авторизации и аутентификации пользователей	6				6	
Тема 13.	Безопасность сетей ЭВМ	8				8	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Тема 1.1, тема 1.2, тема 1.3, тема 1.4	Тест №1 (Приложение 4)	Тест по вариантам из 66 вопросов	66 баллов: 1 балл за каждый вопрос
Тема 1.5, тема 1.6, тема 1.7, тема 1.8	Тест №2 (Приложение 4)	Тест по вариантам из 54 вопросов	54 баллов: 1 балл за каждый вопрос
Тема 1.9, тема 1.10, тема 1.11, тема 1.12, тема 1.13	Тест №3 (Приложение 4)	Тест по вариантам из 60 вопросов	60 баллов: 1 балл за каждый вопрос
Промежуточный контроль (Приложение 5)			
5 семестр (За)	Зачетные билеты (Приложение 5)	27 билетов, состоящих из 1 теоретического и 1 практического задания	70 баллов: 20 + 50 соответственно

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущей и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущая аттестация. Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущей аттестации, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.2 Содержание практических занятий и лабораторных работ

Тема 2. Криптография и криптоанализ. Математика криптографии Нахождение НОД. Нахождение модульных инверсий. Нахождение обратных матриц. Испытание простоты чисел
Тема 4. Симметричные алгоритмы шифрования Знакомство с пакетом OpenSSL
Тема 5. Хэш-функции Симметричное шифрование. Работа с пакетом OpenSSL
Тема 7. Асимметричные алгоритмы шифрования Асимметричное шифрование. Работа с пакетом OpenSSL
Тема 8. Стеганография и стеганоанализ Текстовая стеганография. Работа с пакетом OpenPuff
Тема 9. Уязвимости программного обеспечения Исследование уязвимостей программного обеспечения. Работа с программой IDA Pro
Тема 10. Компьютерные вирусы и методы их обнаружения Исследование компьютерных вирусов в дизассемблере. Работа с программой IDA Pro

7.3. Содержание самостоятельной работы

Тема 1. Основные понятия и анализ угроз информационной безопасности Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности и их классификация
Тема 2. Криптография и криптоанализ. Математика криптографии Основные понятия криптографической защиты информации. Модульная арифметика, сравнения и матрицы. Алгебраические структуры (группы, кольца, поля). Простые числа и уравнения
Тема 3. Классическая криптография Симметричные шифры замены и перестановок. Шифры: афинный, Вижинера, Хилла. Криптоанализ классических шифров.
Тема 4. Симметричные алгоритмы шифрования Алгоритмы DES, AES, ГОСТ 28147-89
Тема 5. Хэш-функции Односторонняя функция и односторонняя функция с секретом. Хэш-функции, их свойства и применение. Обзор хэш-функций SHA, Whirpool
Тема 6. Электронно-цифровая подпись Понятие об электронно-цифровая подпись (ЭЦП). Схема формирования ЭЦП.
Тема 7. Асимметричные алгоритмы шифрования Алгоритм RSA, системы шифрования на эллиптических кривых
Тема 8. Стеганография и стеганоанализ Классическая и компьютерная стеганография. Методы компьютерной стеганографии. Цифровые водяные знаки. Стеганоанализ. Методы стеганоанализа
Тема 9. Уязвимости программного обеспечения Уязвимости переполнения буфера, переполнения целочисленных значений, форматирующей строки, возвращения управления в libc. Основы работы с отладчиком и дизассемблером
Тема 10. Компьютерные вирусы и методы их обнаружения Классификация вредоносного программного обеспечения. Способы обнаружения компьютерных вирусов. Антивирусы
Тема 11. Разделение прав в операционных системах Принципы построения многопользовательской операционной системы. Принципы организации безопасности на уровне операционной системы

Тема 12. Методы авторизации и аутентификации пользователей Методы авторизации и аутентификации пользователей. Фиксированные и одноразовые пароли.
Тема 13. Безопасность сетей ЭВМ Безопасность на прикладном, на транспортном, на сетевом уровнях. Принципы построения виртуальных защищенных сетей. Принципы работы межсетевых экранов и систем обнаружения вторжений.

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
Не предусмотрено

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
Материалы не предусмотрены

7.6 Методические рекомендации по выполнению курсовой работы
материалы не предусмотрены

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

1. Глинская Е.В., Чичварин Н.В.. Информационная безопасность конструкций ЭВМ и систем:учебное пособие для студентов вузов, обучающихся по направлениям подготовки 09.03.03 "Прикладная информатика" и 10.03.01 "Информационная безопасность" (квалификация (степень) "бакалавр"). - Москва: ИНФРА-М, 2019. - 118 с.

2. Крамаров С.О., Тищенко Е.Н.. Криптографическая защита информации:Учебное пособие. - Москва: Издательский Центр РИОР, 2019. - 324 с.

3. Крамаров С. О., Митясова О. Ю., Соколов С. В., Тищенко Е. Н., Шевчук П. С., Крамаров С. О.. Криптографическая защита информации:учебное пособие. - Москва: РИОР: ИНФРА-М, 2018. - 321 с.

4. Крамаров С.О., Тищенко Е.Н.. Криптографическая защита информацииv922:. - Москва: Издательский Центр РИОР, 2019. - 324 с.

5. Крамаров С.О., Тищенко Е.Н.. Криптографическая защита информации [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИОР, 2018. - 324 с. – Режим доступа: https://new.znanium.com/catalog/product/901659

6. Глинская Е.В., Чичварин Н.В.. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2018. - 118 с. – Режим доступа: https://new.znanium.com/catalog/product/925825

7. Шаньгин В. Ф.. Комплексная защита информации в корпоративных системах [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2019. - 592 с. – Режим доступа: https://new.znanium.com/catalog/product/996789

8. Крамаров С.О., Тищенко Е.Н.. Криптографическая защита информации [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИОР, 2019. - 324 с. – Режим доступа: https://new.znanium.com/catalog/product/1018903

9. Крамаров С. О., Митясова О. Ю., Соколов С. В., Тищенко Е. Н., Шевчук П. С., Крамаров С. О.. Криптографическая защита информации [Электронный ресурс]:учебное пособие. - Москва: РИОР: ИНФРА-М, 2018. - 321 с. – Режим доступа: http://znanium.com/go.php?id=901659

10. Крамаров С.О., Тищенко Е.Н.. Криптографическая защита информации [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО, 2019. - 324 с. – Режим доступа: http://znanium.com/go.php?id=1018903znanium.com

Дополнительная литература:

1. Ковалев Д. В., Богданова Е. А.. Информационная безопасность:учебное пособие. - Ростов-на-Дону: Издательство Южного федерального университета (ЮФУ), 2016. - 74 с.

2. Бирюков А. А.. Информационная безопасность: защита и нападение:производственно-практическое издание. - Москва: ДМК Пресс, 2017. - 433 с.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионное программное обеспечение:

Microsoft Windows 10 .Акт предоставления прав № Tr060590 от 19.09.2017. Срок действия лицензии 30.09.2020.

Microsoft Office 2016. Акт предоставления прав № Tr060590 от 19.09.2017. Срок действия лицензии 30.09.2020.

