МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

КГЭУ

«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «КГЭУ»)

АКТУАЛИЗИРОВАНО
Решением Ученого совета ИЦТЭ КГЭУ
Протокол №7 от 19.03.2024

Подписан: ФГБОУ ВО «КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
Владелец: Беляев Эдуард Ирекович
Директор Института цифровых технологий и экономики
Сертификат: 01E4B4530091B044A4464D6B8C379A8EBA
Действителен с 04.10.2023 по 04.10.2024

«УТВЕРЖДАЮ»
Директор института Цифровых технологий и экономики
_____ Торкунова Ю.В.

«26»_октября_2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации

Направление подготовки 01.03.04 Прикладная математика

Квалификация бакалавр

г. Казань, 2020

Рабочая программа дисциплины разработана в соответствии с ФГОС ВО - бакалавриат по направлению подготовки 01.03.04 Прикладная математика (приказ Минобрнауки России от 10.01.2018 г. № 11)

Программу разработал(и):

доцент,к.т.н. _____ Косулин Валерий Валентинович

Программа рассмотрена и одобрена на заседании выпускающей кафедры Инженерная кибернетика, протокол № 11 от 26 октября 2020 г.

Зав. кафедрой _____ Смирнов Ю.Н.

Программа одобрена на заседании методического совета института Цифровых технологий и экономики, протокол № 2 от 26.10.2020

Зам. директора института
Цифровых технологий и экономики _____ /Косулин В.В./

Программа принята решением Ученого совета института Цифровых технологий и экономики
протокол № 2 от 26 октября 2020 г.

Согласовано:

Руководитель ОПОП _____ / Смирнов Ю.Н./

1. Цель, задачи и планируемые результаты обучения по дисциплине

Целью освоения дисциплины "Защита информации" является изучение методов и средств защиты информации, обеспечения ее конфиденциальности, целостности и доступности в процессе хранения и передачи: криптографических алгоритмов и протоколов, протоколов и систем аутентификации, электронной цифровой подписи, технологий межсетевых экранов и виртуальных частных сетей.

Задачами дисциплины "Защита информации" является: получение базовых теоретических представлений о современных методах и технических средствах защиты компьютерной информации и практических навыков использования этих средств при реализации программных и аппаратных средств информационных систем масштаба предприятия.

Компетенции, формируемые у обучающихся, запланированные результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине (знать, уметь, владеть)
Общепрофессиональные компетенции (ОПК)		
ОПК-4 Способен разрабатывать и использовать современные методы и программные средства информационно- коммуникационных технологий	ОПК-4.1 Использует современные методы проектирования, разработки программных средств	*Знать:* основные тенденции и направления развития методов и средств защиты информации и их применения в информационных технологиях типовые программные продукты, ориентированные на решение задач информационной безопасности в корпоративных информационных системах *Уметь:* применять встроенные механизмы защиты в современных операционных системах *Владеть:* навыками использования существующих криптографических программных интерфейсов прикладного программирования, входящих в состав операционных систем
ОПК-4 Способен разрабатывать и использовать современные методы и программные средства информационно- коммуникационных технологий	ОПК-4.2 Реализовывает алгоритмы решения задач профессиональной деятельности на языке программирования	*Знать:* типовые программные продукты, ориентированные на решение задач информационной безопасности в корпоративных информационных системах *Уметь:* разрабатывать программные модули и подсистемы в составе программных комплексов обеспечивающие средства защиты информации, аутентификации пользователей и их авторизации использовать методы и средства защиты информации при передачи по открытым каналам связи использовать криптографические алгоритмы для защиты информации в программных средствах информационно-измерительных систем применять программные средства антиви-

		русной защиты *Владеть:* навыками разработки и отладки программных средств информационной безопасности навыками использования существующих интерфейсов прикладного программирования обеспечивающих готовые развитые средства аутентификации и авторизации пользователей
ОПК-2 Способен обоснованно выбирать, дорабатывать и применять для решения исследовательских и проектных задач математические методы и модели, осуществлять проверку адекватности моделей, анализировать результаты, оценивать надежность и качество функционирования систем	ОПК-2.2 Осуществляет проверку адекватности моделей, анализирует результаты, оценивает надежность и качество функционирования систем	*Знать:* основ функционирования межсетевых экранов и виртуальных частных сетей *Уметь:* использовать криптографические алгоритмы для защиты информации в программных средств в информационных системах в соответствии с их криптостойкостью *Владеть:* навыками использования, настройки и внедрения существующих программных средств межсетевого экранирования и построения защищенных коммуникационных каналов на основе технологии виртуальных частных сетей
ОПК-4 Способен разрабатывать и использовать современные методы и программные средства информационно- коммуникационных технологий	ОПК-4.2 Реализовывает алгоритмы решения задач профессиональной деятельности на языке программирования	*Знать:* типовые программные продукты, ориентированные на решение задач информационной безопасности в корпоративных информационных системах *Уметь:* разрабатывать программные модули и подсистемы в составе программных комплексов обеспечивающие средства защиты информации, аутентификации пользователей и их авторизации использовать методы и средства защиты информации при передачи по открытым каналам связи использовать криптографические алгоритмы для защиты информации в программных средствах информационно-измерительных систем применять программные средства антивирусной защиты *Владеть:* навыками разработки и отладки программных средств информационной безопасности навыками использования существующих интерфейсов прикладного программирования обеспечивающих готовые развитые средства аутентификации и авторизации пользователей
	ОПК-4.3 Применяет	*Знать:*

	современные методы и программные средства информационно-коммуникационных технологий	основы программирования средств защиты информации в прикладных программах общего назначения и программных средствах распределенных корпоративных информационных систем принципы реализации подсистем аутентификации в различных информационных системах *Уметь:* применять программные средства антивирусной защиты использовать методы и средства защиты информации при передачи по открытым каналам связи *Владеть:* навыками проектирования программных модулей криптографической защиты данных, подсистем локальной и распределенной аутентификации

2. Место дисциплины в структуре ОПОП

Дисциплина Защита информации относится к обязательной части учебного плана по направлению подготовки 01.03.04 Прикладная математика.

Код компетенции	Предшествующие дисциплины (модули), практики, НИР, др.	Последующие дисциплины (модули), практики, НИР, др.
ОПК-4	Информационные технологии Архитектура вычислительных систем	
ПК-2		Проектирование цифровых двойников предприятий
ПК-3		Проектирование цифровых двойников предприятий Управление в технических системах
ПК-5		Проектирование мобильных приложений
ПК-6		Проектирование мобильных приложений

Для освоения дисциплины обучающийся должен:

До начала изучения дисциплины студент должен:

Знать: основные положения теории информации; принципы функционирования аппаратных средств вычислительных систем, форматы представления данных в ЭВМ; основные положения теории алгоритмизации.

Уметь: разрабатывать алгоритмы решения задач; разрабатывать, отлаживать и тестировать программы на современных языках программирования

Владеть: навыками работы в среде операционных систем Windows и разработки, отладки и тестирования программ.

3. Структура и содержание дисциплины

3.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) (ЗЕ), всего 108 часов, из которых 45 часов составляет контактная работа обучающегося с преподавателем (занятия лекционного типа 16 час., занятия семинарского типа (практические, семинарские занятия, лабораторные работы и т.п.) 24 час., групповые и индивидуальные консультации 2 час., прием экзамена (КПА), зачета с оценкой - 1 час., самостоятельная

работа обучающегося 28 час, контроль самостоятельной работы (КСР) - 2 час. . Практическая подготовка по виду профессиональной деятельности составляет 10 часов.

Вид учебной работы	Всего ЗЕ	Всего часов	Семестр
			6
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ	3	108	108
КОНТАКТНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ, в том числе:	1,25	45	45
Лекционные занятия (Лек)	0,44	16	16
Лабораторные занятия (Лаб)	0,44	16	16
Практические занятия (Пр)	0,22	8	8
Контроль самостоятельной работы и иная контактная работа (КСР)	0,06	2	2
Консультации (Конс)	0,06	2	2
Контактные часы во время аттестации	0,03	1	1
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ (СРС):	0,78	28	28
Подготовка к промежуточной аттестации в форме: (экзамен)	0,97	35	35
ФОРМА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ		Э	Э

3.2. Содержание дисциплины, структурированное по разделам и видам занятий

Разделы дисциплины	**Семестр**	**Распределение трудоемкости (в часах) по видам учебной работы, включая СРС**								**Формируемые результаты обучения (знания, умения, навыки)**	**Литература**	**Формы текущего контроля успеваемости**	**Формы промежуточной аттестации**	**Максимальное количество баллов по балльно-рейтинговой системе**
		Занятия лекционного типа	Занятия практического / семинарского типа	Лабораторные работы	Групповые консультации	Самостоятельная работа студента, в т.ч.	Контроль самостоятельной работы (КСР)	*подготовка к промежуточной аттестации*	Сдача зачета / экзамена	**Итого**				
Раздел 1. Основные понятия и анализ угроз информационной безопасности и защиты информации														
1. Основные понятия информационной безопасности и защиты информации	6	2				2				4	ОПК-4.1-31, ОПК-4.1-32	Л1.1, Л2.3	КОНСП ТЕСТ	Э	2
Раздел 2. Технологии защиты данных														

