Автономная образовательная некоммерческая организация
высшего образования
«Институт Бизнеса и Информационных Систем»
(АОНО ВО «ИБИС»)

Факультет Бизнеса и информационных систем
Кафедра Информационных технологий

УТВЕРЖДАЮ
Проректор по учебно-воспитательной работе
_____М.В. Доможирова
«12» 05 2023 г.

РАБОЧАЯ ПРОГРАММА И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

дисциплины

Б1.В.ДВ.03.02 «Средства и методы защиты информации»

Уровень образования:	Высшее образование – бакалавриат
Направление подготовки:	09.03.02 Информационные системы и технологии
Направленность (профиль):	Информационные системы и сетевые технологии
Форма обучения:	Очная, заочная
Составитель:	д.т.н. Мельников А.В.

Воронеж 2023 г.

Разработчик рабочей программы дисциплины: д.т.н. Мельников Александр Владимирович

Рабочая программа дисциплины рассмотрена и утверждена на заседаниях:

кафедры «Информационных технологий», протокол №2 от «24» апреля 2023 года.

Ученого совета АОНО «Институт Бизнеса и Информационных Систем», протокол № 3 от «11» мая 2023 года.

1. Цели и задачи учебной дисциплины

Цель освоения дисциплины «Средства и методы защиты информации»: является изучение организационных, технических, алгоритмических и других методов и средств защиты компьютерной информации, законодательства и стандартов в этой области, современных криптосистем, методов борьбы с вирусами.

Задачи дисциплины:

– изучить методологические основы исследования проблем защиты информации;

– изучить основные методы и системы защиты информации различных направлений обеспечения информационной безопасности;

– подготовить обучающихся к применению полученных знаний для анализа моделей

– объектов и формирования моделей и методов управления и обеспечения защиты информации

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Средства и методы защиты информации» относится к вариативной части дисциплин по выбору Блока 1 и ориентирована на обучающихся, имеющих начальную подготовку в рамках дисциплин: «Информатика», «Сети и телекоммуникации», «Инструментальные средства информационных систем», «Моделирование процессов и систем».

Дисциплина может быть использована при изучении дисциплин: «Администрирование сетевого оборудования», «Автоматизация проектирования информационных систем», в рамках практик, подготовки выпускной квалификационной работы

3. Перечень планируемых результатов обучения по дисциплине, соотнесенные с установленными в ОП ВО индикаторами достижения компетенций

Задача профессиональной деятельности	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
Применение современных информационно-коммуникационных технологий процессе осуществления профессиональных функций	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1 Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знает: - основные принципы построения кодов, криптосистем и крипто протоколов; - основные методы анализа криптостойкости информационных систем; - основные алгоритмы шифрования; - основные протоколы защищенной передачи данных
		ОПК-3.2 Уметь: решать стандартные задачи профессиональной деятельности на основе информацион-	Умеет - конструировать криптостойкие алгоритмы и протоколы; - проводить анализ

		ной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	криптостойкости алгоритмы и протоколов; - создавать программы, реализующие алгоритмы и протоколы защищенной передачи данных;
		ОПК-3.3 Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Владеет: - приемами чтения, построения и записи алгоритмов; - навыками шифрования и дешифрования данных.
Исследование моделей и методов информационных систем и технологий на базе современных программных пакетов моделирования, проектирования и автоматизации.	ПК-5 Способен к организации и проведению экспериментальных исследований и компьютерного моделирования с применением современных средств и методов	ПК-5.1 Знать: основные научные методики, применяемые при разработке, внедрении и сопровождении информационных технологий и систем.	Знает: - основные методы и модели обеспечения и управления информационной безопасностью; - методологические основы исследования проблем информационной безопасности объектов
		ПК-5.2 Уметь: применять выбранные научно-исследовательские методики.	Умеет: - применять научно-методологический базис для моделирования и исследования объектов защиты; - применять методы и системы защиты информации для обеспечения информационной безопасности объектов
		ПК-5.3. Имеет навыки анализа и критической оценки полученных результатов.	Владеет: - методологией построения моделей и методов информационной безопасности объектов; - навыками анализа и синтеза методов и моделей измерения и

			оценивания информационной безопасности в зависимости от целей и особенностей объекта защиты

4. Объем и структура дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 час.

Вид учебной работы	Формы обучения					
	Очная			Заочная		
	Всего часов	из них в семестре		Всего часов	из них в семестре	
		6			8	
Общая трудоемкость дисциплины	108	108		108	108	
Контактная работа обучающихся с преподавателем, всего	54	54		10	10	
в том числе:						
Лекции	18	18		4	4	
Лабораторные работы						
Практические занятия	36	36		6	6	
Самостоятельная работа	54	54		94	94	
Промежуточная аттестация (подготовка и сдача)	-	-		4	4	
Курсовая работа/проект	-	-		-	-	
Контрольная работа	-	-		-	-	
Промежуточная аттестация: экзамен/зачет/зачет с оценкой	Зачет	Зачет		Зачет	Зачет	

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Содержание тем дисциплины, структурированное по темам с указанием дидактического материала по каждой изучаемой теме

№ п/п	Наименование темы	Содержание темы
1	Тема 1. Законодательные и правовые основы защиты компьютерной информации и информационных технологий	Информация как объект юридической и физической защиты. Государственные информационные ресурсы. Защита государственной тайны как особого вида защищаемой информации. Защита конфиденциальной информации, в том числе интеллектуальной собственности и коммерческой тайны. Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления и особенности их расследования.

2	Тема 2. Парольные системы	Построение парольных систем; особенности применения криптографических методов; Способы реализации криптографической подсистемы; особенности реализации систем с симметричными и несимметричными ключами; Концепция защищенного ядра; методы верификации;
3	Тема 3. Защита систем	Защищенные домены; Применение иерархического метода для построения защищенной операционной системы; Исследование корректности систем защиты; методология обследования и проектирования защиты; Модель политики контроля целостности.
4	Тема 4. Криптосистемы	Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Дисковые шифраторы. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома.
5	Тема 5. Симметричные системы шифрования	Поточные шифры, блочные шифры. Аддитивные поточные шифры. Методы генерации криптографически качественных псевдослучайных последовательностей.
6	Тема 6. Стандарты шифрования	Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования.
7	Тема 7. Асимметричные системы шифрования	Основные требования к алгоритмам асимметричного шифрования. Криптоанализ алгоритмов с открытым ключом. Схема Эль-Гамаля. 3. Разложения числа на простые сомножители. 4. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.А. Алгоритм Диффи-Хеллмана
8	Тема 8. Идентификация и аутентификация	Основные понятия и концепции. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователя. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль-Гамаля

		(EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.
9	Тема 9. Программно-аппаратные средства защиты ПЭВМ и сетей.	Методы средства ограничения доступа к компонентам сети; Методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям: Методы и средства хранения ключевой информации; Защита программ от изучения; защита от разрушающих программных воздействий; защита от изменений и контроль целостности.

Тематический план (очная форма обучения)

№ п/п	Наименование тем	Всего часов по учебному плану	Контактная работа с преподавателем:					Самостоятельная работа
			Всего часов	Лекции	Занятия семинарского типа			
					Семинарские занятия	Практические занятия	Другие виды занятий	
6 семестр								
1	Тема 1. Законодательные и правовые основы защиты компьютерной информации и информационных технологий	12	6	2		4		6
2	Тема 2. Парольные системы	12	6	2		4		6
3	Тема 3. Защита систем	12	6	2		4		6
4	Тема 4. Криптосистемы	12	6	2		4		6
5	Тема 5. Симметричные системы шифрования	12	6	2		4		6
6	Тема 6. Стандарты шифрования	12	6	2		4		6
7	Тема 7. Асимметричные системы шифрования	12	6	2		4		6
8	Тема 8. Идентификация и аутентификация	12	6	2		4		6
9	Тема 9. Программно-аппаратные средства защиты ПЭВМ и сетей.	12	6	2		4		6
Форма контроля: Зачет								
Итого за семестр		108	54	18		36		54

Тематический план (заочная форма обучения)

№ п/п	Наименование тем	Всего часов по учебному плану	Контактная работа с преподавателем:					Самостоятельная работа
			Всего часов	Лекции	Занятия семинарского типа			
					Семинарские занятия	Практические занятия	Другие виды занятий	
8 семестр								
1	Тема 1. Законодательные и правовые основы защиты компьютерной информации и информационных технологий	12	2	2				10
2	Тема 2. Парольные системы	12	2			2		10
3	Тема 3. Защита систем	10						10
4	Тема 4. Криптосистемы	12	2			2		10
5	Тема 5. Симметричные системы шифрования	12	2	2				10
6	Тема 6. Стандарты шифрования	10						10
7	Тема 7. Асимметричные системы шифрования	12	2			2		10
8	Тема 8. Идентификация и аутентификация	12						12
9	Тема 9. Программно-аппаратные средства защиты ПЭВМ и сетей.	12						12
Форма контроля: Зачет		4						4
Итого за семестр		**108**	**10**	**4**		**6**		**98**