Adobe Reader. Лицензия freeeware. Срок действия лицензии - без органичения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации

Приложение 1

к рабочей программе

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену

К зачету

1. Научные и законодательные определения информации. Соотношение понятий «информация», «документированная информация», «информационные ресурсы», «документ».
2. Сущность и понятие информационной безопасности. Связь информационной безопасности с информатизацией общества.
3. Понятие и назначение доктрины информационной безопасности. Основные положения доктрины информационной безопасности Российской Федерации и их реализация.
4. Сущность и понятие защиты информации. Уязвимость информации. Цели защиты информации.
5. Законодательная база защиты документированной информации в РФ.
6. Подзаконные нормативно-правовые акты в сфере защиты информации.
7. Понятие и виды конфиденциальной информации в современном российском законодательстве.
8. Государственная тайна, ее нормативное регулирование.
9. Правовой режим персональных данных. Общая характеристика Федерального закона «О персональных данных»
10. Понятие коммерческой тайны. Общая характеристика Федерального закона «О коммерческой тайне».
11. Понятие и разновидности служебной и профессиональной тайн.
12. Перечень конфиденциальных сведений и Перечень конфиденциальных документов, методика их формирования.
13. Служба конфиденциального делопроизводства, ее статус в структуре организации. Квалификационные характеристики и требования к сотрудникам службы КД.
14. Цели и задачи, права и обязанности, нормативно-методическая база службы КД
15. Анализ угроз несанкционированного получения документированной информации, хищения или уничтожения документов, их фальсификации или подмены. Предполагаемые рубежи и уровни защиты документопотоков
16. Понятие «защищенный документооборот», его цели и задачи.
17. Гриф ограничения доступа к документу: понятие, назначение, виды.
18. Избирательность и разрешительная система доступа к конфиденциальным документам.
19. Прием и регистрация конфиденциальных документов.
20. Принципы и этапы документирования конфиденциальных сведений.
21. Учетные формы: виды, правила оформления и ведения.
22. Составление, учет и уничтожение проектов конфиденциальных документов.
23. Особенности оформления реквизитов конфиденциальных документов.
24. Правила издания, копирования и тиражирования конфиденциальных документов
25. Экспедиционная обработка исходящих конфиденциальных документов.
26. Организация и контроль исполнения конфиденциальных документов. Правила работы исполнителя.
27. Экспертиза ценности конфиденциальных документов
28. Номенклатура конфиденциальных дел. Установление сроков конфиденциальности при составлении номенклатуры дел.
29. Правила формирования и оформления конфиденциальных дел.
30. Учет выдачи дел во временное пользование.
31. Подготовка конфиденциальных дел и документов для архивного хранения.

Приложение 2

к рабочей программе

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену

Примерные практические задания к зачету

Задание 1. Используя любой язык программирования, напишите программу, реализующую модифицированный шифр Цезаря (ключом является любое число).

Задание 2. Используя любой язык программирования, напишите программу, реализующую моноалфавитный шифр (шифр простой замены)

Задание 3. Используя любой язык программирования, напишите программу, реализующую шифр Гронсфельда

Задание 4. Используя любой язык программирования, напишите программу, реализующую шифр Плейфейера

Задание 5. Используя любой язык программирования, напишите программу, реализующую шифр Хилла

Задание 6. Используя любой язык программирования, напишите программу, реализующую простой перестановочный шифр

Задание 7. Используя любой язык программирования, напишите программу, реализующую решетку Флейберга

Задание 8. Используя любой язык программирования, напишите программу, реализующую скремблер

Задание 9. Напишите программу, реализующую протокол строгой двусторонней аутентификации на основе случайных чисел. Используйте Шифр Хилла в качестве симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования.

Задание 10. Напишите программу, реализующую протокол строгой двусторонней аутентификации на основе случайных чисел. Используйте Шифр Гронсфельда в качестве симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования.

Задание 11. Напишите программу, реализующую протокол строгой двусторонней аутентификации на основе случайных чисел. Используйте решетку Флейберга в качестве симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования.

Задание 12. Напишите программу, реализующую протокол строгой двусторонней аутентификации на основе случайных чисел. Используйте Шифр Плейфейера в качестве симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования.

Задание 13. Запрограммируйте линейный конгруэнтный генератор псевдослучайных чисел.

Задание 14. Запрограммируйте смешанный квадратичный генератор псевдослучайных чисел

Задание 15. Разработайте программу, реализующую модель безопасности Белла-ЛаПадула. Основные функции программы: регистрация пользователей (при регистрации пользователь получает уровень допуска), авторизация, создание текстовых заметок (при создании заметка получает уровень секретности), просмотр и редактирование заметок.

Задание 16. Разработайте программу, реализующую диспетчер безопасности на основе ACL. Функции программы: регистрация объектов, регистрация субъектов, просмотр и редактирование привилегий, вход от лица субъекта и попытка доступа к объекту.

Задание 17. Разработайте программу, реализующую диспетчер безопасности на основе списков полномочий субъектов. Функции программы: регистрация объектов, регистрация субъектов, просмотр и редактирование привилегий, вход от лица субъекта и попытка доступа к объекту.

Приложение 4

к рабочей программе

Федеральное государственное бюджетное образовательное учреждение высшего образования

УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНЫ

на заседании кафедры Шахматного искусства и компьютерной математики

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ

ТЕКУЩЕГО КОНТРОЛЯ

по дисциплине

Информационная безопасность

Тест №1 по темам «Основные понятия и анализ угроз информационной безопасности», «Криптография и криптоанализ. Математика криптографии», «Классическая криптография», «Симметричные алгоритмы шифрования»

1. Что означает термин «Безопасность информации»?

1. Защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.
2. Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию.
3. Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

2. Кто является хакером?

1. Это лица, проявляющие чрезмерный интерес к устройству сложных систем, как правило компьютерных, и в следствии этого интереса обладающие большими познаниями по части архитектуры и принципов устройства вычислительной среды или технологии телекоммуникаций, что используется для похищения информации.
2. Это лица, изучающие систему с целью ее взлома. Они реализуют свои криминальные наклонности в похищении информации и написании разрушающего программного обеспечения и вирусов, при этом применяют различные способы атак на компьютерную систему, используя принципы построения протоколов сетевого обмена.
3. Это лица, которые «взламывая» интрасети, получают информацию о топологии этих сетей, используемых в них программно-аппаратных средствах и информационных ресурсах, а также реализованных методах защиты. Эти сведения они продают заинтересованным лицам.

3. Кто является кракером?

1. Это лица, изучающие систему с целью ее взлома. Они реализуют свои криминальные наклонности в похищении информации и написании разрушающего программного обеспечения и вирусов, при этом применяют различные способы атак на компьютерную систему, используя принципы построения протоколов сетевого обмена.
2. Это лица, проявляющие чрезмерный интерес к устройству сложных систем, как правило компьютерных, и в следствии этого интереса обладающие большими познаниями по части архитектуры и принципов устройства вычислительной среды или технологии телекоммуникаций, что используется для похищения информации.
3. Это лица, которые «взламывая» интрасети, получают информацию о топологии этих сетей, используемых в них программно-аппаратных средствах и информационных ресурсах, а также реализованных методах защиты. Эти сведения они продают заинтересованным лицам.

4. Кто является фракером?