2. Криптография	6	5	8	16		17				46	ОПК-4.1-31, ОПК-4.2-31, ОПК-4.3-31, ОПК-4.1-32, ОПК-4.1-У1, ОПК-4.2-У1, ОПК-4.2-У2, ОПК-4.2-В1, ОПК-4.2-В2, ОПК-4.3-У2, ОПК-4.3-В1, ОПК-4.1-В1	Л1.1, Л2.3, Л1.3, Л2.1, Л2.2, Л1.2	КОНСП ТЕСТ КР ОТЧЕТ	Э	45
3. Аутентификация	6	2				1				3	ОПК-4.1-31, ОПК-4.1-32, ОПК-4.1-У1, ОПК-4.3-32	Л1.1, Л2.3	КОНСП ТЕСТ	Э	2
Раздел 3. Многоуровневая защита корпоративных информационных систем															
4. Корпоративная информационная система.	6	2				2				4	ОПК-4.1-31, ОПК-4.1-32, ОПК-4.1-У1, ОПК-4.2-31, ОПК-4.3-У2	Л1.1, Л2.3	КОНСП ТЕСТ	Э	2
5. Межсетевое экранирование	6	2				2				4	ОПК-4.1-31, ОПК-4.1-У1, ОПК-4.2-В1, ОПК-4.1-32	Л1.1, Л2.3	КОНСП ТЕСТ	Э	3
6. Сети VPN	6	1				2				3	ОПК-4.1-31, ОПК-4.1-32, ОПК-4.2-31	Л1.1, Л2.3	КОНСП ТЕСТ	Э	3
Раздел 4. Встраиваемые средства защиты информации современных интерфейсов прикладного программирования															
7. Встраиваемые средства защиты	6	2				2				4	ОПК-4.1-31, ОПК-4.1-32, ОПК-4.1-У1, ОПК-4.2-31, ОПК-	Л1.1, Л2.3	КОНСП ТЕСТ	Э	3

											4.2-У3, ОПК-4.3-У1				
Раздел 5. Контроль самостоятельной работы															
8. Контроль самостоятельной работы	6						2			2	ОПК-4.1-З1, ОПК-4.1-З2, ОПК-4.1-У1, ОПК-4.1-В1, ОПК-4.2-З1, ОПК-4.2-У1, ОПК-4.2-У2, ОПК-4.2-У3, ОПК-4.2-В1, ОПК-4.2-В2, ОПК-4.3-З1, ОПК-4.3-З2, ОПК-4.3-У1, ОПК-4.3-У2, ОПК-4.3-В1	Л1.2, Л1.3, Л2.1, Л2.2, Л2.3			
Раздел 6. Консультации															
9. Консультации	6									2	ОПК-4.1-З1, ОПК-4.1-З2, ОПК-4.1-У1, ОПК-4.1-В1, ОПК-4.2-З1, ОПК-4.2-У1, ОПК-4.2-У2, ОПК-4.2-У3, ОПК-4.2-В1, ОПК-4.2-В2, ОПК-4.3-З1, ОПК-4.3-З2, ОПК-4.3-У1, ОПК-4.3-У2, ОПК-4.3-В1	Л1.2, Л1.3, Л2.1, Л2.2, Л2.3			
Раздел 7. Контактные часы во время аттестации															

10. Контактные часы во время аттестации	6								1	1	ОПК-4.1-З1, ОПК-4.1-З2, ОПК-4.1-У1, ОПК-4.1-В1, ОПК-4.2-З1, ОПК-4.2-У1, ОПК-4.2-У2, ОПК-4.2-У3, ОПК-4.2-В1, ОПК-4.2-В2, ОПК-4.3-З1, ОПК-4.3-З2, ОПК-4.3-У1, ОПК-4.3-У2, ОПК-4.3-В1	Л1.2, Л1.3, Л2.1, Л2.2, Л2.3			
Промежуточная аттестация (экзамен)											ОПК-4.1-З1, ОПК-4.1-З2, ОПК-4.1-У1, ОПК-4.1-В1, ОПК-4.2-З1, ОПК-4.2-У1, ОПК-4.2-У2, ОПК-4.2-У3, ОПК-4.2-В1, ОПК-4.2-В2, ОПК-4.3-З1, ОПК-4.3-З2, ОПК-4.3-У1, ОПК-4.3-У2, ОПК-4.3-В1	Л1.2, Л1.3, Л2.1, Л2.2, Л2.3		Э	40
ИТОГО		16	8	16		28	2	35	1	108				Э	100

3.3. Тематический план лекционных занятий

Номер раздела дисциплины	Темы лекционных занятий	Трудоемкость, час.
1	Основные понятия информационной безопасности и защиты информации	1
2	Политика безопасности организации	1
3	Основные понятия криптографии. Симметричные криптосистемы	2
4	Ассиметричные криптосистемы. Хэширование	2
5	Управление криптоключами	1
6	Управление доступом к ресурсам информационных систем	2
7	Корпоративная информационная система с традиционной структурой	2
8	Технологии межсетевого экранирования	2
9	Технология виртуальных защищенных сетей VPN	1
10	Антивирусная защита информации	2
	Всего	16

3.4. Тематический план практических занятий

Номер раздела дисциплины	Темы практических занятий	Трудоемкость, час.
1	Симметричная криптоалгоритмы	2
2	Ассиметричные криптоалгоритмы	2
3	Электронно-цифровая подпись	4
	Всего	8

3.5. Тематический план лабораторных работ

Номер раздела дисциплины	Темы лабораторных работ	Трудоемкость, час.
1	Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации	2
2	Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей	2
3	Стандарт симметричного шифрования AES Rijndael	2
4	Генерация простых чисел, используемых в асиметричных системах шифрования	2
5	Изучение программных продуктов защиты информации. Программа PGP.	2
6	Защита программного обеспечения методами стеганографии	2
7	Защита электронных документов с использованием цифровых водяных знаков	2
8	Стегокомплексы, допускающие использование аудиоконтейнеров, на примере программы Invisible Secrets-4.	2
	Всего	16

3.6. Самостоятельная работа студента

Номер раздела дисциплины	Вид СРС	Содержание СРС	Трудоемкость, час.
1	Подготовка к лекционному занятию и формам контроля	Основные понятия информационной безопасности и защиты информации Политика безопасности организации	2
2	Подготовка к лекционному занятию и формам контроля	Основные понятия криптографии. Симметричные криптосистемы	1

3	Подготовка к лекционному занятию и формам контроля	Ассиметричные криптоалгоритмы. Хэширование	1
4	Подготовка к лекционному занятию и формам контроля	Управление ключами	1
5	Подготовка к практическому занятию и формам контроля	Симметричные криптоалгоритмы	2
6	Подготовка к практическому занятию и формам контроля	Ассиметричные криптоалгоритмы	2
7	Подготовка к практическому занятию и формам контроля	Эдектронно-цифровая подпись	2
8	Подготовка к лабораторной работе и формам контроля	Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации	1
9	Подготовка к лабораторному занятию и формам контроля	Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей	1
10	Подготовка к лабораторному занятию и формам контроля	Стандарт симметричного шифрования AES Rijndael	1
11	Подготовка к лабораторному занятию и формам контроля	Генерация простых чисел, используемых в асиметричных системах шифрования	1
12	Подготовка к лабораторному занятию и формам контроля	Изучение программных продуктов защиты информации. Программа PGP.	1
13	Подготовка к лабораторному занятию и формам контроля	Защита программного обеспечения методами стеганографии	1
14	Подготовка к лабораторному занятию и формам контроля	Защита электронных документов с использованием цифровых водяных знаков	1
15	Подготовка к лабораторному занятию и формам тестирования	Стегокомплексы, допускающие использование аудиоконтейнеров, на примере программы Invisible Secrets-4.	1
16	Подготовка к лекционному занятию и формам контроля	Управление доступом к ресурсам информационных систем	1
17	Подготовка к лекционному занятию и формам контроля	Корпоративная информационная система с традиционной структурой	2
18	Подготовка к лекции и формам тестирования	Технологии межсетевого экранирования	2
19	Подготовка к лекционному занятию и формам тестирования	Технология виртуальных защищенных сетей VPN	2
20	Подготовка к лекционному занятию и формам контроля	Антивирусная защита информации	2
		Всего	28

4. Образовательные технологии

Основные формы проведения занятий – все виды занятий проводятся с использованием технических средств обучения, презентаций. В рамках дисциплины применяются следующие технологии:

Технологии проблемного обучения - проблемные лекции с конструированием проблемной ситуации, метод эвристических заданий для практических и лабораторных занятиях.

Технологии игрового обучения, включающие моделирование предметного и социального содержания профессиональной деятельности бакалавра.

Технологии, обеспечивающие развитие критического мышления: интерактивная форма подачи учебного материала, вовлечение учащихся в осмысление проблемных ситуаций.

В качестве основных форм самостоятельной работы студентов предполагается аналитическая обработка текста (аннотирование и конспектирование); работа со справочной литературой; выполнение индивидуальных заданий по личной инициативе студента; подготовка к докладу на научных конференциях.

Дистанционные образовательные технологии, реализуемые в электронной форме через сеть Интернет с применением LMS Moodle а также выставление учебного и методического материала в личных кабинетах студентов

5. Оценивание результатов обучения

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля успеваемости, проводимого по балльно-рейтин-говой системе (БРС), и промежуточной аттестации.