6. Самостоятельная работа обучающихся в ходе освоения дисциплины

№ п/п	Вид самостоятельной работы	Наименование работы и содержание
1	Освоение учебного материала по конспекту лекций и дополнительной литературе	Доработать конспект, желательно в тот же день. Прочитать записи, восстановить текст в памяти, а также исправить описки, расшифровать не принятые ранее сокращения, заполнить пропущенные места, понять текст, вникнуть в его смысл. Изучить материал, используя рекомендуемую литературу, разрешая в ходе чтения, возникшие ранее затруднения, находя ответы на вопросы, а также дополняя и исправляя свои записи. Записи должны быть наглядными, для чего следует применять различные способы выделений. Подготовленный конспект и рекомендуемая литература используются при подготовке к практическому занятию.
2	Подготовка к практическим занятиям	Подготовка к практическому занятию включает следующие элементы самостоятельной деятельности: четкое представление цели и задач его проведения; выделение

		навыков умственной, аналитической деятельности, которые станут результатом предстоящей работы. Выработка навыков осуществляется с помощью получения новой информации об изучаемых процессах и с помощью знания о том, в какой степени в данное время студент владеет методами исследовательской деятельности, которыми он станет пользоваться на практическом занятии.
3	Изучение основной и дополнительной литературы	Самостоятельная работа с учебниками и книгами (а также самостоятельное теоретическое исследование проблем, обозначенных преподавателем на лекциях) – это важнейшее условие познания. В самостоятельной работе рекомендуется прибегать к таким видам систематизированной записи прочитанного как аннотирование, тезирование, цитирование, конспектирование. Причем конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.
4	Подготовка к зачету	Необходимо перечитать лекции, вспомнить то, что говорилось преподавателем на семинарах и практических занятиях, а также самостоятельно полученную ин формацию при подготовке к ним. важно сформировать целостное представление о содержании ответа на каждый вопрос, что предполагает знание разных научных трактовок сущности того или иного явления, процесса, умение раскрывать факторы, определяющие их противоречивость, знание имен ученых, изучавших обсуждаемую проблему. необходимо также привести информацию о материалах эмпирических исследований, что указывает на всестороннюю подготовку студента к зачету. ответ, в котором присутствуют все указанные блоки информации, наверняка будет отмечен высокими баллами. для их получения требуется ответить и на дополнительные вопросы, если зачет проходит в устной форме. Рекомендуется подготовку к зачету осуществлять в два этапа. На первом, в течение 2–3 дней, подбирается из разных источников весь материал, необходимый для развернутых ответов на все вопросы. ответы можно записать в виде краткого конспекта. На втором этапе по памяти восстанавливается содержание того, что записано в ответах на каждый вопрос.

7. Фонд оценочных средств для текущей и промежуточной аттестации по дисциплине

Оценочные средства для проведения текущей и промежуточной аттестации

Код контролируемого индикатора освоения компетенции	Наименование оценочного средства для проведения текущей аттестации	Наименование оценочного средства для проведения промежуточной аттестации
ОПК-3.1, ОПК-3.2,	контрольные вопросы, те-	Зачет

ОПК-3.3 ПК-5.1, ПК-5.2, ПК-5.3	стовые задания, практические работы	

Критерии оценивания результата обучения по дисциплине и шкала оценивания

Код контролируемой компетенции	Критерии оценивания результата обучения по дисциплине и шкала оценивания			
	неудовлетворительно	удовлетворительно	хорошо	отлично
	Не зачтено	Зачтено		
ОПК-3	Отсутствие или фрагментарные способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	Неполные способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	Сформированные, но содержащие отдельные пробелы способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	Сформированные систематические решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий
ПК-5	обучающийся обнаруживает незнание ответа на соответствующее задание, допускает принципиальные ошибки в формулировке определений и правил, в течение семестра не сформировал необходимых умений и навыков	обучающийся демонстрирует удовлетворительное, но не систематизированное владение способностями к организации и проведению экспериментальных исследований и компьютерного моделирования с применением современных средств и методов	обучающийся демонстрирует достаточно полное, с небольшими неточностями, владение способностями к организации и проведению экспериментальных исследований и компьютерного моделирования с применением современных средств и методов	обучающийся демонстрирует полное, систематизированное владение способностями к организации и проведению экспериментальных исследований и компьютерного моделирования с применением современных средств и методов

8. Ресурсное обеспечение учебной дисциплины

Основная литература:

1. Бондаренко, И. С. Методы и средства защиты информации : лабораторный практикум / И. С. Бондаренко, Ю. В. Демчишин. - Москва : Изд. Дом НИТУ «МИСиС», 2018. - 32 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232228 (дата обращения: 20.12.2021). – Режим доступа: по подписке.

Дополнительная литература:

2. Зайцев, А. П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; Под ред. А.П.Зайцева - 7 изд., исправ. - Москва : Гор. линия-Телеком, 2012. - 442с.; - (Уч. для вузов). ISBN 978-5-9912-0233-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/390284 (дата обращения: 20.12.2021). – Режим доступа: по подписке.

3. Костин, В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. - Москва : Изд. Дом НИТУ «МИСиС», 2018. - 31 с. - ISBN 978-5-906953-53-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232355 (дата обращения: 20.12.2021). – Режим доступа: по подписке.

4. Методы и средства комплексной защиты информации в технических системах : учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. - Саров : РФЯЦ-ВНИИЭФ, 2019. - 224 с. - ISBN 978-5-9515-0429-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1230827 (дата обращения: 20.12.2021). – Режим доступа: по подписке

5. Костин, В. Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / В. Н. Костин. - Москва : Изд. Дом НИТУ «МИСиС», 2018. - 21 с. - ISBN 978-5-906953-22-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232357 (дата обращения: 20.12.2021). – Режим доступа: по подписке.

6. Астайкин, А. И. Методы и средства обеспечения программно-аппаратной защиты информации: Научно-техническое издание / Астайкин А.И., Мартынов А.П., Николаев Д.Б. - Саров:ФГУП"РФЯЦ-ВНИИЭФ", 2015. - 214 с.: ISBN 978-5-9515-0305-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/950073 (дата обращения: 20.12.2021). – Режим доступа: по подписке.

Электронные ресурсы:

1. Федеральная служба государственной статистики [Электронный ресурс]. – Режим доступа: http://www.gks.ru/, свободный (дата обращения 30.09.2021Интернет Университет Информационных технологий. [Электронный ресурс] : сайт. – Режим доступа: http://www.intuit.ru/, свободный (дата обращения 30.09.2021

2. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека. – Режим доступа: http://elibrary.ru/defaultx.asp, свободный (дата обращения: 30.09.2021).

3. Информационные системы и технологии : [сайт]. – URL: https://studfiles.net/preview/4171546/page:4/ (дата обращения: 25.09.2021). – Режим доступа : свободный. – Текст : электронный.

4. Портал Федеральных государственных образовательных стандартов высшего образования: [сайт]. – URL: http://fgosvo.ru. (дата обращения: 25.09.2021). – Режим доступа : свободный. – Текст : электронный.

5. Федеральный центр информационно-образовательных ресурсов (ФЦИОР): [сайт]. – URL: http://edu.ru (дата обращения: 25.09.2021). – Режим доступа : свободный. – Текст : электронный.

6. Единая коллекция цифровых образовательных ресурсов (Единая коллекция ЦОР) : [сайт]. – URL: http://school-collection.edu.ru (дата обращения: 25.09.2021). – Режим доступа : свободный. – Текст : электронный.

7. Информационная система «Единое окно доступа к образовательным ресурсам» (ИС «Единое окно») : [сайт]. – URL: http://window/edu.ru (дата обращения: 25.09.2021). – Режим доступа : свободный. – Текст : электронный.

9. Материально-техническое обеспечение дисциплины

Учебная аудитория № 224 -учебная аудитория для проведения занятий лекционного типа; -учебная аудитория для проведения занятий семинарского тип и практических занятий; -учебная аудитория групповых и индивидуальных консультаций; -учебная аудитория для проведения текущего контроля и промежуточной аттестации. Оснащение оборудованием и техническими средствами обучения: - комплект учебной мебели для обучающихся; - рабочее место преподавателя; -доска меловая; -переносное видеопроекционное оборудование для мультимедиа презентации, средства звуковоспроизведения (персональный компьютер, проектор, экран, колонки). Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 7; - Microsoft Office Standard 2007. 2) отечественного производства: - Kaspersky EndPoint Security для Windows. Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	394026, Воронежская область, г. Воронеж, ул. Дружинников, д.8 Кабинет № 224 (2 этаж № 3)
Учебная аудитория № 313 -учебная аудитория для проведения занятий лекционного типа; -учебная аудитория для проведения занятий семинарского тип и практических занятий; -учебная аудитория групповых и индивидуальных консультаций; -учебная аудитория для проведения текущего контроля и промежуточной аттестации; -учебная аудитория для курсового проектирования (выполнения курсовых работ); -компьютерный класс; -помещение для самостоятельной работы обучающихся. Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; -автоматизированное рабочее место преподавателя; -доска мар-	394036, город Воронеж, ул. Карла Маркса, д.67 Кабинет № 313 (3 этаж № 62)

керная; - стационарное видеопроекционное оборудование для мультимедиа презентации, средства звуковоспроизведения (экран, проектор, колонки). Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 10; - Microsoft Office Standard 2007; - MS Visio; - MS Access 2016; - MS Project; - Microsoft SQL Server 2019; - Visual Studio 2010. 2) отечественного производства: - Kaspersky EndPoint Security для Windows. Свободно распространяемое программное обеспечение иностранного производства: - PascalABC.NET; - FreePascal IDE; - Eclipse; - IntelliJ IDEA; - GIMP; - Blender; - Firefox; - Vuze; - FileZilla; - Denver; - Maxima + WxMaxima, iTest; - Inkscape; - QCad. Российская информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	
Учебная аудитория № 318 -учебная аудитория для проведения занятий лекционного типа; -учебная аудитория для проведения занятий семинарского тип и практических занятий; -учебная аудитория групповых и индивидуальных консультаций; -учебная аудитория для проведения текущего контроля и промежуточной аттестации; -учебная аудитория для курсового проектирования (выполнения курсовых работ); -компьютерный класс; -помещение для самостоятельной работы обучающихся. Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; -автоматизированное рабочее место преподавателя; -доска двусторонняя (маркерно-меловая); - переносное видеопроекционное оборудование для мультимедиа	394026, Воронежская область, г. Воронеж, ул. Дружинников, д.8 Кабинет № 318 (3 этаж № 50)

