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

«Утверждаю»
Заведующий кафедрой ТО и ЗИ

А.А. Сирота
«23» 04 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.52 Методы оценки безопасности компьютерных систем

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

2. Профиль подготовки / специализация/магистерская программа:
Безопасность компьютерных систем

3. Квалификация (степень) выпускника:
Бакалавр

4. Форма обучения:
Очная

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

6. Составители программы:
Вялых Сергей Ариевич, кандидат технических наук

7. Рекомендована:
протокол НМС ФКН № 5 от 05.03.2024 г.

8. Учебный год: 2026-2027 **Семестр(ы):** 6

9. Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

изучение основ и принципов построения защищенных информационных систем, требований разработки и применения в них средств защиты информации, овладение практическими методами и навыками выбора, подготовки и проведения комплекса процедур, направленных на оценку безопасности при проектировании, эксплуатации и выводе из эксплуатации информационных систем различного назначения; получение профессиональных компетенций в области современных технологий обработки и защиты информации.

Задачи дисциплины:

- освоение студентами положений и требований, современных нормативно-методических документов, регламентирующих меры, обеспечивающие информационную безопасность информационных систем различного назначения;
- формирование представления о возможных методах оценки безопасности компьютерных систем в организации;
- овладение практическими навыками разработки и оценки системы документов, регламентирующих требования и меры, обеспечивающие информационную безопасность в информационных системах различного назначения, разработки модели угроз, выявления и анализа уязвимостей информационной безопасности;
- формирование представления о процедурах практической реализации процессов, направленных на оценку безопасности информационных систем различного назначения и контроля выполнения мер по защите информации.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к профессиональному циклу дисциплин и блоку обязательных дисциплин базовой профильной части Б1.О.

Для успешного освоения дисциплины необходимы входные знания в области операционных систем, принципах их работы, сетевых технологий, теории вероятностей, основ информационной безопасности, программно-аппаратных средств защиты информации, криптографических методов защиты информации, требований обеспечения информационной безопасности в информационных системах различного назначения.

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 -1.4	Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ОПК-1.4.1	знает требования стандартов по оценке уровня безопасности;	**Знать:** нормативные и методические документы в области информационной безопасности: Федеральные законы; постановления Правительства РФ; приказы и методики ФСТЭК России; приказы и методики ФСБ России; рекомендации и требования Минцифры России; рекомендации и требования Роскомнадзора. **Уметь**: определять классы защищенности автоматизированных систем и средств вычислительной техники; классы защищенности государственных информационных систем; уровни защищенности персональных данных; класс средств криптозащиты информации; обосновывать требования безопасности информации для ин-
		ОПК-1.4.2	умеет определять уровень безопасности и соответствие профилю защиты;	
		ОПК-1.4.3	знает источники угроз информационной безопасности в компьютерных системах и сетях и меры по их предотвращению;	
		ОПК-1.4.4	умеет анализировать угрозы безопасности информации в компьютерных системах и сетях;	

				формационных систем различного назначения и проводить оценку эффективности их защиты; осуществлять анализ информационных систем на наличие уязвимостей и обеспечивать их устранение; определять актуальные угрозы безопасности информации. **Владеть**: практическими навыками применения нормативно методических документов по информационной безопасности при создании защищенных информационных систем для обоснования требований и оценки их защищенности; навыками использования инструментальных средств анализа уязвимостей; методиками оценки и определения возможных нарушителей безопасности информации и актуальных угроз безопасности информации в оцениваемых информационных системах.

12. Объем дисциплины в зачетных единицах/час — 3/108.
Форма промежуточной аттестации: *экзамен.*

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра 6	№ семестра	…
Аудиторные занятия		60	68		
в том числе:	лекции	30	30		
	лабораторные	30	30		
	контроль	36	36		
Самостоятельная работа		12	12		
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(экзамен – __час.)*					
Итого:		108	108		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Оценка безопасности компьютерных систем. Основные методы и цели.	1. Введение. Обзор методов и методик оценки безопасности программно-аппаратных средств и информационных систем. Цели оценки безопасности компьютерных систем. Требуемая точность оценки. Основные методы оценки.	

