МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
заведующий каферой
кибербезопасности информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.11 Введение в специальность

1. Код и наименование направления подготовки/специальности:

10.05.01. Компьютерная безопасность

2. Профиль подготовки / специализация / магистерская программа:

математические методы защиты информации

3. Квалификация (степень) выпускника: специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: кибербезопасности информационных систем

6. Составители программы: Кенин Сергей Леонидович
кандидат технических наук, доцент

7. Рекомендована: НМС факультета ПММ, протокол № 5 от 22.03.2024

_____
отметки о продлении вносятся вручную)

8. Учебный год: 2025/2026 Семестр(ы): 3

9.Цели и задачи учебной дисциплины: Целью изучения дисциплины «Введение в специальность» является знакомство с положением, которое занимает специальность "Компьютерная безопасность" в общей системе высшего образования в РФ, с основными проблемами, стоящими в настоящее время в области информационной безопасности, с основными подходами к решению этих проблем, с особой ролью криптографических и математических методов в решении этих проблем. Дисциплина «Введение в специальность» базируется на знаниях, полученных в школе.

10. Место учебной дисциплины в структуре ООП: Дисциплина «Введение в специальность» входит в обязательную часть блока Б1 учебного плана

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-1	Способен оценивать роль информации, информационны х технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1	Знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;	Знает основные понятия об информации как предмете защиты. Знает принципы и модели взаимодействия «открытых» систем, информационно- вычислительных систем. Знает основные угрозы безопасности информации, обрабатываемой в компьютерных системах. Знает методы и средства защиты информации. Имеет представление о технических каналах утечки информации; каналах перехвата при передаче информации системами связи; каналы утечки акустической и видовой информации; компьютерные методы съёма информации. Знает технические, правовые и организационные методы и средства защиты информации. Знает стандарты шифрования, хэширования, и цифровой подписи
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.2	Знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России	Знает и понимает содержание Конституции РФ, Законов РФ «Об образовании», «О высшем и послевузовском образовании». Знает содержание федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 10.05.01 «Компьютерная безопасность» Знает и понимает национальные интересы Российской Федерации в информационной сфере и их обеспечение. Знает организационную структуру и основные функции системы обеспечения информационной безопасности Российской Федерации. Знает и понимает задачи обеспечения безопасности России в информационной сфере.

12. Объем дисциплины в зачетных единицах/час.(*в соответствии с учебным планом)* **—** 2/72.

Форма промежуточной аттестации*(зачет/экзамен)* зачет.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			3 сем.			
Аудиторные занятия	16		16			
в том числе: лекции	16		16			
Практические	0		0			
Лабораторные	0		0			
Самостоятельная работа	56		56			
Итого:	72		72			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1	Организация высшего образования в области компьютерной безопасности	Правовые основы высшего образования: Конституция РФ, Законы РФ «Об образовании», «О высшем и послевузовском образовании». Права и обязанности обучающихся. Организация высшего образования в РФ. Федеральные государственные образовательные стандарты. Направления подготовки и специальности. Подготовка научных кадров высшей квалификации: аспирантура и докторантура. Содержание федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 10.05.01 «Компьютерная безопасность»	Введение в специальность (10.05.01)
2	Общие понятия об информации и информационной безопасности	Определение, признаки и классификация информации. Понятие об информации как предмете защиты; основные свойства информации, информация как товар, неисчерпаемость ресурса и др. Задачи обеспечения безопасности России в информационной сфере.	
3	Обработка и передача информации в вычислительных и управляющих системах и сетях связи	Человек и информация; сообщения, сигналы; обобщенная структурная схема систем электросвязи. Компьютерная информация; системное, прикладное и специальное программное обеспечение; понятие «открытой» системы; модель взаимодействия элементов «открытых» систем, информационно- вычислительная система.	
4	Доктрина информационной безопасности Российской Федерации (выборочные	Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Основные функции системы обеспечения	

