МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

КГЭУ

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

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

«26» октября 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки 09.03.03 Прикладная информатика

Квалификация бакалавр

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 04637A9600B7AE93974C7182805C6B90EF
Владелец: Торкунова Юлия Владимировна
Действителен: с 17.06.2022 до 17.06.2023

г. Казань, 2020

Рабочая программа дисциплины разработана в соответствии с ФГОС ВО - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)

Программу разработал:
доцент,к.т.н. _____ Исмагилов И.Р.

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатика и информационно-управляющие системы, протокол №24 от 26.10.2020 г.
Зав. кафедрой _____ Торкунова Ю.В.

Программа рассмотрена и одобрена на заседании выпускающей кафедры Информатика и информационно-управляющие системы, протокол №24 от 26.10.2020 г.
Зав. кафедрой _____ Торкунова Ю.В.

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

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

Программа принята решением Ученого совета института Цифровых технологий и экономики
протокол № 2 от 26.10.2020 г.

Согласовано:

Руководитель ОПОП _____ Сибаева Г.Р

1. Цель, задачи и планируемые результаты обучения по дисциплине

Целью освоения дисциплины является получение базовых теоретических представлений о современных методах и средствах защиты информации и практических навыков использования этих средств при реализации программных и аппаратных средств информационных систем масштаба предприятия.

Задачами дисциплины является формирование у обучающихся:

1. знаний

- терминологии в области информационной безопасности и защиты информации
- основных нормативных и правовых актов, регламентирующих сферу информационной безопасности и защиты информации
- принципов организации защиты информации на предприятиях;
- мер и средств защиты информации

2. умений

- выявлять основные виды угроз и уязвимостей безопасности информации;
- разрабатывать нормативно-техническую документацию с учетом требований нормативных и правовых актов в области информационной безопасности и защиты информации
- криптографические методы обеспечения целостности и конфиденциальности информации

3. владения:

- навыками применения программно-аппаратных средств для обеспечения информационной безопасности
- навыками программной реализации криптографических алгоритмов

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-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 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	*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 *Уметь:* решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности *Владеть:*

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине (знать, уметь, владеть)
		навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
	ОПК-3.2 Учитывает при решении задач профессиональной деятельности основные требования информационной безопасности	*Знать:* основные виды угроз безопасности информации, уязвимостей информационных систем, а также меры и средства противодействия атакам на информационные ресурсы при проектировании, разработке и внедрении программного обеспечения информационных систем *Уметь:* разрабатывать проектно-техническую документацию для информационных систем с учетом требований текущего законодательства, нормативно-правовых актов, стандартов и ведущих практик в области информационной безопасности *Владеть:* навыками применения программно-аппаратных средств для анализа защищенности информационных систем для выработки мер противодействия известным угрозам безопасности информации

2. Место дисциплины в структуре ОПОП

Дисциплина Информационная безопасность относится к обязательной части учебного плана по направлению подготовки 09.03.03 Прикладная информатика.

Код компетенции	Предшествующие дисциплины (модули), практики, НИР, др.	Последующие дисциплины (модули), практики, НИР, др.
УК-1		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
УК-2		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
УК-3		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ Производственная практика (преддипломная)
УК-4		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
УК-5		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ Производственная практика (преддипломная)
УК-6		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
УК-7		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ Производственная практика (преддипломная)
УК-8		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ Производственная практика (преддипломная)
ОПК-1		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ

ОПК-1	Высшая математика Физика	
ОПК-2		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
ОПК-2	Информационные технологии	
ОПК-3		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
ОПК-4		Проектирование информационных систем Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
ОПК-5		Производственная практика (проектно-технологическая) Операционные системы Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
ОПК-6		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
ОПК-7		Сети и телекоммуникации Производственная практика (проектно-технологическая) Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
ОПК-8		Производственная практика (проектно-технологическая) Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
ОПК-8	Алгоритмизация и программирование	
ОПК-9		Производственная практика (проектно-технологическая) Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ
ПК-1		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ Производственная практика (преддипломная)
ПК-1	Программирование	

ПК-2		Выполнение и защита выпускной квалификационной работы ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ Производственная практика (преддипломная)

Для освоения дисциплины обучающийся должен:

Знать:

1. основы математики, физики, вычислительной техники и программирования
2. современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности
3. алгоритмические языки программирования, операционные системы и оболочки, современные среды разработки программного обеспечения

Уметь:

1. решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования
2. выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности
3. составлять алгоритмы, писать и отлаживать коды на языке программирования, тестировать работоспособность программы, интегрировать программные модули

Владеть:

1. навыками применения современных информационных технологий и программных средств при решении задач профессиональной деятельности

3. Структура и содержание дисциплины

3.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц (ЗЕ), всего 216 часов, из которых 87 часов составляет контактная работа обучающегося с преподавателем (занятия лекционного типа 34 час., занятия семинарского типа (практические, семинарские занятия, лабораторные работы и т.п.) 48 час., групповые и индивидуальные консультации 2 час., контроль самостоятельной работы (КСР) 2 час, прием экзамена (КПА) 1 час), самостоятельная работа обучающегося 94 час. подготовка к промежуточной аттестации 35 час.

Вид учебной работы	Всего часов	Семестр
		5
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ	216	216
КОНТАКТНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ, в том числе:	87	87
Лекционные занятия (Лек)	34	34
Лабораторные занятия (Лаб)	32	32
Практические занятия (Пр)	16	16
Контроль самостоятельной работы и иная контактная работа (КСР)	2	2
Консультации (Конс)	2	2
Контактные часы во время аттестации (КПА)	1	1
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ (СРС)	94	94
Подготовка к промежуточной аттестации в форме: (экзамен)	35	35
ФОРМА ПРОМЕЖУТОЧНОЙАТТЕСТАЦИИ	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*	Сдача зачета / экзамена	Итого					
Раздел 1. Основные понятия и нормативно-правовая база информационной безопасности															
1. Основные понятия информационной безопасности	5	2				2				4	ОПК-3.1-З1	Л1.3, Л2.1, Л2.3	Т10		1
2. Государственная политика в области информационной безопасности	5	2				2				4	ОПК-3.1-У1, ОПК-3.2-У1, ОПК-3.1-В1, ОПК-3.1-З1, ОПК-3.2-З1	Л1.3, Л2.1, Л2.3	Т10		1

3. Классификация информации, доступ к которой ограничен федеральными законами РФ	5		2			4				6	ОПК-3.1-В1, ОПК-3.1-З1, ОПК-3.1-У1	Л2.3, Л2.1	ОПР		2
4. Модель угроз безопасности информации предприятия	5			4		4				8	ОПК-3.2-У1, ОПК-3.2-З1	Л1.3, Л2.1, Л2.3	ОЛР		2
Раздел 2. Управление информационной безопасностью															
5. Международные и российские стандарты в сфере информационной безопасности	5	2				2				4	ОПК-3.1-З1, ОПК-3.1-У1, ОПК-3.1-В1, ОПК-3.2-У1, ОПК-3.2-З1	Л1.3, Л2.1, Л2.3	Т10		1
6. Политика информационной безопасности	5	2				2				4	ОПК-3.2-У1, ОПК-3.1-У1, ОПК-3.1-З1, ОПК-3.2-З1	Л1.3, Л2.3	Т10		1
7. Менеджмент рисков информационной безопасности предприятия	5			4		2				6	ОПК-3.2-У1, ОПК-3.1-В1, ОПК-3.1-У1, ОПК-3.1-З1	Л1.3, Л2.3	ОЛР		2
Раздел 3. Меры и средства защиты информации. Криптографические средства защиты информации (КСЗИ)															
8. Симметричные криптосистемы шифрования. Стандарты шифрования DES, 3DES, AES, ГОСТ 28147-89.	5	2		8		8				18	ОПК-3.2-В1, ОПК-3.2-З1, ОПК-3.1-У1	Л1.2, Л1.3, Л2.3, Л2.1	Т10, ОЛР		6
9. Стеганографические методы защиты информации	5		2			2				4	ОПК-3.2-В1, ОПК-3.2-З1, ОПК-3.1-У1	Л1.2, Л1.3, Л2.3, Л2.1	ОПР		2
10. Асимметричные криптосистемы шифрования	5	2	2			6				10	ОПК-3.2-В1, ОПК-3.2-З1,	Л1.2, Л1.3, Л2.3	Т10, ОПР		4

											ОПК-3.1-У1				
11. Защита информации в электронных документах путем шифрования и формирования электронной подписи	5		2			2				4	ОПК-3.2-В1, ОПК-3.2-З1, ОПК-3.1-У1	Л1.2, Л1.3, Л2.3, Л2.1	ОПР		2
12. Управление криптоключами. Инфраструктура открытых ключей (PKI)	5	2				2				4	ОПК-3.2-У1, ОПК-3.2-З1, ОПК-3.1-У1, ОПК-3.1-З1	Л1.2, Л1.3, Л2.3, Л2.1	Т10		2
Раздел 4. Идентификация, аутентификация и управление доступом															
13. Технологии аутентификации	5	2	2			2				6	ОПК-3.2-У1, ОПК-3.2-З1, ОПК-3.1-У1, ОПК-3.1-З1	Л1.3, Л2.3	Т10		2
14. Криптографические протоколы аутентификации. Биометрическая аутентификация	5	2				2				4	ОПК-3.2-У1, ОПК-3.2-З1, ОПК-3.1-З1, ОПК-3.1-У1	Л1.3, Л2.3	Т10		2
15. Модели разграничения доступа	5	2				2				4	ОПК-3.2-У1, ОПК-3.2-З1, ОПК-3.1-З1	Л1.3, Л2.3	Т10		2
Раздел 5. Обеспечение безопасности информации в операционных системах															
16. Обеспечение безопасности информации в операционных системах семейства Windows	5	2				2				4	ОПК-3.2-В1, ОПК-3.2-У1, ОПК-3.2-З1, ОПК-3.1-У1, ОПК-3.1-З1	Л1.3, Л2.3	Т10		2
17. Автоматизированное обнаружение уязвимостей	5		2			2				9	ОПК-3.2-В1, ОПК-3.2-У1,	Л1.3, Л2.3	Т10		2