1.2	Практические подходы. Средства анализа уязвимостей информационных систем.	2. Средства анализа уязвимостей информационных систем и их основные возможности.	
1.3	Модели информационных систем.	3. Моделирование информационных систем и оценка возможностей реализации угроз безопасности информации (математические методы, экспертные методы, базовая модель угроз, банк данных угроз безопасности информации, банк данных об уязвимостях программного обеспечения и программно-аппаратных средств).	
1.4	Оценка средств защиты информации	4. Понятие сертификации. Реестры сертифицированных средств защиты информации.	
1.5	Государственная информационная система, классы защищённости информационной системы	5. Государственная информационная система, классы защищённости информационной системы. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Аттестация государственной информационная системы и оценка эффективности принимаемых мер защиты информации.	
1.6	Обеспечение безопасности персональных данных при их обработке в информационных системах	6. Определение уровня защищенности информационных систем персональных данных. Определение требований защиты персональных данных. Оценка эффективности принимаемых мер защиты персональных данных в информационных системах персональных данных.	
1.7	Требования безопасности информации при использовании криптографических средств защиты	7. Криптографические средства защиты информации. Приказ ФСБ № 378 от 10 июля 2014 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности». Приказ ФСБ России от 24 октября 2022г № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств».	
1.8	Модели угроз безопасности информации.	8. Методика определения угроз безопасности информации в информационных системах. 9. Модель и оценка возможного нарушителя. 10. Модель угроз безопасности информации. Оценка актуальных угроз безопасности информации.	
1.9	Оценка (контроль) выполнения требований по обеспечению безопасности информации	11. Оценка (контроль) выполнения требований по обеспечению безопасности информации в государственных информационных системах и информационных системах персональных данных.	
2. Практические занятия			
2.1	нет		
3. Лабораторные работы			
3.1	Средства анализа уязвимостей информационных систем.	1. Исследование возможностей средства анализа уязвимостей ScanOval. 2. Исследование возможностей средства анализа уязвимостей СканерВС.	
3.2	Государственная информационная система, классы защищённости информационной системы	3. Определение класса защищенности государственной информационной системы. Формирование требований к мерам защиты информации для различных классов защищенности в государственных информационных системах и оценка их выполнения.	

3.3	Обеспечение безопасности персональных данных при их обработке в информационных системах	4. Определение уровня защищенности информационной системы, обрабатывающей персональные данные. Формирование требований к мерам защиты информации для различных уровней защищенности в информационных системах обрабатывающих персональные данные и оценка их выполнения.	
3.4	Требования безопасности информации при использовании криптографических средств защиты	5. Формирование состава и содержания организационных и технических мер по обеспечению безопасности в информационных системах персональных с использованием средств криптографической защиты. 6. Формирование состава и содержания организационных и технических мер по обеспечению безопасности в государственных информационных системах с использованием средств криптографической защиты.	
3.5	Модели угроз безопасности информации	7. Определение источников угроз безопасности информации. 8. Оценка негативных последствий от реализации угроз безопасности информации. 9. Оценка возможностей нарушителей по реализации угроз безопасности информации (разработка модели нарушителя). 10. Оценка возможных способов реализации угроз безопасности информации. 11. Оценка возможных тактик и стратегий реализации угроз безопасности информации. 12. Определение актуальных угроз безопасности информации в информационной системе. 13. Определение угроз безопасности информации при использовании средств криптографической защиты. 14. Разработка модели угроз безопасности информации в информационной системе.	
3.6	Оценка (контроль) выполнения требований по обеспечению безопасности информации.	15. Оценка (контроль) выполнения требований по обеспечению безопасности информации: в государственных информационных системах; в информационных системах обрабатывающих персональные данные; в информационных системах использующих средства криптозащиты информации.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Лабораторные	Сам. работа	Контроль	Всего
1	Оценка безопасности компьютерных систем. Основные методы и цели.	4	-	-	2	6
2	Практические подходы. Средства анализа уязвимостей информационных систем.	2	4	2	4	12
3	Модели информационных систем.	4	-	-	2	6
4	Оценка средств защиты информации.	2	-	-	2	4
5	Государственная информационная система, классы защищённости информационной системы.	4	6	2	6	18
6	Обеспечение безопасности персональных данных при их обработке в информационных системах	4	4	2	6	16
7	Требования безопасности информации при использовании криптографических средств защиты.	2	6	2	6	16
8	Модели угроз безопасности информации.	4	6	2	4	16

9	Оценка (контроль) выполнения требований по обеспечению безопасности информации	4	4	2	4	14
	Итого:	30	30	12	36	108

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

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.