	главы)	информационной безопасности Российской Федерации. Организационная структура системы информационной безопасности Российской Федерации.	
5	Введение в проблему безопасности информации в информационных системах и сетях связи	Актуальность проблемы; угрозы безопасности информации, обрабатываемой в компьютерных системах; основные понятия; направления, методы и средства защиты информации; человеческий фактор влияния на безопасность информационных систем.	
6	Каналы утечки информации на объектах защиты	Технические каналы утечки: электромагнитные, электрические, параметрические. Каналы перехвата при передаче информации системами связи: электромагнитные, электрические, индукционные. Каналы утечки акустической и видовой информации. Компьютерные методы съёма информации.	
7	Общие вопросы организации системы защиты информации на предприятии	Технические, правовые и организационные методы и средства защиты информации. Уязвимые места информационновычислительных и управляющих систем на предприятии: кабельная система, система электроснабжения, система архивирования и дублирования информации. Защита от стихийных бедствий.	
8	Стандарты информационной безопасности	Стандарты шифрования, хэширования, цифровой подписи	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практ.	Лаб. раб	Самостоятельная работа	Всего
1	Организация высшего образования в области компьютерной безопасности	1			4	5
2	Общие понятия об информации и информационной безопасности	1			6	7
3	Обработка и передача информации в вычислительных и управляющих системах и сетях связи	2			8	10
4	Доктрина информационной безопасности Российской Федерации (выборочные главы)	2			6	8
5	Введение в проблему безопасности					

	информации в информационных системах и сетях связи	2			8	10
6	Каналы утечки информации на объектах защиты	4			6	10
7	Общие вопросы организации системы защиты информации на предприятии	2			6	8
8	Стандарты инфомационной безопасности	2			12	14
	Итого:	16			56	72

14. Методические указания для обучающихся по освоению дисциплины

Изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой литературе, повторение теоретического материала, изложенного в курсе лекций. Подготовка реферата по заданной теме и подготовка к зачёту.

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1.	Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2012. — 592 с. — ISBN 978-5-94074-637-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/3032 (дата обращения: 10.02.2019). — Режим доступа: для авториз. пользователей.
2.	Нормативно-правовые и организационные методы обеспечения информационной безопасности при разработке устройств, использующих средства криптозащиты : учебное пособие для вузов : [для студ. 4 курса днев. отд-ния, 4 курса вечер. отд-ния и для магистров 5 курса днев. отд-ния, для специальности 010501 – Прикладная математика и информатика] / Воронеж. гос. ун-т ; сост. : Б. Н. Воронков, А. В. Кузнецов . – Воронеж : ИПЦ ВГУ, 2011. – 135 с. : [текст]. – (URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m1101.pdf) (дата обращения 14.01.2020).
3.	Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А. Ю. Щербаков. – Москва. : Книжный мир, 2009. – 352 с. URL: https://computer-museum.ru/books/computer_safety.pdf (дата обращения 10.02.2020).

б) дополнительная литература:

№ п/п	Источник
4.	Основы управления информационной безопасностью / А. П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2013 .— 244 с. URL: https:// file.ashx?guid=371d693d-40a2-450a-b5a5-42fcc83a7790 (yandex.ru).
5.	Гончаров И. В., Кирсанов Ю.Г., Райков О. В. Информационная безопасность : словарь по терминологии : дополнение ко второму изданию / Гончаров И. В., Кирсанов Ю. Г., Райков О.

	В. ; [Акционерное общество "Научное производственное объединение "Инфобезопасность"]. - Воронеж : НПО "Инфобезопасность", 2017. - 85, [1] с. : табл. ; 20 см.. - Библиогр. в конце кн. (10 назв.) URL: https://primo.nlr.ru/primo_library/libweb/action/display.do;jsessionid=5E200698EC5E90D67AA9D233C0950000?tabs=detailsTab&ct=display&fn=search&dc (дата обращения 10.02.2020).

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
1.	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
2.	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
3.	Введение в специальность (10.05.01) /В.В. Текунов. — Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru.

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению лабораторных и контрольных работ)

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка реферата по заданной теме.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебное пособие, указания по подготовке к зачету. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

№ п/п	Источник
1	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
2	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
3	Введение в специальность (10.05.01) /В.В. Текунов. — Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

При реализации дисциплины используются модульно-рейтинговая и личностно-ориентированные технологии обучения (ориентированные на индивидуальность студента, компьютерные и коммуникационные технологии). В рамках дисциплины предусмотрены следующие виды лекций: информационная, лекция-визуализация, лекция с применением обратной связи.

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий, для организации самостоятельной работы обучающихся используется онлайн-курс, размещенный на платформе Электронного университета ВГУ (LMS moodle), а также другие Интернет-ресурсы, приведенные в п.15в

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория для проведения лекций: компьютер преподавателя, компьютер учащегося, мультимедиа оборудование (проектор, средства звуковоспроизведения), доска маркерная, специализированная мебель.

Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ необходимы компьютерные классы, помещения, оснащенные компьютерами с доступом к сети Интернет

Программное обеспечение (см.файл МТО): Windows 10 (лицензионное ПО); Intellij IDEA Community Edition (свободное и/или бесплатное ПО); Paskal ABC NET (свободное и/или бесплатное ПО); Jet Brains PyCharm Community Edition (свободное и/или бесплатное ПО); Anaconda (свободное и/или бесплатное ПО); Maxima (свободное и/или бесплатное ПО); Scilab (свободное и/или бесплатное ПО); LibreOffice (свободное и/или бесплатное ПО); NetBeans IDE (свободное и/или бесплатное ПО); Adobe Reader (свободное и/или бесплатное ПО); Microsoft Visual Studio Community Edition (свободное и/или бесплатное ПО); Notepad ++ (свободное и/или бесплатное ПО); Free Pascal (свободное и/или бесплатное ПО); Anylogic (свободное и/или бесплатное ПО); Справочно-правовая система Гарант (лицензионное ПО); Mozilla Firefox (свободное и/или бесплатное ПО); 1С:Предприятие 8.3 (лицензионное ПО); Matlab (лицензионное ПО); 7-zip (свободное и/или бесплатное ПО).

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Общие понятия об информации и информационной безопасности Обработка и передача информации в вычислительных и управляющих системах и сетях связи Введение в проблему безопасности информации в информационных системах и сетях связи Каналы утечки информации на объектах защиты Общие вопросы организации системы защиты информации на предприятии Стандарты информационной безопасности	ОПК-1	ОПК-1.1	Устный опрос, рефераты
2.	Организация высшего образования в области компьютерной безопасности Общие понятия об информации и информационной безопасности Доктрина информационной безопасности Российской Федерации (выборочные главы)	ОПК-5	ОПК-5.2	Устный опрос
Промежуточная аттестация форма контроля - зачет				Перечень вопросов

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

20.1 Текущий контроль успеваемости

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Теку-

щая аттестация проводится в формах: устного опроса (индивидуальный опрос, фронтальная беседа).

Перечень тем рефератов

1. Формы психологической защиты человека от информационной перегрузки.
2. Социально вредная информация в средствах массовой информации.
3. Вредная и опасная информация в сети Интернет.
4. Формы и методы недобросовестной рекламной деятельности.
5. Формы обмана и мошенничества в сети Интернет.
6. Атаки на информационные системы путём перегрузки каналов связи и входных буферов памяти. Использование «протоколов вежливости» для реализации сетевых атак.
7. Способы подделки компьютерной информации (денег, документов, доказательств) и программный инструментарий.
8. Компьютерное «пиратство» и его формы. Перспективы противодействия незаконному копированию компьютерной информации.
9. Формы незаконного использования информации. Законодательные меры против незаконного использования информации.
10. Формы и методы диверсионно-террористической деятельности с использованием современных информационных технологий.
11. Виды и формы применения информационно-технологического оружия.
12. Доктрина информационной безопасности России и реальности её осуществления.
13. Анализ способов информационного воздействия и форм информационной защиты, отражённых в сказках, сказаниях, былинах и мифах.
14. Государственная система защиты граждан и общества от опасной информации (законодательство и практика).
15. Вопросы информационной безопасности в теории военного искусства.
16. Вопросы информационной безопасности в политике и дипломатии.
17. Формы и методы выживания биологических особей и возможности их применения при защите информации.
18. Стратегия пассивной информационной защиты.
19. Стратегия уничтожения источника угроз в сфере информационной защиты.
20. Стратегия обмана и её использование в сфере информационной защиты.
21. Модель комплексной информационной защиты и её элементы.
22. Модель информационной защиты каналов связи.
23. Угрозы скрытого информационного воздействия на пользователей сети Интернет.
24. Формы и методы защиты признаковой информации.
25. Информация как ценность и объект преступных посягательств.
26. Угрозы конфиденциальности и формы их реализации.
27. Модель информационного нарушителя, посягающего на конфиденциальную информацию методами несанкционированного доступа.
28. Модель компьютерного вирмейкера.
29. Задачи информационной защиты в финансовой сфере.
30. Задачи информационной защиты в сфере предоставление услуг связи.
31. Организационно-распорядительные меры информационной защиты.
32. Традиционные направления информационной защиты и пути их интеграции.
33. Защита информации в ERP-системах.
34. Методы повышения скрытности в системах связи.
35. Криптографическая защита в ERP-системах.

Описание технологии проведения

Студент выбирает тему реферата из предложенного перечня, работает над ней в течение семестра и оформляет результаты исследования в виде письменной работы. Требования по оформлению являются типовыми по факультету.