Обобщенные критерии и шкала оценивания уровня сформированности компетенции (индикатора достижения компетенции) по итогам освоения дисциплины:

Планируемые результаты обучения	Обобщенные критерии и шкала оценивания результатов обучения			
	неудовлетворительно	удовлетворительно	хорошо	отлично
	не зачтено	зачтено		
Полнота знаний	Уровень знаний ниже минимальных требований, имеют место грубые ошибки	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок
Наличие умений	При решении стандартных задач не продемонстрированы	Продемонстрированы основные умения, решены типовые задачи с негрубыми	Продемонстрированы все основные умения, решены все основные задачи с	Продемонстрированы все основные умения, решены все основные задачи с
	основные умения, имеют место грубые ошибки	ошибками, выполнены все задания, но не в полном объеме	негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	отдельными несущественными недочетами, выполнены все задания в полном объеме

Наличие навыков (владение опытом)	При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов
Характеристика сформированности компетенции (индикатора достижения компетенции)	Компетенция в полной мере не сформирована. Имеющихся знаний, умений,навыков недостаточно для решения практических (профессиональных) задач	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практи- ческих (профессиональных) задач, но требуется дополнительная практика по большинству практических задач	Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений,навыков и мотивации в целом достаточно для решения стандартных практичес-ких (профессиональных) задач	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач
Уровень сформированности компетенции (индикатора достижения компетенции)	Низкий	Ниже среднего	Средний	Высокий

Шкала оценки результатов обучения по дисциплине:

Код компетенции	Код индикатора достижения	Запланированные результаты обучения по дисциплине	Уровень сформированности компетенции (индикатора достижения компетенции)			
			Высокий	Средний	Ниже среднего	Низкий
			Шкала оценивания			
			отлично	хорошо	удовлет-ворительно	неудовлет-ворительно
			зачтено			не зачтено
ОПК-2	ОПК-2.2	Знать				
		основ функционирования межсетевых экранов и виртуальных частных сетей	знает в совершенстве	Знает основные принципы	Знает отдельные принципы	Имеет представление
		Уметь				
		использовать криптографические алгоритмы для защиты информации в программных средств в информационных системах в соответствии с их криптостойкостью	Умеет в совершенстве	Умеет с некритичными ошибками	Допускает отдельные грубые ошибки	Не может без посторонней помощи использовать
		Владеть				

		навыками использования, настройки и внедрения существующих программных средств межсетевого экранирования и построения защищенных коммуникационных каналов на основе технологии виртуальных частных сетей	Владеет в совершенстве	Владеет отдельными навыками	Владеет отдельными навыками с недочетами	Не владеет без посторонней помощи
ОПК-4	ОПК- 4.1	Знать				
		основные тенденции и направления развития методов и средств защиты информации и их применения в информационных технологиях	Знает в совершенстве	Знает основные	Знает отдельные	Имеет общее представление
		типовые программные продукты, ориентированные на решение задач информационной безопасности в корпоративных информационных системах	Знает в совершенстве большинство программных продуктов	Знает основные программные продукты	Знает отдельные программные продукты	Имеет общее представление о программных продуктах
		Уметь				
		применять встроенные механизмы защиты в современных операционных системах	Умеет в совершенстве	Умеет с некритичными ошибками	Допускает отдельные грубые ошибки	Не может без посторонней помощи применять
		Владеть				
		навыками использования существующих криптографических программных интерфейсов прикладного программирования, входящих в состав операционных систем	Владеет в совершенстве	Владеет отдельными навыками	Владеет отдельными навыками с недочетами	Не владеет без посторонней помощи
		Знать				
		типовые программные продукты, ориентированные на решение задач информационной безопасности в корпоративных информационных системах	Знает в совершенстве большинство программных продуктов	Знает основные программные продукты	Знает отдельные программные продукты	Имеет общее представление о программных продуктах
		Уметь				
		разрабатывать программные модули и подсистемы в составе программных комплексов обеспечивающие средства защиты информации, аутентификации пользователей и их авторизации	Умеет в совершенстве	Умеет с некритичным ошибками	Допускает отдельные грубые ошибки	Не умеет разрабатывать самостоятельн о
		использовать криптографические алгоритмы для защиты информации в программных средствах информационно- измерительных систем	Умеет в совершенстве	Умеет с некритичными ошибками	Допускает отдельные грубые ошибки	Не может без посторонней помощи использовать
		использовать методы и средства защиты информации при передачи по открытым каналам связи	Умеет в совершенстве	Умеет с некритичными ошибками	Допускает отдельные грубые ошибки	Не может без посторонней помощи использовать
		применять программные средства антивирусной	Умеет в совершенстве	Умеет с некритичными ошибка-	Допускает отдельные грубые	Не может применять без посто-

		защиты		ми	ошибки	ронней помощи
		Владеть				
		навыками разработки и отладки программных средств информационной безопасности	Владеет в совершенстве	Владеет отдельными навыками	Владеет отдельными навыками с недочетами	Не владеет без посторонней помощи
		навыками использования существующих интерфейсов прикладного программирования обеспечивающих готовые развитые средства аутентификации и авторизации пользователей	Владеет в совершенстве	Владеет отдельными навыками	Владеет отдельными навыками с недочетами	Не владеет без посторонней помощи
	ОПК-4.3	Знать				
		основы программирования средств защиты информации в прикладных программах общего назначения и программных средствах распределенных корпоративных информационных систем	Знает в совершенстве	Знает основные принципы	Знает отдельные принципы	Имеет представление
		принципы реализации подсистем аутентификации в различных информационных системах	Знает в совершенстве	Знает основные принципы	Знает отдельные принципы	Имеет представление
		Уметь				
		применять программные средства антивирусной защиты	Умеет в совершенстве	Умеет с некритичными ошибками	Допускает отдельные грубые ошибки	Не может применять без посторонней помощи
		использовать методы и средства защиты информации при передачи по открытым каналам связи	Умеет в совершенстве	Умеет с некритичными ошибками	Допускает отдельные грубые ошибки	Не может без посторонней помощи использовать
		Владеть				
		навыками проектирования программных модулей криптографической защиты данных, подсистем локальной и распределенной аутентификации	Владеет в совершенстве	Владеет 1-2 стандартными методами	Владеет с негрубыми погрешностям и	Не владеет без посторонней помощи

Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации приведены в Приложении к рабочей программе дисциплины. Полный комплект заданий и материалов, необходимых для оценивания результатов обучения по дисциплине, хранится на кафедре-разработчике в бумажном и электронном виде.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Учебно-методическое обеспечение

Основная литература

№ п/п	Автор(ы)	Наиме- нование	Вид издания (учебник, учебное пособие, др.)	Место издания, издательство	Год издания	Адрес электронного ресурса	Кол-во экземпля- ров в библиотеке КГЭУ
1	Баранова Е. К., Бабаш А. В.	Криптографические методы защиты	Учебное пособие	М.: Кнорус	2017	https://www.book.ru/book/920017/	

		информации. Лабораторный практикум					
2	Мельников В. П., Куприянов А. И., Васильева Т. Ю.	Информационная безопасность	учебник	М.: Кнорус	2018	https://www.book.ru/book/929884	
3	Бабаш А. В., Баранова Е. К., Мельников Ю. Н.	Информационная безопасность. Лабораторный практикум (+CD)	Учебное пособие	М.: Кнорус	2016	https://www.book.ru/book/918700/	

Дополнительная литература

№ п/п	Автор(ы)	Наименование	Вид издания (учебник, учебное пособие, др.)	Место издания, издательство	Год издания	Адрес электронного ресурса	Кол-во экземпляров в библиотеке КГЭУ
1	Тараскин М. М., Захаров А. Г., Коваленко Ю. И., Москвитин Г. И.	Комплексная защита информации в организации	монография	М.: Русайнс	2016	https://www.book.ru/book/920774	
2	Леонтьев В.Е.	Практика применения методов криптографической защиты информации при работе с электронными документам и	учебное пособие по курсу "Информационная безопасность и защита информации"	Казань: КГЭУ	2008		6
3	Бабаш А. В., Баранова Е. К.	Криптографические методы защиты информации	Учебник	М.: Кнорус	2016	https://www.book.ru/book/918549/	

6.2. Информационное обеспечение

6.2.1. Электронные и интернет-ресурсы

№ п/п	Наименование электронных и интернет-ресурсов	Ссылка
1	ЭБС IBOOKS.RU	https://ibooks.ru
2	ЭБС LANBOOK.COM	https://e.lanbook.com

6.2.2. Профессиональные базы данных

№ п/п	Наименование профессиональных баз данных	Адрес	Режим доступа
1	Российская национальная библиотека	http://nlr.ru/	http://nlr.ru/
2	Общероссийский математический портал	http://www.mathnet.ru/	http://www.math

			net.ru/
3	КиберЛенинка	В https://cyberleninka.ru/	В https://cyberleninka.ru/
4	Национальная электронная библоиотека (НЭБ)	https://rusneb.ru/	https://rusneb.ru/
5	Техническая библиотека	http://techlibrary.ru	http://techlibrary.ru

6.2.3. Информационно-справочные системы

№ п/п	Наименование информационно-справочных систем	Адрес	Режим доступа
1	ИСС «Кодекс» / «Техэксперт»	http://app.kgeu.local/Home/Apps	http://app.kgeu.local/Home/Apps
2	«Консультант плюс»	http://www.consultant.ru/	http://www.consultant.ru/
3	«Гарант»	http://www.garant.ru/	http://www.garant.ru/

6.2.4. Лицензионное и свободно распространяемое программное обеспечение дисциплины

№ п/п	Наименование программного обеспечения	Описание	Реквизиты подтверждающих документов
1	Windows 7 Профессиональная (Pro)	Пользовательская операционная система	ЗАО "СофтЛайнТрейд" №2011.25486 от 28.11.2011 Неискл. право. Бессрочно
2	Office Professional Plus 2007 Windous32 Russian DiskKit MVL CD	Пакет программных продуктов содержащий в себе необходимые офисные программы	ЗАО "СофтЛайнТрейд" №225/10 от 28.01.2010 Неискл. право. Бессрочно
3	LMS Moodle	ПО для эффективного онлайн-взаимодействия преподавателя и студента	Свободная лицензия Неискл. право. Бессрочно
4	Браузер Chrome	Система поиска информации в сети интернет	Свободная лицензия Неискл. право. Бессрочно
5	Office Standard 2007 Russian OLP NL AcademicEdition+	Пакет программных продуктов содержащий в себе необходимые офисные программы	ЗАО "СофтЛайнТрейд", №21/2010 от 04.05.2010 Неискл. право. Бессрочно
6	Windows 10	Пользовательская операционная система	ООО "Софтлайн трейд" № Tr096148 от 29.09.2020, неискл. право, срок действия лицензии - до 14.09.2021

7. Материально-техническое обеспечение дисциплины

№ п/п	Вид учебной работы	Наименование специальных помещений и помещений для СРС	Оснащенность специальных помещений и помещений для СРС
1	Лекционные занятия	Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций	доска аудиторная, моноблок (10шт.)
2	Практические занятия	Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консульта-	Персональный компьютер (15 шт.),доска ученическая.