В ходе самостоятельной работы необходимо уделить основное внимание работе с текстом конспекта лекции, изучению рекомендованной литературы, изучению нормативных документов по информационной безопасности.

4) При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online 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	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
2	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.

б) дополнительная литература:

№ п/п	Источник
3	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с. : ил .— (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
4	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.

5	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451
6	Приказ Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета, № 136, 26.06.2013.
7	Приказ Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета, № 107, 22.05.2013.
8	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).
9	Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.
10	Приказ ФСБ № 378 от 10 июля 2014 г. «Об утвер-ждении состава и содержания организационных и технических мер по обеспечению безопасности пер-сональных данных при их обработке в информаци-онных системах персональных данных с использова-нием средств криптографической защиты информа-ции, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уров-ней защищенности».
11	Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8-го Центра ФСБ России 31.03.2015 № 149/7/2/6-432.
12	Приказ ФСБ России от 24 октября 2022г № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (крипто-графических) средств».
11	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.
12	Постановление правительства Воронежской области от 28 апреля 2011 года № 340 «Об утверждении положения о едином реестре государственных информационных систем Воронежской области» // Собрание законодательства Воронежской области 20.06.2011 № 4, ст. 285.

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

№ п/п	Ресурс
13	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
14	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
15	Методический документ. Методика определения угроз безопасности информации в информационных системах, проект, ФСТЭК России, май 2015 г., http://fstec.ru/component/attachments/download/812.
16	Методика оценки угроз безопасности информации. ФСТЭК России, февраль 2021 г., https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/2169-informatsionnoe-soobshchenie-fstek-rossii-ot-15-fevralya-2021-g-n-240-22-690
17	Банк данных угроз безопасности информации, ФСТЭК России, март 2015 г., http://bdu.fstec.ru/
18	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), ЭБС «Университетская библиотека online» (Контракт №3010 06/11 23 от 26.12.2023 (с 26.12.2023 по 25.12.2024), ЭБС «Консультант студента» – Лицензионный договор №980КС/12-2023 / 3010-06/01-24 от 24.01.2024 с 24.01.2024 по 11. 01.2025), 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), ЭБС BOOK.ru, Договор №3010 15/983 23 от 20.12.2023, (с 01.02.2024 по 31.01.2025)

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	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.
2	Методический документ. Методика определения угроз безопасности информации в информационных системах, проект, ФСТЭК России, май 2015 г., http://fstec.ru/component/attachments/download/812.
3	Методический документ. Методика определения угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г. https://fstec.ru/component/attachments/download/2919

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

Для реализации учебного процесса используется установленная версия пакета среды виртуализации Oracle VM VirtualBox; образы операционных систем семейства Windows v.7, 8, 10; доступ в сеть Интернет; LibreOffice v.5-7; Foxit PDF Reader; Dr. Web Enterprise Security Suite; ScanOval; Kali Linux; Справочно-правовая система (СПС) Консультант+ для образования.

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

1) Учебная аудитория (компьютерный класс) (одна из №1-4 корп. 1а, ауд. № 382-385): специализированная мебель, персональные компьютеры на базе i5-9600KF-3,7ГГц, мониторы ЖК 24'' (16 шт.), 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, выход в Интернет.ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

2) Для проведения лабораторных и практических работ. Компьютерный класс (один из №1-3 корп. 1а, ауд. № 290, 293, 383), ПК-Intel-i7 16 шт. (с оперативной памятью не менее 8 гигабайт, рекомендуется 16 гигабайт), 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, выход в Интернет.