Перечень контрольных вопросов для устного опроса

1. Какую угрозу представляет для людей избыточная информация?
2. Какая информация может представлять угрозу для общества и государства?
3. Почему в законодательстве Российской Федерации предусмотрена уголовная ответственность за создание вредоносных компьютерных программ и не предусмотрена – за создание опасных видов оружия?
4. Как следует понимать конституционное право гражданина на получение информации?
5. Какую пользу приносит информационный голод и в чем заключается его вред?
6. Каким образом связаны процессы усвоения и создания информации человеком с его эмоциями?
7. Что такое «информационный шум»?
8. Как взаимосвязаны понятия «информация», «сообщение», «сигнал», «носитель»?
9. Для чего потребовалось оценивать защищённость информации на различных уровнях её представления?
10. Перечислите виды семантической и признаковой информации.
11. В каких случаях требуется защищать признаковую информацию?
12. Как соотносятся философские категории формы и содержания с понятиями признаковой и семантической информации?
13. Как формы и методы защиты информации зависят от её носителей?
14. Как следует толковать правило: «Защита информации – это защита её носителя»?
15. Какие существуют виды копирования компьютерной информации и в каких случаях они рекомендуются?
16. Укажите формы представления компьютерной информации и особенности её защиты.
17. В чем заключается защита информации на уровне устройств ее чтения и записи?
18. Назовите способы кодирования информации и перечислите их защитные функции.
19. Охарактеризуйте виды сжатия данных и их защитную роль.
20. Какие методы защиты информации реализуются на семантическом и прагматическом уровнях?
21. Какие меры предусмотрены Федеральным законодательством России для защиты населения от опасной информации?
22. Какие вам известны законодательные меры для противодействия неинформированности граждан?
23. Почему защите подлежит не информация, а право собственности на неё?
24. Могут ли секретные сведения представлять коммерческую ценность? Почему?
25. Какие категории сведений нормативно отнесены к категории государственной тайны?
26. Являются ли тождественными понятия «степень секретности» и «гриф секретности»?
27. Каким должен быть порядок засекречивания и рассекречивания информации?
28. Как оформляется допуск лиц к работе со сведениями, составляющими государственную тайну?
29. В чем заключается специфика защиты сведений, отнесённых к коммерческой тайне?
30. Перечислите виды и укажите особенности защиты профессиональных тайн.
31. С какой целью осуществляется лицензирование услуг по защите информации?
32. Каковы, по Вашему мнению, причины современной компьютерной преступности?
33. Что такое «незаконный оборот информации»?
34. Укажите недостатки, свойственные нормативно-правовой защите информационных отношений.

35. Почему персонал организации считается самым слабым звеном в информационной защите?
36. Что включает в себя работа с кадрами?
37. Как регламентируется работа с носителями конфиденциальной информации?
38. Какие общие требования информационной безопасности должен соблюдать каждый сотрудник, работающий с конфиденциальными сведениями?
39. Что такое «режим ограничения информированности»?
40. С какой целью осуществляется контроль за персоналом? Какие формы контроля не противоречат правам человека?
41. Что такое дезинформация?
42. Как правильно организовать легендирование?
43. Какие обязанности возлагаются на администратора безопасности?
44. Как можно увеличить популярность и действенность мер организационно- распорядительной защиты информации?
45. Как следует понимать термин «утечка информации по техническому каналу»?
46. Что такое канал утечки информации?
47. Какие особенности характерны для образования и использования технических каналов утечки информации?
48. Перечислите меры противодействия визуально-оптической разведке.
49. Назовите несколько источников, создающих утечку по электромагнитному каналу.
50. Перечислите меры, препятствующие образованию виброакустических каналов утечки информации.
51. Какие меры рекомендуются для предотвращения утечки конфиденциальной признаковой информации?
52. Что называют контролируемой зоной режимного объекта?
53. Какие меры противодействия перехвату информации могут быть рекомендованы, если каналы утечки простираются за пределы контролируемой зоны объекта?
54. В чем заключается сущность электромагнитного и акустического зашумления?
55. Что представляет собой энергетическое сокрытие информации?
56. Дайте классификацию средств технической разведки (СТР).
57. Почему автономные «интеллектуальные» средства технической разведки рассматриваются в качестве самостоятельных информационных «нарушителей»?
58. Перечислите основные демаскирующие признаки устройств негласного подслушивания.
59. Где, как и какими способами обнаруживаются средства технической разведки?
60. В чем заключается различие между режимным помещением, и помещением, выделенным для проведения конфиденциальных переговоров?
61. Как можно нейтрализовать диктофон, включённый для негласной записи разговоров?
62. Что такое радиомониторинг? Какими средствами он обеспечивается?
63. Как обнаруживаются замаскированные радиозакладки?
64. Для чего используется высокочастотное навязывание?
65. Что представляет собой специальная лабораторная проверка?
66. Перечислите основные меры противодействия электронному шпионажу.
67. Что представляют собой системы распознавания образов и в каких сферах деятельности они применяются?
68. Что называют системой управления доступом?
68. Сформулируйте требования к выбору надёжного пароля.
69. В чем заключаются достоинства и недостатки систем распознавания с носителями ключевой информации?
70. Укажите достоинства и недостатки систем биометрической аутентификации.
71. Перечислите специальные режимы работы систем управления физическим доступом.