		ций, текущего контроля	
3	Лабораторные работы	Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля	Персональный компьютер (15 шт.),доска ученическая.
4	Самостоятельная работа обучающегося	Компьютерный класс с выходом в Интернет	моноблок (30 шт.), проектор, экран
5	Промежуточная аттестация	Учебная аудитория для проведения групповых и индивидуальных консультаций, промежуточной аттестации	персональный компьютер (15 шт.), доска ученическая

8. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья и инвалидов

Лица с ограниченными возможностями здоровья (ОВЗ) и инвалиды имеют возможность беспрепятственно перемещаться из одного учебно-лабораторного корпуса в другой, подняться на все этажи учебно-лабораторных корпусов, заниматься в учебных и иных помещениях с учетом особенностей психофизического развития и состояния здоровья.

Для обучения лиц с ОВЗ и инвалидов, имеющих нарушения опорно-

двигательного аппарата, обеспечены условия беспрепятственного доступа во все учебные помещения. Информация о специальных условиях, созданных для обучающихся с ОВЗ и инвалидов, размещена на сайте университета www//kgeu.ru. Имеется возможность оказания технической помощи ассистентом, а также услуг сурдопереводчиков и тифлосурдопереводчиков.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушенным слухом справочного, учебного материала по дисциплине обеспечиваются следующие условия:

- для лучшей ориентации в аудитории, применяются сигналы оповещения о начале и конце занятия (слово «звонок» пишется на доске);
- внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);
- разговаривая с обучающимся, педагогический работник смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих обучающихся проводится путем:

- использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;
- регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;
- обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой по выбранному направле-нию подготовки, обеспечиваются следующие условия:

- ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;
- педагогический работник, его собеседник (при необходимости), присутствующие на занятии, представляются обучающимся, при этом каждый раз называется тот, к кому педагогический работник обращается;
- действия, жесты, перемещения педагогического работника коротко и ясно комментируются;
- печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается;
- обеспечивается необходимый уровень освещенности помещений;
- предоставляется возможность использовать компьютеры во время занятий и право записи объяснений на диктофон (по желанию обучающихся).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ и инвалидов определяется педагогическим работником в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ, инвалиду с учетом их индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.

Лист регистрации изменений

Дополнения и изменения в рабочей программе дисциплины на 20___ /20____ учебный год

В программу вносятся следующие изменения:

1. _____

2. _____

3. _____

Указываются номера страниц, на которых внесены изменения,
и кратко дается характеристика этих изменений

Программа одобрена на заседании кафедры –разработчика «__» _____ 20_г., протокол № _____

Зав. кафедрой _____ Смирнов Ю.Н.

Программа одобрена методическим советом института _____
«___»_____ 20____г., протокол № _____

Зам. директора по УМР_____ /_____/

Подпись, дата

Согласовано:

Руководитель ОПОП _____ /_____/

Подпись, дата

Приложение к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

КГЭУ **«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «КГЭУ»)**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
по дисциплине

Защита информации

Направление подготовки 01.03.04 Прикладная математика

Квалификация бакалавр

г. Казань, 2020

Оценочные материалы по дисциплине «Защита информации» - комплект контрольно-измерительных материалов, предназначенных для оценивания результатов обучения на соответствие индикаторам достижения компетенции(й):

ОПК-2. Способен обоснованно выбирать, дорабатывать и применять для решения исследовательских и проектных задач математические методы и модели, осуществлять проверку адекватности моделей, анализировать результаты, оценивать надежность и качество функционирования систем	ОПК-2.2. Осуществляет проверку адекватности моделей, анализирует результаты, оценивает надежность и качество функционирования систем
ОПК-4. Способен разрабатывать и использовать современные методы и программные средства информационно-коммуникационных технологий	ОПК-4.1. Использует современные методы проектирования, разработки программных средств. ОПК-4.2. Реализовывает алгоритмы решения задач профессиональной деятельности на языке программирования ОПК-4.3. Применяет современные методы и программные средства информационно-коммуникационных технологий

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля успеваемости, проводимого по балльно-рейтинговой системе (БРС), и промежуточной аттестации.

Текущий контроль успеваемости обеспечивает оценивание процесса обучения по дисциплине. При текущем контроле успеваемости используются следующие оценочные средства: лекции, лабораторные и практические занятия, тестирование, контрольная работа, промежуточная аттестация.

Промежуточная аттестация имеет целью определить уровень достижения запланированных результатов обучения по дисциплине за 6 семестр. Форма промежуточной аттестации экзамен.

Оценочные материалы включают задания для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, разработанные в соответствии с рабочей программой дисциплины.

1.Технологическая карта

Семестр 6

Номер раздела/ темы дисциплины	Вид СРС	Наименование оценочного средства	Код индикатора достижения компетенций	Уровень освоения дисциплины, баллы			
				неудов-но	удов-но	хорошо	отлично
				не зачте-	зачтено		
				низкий	ниже среднего	средний	высокий
Текущий контроль успеваемости							
1	Подготовка к лекционному занятию и формам контроля	ТЕСТ	ОПК-4	менее 0	0 - 1	1 - 2	2 - 2

2	Подготовка к лекционному занятию и формам тестирования	ТЕСТ	ОПК-4, ОПК-4, ОПК-4	менее 0	0 - 1	1 - 2	2 - 2
2	Подготовка к лекционному занятию и формам тестирования	ТЕСТ	ОПК-4, ОПК-4, ОПК-4	менее 0	0 - 1	1 - 2	2 - 2
2	Подготовка к лекционному занятию и формам контроля	ТЕСТ	ОПК-4	менее 0	0 - 1	1 - 2	2 - 2
2	Подготовка к практическому занятию и контрольной работе	КР	ОПК-4, ОПК-4, ОПК-4	менее 0	1 - 2	3 - 4	4 - 5
2	Подготовка к практическому занятию и контрольной работе	КР	ОПК-4, ОПК-4, ОПК-4	менее 0	1 - 2	3 - 4	4 - 5
2	Подготовка к практическому занятию и контрольной работе	КР	ОПК-4, ОПК-4, ОПК-4	менее 0	1 - 2	3 - 4	4 - 5
2	Подготовка к лабораторной работе и формам отчетности	ТЕСТ	ОПК-4, ОПК-4	менее 0	0 - 1	2 - 2	3 - 3
2	Подготовка к лабораторному занятию и формам контроля	ТЕСТ	ОПК-4, ОПК-4, ОПК-4	менее 0	0 - 1	2 - 2	3 - 3
2	Подготовка к лабораторному занятию и формам контроля	ТЕСТ	ОПК-4, ОПК-4	менее 0	0 - 1	2 - 2	3 - 3
2	Подготовка к лабораторному занятию и формам контроля	ТЕСТ	ОПК-4, ОПК-4	менее 0	0 - 1	2 - 2	3 - 3
2	Подготовка к лабораторному занятию и формам контроля	ТЕСТ	ОПК-4, ОПК-4	менее 0	0 - 1	2 - 2	3 - 3

2	Подготовка к лабораторному занятию и формам контроля	ТЕСТ	ОПК-4, ОПК-4	менее 0	0 - 1	2 - 2	3 - 3
2	Подготовка к лабораторному занятию и формам контроля	ТЕСТ	ОПК-4, ОПК-4	менее 0	0 - 1	2 - 2	3 - 3
2	Подготовка к лабораторному занятию и формам тестирования	ТЕСТ	ОПК-4, ОПК-4	менее 0	0 - 1	2 - 2	3 - 3
3	Подготовка к лекционному занятию и формам контроля	ТЕСТ	ОПК-4, ОПК-4	менее 0	0 - 1	1 - 2	2 - 2
4	Подготовка к лекционному занятию и формам контроля	ТЕСТ	ОПК-4, ОПК-4	менее 0	0 - 1	1 - 2	2 - 2
5	Подготовка к лекции и формам тестирования	ТЕСТ	ОПК-4	менее 0	0 - 1	1 - 2	2 - 3
6	Подготовка к лекционному занятию и формам тестирования	ТЕСТ	ОПК-4, ОПК-4	менее 0	0 - 1	1 - 2	2 - 3
7	Подготовка к лекционному занятию и формам контроля	ТЕСТ	ОПК-4, ОПК-4, ОПК-4	менее 0	0 - 1	2 - 2	3 - 3
			Всего баллов	0	3-23	35-46	55-60
Промежуточная аттестация							
Подготовка к экзамену	Задания экзамену						
			Итого баллов	**0 - 54**	**55-69**	**70-84**	**85-100**

Наименование оценочного средства	Краткая характеристика оценочного средства	Оценочные материалы
Лекции (КОНСПЕКТ)	Краткое письменное описание материала, преподнесенного на лекционном занятии	Конспект лекций
Лабораторные и практические занятия (ОТЧЕТ)	Выполнение лабораторной или практической работы и оформление результатов выполненных действий	Отчет по лабораторным и практическим занятиям