презентации (ноутбук, проектор, экран, колонки). Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 7; - Microsoft Office Standard 2007; - MS Visio 2007; - MS Project 2010; - Microsoft SQL Server 2012; - Microsoft Visual Studio. 2) отечественного производства: - Kaspersky EndPoint Security для Windows; - Автоматизированная банковская система «Управление кредитной организацией» для ВУЗов. Свободно распространяемое программное обеспечение: 1) иностранного производства: - PascalABC.NET; - FreePascal IDE; - GIMP; - Blender; - Firefox; - Vuze; - FileZilla; - Denver; - Maxima + WxMaxima; - iTest; - Inkscape; - QCad; 2) отечественного производства: - программа Фоторобот. Российская информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	
Помещение для самостоятельной работы обучающихся № 102 - помещение для самостоятельной работы обучающихся с доступом к сети «Интернет» и электронной информационно-образовательной среде организации; - читальный зал библиотеки - учебная аудитория для курсового проектирования (выполнения курсовых работ); -учебная аудитория для выполнения и защиты выпускной квалификационной работы. Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; - ноутбуки; - телевизор; - столы для чтения; - стулья; - шкафы для документов; -стол офисный;	394026, Воронежская область, г. Воронеж, ул. Дружинников, д.8 Кабинет № 102 (1 этаж № 84)

- стеллажи для книг; -стойка выдачи литературы; -тумба напольная; -информационная стойка. Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 7 pro; - Microsoft Office Standard 2007; - MS Access 2016. 2) отечественного производства: - Kaspersky EndPoint Security для Windows; Свободно распространяемое программное обеспечение: - 7-Zip; - Интернет цензор. Российская информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации	
Учебная аудитория № 314 - помещение для самостоятельной работы обучающихся с доступом к сети «Интернет» и электронной информационно-образовательной среде организации; -учебная аудитория для курсового проектирования (выполнения курсовых работ); -учебная аудитория для выполнения выпускной квалификационной работы; - компьютерный класс. Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; - автоматизированное рабочее место преподавателя; -доска двусторонняя (маркерно - меловая); -наушники; -принтер; -телевизор. Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 8.1 Корпоративная; - Microsoft Office Standard 2007; - iSpring suite 8; - MS Visio; - MS Access 2016; - MS Project; - Microsoft SQL Server 2014; - Visual Studio 2017. 2) отечественного производства: - Kaspersky EndPoint Security для Windows; -1С: Предприятия 8. Комплект для обучения в высших и средних учебных заведениях. Свободно распространяемое программное обеспечение иностранного производства:	394026, Воронежская область, г. Воронеж, ул. Дружинников, д.8 Кабинет № 314 (3 этаж № 48)

- PascalABC.NET; - FreePascal IDE; - Eclipse; - IntelliJ IDEA; - GIMP; - Blender; - Firefox; - Vuze; - FileZilla; - Denver, Maxima + WxMaxima; - iTest; - Inkscape; - QCad. Информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	
Учебная аудитория № 318 - помещение для самостоятельной работы обучающихся с доступом к сети «Интернет» и электронной информационно-образовательной среде организации; -учебная аудитория для курсового проектирования (выполнения курсовых работ); -учебная аудитория для выполнения выпускной квалификационной работы; Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; - автоматизированное рабочее место преподавателя; -доска двусторонняя (маркерно-меловая); - переносное видеопроекционное оборудование для мультимедиа презентации (ноутбук, проектор, экран, колонки). Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 7; - Microsoft Office Standard 2007; - MS Visio 2007; - MS Project 2010; - Microsoft SQL Server 2012; - Microsoft Visual Studio. 2) отечественного производства: - Kaspersky EndPoint Security для Windows; -Автоматизированная банковская система «Управление кредитной организацией» для ВУЗов. Свободно распространяемое программное обеспечение: 1) иностранного производства: - PascalABC.NET; - FreePascal IDE; - GIMP; - Blender; - Firefox;	394026, Воронежская область, г. Воронеж, ул. Дружинников, д.8 Кабинет № 318 (3 этаж № 50)

- Vuze; - FileZilla; - Denver; - Maxima + WxMaxima; - iTest; - Inkscape; - QCad; 2) отечественного производства: - программа Фоторобот. Российская информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	
Учебная аудитория № 313 - помещение для самостоятельной работы обучающихся с доступом к сети «Интернет» и электронной информационно-образовательной среде организации; -учебная аудитория для курсового проектирования (выполнения курсовых работ); -учебная аудитория для выполнения выпускной квалификационной работы; - компьютерный класс. Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; -автоматизированное рабочее место преподавателя; -доска маркерная; - стационарное видеопроекционное оборудование для мультимедиа презентации, средства звуковоспроизведения (экран, проектор, колонки). Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 10; - Microsoft Office Standard 2007; - MS Visio; - MS Access 2016; - MS Project; - Microsoft SQL Server 2019; - Visual Studio 2010; 2) отечественного производства: - Kaspersky EndPoint Security для Windows. Свободно распространяемое программное обеспечение иностранного производства: - PascalABC.NET; - FreePascal IDE; - Eclipse; - IntelliJ IDEA; - GIMP; - Blender; - Firefox; - Vuze;	394036, город Воронеж, ул. Карла Маркса, д.67 Кабинет № 313 (3 этаж № 62)

- FileZilla; - Denver; - Maxima + WxMaxima, iTest; - Inkscape; - QCad. Российская информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	
Учебная аудитория № 314 - помещение для самостоятельной работы обучающихся с доступом к сети «Интернет» и электронной информационно-образовательной среде организации; -учебная аудитория для курсового проектирования (выполнения курсовых работ); -учебная аудитория для выполнения выпускной квалификационной работы; - компьютерный класс. Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; - автоматизированное рабочее место преподавателя; -доска двусторонняя (маркерно - меловая); -наушники; -принтер; -телевизор. Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 8.1 Корпоративная; - Microsoft Office Standard 2007; - iSpring suite 8; - MS Visio; - MS Access 2016; - MS Project; - Microsoft SQL Server 2014; - Visual Studio 2017. 2) отечественного производства: - Kaspersky EndPoint Security для Windows; -1С: Предприятия 8. Комплект для обучения в высших и средних учебных заведениях. Свободно распространяемое программное обеспечение иностранного производства: - PascalABC.NET; - FreePascal IDE; - Eclipse; - IntelliJ IDEA; - GIMP; - Blender; - Firefox; - Vuze; - FileZilla;	394036, город Воронеж, ул. Карла Маркса, д.67 Кабинет № 314 (3 этаж № 61)

- Denver, Maxima + WxMaxima; - iTest; - Inkscape; - QCad. Информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	

10. Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

10.1 Материалы для текущего контроля освоения дисциплины

Тема 1. Законодательные и правовые основы защиты компьютерной информации и информационных технологий

Контрольные вопросы:

1) Информация как объект юридической и физической защиты.
2) Государственные информационные ресурсы. Защита государственной тайны как особого вида защищаемой информации.
3) Защита конфиденциальной информации, в том числе интеллектуальной собственности и коммерческой тайны.
4) Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления и особенности их расследования.

Практическая работа № 1. Шифрование данных методами подстановки, перестановки и полиалфавитными шифрами

Цель работы: Приобретение навыков шифрования информации с использованием простейших методов шифрования.

Вопросы по практической работе:

1. Почему метод подстановки имеет слабую надежность?
2. Что такое частотный анализ?
3. Что является криптографическим ключом в методе перестановки?
4. Как связаны метод подстановки и многоалфавитные шифры?
5. В чем отличие криптографии от криптоанализа?
6. По какому признаку шифры делят на симметричные и асимметричные?

Тема 2. Парольные системы

Контрольные вопросы:

1) Построение парольных систем; особенности применения криптографических методов;
2) Способы реализации криптографической подсистемы; особенности реализации систем с симметричными и несимметричными ключами;
3) Концепция защищенного ядра; методы верификации.

Практическая работа №2. Шифр гаммирования

Цель работы: Освоение принципов шифрования гаммированием, изучение свойств

генератора псевдослучайных чисел, программная реализация метода гаммирования.

Вопросы по практической работе:

1. Какие параметры конгруэнтного генератора необходимо выбрать для получения максимальной длины последовательности псевдослучайных чисел?
2. От чего зависит длина псевдослучайной последовательности?
3. Каков принцип действия генераторов с обратной связью?
4. Какую операцию используют для шифрования в методе гаммирования?
5. Каковы достоинства и недостатки метода гаммирования?
6. Что является ключом в шифрах гаммирования?

Тема 3. Защита систем

Контрольные вопросы:

1) Защищенные домены;
2) Применение иерархического метода для построения защищенной операционной системы;
3) Исследование корректности систем защиты; методология обследования и проектирования защиты;
4) Модель политики контроля целостности.