1. Это лица, которые «взламывая» интрасети, получают информацию о топологии этих сетей, используемых в них программно-аппаратных средствах и информационных ресурсах, а также реализованных методах защиты. Эти сведения они продают заинтересованным лицам.
2. Это лица, проявляющие чрезмерный интерес к устройству сложных систем, как правило компьютерных, и в следствии этого интереса обладающие большими познаниями по части архитектуры и принципов устройства вычислительной среды или технологии телекоммуникаций, что используется для похищения информации.
3. 3. Это лица, изучающее систему с целью ее взлома. Они реализуют свои криминальные наклонности в похищении информации и написании разрушающего программного обеспечения и вирусов. При этом применяют различные способы атак на компьютерную систему, используя принципы построения протоколов сетевого обмена.

5. Что означает термин «Доступность информации»?

1. Это свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.
2. Это свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).
3. Это подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.

6. Что означает термин «Целостность информации»?

1. Это свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).
2. Это свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.
3. Это подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.

7. Что означает термин «Уязвимость информации»?

1. Это подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.
2. Это свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.
3. Это свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

8. В чем заключается конфиденциальность компонента системы?

1. В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.
2. В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.
3. В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

9. В чем заключается целостность компонента системы?

1. В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.
2. В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.
3. В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

10. В чем заключается доступность компонента системы?

1. В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).
2. В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.
3. В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.

11. Что означает термин «Правовые меры защиты информации»?

1. Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие

тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.
2. Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации.
3. Это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.
4. Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам автоматических систем и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.
5. Это различные электронные устройства и специальные программы, входящие в состав автоматических систем, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

12. Что означает термин «Морально-этические меры защиты информации»?

1. Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации.
2. Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.
3. Это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.
4. Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам автоматических систем и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.
5. Это различные электронные устройства и специальные программы, входящие в состав автоматических систем, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

13. Что означает термин «Организационные (административные) меры защиты информации»?

1. Это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.
2. Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.
3. Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как

законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации.
4. Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам автоматических систем и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.
5. Это различные электронные устройства и специальные программы, входящие в состав автоматических систем, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

14. Что означает термин «Физические меры защиты информации»?

1. Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам автоматических систем и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.
2. Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.
3. Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации.
4. Это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.
5. Это различные электронные устройства и специальные программы, входящие в состав автоматических систем, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

15. Что означает термин «Технические (аппаратно-программные) средства защиты информации»?

1. Это различные электронные устройства и специальные программы, входящие в состав автоматических систем, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).
2. Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.
3. Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации.
4. Это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.
5. Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях

проникновения и доступа потенциальных нарушителей к компонентам автоматических систем и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.

16. Что означает термин «Аутентификация»?

1. Это проверка подлинности субъекта или объекта.
2. Это проверка целостности информации, программы, документа и т.д.
3. Это присвоение имени субъекту или объекту.

17. Что означает термин «Верификация»?

1. Это проверка целостности информации, программы, документа и т.д.
2. Это проверка подлинности субъекта или объекта.
3. Это присвоение имени субъекту или объекту.

18. Что означает термин «Идентификация»?

1. Это присвоение имени субъекту или объекту.
2. Это проверка подлинности субъекта или объекта.
3. Это проверка целостности информации, программы, документа и т.д.

19. Что означает термин «Криптография»?

1. Это метод специального преобразования информации с целью сокрытия от посторонних лиц.
2. Это преобразование информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и ввода-вывода.
3. Это криптографическое преобразование информации при ее передаче по каналам связи от одного элемента вычислительной сети к другому.

20. Что означает термин «Кодирование информации»?

1. Это преобразование информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и ввода-вывода.
2. Это метод специального преобразования информации с целью сокрытия от посторонних лиц.
3. Это криптографическое преобразование информации при ее передаче по каналам связи от одного элемента вычислительной сети к другому.

21. Что означает термин «Линейное шифрование»?

1. Это криптографическое преобразование информации при ее передаче по каналам связи от одного элемента вычислительной сети к другому.
2. Это метод специального преобразования информации с целью сокрытия от посторонних лиц.
3. Это преобразование информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и ввода-вывода.

22. Как классифицируются виды угроз информации по природе возникновения?

1. Стихийные бедствия, несчастные случаи, ошибки обслуживающего персонала и пользователей, злоупотребления обслуживающего персонала и пользователей, злоумышленные действия нарушителей, сбои и отказы оборудования.
2. Угрозы персоналу, информации, информационным системам, материальным, финансовым, информационным данным.
3. Угрозы информационным системам, материальным, финансовым, информационным данным, злоумышленные действия нарушителей, сбои и отказы оборудования.

23. Как классифицируются виды угроз информации по ориентации на ресурсы?

1. Угрозы персоналу, информации, информационным системам, материальным, финансовым, информационным данным.
2. Стихийные бедствия, несчастные случаи, ошибки обслуживающего персонала и пользователей, злоупотребления обслуживающего персонала и пользователей, злоумышленные действия нарушителей, сбои и отказы оборудования.

3. Угрозы информационным системам, материальным, финансовым, информационным данным, злоумышленные действия нарушителей, сбои и отказы оборудования.

24. Какие угрозы информации относятся к естественным?

1. отказы и сбои аппаратуры;
помехи на линиях связи от воздействий внешней среды;

аварийные ситуации;

стихийные бедствия.

2. ошибки человека как звена системы;
схемные и системотехнические ошибки разработчиков;

структурные, алгоритмические и программные ошибки;

действия человека, направленные на несанкционированные воздействия на информацию.

3. аварийные ситуации;
стихийные бедствия;

ошибки человека как звена системы;

схемные и системотехнические ошибки разработчиков.

25. Какие угрозы информации относятся к искусственным?

1. ошибки человека как звена системы;
схемные и системотехнические ошибки разработчиков;

структурные, алгоритмические и программные ошибки;

действия человека, направленные на несанкционированные воздействия на информацию.

2. отказы и сбои аппаратуры;
помехи на линиях связи от воздействий внешней среды;

аварийные ситуации;

стихийные бедствия.

3. аварийные ситуации;
стихийные бедствия;

ошибки человека как звена системы;

схемные и системотехнические ошибки разработчиков.

26. Какие угрозы информации относятся к случайным?

1. проявление ошибок программно-аппаратных средств автоматических систем;
некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;

неправомерное включение оборудования или изменение режимов работы устройств и программ;

неумышленная порча носителей информации;

пересылка данных по ошибочному адресу абонента (устройства).

2. несанкционированное чтение информации;

несанкционированное изменение информации;

несанкционированное уничтожение информации;

полное или частичное разрушение операционной системы.

3. пересылка данных по ошибочному адресу абонента (устройства);
ввод ошибочных данных;

несанкционированное уничтожение информации;

полное или частичное разрушение операционной системы.

27. Какие угрозы информации относятся к преднамеренным?

1. несанкционированное чтение информации;
несанкционированное изменение информации;

несанкционированное уничтожение информации;

полное или частичное разрушение операционной системы.

2. проявление ошибок программно-аппаратных средств автоматических систем;
некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;

неправомерное включение оборудования или изменение режимов работы устройств и программ;

неумышленная порча носителей информации;

пересылка данных по ошибочному адресу абонента (устройства).

3. пересылка данных по ошибочному адресу абонента (устройства);
ввод ошибочных данных;

несанкционированное уничтожение информации;

полное или частичное разрушение операционной системы.

28. Источником каких угроз информации является природная среда?

1. стихийные бедствия;
магнитные бури;

радиоактивное излучение.