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.	Разделы 1.1-1.7. Основные подходы оценки безопасности информационных систем и средств.	ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями ОПК-1.4.1 знает требования стандартов по оценке уровня безопасно-сти;	**Знать:** нормативные и методические документы в области информационной безопасности: Федеральные законы; постановления Правительства РФ; приказы и методики ФСТЭК России; приказы и методики ФСБ России; рекомендации и требования Минцифры России; рекомендации и требования Роскомнадзора. **Уметь:** определять классы защищенно-сти автоматизированных систем и средств вычислительной техники; классы защищенности государственных информационных систем; уровни защищенности персональных данных; класс средств криптозащиты информации; обосновывать требования безопасности информации для информационных систем различного назначения и проводить оценку эффективности их защиты; осуществлять анализ информационных систем на наличие уязвимостей и обеспечивать их устранение; определять актуальные угрозы безопасности информации. **Владеть:** практическими навыками применения нормативно методических документов по информационной безопасности при создании защищенных информационных систем для обоснования требований и оценки их защищенности; навыками использования инструментальных средств анализа уязвимостей; методиками оценки и определения возможных нарушителей безопасности информации и актуальных угроз безопасности ин-формации в оцениваемых ин-формационных системах.	Устный опрос. Лабораторные работы 1-6. Контрольная работа по соответствующим разделам или тест
2.	Разделы 1.5-1.7 Требования безопасности информации при использовании криптографических средств защиты средств защиты информации	ОПК-1.4.2 умеет определять уровень безопасности и соответствие профилю защиты;		Устный опрос. Лабораторные работы 3-6. Контрольная работа по соответствующим разделам или тест
3.	Разделы 1.1-1.8 Моделирование угроз безопасности информации	ОПК-1.4.3 знает источники угроз информационной безопасности в компьютерных системах и сетях и меры по их предотвращению;		Устный опрос. Лабораторные работы 1-15. Контрольная работа по соответствующим разделам или тест
4.	Разделы 1.1-1.9 Оценка (контроль) выполнения требований по обеспечению безопасности информации	ОПК-1.4.4 умеет анализировать угрозы безопасности информации в компьютерных системах и сетях;		Устный опрос. Лабораторные работы 1-15. Контрольная работа по соответствующим разделам или тест

Промежуточная аттестация форма контроля – контрольная работа	Комплект КИМ

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; Контрольная работа по теоретической части курса; Лабораторные работы

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2
3	Лабораторная работа	Содержит 15 лабораторных заданий, предусматривающие разработку требований по уровням и классам защищенности различных информационных систем, разработки и внедрения их систем защиты, а также контроля ее эффективности.	При успешно выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.
4	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 заданий вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 20.2

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине

Компетенция ОПК-1.4

Задания закрытого типа

1. **На каких этапах жизненного цикла государственной информационной системы должна обеспечиваться в ней защита информации?**

а) на этапе создания информационной системы;

б) на этапе создания информационной системы и в ходе ее эксплуатации;

в) на этапе создания информационной системы, в ходе ее эксплуатации, в том числе при развитии (модернизации);

г) должна носить систематический характер и осуществляться как на этапе создания системы, так и в ходе ее эксплуатации, в том числе при развитии (модернизации);

д) на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации;

2. На каких этапах жизненного цикла государственной информационной системы должна осуществляться оценка угроз безопасности информации?

а) на этапе создания информационных систем;

б) на этапе создания информационных систем и в ходе их эксплуатации;

в) на этапе создания информационных систем, в ходе их эксплуатации, в том числе при развитии (модернизации);

г) должна носить систематический характер и осуществляться как на этапе создания систем, так и в ходе их эксплуатации, в том числе при развитии (модернизации).

д) на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации;

3. Чем удостоверяется соответствие средств защиты информации, требованиям по защите информации?

а) аттестатом соответствия;

б) лицензией;

в) сертификатом соответствия;

г) аттестатом аккредитации;

4. Сколько классов средств криптографической защиты информации может применяться для нейтрализации атак, организуемых с целью нарушения безопасности защищаемых персональных данных?

а) два класса;

в) три класса;

г) четыре класса;

д) пять классов;

5. Перечислить случаи, которые определяют необходимость проведения дополнительных аттестационных испытаний и внесения изменений в технический паспорт государственной информационной системы при ее развитии (модернизации):

а) изменена конфигурация (параметры настройки) программных, программно-технических средств и средств защиты информации;

б) исключены программные, программно-технические средства и средства защиты информации;

в) включены аналогичные средства или заменены на аналогичные средства;

г) в ходе которого изменена конфигурация (параметры настройки) программных, программно-технических средств и средств защиты информации, исключены программные, программно-технические средства и средства защиты информации, дополнительно включены аналогичные средства или заменены на аналогичные средства;

6. Перечислить случаи, которые определяют необходимость проведения повторных аттестационных испытаний государственной информационной системы при ее развитии (модернизации):

а) изменена конфигурация (параметры настройки) программных, программно-технических средств и средств защиты информации;

б) исключены программные, программно-технические средства и средства защиты информации;