Практическая работа № 3. Сеть Фейштеля

Цель работы: изучить принципы работы сети Фейштеля, научиться шифровать информацию посредством использования блочного криптоалгоритма.

Вопросы по практической работе:

1. Какова структура классической сети Фейштеля?
2. Что называется раундом в сети Фейштеля?
3. Какими свойствами обладает сеть Фейштеля?
4. Каким образом используется материал ключа при шифровании?
5. В чем отличие процессов шифрования и дешифрования?
6. Назовите достоинства и недостатки блочных шифров.

Тема 4. Криптосистемы

Контрольные вопросы:

1) Основные понятия и определения.
2) Подстановочные и перестановочные шифры.
3) Шифры Цезаря, Виженера, Вернома.
4) Дисковые шифраторы.
5) Исследования Шеннона в области криптографии.
6) Нераскрываемость шифра Вернома.

Практическая работа №4. Изучение алгоритма RSA

Цель работы: Освоить механизм шифрования и дешифрования данных в криптографической системе с открытыми ключами RSA.

Вопросы по практической работе:

1. Что такое однонаправленные функции?
2. Основные свойства однонаправленных функций с потайным ходом.
3. Какие числа называются взаимно простыми?
4. Как реализуется программное возведение в степень для больших чисел?
5. На чем основана криптостойкость алгоритма RSA?

6. Каковы достоинства и недостатки асимметричных алгоритмов?

Тема 5. Симметричные системы шифрования

Контрольные вопросы:

1) Поточные шифры, блочные шифры.
2) Аддитивные поточные шифры.
3) Методы генерации криптографически качественных псевдослучайных последовательностей.

Практическая работа № 5. Создание электронной подписи в документе

Цель работы: разработка процедур выработки и проверки электронной цифровой подписи (ЭЦП) сообщений на базе асимметричного криптографического алгоритма с применением функции хеширования.

Вопросы по практической работе:

1. Какие криптоалгоритмы используются для создания электронной цифровой подписи?
2. Что такое криптографическая хэш-функция, какими свойствами она должна обладать?
3. Как содержание сообщение влияет на электронную цифровую подпись?
4. Где используется ЭЦП?
5. В каком случае электронная цифровая подпись при проверке отвергается?
6. От каких угроз информации защищает ЭЦП?

Тема 6. Стандарты шифрования

Контрольные вопросы:

1) Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости.
2) Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования.

Практическая работа №6. Защита графического файла с помощью цифрового водяного знака

Цель работы: Изучение стеганографических методов защиты информации. Реализация программы с использованием стеганографических принципов защиты информации.

Вопросы по практической работе:

1. Что собой представляет стеганография?
2. Перечислите области применения стеганографических алгоритмов.
3. Каковы требования к цифровым водяным знакам?
4. В чем суть LSB-алгоритма?
5. От чего зависит стойкость стегосистем?
6. Каковы особенности встраивания и извлечения информации из стегоконтейнера?

Тема 7. Асимметричные системы шифрования

Контрольные вопросы:

1) Основные требования к алгоритмам асимметричного шифрования.
2) Криптоанализ алгоритмов с открытым ключом.
3) Схема Эль-Гамаля.
4) Разложения числа на простые сомножители.
5) Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.

6) Алгоритм Диффи-Хеллмана

Практическая работа № 7. Парольная защита

Цель работы: изучение принципов организации парольной защиты программ, ознакомление с видами паролей, реализация парольной защиты.

Вопросы по практической работе:

1. При соблюдении каких условий парольная защита является эффективной?
2. Каковы недостатки парольной защиты?
3. Что такое метод рукопожатия?
4. Какие операционные системы имеют встроенную парольную защиту?
5. Сравните методы простой парольной защиты и выборку символов.
6. Как реализуют пароли однократного использования.

Тема 8. Идентификация и аутентификация

Контрольные вопросы:

1) Основные понятия и концепции.
2) Идентификация и механизмы подтверждения подлинности пользователя.
3) Взаимная проверка подлинности пользователя.
4) Протоколы идентификации с нулевой передачей знаний.
5) Упрощенная схема идентификации с нулевой передачей знаний.
6) Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA.
7) Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.
8) Отечественный стандарт хэш-функции. Алгоритм цифровой подписи RSA.
9) Алгоритм цифровой подписи Эль-Гамаля (EGSA).
10) Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.

Практическая работа № 8. Реализация протокола Диффи-Хеллмана на эллиптических кривых

Цель работы: изучение особенностей реализации криптографических протоколов распределения ключей, асимметричной криптографии на эллиптических кривых, разработка системы распределения криптографических ключей.

Вопросы по практической работе:

1. Цель применения протокола Диффи-Хеллмана.
2. Что представляет собой эллиптическая кривая?
3. Какие операции определены на эллиптической кривой при использовании в криптографических приложениях?
4. Как выполнить умножение точки эллиптической кривой на число?
5. Как вычислить число. Обратное к данному по заданному модулю?
6. Что является нулем эллиптической кривой?

Тема 9. Программно-аппаратные средства защиты ПЭВМ и сетей

Контрольные вопросы:

1) Методы средства ограничения доступа к компонентам сети;
2) Методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям:
3) Методы и средства хранения ключевой информации;
4) Защита программ от изучения; защита от разрушающих программных воздействий; защита от изменений и контроль целостности.

Практическая работа № 9. Корректирующие коды. Коды Хэмминга

Цель: ознакомиться с общими принципами построения и использования корректирующих кодов для контроля целостности информации, распространяемой по телекоммуникационным каналам, изучить метод кодирования по Хэммингу

Вопросы по практической работе::

1. Охарактеризуйте понятие «корректирующий код»
2. Перечислите ошибки, возникающие при передаче информации
3. Приведите алгоритм построения кода Хэмминга
4. К какому виду кодирования относится метод Хэмминга?
5. Поясните алгоритм вычисления функции H(X)
6. Каким образом можно установить наличие ошибки в сообщении X? Как определить место ошибки?

Тестовые задания

1. Угрозы, вызваные действием человеческого фактора
- естественными угрозы
+ искусственные угрозы
- случайные угрозы
- преднамеренные угрозы
-апеллируемость
2. Угрозы, вызванные халатностью или непреднамеренными ошибками персонала
- естественными угрозы
- искусственные угрозы
+ случайные угрозы
- преднамеренные угрозы
-апеллируемость
3. Угрозы, вызванные направленной деятельностью злоумышленника
- естественными угрозы
- искусственные угрозы
- случайные угрозы
- апеллируемость
4 Алгоритм DES использует длину блока:
+ 64 бит
- 256 бит
- 128 бит
- 8 бит
- 16 бит
5 Алгоритм DES использует длину ключа
+ 56 бит
- 256 бит
- 128 бит
- 8 бит
- 16 бит
6 Алгоритм Диффи-Хеллмана используется для
+ открытого распределения ключей
- вычисления хэш-функции
- генерации простых чисел
- генерации случайных чисел
- безопастного хранения ключей
7 Алгоритм Диффи-Хелмана позволяет
+использовать незащищенный от прослушивания, но защищённый от подмены, канал связи
- генерировать новые простые числа
- вычислить хэш функцию
- генерировать случайные числа
- безопасно хранить ключи
8 Алгоритм шифрования SHA предназначен для использования совместно с алгоритмом цифровой подписи
+ DSA
- DOS
- DES
- EGS
- RSA

9 Объект «А» заявляет, что он не посылал сообщение объекту «Б», хотя на самом деле он все-таки посылал:

+отказ (ренегатство)

- подделка
- модификация (переделка)
- маскировка
- активный перехват

10 Антивирус – это программа, которая

+ удаляет некоторые категории вредоносных программ, достигая успеха менее чем в 100 процентах случаев

- удаляет все виды вредоносного ПО с вашего компьютера
- может быть обновлена средствами «Автоматического обновления Windows» для получения новых сигнатур
- позволяет «откатить» все изменения, произведенные с момента активации враждебной программы, либо воспрепятствует ее активации в первую очередь
- удаляет все виды вредоносного ПО с компьютера

11Аспектами информационной безопасности являются

+ конфиденциальность, доступность, целостность

- неизменность, доступность, целостность
- неизменность , конфиденциальность
- конфиденциальность, целостность
- доступность, конфиденциальность

12 Аудит информационной безопасности должен включать в себя

+ анализ информационных рисков с целью оценки вероятного ущерба и инструментальной проверки защищенности для определения возможности реализации угроз

- оценку угроз
- анализ и классификацию угроз безопасности согласно модели нарушителя
- оценку стоимости ресурсов и информации.
- оценку зависимости компании от внешних связей и тесты на проникновение

13 Безопасность данных в информационной базе обеспечивается

+ конфиденциальностью, целостностью и доступностью информации

- периодичностью обновления информации
- шифрованием информации
- идентификацией абонентов
- определением полномочий

14 Абонент «А» изменяет сообщение и утверждает, что данное (измененное) сообщение послал ему абонент «Б»

+ модификация (переделка)

- маскировка
- активный перехват
- отказ
- подделка

15Абонент «А» формирует сообщение и утверждает, что данное (измененное) сообщение послал ему абонент «Б»

+ подделка

- активный перехват
- отказ
- модификация
- маскировка

16 Более усовершенствованный вид мнемокодов

+ автокоды

- RSS-коды

- штрихкоды
- чит-коды
- отладочный код

17В каком году был представлен алгоритм Диффи-Хелмана:

+ 1975г
- 1974г
- 1978г
- 1977г
- 1976г

18В Каком году и где был разработан алгоритм SHA

+ 1993 году в США
- 1991 году в США
- 1995 году в США
- 1992 году в США
- 1994 году в США

19 В MS OFFICE компания MICROSOFT использует алгоритм шифрования

+ AES с 128-битным ключом
- AES с 256-битным ключом
- AES с 16-битным ключом
- AES с 32-битным ключом
- AES с 8 -битным ключом

20В Процедуре постановки подписи используется

+секретный ключ отправителя сообщения
- закрытый ключ отправителя сообщения
- открытый ключ отправителя сообщения
- чит-код
- хеш-функция

21В Процедуре проверки подписи используется:

+открытый ключ отправителя
- генерация пары ключей
- секретный ключ отправителя
- хеш-функция
- аудит подписи

22В Процедуре формирования подписи используется

+секретный ключ отправителя
- открытый ключ отправителя
- генерация пары ключей
- идентификация субъекта
- идентификация объекта

23 Абонент «А» только что прислал вам по icq ссылку на *.exe файл в интернете, предложил запустить его и вышел из сети, так что вы не можете уточнить детали. правильные действия:

+никогда не открою ссылку, даже если она от друга
- открою ссылку
- открою ссылку, если известен ключ
- .exe файл заблокируется
- открою ссылку после перезагрузки

24 Вид злоумышленного действия , если абонент с повторяет ранее переданный документ, который абонент а посылал абоненту В.

