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

УТВЕРЖДАЮ

Заведующий кафедрой
технологий обработки и защиты информации

А.А. Сирота

23.04.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.11 Введение в специальность

1. Шифр и наименование направления подготовки/специальности:
10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализации: Анализ безопасности компьютерных систем

3. Квалификация (степень) выпускника: специалист

4. Форма образования: очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра технологий обработки и защиты информации

6. Составители программы:
Филиппова Неля Викторовна, к.ю.н. доцент

7. Рекомендована:
Научно-методическим советом ФКН, протокол № 5 от 05.03.2024 г.

8. Учебный год: 2024-2025 **Семестр(ы): 1**

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 относится к обязательной части блока Б1.

Входные знания в области нормативной и законодательной базы в области информационной безопасности, физики, распространения сигналов, теории вероятностей и математической статистики, информатики.

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, информационных 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 — 2/72.

Форма промежуточной аттестации: *зачёт*.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра 1	№ семестра	Итого
Аудиторные занятия		16	16		16
в том числе:	лекции	16	16		16
	практические	-	-		-
	лабораторные	-	-		-
Самостоятельная работа		56	56		56
в том числе: курсовая работа (проект)		-	-		-
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*		-	-		-
Итого:		72	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»	
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	Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Основные функции системы обеспечения 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 объекта	Технические, правовые и организационные методы и средства защиты информации. Уязвимые места информационно-вычислительных и управляющих систем объекта защиты: кабельная система, система электроснабжения, система архивирования и дублирования информации. Защита от стихийных бедствий.	
8	Стандарты информационной безопасности	Стандарты шифрования, хэширования, цифровой подписи	
2. Практические занятия			
2.1	нет		
3. Лабораторные работы			
3.1	нет		

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)			
		Лекции	Практические	Сам. работа	Всего
1.	Организация высшего образования в области компьютерной безопасности	2		6	8
2.	Общие понятия об информации и информационной безопасности	2		6	8
3.	Обработка и передача информации в вычислительных и управляющих системах и сетях связи	2		6	8
4.	Доктрина информационной безопасности Российской Федерации	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	2		8	10
7.	Общие вопросы организации системы защиты информации объекта	2		8	10
8.	Стандарты информационной безопасности	2		8	10
	Итого:	16		56	72

14. Методические указания для обучающихся по освоению дисциплины

1) При изучении дисциплины рекомендуется использовать следующие средства**:**

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- подготовка реферата по заданной теме;
- электронные версии учебников (при необходимости материалы рассылаются по электронной почте).

2) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций он-лайн используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

3) При использовании дистанционных образовательных технологий и электронного обучения обучающиеся должны выполнять все указания преподавателей,

вовремя подключаться к онлайн - занятиям, ответственно подходить к заданиям для 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/m11-01.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
1.	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.
2.	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).
3.	Хорев А.А. Защита информации от утечки по техническим каналам утечки информации. Часть 1. Технические каналы утечки информации. - М.: Гостехкомиссия России, 1998.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет) *:

№ п/п	Ресурс
1	ЭБС Лань, Лицензионный договор №3010, (с 01/03/2024 по 28.02.2025) 06/02 24 от 13.02.2024 (с дополнительным соглашением №1 от 14.03.2024)
2	ЭБС «Университетская библиотека online» (Контракт №3010 06/11 23 от 26.12.2023 (с 26.12.2023 по 25.12.2024)
3	ЭБС «Консультант студента» – Лицензионный договор №980КС/12-2023 / 3010-06/01-24 от 24.01.2024 с 24.01.2024 по 11. 01.2025)
4	Электронная библиотека ВГУ, Договор №ДС-208 от 01.02.2021 с ООО «ЦКБ «БИБКОМ» и ООО «Агентство «Книга-Сервис» о создании Электронной библиотеки ВГУ, (с 01.02.2021 по 31.01.2027)
5	ЭБС BOOK.ru, Договор №3010 15/983 23 от 20.12.2023, (с 01.02.2024 по 31.01.2025)

* 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 практических (контрольных) работ и др.)

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.

№ п/п	Источник
1.	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.
2.	ЭБС Лань, Лицензионный договор №3010, (с 01/03/2024 по 28.02.2025) 06/02 24 от 13.02.2024 (с дополнительным соглашением №1 от 14.03.2024)
3.	ЭБС «Университетская библиотека online» (Контракт №3010 06/11 23 от 26.12.2023 (с 26.12.2023 по 25.12.2024)

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

Для реализации учебного процесса используются:

1) ПО Microsoft в рамках подписки "Imagine/Azure Dev Tools for Teaching", договор №3010-16/96-18 от 29 декабря 2018г.

2) ОС Windows v.7, 8, 10; LibreOffice v.5-7; Foxit PDF Reader; MATLAB “Total Academic Headcount – 25”; Windows Server v. 2008-2019

3) LibreOffice v.5-7.

4) Foxit PDF Reader.