Тестирование (ТЕСТ)	испытуемому дается инструкция, как работать с тестом. После этого выдаются тестовые задания. Они могут или читаться вслух перед группой испытуемых, или раздаваться испытуемым в виде брошюры, или, при компьютерном тестировании, выдаваться на экран дисплея. Испытуемые дают ответы в соответствии с инструкцией - или на специальных бланках для ответов, или на дисплее компьютера	Набор тестовых заданий
Контрольная работа (КР)	Решение стандартных задач	Набор задач для контрольных работ
Промежуточная аттестация (Э)	Письменная работа - ответ на оценочные задания, представленные в билете	Экзаменационные билеты

3. Оценочные материалы текущего контроля успеваемости обучающихся

Наименование оценочного средства	
Представление и содержание оценочных материалов	***Фонд тестовых заданий*** 1. Открытый трафик – это: а) поток пакетов, незашифрованных на сетевом и прикладном уровне; б) поток пакетов, незашифрованных на сетевом уровне, причем данные могут быть зашифрованы на прикладном уровне; в) поток пакетов, незашифрованных на прикладной уровне, причем данные могут быть зашифрованы на сетевом уровне; г) поток пакетов от пакетов от компьютеров, не входящих в сеть ViPNet. 2. Меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе работы с информацией для обеспечения заданного уровня ее безопасности, относятся к: а) гражданско-правовым методам обеспечения информационной безопасности; б) внутриобъектовым методам обеспечения информационной безопасности; в) организационным методам обеспечения информационной безопасности; г) правовым методам обеспечения информационной безопасности. 3. Путь несанкционированного распространения носителя информации от источника к злоумышленнику называется: а) несанкционированным доступом к информации; б) каналом утечки информации; в) утечкой информации; г) несанкционированным распространением информации. 4. Злонамеренный код обладает следующими отличительными чертами: не требует программы-носителя, вызывает распространение своих копий и их выполнение (для активизации вируса требуется запуск зараженной программы). Назовите тип этого злонамеренного кода. а) макровирус; б) троянский конь; в) червь; г) файловый вирус. 5. На какие виды по физической природе подразделяются технические каналы утечки информации? а) оптические; б) видимые; в) вещественные; г) акустические; д) разведывательные; е) инфракрасные;

ж) радиоэлектронные.

6. К косвенным каналам утечки информации относятся:
а) кража или утеря носителей информации;
б) копирование защищаемой информации из информационной системы;
в) исследование не уничтоженного мусора;
г) перехват электромагнитных излучений;
д) инсайдерские действия.

7. Какие задачи информационной безопасности решаются на организационном уровне?
а) внедрение системы безопасности;
б) разработка документации;
в) обучение персонала;
г) сертификация средств защиты информации;
д) ограничение доступа на объект;
е) внедрение системы контроля и управления доступом.

8. К источникам случайных воздействий можно отнести:
а) неисправные технические средства сбора, обработки, передачи и хранения информации
б) ошибки персонала;
в) стихийные силы;
г) программы, содержащие вирусы;
д) действие создаваемых злоумышленником полей и сигналов.

9. По аспекту информационной безопасности угрозы классифицируются на:
а) угрозы нарушения конфиденциальности и секретности;
б) угрозы нарушения конфиденциальности, целостности, доступности;
в) угрозы нарушения конфиденциальности и криптографического скрытия;
г) угрозы нарушения криптографического скрытия.

10. Атака «man in the middle» является:
а) пассивной;
б) активной;
в) может быть как активной, так и пассивной;
г) нет верного ответа.

11. Межсетевой экран позволяет:
а) разделять сети друг от друга;
б) принимать решение о возможности дальнейшего направления трафика к пункту назначения;
в) проверять весь входящий и исходящий трафик;
г) все перечисленные выше варианты верны.

12. Что включают в себя технические мероприятия по защите информации?
а) поиск и уничтожение технических средств разведки;
б) кодирование информации или передаваемого сигнала;
в) подавление технических средств постановкой помехи;
г) применение детекторов лжи;
д) все вышеперечисленное.

13. Алгоритм RSA основан на:
а) задаче дискретного логарифмирования;
б) задаче факторизации числа;
в) задаче определения, является ли данное число простым;
г) нет верного ответа.

14. Алгоритм ГОСТ 28147:
а) имеет переменную длину ключа;
б) основан на сети Фейстеля;
в) разбивает блок на фиксированные 16-битные подблоки;
г) нет верного ответа.

15. Алгоритм Диффи-Хеллмана дает возможность:
а) безопасно обменяться общим секретом;

б) безопасно обменяться общим секретом при условии аутентификации сторон;
в) подписать сообщение;
г) нет верного ответа.

16. Алгоритм Диффи-Хеллмана основан на:
а) задаче дискретного логарифмирования;
б) задаче факторизации числа;
в) задаче определения, является ли данное число простым;
г) нет верного ответа.

17. Алгоритм симметричного шифрования называется блочным, если:
а) алгоритм основан на сети Фейстеля;
б) для шифрования исходный текст разбивается на блоки фиксированной длины;
в) в алгоритме используются S-box;
г) нет верного ответа.

18. Аутентификация – это:
а) невозможность несанкционированного доступа к данным;
б) подтверждение того, что информация получена из законного источника законным получателем;
в) невозможность несанкционированного просмотра и модификации информации;
г) нет верного ответа.

19. В DSS используется следующая хэш-функция:
а) MD5;
б) SHA-1;
в) SHA-2;
г) нет верного ответа.

20. В алгоритмах симметричного шифрования используются только следующие операции:
а) операции перестановки и сдвига;
б) S-box и побитовое исключающее или (XOR);
в) любые из перечисленных выше операций, а также многие другие;
г) нет верного ответа.

21. Информация, составляющая государственную тайну не может иметь гриф…
а) «особой важности»
б) «совершенно секретно»
в) «для служебного пользования»
г) «секретно»

22. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …
а) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
б) способна противостоять только внешним информационным угрозам
в) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды
г) способна противостоять только информационным угрозам, как внешним так и внутренним

23. Преднамеренная угроза безопасности информации
а) наводнение
б) повреждение кабеля, по которому идет передача, в связи с погодными условиями
в) ошибка разработчика
г) кража

24. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности
а) рекомендации X.800

б) Закону «Об информации, информационных технологиях и о защите информации»
в) Оранжевая книга

25. Основные угрозы доступности информации (можно выбрать 1 или несколько вариантов ответа):
а) отказ программного и аппаратно обеспечения
б) непреднамеренные ошибки пользователей
в) разрушение или повреждение помещений
г) злонамеренное изменение данных
д) перехват данных
е) хакерская атака

26. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на … (можно выбрать 1 или несколько вариантов ответа)
а) выявление нарушителей и привлечение их к ответственности
б) соблюдение норм международного права в сфере информационной безопасности
в) разработку методов и усовершенствование средств информационной безопасности
г) реализацию права на доступ к информации»
д) соблюдение конфиденциальности информации ограниченного доступа
е) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации

27. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)
а) МЭ работают только на сетевом уровне, а СОВ – еще и на физическом
б) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения
в) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты

28. К формам защиты информации не относится…
а) организационно-техническая
б) страховая
в) аналитическая
г) правовая

29. Утечка информации – это …
а) процесс раскрытия секретной информации
б) непреднамеренная утрата носителя информации
в) несанкционированный процесс переноса информации от источника к злоумышленнику
процесс уничтожения информации

30. Средства защиты объектов файловой системы основаны на…
а) определении прав пользователя на операции с файлами и каталогами
б) задании атрибутов файлов и каталогов, независящих от прав пользователей

31. Защита информации обеспечивается применением антивирусных средств
а) не всегда
б) нет
в) да

32. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …
а) перехвата или подмены данных на путях транспортировки
б) вмешательства в личную жизнь
в) поставки неприемлемого содержания
г) несанкционированного управления удаленным компьютером
д) внедрения агрессивного программного кода в рамках активных объектов Web-страниц

33. Суть компрометации информации
а) внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
б) внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден

либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений
в) несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

34. Сервисы безопасности:
а) экранирование
б) контроль целостности
в) обеспечение безопасного восстановления
г) кэширование записей
д) шифрование
е) регулирование конфликтов
ж) идентификация и аутентификация
з) инверсия паролей

35. Какие из перечисленных ниже алгоритмов не являются симметричными?
а) Подстановочные шифры (простой подстановочный шифр, или моноалфавитный шифр, однозвучный подстановочный шифр, полиграммный подстановочный шифр, полиалфавитный подстановочный шифр)
б) Перестановочные шифры (шифром перестановки, шифры с фигурами перестановки, использующие некоторую геометрическую фигуру, маршрутной перестановкой, поворотная решетка, шифр вертикальной перестановки)
в).Шифры гаммирования.
г).Блочного шифры: DES (Data Encription Standart), TripleDES (3DES), AES (Advanced Encryption Standart), он же RIJNDAEL, SERPENT, TWOFISH, RC6, MARS, ГОСТ 28147-89, Blowfish. (P.S больше вспомнить не могу, если что-то еще кто-то припомнит, то напишите..)
д) Поточные шифры.

36. Какую длину имеет секретный ключ в криптосистеме DES?

37. Блочные криптоалгоритмы в ходе своей производят преобразование…

38. Что такое раунд (round)?

39. Какая процедура распределения ключей не требует использования защищенного канала для передачи секретного ключа адресату?

40. Какая из систем с открытым ключом используется исключительно для генерации цифровой подписи?

41. Какие трудноразрешимые задачи используются для повышения стойкости алгоритма RSA?