программного обеспечения на рабочих станциях под управлением операционных систем семейства Microsoft Windows											ОПК-3.2-З1, ОПК-3.1-У1, ОПК-3.1-З1				
18. Локальные и групповые политики безопасности ОС Microsoft Windows	5			4		2				11	ОПК-3.2-В1, ОПК-3.2-У1, ОПК-3.2-З1, ОПК-3.1-У1, ОПК-3.1-З1	Л1.3, Л2.3	ОПР		2
Раздел 6. Средства антивирусной защиты (САВЗ)															
19. Классификация вредоносных программ	5	2				4				11	ОПК-3.2-З1, ОПК-3.2-У1, ОПК-3.1-З1	Л1.3, Л2.3, Л2.1	ОЛР		2
20. Средства антивирусной защиты информации	5	2				4				11	ОПК-3.1-З1, ОПК-3.2-З1, ОПК-3.2-У1	Л1.3, Л2.3, Л2.1	Т10		2
21. Сравнительный анализ средств антивирусной защиты информации с использованием результатов независимых тестов	5		2			4				11	ОПК-3.2-В1, ОПК-3.2-У1, ОПК-3.2-З1, ОПК-3.1-З1	Л1.3, Л2.3	Т10		2
Раздел 7. Обеспечение безопасности информации в компьютерных сетях															
22. Основы построения компьютерных сетей. Модель OSI. Классификация угроз безопасности информации и атак в компьютерных сетях	5	2				4				11	ОПК-3.2-З1, ОПК-3.1-З1, ОПК-3.2-В1	Л1.3, Л2.2, Л2.3	Т10		2

23. Технология виртуальных локальных сетей (VLAN)	5	2		4		8				14	ОПК-3.1-З1, ОПК-3.2-З1, ОПК-3.2-В1, ОПК-3.2-У1, ОПК-3.1-У1	Л1.3, Л2.2, Л2.3	Т10, ОЛР		4
24. Технологии межсетевого экранирования	5	2	2			8				12	ОПК-3.2-В1, ОПК-3.2-У1, ОПК-3.2-З1, ОПК-3.1-З1, ОПК-3.1-У1	Л1.3, Л2.2, Л2.3	Т10, ОПР		4
25. Технологии виртуальных частных сетей (VPN)	5	2				4				14	ОПК-3.2-В1, ОПК-3.2-У1, ОПК-3.2-З1, ОПК-3.1-З1, ОПК-3.1-У1	Л1.3, Л2.2, Л2.3	Т10		2
26. Изучение средств инструментального анализа защищенности ИТ-инфраструктуры	5			8		8				16	ОПК-3.2-В1, ОПК-3.2-У1, ОПК-3.2-З1, ОПК-3.1-У1, ОПК-3.1-З1	Л1.3, Л2.2, Л2.3	Т10, ОЛР		4
Подготовка к промежуточной аттестации					2		2		1						
Промежуточная аттестация (экзамен)								35						Эк	40
ИТОГО		34	16	32	2	94	2	35	1	216					100

3.3. Тематический план лекционных занятий

Номер раздела дисциплины	Темы лекционных занятий	Трудоемкость, час.
1	Основные понятия информационной безопасности	2
2	Государственная политика в области информационной безопасности	2
3	Международные и российские стандарты информационной безопасности	2
4	Формирование политики информационной безопасности на предприятии	2
5	Симметричные криптосистемы шифрования. Стеганография	2
6	Асиметричные криптосистемы шифрования и электронная подпись	2
7	Управление криптоключами. Инфраструктура открытых ключей	2
8	Технологии аутентификации	2
9	Криптографические протоколы аутентификации. Биометрическая аутентификация	2
10	Модели разграничения доступа	2
11	Обеспечение безопасности информации в операционных системах семейства Windows	2
12	Средства антивирусной защиты информации	2
13	Классификация вредоносных программ	2
14	Классификация угроз безопасности информации и атак в компьютерных сетях	2
15	Технология виртуальных локальных сетей (VLAN)	2
16	Технологии межсетевого экранирования	2
17	Технологии виртуальных частных сетей (VPN)	2
	Всего	34

3.4. Тематический план практических занятий

Номер раздела дисциплины	Темы практических занятий	Трудоемкость, час.
1	Изучение видов информации, доступ к которым ограничен федеральными законами РФ	2
2	Программная реализация стеганографии в графических файлах	2
3	Программная реализация асимметричного алгоритма шифрования RSA	2
4	Защита информации в электронных документах путем шифрования и формирования электронной подписи	2
5	Парольная аутентификация	2
6	Автоматизированное обнаружение уязвимостей программного обеспечения на рабочих станциях под управлением операционных систем семейства Microsoft Windows	2

7	Сравнительный анализ средств антивирусной защиты информации с использованием результатов независимых тестов	2
8	Изучение технологий межсетевого экранирования с помощью программы моделирования сетей Cisco Packet Tracer	2
	Всего	16

3.5. Тематический план лабораторных работ

Номер раздела дисциплины	Темы лабораторных работ	Трудоемкость, час.
1	Разработка модели угроз безопасности информации предприятия	4
2	Анализ рисков информационной безопасности предприятия	4
3	Моноалфавитные и полиалфавитные шифры. Частотный криптоанализ	4
4	Программная реализация классических алгоритмов шифрования и их криптоанализа	4
5	Настройка локальных и групповых политик ОС Microsoft Windows	4
6	Изучение технологий виртуальных локальных сетей (VLAN) с помощью программы моделирования сетей Cisco Packet Tracer	4
7	Использование программы Wireshark для анализа кадров Ethernet с целью изучения процессов обмена данными по протоколам TCP и UDP	4
8	Изучение работы сканеров портов и сетевых служб, сканеров безопасности сети на примере утилит nmap и OpenVAS с использованием технологий виртуализации.	4
	Всего	32

3.6. Самостоятельная работа студента

Номер раздела дисциплины	Вид СРС	Содержание СРС	Трудоемкость, час.
1	подготовка к практическому занятию	Классификация информации, доступ к которым ограничен федеральными законами РФ. Виды юридической ответственности и правоприменительная практика в области информационной безопасности	4
2	изучение теоретического материала	Возникновение и история развития проблемы защиты информации. Понятие информационного общества. Актуальность проблемы обеспечения безопасности информации.	2
3	изучение теоретического материала	Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ	2
4	подготовка к лабораторной работе	Моделирование и оценка угроз безопасности информации. Модель нарушителя. Методика определения актуальных угроз безопасности информации.	4

5	изучение теоретического материала	Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий	2
6	изучение теоретического материала	Структура политики безопасности организации. Разработка политики безопасности организации	2
7	подготовка к лабораторной работе	Методика определения рисков информационной безопасности	2
8	изучение теоретического материала	Классификация симметричных криптосистем. Криптостойкость симметричных криптосистем.	2
9	подготовка к лабораторной работе	Блочные и потоковые шифры. Шифр Цезаря. Шифр Виженера. Шифрование методом перестановки. Гаммирование.	2
10	подготовка к лабораторной работе	Шифр playfair. Шифр Полибия. Афинный шифр. Виды криптоанализа. Установка языка программирования Python, изучение базового синтаксиса. Работа с командной строкой Windows.	4
11	подготовка к практическому занятию	Классификация стеганографических средств защиты информации	2
12	изучение теоретического материала	Генерация простых чисел для формирования ключей шифрования. Криптография на эллиптических кривых	2
13	подготовка к практическому занятию	Генерация простых чисел для формирования пары ключей для шифрования. Библиотеки Python для программной реализации асимметричных криптоалгоритмов.	4
14	подготовка к практической работе	PGP шифрование. Криптографические хеш-функции. Виды электронной подписи	2
15	изучение теоретического материала	Удостоверяющие центры и сертификаты.	2
16	изучение теоретического материала	Строгая аутентификация. Многофакторная аутентификация.	2
17	изучение теоретического материала	Виды биометрической идентификации	2
18	изучение теоретического материала	Классификация моделей разграничения доступа.Модель систем дискреционного разграничения доступа. Мандатное управление доступом. Ролевое разграничение. Сравнительный анализ моделей разграничения доступа.	2
19	изучение теоретического материала	Управление пользовательскими учетными записями (User Account Control - UAC). Брандмауэр.	2

20	подготовка к практическому занятию	Сканеры уязвимостей типа host-based. Система оценки уязвимостей - CVSS2.0 и CVSS3.0	2
21	подготовка к лабораторной работе	Локальные и групповые политики ОС Microsoft Windows	2
22	изучение теоретического материала	Основные каналы распространения вредоносных программ. Антивирусные программы: основы работы антивирусных программ, особенности «облачной» антивирусной технологии, виды антивирусных программ, дополнительные модули антивирусных программ, режимы работы антивируса	4
23	изучение теоретического материала	Антивирусные программные комплексы: антивирус Касперского, антивирус Dr. Web, антивирус Norton AntiVirus от Symantec, антивирус McAfee, антивирус AntiVir Personal Edition	4
24	подготовка к практическому занятию	Методы обнаружения вредоносных программ. Режим "песочницы".	4
25	изучение теоретического материала	ARP-спуфинг. SYN-флуд. Smurf- атака. Атаки на беспроводные сети.	4
26	изучение теоретического материала	Сегментация сети с помощью технологии VLAN. Использование протокола 802.1Q	4
27	подготовка к лабораторной работе	Преимущества сегментирования локальных сетей. Настройка VLAN на коммутаторах фирмы Cisco.	4
28	изучение теоретического материала	Функции межсетевого экрана. Классификация МЭ.	4
29	подготовка к практическому занятию	Списки доступа (ACL). Демилитаризованная зона (DMZ)	4
30	изучение теоретического материала	VPN-туннелирование. VPN-сервер. VPN - клиент. Классификация VPN.	4
31	подготовка к лабораторной работе	Установление TCP соединения. Структура TCP-пакета. Флаги состояния. Применение фильтров для анализа трафика в Wireshark	4
32	подготовка к лабораторной работе	Разновидности сканеров безопасности сети. Виртуальные машины. ПО для работы с виртуальными машинами (Virtual Box)	4
		Всего	94

4. Образовательные технологии

При реализации дисциплины применяются электронное обучение и дистанционные образовательные технологии.

