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.45 Комплексное обеспечение защиты информации объекта информатизации

1. Шифр и наименование направления подготовки/специальности:
10.03.01 Информационная безопасность

2. Профиль подготовки/специализации: Безопасность компьютерных систем

3. Квалификация (степень) выпускника: бакалавр

4. Форма образования: очная

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

6. Составители программы:
Мальцев Алексей Сергеевич, к.т.н.

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

8. Учебный год: 2027-2028 **Семестр(ы):** 8

9. Цели и задачи учебной дисциплины:

Целями освоения учебной дисциплины являются:

– изучение основ и овладение практическими навыками планирования, развертывания и поддержания комплекса регламентов и процедур, направленных на минимизацию рисков нарушения информационной безопасности на объектах информатизации.

Задачи учебной дисциплины:

– формирование системного подхода к оценке угроз безопасности информации на объектах информатизации и комплексного обеспечения их защиты;

– освоение студентами положений и требований, современных нормативно-методических документов, регламентирующих меры, обеспечивающие информационную безопасность на объектах информатизации;

– формирование представления о процедурах подготовки объектов информатизации к эксплуатации, включая вопросы применения мер и средств защиты информации и аттестации объектов;

– овладение практическими навыками разработки системы документов, регламентирующих требования и меры, обеспечивающие информационную безопасность на объектах информатизации.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к блоку Б1 обязательных дисциплин общепрофессиональной части.

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-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1	знает принципы и порядок работы информационно-справочных систем	знает принципы и порядок работы информационно-справочных систем
		ОПК-8.2	знает способы поиска и обработки информации, методы работы с научной информацией, принципы и правила построения суждений и оценок	знает способы поиска и обработки информации, методы работы с научной информацией, принципы и правила построения суждений и оценок
		ОПК-8.3	умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности	умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности
		ОПК-8.4	умеет различать факты, интерпретации, оценки и аргументированно отстаивать свою позицию в процессе коммуникации	умеет различать факты, интерпретации, оценки и аргументированно отстаивать свою позицию в процессе коммуникации
		ОПК-8.5	умеет пользоваться информационно-справочными системами	умеет пользоваться информационно-справочными системами

		ОПК-8.6	владеет навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов	владеет навыком составления и оформления реферата по результатам обзора научно технической литературы, нормативных и методических документов
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1	знает принципы формирования политики информационной безопасности в информационных системах	знает принципы формирования политики информационной безопасности в информационных системах;
		ОПК-12.2	знает принципы организации информационных систем в соответствии с требованиями по защите информации	знает принципы организации информационных систем в соответствии с требованиями по защите информации;
		ОПК-12.3	знает требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации	знает требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации;
		ОПК-12.4	знает основные этапы процесса проектирования и общие требования к содержанию проекта	знает основные этапы процесса проектирования и общие требования к содержанию проекта;
		ОПК-12.5	умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
		ОПК-12.6	умеет анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	умеет анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;
		ОПК-12.7	умеет формировать требования и раз-	умеет формировать требования и разрабатывать внешние специфи-

			рабатывать внешние спецификации для разрабатываемого программного обеспечения	кации для разрабатываемого программного обеспечения;
		ОПК-12.8	умеет оценивать информационные риски в автоматизированных системах	умеет оценивать информационные риски в автоматизированных системах;
		ОПК-12.9	умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений	умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений;

12. Объем дисциплины в зачетных единицах/час — 4/144.
Форма промежуточной аттестации: *экзамен*.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра	№ семестра 8	Итого
Аудиторные занятия		72		72	72
в том числе:	лекции	36		36	36
	практические	36		36	36
	лабораторные				
Самостоятельная работа		36		36	36
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – 36 час.)*		36		36	36
Итого:		144		144	144

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.	Защита информации на объекте информатизации. Общие положения	1. Понятие, сущность и актуальность предмет и объект защиты информации. 2. Основные определения и задачи информационной безопасности.	Создан электронный онлайн - курс, раз-