42. Чему равен результат вычисления хэш-функции по алгоритму SHA-1?

43. Что такое двухфакторная аутентификация

44. Петр, находясь в сети организации, перевел свою сетевую карту в режим монитора для прослушивания пакетов. Какой вид атаки осуществляет Петр?
а) Отказ в обслуживании
б) Фишинг
в) Снифинг
г) Активный спуфинг
д) Пассивный спуфинг

45. Какой сервис не реализовывает VPN-тунель?
а) Обеспечение отказоустойчивости канала связи
б) Обеспечение конфиденциальности информации
в) Обеспечение целостности информации
г) Обеспечение аутентификации пользователей
д) Предотвращение отказа от авторства

46. Что из перечисленного не используется в биометрической аутентификации?
а) Рисунок папиллярного узора
б) Радужная оболочка глаза
в) PIN-код
г) Клавиатурный почерк
д) Пластиковая карта с магнитной полосой

47. Что лежит в основе мандатных политик безопасности?
а) Таблицы доступа
б) Роли
в) Метки секретности
г) Нет верного ответа
д) Матрицы доступа

48. Какой из перечисленных паролей является наиболее надежным для пользователя admin?
а) pa$$word
б) P@ssw0rd
в) password
г) passw0rd
д) Password

49. Каким термином называется способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ?
а) Линейное шифрование
б) Одноуровневое шифрование
в) Простое шифрование
г) Симметричное шифрование
д) "One-key" шифрование

50. Какой метод обмена ключами из перечисленных позволяет сторонам обменяться секретными ключами, не раскрывая их через незащищенную среду?
а) Diffie-Hellman
б) Ceasar
в) Merkle-Hellman Knapsack
г) MD5
д) Twofish

51. Какой из следующих параметров веб-браузера необходимо использовать для настройки того, каким образом браузер получает информацию и загружает содержимое веб-сайтов?
а) Cookies
б) Ничего из вышеперечисленного
в) Прокси-сервер
г) Сертификат
д) Безопасность

52. Вы получили по электронной почте письмо с вложением "От отдела IT". В тексте письма говорится, что ваш компьютер был заражен вирусом. Поэтому вам необходимо открыть вложение и следовать инструкциям, чтобы избавиться от вируса. Что необходимо сделать? (Выберите все подходящие варианты).
а) Связаться с IT-отделом для уточнения информации о полученном письме.
б) Откройте вложение, чтобы увидеть его содержание.
в) Следуйте инструкциям, чтобы удалить вирус.
г) Написать письмо отправителю с просьбой удалить из списка рассылки.
д) Удалить сообщение из неизвестного источника

53. На каком устройстве обычно используют технологию VLAN с целью разделения сети на сегменты?
а) Брандмауер
б) Точка доступа

в) Повторитель
г) Маршрутизатор
д) Коммутатор

54. Процесс регистрации пользователя в системе состоит из трёх взаимосвязанных, последовательно выполняемых процедур: ... (укажите их с учетом правильного порядка)

55. Какая из перечисленных технологий не относится к технологиям вероятностного анализа, применяемым в антивирусах?
а) Анализ контрольных сумм
б) Сигнатурный анализ
в) Нет верного ответа
г) Поведенческий анализ
д) Эвристический анализ

56. Определите название атаки, механизм которой обозначен на рисунке?

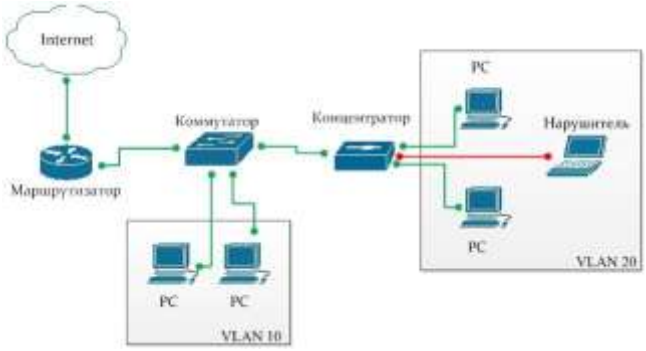
а) Buffer Overflow
б) Spoofing
в) DDoS
г) IP-spoofing
д) Man-in-the-Middle

57. Для чего не используются сканеры уязвимостей при аудите?
а) Для определения необходимых обновлений
б) Для выявления информации о небезопасном коде в приложениях
в) Для выявления открытых портов и сервисов, которые могут быть использованы хакерами для возможных атак
г) Для определения неверных (с точки зрения информационной безопасности) настроек системы
д) Для определения максимальной пропускной способности канала

58. Попытка реализации угрозы информационной безопасности - это... (выберите понятие в терминах информационной безопасности)
а) Уязвимость
б) Атака
в) Нападение
г) Штурм
д) Контратака

59. На каком устройстве обычно используют технологию VLAN с целью разделения сети на сегменты?
а) Брандмауер
б) Точка доступа
в) Повторитель
г) Маршрутизатор
д) Коммутатор

60. Какой трафик будет прослушивать нарушитель, если запустит пассивный снифинг пакетов?



а) Весь трафик сети
б) Весь трафик, идущий через маршрутизатор
в) Весь трафик VLAN 20
г) Только свой собственный
д) Весь трафик VLAN 10 и VLAN 20

61. Алгоритм RC6 обладает следующими свойствами
а) имеет самое быстрое установление ключа;
б) имеет самое быстрое шифрование/дешифрование;
в) имеет возможность вычисления подключей на лету;
г) шифрование и дешифрование имеют идентичные функции.

62. Алгоритм RSA может использоваться для
а) подписывания;
б) шифрования;
в)обмена общим секретом;
г) все выше перечисленное.

63. Алгоритм Serpent обладает следующими свойствами
а) имеет самое быстрое установление ключа;
б) имеет самое быстрое шифрование/дешифрование;
в) имеет возможность вычисления подключей на лету;
г) шифрование и дешифрование имеют идентичные функции.

64. В DSS используется следующая хэш-функция
а) MD5;
б) SHA-1;
в) SHA-2;
г) нет верного ответа.

65. В алгоритме RC6 используются следующие операции
а) XOR слов;
б) циклический сдвиг на несколько битов;
в) S-box;
г) нет верного ответа.

66. Выберите правильное высказывание
а) подпись с использованием эллиптических кривых является детерминированной;
б) подпись с использованием эллиптических кривых является рандомизированной;
в) уравнения на эллиптических кривых нельзя использовать для создания цифровых подписей;
г) нет верного высказывания.

67. Выберите правильное утверждение

а) в основе алгоритма RC6 лежит традиционная сеть Фейштеля;
б) в основе алгоритма RC6 не лежит сеть Фейштеля;
в) в основе алгоритма RC6 лежит сеть Фейштеля смешанного типа с 4 ветвями;
г) нет верного утверждения.

68. Выберите правильное утверждение

а) должно быть вычислительно невозможно подделать цифровую подпись как созданием нового сообщения для существующей цифровой подписи, так и созданием ложной цифровой подписи для некоторого сообщения;
б) цифровая подпись должна быть достаточно компактной и не занимать много памяти;
в) подпись обязательно должна быть рандомизированной;
г) нет верного утверждения.

69. Выберите правильное утверждение:

а) в криптографии с использованием эллиптических кривых все значения вычисляются по модулю n, где n – произведение двух простых чисел;
б) в криптографии с использованием эллиптических кривых все значения вычисляются по модулю простого числа p;
в) в криптографии с использованием эллиптических кривых все значения вычисляются по модулю произвольного числа p
г) нет верного утверждения.

70. Выберите правильное утверждение:

а) в любом протоколе аутентификации ключ сессии всегда создается третьей доверенной стороной;
б) в любом протоколе аутентификации ключ сессии всегда создается участником A;
в) существуют различные протоколы, в одних ключ сессии создается KDC, в других - одним из участников A или B;
г) нет верного утверждения.

71. Выберите правильное утверждение:

а) в протоколах аутентификации с использованием шифрования с открытым ключом участники должны знать открытый ключ AS или KDC;
б) в протоколах аутентификации с использованием шифрования с открытым ключом участники должны знать открытые ключи друг друга;
в) в протоколах аутентификации с использованием шифрования с открытым ключом участники должны знать как открытый ключ AS или KDC, так и открытые ключи друг друга;
г) нет верного утверждения.

72. Выберите правильное утверждение:

а) в основе алгоритма DES лежит сеть Фейштеля;
б) в алгоритме DES используются S-boxes;
в) в алгоритме DES используется умножение по модулю 216 + 1;
г) нет верного утверждения.

73. Выберите правильное утверждение:

а) подпись должна быть битовым образцом, который зависит от подписываемого сообщения;
б) подпись должна использовать некоторую уникальную информацию отправителя для предотвращения подделки или отказа;
в) подпись должна обеспечивать невозможность просмотра сообщения;
г) нет верного утверждения.

74. Выберите правильные утверждения:

а) должно быть относительно легко создавать цифровую подпись;
б) должно быть относительно трудно создавать цифровую подпись;
в) должно быть относительно легко проверять цифровую подпись;
г) нет верного утверждения.

75. Выберите правильное утверждение:

а) мастер-ключ должен быть более защищенным, чем ключ сессии+++++;
б) ключ сессии должен быть более защищенным, чем мастер-ключ;
в) мастер-ключ и ключ сессии должны иметь одинаковую степень защиты;
г) нет верного утверждения.

76. Выходом хэш-функции является:
а) сообщение той же длины, что и входное сообщение;
б) сообщение фиксированной длины;
в) сообщение меньшей длины;
г) нет верного ответа.

77. Длина блоков, на которые делится сообщение в хэш-функции SHA-1, равна:
а) 160 бит;
б) 512 бит;
в) 1024 бит;
г) нет верного ответа.