В образовательном процессе используются:

- дистанционные курсы (ДК), размещенные на площадке LMS Moodle, URL: http://lms.kgeu.ru/;
- электронные образовательные ресурсы (ЭОР), размещенные в личных кабинетах студентов Электронного университета КГЭУ, URL: http://e.kgeu.ru/

5. Оценивание результатов обучения

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля успеваемости, проводимого по балльно-рейтинговой 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 основные умения, имеют место грубые ошибки	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме
Наличие навыков (владение	При решении стандартных задач не продемонстрированы	Имеется минимальный набор навыков для решения	Продемонстрированы базовые навыки при решении стандартных задач с	Продемонстрированы навыки при решении нестандартных задач

опытом)	базовые навыки, имеют место грубые ошибки	стандартных задач с некоторыми недочетами	некоторыми недочетами	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 сформиро-ванности компетенции (индикатора достижения компетенции)	Низкий	Ниже среднего	Средний	Высокий

Шкала оценки результатов обучения по дисциплине:

Код компетенции	Код индикатора достижения компетенции	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-	ОПК-	Знать				

3	3.1	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	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки
		Уметь				
		решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки
		Владеть				
		навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки
	ОПК-3.2					
		Знать				

		основные виды угроз безопасности информации, уязвимостей информационных систем, а также меры и средства противодействия атакам на информационные ресурсы при проектировании, разработке и внедрении программного обеспечения информационных систем	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки
		Уметь				
		разрабатывать проектно-техническую документацию для информационных систем с учетом требований текущего законодательства, нормативно-правовых актов, стандартов и ведущих практик в области информационной безопасности	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки
		Владеть				
		навыками применения программно-аппаратных средств для анализа защищенности информационных систем для выработки мер противодействия известным угрозам безопасности информации	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки

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)	Наименование	Вид издания (учебник, учебное пособие, др.)	Место издания, издательство	Год издания	Адрес электронного ресурса	Кол-во экземпляров в библиотеке КГЭУ
2	Баранова Е. К., Бабаш А. В.	Криптографические методы защиты информации. Лабораторный практикум	Учебное пособие	М.: Кнорус	2017	https://www.book.ru/book/920017/	1
3	Демушкин А. С., Кондрашова Т. В., Фабричнов А. Г., Куняев Н. Н.	Конфиденциальное делопроизводство и защищенный электронный документооборот	учебник для вузов	М.: Логос	2013	https://ibooks.ru/reading.php?productid=29403	1

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	Крылов Г. О., Ларионова С. Л., Никитина В. Л.	Базовые понятия информационной безопасности	учебное пособие	М.: Русайнс	2016	https://www.book.ru/book/921926	1
2	Шевченко В. П.	Вычислительные системы, сети и телекоммуникации	Учебник	М.: Кнорус	2017	https://www.book.ru/book/920410/	1

3	Мельников В. П., Куприянов А. И., Васильева Т. Ю.	Информационная безопасность	учебник	М.: Кнорус	2018	https://www.book.ru/book/929884	1

6.2. Информационное обеспечение

6.2.1. Электронные и интернет-ресурсы

№ п/п	Наименование электронных и интернет-ресурсов	Ссылка
1	Справочно-правовая система "Консультант Плюс"	http://www.consultant.ru/
2	Справочно-правовая система "Гарант"	http://www.garant.ru/
3	Банк данных угроз безопасности информации	https://bdu.fstec.ru/
4	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных	https://fstec.ru/component/attachments/download/289
5	ISO27000 - Искусство управления информационной безопасностью	http://www.iso27000.ru/standarty
6	Учебный курс на портале НОУ "ИНТУИТ" - Стандарты информационной безопасности	https://www.intuit.ru/studies/courses/30/30/info
7	Учебный курс на портале НОУ "ИНТУИТ" - Информационная безопасность. Технологии Microsoft	https://www.intuit.ru/studies/professional_retraining/952/courses/419/lecture/9577?page=2
8	Учебный курс на портале НОУ "ИНТУИТ" - Информационная безопасность. Технологии Microsoft: Анализ и управление рисками в информационных системах на базе операционных систем Microsoft	https://www.intuit.ru/studies/professional_retraining/952/courses/387/info
9	Anti-Malware Testing Standards Organization	https://www.amtso.org/
10	AV-TEST - The Independent IT-Security Institute	https://www.av-test.org/en/
11	AV-Comparatives - Independent Tests of Anti-Virus Software	https://www.av-comparatives.org/
12	Wireshark — программа-анализатор трафика для компьютерных сетей Ethernet	https://www.wireshark.org/
13	Справочное руководство Nmap на русском языке	https://nmap.org/man/ru/index.html
14	OpenVAS Russia. Русскоязычное сообщество пользователей сканера уязвимостей OpenVAS	https://openvas.ru/
15	Cisco Networking Academy	https://www.netacad.com/
16	Cisco Networking Academy - маршрутизация и коммутация	http://ccna.mpei.ac.ru/RoutingAndSwitching/

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	Научная электронная библиотека eLIBRARY.RU	http://elibrary.ru	http://elibrary.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	«Гарант»	http://www.garant.ru/	http://www.garant.ru/
3	«Консультант плюс»	http://www.consultant.ru/	http://www.consultant.ru/

6.2.4. Лицензионное и свободно распространяемое программное обеспечение дисциплины

№ п/п	Наименование программного обеспечения	Описание	Реквизиты подтверждающих документов
1	Браузер Chrome	Система поиска информации в сети интернет	Свободная лицензия, тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно.
2	Office Standard 2007 Russian OLP NL AcademicEdition+	Пакет программных продуктов, содержащий в себе необходимые офисные программы	Договор №21/2010 от 04.05.2010, лицензиар - ЗАО «Софт Лайн Трейд», тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно
3	Office Professional Plus 2007 Windous32 Russian DiskKit MVL CD	Пакет программных продуктов, содержащий в себе необходимые офисные программы	Договор №225/10 от 28.01.2010, лицензиар - ЗАО «Софт Лайн Трейд», тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно
4	LMS Moodle	ПО для эффективного онлайн-взаимодействия преподавателя и студента	Свободная лицензия, тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно.
5	Windows 7 Профессиональная (Pro)	Пользовательская операционная система	Договор №2011.25486 №2011.25486 от 28.11.2011, лицензиар – ЗАО «Софт Лайн Трейд», тип (вид) лицензии – неискл. право, срок действия лицензии – бессрочно;

6	Windows 7 Профессиональная (сертифицированная ФСТЭК).	Пользовательская операционная система	Договор №ПО-ЛИЦ 0000/2014 от 27.05.2014, лицензиар – ЗАО «ТаксНет Сервис», тип (вид) лицензии – неискл. право, срок действия лицензии бессрочно
7	Windows 10	Пользовательская операционная система	Договор № Tr096148 от 29.09.2020, лицензиар - ООО "Софтлайн трейд", тип (вид) лицензии - 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	Доска аудиторная, акустическая система, проектор, усилитель-микшер для систем громкой связи, экран, микрофон, миникомпьютер, монитор
2	Практические занятия	Учебная аудитория для проведения занятий практического типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Персональный компьютер (26 шт.), интерактивная доска, мультимедийный проектор
3	Лабораторные работы	Учебная лаборатория	Персональный компьютер (26 шт.), интерактивная доска, мультимедийный проектор
4	Самостоятельная работа обучающегося	Компьютерный класс с выходом в Интернет	Моноблок (30 шт.), проектор, экран
		Читальный зал библиотеки	Проектор, переносной экран, тонкие клиенты (13 шт.), компьютеры (5 шт.)

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 направлению 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.

9. Методические рекомендации для преподавателей по организации воспитательной работы с обучающимися

Методическое обеспечение процесса воспитания обучающихся выступает одним из определяющих факторов высокого качества образования. Преподаватель вуза, демонстрируя высокий профессионализм, эрудицию, четкую гражданскую позицию, самодисциплину, творческий подход в решении профессиональных задач, в ходе образовательного процесса способствует формированию гармоничной личности.

При реализации дисциплины преподаватель может использовать следующие методы воспитательной работы:

- методы формирования сознания личности (беседа, диспут, внушение, инструктаж, контроль, объяснение, пример, самоконтроль, рассказ, совет, убеждение и др.);
- методы организации деятельности и формирования опыта поведения (задание, общественное мнение, педагогическое требование, поручение, приучение, создание воспитывающих ситуаций, тренинг, упражнение, и др.);
- методы мотивации деятельности и поведения (одобрение, поощрение социальной активности, порицание, создание ситуаций успеха, создание ситуаций для эмоционально-нравственных переживаний, соревнование и др.)

При реализации дисциплины преподаватель должен учитывать следующие направления воспитательной деятельности:

Гражданское и патриотическое воспитание:

- формирование у обучающихся целостного мировоззрения, российской идентичности, уважения к своей семье, обществу, государству, принятым в семье и обществе духовно-нравственным и социокультурным ценностям, к национальному, культурному и историческому наследию, формирование стремления к его сохранению и развитию;
- формирование у обучающихся активной гражданской позиции, основанной на традиционных культурных, духовных и нравственных ценностях российского общества, для повышения способности ответственно реализовывать свои конституционные права и обязанности;
- развитие правовой и политической культуры обучающихся, расширение конструктивного участия в принятии решений, затрагивающих их права и интересы, в том числе в различных формах самоорганизации, самоуправления, общественно-значимой деятельности;
- формирование мотивов, нравственных и смысловых установок личности, позволяющих противостоять экстремизму, ксенофобии, дискриминации по социальным, религиозным, расовым, национальным признакам, межэтнической и межконфессиональной нетерпимости, другим негативным социальным явлениям.

Духовно-нравственное воспитание:

- воспитание чувства достоинства, чести и честности, совестливости, уважения к родителям, учителям, людям старшего поколения;
- формирование принципов коллективизма и солидарности, духа милосердия и сострадания, привычки заботиться о людях, находящихся в

трудной жизненной ситуации;

- формирование солидарности и чувства социальной ответственности по отношению к людям с ограниченными возможностями здоровья, преодоление психологических барьеров по отношению к людям с ограниченными возможностями;

- формирование эмоционально насыщенного и духовно возвышенного отношения к миру, способности и умения передавать другим свой эстетический опыт.