		3. Лицензирование деятельности в области защиты государственной тайны 4. Общие вопросы аттестации объектов информатизации. 5. Система сертификации средств защиты информации.	мещены материалы к лекциям и лабораторным занятиям
2.	Технические каналы утечки информации	1. Общая характеристика и классификация технического канала утечки информации. 2. Исследование технических каналов утечки информации	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям
3.	Требования к защите информации в информационных системах	1. Формирование требований к защите информации, содержащейся в информационной системе 2. Разработка системы защиты информации информационной системы 3. Внедрение системы защиты информации информационной системы 4. Аттестация информационной системы и ввод ее в действие 5. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы 6. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации 7. Требования к мерам защиты информации, содержащейся в информационной системе 8. Определение класса защищенности информационной системы	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям
4.	Методика определения угроз безопасности информации в информационных системах	1. Порядок оценки угроз безопасности информации 2. Определение негативных последствий от реализации (возникновения) угроз безопасности информации 3. Определение возможных объектов воздействия угроз безопасности информации 5. Оценка возможности реализации (возникновения) угроз 6. Формирование экспертной группы и проведение экспертной оценки при оценке угроз безопасности информации 7. Анализ структуры модели угроз безопасности информации 8. Анализ видов рисков (ущерба) и типовые негативные последствия от реализации	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям

		угроз безопасности информации 9. Определения объектов воздействия и видов воздействия на них 10. Возможные цели реализации угроз безопасности информации нарушителями 11. Пример оценки целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации 12. Уровни возможностей нарушителей по реализации угроз безопасности информации 13. Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности 14. Анализ перечня основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации	
5.	Методика моделирования угроз безопасности информации	1. Порядок моделирования угроз безопасности информации и разработки моделей угроз безопасности информации 2. Определение возможных негативных последствий от реализации угроз безопасности информации 3. Оценка условий реализации угроз безопасности информации	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям
6.	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных	1. Классификация угроз безопасности персональных данных. 2. Угрозы утечки информации по техническим Каналам 3. Угрозы несанкционированного доступа к информации в информационной системе персональных данных. 4. Общая характеристика источников угроз, уязвимостей и угроз непосредственного доступа в операционную среду информационной системы. 5. Общая характеристика угроз безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия. 6. Общая характеристика угроз программно-математических воздействий, нетрадиционных информационных каналов, результатов несанкционированного или случайного доступа. 7. Типовые модели угроз безопасности персональных данных, обрабатываемых в ин-	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям

		формационных системах персональных данных	
7.	Меры защиты информации в государственных информационных системах	1. Выбор мер защиты информации для их реализации в информационной системе в рамках системы защиты информации 2. Содержание мер защиты информации в информационной системе	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям
2. Практические занятия			
2.1	нет		
3. Лабораторные работы			
3.1	Методы и средства защиты информации на объекте информатизации	1. Контроль уязвимостей на уровне операционных систем и прикладного ПО 2. Контроль уязвимостей на уровне системы управления базами данных 3. Проверка организации контроля доступа клиентсерверных приложений к объектам баз данных. Разграничение полномочий пользователей с использованием ролей и привилегий 4. Детальный контроль доступа пользователей к базам данных 5. Мандатный контроль доступа пользователей 6. Контроль аудита действий пользователей средствами разработчика, встроенными средствами СУБД, аудит действий пользователя с привилегией «sysdba» 7. Контроль детального аудита действий пользователей в СУБД 8. Контроль восстановления базы данных при разных сценариях потери/повреждения файлов, физического копирования и архивирования данных 9. Контроль восстановления базы данных методами логического копирования	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Лабораторные работы	Сам. работа	Промежуточная аттестация (экзамен)	Всего
1.	Защита информации на объекте информатизации. Общие положения	6	4	4		

2.	Технические каналы утечки информации	4	4	6		
3.	Требования к защите информации в информационных системах	4	4	6		
4.	Методика определения угроз безопасности информации в информационных системах	6	4	6		
5.	Методика моделирования угроз безопасности информации	2	4	6		
6.	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных	8	8	4		
7.	Меры защиты информации в государственных информационных системах	6	8	4		
8.	Экзамен				36	36
	Итого:	36	36	36	36	144

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;
- электронные версии учебников и методических указаний для выполнения практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении практических занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка знаний основ информационной безопасности.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций онлайн и проведения практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

5) 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	Казарин Олег Викторович. Программно-аппаратные средства защиты информа-