78. Длина блоков, на которые делится сообщение в хэш-функции SHA-512, равна:
а) 512 бит;
б) 1024 бит;
в) 1024 байт;
г) нет верного ответа.

79. Длина блоков, на которые делится сообщение в хэш-функции ГОСТ 3411, равна:
а) 256 бит;
б) 512 бит;
в) 1024 бит;
г) нет верного ответа.

80. Длина ключа в алгоритме ГОСТ 28147:
а) 56 бит;
б) 128 бит;
в) 256 бит;
г) 448 бит.

81. Длина хэш-кода, создаваемого хэш-функцией SHA-1, равна:
а) 128 бит;
б) 160 бит;
в) 512 бит;
г) 1024 бит.

82. Дополнительными параметрами хэш-функции ГОСТ 3411 являются:
а) стартовый вектор хэширования;
б) ключи для алгоритма симметричного шифрования ГОСТ 28147;
г) начальное значение хэш-кода;
г) нет верного ответа.

83. Каждый блок сообщения в хэш-функции MD5 обрабатывается:
а) 4 раза;
б) 16 раз;
в) 64 раза;
г) 128 раз.

84. Из двух компонент (r, s) состоит подпись, полученная с использованием алгоритма:
а) RSA;
б) DSS;
в) ГОСТ 3410;
г) нет верного ответа.

85. Зависимость между ключами шифрования и дешифрования в алгоритмах симметричного шифрования должна быть следующей:
а) ключи шифрования и дешифрования должны в точности совпадать;
б) ключ дешифрования должен легко получаться из ключа шифрования;
в) между ключами шифрования и дешифрования не должно быть никакой зависимости;

г) нет верного ответа.

86. Криптографическая система называется симметричной, потому что:
а) шифруемый блок разбивается на подблоки одинаковой длины;
б) для шифрования и дешифрования используются одинаковые или легко выводимые один из другого ключи;
г) алгоритм использует циклически повторяющиеся операции, называемые раундами;
г) нет верного ответа.

87. Криптография с использованием эллиптических кривых дает преимущества по сравнению с другими алгоритмами, потому что:
а) принципиально не может быть взломана;
б) обеспечивает эквивалентную защиту при меньшей длине ключа;
г) проще в реализации;
г) нет верного ответа.

88. Нулевым элементом эллиптической кривой считается точка O, которая:
а) имеет координаты (0, 0);
б) является бесконечно удаленной точкой, в которой сходятся все вертикальные прямые;
в) имеет координаты (0, 1) или (1, 0);
г) нет верного ответа.

89. Побитовый XOR блоков нельзя считать криптографической хэш-функцией, потому что:
а) противник может легко подобрать другое сообщение, имеющее тот же хэш-код;
б) побитовый XOR плохо защищает от случайного сбоя;
в) побитовый XOR требует сложных вычислений;
г) нет верного ответа.

90. Под DoS-атакой понимается:
а) модификация передаваемого сообщения;
б) повторное использование переданного ранее сообщения;
в) невозможность получения сервиса законным пользователем;
г) нет верного ответа.

91. Под replay-атакой понимается:
а) модификация передаваемого сообщения;
б) повторное использование переданного ранее сообщения;
в) невозможность получения сервиса законным пользователем;
г) нет верного ответа.

92. Подпись называется детерминированной, если:
а) для одного и того же сообщения с использованием разных закрытых ключей при каждом подписывании создается одна и та же подпись;
б) для разных сообщений с использованием одного и того закрытого ключа при каждом подписывании создается одна и та же подпись;
в) для одного и того же сообщения с использованием одного и того же закрытого ключа при каждом подписывании создается одна и та же подпись;
г) нет верного ответа.

93. При использовании криптографии на эллиптических кривых в качестве аналога алгоритма Диффи-Хеллмана в уравнении PA = nA×G:
а) открытым ключом участника A является PA, закрытым ключом участника A является nA;
б) открытым ключом участника A является nA, закрытым ключом участника A является PA;
в) открытым ключом участника A является PA, закрытым ключом участника A является G;
г) нет верного ответа.

94. При односторонней аутентификации ключ сессии может шифроваться:
а) открытым ключом получателя;
б) закрытым ключом отправителя;
в) мастер-ключом для симметричного шифрования, разделяемым отправителем и KDC;
г) нет верного ответа.

95. Причина использования двух ключей в тройном DES состоит в том, что:
а) в этом случае отсутствует атака «встреча посередине»;
б) стойкость алгоритма не повышается при использовании трех ключей вместо двух;
в) при использовании трех ключей общая длина ключа равна 168 битам, что может потребовать существенно больших вычислений при его распределении;
г) нет верного ответа.

96. Сервис, который гарантирует, что информация получена из законного источника и получателем является тот, кто нужно, называется:
а) аутентификацией;
б) целостностью;
в) конфиденциальностью;
г) нет верного ответа.

97. Сервис, который обеспечивает невозможность несанкционированного просмотра данных, называется:
а) аутентификацией;
б) целостностью;
в) конфиденциальностью;
г) нет верного ответа.

98. Хэш-функции предназначены для:
а) сжатия сообщения;
б) получения «отпечатков пальцев» сообщения;
в) шифрования сообщения;
г) нет верного ответа.

99. Хэш-функция должна обладать следующими свойствами:
а) хэш-функция должна применяться к блоку данных любой длины;
б) хэш-функция должна создавать выход произвольной длины;
в) для любого данного значения хэш-кода h вычислительно невозможно найти M такое, что H (M) = h;
г) нет верного ответа.

100. Шифрование/дешифрование с использованием эллиптических кривых выполняется следующим образом:
а) участник А выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение Cm, являющееся точкой на эллиптической кривой Cm = {k ×G, Pm + k ×PB};
б) участник А выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение Cm, являющееся точкой на эллиптической кривой Cm = { Pm + k ×PB};
в) участник А выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение Cm, являющееся точкой на эллиптической кривой Cm = {k ×G};
г) нет верного ответа.

Контрольная работа

1. Персоналу в случае возникновения нештатной ситуации необходимо иметь:
2. Повторное использование переданного ранее сообщения называется …
3. Политика безопасности – это …
4. Политика информационной безопасности в общем случае является руководящим документом для …
5. Политика информационной безопасности, прежде всего, необходима для …
6. Пользователь осуществляет удаленный доступ к информации на сервере. Пусть условный уровень защищенности информации на сервере - 24 единицы; условный уровень защищенности рабочего места пользователя - 10 единиц. Оцените условный уровень защищенности удаленного доступа пользователя к информации на сервере.
7. Пороговый метод выявления атак хорош тем, что …
8. После идентификации угрозы необходимо оценить …
9. Правило, которым необходимо пользоваться при формировании матрицы доступа …
10. Предположим, информационная система компании надежно защищена ком-

плексом средств информационной защиты (межсетевые экраны, антивирусы, системы защиты от НСД, системы обнаружения атак и т.д.). Как на существующий уровень рисков влияет реализация требований политики безопасности?

11. При внесении изменений в систему требуется …

12. При выведении из эксплуатации устройств хранения информации необходимо …

13. При использовании версии сервера аутентификации Kerberos, описанной в курсе, шифрование …

14. При односторонней аутентификации осуществляется аутентификация …

15. Применение метода разделения обязанностей необходимо для …

16. Принцип усиления самого слабого звена можно переформулировать как принцип …

17. Протоколирование и аудит могут использоваться для …

18. Процедура входа в систему (login) не должна выдавать …

19. Пункт, в котором перечислено наибольшее число событий, которые рекомендуется фиксировать в журнале данных о доступе …

20. Пункт, точно соответствующий рекомендованным стандартом ограничениям на использование системных утилит…

21. Согласно "Оранжевой книге", политика безопасности включает в себя следующие элементы …

22. Согласно рекомендациям X.800, аутентификация не может быть реализована на …

23. Согласно стандарту X.700, в число функций управления конфигурацией входят …

24. Специальные соглашения, необходимые при приеме персонала на работу о(об) …

25. Список открытых портов, наиболее свойственный для системы Windows 9x …

26. Стандарт, широко признанный как стандарт лучшей практики защиты …

27. Тип межсетевого экрана, который может контролировать выполнение команды PUT сервиса FTP и фильтровать теги HTTP …

28. Требование односторонности хэш-функции состоит в следующем …

29. Туннелирование может применяться для достижения следующих целей …

30. Формируя привилегии индивидуальных пользователей, выдаваемым по мере необходимости, следует пользоваться принципом наделения пользователей …

31. Функция, используемая в криптосистеме с открытым ключом, должна обладать следующими свойствами …

32. Цифровой сертификат содержит ЭЦП …

33. Чтобы узнать открытые порты на своем компьютере, необходимо выполнить команду …

34. Алгоритм симметричного шифрования называется блочным, если…

35. Международный стандарт управления информационной безопасностью ISO 17799 предъявляет …

Критерии оценки и шкала оценивания в баллах

Шкала и критерии оценивания уровня освоения дисциплинарных частей компетенций, приобретаемых при выполнении практических, лабораторных, расчетно-графических работ и индивидуальных заданий

Балл за		**Критерии оценивания уровня освоения дисциплинарных компетенций после изучения учебного материала**
знания	**умения**	
5	5	*Задание по работе выполнено в полном объеме. Студент точно ответил на контрольные вопросы, свободно ориентируется в предложенном решении, может его модифицировать при изменении условия задачи. Отчет выполнен аккуратно и в соответствии с предъявляемыми требованиями.*
4	4	*Задание по работе выполнено в полном объеме. Студент ответил на теоретические вопросы, испытывая небольшие затруднения. Качество оформления отчета к работе не полностью соответствует требованиям*
3	3	*Студент правильно выполнил задание к работе. Составил отчет в установленной форме, представил решения большинства заданий, предусмот-*