Культурно-просветительское воспитание:

- формирование уважения к культурным ценностям родного города, края, страны;

- формирование эстетической картины мира;

- повышение познавательной активности обучающихся.

Научно-образовательное воспитание:

- формирование у обучающихся научного мировоззрения;

- формирование умения получать знания;

- формирование навыков анализа и синтеза информации, в том числе в профессиональной области.

Физическое воспитание:

- формирование ответственного отношения к своему здоровью, потребности в здоровом образе жизни;

- формирование культуры безопасности жизнедеятельности;

- формирование системы мотивации к активному и здоровому образу жизни, занятиям спортом, культуры здорового питания и трезвости.

Профессионально-трудовое воспитание:

- формирование добросовестного, ответственного и творческого отношения к разным видам трудовой деятельности;

- формирование навыков высокой работоспособности и самоорганизации, умение действовать самостоятельно, мобилизовать необходимые ресурсы, правильно оценивая смысл и последствия своих действий;

Экологическое воспитание:

- формирование экологической культуры, бережного отношения к родной земле, экологической картины мира, развитие стремления беречь и охранять природу.

Структура дисциплины по заочной форме обучения

Вид учебной работы	Всего часов	Курс
		3
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ	216	216
КОНТАКТНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ, в том числе:	23	23
Лекционные занятия (Лек)	6	6
Лабораторные занятия (Лаб)	8	8
Практические занятия (Пр)	4	4
Контроль самостоятельной работы и иная контактная работа (КСР)*	4	4
Контактные часы во время аттестации (КПА)	1	1
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ (СРС):	185	185
Подготовка к промежуточной аттестации в форме: (экзамен)	8	8
ФОРМА ПРОМЕЖУТОЧНОЙАТТЕСТАЦИИ	Эк	Эк

Лист внесения изменений

Дополнения и изменения в рабочей программе дисциплины «Информационная безопасность» на 2021/2022 учебный год.

В программу вносятся следующие изменения:

1. РПД дополнена разделом 9 «Методические рекомендации для преподавателей по организации воспитательной работы с обучающимися» (стр. 27-28).

Программа одобрена на заседании кафедры-разработчика 17.06.2021 г., протокол № 9. Зав. кафедрой Торкунова Ю.В.

Программа одобрена методическим советом ИЦТЭ 22.06.2021 г., протокол № 10

Зам. директора по УМР Косулин В.В.

Согласовано:

Руководитель ОПОП Сибаева Г.Р.

Приложение к рабочей программе дисциплины

КГЭУ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
по дисциплине
Информационная безопасность

Направление подготовки 09.03.03 Прикладная информатика

Квалификация бакалавр

Форма обучения очная

г. Казань, 2020

Рецензия

на оценочные материалы для проведения промежуточной аттестации обучающихся по дисциплине «Информационная безопасность»

Содержание ОМ соответствует требованиям федерального государственного стандарта высшего образования по направлению подготовки 09.03.03 «Прикладная информатика» и учебному плану.

Перечень формируемых компетенций: 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 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий; ОПК-3.2 Учитывает при решении задач профессиональной деятельности основные требования информационной безопасности), которыми должен овладеть обучающийся в результате освоения дисциплины, соответствует ФГОС ВО.

Показатели и критерии оценивания компетенций, а также шкалы оценивания обеспечивают возможность проведения всесторонней оценки уровней сформированности компетенций.

Контрольные задания оценки результатов освоения разработаны на основе принципов оценивания: валидности, определённости, однозначности, надёжности, позволяют объективно оценить уровни сформированности компетенций.

Заключение. Учебно-методический совет делает вывод о том, что представленные материалы соответствуют требованиям ФГОС ВО по направлению подготовки 09.03.03 «Прикладная информатика» и рекомендуются для использования в учебном процессе.

Рассмотрено на заседании учебно-методического совета института Цифровых технологий и экономики от «26» октября 2020 г., протокол № 2

Председатель УМС Торкунова Ю.В.

Рецензент
эксперт 1 категории отдела разработки
перспективной платежной системы
в региональном центре развития «Казань»
в отделении - Нац. банк по РТ
Волго-Вятского ГУ ЦБ РФ,
кандидат технических наук Шершуков В.В.

Оценочные материалы по дисциплине «Информационная безопасность » - комплект контрольно-измерительных материалов, предназначенных для оценивания результатов обучения на соответствие индикаторам достижения компетенций:

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 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий

ОПК-3.2 Учитывает при решении задач профессиональной деятельности основные требования информационной безопасности

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: тест по теме лекции, тест по всем темам дисциплины, отчет по лабораторной работе, доклад с презентацией, отчет по практической работе.

Промежуточная аттестация имеет целью определить уровень достижения запланированных результатов обучения по дисциплине за 5 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 5

Номер раздела/ темы дисциплины	Вид СРС	Наименование оценочного средства	Код индикатора достижения компетенций	Уровень освоения дисциплины, баллы			
				неудов-но	удов-но	хорошо	отлично
				не зачтено	зачтено		
				низкий	ниже среднего	средний	высокий
Текущий контроль успеваемости							
1	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	1 - 1
2	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	1 - 1
3	подготовка к практическому занятию	ОПР	ОПК-3.1; ОПК-3.2	менее 0	1 - 1	2 - 2	2 - 2
4	подготовка к лабораторной работе	ОЛР	ОПК-3.1; ОПК-3.2	менее 1	1 - 1	2 - 2	2 - 2
5	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	1 - 1

6	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	1 - 1
7	подготовка к лабораторной работе	ОЛР	ОПК-3.1; ОПК-3.2	менее 1	1 - 1	2 - 2	2 - 2
8	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
8	подготовка к лабораторной работе	ОЛР	ОПК-3.1; ОПК-3.2	менее 1	1 - 1	2 - 2	2 - 2
8	подготовка к лабораторной работе	ОЛР	ОПК-3.1; ОПК-3.2	менее 1	1 - 1	2 - 2	2 - 2
9	подготовка к практическому занятию	ОПР	ОПК-3.1; ОПК-3.2	менее 0	1 - 1	2 - 2	2 - 2
10	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
10	подготовка к практическому занятию	ОПР	ОПК-3.1; ОПК-3.2	менее 0	1 - 1	2 - 2	2 - 2
11	подготовка к практической работе	ОПР	ОПК-3.1; ОПК-3.2	менее 0	1 - 1	2 - 2	2 - 2
12	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
13	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
14	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
15	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
16	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
17	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
18	подготовка к практическому занятию	ОПР	ОПК-3.1; ОПК-3.2	менее 0	1 - 1	2 - 2	2 - 2
19	подготовка к лабораторной работе	ОЛР	ОПК-3.1; ОПК-3.2	менее 1	1 - 1	2 - 2	2 - 2
20	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
21	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2

22	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
23	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
23	изучение теоретического материала	ОЛР	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
24	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
24	изучение теоретического материала	ОЛР	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
25	подготовка к практическому занятию	ОПР	ОПК-3.1; ОПК-3.2	менее 0	1 - 1	2 - 2	2 - 2
26	изучение теоретического материала	Т10	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
26	изучение теоретического материала	ОЛР	ОПК-3.1; ОПК-3.2	менее 0	0 - 0	1 - 1	2 - 2
Итого баллов				**менее 55**	**55-69**	**70-84**	**85-100**

2. Перечень оценочных средств

Краткая характеристика оценочных средств, используемых при текущем контроле успеваемости и промежуточной аттестации обучающегося по дисциплине:

Наименование оценочного средства	Краткая характеристика оценочного средства	Оценочные материалы
Тест по теме лекции (Т10)	Тест из 10 вопросов для закрепления лекционного материала	Тест из 10 вопросов разного типа (база 200)
Отчет по лабораторной работе (ОЛР)	Отчет по лабораторной работе выполняется индивидуально каждым из студентов согласно Методическим указаниям, выданным на занятии. Отчет загружается в электронном виде в соответствующее задание на курсе в LMS Moodle. Преподаватель после проверки проставляет оценку по шкале "зачтено/не зачтено" с указанием замечаний, при необходимости отправляет отчет на доработку.	Задания к лабораторным работам

Отчет по практической работе (ОПР)	Отчет по практической работе выполняется индивидуально каждым из студентов согласно Методическим указаниям, выданным на занятии. Отчет загружается в электронном виде в соответствующее задание на курсе в LMS Moodle. Преподаватель после проверки проставляет оценку по шкале "зачтено/не зачтено" с указанием замечаний, при необходимости отправляет отчет на доработку.	Задание к практической работе

3. Оценочные материалы текущего контроля успеваемости обучающихся

Наименование оценочного средства	**Тест по теме лекции (Т10)**
Представление и содержание оценочных материалов	Тест из 10 вопросов разного типа по определенному разделу дисциплины Примеры тестов из раздела дисциплины «Основные понятия и нормативно-правовая база информационной безопасности»: 1.2 Возможность за приемлемое время получить требуемую информационную услугу - это _____ a) доступность b) конфиденциальность c) целостность d) адекватность e) неотказуемость 1.8 Совокупность условий или действий, создающих потенциальную или реально существующую опасность нарушения безопасности информации a) угроза безопасности информации b) риск безопасности информации c) уязвимость безопасности информации d) атака на информационные ресурсы Ниже приведены тестовые задания, которые используются для текущего контроля, сгруппированные по разделам дисциплины и типу **1. Основные понятия и нормативно-правовая база информационной безопасности** *Тестовые задания с выбором единственного правильного ответа:* 1.1 Защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности - это _____ a) информационная безопасность b) защита информации c) интернет-безопасность d) разграничение доступа к информации e) политика безопасности информации 1.2 Возможность за приемлемое время получить требуемую информационную услугу - это _____ f) доступность g) конфиденциальность h) целостность i) адекватность j) неотказуемость 1.3 Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения - это ____ a) целостность b) доступность c) конфиденциальность d) неотказуемость e) адекватность 1.4 Статус, предоставленный информации и определяющий требуемую степень ее защиты a) конфиденциальность b) подлинность c) аутентичность d) целостность 1.5 Способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты

a) неотказуемость
b) подлинность
c) аутентичность
d) адекватность
e) целостность

1.6 Свойство, гарантирующее, что субъект или ресурс идентичны заявленному
a) подлинность
b) доступность
c) неотказуемость
d) конфиденциальность
e) целостность