+повтор
- замена
- подмена

- ренегатство
- копирование

25 Абонент «В» перехватывает сообщения между абонентом «А» и абонентом «Б» с целью их скрытой модификации:

+активный перехват
- подделка
- отказ
- маскировка
- модификация

26Абонент «В» повторяет ранее переданное сообщение, которое абонент «А» посылал ранее «Б»

+повтор
- маскировка
- имитация
- модификация
- подделка

27Абонент «В» посылает абоненту «Б» сообщение от имени абонента «А»

+Маскировка (имитация)
- модификация
- отказ
- подделка
- активный перехват

28Возможность использовать одинаковые имена для методов входящих различные классы называются:

+ полиформизм
- метоморфизм
- декапсуляция
- наследование
- инкапсуляция

29 ВОЗМОЖНЫЕ ПОСЛЕДСТВИЯ BOTNET-ИНФЕКЦИИ:

+заражение boot-секторов дисков, могут привести к полной потере всей информации, хранящейся на диске
- компьютер будет захвачен и втайне использован для рассылки спама и проведения атак на другие ПК
- ваш ПК будет действовать как сервер, подчиняясь удаленным командам хакера
- часть вашего Интернет-канала будет использоваться под вредоносный исходящий трафик
- проведение атак на другие ПК

30 ВЫ ПОЛУЧАЕТЕ EMAIL ОТ ВАШЕГО БАНКА С ПРОСЬБОЙ В ТЕЧЕНИЕ НЕДЕЛИ ПОДТВЕРДИТЬ ВАШИ ПОСЛЕДНИЕ ПОКУПКИ, ПЕРЕЙДЯ НА СООТВЕТСТВУЮЩУЮ СТРАНИЦУ САЙТА БАНКА. ВАШИ ДЕЙСТВИЯ

+ буду бдительным - уточню в банке подлинность письма, не буду кликать ни по каким ссылкам в письме и проверю свой счет, вручную набрав нужный адрес в адресной строке браузера
- проследую по ссылке из письма и введу требуемую информацию, т.к письмо имеет все признаки послания от легитимной организации
- развлекусь, введя на требуемой странице ложную информацию -
- все равно я ничего не теряю; - я знаю, что это phishing - поэтому удалю сообщение из почтового ящика
- решу, как поступить позже

31ВЫБЕРИТЕ ВИД АНТИВИРУСНЫХ ПРОГРАММ, ПЕРЕХВАТЫВАЮЩИХ «ВИРУСО-ОПАСНЫЕ» СИТУАЦИИ И СООБЩАЮЩИХ ОБ ЭТОМ ПОЛЬЗОВАТЕЛЮ

+ блокировщик
- сканер
- CRC-сканер
- детектор
- имунизатор

32ВЫБЕРИТЕ ИЗ СПИСКА ПАРОЛЬ, КОТОРЫЙ НАИБОЛЕЕ ТОЧНО СООТВЕТСТВУЕТ ТРЕБОВАНИЯМ СТАНДАРТА

+ l#derk!
- gfhjkm23
- 1234567
- 114*%!
- poiuytre

33НЕВЫПОЛНЕНИЕ КАКОГО ИЗ СЛЕДУЮЩИХ ТРЕБОВАНИЙ ПОЛИТИКИ БЕЗОПАСНОСТИ МОЖЕТ НАИБОЛЬШИМ ОБРАЗОМ ПОВЫСИТЬ СУЩЕСТВУЮЩИЕ В СИСТЕМЕ ИНФОРМАЦИОННЫЕ РИСКИ

+ регулярное обновление антивирусных баз
- регулярное выключение компьютера
- завершение активной сессии пользователя по окончании работы
- создание и подержание форума по информационной безопасности для всех специалистов, вовлеченных в процесс обеспечения ИБ
- классификация ресурсов по степени важности с точки зрения ИБ номера заданий

34 ДЛЯ «СЖАТИЯ» ПРОИЗВОЛЬНОГО СООБЩЕНИЯ СЛУЖАТ

+ ХЭШ-функции
- EGSA-Функции
- DES-Функции
- RSA-Функции
- DOS-Функции

35 ДЛЯ ЗАЩИТЫ СИСТЕМЫ ШИФРОВАННОЙ СВЯЗИ ОТ НАВЯЗЫВАНИЯ ЛОЖНЫХ ДАННЫХ ИСПОЛЬЗУЕТСЯ

+ имитозащита
- пароль
- имитоконтроль
- брандмауэр
- шифрование

36ДЛЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ ПЕРЕДАВАЕМЫХ ПО СЕТЯМ ДАННЫХ ИСПОЛЬЗУЕТСЯ

+ электронная цифровая подпись
- межсетевое экранирование
- аудит событий
- идентификация данных
- аутентификация данных

37ДЛЯ ПРОВЕДЕНИЯ АНАЛИЗА ИНФОРМАЦИОННЫХ РИСКОВ НЕОБХОДИМо

+ построение полной модели информационной системы с точки зрения информационной безопасности
- вероятностные оценки угроз безопасности
- модель нарушителя
- модель пользователя
- градация информационных рисков

38ДЛЯ ПРОВЕРКИ ПОДПИСИ НЕОБХОДИМО ИСПОЛЬЗОВАть

+ оба ключа - секретный и открытый
- секретный ключ получателя сообщения

- открытый ключ получателя сообщения
- секретный ключ отправителя сообщения
- открытый ключ отправителя сообщения

39 ДЛЯ ЧЕГО ИСПОЛЬЗУЕТСЯ АЛГОРИТМ ДИФФИ-ХЕЛЛМАНА

+ для получения общего секретного ключа при общении через незащищенный канал связи
- подключения к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации
- для прямого обмена ключами между пользователями информационной системы
- для создания одного или нескольких центров распределения ключей
- для создания открытого и закрытого ключей

40ДОСТУПНОСТЬ ИНФОРМАЦИИ ГАРАНТИРУЕТ

+ получение требуемой информации за определенное время
- защищенность информации от возможных угроз
- доставка информации за конкретное время
- неизменность информации в любое время
- получение требуемой информации за неопределенное время

411ЕВРОПЕЙСКИЕ КРИТЕРИИ АСПЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

+ конфиденциальность, целостность, доступность
- верифицируемость
- непротиворечивость, конфиденциальность
- защита от несанкционированного прочтения, доступность
- условия доступа

42ЗАГРУЗОЧНЫЕ ВИРУСЫ ХАРАКТЕРИЗУЮТСЯ ТЕМ, ЧТО:

+ поражают загрузочные сектора дисков
- всегда меняют начало и длину файла
- весь код заражаемого файла
- запускаются при загрузке компьютера
- поражают программы в начале их работы

43 ЗЛОУМЫШЛЕННЫЕ ДЕЙСТВИЯ ОТПРАВИТЕЛЯ ЗАЯВЛЯЮЩЕГО, ЧТО ОН НЕ ПОСЫЛАЛ сообщение

+ отказ (ренегатство)
- подделка
- модификация
- усовершенствованный вид мнемокодов
- использование имитовставок

44ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИИ ПРИМЕНЯЮТСЯ

+ для ограничения доступа случайных и незаконных субъектов к информационной системе
- защиты информации
- идентификации визави
- для защиты от незаконного проникновения
- для получения требуемой информации

45 ИМИТАЦИЕЙ СООБЩЕНИЯ ЯВЛЯЕТСЯ

+ маскировка
- перехват
- модификация
- подделка
- повтор

46 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ХАРАКТЕРИЗУЕТ ЗАЩИЩЕННОСТЬ

+ информации и поддерживающей ее инфраструктуры
- защищенность инфраструктуры
- гарантии получения требуемой информации
- защиту от незаконного проникновения
- от несанкционированного доступа

47К ГРУППЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ, В КОТОРОЙ ОСНОВНЫМ СРЕДСТВОМ ЯВЛЯЕТСЯ АППАРАТУРА, ОТНОСЯТСЯ

+ подключение к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации
- исключение несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным
- копирование программой информации с носителей
- исключение значительной части загрузочных модулей из сферы их досягаемости
- хищение носителей информации магнитных дисков, дискет, лент

