Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Сирота Александр Анатольевич

Кафедра технологий обработки и защиты информации

01.07.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.45 Комплексное обеспечение защиты информации объекта информатизации

1. Код и наименование направления подготовки/специальности:

10.03.01 Информационная безопасность

2. Профиль подготовки/специализация:

Безопасность компьютерных систем

3. Квалификация (степень) выпускника:

Бакалавриат

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Степанцов Вячеслав Алексеевич, кандидат технических наук, доцент

7. Рекомендована:

протокол Ученого совета ФКН №6 от 07.06.2021

8. Учебный год:

2024-2025

9.Цели и задачи учебной дисциплины:

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

Основные задачи 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:

Блок Б1.О обязательные дисциплины.
Входные знания в области физики, распространения сигналов, основ информационной безопасности, организационного и правового обеспечения информационной безопасности, программно-аппаратных средств защиты информации.

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

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
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 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	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 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	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

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	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 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.5 умеет пользоваться информационно-справочными системами	умеет пользоваться информационно-справочными системами
ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	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;

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	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 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	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 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	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 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.5 умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;	умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	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 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.7 умеет формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;	умеет формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.8 умеет оценивать информационные риски в автоматизированных системах;	умеет оценивать информационные риски в автоматизированных системах;
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	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	Семестр 8	Всего
Аудиторные занятия	72	72
Лекционные занятия	36	36
Практические занятия		0
Лабораторные занятия	36	36
Самостоятельная работа	36	36
Курсовая работа		0
Промежуточная аттестация	36	36
Часы на контроль	36	36
Всего	144	144

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
	Лекции		
1	Защита информации на объекте информатизации,основные положения.	1. Защита конфиденциальности, целостности, доступности. Средства и меры защиты. Комплексное обеспечение защиты информации. 2. Лицензирование деятельности в области защиты информации. Сертификация средств защиты информации.	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
2	Технические каналы утечки информации	3. Технические каналы утечки информации. Классификация, причины и источники образования. 4. Радиоканалы. Акустические каналы. Электрические каналы. 5. Линии связи. Визуально-оптические каналы. 6. Материально-вещественные каналы. 7. Методы и средства несанкционированного получения информации по техническим каналам.	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
3	Угрозы несанкционированного доступа к информации в компьютерных системах	8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). (https://fstec.ru/component/attachments/download/289). Банк данных угроз безопасности информации ФСТЭК России, http://bdu.fstec.ru/. 9. Методика определения угроз безопасности информации в информационных системах, проект, ФСТЭК России, май 2015 г., (http://fstec.ru/component/attachments/download/812). 10. Меры защиты информации в государственных информационных системах. Методические документы ФСТЭК России. (https://fstec.ru/component/attachments/download/675). 11. Методика моделирования угроз безопасности информации. Методические документы ФСТЭК России. (https://fstec.ru/component/attachments/download/2727).	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
4	Методы и средства защиты информации на объекте информатизации	12. Правовые и организационные методы и средства защиты информации на объекте информатизации. 13. Физические, технические методы и средства защиты информации на объекте информатизации. 14. Программные методы защиты информации на объекте информатизации. 15. Криптографические средства защиты информации.	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
5	Контроль эффективности защиты информации на объекте информатизации.	16. Документы, необходимые для ввода объекта информатизации в эксплуатацию. 17. Аттестации объекта информатизации по требованиям безопасности информации. 18. Тестирование на проникновение в компьютерных системах.	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
	Лабораторные занятия		
1	Методы и средства защиты информации на объекте информатизации	Контроль уязвимостей на уровне операционных систем и прикладного ПО	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
2	Методы и средства защиты информации на объекте информатизации	Контроль уязвимостей на уровне системы управления базами данных	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
3	Методы и средства защиты информации на объекте информатизации	Проверка организации контроля доступа клиент-серверных приложений к объектам баз данных. Разграничение полномочий пользователей с использованием ролей и привилегий	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
4	Методы и средства защиты информации на объекте информатизации	Детальный контроль доступа пользователей к базам данных	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
5	Методы и средства защиты информации на объекте информатизации	Мандатный контроль доступа пользователей	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
6	Методы и средства защиты информации на объекте информатизации	Контроль аудита действий пользователей средствами разработчика, встроенными средствами СУБД, аудит действий пользователя с привилегией «sysdba»	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
7	Методы и средства защиты информации на объекте информатизации	Контроль детального аудита действий пользователей в СУБД	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
8	Контроль эффективности защиты информации на объекте информатизации.	Контроль восстановления базы данных при разных сценариях потери/повреждения файлов, физического копирования и архивирования данных	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
9	Контроль эффективности защиты информации на объекте информатизации.	Контроль восстановления базы данных методами логического копирования	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Защита информации на объекте информатизации,основные положения.	4			2	6
2	Технические каналы утечки информации	10			4	14
3	Угрозы несанкционированного доступа к информации в компьютерных системах	8			4	12

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
4	Методы и средства защиты информации на объекте информатизации	8		28	18	54
5	Контроль эффективности защиты информации на объекте информатизации.	6		8	8	22
		36	0	36	36	108

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 лабораторно-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 лабораторных занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.
4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций онлайн и проведения лабораторно- 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. В ходе самостоятельной работы необходимо уделить основное внимание работе с текстом конспекта лекции, изучению рекомендованной литературы, изучению нормативных документов по информационной безопасности.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

№ п/п	Источник
1	Казарин Олег Викторович. Программно-аппаратные средства защиты информации. 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.