1.7 Пассивные компоненты информационной системы, хранящие, принимающие или передающие информацию
a) объекты системы
b) субъекты системы
c) узлы системы
d) пользователи системы

1.8 Совокупность условий или действий, создающих потенциальную или реально существующую опасность нарушения безопасности информации
a) угроза безопасности информации
b) риск безопасности информации
c) уязвимость безопасности информации
d) атака на информационные ресурсы

1.9 Свойство информационной системы, обусловливающее возможность реализации угрозы безопасности обрабатываемой в ней информации
a) уязвимость безопасности информации
b) угроза безопасности информации
c) риск информационной безопасности
d) атака на компьютерную систему
e) инцидент информационной безопасности

1.10 Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию - это _____
a) защита информации
b) информационная безопасность
c) управление безопасностью информации
d) менеджмент информационной безопасности

1.11 Техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации (ЗИ)
a) средство ЗИ
b) мера ЗИ
c) инструмент ЗИ
d) устройство ЗИ
e) способ ЗИ

1.12 Порядок и правила применения определенных принципов и средств защиты информации (ЗИ)
a) способ ЗИ
b) технология ЗИ
c) прием ЗИ
d) средство ЗИ
e) тактика ЗИ

Тестовые задания с несколькими возможными правильными ответами:

1.13 Какие из перечисленных компонентов информационной системы могут выступать в роли субъектов?
a) пользователи
b) активные программы
c) процессы
d) линии передачи информации
e) коммутационное оборудование

1.14 Среди перечисленных видов нарушителей информационной безопасности выберите ВНЕШНИХ нарушителей
a) Разработчики, производители, поставщики программных, технических и программно-технических средств
b) Бывшие работники
c) Конкурирующие организации
d) Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ
e) Пользователи информационной системы
f) Администраторы информационной системы и администраторы безопасности

1.15 Среди перечисленных видов нарушителей информационной безопасности выберите ВНУТРЕННИХ нарушителей

a) Администраторы информационной системы и администраторы безопасности
b) Пользователи информационной системы
c) Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ
d) Преступные группы (криминальные структуры)
e) Бывшие работники (пользователи)

1.16 Среди перечисленных целей (мотивации) реализации угроз безопасности информации выберите возможные цели, которые характерны для преступных групп (криминальных структур)
a) Причинение имущественного ущерба путем мошенничества или иным преступным путем.
b) Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
c) Идеологические или политические мотивы
d) Любопытство или желание самореализации (подтверждение статуса).
e) Дестабилизация деятельности органов государственной власти, организаций

1.17 Среди перечисленных целей (мотивации) реализации угроз безопасности информации выберите возможные цели, которые характерны для террористических, экстремистских группировок
a) Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики.
b) Совершение террористических актов
c) Идеологические или политические мотивы
d) Дестабилизация деятельности органов государственной власти, организаций
e) Любопытство или желание самореализации (подтверждение статуса).

1.18 Среди перечисленных целей (мотивации) реализации угроз безопасности информации выберите возможные цели, которые характерны для бывших работников (пользователей)
a) Причинение имущественного ущерба путем мошенничества или иным преступным путем
b) Месть за ранее совершенные действия
c) Непреднамеренные, неосторожные или неквалифицированные действия
d) Идеологические или политические мотивы.

1.19 Среди перечисленных видов нарушителей выберите нарушителей с базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе
a) внешние субъекты (физические лица)
b) лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора
c) пользователи информационной системы
d) лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ
e) администраторы информационной системы и администраторы безопасности
f) разработчики, производители, поставщики программных, технических и программно-технических средств

1.20 Среди перечисленных видов нарушителей выберите нарушителей с базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе
a) террористические, экстремистские группировки
b) преступные группы (криминальные структуры
c) конкурирующие организации
d) разработчики, производители, поставщики программных, технических и программно-технических средств
e) администраторы информационной системы и администраторы безопасности
f) специальные службы иностранных государств (блоков государств)

Тестовые задания открытой формы:

1.21 Информация, или носитель информации, или информационный процесс, в отношении которого необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации - это _____ (два слова через пробел)

1.22 Лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы - это _____ нарушители

1.23 Лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам - это _____ нарушители

Тестовые задания на установление соответствия:

1.24 Установите соответствие между понятиями и определениями:

1) процедура распознавания субъекта по его идентификатору	a) активация
2) проверка подлинности субъекта с данным идентификатором	b) верификация
3) процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы	c) авторизация
	d) идентификация
	e) аутентификация

1.25 Установите соответствие между способом защиты информации и применяемыми для его реализации средствами защиты информации:

1) регламентация
2) побуждение
3) управление доступом

a) Законодательные средства ЗИ
b) Организационные средства ЗИ
c) Морально-этические средства ЗИ
d) Программные средства ЗИ
e) Технические средства ЗИ

1.26 Установите соответствие между способом защиты информации и применяемыми для его реализации средствами защиты информации:

1) принуждение
2) маскировка
3) препятствия

a. Законодательные средства ЗИ
b. Организационные средства ЗИ
c. Морально-этические средства ЗИ
d. Программные средства ЗИ
e. Технические средства ЗИ

1.27 Угрозы безопасности информации могут быть реализованы нарушителями за счет НСД и/или воздействия на объекты разных уровней функционирования информационной системы. Установите соответствие между уровнями и их объектами.

1) аппаратный уровень
2) общесистемный уровень
3) прикладной уровень
4) сетевой уровень

a) Микропрограммы, «прошитые» в чипсетах
b) Операционные системы
c) Машинные носители информации
d) Сетевое оборудование
e) Веб-приложение

Тестовые задания на установление последовательности

1.28 Укажите последовательность этапов реализации преднамеренных угроз безопасности информации. Ответ запишите в виде последовательности букв

a) сбор информации об информационной системе, ее структурно-функциональных характеристиках, условиях функционирования
b) выбор (разработка, приобретение) методов и средств, используемых для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и условиями функционирования
c) проникновение в информационную систему
d) закрепление в информационной системе
e) реализация неправомерных действий
f) устранение признаков и следов неправомерных действий в информационной системе

3. Меры и средства защиты информации. Криптографические средства защиты информации (КСЗИ)

Тестовые задания с выбором единственного правильного ответа

3.1 Что такое криптограмма?

a) шифротекст
b) исходный текст сообщения
c) алгоритм шифрования
d) дезинформация

3.2 Совокупность процедур и правил криптографических преобразований, используемых для зашифровывания и расшифровывания информации по ключу шифрования

a) шифр
b) алгоритм
c) криптосистема
d) хеширование

3.3 Процесс расшифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования.

a) криптоанализ
b) криптология
c) криптография
d) хеширование
e) стеганография

3.4 Метод криптозащиты, представляющий собой контрольное преобразование информации: из данных неограниченного размера путем выполнения криптографических преобразований вычисляется дайджест фиксированной длины, однозначно соответствующее исходным данным

a) хеширование
b) криптоанализ
c) стеганография

d) электронная подпись
e) аутентификация

3.5 С помощью какого механизма обеспечивается целостность данных при симметричном шифровании
a) имитоприставка
b) сжатие
c) кодирование
d) асимметричное шифрование

3.6 Какой метод построения блочных шифров положен в основу стандарта шифрования DES
a) Сеть Фейстеля
b) Подстановочно-перестановочная сеть
c) Алгоритм SQUARE
d) SP-сеть

3.7 Какой из перечисленных режимов работы DES наиболее подвержен атакам нарушения целостности (с удалениями и вставками)
a) ECB
b) CBC
c) CFB
d) OFB

3.8 Какой из перечисленных режимов работы алгоритма шифрования DES наиболее защищен от атак на нарушение целостности передаваемых зашифрованных сообщений
a) CBC
b) ECB
c) CFB
d) OFB

3.9 Использование какого элемента в таких режимах работы DES, как CBC, CFB позволяет получать разные результаты шифрования с использованием одного и того же секретного ключа?
a) вектор инициализации
b) дополнительный ключ
c) дополнительный раунд
d) S-box
e) P-box

3.10 Какой метод построения блочных шифров положен в основу стандарта шифрования AES
a) подстановочно-перестановочная сеть
b) сеть Фейстеля
c) метод гаммирования
d) метод перемешивания битов

3.11 В основу криптографической системы с открытым ключом RSA положена
a) сложность задачи разложения на простые множители произведения двух больших простых чисел
b) сложность задачи деления с остатком произведения двух больших простых чисел
c) сложность задачи возведения в степень больших простых чисел
d) сложность задачи логарифмирования произведения двух больших простых чисел

3.12 Вид электронной подписи, позволяющий организовать юридически значимый электронный документооборот с партнерскими компаниями, органами государственной власти и внебюджетными фондами?
a) квалифицированная электронная подпись
b) простая электронная подпись
c) неквалифицированная электронная подпись
d) расширенная электронная подпись

3.13 Какой закон позволил участникам гражданско-правовых отношений обмениваться электронными договорами, актами, накладными и иными документами и установил условия, при выполнении которых эти документы равнозначны аналогичным на бумажных носителях?
a) Федеральный закон "Об электронной цифровой подписи" от 10.01.2002 N 1-ФЗ
b) Федеральный закон от 06.04.2011 № 63-ФЗ "Об электронной подписи"
c) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

3.14 Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи
a) средства электронной подписи
b) средства удостоверяющего центра
c) ключ электронной подписи
d) ключ проверки электронной подписи

3.15 Электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом
a) простая электронная подпись
b) усиленная электронная подпись

c) усиленная квалифицированная электронная подпись
d) усиленная неквалифицированная электронная подпись
e) усиленная простая электронная подпись
f) простая неквалифицированная электронная подпись

3.16 Информация в электронной форме, которая присоединена к другой информации в электронной форме или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию
a) электронная подпись
b) сертификат ключа проверки электронной подписи
c) ключ электронной подписи
d) ключ проверки электронной подписи
e) квалифицированный сертификат

3.17 Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи
a) сертификат ключа проверки электронной подписи
b) квалифицированный сертификат ключа проверки электронной подписи
c) свидетельство проверки ключа электронной подписи
d) аккредитованный сертификат на проверку ключа электронной подписи
e) лицензированный сертификат ключа проверки электронной подписи

3.18 Сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи" и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи
a) квалифицированный сертификат ключа проверки электронной подписи
b) аккредитованный сертификат ключа проверки электронной подписи
c) усиленный сертификат ключа проверки электронной подписи
d) лицензированный сертификат на проверку ключа электронной подписи
e) сертификат ключа проверки электронной подписи

3.19 Уникальная последовательность символов, предназначенная для создания электронной подписи
a) ключ электронной подписи
b) пароль электронной подписи
c) код электронной подписи
d) PIN-код электронной подписи
e) сертификат электронной подписи
f) идентификатор электронной подписи

Тестовые задания с несколькими возможными правильными ответами:

3.20 Укажите режимы работы DES, при которых каждый блок шифруется отдельно, не взаимодействуя с другими блоками
a) ECB
b) OFB
c) CBC
d) CFB

3.21 Какие из перечисленных режимов работы DES используются для передачи по каналам связи с большим числом искажений
a) ECB
b) CBC
c) CFB
d) OFB

3.22 В каких режимах работы DES вырабатывается блочная гамма?
a) ECB
b) CBC
c) CFB
d) OFB

3.23 Неквалифицированной электронной подписью является электронная подпись, которая
a) получена в результате криптографического преобразования информации с использованием ключа электронной подписи
b) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания
c) позволяет определить лицо, подписавшее электронный документ
d) создается с использованием средств электронной подписи
e) посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом
f) имеет ключ проверки электронной подписи указан в квалифицированном сертификате

3.24 Квалифицированная электронная подпись соответствует следующим признакам:
a) имеет все признаки неквалифицированной электронной подписи
b) имеет все признаки простой электронной подписи

c) ключ проверки электронной подписи указан в квалифицированном сертификате
d) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом "Об электронной подписи" от 06.04.2011 N 63-ФЗ

3.25 Какие из перечисленных утверждений являются верными?
a) криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа
b) криптостойкость обеспечивается не секретностью ключа ,а секретностью алгоритма шифрования.
c) криптостойкость шифра противостоять криптоанализу должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей
d) стоимость шифрования должна превышать стоимость закрываемой информации как минимум в 2 раза
e) надежный шифртекст должен более чем на 10% превосходить по объему исходную информацию

3.26 Выберите верные утверждения
a) Симметричное шифрование имеет высокую скорость шифрования, но сложно в реализации
b) Симметричное шифрование применимо для шифрования данных произвольной длины
c) При симметричном шифровании передача секретного ключа может быть осуществлена по общедоступным каналам связи
d) Проблема распределения ключей шифрования между пользователями присутствует только для асимметричного шифрования

Тестовые задания открытой формы:

3.27 Распространение влияния одного знака открытого текста на много знаков шифртекста, что позволяет скрыть статистические свойства открытого текста называется _____

3.28 _____ - предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текстов

3.29 Проявление зависимости всех выходных битов шифротекста от каждого входного бита открытого текста называется _____ эффектом

Тестовые задания на установление соответствия

3.30 Установите соответствие между типами криптосистем и видами криптографических преобразований

1) бесключевые	a) хеширование
2) одноключевые	b) симметричное шифрование
3) двухключевые	c) асимметричное шифрование

3.31 Установите соответствие стандартов шифрования и количества используемых в них раундов шифрования

1) AES128	a) 10 раундов
2) AES192	b) 12 раундов
3) AES256	c) 14 раундов
4) DES	d) 16 раундов
5) 3DES	e) 24 раунда
	f) 48 раундов

2. Идентификация, аутентификация и управление доступом

Тестовые задания с выбором единственного правильного ответа

4.1 Название атаки на протоколы аутентификации, при которой злоумышленник участвует в процессе аутентификационного обмена между двумя сторонами с целью модификации проходящего через него трафика:
a) маскарад
b) подмена стороны аутентификационного обмена
c) принудительная задержка
d) атака с выборкой текста
e) повторная передача

4.2 EEPROM, входящая в USB-токен, предназначена для
a) управления и обработки данных
b) реализации криптографических алгоритмов
c) обеспечения интерфейса с USB-портом компьютера
d) хранения изменяемых данных
e) хранения ключей шифрования, паролей, сертификатов и других важных данных
f) хранения команд и констант

4.3 Разложение матрицы доступа по строкам позволяет получить
a) мандаты возможностей
b) домены безопасности
c) мандаты полномочий
d) списки прав доступа
e) домены прав доступа

Тестовые задания с несколькими возможными правильными ответами:

4.4 Выберите процессы аутентификации, основанные на знании чего-либо:

a) использование USB-токена
b) ввод пароля
c) ввод PIN-кода для USB-токена
d) считывание данных со смарт-карты
e) сканирование отпечатков пальцев
f) сканирование сетчатки глаза

4.5 Выберите процессы аутентификации, основанные на обладании чем-либо

a) использование USB-токена
b) ввод пароля
c) ввод PIN-кода для USB-токена
d) считывание данных со смарт-карты
e) сканирование отпечатков пальцев
f) сканирование сетчатки глаза

Тестовые задания открытой формы:

4.6 Процедура распознавания пользователя по его идентификатору, присвоенному данному пользователю ранее и занесенному в базу данных в момент его регистрации в качестве легального пользователя системы называется _____

4.7 Процедура проверки подлинности входящего в систему объекта (пользователя, процесса или устройства), предъявившего свой идентификатор называется _____

4.8 Процедура предоставления пользователю (процессу или устройству) определенных прав доступа к ресурсам системы после успешного прохождения им процедуры аутентификации называется _____

4.9 Процесс управления доступом пользователей к ресурсам системы называется _____

4.10 Название атаки на протоколы аутентификации, в которой пользователь пытается выдать себя за другого с целью получения полномочий и возможности действий от лица другого пользователя _____

4.11 Вычислите вероятность (в %) угадывания PIN-кода, если он состоит из 5 цифр и количество попыток ввода равно 5. Ответ напишите БЕЗ знака процента _____

3. Обеспечение безопасности информации в операционных системах

Тестовые задания с выбором единственного правильного ответа

5.1 Средство защиты ОС Windows, отвечающее за параметры безопасности, настройку административных задач, резервное копирование, разрешения проблем, диагностики и обновления ОС

a) Action Center
b) PowerShell 2
c) User Account Control
d) Windows Filtering Platform
e) Windows Firewall

5.2 Средство защиты, используемое в ОС Windows для снижения риска установки вредоносным ПО нежелательной программы или внесения опасных изменений в систему.

a) User Account Control
b) PowerShell
c) Action Center
d) Windows Filtering Platform
e) Windows Filrewall

5.3 Какой из типов UAC установлен по умолчанию в ОС Windows?

a) «Уведомлять при установке программ или попытке внесения ими изменений, а также при изменении параметров Windows пользователем»
b) «Уведомлять при установке программ или попытке внесения ими изменений»
c) «Уведомлять при попытке установки программ или попытке внесения ими изменений (не затемнять рабочий стол)»
d) «Не уведомлять ни при установке программ или попытке внесения ими изменений, ни при изменении параметров Windows пользователем»
e) «Уведомлять при удалении программ или попытке внесения в них изменений»

5.4 Набор интерфейсов прикладного программирования (API), с помощью которой разработчики могут использовать эту платформу для интеграции отдельных компонентов брандмауэра Windows Firewall в свои приложения

a) Windows Filtering Platform (WFP)
b) Windows Firewall
c) Action Center
d) PowerShell
e) User Account Control

5.5 При избирательном разграничении доступа данное понятие определяет набор объектов и типов операций, которые могут производиться над каждым объектом операционной системы

a) матрица доступа
b) домен безопасности

c) матрица мандатов
d) домен полномочий
e) домен доступа

5.6 Разложение матрицы доступа по столбцам позволяет получить
a) домены безопасности
b) списки прав доступа
c) мандаты возможностей
d) мандаты полномочий
e) мандаты привилегий

Тестовые задания с несколькими возможными правильными ответами:

3.7 Выберите верные утверждения, касающиеся требований к аудиту событий в ОС
a) Добавлять записи в журнал аудита может операционная система и администратор
b) Редактировать или удалять отдельные записи в журнале аудита не может ни один субъект доступа, кроме самой ОС
c) Просматривать журнал аудита могут только пользователи, обладающие соответствующей привилегией
d) Очищать журнал аудита могут только пользователи-аудиторы
e) Операционная система не должна поддерживать возможность сохранения журнала аудита перед очисткой в другом файле

Тестовые задания открытой формы:

5.8 Любой элемент операционной системы, доступ к которому пользователей и других субъектов доступа может быть произвольно ограничен (если ответ состоит из больше чем одного слова, напишите слова через пробел) называется _____

5.9 Пользователь, обладающий правом чтения журнала безопасности операционной системы называется _____

5.10 Совокупность правил, определяющих то, какие события должны регистрироваться в журнале безопасности называется _____

5.11 Короткие однострочные команды для управления различными параметрами системы, в том числе настройками безопасности групповой политики называется _____

5.12 Технология шифрования всей информации, размещенной на жестком диске для защиты от утечки данных называется _____

5.13 Любая сущность, способная инициировать выполнение операций над объектами (обращаться к объектам по некоторым методам доступа) называется _____

5.14 Встраиваемый компонент, обеспечивающий защиту целостности данных при использовании технологии шифрования BitLocker называется _____

4. Средства антивирусной защиты (САВЗ)

Тестовые задания с выбором единственного правильного ответа

6.1 Вредоносная программа, использующая для создания своих копий на других компьютерах сетевые ресурсы и сервисы, называется:
a) спуфер
b) троянская программа
c) червь
d) эксплоит
e) бэкдор