	ции. Защита программного обеспечения : учебник и практикум для вузов : [для студ. вузов, обучающихся по инженер.-техн. направлениям] / О.В. Казарин, А.С. Забабурин .— Москва : Юрайт, 2018 .— 311, [1] с. : ил., табл. — (Специалист) .— Библиогр. в конце гл. — ISBN 978-5-9916-9043-0.
2	Баранова Елена Константиновна. Информационная безопасность и защита информации : учебное пособие : [для студ., обучающихся по направлению "Прикладная информатика"] / Е.К. Баранова, А.В. Бабаш .— 4-е изд. перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019 .— 334, [1] с. : ил., табл. — (Высшее образование) .— Библиогр.: с. 327-330 .— ISBN 978-5-369-01761-6 .— ISBN 978-5-16-013849-7.
3	Мельников, Владимир Павлович. Информационная безопасность : [учебник для студ. вузов, обучающихся по направлениям подготовки "Конструкторско-технологическое обеспечение машиностроительных производств", "Автоматизация технологических процессов и производств"] / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева ; под ред. В.П. Мельникова .— 2-е изд., перераб. и доп. — Москва : КноРус, 2018 .— 371 с. : ил., цв. ил., табл. — (Бакалавриат) .— Библиогр.: с. 369-371.

б) дополнительная литература:

№ п/п	Источник
1	Ищейнов Вячеслав Яковлевич. Защита конфиденциальной информации : [учебное пособие для студ. вузов., обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 «Комплексная защита объектов информатизации»] / В.Я. Ищейнов, М.В. Мецатунян .— М. : ФОРУМ, 2009 .— 254 с. : ил. — (Высшее образование) .— Библиогр.: с.249-254 .— ISBN 978-5-91134-336-1.
2	Хорев Павел Борисович. Методы и средства защиты информации в компьютерных системах: учебное пособие для студ. вузов, обуч. по направлению 230100 (654600) "Информатика и вычислительная техника" / П.Б. Хорев .— М. : ACADEMIA, 2005 .— 254, [1] с. : ил. — (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с. 251-252 .— ISBN 5-7695-1839-1.
3	Малюк Анатолий Александрович. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие для студ. вузов, обуч. по специальности 075400 - "Комплексная защита объектов информации" / А.А. Малюк .— М. : Горячая линия-Телеком , 2004 .— 280 с. : ил/ .— (Учебное пособие) .— Библиогр.: с. 276-278 .— ISBN 5-93517-197-X.
4	Галицкий, Александр Владимирович. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин .— М. : ДМК Пресс, 2004 .— 613 с. : ил .— (Администрирование и защита) .— Библиогр.: с.599-608 .— Предм. указ.:с.603-613 .— ISBN 5-94074-244-0.
5	Варлатая Светлана Климентьевна. Защита и обработка конфиденциальных документов : учебно-методический комплекс / С.К. Варлатая, М.В. Шаханова ; Дальневост. федер. ун-т .— Москва : Проспект, 2015 .— 178, [1] с. : ил., табл. — Библиогр.: с. 177 .— ISBN 978-5-392-19176-5
6	Андрианов В. И. "Шпионские штучки 2", или Как сберечь свои секреты / Под общ. ред. Колесниченко О. В. и др. — СПб. : Полигон, 1997 .— 271 с. — ISBN 5-89173-015-4 : 12.33.

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.)*

№ 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.

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

Для реализации учебного процесса используются:

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).

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

1) 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, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры).

2) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 292

Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam Group и ноутбук 15.6’’ FHD Lenovo V155-15API

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

3) 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, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

4) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 290

Учебная аудитория: специализированная мебель, персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27'' (12 шт.), мультимедийный проектор, экран.

Лабораторное оборудование искусственного интеллекта: рабочие места – персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); модули АО НПЦ «ЭЛВИС»: процессорный Салют-ЭЛ24ПМ2 (9 шт.), отладочный Салют-ЭЛ24ОМ1 (9 шт.), эмулятор MC-USB-JTAG (9 шт.).

Лабораторное оборудование электроники, электротехники и схемотехники: рабочие ме-ста – персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); стенд для практических занятий по электрическим цепям (KL-100); стенд для изучения аналоговых электрических схем (KL-200); стенд для изучения цифровых схем (KL-300).