5) При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 477

Учебная аудитория: специализированная мебель, ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 479

Учебная аудитория: специализированная мебель, компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19", мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, ауд. 505п

Учебная аудитория: специализированная мебель, компьютер преподавателя i5-3220-3.3ГГц, монитор с ЖК 17", мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 292

Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 380
Учебная аудитория: специализированная мебель, компьютер преподавателя i3-3240-3,4ГГц, монитор с ЖК 17", мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, ауд. 305п
Учебная аудитория: специализированная мебель, ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, ауд. 307п
Учебная аудитория: специализированная мебель, ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

Перечень программного обеспечения, используемого в образовательном процессе

№ пп	Наименование ПО	Производитель ПО (или торговая марка, Или правообладатель) при наличии
	ОС Windows v.7, 8, 10	Microsoft (прим. 1)
2	СУБД Oracle Database 11g Express Edition	Oracle
3	Microsoft Visio, Access, OneNote v. 2010-2019	Microsoft
4	Visual Studio, v. 2010-2019	Microsoft
5	Набор утилит (архиваторы, файл-менеджеры)	GNU, BSD
6	ОС GNU/Linux (CentOS) v.6-8	RedHat, GNU
7	LibreOffice v.5-7	The Document Foundation, GNU
8	Среда разработки Eclipse	Eclipse Foundation
9	GlassFish Java EE	Eclipse Foundation
10	Python ver 3.8	Python Software Foundation
11	MySQL Workbench Community	GNU
12	PyCharm Community	JetBrains
13	IntelliJ IDEA	JetBrains
14	Среда разработки NetBeans IDE	ORACLE
15	Дистрибутив Anaconda/Python	BSD
16	Системы моделрования системной Динамики Vensim	Ventana Systemms Inc.
17	Системы моделирования бизнес процессов BizAgi	BizAgi
18	Системы управления проектами Wrike	Wrike Inc.
19	Системы моделирования Modelio	Modeliosoft
20	MATLAB “Total Academic Headcount – 25”	MathWorks (прим. 2)
21	HUGIN EXPERT / HUGIN Lite (open-source)	HUGIN EXPERT A/S
22	Справочно-правовая система (СПС) Консультант+ для образования	Консультант+ (прим. 7)
23	Microsoft SQL Server	Microsoft
24	Packet Tracer	CISCO Systems

25	Virtual Box	ORACLE
26	Microsoft Windows Virtual PC	Microsoft
27	VLC media player	VideoLAN, GNU
28	Google Workspace for Education Fundamentals (ранее G Suite for Education и Google-Apps for Education)	Google Inc.
29	SecretNet Studio 8 (демоверсия)	ООО Код Безопасности
30	Dr. Web Enterprise Security Suite	Компания «Доктор Веб» (прим. 3)
31	XSpider	Компания Positive Technologies (прим. 4)
32	СКЗИ «КриптоПро Рутокен CSP»	Компания КриптоПро (прим. 5)
33	ViPNet	ОАО ИнфоТеКС (прим. 6)
34	ERwin Data Modeler Standard Edition	CA Technologies (лицензия до 2025 г., Contract#: 40217535)
35	Платформа электронного обучения LMS-Moodle, основа Образовательного портала «Электронный университет ВГУ»	Moodle Pty Ltd, GNU General Public License
36	PHP	PHP Group
37	Notepad++	GNU
38	PuTTY	MIT
39	Ramus Educational	Алексей Чижевский
40	ОС GNU/Linux (Ubuntu)	Canonical Ltd, GNU
41	Foxit PDF Reader	корпорация FOXIT SOFTWARE INC., проприетарная бесплатная лицензия
42	Операционная система РЕД ОС	ООО Ред Софт (прим. 9)
43	Система виртуализации РЕД Виртуализация	ООО Ред Софт (прим. 9)

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, реферат
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

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
Промежуточная аттестация форма контроля – зачет				

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: устный опрос, темы рефератов.

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.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, практические работы). При оценивании используется количественная шкала. Критерии оценивания приведены таблице.

Критерии оценивания компетенций и шкала оценок

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

20.2. Промежуточная аттестация

Контроль успеваемости по дисциплине осуществляется с помощью контрольной работы на проверку знаний по дисциплине и собеседования по ее результатам.

Для оценивания результатов обучения на зачете с оценкой используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение проводить обоснование и представление основных теоретических и практических результатов (теорем, алгоритмов, методик) с использованием математических выкладок, блок-схем, структурных схем и стандартных описаний к ним;

3) умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторно-практических заданий;

4) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций):

– высокий (углубленный) уровень сформированности компетенций;
– повышенный (продвинутый) уровень сформированности компетенций;
– пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на зачете с оценкой используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

В ходе промежуточной аттестации используется контрольно-измерительный материал, включающий в себя два-три вопроса.

Оценивание уровня сформированности компетенций осуществляется по содержанию вопросов, приведенных ниже.

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 государствен-

ной 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.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на зачете с оценкой представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно