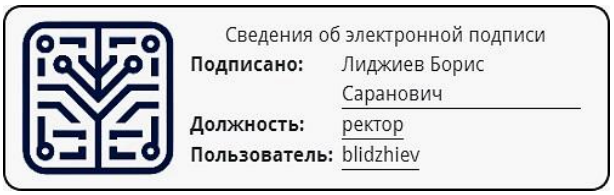
Автономная некоммерческая организация высшего образования
«Информационно-технологический университет»
(АНО ВО ИТУ)

УТВЕРЖДАЮ

Ректор АНО ВО ИТУ Лиджиев Б.С.



«04» июня 2024 г.

Б1.О.04 МОДУЛЬ ОБЩЕПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04.15 ЗАЩИТА ИНФОРМАЦИИ

Для направления подготовки:
09.03.01 Информатика и вычислительная техника
(уровень бакалавриата)

Типы задач профессиональной деятельности:
производственно-технологический

Направленность (профиль):
Информационные системы

Форма обучения:
очная, очно-заочная, заочная

г. Элиста, 2024

Разработчик: Горяев Владимир Михайлович, кандидат педагогических наук, заведующий кафедрой Математики и информационных технологий Автономной некоммерческой организации высшего образования «Информационно-технологический университет».

Рабочая программа разработана в соответствии с требованиями ФГОС ВО 09.03.01 Информатика и вычислительная техника (уровень бакалавриата), утв. Приказом Министерства образования и науки РФ № 929 от 19.09.2017 г.

СОГЛАСОВАНО:
Заведующий кафедрой
Математики и информационных технологий
АНО ВО ИТУ
канд. пед. наук, доцент Горяев В.М.

Протокол заседания кафедры № 01 от «04» июня 2024 г.

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель освоения дисциплины: формирование у обучающихся теоретических знаний и практических навыков применения методов и средств защиты информации в профессиональной деятельности.

Задачи:

– формирование системы знаний в сфере источников угроз безопасности информации в компьютерной системе;

– формирование системы знаний в сфере юридических основ правового обеспечения безопасности компьютерных систем;

– формирование системы знаний о технических и программных средствах обеспечения безопасности компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Место дисциплины в учебном плане:

Блок: Блок 1. Дисциплины (модули).

Часть: Обязательная часть.

Модуль: модуль общепрофессиональной подготовки.

Осваивается (семестр):

очная форма обучения – 6

очно-заочная форма обучения – 7

заочная форма обучения - 7

3. КОМПЕТЕНЦИИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК-2 - способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.

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.

4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМСЯ

Код и наименование компетенции	Индикаторы достижения компетенции	Результаты обучения
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**УК-2.2.** Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов

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-3.2**. Самостоятельно проводит научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знает:** методологию проведения научно-исследовательской работы **Умеет:** самостоятельно проводить научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **Владеет:** навыками самостоятельного проведения научно-исследовательской работы

5. ОБЪЕМ ДИСЦИПЛИНЫ И РАСПРЕДЕЛЕНИЕ ВИДОВ УЧЕБНОЙ РАБОТЫ ПО СЕМЕСТРАМ

Общая трудоемкость дисциплины «Защита информации» для студентов всех форм обучения, реализуемых в АНО ВО ИТУ по направлению подготовки 09.03.01 Информатика и вычислительная техника составляет: 4 з.е. / 144 час.

Вид учебной работы	Всего число часов и (или) зачетных единиц (по формам обучения)		
	Очная	Очно-заочная	Заочная
Аудиторные занятия	54	30	12
в том числе:			
Лекции	18	10	4
Практические занятия	36	20	8
Лабораторные работы	-	-	-
Самостоятельная работа	54	78	123
в том числе:			
часы на выполнение КР / КП	-	-	-
Промежуточная аттестация:			
Вид	Экзамен – 6 сем.	Экзамен – 7 сем.	Экзамен – 7 сем.
Трудоемкость (час.)	36	36	9
Общая трудоемкость з.е. / час.	**4 з.е. / 144 час.**		

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№	Наименование темы дисциплины	Лекции	Практические занятия	Лабораторные работы	Самост. работа *(в т.ч. КР / КП)*
Очная форма обучения					
1	Введение в информационную безопасность	3	7		10
2	Организационно-правовое обеспечение защиты информации	3	7		11
3	Методы и средства технической защиты информации	3	7		11

№	Наименование темы дисциплины	Лекции	Практические занятия	Лабораторные работы	Самост. работа *(в т.ч. КР / КП)*
4	Программно-технические средства защиты информации	4	7		11
5	Криптографические средства защиты информации	4	8		11
	Итого (часов)	18	36		54
	Форма контроля:	**Экзамен**			**36**
Очно-заочная форма обучения					
1	Введение в информационную безопасность	2	4		15
2	Организационно-правовое обеспечение защиты информации	2	4		15
3	Методы и средства технической защиты информации	2	4		16
4	Программно-технические средства защиты информации	2	4		16
5	Криптографические средства защиты информации	2	4		16
	Итого (часов)	10	20		78
	Форма контроля:	**Экзамен**			**36**
Заочная форма обучения					
1	Введение в информационную безопасность	0,5	1		24
2	Организационно-правовое обеспечение защиты информации	0,5	1		24
3	Методы и средства технической защиты информации	1	2		25
4	Программно-технические средства защиты информации	1	2		25
5	Криптографические средства защиты информации	1	2		25
	Итого (часов)	4	8		123
	Форма контроля:	**Экзамен**			**9**
	Всего по дисциплине:	**4 з.е. / 144 час.**			

СОДЕРЖАНИЕ ТЕМ ДИСЦИПЛИНЫ

Тема 1. Введение в информационную безопасность

Особенности обеспечения информационной безопасности Российской Федерации (роль и место информационной безопасности в общей системе национальной безопасности РФ. Основные цель и задачи обеспечения информационной безопасности РФ. Объекты информационной безопасности РФ. Внешние и внутренние источники угроз информационной безопасности в РФ).