2. внедрение агентов в число персонала системы;
вербовка персонала или отдельных пользователей, имеющих определенные полномочия;

угроза несанкционированного копирования секретных данных пользователем;

разглашение, передача или утрата атрибутов разграничения доступа.

3. запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
возникновение отказа в работе операционной системы.

4. нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

заражение компьютера вирусами с деструктивными функциями.

29. Источником каких угроз информации является человек?

1. внедрение агентов в число персонала системы;

вербовка персонала или отдельных пользователей, имеющих определенные полномочия;

угроза несанкционированного копирования секретных данных пользователем;

разглашение, передача или утрата атрибутов разграничения доступа.

стихийные бедствия;

магнитные бури;

радиоактивное излучение.

2. запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

возникновение отказа в работе операционной системы.

3. нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

заражение компьютера вирусами с деструктивными функциями.

30. Источником каких угроз информации являются санкционированные программно-аппаратные средства?

1. запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

возникновение отказа в работе операционной системы.

2. стихийные бедствия;

магнитные бури;

радиоактивное излучение.

3. внедрение агентов в число персонала системы;

вербовка персонала или отдельных пользователей, имеющих определенные полномочия;

угроза несанкционированного копирования секретных данных пользователем;

разглашение, передача или утрата атрибутов разграничения доступа.

4. нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

заражение компьютера вирусами с деструктивными функциями.

31. Источником каких угроз информации являются несанкционированные программно-аппаратные средства?

1. нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

заражение компьютера вирусами с деструктивными функциями.

2. стихийные бедствия;

магнитные бури;

радиоактивное излучение.

3. внедрение агентов в число персонала системы;

вербовка персонала или отдельных пользователей, имеющих определенные полномочия;

угроза несанкционированного копирования секретных данных пользователем;

разглашение, передача или утрата атрибутов разграничения доступа.

4. запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

возникновение отказа в работе операционной системы.

32. Какими основными свойствами обладает компьютерный вирус?

1. способностью к созданию собственных копий;

наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.

2. способностью к созданию собственных копий;

способностью уничтожать информацию на дисках;

способность создавать всевозможные видео и звуковые эффекты.

3. наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы;

способностью оставлять в оперативной памяти свою резидентную часть;

способностью вируса полностью или частично скрыть себя в системе.

33. Как классифицируются вирусы в зависимости от среды обитания?

1. файловые;

загрузочные;

макровирусы;

сетевые.

2. Заражающие DOS, Windows, Win95/NT, OS/2, Word, Excel, Office 97.
3. использование резидентность;

использование «стелс»-алгоритмов;

использование самошифрование и полиморфичность;

использование нестандартных приемов.

4. безвредные;
неопасные;

опасные;

очень опасные.

34. Как классифицируются вирусы в зависимости от заражаемой ОС?

1. Заражающие DOS, Windows, Win95/NT, OS/2, Word, Excel, Office 97.
2. файловые;
загрузочные;

макровирусы;

сетевые.

3. использование резидентность;
использование «стелс»-алгоритмов;

использование самошифрование и полиморфичность;

использование нестандартных приемов.

4. безвредные;
неопасные;

опасные;

очень опасные.

35. Как классифицируются вирусы в зависимости от особенностей алгоритма работы?

1. использование резидентность;
использование «стелс»-алгоритмов;

использование самошифрование и полиморфичность;

использование нестандартных приемов.

2. файловые;
загрузочные;

макровирусы;

сетевые.

3. Заражающие DOS, Windows, Win95/NT, OS/2, Word, Excel, Office 97.
4. безвредные;
неопасные;

опасные;

очень опасные.

36. Как классифицируются вирусы в зависимости от деструктивных возможностей?

1. безвредные;
2. неопасные;
опасные;

очень опасные.

3. файловые;
загрузочные;

макровирусы;

сетевые.

4. Заражающие DOS, Windows, Win95/NT, OS/2, Word, Excel, Office 97.
5. использование резидентность;
использование «стелс»-алгоритмов;

использование самошифрование и полиморфичность;

использование нестандартных приемов.

37. В чем заключается принцип работы файлового вируса?

1. Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы;
2. записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.
3. Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.
4. Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

38. В чем заключается принцип работы загрузочного вируса?

1. Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.
2. Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы;
3. Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.
4. Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

39. В чем заключается принцип работы макровируса?

1. Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.
2. Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы;
3. Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.
4. Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

40. В чем заключается принцип работы сетевого вируса?

1. Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.
2. Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы;
3. Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.
4. Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.

41. На чем основан алгоритм работы резидентного вируса?

1. Вирус при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы

находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.
2. Использование этих алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов и затем вирусы либо временно лечат их, либо подставляют вместо себя незараженные участки информации.
3. Используются для того, чтобы максимально усложнить процедуру обнаружения вируса. Эти вирусы достаточно трудно поддаются обнаружению, они не имеют сигнатур, т.е. не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного и того же вируса не будут иметь ни одного совпадения.

42. На чем основан алгоритм работы вируса с использованием «стелс»-алгоритмов?

1. Использование этих алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов, затем вирусы либо временно лечат их, либо подставляют вместо себя незараженные участки информации.
2. Вирус при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.
3. Используются для того, чтобы максимально усложнить процедуру обнаружения вируса. Эти вирусы достаточно трудно поддаются обнаружению, они не имеют сигнатур, т.е. не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного и того же вируса не будут иметь ни одного совпадения.

43. На чем основан алгоритм работы вируса с использованием самошифрования и полиморфичности?

1. Используются для того, чтобы максимально усложнить процедуру обнаружения вируса. Эти вирусы достаточно трудно поддаются обнаружению, они не имеют сигнатур, т.е. не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного и того же вируса не будут иметь ни одного совпадения.
2. Вирус при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.
3. Использование этих алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов, затем вирусы либо временно лечат их, либо подставляют вместо себя незараженные участки информации.

44. По деструктивным возможностям, как влияют на работу компьютера безвредные вирусы?

1. Никак не влияющие на работу компьютера кроме уменьшения свободной памяти на диске в результате своего распространения.
2. Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами.
3. Могут привести к серьезным сбоям в работе компьютера.
4. В алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

45. По деструктивным возможностям, как влияют на работу компьютера неопасные вирусы?

1. Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами.
2. Никак не влияющие на работу компьютера кроме уменьшения свободной памяти на диске в результате своего распространения.
3. Могут привести к серьезным сбоям в работе компьютера.

4. В алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

46. По деструктивным возможностям, как влияют на работу компьютера опасные вирусы?

1. Могут привести к серьезным сбоям в работе компьютера.
2. Никак не влияющие на работу компьютера кроме уменьшения свободной памяти на диске в результате своего распространения.
3. Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами.
4. В алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

47. По деструктивным возможностям, как влияют на работу компьютера очень опасные вирусы?

1. В алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.
2. Никак не влияющие на работу компьютера кроме уменьшения свободной памяти на диске в результате своего распространения.
3. Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами.
4. Могут привести к серьезным сбоям в работе компьютера.

48. По способу заражения файловых вирусов, как работают overwriting-вирусы?

1. Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое.
2. Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.
3. Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.
4. При запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.
5. Вирусы никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем.

49. По способу заражения файловых вирусов, как работают parasitic-вирусы?

1. Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.
2. Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое.
3. Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.
4. Вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.
5. Вирусы никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем.

50. По способу заражения файловых вирусов, как работают companion-вирусы?

1. Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.
2. Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое.

3. Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.
4. Вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполнит свой код. Этой цели они достигают модификацией необходимых полей файловой системы.
5. Вирусы никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем.

51. По способу заражения файловых вирусов, как работают link-вирусы?

1. Вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.
2. Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое.
3. Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.
4. Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.
5. Вирусы никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем.

52. По способу заражения файловых вирусов, как работают файловые черви?

1. Вирусы никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем.
2. Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое.
3. Вирус при распространении своих копий обязательно изменяет содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.
4. Вирус не изменяет заражаемых файлов. Алгоритм работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.
5. Вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

53. Какие программы относятся к программам «Троянские кони» (логические бомбы)?

1. Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.
2. Это программы, которые на первый взгляд являются стопроцентными вирусами, но неспособны размножаться по причине ошибок. Например, вирус, который при заражении «забывает» поместить в начало файлов команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (что в подавляющем большинстве случаев завешивает компьютер).
3. Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы.
4. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

54. Какие программы относятся к программам Intended-вирусы?

1. Это программы, которые на первый взгляд являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении «забывает» поместить в начало файлов команду передачи управления на код вируса, либо

записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (что в подавляющем большинстве случаев завешивает компьютер).
2. Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.
3. Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы.
4. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

55. Какие программы относятся к программам Конструкторы вирусов?

1. Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы.
2. Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.
3. Это программы, которые на первый взгляд являются стопроцентными вирусами, но неспособны размножаться по причине ошибок. Например, вирус, который при заражении «забывает» поместить в начало файлов команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (что в подавляющем большинстве случаев завешивает компьютер).
4. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

56. Какие программы относятся к программам полиморфик-генераторы?

1. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.
2. Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.
3. Это программы, которые на первый взгляд являются стопроцентными вирусами, но неспособны размножаться по причине ошибок. Например, вирус, который при заражении «забывает» поместить в начало файлов команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (что в подавляющем большинстве случаев завешивает компьютер).
4. Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы.

57. На чем основан принцип работы антивирусных мониторов?

1. На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю.
2. На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски.
3. На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т. д.
4. На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные.

58. На чем основан принцип работы антивирусных иммунизаторов?

1. На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные.

2. На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски.
3. На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т. д.
4. На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю.

59. Что необходимо сделать при обнаружении файлового вируса?

1. Компьютер необходимо отключить от сети и проинформировать системного администратора.
2. Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.
3. Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен.

60. Что необходимо сделать при обнаружении загрузочного вируса?

1. Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.
2. Компьютер необходимо отключить от сети и проинформировать системного администратора.
3. Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен.

61. Что необходимо сделать при обнаружении макровируса?

1. Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен.
2. Компьютер необходимо отключить от сети и проинформировать системного администратора.
3. Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.

62. В чем заключается метод защиты информации - ограничение доступа?

1. В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.
2. В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.
3. В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
4. В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.
5. В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

63. В чем заключается метод защиты информации - разграничение доступа?

1. В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

2. В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.
3. В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
4. В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.
5. В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

64. В чем заключается метод защиты информации - разделение доступа (привилегий)?

1. В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
2. В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.
3. В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.
4. В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.
5. В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

65. В чем заключается криптографическое преобразование информации?

1. В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.
2. В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.
3. В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.
4. В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
5. В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

66. В чем заключаются законодательные меры при защите информации?

1. В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.
2. В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.
3. В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.
4. В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
5. В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.

Тест №2 по темам «Хэш-функции», «Электронно-цифровая подпись», «Асимметричные алгоритмы шифрования», «Стеганография и стеганоанализ»

1. Собственником информации не может быть:
   1. государство;
   2. юридическое лицо;
   3. группа физических лиц;
   4. физическое лицо;
   5. ответы а – г правильны;
   6. нет правильного ответа.
2. Терминология в сфере защиты информации регулируется
   1. ГОСТ Р 6.30 – 2003
   2. ГОСТ 51141 – 98
   3. ГОСТ 50922 – 96
   4. Гражданским кодексом.
3. Заранее намеченный результат защиты информации – это
   1. замысел защиты информации;
   2. цель защиты информации;
   3. уровень эффективности защиты информации.
4. Содержание и порядок действий, направленных на обеспечение защиты информации – это
   1. мероприятие по защите информации;
   2. система защиты информации
   3. организация защиты информации.
5. Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и (или) собственником информации – это
   1. носитель информации
   2. собственник информации
   3. владелец информации
   4. пользователь информации
6. В настоящее время по степени конфиденциальности можно классифицировать информацию,
   1. составляющую коммерческую тайну;
   2. составляющую государственную тайну;
   3. составляющую служебную тайну;
   4. составляющую профессиональную тайну.
7. В каких областях деятельности может быть государственная тайна
   1. военной
   2. образовательной
   3. экономической
   4. контрразведывательной
   5. внешнеполитической
   6. внутриполитической
   7. разведывательной
   8. оперативно-розыскной
   9. экологической
   10. правильны все ответы.
8. Классифицированный список типовой и конкретной ценной информации о выполняемых работах, производимой продукции, научных и деловых идеях, технологических новшествах – это
   1. перечень ценных и конфиденциальных документов организации
   2. перечень конфиденциальных сведений организации
   3. перечень типовых документов, образующихся в деятельности организации.
9. Организацией конфиденциального делопроизводства непосредственно занимаются:
   1. все сотрудники организации в меру своих сил и обязанностей

2. служба безопасности
3. сектор конфиденциального делопроизводства в составе службы безопасности
4. первый руководитель организации
5. постоянно действующая экспертная комиссия
6. комиссии по проверке наличия, состояния и учета документов

10. Кто имеет право давать разрешение на ознакомление со всеми видами конфиденциальных документов организации всем категориям сотрудников и другим лицам?

1. руководитель службы безопасности
2. первый руководитель организации
3. руководитель сектора конфиденциального делопроизводства в составе службы безопасности
4. правильны все варианты

11. Для работы сотруднику подразделения понадобились конфиденциальные сведения и документы другого подразделения. Кто должен дать разрешение на ознакомление со сведениями и документами?

1. непосредственный начальник этого сотрудника
2. заместитель руководителя организации, курирующий данное направление
3. начальник подразделения, содержащего необходимые конфиденциальные сведения и документы
4. только первый руководитель организации.

12. Конфиденциальные документы уничтожаются, если

1. они являются исполненными
2. истек срок их конфиденциальности
3. истек срок их хранения

13. Отправка нешифрованного конфиденциального документа по факсу

1. не допускается
2. допускается
3. допускается, если на документе стоит гриф конфиденциальности

14. При проверках наличия конфиденциальных документов:

1. проверяют только документы, не трогая дела и иные носители конфиденциальной информации, т.к. в противном случае проверки будут очень громоздкими и долговременными
2. проверяют документы и дела, не трогая иные носители конфиденциальной информации, т.к. все, что связано с компьютерными технологиями, будет проверено специалистами по компьютерной безопасности
3. проверяют документы и дела, а также иные носители конфиденциальной информации

15. Основная масса угроз информационной безопасности приходится на:

1. Троянские программы
2. Шпионские программы
3. Черви

16. Какой вид идентификации и аутентификации получил наибольшее распространение:

1. системы PKI
2. постоянные пароли
3. одноразовые пароли

17. Под какие системы распространение вирусов происходит наиболее динамично:

1. Windows
2. Mac OS
3. Android

18. Заключительным этапом построения системы защиты является:

1. сопровождение
2. планирование
3. анализ уязвимых мест

19. Какие угрозы безопасности информации являются преднамеренными:

1. ошибки персонала
2. открытие электронного письма, содержащего вирус
3. не авторизованный доступ

20. Какой подход к обеспечению безопасности имеет место:

1. теоретический
2. комплексный
3. логический

21. Системой криптографической защиты информации является:

1. BFox Pro
2. CAudit Pro
3. Крипто Про

22. Какие вирусы активизируются в самом начале работы с операционной системой:

1. загрузочные вирусы
2. троянцы
3. черви

23. Stuxnet – это:

1. троянская программа
2. макровирус
3. промышленный вирус

24. Таргетированная атака – это:

1. атака на сетевое оборудование
2. атака на компьютерную систему крупного предприятия
3. атака на конкретный компьютер пользователя

25. Под информационной безопасностью понимается:

1. защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре
2. программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
3. нет верного ответа

26. Защита информации:

1. небольшая программа для выполнения определенной задачи
2. комплекс мероприятий, направленных на обеспечение информационной безопасности
3. процесс разработки структуры базы данных в соответствии с требованиями пользователей

27. Информационная безопасность зависит от:

1. компьютеров, поддерживающей инфраструктуры
2. пользователей
3. информации

28. Конфиденциальностью называется:

1. защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
2. описание процедур
3. защита от несанкционированного доступа к информации

29. Для чего создаются информационные системы:

1. получения определенных информационных услуг
2. обработки информации
3. оба варианта верны

30. Кто является основным ответственным за определение уровня классификации информации:

1. руководитель среднего звена
2. владелец
3. высшее руководство

31. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:

1. хакеры
2. контрагенты
3. сотрудники

32. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:

1. снизить уровень классификации этой информации
2. улучшить контроль за безопасностью этой информации
3. требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

33. Что самое главное должно продумать руководство при классификации данных:

1. управление доступом, которое должно защищать данные
2. оценить уровень риска и отменить контрмеры
3. необходимый уровень доступности, целостности и конфиденциальности

34. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:

1. владельцы данных
2. руководство
3. администраторы

35. Процедурой называется:

1. пошаговая инструкция по выполнению задачи
2. обязательные действия
3. руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

36. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании:

1. проведение тренингов по безопасности для всех сотрудников
2. поддержка высшего руководства
3. эффективные защитные меры и методы их внедрения

37. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков:

1. когда риски не могут быть приняты во внимание по политическим соображениям
2. для обеспечения хорошей безопасности нужно учитывать и снижать все риски
3. когда стоимость контрмер превышает ценность актива и потенциальные потери

38. Что такое политика безопасности:

1. детализированные документы по обработке инцидентов безопасности
2. широкие, высокоуровневые заявления руководства
3. общие руководящие требования по достижению определенного уровня безопасности

39. Какая из приведенных техник является самой важной при выборе конкретных защитных мер:

1. анализ рисков
2. результаты ALE
3. анализ затрат / выгоды

40. Что лучше всего описывает цель расчета ALE:

1. количественно оценить уровень безопасности среды
2. оценить потенциальные потери от угрозы в год
3. количественно оценить уровень безопасности среды

41. Тактическое планирование:

1. среднесрочное планирование
2. ежедневное планирование
3. долгосрочное планирование

42. Эффективная программа безопасности требует сбалансированного применения:

1. контрмер и защитных механизмов
2. процедур безопасности и шифрования
3. технических и нетехнических методов

43. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

1. уровень доверия, обеспечиваемый механизмом безопасности
2. внедрение управления механизмами безопасности
3. классификацию данных после внедрения механизмов безопасности

44. Что из перечисленного не является целью проведения анализа рисков:

1. выявление рисков
2. делегирование полномочий
3. количественная оценка воздействия потенциальных угроз

45. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:

1. меры обеспечения целостности;
2. административные меры;
3. меры обеспечения конфиденциальности.

46. Дублирование сообщений является угрозой:

1. доступности;
2. конфиденциальности;
3. целостности.

47. Вредоносное ПО Melissa подвергает атаке на доступность:

1. системы электронной коммерции;
2. геоинформационные системы;
3. системы электронной почты.

48. Выберите вредоносную программу, которая открыла новый этап в развитии данной области.

1. Melissa.
2. Bubble Boy.
3. ILO VE YOU.

49. Самыми опасными источниками внутренних угроз являются:

1. некомпетентные руководители;
2. обиженные сотрудники;
3. любопытные администраторы.

50. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности.

1. просчеты при администрировании информационных систем;
2. необходимость постоянной модификации информационных систем;
3. сложность современных информационных систем.

51. Агрессивное потребление ресурсов является угрозой:

1. доступности
2. конфиденциальности
3. целостности

52. Программа Melissa — это:

1. бомба;

2. вирус;
3. червь.

53. Для внедрения бомб чаще всего используются ошибки типа:

1. отсутствие проверок кодов возврата;
2. переполнение буфера;
3. нарушение целостности транзакций.

54. Окно опасности появляется, когда:

1. становится известно о средствах использования уязвимости;
2. появляется возможность использовать уязвимость;
3. устанавливается новое ПО.

Тест №3 по темам «Уязвимости программного обеспечения», «Компьютерные вирусы и методы их обнаружения», «Разделение прав в операционных системах», «Методы авторизации и аутентификации пользователей», «Безопасность сетей ЭВМ»

1. Под информационной безопасностью понимается…

    1. защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
    2. программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
    3. нет правильного ответа
2. Защита информации – это..

    1. комплекс мероприятий, направленных на обеспечение информационной безопасности.
    2. процесс разработки структуры базы данных в соответствии с требованиями пользователей
    3. небольшая программа для выполнения определенной задачи
3. От чего зависит информационная безопасность?

    1. от компьютеров
    2. от поддерживающей инфраструктуры
    3. от информации
4. Основные составляющие информационной безопасности:

    1. целостность
    2. достоверность
    3. конфиденциальность
5. Доступность – это…

    1. возможность за приемлемое время получить требуемую информационную услугу.
    2. логическая независимость
    3. нет правильного ответа
6. Целостность – это..

    1. целостность информации
    2. непротиворечивость информации
    3. защищенность от разрушения
7. Конфиденциальность – это..

    1. защита от несанкционированного доступа к информации
    2. программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
    3. описание процедур
8. Для чего создаются информационные системы?

    1. получения определенных информационных услуг
    2. обработки информации
    3. все ответы правильные
9. Целостность можно подразделить:

    1. статическую
    2. динамичную
    3. структурную
10. Где применяются средства контроля динамической целостности?

    1. анализе потока финансовых сообщений
    2. обработке данных
    3. при выявлении кражи, дублирования отдельных сообщений

11. Какие трудности возникают в информационных системах при конфиденциальности?

    1. сведения о технических каналах утечки информации являются закрытыми
    2. на пути пользовательской криптографии стоят многочисленные технические проблемы
    3. все ответы правильные
12. Угроза – это…

    1. потенциальная возможность определенным образом нарушить информационную безопасность
    2. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
    3. процесс определения отвечает на текущее состояние разработки требованиям данного этапа
13. Атака – это…

    1. попытка реализации угрозы
    2. потенциальная возможность определенным образом нарушить информационную безопасность
    3. программы, предназначенные для поиска необходимых программ.
14 .Источник угрозы – это..

    1. потенциальный злоумышленник
    2. злоумышленник
    3. нет правильного ответа
15. Окно опасности – это…

    1. промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.
    2. комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
    3. формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере
16. Какие события должны произойти за время существования окна опасности?

    1. должно стать известно о средствах использования пробелов в защите.
    2. должны быть выпущены соответствующие заплаты.
    3. заплаты должны быть установлены в защищаемой информационной системе
17. Угрозы можно классифицировать по нескольким критериям:

    1. по спектру информационной безопасности
    2. по способу осуществления
    3. по компонентам информационных систем
18. По каким компонентам классифицируется угрозы доступности:

    1. отказ пользователей
    2. отказ поддерживающей инфраструктуры
    3. ошибка в программе
19. Основными источниками внутренних отказов являются:

    1. отступление от установленных правил эксплуатации
    2. разрушение данных
    3. все ответы правильные
20. Основными источниками внутренних отказов являются:

    1. ошибки при конфигурировании системы
    2. отказы программного или аппаратного обеспечения
    3. выход системы из штатного режима эксплуатации
21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

    1. невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
    2. обрабатывать большой объем программной информации

3. нет правильного ответа

22. Какие существуют грани вредоносного ПО?

1. вредоносная функция
2. внешнее представление
3. способ распространения

23. По механизму распространения ПО различают:

1. вирусы
2. черви
3. все ответы правильные

24. Вирус – это…

1. код обладающий способностью к распространению путем внедрения в другие программы
2. способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
3. небольшая программа для выполнения определенной задачи

25. Черви – это…

1. код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по информационным системам и их выполнения
2. код обладающий способностью к распространению путем внедрения в другие программы
3. программа действий над объектом или его свойствами

26. Конфиденциальную информацию можно разделить:

1. предметную
2. служебную
3. глобальную

27. Природа происхождения угроз:

1. случайные
2. преднамеренные
3. природные

28. Предпосылки появления угроз:

1. объективные
2. субъективные
3. преднамеренные

29. К какому виду угроз относится присвоение чужого права?

1. нарушение права собственности
2. нарушение содержания
3. внешняя среда

30. Отказ, ошибки, сбой – это:

1. случайные угрозы
2. преднамеренные угрозы
3. природные угрозы

31. Отказ - это…

1. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
2. некоторая последовательность действий, необходимых для выполнения конкретного задания
3. структура, определяющая последовательность выполнения и взаимосвязи процессов

32. Ошибка – это…

1. неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния

2. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
3. негативное воздействие на программу

33. Сбой – это…

1. такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
2. неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
3. объект-метод

34. Побочное влияние – это…

1. негативное воздействие на систему в целом или отдельные элементы
2. нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
3. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

35. СЗИ (система защиты информации) делится:

1. ресурсы автоматизированных систем
2. организационно-правовое обеспечение
3. человеческий компонент

36. Что относится к человеческому компоненту СЗИ?

1. системные порты
2. администрация
3. программное обеспечение

37. Что относится к ресурсам автоматических средств СЗИ?

1. лингвистическое обеспечение
2. техническое обеспечение
3. все ответы правильные

38. По уровню обеспеченной защиты все системы делят:

1. сильной защиты
2. особой защиты
3. слабой защиты

39. По активности реагирования СЗИ системы делят:

1. пассивные
2. активные
3. полупассивные

40. Правовое обеспечение безопасности информации – это…

1. совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
2. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
3. нет правильного ответа

41. Правовое обеспечение безопасности информации делится:

1. международно-правовые нормы
2. национально-правовые нормы
3. все ответы правильные

42. Информацию с ограниченным доступом делят:

1. государственную тайну
2. конфиденциальную информацию
3. достоверную информацию

43. Что относится к государственной тайне?

1. сведения, защищаемые государством в области военной, экономической … деятельности
2. документированная информация
3. нет правильного ответа

44. Вредоносная программа - это…

1. программа, специально разработанная для нарушения нормального функционирования систем
2. упорядочение абстракций, расположение их по уровням
3. процесс разделения элементов абстракции, которые образуют ее структуру и поведение

45. Основополагающие документы для обеспечения безопасности внутри организации:

1. трудовой договор сотрудников
2. должностные обязанности руководителей
3. коллективный договор

46. К организационно - административному обеспечению информации относится:

1. взаимоотношения исполнителей
2. подбор персонала
3. регламентация производственной деятельности

47. Что относится к организационным мероприятиям:

1. хранение документов
2. проведение тестирования средств защиты информации
3. пропускной режим

48. Какие средства используется на инженерных и технических мероприятиях в защите информации:

1. аппаратные
2. криптографические
3. физические

49. Программные средства – это…

1. специальные программы и системы защиты информации в информационных системах различного назначения
2. структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
3. модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

50. Криптографические средства – это…

1. средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования
2. специальные программы и системы защиты информации в информационных системах различного назначения
3. механизм, позволяющий получить новый класс на основе существующего

51 .Среди ниже перечисленных отметьте две троянские программы:

1. I LOVE YOU;
2. Back Orifice;
3. Netbus.

52. Уголовный кодекс РФ не предусматривает наказания за:

1. создание, использование и распространение вредоносных программ;
2. ведение личной корреспонденции на производственной технической базе;
3. нарушение правил эксплуатации информационных систем.

53. Под определение средств защиты информации, данное в Законе «О государственной тайне», подпадают:

1. средства выявления злоумышленной активности;
2. средства обеспечения отказоустойчивости;
3. средства контроля эффективности защиты информации.

54. Уровень безопасности B согласно «Оранжевой книге» характеризуется:

1. произвольным управлением доступом;
2. принудительным управлением доступом;
3. верифицируемой безопасностью.

55. В число классов требований доверия безопасности «Общих критериев» входят:

1. разработка;
2. оценка профиля защиты;
3. сертификация.

56. Согласно «Оранжевой книге» политика безопасности включает в себя следующие элементы:

1. периметр безопасности;
2. метки безопасности;
3. сертификаты безопасности.

57. Согласно рекомендациям X.800 выделяются следующие сервисы безопасности:

1. управление квотами;
2. управление доступом;
3. экранирование.

58. Уровень безопасности A согласно «Оранжевой книге» характеризуется:

1. произвольным управлением доступом;
2. принудительным управлением доступом;
3. верифицируемой безопасностью.

59. Согласно рекомендациям X.800 аутентификация может быть реализована на:

1. сетевом уровне;
2. транспортном уровне;
3. прикладном уровне.

60. В число целей политики безопасности верхнего уровня входят:

1. решение сформировать или пересмотреть комплексную программу безопасности;
2. обеспечение базы для соблюдения законов и правил;
3. обеспечение конфиденциальности почтовых сообщений.

Приложение 5

к рабочей программе

Федеральное государственное бюджетное образовательное учреждение высшего образования

УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНЫ

на заседании кафедры Шахматного искусства и компьютерной математики

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ

ПРОМЕЖУТОЧНОГО КОНТРОЛЯ

по дисциплине

Информационная безопасность

Зачетный билет №1

1. Понятие информационной безопасности. Основные составляющие. Важность проблемы.