72. Как происходит распознавание зарегистрированного пользователя в локальной компьютерной системе?
73. Для чего нужны системы аутентификации с передачей «доказательства с нулевым разглашением»? Как они, по Вашему мнению, могут быть организованы?
74. Что обозначает понятие «вредоносное программное воздействие»?
75. Можно ли считать вирмейкеров квалифицированными программистами? Почему?
76. Какие признаки позволяют относить компьютерные программы к числу вредоносных?
77. Назовите основные признаки компьютерных вирусов.
78. Что представляют собой мифические компьютерные вирусы?
79. Какие функции характерны для программных закладок?
80. В чем заключаются особенности сетевых вредоносных программ?
81. Какие способы скрытого внедрения и запуска вредоносных программ вам известны?
83. Что такое полиморфизм?
84. Как обеспечить безопасную изоляцию программной среды компьютера?
85. Что означает термин «семантическое сокрытие информации»?
86. Для чего используется скремблирование сообщений?
87. Какие допущения принимаются во внимание при использовании способов криптозащиты?
88. Какие проблемы свойственны классической криптографии?
89. В чем заключается сходство и различие асимметричных криптосистем и систем с электронной подписью?
90. С какой целью применяются гибридные способы криптозащиты?
91. Перечислите и охарактеризуйте виды стенографической защиты информации.

20.2 Промежуточная аттестация

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: теоретические вопросы. При этом на промежуточной аттестации учитываются результаты подготовки реферата.

Перечень вопросов зачету

1. Какую угрозу представляет для людей избыточная информация?
2. Какая информация может представлять угрозу для общества и государства?
3. Почему в законодательстве Российской Федерации предусмотрена уголовная ответственность за создание вредоносных компьютерных программ и не предусмотрена – за создание опасных видов оружия?
4. Как следует понимать конституционное право гражданина на получение информации?
5. Какую пользу приносит информационный голод и в чем заключается его вред?
6. Каким образом связаны процессы усвоения и создания информации человеком с его эмоциями?
7. Что такое «информационный шум»?
8. Как взаимосвязаны понятия «информация», «сообщение», «сигнал», «носитель»?
9. Для чего потребовалось оценивать защищённость информации на различных уровнях её представления?
10. Перечислите виды семантической и признаковой информации.
11. В каких случаях требуется защищать признаковую информацию?
12. Как соотносятся философские категории формы и содержания с понятиями признаковой и семантической информации?

13. Как формы и методы защиты информации зависят от её носителей?
14. Как следует толковать правило: «Защита информации – это защита её носителя»?
15. Какие существуют виды копирования компьютерной информации и в каких случаях они рекомендуются?
16. Укажите формы представления компьютерной информации и особенности её защиты.
17. В чем заключается защита информации на уровне устройств ее чтения и записи?
18. Назовите способы кодирования информации и перечислите их защитные функции.
19. Охарактеризуйте виды сжатия данных и их защитную роль.
20. Какие методы защиты информации реализуются на семантическом и прагматическом уровнях?
21. Какие меры предусмотрены Федеральным законодательством России для защиты населения от опасной информации?
22. Какие вам известны законодательные меры для противодействия неинформированности граждан?
23. Почему защите подлежит не информация, а право собственности на неё?
24. Могут ли секретные сведения представлять коммерческую ценность? Почему?
25. Какие категории сведений нормативно отнесены к категории государственной тайны?
26. Являются ли тождественными понятия «степень секретности» и «гриф секретности»?
27. Каким должен быть порядок засекречивания и рассекречивания информации?
28. Как оформляется допуск лиц к работе со сведениями, составляющими государственную тайну?
29. В чем заключается специфика защиты сведений, отнесённых к коммерческой тайне?
30. Перечислите виды и укажите особенности защиты профессиональных тайн.
31. С какой целью осуществляется лицензирование услуг по защите информации?
32. Каковы, по Вашему мнению, причины современной компьютерной преступности?
33. Что такое «незаконный оборот информации»?
34. Укажите недостатки, свойственные нормативно-правовой защите информационных отношений.
35. Почему персонал организации считается самым слабым звеном в информационной защите?
36. Что включает в себя работа с кадрами?
37. Как регламентируется работа с носителями конфиденциальной информации?
38. Какие общие требования информационной безопасности должен соблюдать каждый сотрудник, работающий с конфиденциальными сведениями?
39. Что такое «режим ограничения информированности»?
40. С какой целью осуществляется контроль за персоналом? Какие формы контроля не противоречат правам человека?
41. Что такое дезинформация?
42. Как правильно организовать легендирование?
43. Какие обязанности возлагаются на администратора безопасности?
44. Как можно увеличить популярность и действенность мер организационно- распорядительной защиты информации?
45. Как следует понимать термин «утечка информации по техническому каналу»?
46. Что такое канал утечки информации?
47. Какие особенности характерны для образования и использования технических каналов утечки информации?
48. Перечислите меры противодействия визуально-оптической разведке.
49. Назовите несколько источников, создающих утечку по электромагнитному каналу.
50. Перечислите меры, препятствующие образованию виброакустических каналов утечки информации.
51. Какие меры рекомендуются для предотвращения утечки конфиденциальной признаковой информации?

52. Что называют контролируемой зоной режимного объекта?
53. Какие меры противодействия перехвату информации могут быть рекомендованы, если каналы утечки простираются за пределы контролируемой зоны объекта?
54. В чем заключается сущность электромагнитного и акустического зашумления?
55. Что представляет собой энергетическое сокрытие информации?
56. Дайте классификацию средств технической разведки (СТР).
57. Почему автономные «интеллектуальные» средства технической разведки рассматриваются в качестве самостоятельных информационных «нарушителей»?
58. Перечислите основные демаскирующие признаки устройств негласного подслушивания.
59. Где, как и какими способами обнаруживаются средства технической разведки?
60. В чем заключается различие между режимным помещением, и помещением, выделенным для проведения конфиденциальных переговоров?
61. Как можно нейтрализовать диктофон, включённый для негласной записи разговоров?
62. Что такое радиомониторинг? Какими средствами он обеспечивается?
63. Как обнаруживаются замаскированные радиозакладки?
64. Для чего используется высокочастотное навязывание?
65. Что представляет собой специальная лабораторная проверка?
66. Перечислите основные меры противодействия электронному шпионажу.
67. Что представляют собой системы распознавания образов и в каких сферах деятельности они применяются?
68. Что называют системой управления доступом?
68. Сформулируйте требования к выбору надёжного пароля.
69. В чем заключаются достоинства и недостатки систем распознавания с носителями ключевой информации?
70. Укажите достоинства и недостатки систем биометрической аутентификации.
71. Перечислите специальные режимы работы систем управления физическим доступом.
72. Как происходит распознавание зарегистрированного пользователя в локальной компьютерной системе?
73. Для чего нужны системы аутентификации с передачей «доказательства с нулевым разглашением»? Как они, по Вашему мнению, могут быть организованы?
74. Что обозначает понятие «вредоносное программное воздействие»?
75. Можно ли считать вирмейкеров квалифицированными программистами? Почему?
76. Какие признаки позволяют относить компьютерные программы к числу вредоносных?
77. Назовите основные признаки компьютерных вирусов.
78. Что представляют собой мифические компьютерные вирусы?
79. Какие функции характерны для программных закладок?
80. В чем заключаются особенности сетевых вредоносных программ?
81. Какие способы скрытого внедрения и запуска вредоносных программ вам известны?
83. Что такое полиморфизм?
84. Как обеспечить безопасную изоляцию программной среды компьютера?
85. Что означает термин «семантическое сокрытие информации»?
86. Для чего используется скремблирование сообщений?
87. Какие допущения принимаются во внимание при использовании способов криптозащиты?
88. Какие проблемы свойственны классической криптографии?
89. В чем заключается сходство и различие асимметричных криптосистем и систем с электронной подписью?
90. С какой целью применяются гибридные способы криптозащиты?
91. Перечислите и охарактеризуйте виды стенографической защиты информации.