48К НЕПРЕДНАМЕРЕННЫМ УГРОЗАМ ОТНОСЯТСЯ

+ ошибки в разработке программных средств КС
- несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями
- изменение или уничтожение информации, сделанное уполномоченным лицом с обоснованной цепью
- угроза нарушения конфиденциальности, утечка информации, хранящейся в КС или передаваемой
- ослабление политики безопасности администратором, отвечающим за безопасность КС

49 К ОСНОВНЫМ ПРОГРАММНО-ТЕХНИЧЕСКИМ МЕРАМ ОТНОСЯТСЯ

+ аутентификация пользователя и установление его идентичности, доступ к данным, целостность данных, протоколирование и аудит, защита коммуникаций между клиентом и сервером
- отражение угроз
- аутентификация пользователя, целостность данных
- отражение угроз, аутентификация пользователя, целостность данных
- защита коммуникаций между клиентом и сервером

50 К ПРИЧИНАМ СЛУЧАЙНЫХ ВОЗДЕЙСТВИЙ ПРИ ЭКСПЛУАТАЦИИ НЕ ОТНОСИТСЯ

+ преднамеренный взлом
- ошибки в программном обеспечении
- аварийные ситуации из-за стихийных бедствий и отключений электропитания
- ошибки в работе персонала
- отказы и сбои аппаратуры

51К УМЫШЛЕННЫМ УГРОЗАМ ОТНОСЯТСЯ

+ несанкционированные действия обслуживающего персонала КС вследствие ослабления политики безопасности администратором
- преднамеренный взлом
- ослабление политики безопасности
- работа под чужой учетной записью
- ошибки в программировании

52НАУКА О МАТЕМАТИЧЕСКИХ МЕТОДАХ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И АУТЕНТИЧНОСТИ, ЦЕЛОСТНОСТИ И ПОДЛИННОСТИ АВТОРСТВА ИНФОРМАЦИИ

+ криптография
- матанализ

- теория вероятности
- методы защиты информации
- математическое моделирование

53 В ПОЛИТИКЕ БЕЗОПАСНОСТИ НЕ РАССМАТРИВАЕТСЯ

+ анализ экономических рисков
- категорирование сотрудников защищенность механизмов безопасности и политика учетных записей
- основные подразделения, работающие в области защиты информации
- защита от вирусов
- резервное копирование

54ЧТОБЫ УМЕНЬШИТЬ ПОДВЕРЖЕННОСТЬ ПК ВОЗДЕЙСТВИЮ НА НЕГО ВРЕДОНОСНОГО КОДА

+ работать под учетной записью с ограниченными правами
- использовать инкрементальное резервирование файлов
- устанавливать разрешения доступа к файлам и принтерам компьютера только для компьютеров из местной подсети
- использовать брандмауэр
- использовать шифрование и антиспам, автоматически удаляющий сообщения от неизвестных отправителей

55ЭЛЕКТРОННАЯ ПОДПИСЬ ШИФРУЕТСЯ

+ с помощью специальной программы создаются два ключа: закрытый и публичный
- подпись шифруется произвольным образом и записывается в файл
- с помощью специальной программы создается графический образ подписи
- посыпается по электронной почте подтверждение
- подпись шифруется симметричным кодом

56НЕ ЯВЛЯЕТСЯ ГРУППОЙ КОМПОНЕНТОВ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

+ среда - период действия, автономность, языковые группы
- обслуживающий персонал и пользователи
- аппаратные средства
- операционные системы и системные программы, утилиты, диагностические программы
- данные, хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.

57ДЛИНА КЛЮЧА НЕДОСЯГАЕМАЯ ДЛЯ ВСЕХ ИЗВЕСТНЫХ АЛГОРИТМОВ ВЗЛОМА:

+ 768 бит
- 1024 бита
- 512 бит
- 128 битов
- 64 бит

58 В ОСНОВЕ DES И ГОСТ 28147-89 ЛЕЖИТ СХЕМА ШИФРОВАНИЯ

+ сеть Фейстеля
- алгоритм Кантора
- шифр Виженера
- Цезаря
- Полибия

Полибия

59 ОСНОВНОЙ НЕДОСТАТОК СОВРЕМЕННЫХ АНТИВИРУСОВ

+ зависимость от вирусных сигнатур незрелость эвристических методов детекции

- высокие аппаратные требования
- низкие аппаратные требования
- высокая цена и отсутствие бесштатной телефонной поддержки
- могут случаться ложные срабатывания и пользователь должен вручную восстанавливать удаленные файлы из карантина

60ДЕЙСТВИЯ ПРИ НАЗНАЧЕНИИ ПРАВ ДОСТУПА ДЛЯ НОВОГО ПОЛЬЗОВАТЕЛЯ

+ ознакомление и документальная фиксация назначенных пользователю прав доступа
- проверка резюме и характеристики пользователя для наделения соответствующих прав доступа
- проверка соответствия прав пользователя выполняемым бизнес задачам
- предоставить и контролировать дальнейшую работу с системой
- проверка наличия у пользователя полученного от ответственного лица разрешения на работу с данной системой

61НАИБОЛЕЕ ТОЧНОЕ ОПРЕДЕЛЕНИЕ КОМПЬЮТЕРНОГО ВИРУСА

+ программа, воспроизводящаяся присоединением части своего кода к обычным файлам с целью распространения и преднамеренного причинения ущерба аппаратному, или программному обеспечению ПК, или файлам
- файл, приказывающий вашему ПК перезагружаться после установки и добавляющий свою запись в ветку "Запуск" реестра Windows
- файл произвольно перегружающий ПК
- программа, прячущая себя в системе и запоминающая введенные пароли, которые позже сообщает злоумышленникам
- устройство, тайно помещенное в компьютере для контроля вашей деятельности и перехвата сигналов

62ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ ДОСТУПНОЕ В ОПЕРАЦИОННОЙ СРЕДЕ

+ средства защиты, системные утилиты, системные редакторы, средства разработки
- системное ПО
- операционная система
- утилиты
- антивирусные программы

63РЕЗУЛЬТАТ ШИФРОВАНИЯ СЛОВА "КОТ" ШИФРОМ ЦЕЗАРЯ С КЛЮЧОМ

+ Мрф
- нрс
- лпу;
- фрм
- ток

64ВИД АНТИВИРУСНЫХ ПРОГРАММ ОСНОВАННЫЙ НА ПОДСЧЕТЕ КОНТРОЛЬНЫХ СУММ ДЛЯ ПРИСУТСТВУЮЩИХ НА ДИСКЕ ФАЙЛОВ СИСТЕМНЫХ СЕКТОРОВ:

+ CRC-сканер
- детектор
- сканер
- блокировщик
- иммунизатор

65ВИД РЕЗЕРВНОГО КОПИРОВАНИЯ, ЗАНИМАЮЩИЙ МЕНЬШЕ ВРЕМЕНИ

+ инкрементное

- в режиме реального времени
- полное
- клонирование
- дифференциальное

66ВИД РЕЗЕРВНОГО КОПИРОВАНИЯ, УСКОРЯЮЩИЙ ПРОЦЕСС ВОССТАНОВЛЕНИЯ:

+ дифференциальное
- клонирование
- инкрементное
- полное
- реального времени

67 НАИЛУЧШИЙ ВАРИАНТ, ОПИСЫВАЮЩИЙ ВОЗМОЖНЫЕ ПОСЛЕДСТВИЯ BOTNET-ИНФЕКЦИИ:

+ ваш ПК будет действовать как сервер, подчиняясь удаленным командам хакера;
- вашего Интернет-канала будет использоваться под вредоносный исходящий трафик
- ваш ПК будет действовать как клиент
- ваш компьютер будет захвачен и в тайне от Вас использован для рассылки спама
- ваш ПК будет использован для проведения атак на другие ПК

68КЛЮЧ, ДОСТУПНЫЙ ВСЕМ, ДЛЯ ПРОВЕРКИ ЦИФРОВОЙ ПОДПИСИ ПОД ДОКУМЕНТОМ

+ открытый
- приватный
- доступный
- внутренний
- закрытый

69ДЛИНА КЛЮЧА, РЕКОМЕНДУЕМАЯ ЛАБОРАТОРИЕЙ RSA, ДЛЯ МЕНЕЕ ЦЕННОЙ ИНФОРМАЦИИ

+ 768 бит
- 512 бит
- 1024 бит
- 64 бит
- 128 битов

70 ДЛИНУ КЛЮЧА, РЕКОМЕНДУЕМАЯ ЛАБОРАТОРИЕЙ RSA, ДЛЯ ОБЫЧНЫХ ЗАДАЧ:

+ 1024 бита
- 2048 битов
- 128 битов;
- 64 бит
- 10654

71ДЛИНА КЛЮЧА, РЕКОМЕНДУЕМАЯ ЛАБОРАТОРИЕЙ RSA, ДЛЯ ОСОБО ВАЖНЫХ ЗАДАЧ:

+ 2048 битов
- 1024 бита
- 768
- 3072 бит
- 526 бит

72ОСНОВНАЯ ЗАДАЧА В ДОЛЖНОСТНОЙ ИНСТРУКЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ДЛЯ КАЖДОГО СОТРУДНИКА

+ обеспечение информационной безопасности

- отчеты о секьюрити инцидентах
- защита от вирусов и троянских программ
- защита от интернет червей
- обеспечение непрерывного ведения бизнеса