			ренных в работе. Студент не может полностью объяснить полученные результаты.
	2	2	*Студент не выполнил все задания работы и не может объяснить полученные результаты.*

Критерии и шкала оценивания уровня ***владений*** освоения дисциплинарных частей компетенций при выполнении лабораторных работ

Балл за владения	Критерии оценивания уровня приобретенных владений
5	*Студент правильно выполнил задание. Показал отличные владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы на защите.*
4	*Студент выполнил задание с небольшими неточностями. Показал хорошие владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов на защите.*
3	*Студент выполнил задание с существенными неточностями. Показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено много неточностей.*
2	*При выполнении задания студент продемонстрировал недостаточный уровень владения умениями и навыками при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено множество неточностей.*

4. Оценочные материалы промежуточной аттестации

Наименование оценочного средства	
Представление и содержание оценочных материалов	1. Сформулируйте понятие информационной безопасности ИС. 2. Объясните понятия целостности, конфиденциальности и доступности информации. 3. Укажите отличия санкционированного доступа к информации от несанкционированного. 4. Перечислите основные признаки классификации возможных угроз безопасности ИС 5. Дайте краткую характеристику угрозы безопасности, обозначаемой термином «троянский конь». 6. Дайте краткую характеристику угроз безопасности, обозначаемых терминами «вирус» и «червь». 7. Назовите и охарактеризуйте наиболее распространенные виды сетевых. 8. Опишите атаку «человек-в-середине». Какие средства позволяют эффективно бороться с атаками такого типа? 9. Опишите атаку типа «отказ в обслуживании» и распределенную атаку «отказ в обслуживании». 10. Опишите особенности фишинга и фарминга. Укажите меры противодействия этим атакам. 11. Каковы источники нарушений безопасности проводных корпоративных сетей? 12. Назовите основные уязвимости и угрозы беспроводных сетей. 13. Объясните понятие «политика безопасности организации». 14. Какие разделы должна содержать документально оформленная политика

	безопасности? 15. Какие проблемы решает верхний уровень политики безопасности? 16. Какие задачи решает средний уровень политики безопасности? 17. Каковы особенности нижнего уровня политики безопасности? 18. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности. 19. Опишите структуру политики безопасности организации. 20. Что представляют собой специализированные политики безопасности? 21. Приведите несколько примеров специализированных политик безопасности с описанием их особенностей. 22. Что представляют собой процедуры безопасности? 23. Приведите несколько примеров процедур безопасности с описанием их особенностей. 24. Перечислите основные этапы разработки политики безопасности организации. 25. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителен и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов. 26. Назовите основные международные стандарты информационной безопасности. 27. Дайте краткую характеристику международного стандарта IS0/IEC 17799:2000 (BS 7799-1:2000). 28. Каковы основные особенности германского стандарта BSI «Руководство но защите информационных технологий для базового уровня защищенности»? 29. Опишите содержание и укажите значение международного стандарта ISO 15408 «Общие критерии безопасности информационных технологий». 30. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику. 31. Назовите стандарты информационной безопасности для Интернета. 32. Каковы назначение и особенности функционирования протокола SET? 33. Каковы назначение и функциональность протоколов SSL и IPSec? В чем эти протоколы существенно различаются? 34. Каковы назначение и функциональность инфраструктуры управления открытыми ключами PKI? 35. Перечислите российские стандарты безопасности информационных технологий. 36. Каково назначение стандарта ГОСТ Р ИСО/МЭК 15408? Назовите и охарактеризуйте три основных части этого стандарта. 37. Что такое криптография? 38. Дайте определения следующих понятий: криптограмма, криптоалгоритм, криптосистема 39. В чем состоит коренное различие симметричных и асимметричных криптосистем? 40. Охарактеризуйте четыре основных режима работы блочного алгоритма. 41. Расскажите о способах комбинирования блочных алгоритмов для получения алгоритмов с более длинным ключом, сравните их между собой. 42. Каковы основные характеристики и режимы работы отечественного стандарта шифрования данных? 43. Сформулируйте концепцию криптосистемы с открытым ключом. 44. Дайте определение однонаправленной функции. Приведите примеры однонаправленных функций 45. Каковы особенности однонаправленных функций с секретом? 45. На чем основывается надежность криптоалгоритма шифрования RSA? 46. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности цифрового документа. 47. Опишите отечественный стандарт цифровой подписи, укажите его пре-

	имущество по сравнению с алгоритмом цифровой подписи DSA. 48. Каково назначение хэш-функция и каким требованиям должна удовлетворять качественная хэш-функция? 49. Каким образом комбинированный метод шифрования позволяет сочетать достоинства ассиметричных и симметричных криптосистем? Опишите протокол реализации комбинированного метода шифрования. 50. Опишите работу алгоритма Диффи-Хэллмана. Укажите достоинства этого алгоритма. 51. Каково назначение инфраструктуры открытых ключей PKI? Опишите функционирование инфраструктуры PKI. 52. Дайте определение понятий «идентификация», «аутентификация», «авторизация», «администрирование». 53. Что понимают под решением задач AAA? 54. Какие задачи решает подсистема управления идентификацией и доступом IAM? 55. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности? 56. Перечислите основные атаки на протоколы аутентификации. 57. Опишите метод аутентификации на основе многоразовых паролей. Каковы его недостатки? 58. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки? 59. Сформулируйте принцип строгой аутентификации. Опишите типы процедур строгой аутентификации. 60. Объясните назначение PIN-кода и особенности его использования. 61. Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используют для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации? 62. Опишите функциональность и характеристики смарт-карт и USB-токенов. 63. Опишите методы биометрической аутентификации пользователя. 64.Что означают термины «коэффициент ошибочных отказов» и «коэффициент ошибочных подтверждений»? 65.Объясните принцип управления доступом но схеме однократного входа с авторизацией SSO. 66. Что такое вредоносная программа? Охарактеризуйте основные типы вредоносных программ. 67. Укажите существенные отличия компьютерных вирусов от сетевых червей. Опишете основные особенности троянских программ. 68. Опишите два основных подхода к обнаружению вредоносных программ. 69. Как выполняется сигнатурный анализ? Каковы его достоинства и недостатки? 70. Что представляют собой проактивные методы обнаружения? Дайте характеристики двух наиболее популярных подходов. 71. Опишите принцип действия, достоинства и недостатки эвристических анализаторов. 72. Опишите принцип действия, достоинства и недостатки поведенческих блокираторов. 73. Назовите и опишите дополнительные модули антивирусных средств. 74. Каковы дополнительные меры и средства защиты от вредоносных программ, расширяющие возможности антивирусных программ? 75. Опишите меры и средства зашиты от спама. 76. Каковы особенности реализации подсистемы защиты корпоративной информации от вредоносных программ и вирусов? 77. Каковы возможности серии продуктов Kaspersky Open Space Security для зашиты

<table>
<tr><td></td><td>корпоративных сетей от современных интернет-угроз?</td></tr>
<tr><td>Критерии оценки и шкала оценивания в баллах</td><td>
Шкала оценивания уровня знаний
<table>
<tr><th>Балл</th><th>Критерии оценивания уровня усвоенных знаний</th></tr>
<tr><td>5</td><td>Студент правильно ответил на теоретический вопрос билета. Показал отличные знания в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы.</td></tr>
<tr><td>4</td><td>Студент ответил на теоретический вопрос билета с небольшими неточностями. Показал хорошие знания в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов.</td></tr>
<tr><td>3</td><td>Студент ответил на теоретический вопрос билета с существенными неточностями. Показал удовлетворительные знания в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей.</td></tr>
<tr><td>2</td><td>При ответе на теоретический вопрос билета студент продемонстрировал недостаточный уровень знаний. При ответах на дополнительные вопросы было допущено множество неправильных ответов.</td></tr>
</table>
Шкала оценивания уровня умений
<table>
<tr><th>Балл</th><th>Критерии оценивания уровня усвоенных знаний</th></tr>
<tr><td>5</td><td>Студент правильно выполнил практическое задание билета. Показал отличные умения в рамках освоенного учебного материала. Ответил на все дополнительные вопросы.</td></tr>
<tr><td>4</td><td>Студент выполнил практическое задание билета с небольшими неточностями. Показал хорошие умения в рамках освоенного учебного материала. Ответил на большинство дополнительных вопросов.</td></tr>
<tr><td>3</td><td>Студент выполнил практическое задание билета с существенными неточностями. Показал удовлетворительные умения в рамках освоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей.</td></tr>
<tr><td>2</td><td>При выполнении практического задания билета студент продемонстрировал недостаточный уровень умений. При ответах на дополнительные вопросы было допущено множество неправильных ответов.</td></tr>
</table>
Шкала оценивания уровня приобретенных владений
<table>
<tr><th>Балл</th><th>Критерии оценивания уровня усвоенных знаний</th></tr>
<tr><td>5</td><td>Студент правильно выполнил комплексное задание билета. Показал отличные владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы.</td></tr>
<tr><td>4</td><td>Студент выполнил комплексное задание билета с небольшими неточностями. Показал хорошие владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов.</td></tr>
<tr><td>3</td><td>Студент выполнил комплексное задание билета с существенными неточностями. Показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей.</td></tr>
<tr><td>2</td><td>При выполнении комплексного задания билета студент продемонстрировал недостаточный уровень владения умениями и навыками при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено множество неточностей.</td></tr>
</table>
</td></tr>
</table>