2. Даны символы a, b, c, d с частотами $f_a = 0,5$; $f_b = 0,25$; $f_c = 0,125$; $f_d = 0,125$. Построить эффективный код методом Хаффмена.

Зачетный билет №2

1. Распространение объектно-ориентированного подхода на информационную безопасность.

2. Даны символы a и b с частотами 0,9 и 0,1, соответственно. Построить эффективный код методом Шеннона-Фано для блоков из двух символов (n = 2).

Зачетный билет №3

1. Понятие угрозы. Наиболее распространенные угрозы. Классификация угроз.

2. Вычислить вручную значение $a^b \pmod c$ для a = 9928, b = 413, c = 82224.

Зачетный билет №4

1. Основные нормативные руководящие документы , касающиеся государственной тайны, нормативно-справочные документы.

2. Разноблочное шифрование и расшифрование («в ручную») пословиц по алгоритму RSA. Использовать четырехразрядные простые p и q.

Зачетный билет №5

1. Законодательный уровень информационной безопасности. Обзор зарубежного законодательства в области ИБ. Назначение и задачи в сфере обеспечения информационной безопасности.

2. Для точек P, Q, R эллиптической кривой $E_{751}(-1,1)$ найти точку 2P + 3Q – R, если P = (58, 139), Q = (67, 667), R = (82, 481).

Зачетный билет №6

1. Международные стандарты информационного обмена. Стандарт ISO/IEC15408. Российские стандарты защищенности автоматизированных систем.

2. Для точки P эллиптической кривой $E_{751}(-1,1)$ и натурального числа n найти точку nP, если P = (62, 372), n =128.

Зачетный билет №7

1. Основные положения теории информационной безопасности. Модели безопасности и их применение.

2. Сгенерируйте ЭЦП для сообщения с известным значением хэш-свертки e, зная секретный ключ подписи d при данном значении выбираемого случайным образом числа k. Используйте кривую $E_{751}(-1,1)$ и генерирующую точку G = (416, 55) порядка n = 13 и параметры e=9, d=3, k=5.

Зачетный билет №8

1. Таксономия нарушений информационной безопасности вычислительной системы и причины ,обуславливающих их существование

2. Проверьте подлинность ЭЦП (r, s) для сообщения с известным значением хэш-свертки e, зная открытый ключ проверки подписи Q. Используйте кривую E_{751} (-1,1) и генерирующую точку G = (562, 89) порядка n = 13 и параметры e=4, Q = (596, 318), (r, s)= (11, 4).

Зачетный билет №9

1. Информационная безопасность в условиях функционирования в России глобальных сетей.

2. Даны символы a, b, c, d с частотами fa = 0,5; fb = 0,25; fc = 0,125; fd= 0,125. Построить эффективный код методом Шеннона-Фано.

Зачетный билет №10

1. Виды противников или "нарушителей". Понятия о видах вирусов Виды возможных нарушений информационной системы. Виды защиты.

2. Используя шифр Полибия, дешифровать криптограмму:

Т = ЕС ИМ АНУШ АЙАСТАНИ АРЕВААМ БАРН ЭМ

СИРУМ МЕР ЙИН САЗИ ВОГБАНВАГ ЛАЦАКУМАЦ

ЛАРН ЭМ СИРУМ

Зачетный билет №11

1. Файловые вирусы. Загрузочные вирусы. Вирусы и операционные системы.

2. Расшифровать сообщение

T=FBRTLWUGAJQINZTHHXTEPHBNXSW,

зашифрованное линейным шифрующим преобразованием триграмм 26-буквенного алфавита A-Z с числовыми эквивалентами 0-25. Известно, что последние три триграммы - это подпись отправителя JAMESBOND. Найти дешифрующую матрицу и прочитать сообщение.

Зачетный билет №12

1. Методы и средства борьбы с вирусами. Профилактика заражения вирусами компьютерных систем.

2. Вычислить хеш строки “сообщение нельзя подделать”. Алгоритм – SHA1.

Зачетный билет №13

1. Защита информации от случайных угроз. Дублирование информации.

2. Реализовать сдвиговый регистр на основе примитивного полинома (8, 4, 3, 2, 0). Нарисовать схему регистра.

Зачетный билет №14

1. Повышение надежности компьютерных систем. Обеспечение отказоустойчивости компьютерных систем. Блокировка ошибочных операций.

2. Провести криптоанализ сообщения. Использована однократная перестановка столбцов по 5 символов: ИЬЖЗНСД_ТДН_ЕТ_НУВЕУРЫГОЫ

Зачетный билет №15

1. Защита информации от традиционного шпионажа и диверсий. Система охраны объектов компьютерных систем.

2. Вычислить хеш массива y = {5 9 12 34 32 45 67 79 101}. Алгоритм – MD5.

Зачетный билет №16

1. Организация работы с конфиденциальными информационными ресурсами.

2. Реализовать регистр на основе полинома (8, 4, 3, 2, 0). Нарисовать схему регистра.

Зачетный билет №17

1. Противодействие подслушиванию и наблюдению в оптическом диапазоне. Средства борьбы с закладными подслушивающими устройствами.

2. Реализовать шифрование фразы «БЕЗОПАСНОСТЬ – ЭТО ПРОФЕССИЯ» шифром Виженера. Ключ – «СЕЙФ».

Зачетный билет №18

1. Защита от злоумышленных действий обслуживающего персонала и пользователей.

2. Провести криптоанализ сообщения. Использована однократная перестановка столбцов по 5 символов: ЯАМРИТ_ДЖЕХ_СВЕД_ТСУВЕТНО

Зачетный билет №19

1. Средства защиты компьютеров. Программно аппаратные методы и средства ограничения доступа к компонентам компьютера. Типы несанкционированного доступа и условия работы средств защиты.

2. Реализовать сдвиговый регистр на основе примитивного полинома (9, 4, 0). Нарисовать схему регистра.

Зачетный билет №20

1. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем.

2. Реализовать шифрование фразы «МЫ ИЗУЧАЕМ ШИФР» шифром Кардано.

Зачетный билет №21

1. Защита от несанкционированного копирования программного обеспечения.

2. Реализовать простую ЭЦП без контроля целостности с использованием алгоритма RSA.

Зачетный билет №22

1. Методы криптографии. Основные понятия шифрования.

2. Найти наибольший общий делитель НОД(1547, 560) двух чисел методом Евклида.

Зачетный билет №23

1. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом. Стандарты шифрования.

2. Найти результат преобразования $5^{17} \bmod 7$ методом, основанным на теореме Эйлера.

Зачетный билет №24

1. Промышленные программные средства Kerberos, PGP.

2. Найти обратное значение числа по модулю $x = 9^{-1} \pmod 5$. при помощи определения кратности k («по определению»).

Зачетный билет №25

1. Методы и средства хранения ключевой информации. Анализ программных реализаций.

2. Найти обратное значение числа по модулю $7^{-1} \pmod{11}$ с использованием функции Эйлера.

Зачетный билет №26

1. Защита от разрушающих программных воздействий. Основные технологии построения защищенных ЭИС.

2. Найти результат преобразования $a^8 \pmod m$ методом цепочек.

Зачетный билет №27

1. Системные вопросы защиты программ и данных. Основные категории требований к средствам обеспечения информационной безопасности

2. Найти методом цепочек $a^n \pmod m = 15^{63} \pmod 7$.