6.2 Вредоносная программа, реализующая несанкционированные действия, направленные на нарушение безопасности ИС, без создания собственных копий, называется
a) вредоносной утилитой
b) бэкдором
c) троянской программой
d) сетевым червем
e) флудером

6.3 Метод обнаружения вредоносных программ, суть которого заключается в поиске участков кода исполняемого объекта, отвечающих за конкретные вредоносные действия, называется
a) комплексным анализом
b) методом точного поиска
c) эвристическим анализом
d) сигнатурным анализом
e) методом эмуляции кода

6.4 Запуск с ограниченными полномочиями заключается в:
a) перехвате запросов исследуемой программы на запись
b) перехвате и анализе всей активности программы
c) запуске в выделенной среде с ограничением, например, прав доступа
d) запуске исследуемой программы в среде эмуляции

6.5 В тесте скорости реакции САВЗ оценивается время между:
a) посещением «зараженных» сайтов сети Интернет и срабатыванием САВЗ
b) помещением в систему вредоносных программ и срабатыванием САВЗ

c) появлением новых вредоносных программ и добавлением поставщиком новых сигнатур в базу САВЗ
d) запуском в системе вредоносных программ и срабатыванием САВЗ

Тестовые задания с несколькими возможными правильными ответами:

6.6 Укажите все действия, включаемые в понятие антивирусной защиты, согласно методическим документам ФСТЭК, содержащих профили защиты САВЗ:
a) препятствование «заражению» объектов в ИС
b) обнаружение вредоносных компьютерных программ
c) изолирование вредоносных компьютерных программ
d) удаление «зараженных» объектов
e) блокирование "зараженных" объектов

6.7 Среди перечисленных пунктов выберите действия, для совершения которых должна быть заведомо предназначена программа, чтобы считаться вредоносной (согласно определению вредоносной программы из Уголовного кодекса РФ)
a) несанкционированное распространение информации
b) несанкционированное уничтожение информации
c) поиск уязвимостей в ИС
d) вывод из строя компонентов ИС
e) нейтрализация средств защиты компьютерной информации

6.8 Укажите все виды вредоносных программ, относящихся к категории троянских программ:
a) спуфер
b) бэкдор
c) флудер
d) руткит
e) эксплоит

6.9 Укажите все свойства сигнатурного анализа, которые можно отнести к его недостаткам:
a) склонен к большому количеству ложных срабатываний
b) требует значительных усилий по обновлению баз сигнатур
c) при успешном определении, лечение «зараженного» объекта часто невозможно
d) не позволяет обнаруживать новые вредоносные программы
e) склонен к большому количеству пропусков вредоносных программ

6.10 Укажите все тесты САВЗ, результаты которых являются информативными при выборе САВЗ для нового персонального компьютера, не имеющего доступ к сети Интернет
a) динамическое тестирование
b) статическое тестирование
c) тест в экстремальных условиях
d) ретроспективный тест

5. Обеспечение безопасности информации в компьютерных сетях

Тестовые задания с выбором единственного правильного ответа

6.11 Основным протоколом уровня межсетевого взаимодействия стека протоколов TCP/IP является
a) протокол IP
b) протокол TCP
c) протокол UDP
d) протокол HTTP
e) протокол ICMP

6.12 Какое из перечисленных сетевых устройств может выполнять функции фаервола?
a) концентратор
b) коммутатор
c) маршрутизатор
d) ретранслятор
e) коммутатор 3 уровня

6.13 Как называют межсетевые экраны, в основу работы которых положена технология фильтрации трафика с контролем состояния соединения?
a) МЭ экспертного уровня
b) МЭ прикладного уровня
c) МЭ сеансового уровня
d) пакетные фильтры
e) экранирующие шлюзы

6.14 Какая функция межсетевого экрана позволяет скрывать топологию внутренней сети от внешних пользователей?
a) кэширование
b) трансляция сетевых адресов
c) идентификация
d) аутентификация
e) администрирование

6.15 Какой вид МЭ дополняет экранирующий маршрутизатор функциями контроля виртуальных соединений и трансляции внутренних IP-адресов?

	a) шлюз сеансового уровня b) экранирующий маршрутизатор c) экранирующий шлюз d) пакетный фильтр e) прикладной шлюз 6.16 Протокол SSL используется для защиты информационного обмена на a) сеансовом уровне b) прикладном уровне c) транспортном уровне d) сетевом уровне *Тестовые задания с несколькими возможными правильными ответами:* 6.17 Какие заголовки пакетов анализирует экранирующий маршрутизатор? a) IP b) TCP c) UDP d) Ethernet e) HTTP 6.18 Выберите утверждения, которые верны для прикладного уровня модели OSI a) обеспечивает удаленный доступ к файлам и базам данных b) обеспечивает пересылку данных по электронной почте c) обеспечивает преобразование протоколов и кодирование/декодирование данных d) обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время e) обеспечивает надёжную передачу данных от отправителя к получателю 6.19 Выберите верное утверждение a) Биты в сетевой части адреса должны быть одинаковыми для всех устройств, которые находятся в одной и той же сети b) Биты в узловой части адреса должны быть уникальными, чтобы можно было определить конкретный узел в сети c) Биты в сетевой части адреса должны отличаться на конкретное значение для всех устройств, которые находятся в одной и той же сети d) Биты в узловой части адреса должны быть одинаковыми, чтобы можно было определить конкретный узел в сети e) Биты в узловой и сетевой части адреса должны совпадать, чтобы можно было определить конкретный узел в сети 6.20 На каких уровнях модели OSI формируются виртуальные защищенные каналы передачи данных? a) сеансовый b) канальный c) сетевой d) прикладной e) представления *Тестовые задания открытой формы:* 6.21 Какие программы-посредники ориентированы на анализ потока сообщений только для определенных видов сервиса? _____ 6.22 Какие из программ-посредников обрабатывают весь поток сообщений? _____ 6.23 На каком уровне модели OSI преимущественно функционирует экранирующий маршрутизатор? _____ 6.24 Какой протокол реализует удаленный доступ к файлу, предоставляет возможность интерактивной работы с удаленной машиной с механизмом аутентификации? _____
Критерии оценки и шкала оценивания в баллах	При количестве правильных ответов: 8-10 – 2 балла, 5-7 – 1 балл, 0-4 – 0 баллов.
Наименование оценочного средства	**Отчет по лабораторной работе (ОЛР)**
Представление и содержание оценочных материалов	Задания представлены в методических указаниях к лабораторным работам.
Критерии оценки и шкала оценивания в баллах	Оценивается по шкале «зачтено-не зачтено» «Зачтено» - 2 балла «Не зачтено» - 0 баллов Работа засчитывается при условии: 1. Оформления отчета по лабораторной работе согласно требованиям, установленным в

	методических указаниях 2. Описания результатов выполнения поставленных задач с прикреплением подтверждающих скриншотов, расчетов, таблиц, диаграмм, файлов 3. Наличия ответов на контрольные вопросы по тематике лабораторной работы
Наименование оценочного средства	**Доклад с презентацией (ДП)**
Представление и содержание оценочных материалов	В рамках данного задания необходимо подготовить доклад в виде информационных блоков, которые будут затрагивать различные аспекты правового регулирования информации с ограниченным доступом. Каждый учащийся выбирают отдельный вид информации с ограниченным доступом согласно своему варианту (например, по списку в журнале группы). Для выбранного вида информации с ограниченным доступом составляются ответы по следующим пунктам: 1. Перечень законодательных актов и нормативно-правовых норм, регулирующих взаимоотношения, связанных с выбранным видом информации с ограниченным доступом 2. Термины и определения, касающиеся выбранного вида информации с ограниченным доступом 3. Порядок предоставления доступа (оформление допуска) к выбранному виду информации с ограниченным доступом 4. Наличие ограничений и льгот (социальных гарантий), предписываемых лицам, имеющих доступ к выбранному виду информации с ограниченным доступом. 5. Юридическая ответственность за правонарушения, связанные с разглашением сведений, относящихся к выбранному виду информации с ограниченным доступом: - уголовная ответственность - административная ответственность - гражданско-правовая ответственность - дисциплинарная ответственность В данном пункте необходимо привести один пример из судебной практики. Темы докладов по практическому занятию «Изучение видов информации, доступ к которым ограничен федеральными законами РФ» 1. Сведения, составляющие государственную тайну. Юридическая ответственность за правонарушения, связанные с разглашением сведений, содержащих государственную тайну. 2. Сведения, составляющие коммерческую тайну. Юридическая ответственность за правонарушения, связанные с разглашением сведений, содержащих коммерческую тайну. 3. Требования к защите персональных данных (ПДн) при их обработке в информационных системах персональных данных. Юридическая ответственность за правонарушения, связанные с разглашением ПДн. 4. Сведения, составляющие служебную тайну. Юридическая ответственность за правонарушения, связанные с разглашением сведений, содержащих служебную тайну. 5. Сведения, составляющие налоговую тайну. Юридическая ответственность за правонарушения, связанные с разглашением сведений, содержащих налоговую тайну. 6. Сведения, составляющие тайну предварительного расследования (тайна следствия). Юридическая ответственность за правонарушения, связанные с разглашением тайны следствия. 7. Сведения, составляющие банковскую тайну. Юридическая ответственность за правонарушения, связанные с разглашением банковской тайны. 8. Сведения, составляющие адвокатскую тайну. Юридическая ответственность за правонарушения, связанные с разглашением банковской тайны 9. Сведения, составляющие тайну связи. Юридическая ответственность за правонарушения, связанные с разглашением тайну связи 10. Сведения, составляющие врачебную тайну. Юридическая ответственность за правонарушения, связанные с разглашением врачебной тайны. 11. Сведения, составляющие аудиторскую тайну. Юридическая ответственность за правонарушения, связанные с разглашением аудиторской тайны.
Критерии оценки и шкала оценивания в баллах	Оцениваются следующие аспекты работы студента: 1. качество оформления презентации для доклада (требования по оформлению презентации указаны ниже в разделе «Практические занятия»): - оформление презентации полностью соответствует требованиям – 2 балла; - требования по оформлению презентации частично не выполнены – 1 балл; - оформление презентации не соответствует требованиям – 0 баллов; 2. знание материала: - содержание материала раскрыто в полном объеме, предусмотренном программой дисциплины – 2 балла; - содержание материала раскрыто неполно, показано общее понимание вопроса, достаточное для дальнейшего изучения программного материала – 1 балл; - не раскрыто основное содержание учебного материала – 0 баллов;

	3. Последовательность изложения: - содержание материала раскрыто последовательно, достаточно хорошо продумано – 2 балла; - последовательность изложения материала недостаточно продумана – 1 балл; - путаница в изложении материала – 0 баллов; 4. Владение речью и терминологией: - материал изложен грамотным языком, с точным использованием терминологии – 2 балла; - в изложении материала имелись затруднения и допущены ошибки в определении понятий и в использовании терминологии – 1 балл; - допущены ошибки в определении понятий – 0 баллов; 5. Применение конкретных примеров: - показано умение иллюстрировать материал конкретными примерами – 2 балла; - приведение примеров вызывает затруднение – 1 балл; - неумение приводить примеры при объяснении материала – 0 баллов. Итоговая оценка выставляется по шкале «зачтено-не зачтено» «Зачтено (2 балла)» - 6-10 баллов «Не зачтено (0 баллов)» - 0-5 баллов
Наименование оценочного средства	**Отчет по практической работе (ОПР)**
Представление и содержание оценочных материалов	Задания представлены в методических указаниях к практическим работам.
Критерии оценки и шкала оценивания в баллах	Оценивается по шкале «зачтено-не зачтено» «Зачтено» - 2 балла «Не зачтено» - 0 баллов Работа засчитывается при условии: 1. Оформления отчета по практической работе согласно требованиям, установленным в методических указаниях 2. Описания результатов выполнения поставленных задач с прикреплением подтверждающих скриншотов, расчетов, таблиц, диаграмм, файлов Наличия ответов на контрольные вопросы по тематике практической работы

4. Оценочные материалы промежуточной аттестации

Наименование оценочного средства	**Экзамен в форме компьютерного тестирования**
Представление и содержание оценочных материалов	Студент авторизуется на площадке LMS Moodle, выбирает курс, созданный для освоения данной дисциплины. Курс содержит банк тестовых заданий (БТЗ) из 200 вопросов, включающих теоретические вопросы и практические задачи. Итоговый тест разделен на две части: теоретическую и практическую. Теоретическая часть содержит 60 теоретических вопросов, выбираемых случайным образом из БТЗ, охватывающих все разделы дисциплины. Время выполнения теоретической части теста составляет 40 минут. Практическая часть состоит из 10 практических заданий, выбираемых случайным образом из БТЗ. Время выполнения практической части теста составляет 40 минут. Примеры практических заданий: 1. Дано: - допустимая вероятность подбора пароля злоумышленником 0,0277972 - скорость подбора пароля злоумышленником 493 паролей(-я) в минуту - срок действия пароля 17 дней(-я) - мощность алфавита пароля 49 символов Найти длину пароля, соответствующую заданным условиям. 2. Дано: - допустимая вероятность подбора пароля злоумышленником 0,0000148 - скорость подбора пароля злоумышленником 493 паролей(-ля,-ль) в минуту - срок действия пароля 1 недель(-я, -и) - мощность алфавита пароля 49 символов Найти: - длину пароля, соответствующую заданным условиям.

	Ответ должен быть целым числом. 3. Дан зашифрованный текст "бшъуэтъвчьттйд" Какое ключевое слово было использовано, если исходный текст "аутентификация". 4. Алиса передала Бобу открытый ключ (7,143). Боб ответил Алисе зашифрованным сообщением "135". Ева перехватила сообщение и произвела на него успешную атаку. Напишите в качестве ответа исходное сообщение Боба (число без кавычек). 5. Боб получил от Алисы три числа: p = 19, g = 5, A = 6. Боб выбрал свой закрытый ключ b = 7 и отправил Алисе открытый ключ B, а также рассчитал общий секретный ключ K. Рассчитайте B и K. Ответ запишите без пробелов числами через запятую в формате: B,K
Критерии оценки и шкала оценивания в баллах	По результатам компьютерного тестирования выставляется максимально 40 баллов: 30 баллов за теоретическую часть (0,5 балла за правильный ответ на 1 задание), 10 баллов за практическую часть (1 балл за правильный ответ на 1 задание). Итоговая оценка по дисциплине представляет собой сумму из баллов, полученных в течении семестра и баллов, полученных на компьютерном тестировании.
Наименование оценочного средства	**Экзамен в форме устного собеседования**
Представление и содержание оценочных материалов	Оценочные материалы, вынесенные на экзамен, состоят из экзаменационных билетов. Примеры экзаменационных билетов. Вопросы для базового уровня 1. Основные понятия информационной безопасности и защиты информации 2. Угрозы информационной безопасности 3. Угрозы и уязвимости беспроводных сетей 4. Основные понятия политики безопасности 5. Структура политики безопасности организации 6. Роль стандартов информационной безопасности 7. Симметричные криптосистемы шифрования 8. Основные режимы работы блочного симметричного алгоритма 9. Особенности применения алгоритмов симметричного шифрования 10. Асимметричные криптосистемы шифрования 11. Функции хэширования 12. Электронная цифровая подпись 13. Управление криптоключами 14. Аутентификация, авторизация и администрирование действий пользователей 15. Комбинированные системы идентификации и аутентификации Вопросы для продвинутого уровня 1. Основные понятия информационной безопасности и защиты информации 2. Угрозы информационной безопасности 3. Характерные особенности сетевых атак 4. Угрозы и уязвимости беспроводных сетей 5. Обеспечение информационной безопасности компьютерных систем 6. Основные понятия политики безопасности 7. Структура политики безопасности организации 8. Разработка политики безопасности организации 9. Роль стандартов информационной безопасности 10. Международные стандарты информационной безопасности 11. Отечественные стандарты безопасности информационных технологий 12. Основные понятия криптографической защиты информации 13. Симметричные криптосистемы шифрования 14. Алгоритмы шифрования DES и 3-DES 15. Стандарт шифрования ГОСТ 28147-89: суть, режимы работы 16. Стандарт шифрования AES 17. Основные режимы работы блочного симметричного алгоритма 18. Особенности применения алгоритмов симметричного шифрования 19. Асимметричные криптосистемы шифрования 20. Алгоритм шифрования RSA 21. Ассиметричные криптосистемы на базе эллиптических кривых. Алгоритм ассиметричного шифрования ECES 22. Функции хэширования. Отечественный стандарт хэширования ГОСТ Р34.11-94 23. Электронная цифровая подпись. Основные процедуры цифровой подписи,

	24. Алгоритм цифровой подписи DSA. Алгоритм цифровой подписи ECDSA 25. Алгоритм цифровой подписи ГОСТ Р 34.10-94. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001 26. Управление криптоключами: использование комбинированной криптосистемы, метод распределения ключей Диффи-Хеллмана 27. Инфраструктура управления открытыми ключами PKI: принцип функционирования PKI, логическая структура и компоненты PKI 28. Аутентификация, авторизация и администрирование действий пользователей 29. Методы аутентификации, использующие пароли: аутентификация на основе многоразовых паролей, аутентификация на основе одноразовых паролей 30. Строгая аутентификация: основные понятия, применение электронных идентификаторов 31. Криптографические протоколы строгой аутентификации 32. Биометрическая аутентификация пользователя: дактилоскопические системы аутентификации, системы аутентификации по лицу и голосу, системы аутентификации по узору радужной оболочки и сетчатки глаз, области применения биометрических систем, биометрические идентификаторы 33. Комбинированные системы идентификации и аутентификации: радиочастотные идентификаторы и USB-ключи, гибридные смарт-карты, биоэлектронные системы. Электронные замки 34. Управление идентификацией и доступом 35. Вредоносные программы и проблемы антивирусной защиты: компьютерные вирусы, жизненный цикл вирусов, сетевые черви, троянские программы, другие вредоносные программы и нежелательная корреспонденция 36. Основные каналы распространения вредоносных программ 37. Антивирусные программы: основы работы антивирусных программ, особенности «облачной» антивирусной технологии, виды антивирусных программ, дополнительные модули антивирусных программ, режимы работы антивируса Вопросы для высокого уровня 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. 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 преимущество 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?
Критерии оценки и шкала оценивания в баллах	Студент выбирает билет, содержащий 3 вопроса из базового и продвинутого уровня, вопросы высокого уровня задаются дополнительно (устно при собеседовании). Билеты формируются преподавателем перед зачетно-экзаменационной сессией. По результатам ответов на промежуточной аттестации выставляется максимально 40 баллов: при полном ответе на вопрос базового уровня – 10 баллов, базового и продвинутого – 25 баллов; базового, продвинутого и высокого – 40 баллов. В случае неполных ответов по билету или спорной оценки задаются дополнительные вопросы из общего списка (вне зависимости от уровня освоения) по усмотрению преподавателя. Итоговая оценка по дисциплине представляет собой сумму из баллов, полученных в течении семестра и баллов полученных на промежуточной аттестации. Шкала оценивания результатов «удовлетворительно»: 55-69 баллов «хорошо»: 70-84 баллов «отлично»: 85-100 баллов

Фонд оценочных средств по дисциплине «Информационная безопасность» разработан в соответствии с требованиями ФГОС ВО по направлению подготовки бакалавров 09.03.03 Прикладная информатика, с учетом профессиональных стандартов 06.015 Специалист по информационным системам

Автор
Доцент кафедры ИИУС _____ И.Р. Исмагилов
(подпись, дата)

Фонд оценочных средств обсужден и одобрен на заседании кафедры ИИУС от «26» октября 2020 г., протокол № 24

Зав. кафедрой ИИУС _____ Ю.В. Торкунова
(подпись, дата)

Одобрен на заседании методического совета института ИЦТЭ от «26» октября 2020, протокол № 2

Зам. директора ИЦТЭ _____ В.В. Косулин
(подпись, дата)

Принят решением Ученого совета ИЦТЭ от «26» октября 2020, протокол № 2

Согласовано:

Зав. кафедрой ИИУС _____ Ю.В. Торкунова
(подпись, дата)