73КЕЙЛОГГЕР – ЭТО

+ программа, использующая технику внедрения в ядро операционной системы для сокрытия присутствия в системе и перехватывающий все нажатия клавиш
- программа, которая размножается посредством рассылки своей копии
- программа, которая изменяет параметры настройки веб-браузера
- программа, которая добавляет свои ссылки в меню «Избранное»
- программа, которая удаляет файлы

74 К РАЗГРАНИЧЕНИЮ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ НЕ ОТНОСИТСЯ

+ матрицы установления полномочий
- вход в систему- под учетной записью
- парольное разграничение доступа
- разграничение криптографических ключей
- разграничение доступа по спискам

75 КЛЮЧ ШИФРА ДОЛЖЕН ОПРЕДЕЛЯТЬСЯ ТОЛЬКО

+ секретностью ключа
- доступностью ключа
- стойкостью криптосистемы
- сложностью шифрования
- длиной ключа

76КОМПЛЕКС ПРЕДУПРЕДИТЕЛЬНЫХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ – ЭТО

+ политика безопасности в защите сети
- надежность информации
- информационная политика
- информационная безопасность
- защита информации

77КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ ГАРАНТИРУЕТ

+ доступность информации кругу лиц, для кого она предназначена
- защищенность информации от возможных угроз
- защищенность информации от фальсификации
- доступность информации только автору
- защищенность информации от потери

78КОСВЕННЫМИ КАНАЛАМИ УТЕЧКИ НАЗЫВАЮТ

+ каналы, не связанные с физическим доступом к элементам КС
- каналы, связанные с физическим доступом к элементам КС
- доступ к информации посредством взлома
- вход в КС на основе специально разработанного кода программы
- кейлоггеры

79 МАСКИРОВКА - ЭТО

+ имитация
- отказ
- ренегатство
- подделка
- переделка

80 МАССИРОВАННАЯ ОТПРАВКА ПАКЕТОВ ДАННЫХ НА УЗЛЫ СЕТИ ПРЕДПРИЯТИЯ, С ЦЕЛЬЮ ИХ ПЕРЕГРУЗКИ И ВЫВЕДЕНИЯ ИЗ СТРОЯ

+ DOS атаки

- хакер атаки
- искусственные атаки
- вирусные атаки
- сетевая атака

81Информационная безопасность должна обеспечиваться на

+ законодательном, административном, процедурном, программном, техническом уровне
- программном, техническом, процедурном уровне
- программном, техническом уровне
- законодательном, административном, процедурном уровне
- процедурном, программном, техническом уровне

82Алгоритм RSA основан на труднорешаемой задаче

+ факторизации чисел
- нормализация чисел
- в вычислении обратного элемента
- дискретного логарифмирования
- нахождения большого простого числа

83Методы защиты от вирусов

+ программный, аппаратный, организационный
- установка антивирусной программы
- разграничение доступа
- установка брандмауэра
- соблюдение правил работы за компьютером

84 Наиболее действенным методом защиты от повтора являются

+ использование имитовставок и учет входящих сообщений
- учет входящих сообщений
- маскировка (имитация), повтор используется аутентификация электронных документов
- подделка, активный перехват
- использование имитовставок

85 Наиболее известные из хэш-функций

+ MD2, MD4, MD5 и SHA
- MD2, MD4, MD9 и SHA
- D2,MD4, MD10 и SHA
- MD2, MD4, MD5-5 и SHA
- MD2, MD4, MD5-6 и SHA

86Наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу - это

+ криптоанализ
- теория вероятностей
- матанлиз
- криптология
- криптография

87Может привести к повышению риска повреждения информации в системе при несоблюдении такого минимального требования, как

+ регулярное обновление антивирусных баз
- укрепление законности
- резервное копирование
- анализ информационных рисков
- построение модели информационной системы с точки зрения информационной безопасности

88Организационными мероприятиями предусматривается

+ исключение несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным

- защита ключей шифрования и электронной цифровой подписи (ЭЦП) и неизменность алгоритма шифрования и ЭЦП
- исключение нахождения в местах наличия информативного сигнала злоумышленника и контроль за его действиями и передвижением;;
- исключение значительной части загрузочных модулей из сферы их досягаемости
- использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ

89 Основной задачей теста на проникновение является

+ оценка возможности осуществления атаки из Интернета на информационную систему компании

- проверка времени реакции взломщика
- оценка возможных потерь при реализации атаки из Интернет
- оценка возможности обнаружения атаки службой ИБ компании
- проверка времени реакции службы обеспечения информационной безопасности

90Основные типы вирусов

+ программные, загрузочные, макровирусы

- программные, загрузочные, аппаратные
- загрузочные и макровирусы
- программные, стэлс-вирусы
- программные, системные

91Основополагающим документом по информационной безопасности в Республики Казахстан является

+ Концепция информационной безопасности Республики Казахстан до 2016 года

- Закон о средствах массовой информации;
- Уголовный Кодекс;
- Закон "О национальной безопасности Республики Казахстан";
- Конституция Республики Казахстан

92Отказ - это

+ ренегатство

- модификация
- имитация
- маскировка
- замена

93По масштабу вредных воздействий компьютерные вирусы делятся

+ на безвредные, неопасные, опасные, очень опасные

- на вредные, неопасные, опасные, очень опасные
- на безвредные, опасные, очень опасные
- на очень опасные
- на неопасные, опасные

94По среде обитания компьютерные вирусы бывают:

+ файловые, загрузочные, макровирусы, сетевые

- файловые, загрузочные, сетевые
- файловые, черви
- загрузочные, макровирусы, сетевые
- файловые, загрузочные, макровирусы

95Под защитой информации понимается

+ совокупность мероприятий, методов и средств, обеспечивающих решение задач по проверке целостности информации и исключении несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным

- совокупность мероприятий, методов и средств, обеспечивающих решение задач по реализации механизма внутренней памяти с разделением адресных пространств
- мероприятия, методы и средства, обеспечивающие решение задач по разграничению прав пользователей
- мероприятия, методы и средства, обеспечивающие решение задач по разграничению прав пользователей и обслуживающего персонала
- мероприятия, методы и средства, обеспечивающие решение задач по реализации механизма виртуальной памяти с разделением адресных пространств

96Под информационной безопасностью понимается

+ защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации
- недоступность
- ошибки в программном обеспечении
- защита от ущерба владельцев или пользователей информации
- группа аспектов информационной безопасности

97Под организацией доступа к ресурсам понимается

+ весь комплекс мер, который выполняется в процессе эксплуатации КС для предотвращения несанкционированного воздействия на технические и программные средства и информацию
- исключение значительной части загрузочных модулей из сферы их досягаемости
- предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние
- исключение несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным; - хранения атрибутов системы защиты
- поддержки криптографического закрытия информации, обработки сбоев и отказов и некоторые другие

98Под угрозой безопасности информации в компьютерной системе (КС) понимают

+ событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации
- возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации
- деятельность по предотвращению несанкционированных и непреднамеренных воздействий на защищаемую информацию
- действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости
- деятельность по предотвращению утечки защищаемой информации

99Трудно обнаружимые вирусы, не имеющие сигнатур, не содержащие ни одного постоянного участка кода - это

+ полиморфик-вирусы
- троянская программа
- стелс-впрусы
- макро-вирусы
- конструкторы вирусов

100Политика информационной безопасности в общем случае является

+ обще-информационным документом
- руководящим документом для ограниченного использования
- руководящим документом для руководства компании, менеджеров, администраторов безопасности и системных администраторов
- руководящим документом для администраторов безопасности и системных администраторов

- руководящим документом для всех сотрудников компании

101. Происхождение термина «криптография» :

+ от слова «тайнопись»;

- от слова «шифрование»;

-от термина «скремблирование»;

- от термина «кодирование»;

- от термина «идентификация»

102. Метод надежной передачи информации по открытому каналу связи использует:

- криптографию;

- стеганографию;

- кодирование;

- скремблирование;

- идентификацию

103. Для чего используется система Kerberos?

+ для симметричной аутентификации;

- для несимметричной аутентификации;

- для выработки ЭЦП;

- для шифрования;

- для несимметричной идентификации

104. Что такое код обнаружения манипуляции с данными MDC?