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

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.	Защита информации на объекте информатизации. Общие положения	ОПК-8	ОПК-8.1-8.6	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
2.	Технические каналы утечки информации	ОПК-8	ОПК-8.1-8.6	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
3.	Требования к защите информации в информационных системах	ОПК-8 ОПК-12	ОПК-8.1-8.6 ОПК12.1-12.9	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
4.	Методика определения угроз безопасности информации в информационных системах	ОПК-8 ОПК-12	ОПК-8.1-8.6 ОПК12.1-12.9	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
5.	Методика моделирования угроз безопасности информации	ОПК-8 ОПК-12	ОПК-8.1-8.6 ОПК12.1-12.9	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
6.	Базовая модель угроз безопасности персо-	ОПК-8 ОПК-12	ОПК-8.1-8.6 ОПК12.1-12.9	Письменная работа либо тестирование в электронной образова-

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
	нальных данных при их обработке в информационных системах персональных данных			тельной среде на проверку знаний
7.	Меры защиты информации в государственных информационных системах	ОПК-8 ОПК-12	ОПК-8.1-8.6 ОПК12.1-12.9	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
Промежуточная аттестация форма контроля – экзамен				

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 Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Устный опрос по темам/разделам дисциплины; Лабораторные работы.

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Лабораторные работы по разделам дисциплины	Содержит 9 работ, по разделам: Методы и средства защиты информации на объекте информатизации. Контроль эффективности защиты информации на объекте информатизации.	При успешном выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.
3	КИМ промежуточной аттестации	Каждый контрольноизмерительный материал для проведения промежуточной аттестации включает 2 задания для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Критерии оценивания приведены выше

Пример лабораторной работы

Лабораторная работа №1

«Контроль уязвимостей на уровне операционных систем и прикладного ПО»

Цель работы: Получение практических навыков анализа работы сканера безопасности на уровне закрытия уязвимостей.

Вариант задания. Проверка доступности узлов сети. Формирование плана проверок узлов сети. Проведение проверок согласно сформированному плану. Просмотр результатов работы проверок и формирование отчетов.

20.2 Промежуточная аттестация

Примерный перечень вопросов к экзамену

№	Содержание
1	Средства и меры защиты конфиденциальности, целостности, доступности информации на объекте информатизации.
2	Лицензирование деятельности в области защиты информации.
3	Технические каналы утечки информации на объектах информатизации.
4	Организация работ по защите конфиденциальной информации на объекте информатизации
5	Требования и рекомендации по защите речевой конфиденциальной информации.
6	Угрозы утечки информации с использованием линий связи и защита от них.
7	Основные требования и рекомендации по защите информации, циркулирующей в защищаемых помещениях.
8	Материально-вещественные каналы утечки информации.
9	Методы и средства несанкционированного получения информации по техническим каналам.
10	Угрозы несанкционированного доступа к информации в компьютерных системах.
11	Модель угроз безопасности информации.
12	Методика определения угроз безопасности информации в информационных системах.
13	Банк данных угроз безопасности информации.
14	Модель нарушителя безопасности информации.
15	Закладные программно-технические средства и возможные способы защиты от них.
16	Виды ущерба безопасности информации и методы его оценки. Технико-экономическое обоснование комплекса мер по обеспечению информационной безопасности.
17	Методы и средства защиты информации на объекте информатизации.
18	Типовые аппаратные средства защиты информации на объектах информатизации.
19	Типовые программные и программно-аппаратные средства защиты информации на объектах информатизации.
20	Требования и меры безопасности информации при использовании криптографических средств защиты.
21	Комплексное обеспечение защиты информации на объекте информатизации.
22	Контроль эффективности защиты информации на объекте информатизации.
23	Аттестации объекта информатизации по требованиям безопасности информации.
24	Тестирование на проникновение в компьютерных системах.
25	Уязвимости в информационных системах и основные методы защиты.

Пример контрольно-измерительного материала

УТВЕРЖДАЮ

Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота

«____»_____ 2028

Направление подготовки / специальность 10.03.01 Информационная безопасность

Дисциплина Б1.О.45 Комплексное обеспечение защиты информации объекта информатизации

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Средства и меры защиты конфиденциальности, целостности, доступности информации на объекте информатизации.
2. Тестирование на проникновение в компьютерных системах.

Преподаватель _____ А.С. Мальцев

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

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

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, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании используется количественная шкала. Критерии оценивания приведены выше.