Информация как объект защиты (определение, виды и источники информации, подлежащей защите. Информация как объект права собственности. Виды защищаемой информации. Угрозы и возможные каналы утечки конфиденциальной информации. Обзор способов реализации угроз информации. Анализ моделей нарушителя. Категории потенциальных нарушителей).

Анализ существующих подходов к обеспечению безопасности информации (особенности современных информационных систем, существенные с точки зрения безопасности. Законодательный, административный и процедурный уровни информационной безопасности. Основные понятия политики безопасности. Структура политики безопасности организации. Программно-технический уровень информационной безопасности. Сервисы безопасности. Место сервисов безопасности в архитектуре информационных систем)

Тема 2. Организационно-правовое обеспечение защиты информации

Международные и отечественные стандарты в сфере защиты информации (роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты для беспроводных сетей. Стандарты информационной безопасности в Интернет. Отечественные стандарты безопасности информационных технологий).

Сертификация и аттестация в области защиты информации (назначение и общая характеристика. Проведение сертификационных испытаний. Аттестация объектов информатизации. Сертификация на региональном и международном уровнях).

Организационные меры по защите информации (концепция безопасности предприятия и ее содержание. Политика информационной безопасности предприятия. Назначение, содержание и структура политики безопасности. Служба безопасности предприятия).

Основы правового обеспечения защиты информации (международный опыт правового обеспечения информационной безопасности. Государственная система правового обеспечения информационной безопасности. Содержание основных законов РФ в области информационной безопасности. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации)

Тема 3. Методы и средства технической защиты информации

Виды и методы технической защиты информации (пассивные и активные методы защиты информации. Средства технической защиты информации. Защита помещений. Системы охранной сигнализации на территории и в помещениях. Системы видеонаблюдения. Системы контроля доступа. Системы контроля вскрытия аппаратуры).

Технические каналы утечки информации (общая характеристика технических каналов утечки информации и их классификация. Каналы утечки речевой информации. Технические средства и методы получения информации по этим каналам. Утечка информации по проводным коммуникациям и за счет побочных электромагнитных излучений и наводок. Технические средства и методы получения информации с использованием этих каналов).

Методы и средства защиты информации от утечки по техническим каналам (основные методы, используемые при создании систем защиты информации. Заземление технических средств передачи информации. Использование сетевых фильтров. Экранирование помещений. Методы защиты от утечек по акустическим каналам. Защита средств связи и телекоммуникаций)

Тема 4. Программно-технические средства защиты информации

Защита информации от несанкционированного доступа (идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Идентификация и аутентификация субъектов “пользователь” и “процесс” при запросах на доступ к компьютерным ресурсам. Использование простого и динамически изменяющегося паролей. Биометрическая идентификация. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств. Разграничение доступа. Защита программных средств от несанкционированного копирования и модификации).

Защита от компьютерных вирусов (основные виды вирусов и схемы их функционирования. Основные каналы распространения вирусов и других вредоносных программ. Обнаружение вирусов и меры по защите и профилактике. Антивирусные программы и комплексы).

Технологии межсетевых экранов (функции межсетевых экранов. Фильтрация трафика. Выполнение функций посредничества. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Схемы сетевой защиты на базе

межсетевых экранов. Схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Обзор современных межсетевых экранов)

Тема 5. Криптографические средства защиты информации

Принципы криптографической защиты информации (основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированные криптосистемы шифрования. Электронная цифровая подпись и функция хэширования. Правовые аспекты применения электронной цифровой подписи).

Криптографические алгоритмы. Средства криптографиической защиты информации (классификация криптографических алгоритмов. Симметричные алгоритмы шифрования. Блочные алгоритмы шифрования. Асимметричные алгоритмы шифрования. Алгоритм шифрования RSA. Алгоритм Диффи-Хеллмана. Алгоритмы цифровой подписи. Средства криптографической защиты информации. Правовые основы разработки и использования средств криптографической защиты информации).

Компьютерная стеганография (принципы компьютерной стеганографии. Секретные средства связи и передачи информации. Методики стеганографии. Стегосистема. Контейнер. Стегоключ)

7. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ

Курсовая работа не предусмотрена

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ: Приложение 1.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

9.1. Рекомендуемая литература:

- Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html
- Никифоров, С. Н. Защита информации. Защита от внешних вторжений : учебное пособие / С. Н. Никифоров. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 84 c. — ISBN 978-5-9227-0757-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/74381.html
- Никифоров, С. Н. Защита информации. Пароли, скрытие, удаление данных : учебное пособие / С. Н. Никифоров, М. М. Ромаданов. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 108 c. — ISBN 978-5-9227-0783-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/80747.html
- Никифоров С.Н. Защита информации. Защищенные сети [Электронный ресурс] : учебное пособие / С.Н. Никифоров. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 80 c. — 978-5-9227-0762-6. — Режим доступа: http://www.iprbookshop.ru/74382

- Алексеев А.П. Многоуровневая защита информации [Электронный ресурс] / А.П. Алексеев. — Электрон. текстовые данные. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. — 128 c. — 978-5-904029-72-2. — Режим доступа: http://www.iprbookshop.ru/75387
- Корнеева Е.В. Программно-технические средства защиты информации. [Электронный ресурс]: рабочий учебник / Корнеева Е.В. - 2022. - http://libary.roweb.online
- Корнеева Е.В., Белянина Н.В. Криптографические средства защиты информации. [Электронный ресурс]: рабочий учебник / Корнеева Е.В., Белянина Н.В. - 2022. - http://libary.roweb.online

9.2. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень лицензионного и свободно распространяемого программного обеспечения.

АНО ВО ИТУ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства.

Программное обеспечение, необходимое для осуществления образовательного процесса по дисциплине:

Лицензионное программное обеспечение (в том числе, отечественного производства):

Операционная система Windows Professional 10;

ПО браузер – приложение операционной системы, предназначенное для просмотра Web-страниц;

Цифровой образовательный сервис «Личная студия обучающегося» (отечественное ПО);

Цифровой образовательный сервис «Личный кабинет преподавателя» (отечественное ПО);

Платформа проведения вебинаров (отечественное ПО);

Платформа проведения аттестационных процедур с использованием каналов связи (отечественное ПО).

Информационная технология. Программа управления образовательным процессом.

Свободно распространяемое программное обеспечение (в том числе отечественного производства):

Мой Офис Веб-редакторы https://edit.myoffice.ru (отечественное ПО);

ПО OpenOffice.Org Calc - http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html;

ПО OpenOffice.Org.Base http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html;

ПО OpenOffice.org.Impress
http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО OpenOffice.Org Writer
http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО Open Office.org Draw
http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО «Блокнот» - стандартное приложение операционной системы (MS Windows, Android и т.д.), предназначенное для работы с текстами.

9.3. Перечень современных профессиональных баз данных, информационных справочных систем и ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://window.edu.ru/ - единое окно доступа к образовательным ресурсам

2. http://www.iprbookshop.ru - Электронно-библиотечная система IPRbooks (ЭБС IPRbooks) –электронная библиотека по всем отраслям знаний
3. https://www.elibrary.ru/ - электронно-библиотечная система eLIBRARY.RU, крупнейшая в России электронная библиотека научных публикаций
4. http://www.consultant.ru/ - справочная правовая система КонсультантПлюс
5. https://www.garant.ru/ - справочная правовая система Гарант
6. https://gufo.me/ - справочная база энциклопедий и словарей
7. https://slovaronline.com - справочная база, полная поисковая система по всем доступным словарям, энциклопедиям и переводчикам в режиме Онлайн
8. Официальный сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет» https://reestr.digital.gov.ru/
9. Общество с ограниченной ответственностью «Интерактивные обучающие технологии» https://htmlacademy.ru/tutorial/php/mysql
10. Web-технологии https://htmlweb.ru/php/mysql.php
11. Справочно-правовая система «Консультант Плюс»

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для осуществления образовательного процесса по дисциплине представляют собой аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.

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

Список аудиторий:

1. Лекционная аудитория, аудитория для групповых и индивидуальных консультаций.

2. Аудитория для проведения практических и семинарских занятий, текущего контроля и промежуточной аттестации.

3. Аудитория для самостоятельной работы обучающихся.

4. Многофункциональная аудитория для лиц с ограниченными возможностями здоровья, актовый зал, электронная библиотека.

5. Аудитория информационных технологий.

11. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины проводится в форме лекций, практических и/или лабораторных занятий, организации самостоятельной работы студентов, консультаций. Главное назначение лекции - обеспечить теоретическую основу обучения, развить интерес к учебной деятельности и конкретной учебной дисциплине, сформировать у студентов ориентиры для самостоятельной работы над учебной дисциплиной.

Основной целью практических и/или лабораторных занятий является обсуждение наиболее сложных теоретических вопросов, их методологическая и методическая проработка, выполнение практических заданий.

Самостоятельная работа с учебной, учебно-методической и научной литературой, дополняется работой с тестирующими системами, тренинговыми программами, с

информационными базами, электронными образовательными ресурсами в электронной информационно-образовательной среде организации и сети Интернет.

Цель самостоятельной работы - подготовка современного компетентного специалиста и формирование способностей и навыков к непрерывному самообразованию и профессиональному совершенствованию.

Реализация поставленной цели предполагает решение следующих задач:

- качественное освоение теоретического материала по изучаемой дисциплине, углубление и расширение теоретических знаний с целью их применения на уровне межпредметных связей;
- систематизация и закрепление полученных теоретических знаний и практических навыков;
- формирование умений по поиску и использованию нормативной, правовой, справочной и специальной литературы, а также других источников информации;
- развитие познавательных способностей и активности, творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самообразованию, самосовершенствованию и самореализации;
- развитие научно-исследовательских навыков;
- формирование умения решать практические задачи (в профессиональной деятельности), используя приобретенные знания, способности и навыки.

Самостоятельная работа является неотъемлемой частью образовательного процесса.

Самостоятельная работа предполагает инициативу самого обучающегося в процессе сбора и усвоения информации, приобретения новых знаний, умений и навыков и ответственность его за планирование, реализацию и оценку результатов учебной деятельности. Процесс освоения знаниями при самостоятельной работе не обособлен от других форм обучения.

Самостоятельная работа по подготовке письменных работ должна:

- быть выполнена индивидуально (или являться частью коллективной работы);
- представлять собой законченную разработку (этап разработки), в которой анализируются актуальные проблемы по определенной теме и ее отдельных аспектов;
- отражать необходимую и достаточную компетентность автора;
- иметь учебную, научную и/или практическую направленность;
- быть оформлена структурно и логически последовательно;
- содержать краткие и четкие формулировки, убедительную аргументацию, доказательность и обоснованность выводов;
- соответствовать этическим нормам (правила цитирования и парафраз; ссылки на использованные библиографические источники; исключение плагиата, дублирования собственного текста и использования чужих работ).

Особенности организации образовательного процесса для обучающихся с ограниченными возможностями здоровья

Обучающиеся с ограниченными возможностями здоровья (далее ОВЗ) имеют свои специфические особенности восприятия и переработки учебного материала. Подбор и разработка учебных материалов должны производиться с учетом того, чтобы предоставлять этот материал в различных формах так, чтобы инвалиды с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально.

Выбор средств и методов обучения осуществляется самим преподавателям. При этом в образовательном процессе рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений обучающихся

с ограниченными возможностями здоровья с научно-педагогическими работниками и другими обучающимися, создания комфортного психологического климата при освоении учебного материала.

Лица с ограниченными возможностями здоровья по зрению имеют право присутствовать на занятиях вместе с ассистентом, оказывающим обучающемуся необходимую помощь; лица с ограниченными возможностями здоровья по слуху имеют право на использование звукоусиливающей аппаратуры.

При проведении промежуточной аттестации по дисциплине обеспечивается соблюдение следующих общих требований:

- проведение аттестации для лиц с ОВЗ в одной аудитории совместно с обучающимися, не имеющими ОВЗ, если это не создает трудностей для лиц с ОВЗ и иных обучающихся при прохождении аттестации;
- присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся с ОВЗ необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с экзаменатором);
- пользование необходимыми обучающимся с ОВЗ техническими средствами при прохождении аттестации с учетом их индивидуальных особенностей;
- обеспечение возможности беспрепятственного доступа обучающихся с ОВЗ в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях.

По письменному заявлению обучающегося с ОВЗ продолжительность сдачи экзамена может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность сдачи экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительность подготовки обучающегося к ответу на экзамене, проводимом в устной форме, - не более чем на 20 минут.

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья организация обеспечивает выполнение следующих требований при проведении аттестации:

а) для лиц с нарушением зрения:

- задания и иные материалы для сдачи экзамена оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением, либо зачитываются ассистентом;
- письменные задания выполняются обучающимися с использованием клавиатуры с азбукой Брайля, либо надиктовываются ассистенту;

б) для лиц с нарушением слуха:

- с использованием информационной системы "Исток";
- аттестационные процедуры проводятся в электронной или письменной форме по выбору обучающихся.

О необходимости обеспечения специальных условий для проведения аттестации обучающийся должен сообщить письменно не позднее, чем за 10 дней до начала аттестации. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в организации).

Приложение 1

Автономная некоммерческая организация высшего образования
«Информационно-технологический университет»
(АНО ВО ИТУ)

Фонд оценочных средств

Текущего контроля и промежуточной аттестации
по дисциплине (модулю)

Б1.О.04.15 ЗАЩИТА ИНФОРМАЦИИ

Для направления подготовки:
09.03.01 Информатика и вычислительная техника
(уровень бакалавриата)

Типы задач профессиональной деятельности:
производственно-технологический

Направленность (профиль):
Информационные системы

Форма обучения:
очная, очно-заочная, заочная

г. Элиста, 2024

Результаты обучения по дисциплине

Код и наименование компетенции	Индикаторы достижения компетенции	Результаты обучения
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**УК-2.2.** Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов
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-3.2**. Самостоятельно проводит научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знает:** методологию проведения научно-исследовательской работы **Умеет:** самостоятельно проводить научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **Владеет:** навыками самостоятельного проведения научно-исследовательской работы

Показатели оценивания результатов обучения

Шкала оценивания			
Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
УК-2.2. Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения			
Не знает: методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Не умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Не владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов	**Поверхностно знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **В целом умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, но испытывает затруднения **В целом владеет:** способами решения конкретных задач в профессиональной	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения, но допускает несущественные ошибки **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, но иногда допускает небольшие ошибки **Владеет:**	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов

	деятельности, исходя из действующих норм, имеющихся ресурсов, но испытывает сильные затруднения	способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов, но иногда допускает ошибки	
ОПК-3.2. Самостоятельно проводит научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности			
Не знает: методологию проведения научно-исследовательской работы **Не умеет:** самостоятельно проводить научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **Не владеет:** навыками самостоятельного проведения научно-исследовательской работы	**Поверхностно знает:** методологию проведения научно-исследовательской работы **В целом умеет:** самостоятельно проводить научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, но испытывает затруднения **В целом владеет:** навыками самостоятельного проведения научно-исследовательской работы, но испытывает сильные затруднения	**Знает:** методологию проведения научно-исследовательской работы, но допускает несущественные ошибки **Умеет:** самостоятельно проводить научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ошибки **Владеет:** навыками самостоятельного проведения научно-исследовательской работы, но иногда допускает ошибки	**Знает:** методологию проведения научно-исследовательской работы **Умеет:** самостоятельно проводить научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **Владеет:** навыками самостоятельного проведения научно-исследовательской работы

Оценочные средства

Задания для текущего контроля

Пример тем для рефератов:

Раздел 1 «Введение в информационную безопасность»

1. Понятие «информационная безопасность».
2. Основные составляющие информационной безопасности.
3. Классификация угроз безопасности информации по способу осуществления.
4. Несанкционированный доступ к информации.
5. Угрозы информационной безопасности при подключении к Интернет.
6. Классические методы взлома интрасетей.
7. Основные каналы утечки информации.

Раздел 2 «Организационно-правовое обеспечение защиты информации»

1. Угрозы нарушения доступности, целостности и конфиденциальности информации.
2. Особенности современных информационных систем, существенных с точки зрения безопасности информации.

3. Задачи, решаемые на законодательном уровне информационной безопасности.
4. Задачи, решаемые на административном уровне информационной безопасности.
5. Задачи, решаемые на процедурном уровне информационной безопасности.
6. Роль стандартов информационной безопасности.
7. Международные стандарты информационной безопасности.

Раздел 3 «Методы и средства технической защиты информации»

1. Виды и методы технической защиты информации (пассивные и активные методы защиты информации.
2. Средства технической защиты информации.
3. Системы охранной сигнализации на территории и в помещениях.
4. Системы видеонаблюдения.
5. Системы контроля доступа.
6. Технические средства и методы получения информации по этим каналам.
7. Утечка информации по проводным коммуникациям и за счет побочных электромагнитных излучений и наводок.
8. Технические средства и методы получения информации с использованием этих каналов).
9. Методы и средства защиты информации от утечки по техническим каналам (основные методы, используемые при создании систем защиты информации.

Раздел 4 «Программно-технические средства защиты информации»

1. Защита информации от несанкционированного доступа (идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.
2. Идентификация и аутентификация субъектов “пользователь” и “процесс” при запросах на доступ к компьютерным ресурсам.
3. Использование простого и динамически изменяющегося паролей.
4. Защита программных средств от несанкционированного копирования и модификации).
5. Защита от компьютерных вирусов (основные виды вирусов и схемы их функционирования.
6. Основные каналы распространения вирусов и других вредоносных программ.
7. Выполнение функций посредничества.
8. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.

Раздел 5 «Криптографические средства защиты информации»

1. Схема работы симметричной криптосистемы.
2. Схема работы асимметричной криптосистемы.
3. Алгоритмы шифрования.
4. Преимущества и недостатки программного шифрования.
5. Преимущества и недостатки аппаратного шифрования.
6. Криптостойкость системы шифрования RSA.
7. Современные системы шифрования.
8. Система персонального шифрования PGP.
9. Криптоалгоритм RC4.

Оценка рефератов производится по шкале «зачтено» / «не зачтено».

Пример теста:

1. _____ информации - состояние защищенности информации от негативного воздействия на нее с точки зрения нарушения ее физической и логической целостности или несанкционированного использования.

a) Уязвимость
b) Безопасность
c) Надежность
d) Защищенность

2. _____ информации - возможность возникновения на каком-либо этапе жизненного цикла системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

a) Уязвимость
b) Безопасность
c) Надежность
d) Защищенность

3. Верны ли утверждения?
А) Национальная безопасность РФ - защищенность жизненно важных интересов личности, общества и государства в различных сферах жизнедеятельности от внутренних и внешних угроз, обеспечивающая устойчивое поступательное развитие страны.
В) Национальная безопасность РФ - безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в РФ.
Подберите правильный ответ.

a) А – да, В - нет
b) А – да, В - да
c) А – нет, В - нет
d) А – нет, В - да

4. Обеспечение _____ - защита от несанкционированного получения информации.

a) целостности
b) конфиденциальности
c) доступности
d) безопасности

5. Верны ли утверждения?
А) Систему безопасности РФ образуют органы законодательной, исполнительной и судебной властей, государственные, общественные и иные организации, объединения, отдельные граждане, принимающие участие в обеспечении безопасности в соответствии с законом.
В) Систему безопасности РФ образует законодательство, регламентирующее отношения в сфере безопасности.
Подберите правильный ответ.

a) А – да, В - нет
b) А – да, В - да
c) А – нет, В - нет
d) А – нет, В - да

6.Основными составляющими информационной безопасности являются

a) конфиденциальность, целостность, доступность
b) глубина, достоверность, адекватность
c) своевременность, актуальность, полнота
d) релевантность, толерантность

7.Система считается безопасной, если

a) она управляет доступом к информации так, что только должным образом авторизованные лица или же действующие от их имени процессы получают право доступа

b) она абсолютно недоступна для взлома

c) все пользователи удовлетворены работой системы

d) она обеспечивает одновременную обработку информации разной степени секретности (конфиденциальности) группой пользователей без нарушения прав доступа

8.Верны ли утверждения?
A) Допускается создание органов обеспечения безопасности, не предусмотренных законом РФ.
B) Основными принципами обеспечения безопасности РФ являются: законность, соблюдение баланса жизненно важных интересов личности, общества и государства, взаимная ответственность личности, общества и государства по обеспечению безопасности.
Подберите правильный ответ.

a) A – да, B - нет

b) A – да, B - да

c) A – нет, B - нет

d) A – нет, B - да

9. Организованная совокупность средств, методов и мероприятий, используемых для регулярной обработки информации, называется

A) автоматизированной системой
B) информационной системой
C) вычислительным комплексом
D) компьютерной системой

10.Из перечисленных свойств: 1) конфиденциальность; 2) восстанавливаемость; 3) доступность; 4) целостность; 5) детерминированность – безопасная система обладает

E) 1, 3, 4
F) 1, 2, 3
G) 2, 4, 5
H) 1, 3, 5

11.Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство

I) доступность
J) целостность
K) восстанавливаемость
L) детерминированность

12. Неизменность параметров настройки устройства характеризует свойство

M) целостность
N) доступность
O) восстанавливаемость
P) детерминированность

13. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется

Q) качеством информации
R) актуальностью информации
S) доступностью
T) целостностью

14. Из перечисленного: 1) степень прогнозируемости; 2) природа происхождения; 3) предпосылки появления; 4) источники угроз; 5) размер ущерба – параметрами классификации угроз безопасности информации являются

U) 2, 3, 4
V) 1, 2, 3
W) 3, 4, 5
X) 1, 5

15. Содержанием параметра угрозы безопасности информации "физическая целостность" является

Y) уничтожение
Z) переструктурирование
AA) несанкционированная модификация
BB) несанкционированное получение

16. Содержанием параметра угрозы безопасности информации "логическая структура" является

CC) искажение
DD) уничтожение
EE) несанкционированная модификация
FF) несанкционированное получение

17.Сутью параметра угрозы безопасности информации "содержание" является
GG) несанкционированная модификация
HH) несанкционированное получение
II) уничтожение
JJ) искажение
18.Содержанием параметра угрозы безопасности информации "конфиденциальность" является
KK) несанкционированное получение
LL) несанкционированная модификация
MM) искажение
NN) уничтожение
19. Из перечисленного: 1) случайная; 2) преднамеренная; 3) стихийная; 4) детерминированная; 5) объективная; 6) субъективная – угрозы безопасности по природе происхождения классифицируются как
OO) 1, 2
PP) 3, 4
QQ) 5, 6
RR) 1, 2, 3, 4
20. Из перечисленного: 1) случайная; 2) преднамеренная; 3) объективная; 4) субъективная; 5) стихийная; 6) детерминированная – угрозы безопасности по предпосылкам появления классифицируются как
SS) 3, 4
TT) 1, 2
UU) 5, 6
VV) 1, 2, 3, 4
21. Неправильное выполнение элементом какой-либо функции называется
WW) ошибкой
XX) сбоем
YY) отказом
ZZ) дефектом
22. Из перечисленного: 1) люди; 2) неадекватная система защиты; 3) технические средства; 4) алгоритмы; 5) устаревшее программное обеспечение; 6) внешняя среда – источником угрозы могут быть
AAA) 1, 3, 4, 6
BBB) 1, 2, 3, 4
CCC) 2, 3, 5 ,6
DDD) 1, 2, 5, 6
23. Из перечисленного: 1) создание ложного маршрутизатора; 2) навязывание сообщений; 3) прослушивание сегмента локальной сети; 4) сборка мусора; 5) запуск программы от имени пользователя, имеющего необходимые полномочия – на уровне системного программного обеспечения возможны атаки
EEE) 1, 2, 3
FFF) 1, 3, 4
GGG) 2, 4, 5
HHH) 2, 3, 5

24. Из перечисленного структура ОС с точки зрения анализа ее безопасности включает уровни: 1) внешний; 2) сетевой; 3) клиентский; 4) серверный; 5) системный; 6) приложений
A) 1, 2, 5, 6
B) 1, 2, 3, 4
C) 3, 4, 5, 6
D) 1, 3, 5, 6
25.Взаимодействие с глобальными ресурсами других организаций определяет уровень ОС
E) внешний
F) сетевой
G) приложений
H) системный
26.С доступом к информационным ресурсам внутри организации связан уровень ОС
I) сетевой
J) внешний
K) приложений
L) системный
27.Средствами проверки подлинности пользователей обеспечивается безопасность информации на уровне ОС
M) сетевом
N) внешнем
O) приложений
P) системном

28.С управлением доступа к ресурсам ОС связан уровень ОС
Q) системный
R) внешний
S) приложений
T) внешний
29.Определение допустимых для пользователя ресурсов ОС происходит на уровне ОС
U) системном
V) сетевом
W) внешнем
X) приложений
30.С использованием прикладных ресурсов ИС связан уровень ОС
Y) приложений
Z) внешний
AA) сетевой
BB) системный
31.Защита информации, определяющей конфигурацию системы, является основной задачей средств защиты
CC) встроенных в ОС
DD) уровня приложений
EE) сетевого уровня
FF) системного уровня
32.В ИС с низкими требованиями к обеспечению безопасности пароль должен меняться
GG) каждые 3 месяца
HH) каждый месяц
II) каждые полгода
JJ) каждые 6 недель
33.В ИС с высокими требованиями к обеспечению безопасности пароль должен меняться
KK) каждые 6 недель
LL) каждый месяц
MM) каждые 3 месяца
NN) каждую неделю
34.Из перечисленного для разграничения доступа к файлу применяются флаги, разрешающие: 1) копирование; 2) чтение; 3) запись; 4) выполнение; 5) удаление
OO) 2, 3, 4
PP) 1, 2, 3
QQ) 3, 4, 5
RR) 1, 2, 5
35.Для реализации технологии RAID создается
SS) псевдодрайвер
TT) компилятор
UU) интерпретатор
VV) специальный процесс
36. Из перечисленного ядро безопасности ОС выделяет типы полномочий: 1) ядра; 2) периферийных устройств; 3) подсистем; 4) пользователей
WW) 1, 3
XX) 2, 3
YY) 1, 2
ZZ) 3, 4
37.Полномочия ядра безопасности ОС ассоциируются с
AAA) процессами
BBB) пользователями
CCC) приложениями
DDD) периферийными устройствами
38.Полномочия подсистем ядра безопасности ОС ассоциируются с
EEE) пользователями
FFF) приложениями
GGG) периферийными устройствами
HHH) процессами

40. _____– процедура распознавания пользователя по его имени
a) Аутентификация
b) Идентификация

c) Авторизация
d) Персонализация

41. _____ – процедура проверки подлинности заявленного пользователя, процесса или устройства
a) Аутентификация
b) Идентификация
c) Авторизация
d) Персонализация

42. _____ – процедура предоставления субъекту определенных полномочий и ресурсов в данной системе
a) Аутентификация
b) Идентификация
c) Авторизация
d) Персонализация

43.Верны ли утверждения?
А) Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей)
В) От идентификации и аутентификации зависит последующее решение системы о том, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу
Подберите правильный ответ
a) А – да, В - нет
b) А – да, В - да
c) А – нет, В - нет
d) А – нет, В - да

44._____ – регистрация действий пользователя в сети, включая его попытки доступа к ресурсам
a) Аутентификация
b) Идентификация
c) Администрирование
d) Персонализация

45. Персональный идентификационный номер PIN является способом _____ держателя пластиковой карты и смарт-карты
a) аутентификации
b) идентификация
c) авторизации
d) администрирования

46._____ пароль – пароль, который после однократного применения больше не используется
a) Открытый
b) Асимметричный
c) Динамический
d) Многоразовый

47.Верны ли утверждения?
А) Если для аутентификации используются сертификаты, то требуется применение цифровых подписей на этих сертификатах
В) Сертификаты выдаются ответственным лицом в организации пользователя, сервером сертификатов или внешней доверенной организацией
Подберите правильный ответ
a) А – да, В - нет
b) А – да, В - да
c) А – нет, В - нет
d) А – нет, В - да

48. Для идентификации контекста защиты процесса или информационного потока используется объект, называемый _____ доступа

a) маркером
b) уровнем
c) кодом
d) сертификатом

49. Пароль подтверждения подлинности пользователя при использовании простого пароля

a) не изменяется от сеанса к сеансу в течение установленного администратором времени
b) изменяется от сеанса к сеансу по правилам, зависящим от используемого метода
c) базируется на проверке биометрических характеристик пользователя
d) требует использования магнитных карт, смарт-карт, сертификатов или устройств touch memory

50. К пакетам шифрования относится

a) PGP
b) Excel
c) Telnet
d) Internet Explorer

Оценка формируется следующим образом:

- оценка «отлично» - 85-100% правильных ответов;
- оценка «хорошо» - 70-84% правильных ответов;
- оценка «удовлетворительно» - 40-69% правильных ответов;
- оценка «неудовлетворительно» - менее 39% правильных ответов.

Промежуточная аттестация

Примерные вопросы к экзамену:

1. Криптографическая стойкость
2. Классы сложности. Иерархия классов сложности
3. Тенденции развития и проблемы защиты информации
4. Шифры
5. Блочные шифры
6. Сеть (схема) Фейстеля
7. Шифр DES
8. Шифр DES — режим ECB
9. Шифр DES — режим CBC
10. Шифр DES — режим CFB
11. Шифр DES — режим OFB
12. Шифр Triple DES
13. Полиномы. Общие алгебраические структуры. Группы
14. Поля GF(2n). Полином с коэффициентами из GF(2)
15. Шифр AES
16. AES. Преобразование SubBytes
17. AES. Преобразование ShiftRow
18. AES. Преобразование MixColomn
19. AES. Преобразование AddRoundKey
20. Анализ AES
21. Режимы блочного шифрования Electronic Code Book
22. Режимы блочного шифрования Cipher Block Chaining

23. Режимы блочного шифрования Cipher Feedback Mode
24. Режимы блочного шифрования Output Feedback Mode
25. Алгоритм Евклида. Расширенный алгоритм Евклида.
26. Криптосистемы с открытым ключом (Public - key cryptosystems)
27. Односторонние функции.Ооднонаправленные хэш-функции
28. Использование асимметричных алгоритмов для шифрования
29. Цифровая подпись на основе алгоритмов с открытым ключом
30. Формирование секретных ключей с использованием асимметричных алгоритмов
31. Требования к алгоритмам шифрования с открытым ключом
32. Алгоритмы с открытым ключом
33. Алгоритм на основе задачи об укладке ранца
34. Алгоритм RSA. Генерация ключей. Зашифровывание и расшифровывание
35. Практическое использованияе алгоритма RSA
36. Шифрование, дешифрование и генерация ключей в криптосистеме Рабина
37. Безопасность криптографической системы Рабина
38. Генерация ключей, шифрование, и дешифрование в криптосистеме Эль-Гамаля
39. Инфраструктура управления открытыми ключами (Public key infrastructure)
40. Цифровые сертификаты
41. Стандарты
42. MAC

ПРАКТИКО-ОРИЕНТИРОВАННАЯ ЧАСТЬ ЭКЗАМЕНА

Пример тестов

1. Укажите соответствие между составляющей информационной безопасности и ее описанием:	
Конфиденциальность информации	гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен
Целостность информации	гарантия сохранности данных в неискаженном виде (неизмененном по отношению к некоторому фиксированному их состоянию), которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные
Доступность информации	гарантия того, что авторизованные пользователи всегда получат доступ к данным

2. Укажите соответствие между критерием классификации угроз информационной безопасности сетей и соответствующей классификацией:	
По природе происхождения угроз	случайные угрозы преднамеренные угрозы
По предпосылкам появления угроз	объективные угрозы субъективные угрозы
По положению источника угроз	вне контролируемой зоны системы в пределах контролируемой зоны системы непосредственно в системе

3. _____ информации - состояние защищенности информации от негативного воздействия на нее с точки зрения нарушения ее физической и логической целостности или несанкционированного использования.	
a)	Уязвимость
b)	Безопасность
c)	Надежность
d)	Защищенность

4. _____ информации - возможность возникновения на каком-либо этапе жизненного цикла системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.	
a)	Уязвимость

b)	Безопасность
c)	Надежность
d)	Защищенность

5. К радиоэлектронным способам воздействия угроз на объекты информационной безопасности РФ относится	
a)	внедрение программ-вирусов
b)	уничтожение и порча средств обработки информации и связи
c)	невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых актов в информационной сфере
d)	перехват информации в технических каналах ее утечки

6. К организационно-правовым способам воздействия угроз на объекты информационной безопасности РФ относится	
a)	внедрение программ-вирусов
b)	уничтожение и порча средств обработки информации и связи
c)	невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых актов в информационной сфере
d)	перехват информации в технических каналах ее утечки

7. _____ - полномочия, устанавливаемые администратором системы для конкретных лиц, позволяющие последним использовать транзакции, процедуры или всю систему в целом.	
a)	Аутентификация
b)	Идентификация
c)	Авторизация
d)	Аудит

8. _____ - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию.	
a)	Политика безопасности
b)	Решение совета директоров
c)	Устав
d)	Решение собрания акционеров

e) 9. На законодательном уровне информационной безопасности особого внимания заслуживают	
	правовые акты и стандарты
	разделение обязанностей и минимизация привилегий
	установка и эксплуатация информационной системы
	документирование и регламентные работы

10. Управление персоналом относится к _____ уровню информационной безопасности.	
a)	процедурному
b)	программному
c)	техническому
d)	законодательному

11. Укажите соответствие между средствами защиты информации в сетях и их описанием:	
Законодательные средства защиты	законы, постановления Правительства, нормативные акты и стандарты
Административные средства защиты	действия, предпринимаемые руководством предприятия или организации
Физические средства защиты	экранирование помещений для защиты от излучения; проверка поставляемой аппаратуры; устройства, блокирующие физический доступ к отдельным блокам компьютера
Технические средства защиты	контроль доступа, аудит, шифрование информации, контроль сетевого трафика

12. Матрица, в строках которой перечислены субъекты, столбцах - объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны разрешенные виды доступа, называется матрицей	
a)	доступа
b)	идентификации
c)	аудита
d)	авторизации

13.Сети, позволяющие организовать прозрачное для пользователей соединение сетей, включенных в Интернет, сохраняя секретность и целостность передаваемой информации с помощью шифрования, называются	
a)	виртуальными
b)	открытыми
c)	корпоративными
d)	прозрачными

14. Совокупность соглашений относительно способа представления данных, обеспечивающего их передачу в нужных направлениях и правильную интерпретацию, называется	
a)	протоколом
b)	уставом
c)	конституцией
d)	алгоритмом

15. Процесс сбора и накопления информации о событиях, происходящих в информационной системе, называется	
a)	протоколированием
b)	аудитом
c)	мониторингом
d)	контролем

16._____ - анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день).	
a)	Аутентификация
b)	Идентификация
c)	Авторизация
d)	Аудит безопасности

17. С помощью эвристических анализаторов антивирусные программы способны находить	
a)	аналоги известных вирусов
b)	только известные вирусы
c)	все возможные вирусы
d)	разработчиков вируса

18. _____ - системы анализа трафика и блокировки доступа в сетях, анализирующие пакеты на предмет разрешенных/запрещенных адресов и сервисов.	
a)	Межсетевые экраны
b)	Мониторы безопасности
c)	Аудиторы
d)	Фильтры

19. Все большее распространение получает _____ аутентификация пользователя, позволяющая аутентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.	
a)	биометрическая
b)	строгая

c)	авторизованная
d)	административная

20.Дактилоскопические системы аутентификации в качестве параметра идентификации используют	
a)	отпечатки пальцев
b)	форму кисти руки
c)	форму и размер лица
d)	голос и «клавиатурный почерк»

21. _____ — программа, способная создавать свои дубликаты и внедрять их в компьютерные сети и/или файлы, системные области компьютера и прочие выполняемые объекты.	
a)	Вирус
b)	Драйвер
c)	Утилита
d)	Контроллер

22. _____ — нежелательная почтовая корреспонденция рекламного характера, загружающая трафик и отнимающая время у пользователей.	
a)	Спам
b)	Апплет
c)	Прокси-сервер
d)	Программная закладка

23. _____ - специализированный комплекс межсетевой защиты.	
a)	Брандмауэр
b)	Концентратор
c)	Маршрутизатор
d)	Коммутатор

24. Укажите соответствие между базовым классом симметричных криптосистем и его описанием:	
Подстановки	вид преобразований, заключающийся в замене символов исходного текста на другие по более или менее сложному правилу
Перестановки	вид преобразований, заключающийся в перестановке местами символов исходного текста по некоторому правилу
Гаммирование	вид преобразований, при котором его символы складываются (по модулю, равному размеру алфавита) с символами псевдослучайной последовательности, вырабатываемой по некоторому правилу

25. Объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей	
a)	стеганогафия
b)	криптоанализ
c)	криптография
d)	криптология

26. Обеспечивает скрытность информации в информационных массивах	
a)	стеганогафия
b)	криптоанализ
c)	криптография
d)	криптология

27. В асимметричных системах шифрования	
a)	открытый ключ доступен всем желающим, а секретный ключ известен только получателю сообщения
b)	для зашифрования и расшифрования используется один ключ

c)	секретный ключ доступен всем желающим, а открытый ключ известен только получателю сообщения
d)	секретный и открытый ключи доступны всем желающим

28. Системы шифрования, в которых используются два ключа - открытый (общедоступный) и секретный, называются системами шифрования	
a)	симметричными
b)	асимметричными
c)	статическими
d)	динамическими

29. Система шифрования DES является системой шифрования	
a)	симметричной
b)	асимметричной
c)	статической
d)	динамической

30. К пакетам шифрования относится	
a)	PGP
b)	Excel
c)	Telnet
d)	Internet Explorer

Оценка формируется следующим образом:

- оценка «отлично» - 85-100% правильных ответов;
- оценка «хорошо» - 70-84% правильных ответов;
- оценка «удовлетворительно» - 40-69% правильных ответов;
- оценка «неудовлетворительно» - менее 39% правильных ответов.

Критерии оценки при проведении промежуточной аттестации

Оценивание знаний обучающихся осуществляется по 4-балльной шкале при проведении экзаменов и зачетов с оценкой (оценки «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно») или 2-балльной шкале при проведении зачета («зачтено», «не зачтено»).

При прохождении обучающимися промежуточной аттестации оцениваются:

1. Полнота, четкость и структурированность ответов на вопросы, аргументированность выводов.

2. Качество выполнения практических заданий (при их наличии): умение перевести теоретические знания в практическую плоскость; использование правильных форматов и методологий при выполнении задания; соответствие результатов задания поставленным требованиям.

3. Комплексность ответа: насколько полно и всесторонне обучающийся раскрыл тему вопроса и обратился ко всем ее аспектам.

Критерии оценивания

4-балльная шкала и 2-балльная шкалы	**Критерии**

«Отлично» или «зачтено»	1. Полные и качественные ответы на вопросы, охватывающие все необходимые аспекты темы. Обучающийся обосновывает свои выводы с использованием соответствующих фактов, данных или источников, демонстрируя глубокую аргументацию. 2. Обучающийся успешно переносит свои теоретические знания в практическую реализацию. Выполненные задания соответствуют высокому уровню качества, включая использование правильных форматов, методологий и инструментов. 3. Обучающийся анализирует и оценивает различные аспекты темы, демонстрируя способность к критическому мышлению и самостоятельному исследованию.
«Хорошо» или «зачтено»	1. Обучающийся предоставляет достаточно полные ответы на вопросы с учетом основных аспектов темы. Ответы обучающегося имеют ясную структуру и последовательность, делая их понятными и логически связанными. 2. Обучающийся способен применить теоретические знания в практических заданиях. Выполнение задания в целом соответствует требованиям, хотя могут быть некоторые недочеты или неточные выводы по полученным результатам. 3. Обучающийся представляет хорошее понимание темы вопроса, охватывая основные аспекты и направления ее изучения. Ответы обучающегося содержат достаточно информации, но могут быть некоторые пропуски или недостаточно глубокие суждения.
«Удовлетворительно» или «зачтено»	1. Ответы на вопросы неполные, не охватывают всех аспектов темы и не всегда структурированы или логически связаны. Обучающийся предоставляет верные выводы, но они недостаточно аргументированы или основаны на поверхностном понимании предмета вопроса. 2. Обучающийся способен перенести теоретические знания в практические задания, но недостаточно уверен в верности примененных методов и точности в их выполнении. Выполненное задание может содержать некоторые ошибки, недочеты или расхождения. 3. Обучающийся охватывает большинство основных аспектов темы вопроса, но демонстрирует неполное или поверхностное их понимание, дает недостаточно развернутые объяснения.
«Неудовлетворительно» или «не зачтено»	1. Обучающийся отвечает на вопросы неполно, не раскрывая основных аспектов темы. Ответы обучающегося не структурированы, не связаны с заданным вопросом, отсутствует их логическая обоснованность. Выводы, предоставляемые обучающимся, представляют собой простые утверждения без анализа или четкой аргументации. 2. Обучающийся не умеет переносить теоретические знания в практический контекст и не способен применять их для выполнения задания. Выполненное задание содержит много ошибок, а его результаты не соответствуют поставленным требованиям и (или) неправильно интерпретируются. 3. Обучающийся ограничивается поверхностным рассмотрением темы и не показывает понимания ее существенных аспектов. Ответ обучающегося частичный или незавершенный, не включает анализ рассматриваемого вопроса, пропущены важные детали или связи.

ФОС для проведения промежуточной аттестации одобрен на заседании кафедры (Протокол заседания кафедры № 01 от «04» июня 2024 г.).