№ п/п	Источник
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

№ п/п	Источник
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:

№ п/п	Источник
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
2	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/).
3	«Университетская библиотека online» - Контракт № 3010-06/05-20 от 28.12.2020 «Консультант студента» - Контракт № 3010-06/06-20 от 28.12.2020 ЭБС «Лань» - Контракт №3010-06/04-21 от 10.03.2021 ЭБС «Лань» - Контракт №3010-06/03-21 от 10.03.2021 «РУКОНТ» (ИТС Контекстум) - Договор ДС-208 от 01.02.2021
4	Меры защиты информации в государственных информационных системах. Методические документы ФСТЭК России. (https://fstec.ru/component/attachments/download/675)
5	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) (https://fstec.ru/component/attachments/download/289)
6	Методика определения угроз безопасности информации в информационных системах, проект, ФСТЭК России, май 2015 г., Методический документ. (http://fstec.ru/component/attachments/download/812).
7	Методика моделирования угроз безопасности информации. Методические документы ФСТЭК России. (https://fstec.ru/component/attachments/download/2727).
8	Банк данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru/).

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Грибунин Вадим Геннадьевич. Комплексная система защиты информации на предприятии : [учебное пособие для студ. вузов, обуч. по специальностям "Организация и технология защиты информации", "Комплекс. защита объектов информатизации" направления подготовки "Информ. безопасность"] / В.Г. Грибунин, В.В. Чудовский .— М. : Академия, 2009 .— 411, [1] с. : ил., табл. — (Высшее профессиональное образование. Информационная безопасность) .— Библиогр.: с.403-406.

№ п/п	Источник
2	Методика определения угроз безопасности информации в информационных системах, проект, ФСТЭК России, май 2015 г., Методический документ. (http://fstec.ru/component/attachments/download/812).

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. ПО MATLAB Classroom ver. 7.0, 10 конкурентных бессрочных лицензий на каждый, компоненты: Matlab, Simulink, Stateflow, 1 тулбокс, N 21127/VRN3 от 30.09.2011 (за счет проекта ЕК TEMPUS/ERAMIS).
3. ПО Матлаб в рамках подписки "Университетская лицензия на программный комплекс для ЭВМ - MathWorks, Headcount – 25 ": лицензия до 31.01.2022, сублицензионный контракт 3010-07/01-19 от 09.01.19.
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:

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 381), ПК-Intel-i3, рабочее место преподавателя: проектор, видеокоммутатор, специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.
2) Компьютерный класс (один из №1-4 корп. 1а, ауд. № 382-385), ПК-Intel-i3 16 шт., оснащенный программным обеспечением в виде среды виртуализации VMware, образами операционных систем семейства Windows и имеющими доступ в сеть Интернет, специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Защита информации на объекте информатизации,основные положения. Угрозы несанкционированного доступа к информации в компьютерных системах	ОПК-8	ОПК-8.1	Устный опрос

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
2	Угрозы несанкционированного доступа к информации в компьютерных системах	ОПК-8	ОПК-8.2	Устный опрос
3	Угрозы несанкционированного доступа к информации в компьютерных системах	ОПК-8	ОПК-8.3	Устный опрос
4	Угрозы несанкционированного доступа к информации в компьютерных системах Контроль эффективности защиты информации на объекте информатизации.	ОПК-8	ОПК-8.4	Устный опрос Лабораторные работы
5	Угрозы несанкционированного доступа к информации в компьютерных системах	ОПК-8	ОПК-8.5	Устный опрос
6	Угрозы несанкционированного доступа к информации в компьютерных системах Контроль эффективности защиты информации на объекте информатизации.	ОПК-8	ОПК-8.6	Устный опрос Лабораторные работы
7	Защита информации на объекте информатизации,основные положения.	ОПК-12	ОПК-12.1	Устный опрос
8	Защита информации на объекте информатизации,основные положения. Угрозы несанкционированного доступа к информации в компьютерных системах Контроль эффективности защиты информации на объекте информатизации.	ОПК-12	ОПК-12.2	Устный опрос
9	Угрозы несанкционированного доступа к информации в компьютерных системах	ОПК-12	ОПК-12.3	Устный опрос

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
10	Угрозы несанкционированного доступа к информации в компьютерных системах	ОПК-12	ОПК-12.4	Устный опрос
11	Технические каналы утечки информации Методы и средства защиты информации на объекте информатизации	ОПК-12	ОПК-12.5	Устный опрос Лабораторные работы
12	Защита информации на объекте информатизации,основные положения. Контроль эффективности защиты информации на объекте информатизации.	ОПК-12	ОПК-12.6	Устный опрос Лабораторные работы
13	Контроль эффективности защиты информации на объекте информатизации.	ОПК-12	ОПК-12.7	Устный опрос Лабораторные работы
14	Защита информации на объекте информатизации,основные положения. Контроль эффективности защиты информации на объекте информатизации.	ОПК-12	ОПК-12.8	Устный оп росЛабораторные работы
15	Контроль эффективности защиты информации на объекте информатизации.	ОПК-12	ОПК-12.9	Устный опрос Лабораторные работы

Промежуточная аттестация

Форма контроля - Экзамен

Оценочные средства для промежуточной аттестации

Для оценивания результатов обучения на экзамене (зачете) используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):
1. знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;
2. умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными;
3. умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу.
Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;

- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – «зачтено» («отлично», «хорошо», «удовлетворительно»), «не зачтено» («неудовлетворительно»).
Соотношение показателей, критериев и шкалы оценивания результатов обучения на экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на экзамене

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	–	Неудовлетворительн

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 контрольно-измерительный 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

«___»_____ 2021

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 _____ В.А. Степанцов

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.