Требования к выполнению заданий, шкалы и критерии оценивания

Для оценивания результатов обучения на зачете используется шкала «зачтено, не зачтено»
Для оценивания результатов обучения на зачете используется – «зачтено, не зачтено».
«Зачтено» выставляется в случае получения 3, 4 и 5 балов по критериям оценивания.
«Не зачтено» выставляется в случае получения 2 балов по критериям оценивания. Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Компетенция	Шкала и критерии оценивания уровня освоения компетенции			
	5	4	3	2
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства. ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	Сформированные знания	Сформированные знания, но содержащие отдельные пробелы	Неполные знания	Фрагментарные знания или их отсутствие
	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений
	Сформированные навыки	Успешные навыки, но содержащие отдельные пробелы	Успешные, но не системные навыки	Фрагментарные навыки или их отсутствие

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

1) **закрытые задания (тестовые, средний уровень сложности):**

1. К источникам угроз безопасности информации относятся:
а) нарушитель;
б) вредоносная программа;
в) программно-аппаратная (аппаратная) закладка
г) все перечисленное.

2. Сколько всего классов защищенности автоматизированных систем?
а) 3;
б) 6;
в) 9;
г) 12.

3. Сколько всего классов защиты государственных информационных систем?
а) 3;
б) 6;
в) 9;

г) 12.

4. Сколько всего классов защиты средств вычислительной техники?
а) 3;
б) 6;
в) 9;
г) 12.

5. Уязвимость характеризуется:
а) слабостью;
б) недостатком;
в) слабостью и (или) недостатком;
г) условиями и факторами.

6. Угроза характеризуется:
а) слабостью;
б) недостатком;
в) слабостью и (или) недостатком;
г) условиями и факторами.

7. ERP – система это:
а) система управления ресурсами предприятия;
б) система регистрации событий безопасности информации;
в) система управления инцидентами безопасности информации;
г) система управления доступом.

Правильные ответы

1. г
2. в
3. а
4. б
5. в
6. г
7. а

2) <u>открытые задания (тестовые, средний уровень сложности):</u>

1. Дайте определение уязвимости информационной системы.
2. Дайте определение угрозы безопасности информационной системы.
3. Какой документ ФСТЭК России содержит номенклатуру мер защиты информации для государственных информационных систем.

Ответы:

1. Уязвимость информационной системы – недостаток (слабость) информационной системы, который может быть использован для реализации угроз безопасности обрабатываемой в ней информации
2. Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации
3. Приказ ФСТЭК России № 17

<u>3) открытые задания (мини-кейсы, средний уровень сложности):</u>
1. Регуляция деятельности по информационной безопасности в Российской Федерации.

Критерии оценивания	Шкала оценок

Обучающийся приводит развернутое и безошибочное описание общих подходов обеспечения деятельности по защите информации. Приводит перечень федеральных органов исполнительной власти по обеспечению безопасности информации. Приводит пример деятельности одного из них.	Отлично (90-100 баллов)
Обучающийся приводит достаточно развернутое описание общих подходов обеспечения деятельности по защите информации. Приводит перечень федеральных органов исполнительной власти по обеспечению безопасности информации.	Хорошо (70-80 баллов)
Представлено недостаточно развернутое описание общих подходов обеспечения деятельности по защите информации	Удовлетворительно (50-70 баллов)
Представлено неполное или содержащее грубые ошибки описание общих подходов обеспечения деятельности по защите информации	Неудовлетворительно (менее 50 баллов)

2. Доктрина информационной безопасности в Российской Федерации.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое и безошибочное описание содержания документа. Приводит цели и задачи документа. Отмечает особенности документа. Приводит историческую справку относительно редакций документа. Приводит примеры реализации положений документа.	Отлично (90-100 баллов)
Обучающийся приводит достаточно развернутое описание содержания документа. Приводит цели и задачи документа. Приводит один пример реализации положений документа..	Хорошо (70-80 баллов)
Представлено недостаточно развернутое описание содержания документа. Приводит цели и задачи документа.	Удовлетворительно (50-70 баллов)
Представлено неполное или содержащее грубые ошибки описание содержания документа. Примеры реализации положений документа отсутствуют	Неудовлетворительно (менее 50 баллов)

3. Административная ответственность за нарушения в области информационной безопасности

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое и безошибочное описание основных статей из Кодекса РФ об административных правонарушениях в области информационной безопасности. Приводит примеры штрафов по статьям.	Отлично (90-100 баллов)
Обучающийся приводит достаточно развернутое описание статей из Кодекса РФ об административных правонарушениях в области информационной безопасности. Приводит примеры штрафов по некоторым статьям.	Хорошо (70-80 баллов)
Представлено недостаточно развернутое описание содержания статей из Кодекса РФ об административных правонарушениях в области информационной безопасности.	Удовлетворительно (50-70 баллов)
Представлено неполное или содержащее грубые ошибки описание статей Кодекса РФ об административных правонарушениях в области информационной безопасности	Неудовлетворительно (менее 50 баллов)

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

1) **закрытые задания (тестовые, средний уровень сложности):**

1. Какие функции не выполняет подсистема идентификации и аутентификации:

а) идентификация и аутентификация пользователей, являющихся работниками оператора;
б) идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных;
в) управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
г) ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).

2. Какие функции не выполняет подсистема управления доступом:
а) управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
б) управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
в) реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
г) управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
д) правильный ответ отсутствует.

3. Какая функция решается подсистемой регистрации событий безопасности информации:
а) идентификация и аутентификация пользователей, являющихся работниками оператора;
б) управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
в) сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.

4. В ходе анализа защищенности информационной системы реализуются:
а) обновление базы данных признаков вредоносных компьютерных программ (вирусов);
б) выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
в) контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
г) контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
д) функции б), в), г);
е) все функции.

5. Принятие решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется:
а) оператором информационной системы;
б) владельцем информационной системы;
в) федеральным органом исполнительной власти.

6. При обеспечении защиты на этапе эксплуатации осуществляются:
а) управление (администрирование) системой защиты информации информационной системы;
б) выявление инцидентов и реагирование на них;
в) управление конфигурацией информационной системы и ее системы защиты информации;
г) контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе
д) все перечисленное.

7. Какой вид не относится к стратегиям защиты информации в компьютерной сети?
а) стратегия периметровой защиты;
б) стратегия отступления;
в) стратегия пресечения;
г) стратегия адаптивной защиты.

8. Недостаток (слабость) информационной системы – это:
а) ошибки в программном обеспечении;
б) ошибки в параметрах настройки;
в) ошибки технологии обработки (передачи) информации;
г) все перечисленное.

Правильные ответы

1. г

2. б
3. в
4. д
5. б
6. д
7. б
8. г

2) открытые задания (тестовые, средний уровень сложности):

1. Перечислите виды нарушителей безопасности информации по уровню их потенциальных возможностей.
2. Перечислите свойства безопасности информации.

Ответы:
1. Высокий, средний, базовый повышенный, базовый
2.Конфиденциальность, целостность, доступность

3) открытые задания (мини-кейсы, средний уровень сложности):

1. Уголовная ответственность в области информационной безопасности

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое и безошибочное описание основных статей из Уголовного Кодекса РФ в области информационной безопасности. Приводит примеры возможных сроков по статьям.	Отлично (90-100 баллов)
Обучающийся приводит достаточно развернутое описание статей из Уголовного Кодекса РФ в области информационной безопасности. Приводит примеры возможных сроков по некоторым статьям.	Хорошо (70-80 баллов)
Представлено недостаточно развернутое описание содержания статей Уголовного Кодекса РФ в области информационной безопасности.	Удовлетворительно (50-70 баллов)
Представлено неполное или содержащее грубые ошибки описание статей Уголовного Кодекса РФ в области информационной безопасности	Неудовлетворительно (менее 50 баллов)

2. Системы управления ресурсами предприятия как объекты защиты информации. Цели и задачи защиты информации. Примеры

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое и безошибочное описание функций системы управления ресурсами предприятия как объекта защиты информации. Указывает цели и задачи защиты информации. Приводит перечень и описание актуальных для таких систем угроз безопасности информации. Приводит примеры внедрения систем управления ресурсами предприятия.	Отлично (90-100 баллов)
Обучающийся приводит достаточно развернутое описание функций системы управления ресурсами предприятия как объекта защиты информации. Указывает цели и задачи защиты информации. Поясняет содержание актуальных для таких систем угроз безопасности информации. Приводит пример внедрения системы управления ресурсами предприятия.	Хорошо (70-80 баллов)
Представлено недостаточно развернутое описание функций системы управления ресурсами предприятия как объекта защиты информации. Указывает цели и задачи защиты информации.	Удовлетворительно (50-70 баллов)

Представлено неполное или содержащее грубые ошибки описание функций системы управления ресурсами предприятия как объекта защиты информации	Неудовлетворительно (менее 50 баллов)

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).