+ есть результат действия хэш-функции;

- циклический контрольный код сообщения;

- код четности;

- имитоприставка;

- имтовставка

105. Наука об обеспечении секретности и / или аутентичности (подлинности) передаваемых сообщений:

- ЭЦП;

+ криптография;

- криптоанализ;

- стеганография;

- криптология

106. Замену символов с открытого текста, соответствующими символами алфавита криптотекста называют:

- простейшим шифром;

- блочным шифром;

- шифром подстановки;

+ шифром замены;

- шифром перестановки

107. Функции, для которых легко найти функцию прямого отображения и нельзя найти обратное называются:

- линейные функции;

- нелинейные функции;

+ односторонние функции;

- функции преобразования;

- хеш-функции

108. Системы, где с помощью открытого ключа шифруют ключ блочного криптоалгоритма, а само сообщение шифруют с помощью этого симметричного секретного ключа, называют:

+ гибридные криптосистемы;

- криптосистема RSA;

- электронная подпись;

- криптографические протоколы;
- функции преобразования;

109. Процесс применения шифра защищаемой информации называют:
- дешифрованием;
- вскрытием шифра;
- простой заменой;
+ шифрованием;
- криптографией

110. Как называют в криптографии сменный элемент шифра, который применяется для шифрования конкретного сообщения:
+ ключ;
-разрядность блока;
-число раундов шифрования;
- алгоритм шифрования;
- шифр

111. Процесс наложения по определенному закону гамма-шифра на открытые данные:
- хэширование;
- имитовставка;
+ гаммирование;
- код четности;
- имтовставка

112. Шифр – это …
- ключевое запоминающее устройство;
+ совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с использованием ключей;
- состояние, выражающее процесс образования зашифрованных данных из открытых данных;
- значение исходных открытых параметров алгоритма криптографического преобразования;
+ необратимые преобразования множества возможных открытых данных

113. Разрядность 3DES равна:
- 56 бит;
+ 112 бит;
- 168 бит;
- 256 бит;
- 64 бит

114. При использовании классических криптографических алгоритмов ключ шифрования и ключ дешифрования совпадают и такие криптосистемы называются:
- простыми криптосистемами;
- гибридными криптосистемами;
- ассиметричными криптосистемами;
+ симметричными криптосистемами;
- сложными криптосистемами

115. Линейное шифрование данных, основанное на поточном способе шифрования называется:
+ гаммированием;
- подстановкой;
- перестановкой;
-имтоприставкой

116. Криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись, разработанная в 1977 году, называется:

+ алгоритм шифрования RSA;
- алгоритм DSA;
- алгоритм DSS;
- алгоритм SHA;
- алгоритм GHA;

117. Цифровая подпись - …

- подпись, которая ставится на документах;
+ небольшое количество дополнительной цифровой информации, передаваемое вместе с подписываемым текстом, по которому можно удостоверится в аутентичности документа;
- код с исправлением ошибок;
- имитоприставка;
- имитовставка;

118. Функция, предназначенная для сжатия подписываемого документа до нескольких десятков, или сотен бит называется:

- логарифмической функцией;
- тригонометрической функцией;
+ хэш- функцией;
- ЭЦП;
- алгоритм RSA

119. алгоритм предназначенный для использования совместно с алгоритмом цифровой подписи DSA:

- DES;
- ГОСТ;
- Rundjael;
+ SHA
-RSA;

120. Чему равна разрядность блока алгоритма шифрования DES:

- 56 битам;
- 128 битам;
+ 64 битам;
+ 256 битам;
- 512 битам

121. Цель атаки на криптосистему:

+ нарушение целостности передачи информации абоненту;
- вскрытие ключа шифрования;
- фальсификация сообщения;
- вскрытие передаваемых зашифрованных сообщений;
-удаление сообщения

122.Установление санкционированным получателем (приемником) того факта, что полученное сообщение послано санкционированным отправителем (передатчиком) называется:

- идентификацией;
+ аутентификацией;
- авторизацией;
- контролем целостности информации;
- достоверностью

123. Совокупность действий (инструкций, команд, вычислений), выполняемых в заданной последовательности двумя или более субъектами с целью достижения определенного результата называется:

- алгоритмом;
- шифрованием;
- дешифрованием;
+ протоколом;
- идентификацией

124. Какова разрядность ключа алгоритма шифрования ГОСТ 28147 – 89 (первого российского стандарта шифрования):

- 56 бит;
- 64 бит;
- 128 бит;
+ 256 бит;
- 512 бит

10.2 Критерии оценки результатов текущего контроля освоения дисциплины

Критерии оценки ответов на контрольные вопросы

Оценка, уровень достижения компетенций	Описание критериев
Отлично, высокий	Обучающийся демонстрирует уверенное знание материала, полно излагает материал, дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка
Хорошо, продвинутый	Обучающийся демонстрирует уверенное знание материала, но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
Удовлетворительно, пороговый	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
Неудовлетворительно, компетенция не освоена	Обучающийся демонстрирует незнание большей части соответствующего вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

Критерии оценки практической работы

Оценка «отлично» – ставиться, если обучающийся демонстрирует знание теоретического и практического материала по теме практической работы, определяет взаимосвязи между показателями задачи, даёт правильный алгоритм решения, определяет междисциплинарные связи по условию задания. А также, если обучающийся имеет глубокие знания учебного материала по теме практической работы, показывает усвоение взаимосвязи основных понятий используемых в работе, смог ответить на все уточняющие и дополнительные вопросы.

Оценка «хорошо» – ставится, если обучающийся демонстрирует знание теоретического и практического материала по теме практической работы, допуская незначительные неточности при решении задач, имея неполное понимание междисциплинарных свя-

зей при правильном выборе алгоритма решения задания. А также, если обучающийся показал знание учебного материала, усвоил основную литературу, смог ответить почти полно на все заданные дополнительные и уточняющие вопросы.

Оценка «удовлетворительно» – ставится, если обучающийся затрудняется с правильной оценкой предложенной задачи, дает неполный ответ, требующий наводящих вопросов преподавателя, выбор алгоритма решения задачи возможен при наводящих вопросах преподавателя. А также, если обучающийся в целом освоил материал практической работы, ответил не на все уточняющие и дополнительные вопросы.

Оценка «неудовлетворительно» – ставится, если обучающийся дает неверную оценку ситуации, неправильно выбирает алгоритм действий. А также, если он имеет существенные пробелы в знаниях основного учебного материала практической работы, который полностью не раскрыл содержание вопросов, не смог ответить на уточняющие и дополнительные вопросы.

Критерии оценки тестовых заданий

Оценка, уровень достижения компетенций	Описание критериев
Отлично, высокий	Содержание правильных ответов в тесте не менее 90%
Хорошо, продвинутый	Содержание правильных ответов в тесте не менее 75%
Удовлетворительно, пороговый	Содержание правильных ответов в тесте не менее 50%
Неудовлетворительно, компетенция не освоена	Содержание правильных ответов в тесте менее 50%

10.3. Оценочные материалы для промежуточной аттестации по дисциплине

Вопросы для проведения зачета

1. Концепция и структура информационной безопасности.
2. Безопасность информации. Цель обеспечения защиты информации.
3. Система защиты информации.
4. Обеспечение защиты информации с точки зрения риска.
5. Критерии оценки защищенной системы. Общее решение задачи проектирования оптимальной системы защиты.
6. Нормативно-правовая база функционирования систем защиты информации.
7. Доктрина информационной безопасности РФ.
8. Уголовный кодекс РФ о преступлениях в сфере компьютерной безопасности.
9. Основные положения закона РФ “Об информации, информационных технологиях и о защите информации”.
10. Понятие угрозы. Классификация угроз.
11. Утечка, разглашение и несанкционированный доступ к конфиденциальной
12. информации.
13. Характеристики информации.
14. Угрозы безопасности информации.
15. Классификация методов и средств защиты информации.
16. Технические методы защиты.
17. Задачи, решаемые техническими методами защиты. Методы решения данных задач.
18. Средства обеспечения информационной безопасности в Internet.
19. История развития, структура и основные понятия криптологии.
20. Криптография как основа информационной безопасности.

21. Подстановочные и перестановочные криптоалгоритмы.
22. Потоковые и блочные криптоалгоритмы.
23. Симметричные и асимметричные криптоалгоритмы.
24. Симметричные криптосистемы. Общая схема симметричной криптосистемы.
25. Модель криптосистемы с открытым ключом. Сертификация открытых ключей.
26. Алгоритм с открытым ключом RSA.
27. Электронная цифровая подпись. Применение хэш-функции.
28. Стандарты шифрования DES и AES.
29. Российский стандарт шифрования ГОСТ 28147-89.
30. Защита информации на электронных носителях информации.
31. Архивация с шифрованием.
32. Аппаратные и программные средства защиты в реализации Microsoft.
33. Принципы построения парольной защиты.
34. Традиционные средства защиты компьютерной информации и их недостатки.
35. Комплексный подход к построению систем безопасности.
36. Классификация сетевых атак по цели.
37. Меры и средства обеспечения информационной безопасности компьютерных сетей.
38. Задачи защиты информации в компьютерных сетях и методы их решения.
39. Идентификация и аутентификация как сервисы безопасности.
40. Управление доступом и его виды.
41. Программные средства разграничения доступа, их сущность, достоинства и недостатки.
42. Модели разграничения доступа. Разграничение доступа по уровням и кольцам секретности, матрицам полномочий и мандатам. Способы и средства повышения надежности разграничения.
43. Примеры систем разграничения доступа. Другие программные средства защиты: регистрации, сигнализации, реагирования и т.п.
44. Программы защиты ЭВМ от электронных вирусов.
45. Способы организации и использования программных средств защиты.
46. Организационно-правовые средства защиты, их сущность, возможности, достоинства и недостатки.

10.4 Показатели, критерии и шкала оценивания ответов на зачете

Оценка, уровень достижения компетенций	Описание критериев
Зачтено, высокий	Обучающийся выполнил все задания, предусмотренные рабочей программой, отчитался об их выполнении, демонстрируя отличное знание освоенного материала и умение самостоятельно решать сложные задачи дисциплины
Зачтено, продвинутый	Обучающийся выполнил все задания, предусмотренные рабочей программой, отчитался об их выполнении, демонстрируя хорошее знание освоенного материала и умение самостоятельно решать стандартные задачи дисциплины
Зачтено, пороговый	Обучающийся выполнил все задания, предусмотренные рабочей программой, отчитался об их выполнении, демонстрируя знание основ освоенного материала и умение решать стандартные задачи дисциплины с помощью преподавателя

Не зачтено, компетенция не освоена	Обучающийся выполнил не все задания, предусмотренные рабочей программой или не отчитался об их выполнении, не подтверждает знание освоенного материала и не умеет решать стандартные задачи дисциплины даже с помощью преподавателя