в) изменена конфигурация (параметры настройки) программных, программно-технических средств и средств защиты информации, исключены программные, программно-технические средства и средства защиты информации, дополнительно включены аналогичные средства или заменены на аналогичные средства;

г) повышение класса защищенности (уровня защищенности) и (или) изменение архитектуры системы защиты информации в части изменения видов и типов программных, программно-технических средств и средств защиты информации, изменение структуры системы защиты информации, состава и мест расположения объекта информации и его компонентов

7. Классификация государственной информационной системы по требованиям защиты информации проводится в зависимости от:

а) рисков нарушения информационной безопасности; мер защиты информации, реализованных в информационной системе;

б) значимости обрабатываемой в ней информации и масштаба информационной системы;

в) категорий обрабатываемой в ней информации и масштаба информационной системы;

г) мер защиты информации, реализованных в информационной системе и масштаба информационной системы;

8. **Классификация информационной системы персональных данных по требованиям защиты информации проводится в зависимости от:**

а) рисков нарушения информационной безопасности и мер защиты информации, реализованных в информационной системе;

б) от значимости обрабатываемой в ней информации и масштаба информационной системы;

в) от категорий и масштаба обрабатываемых в ней персональных данных; типа актуальных угроз персональным данным;

г) от мер защиты информации, реализованных в информационной системе и масштаба информационной системы;

9. **Формирование требований к защите информации, содержащейся в государственной информационной системе, предполагает следующие этапы:**

а) принятие решения о необходимости защиты информации; классификацию информационной системы по требованиям защиты информации; определение угроз безопасности информации; определение требований к системе защиты информации;

б) анализ рисков нарушения информационной безопасности; разработку модели угроз безопасности информации; определение требований к системе защиты информации;

в) анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система; определение угроз безопасности информации; определение требований к системе защиты информации;

г) определение информации, подлежащей защите в информационной системе и ее значимости; классификации информационной системы по требованиям защиты информации; определение угроз безопасности информации; определение требований к системе защиты информации;

10. **В качестве исходных данных для определения угроз безопасности информации, содержащейся в государственной информационной системе, используется:**

а) банк данных угроз безопасности информации (bdu.fstec.ru), а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации;

б) модель угроз безопасности информации, а также результаты анализа уязвимостей информационной системы;

в) модель угроз безопасности информации, результаты анализа уязвимостей информационной системы, а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации;

г) банк данных угроз безопасности информации (bdu.fstec.ru), а также результаты анализа уязвимостей информационной системы;

Задания открытого типа

11. Сколько установлено классов защищенности государственных информационных систем?
12. Сколько уровней защищенности установлено для информационных систем персональных данных?

Задания с развёрнутым ответом

1. **Как определяется уровень защищенности информационных систем персональных данных?**

Критерии оценивания	Шкала оценок
Обучающийся приводит основные параметры оценки информационных систем персональных данных. Подробно описаны критерии оценки необходимых параметров.	Отлично (90-100 баллов)
Обучающийся приводит основные параметры оценки информационных систем персональных данных. Подробно описан каждый из параметров оценки. Допускаются незначительные неточности.	Хорошо (70-80 баллов)

Обучающийся допускает ошибку в параметрах оценки информационных систем персональных данных. Частично описан каждый параметров. Ответ не содержит грубых ошибок.	Удовлетворительно (50-70 баллов)
Не представлены параметры оценки информационных систем персональных данных. Присутствуют грубые ошибки или неточности.	Неудовлетворительно

Компетенция ОПК-1.4

Задания закрытого типа

1. **Модель угроз безопасности информации и (или) техническое задание на создание государственной информационной системы должны быть согласованы (в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации) с:**

а) ФСТЭК России; ФСБ России; Минцифры России; Роскомнадзор;
б) ФСТЭК России; Роскомнадзор; Минцифры России;
в) ФСТЭК России; ФСБ России; Роскомнадзор;
г) ФСТЭК России; ФСБ России;
д) ФСТЭК России; Минцифры России;

2. **При определении требований к системе защиты информации информационной системы учитываются положения политик обеспечения информационной безопасности:**

а) обладателя информации (заказчика), а также политик обеспечения информационной безопасности оператора;

б) обладателя информации (заказчика), а также политик обеспечения информационной безопасности оператора и уполномоченного лица в части, не противоречащей политикам обладателя информации (заказчика);

в) обладателя информации (заказчика), а также политик обеспечения информационной безопасности оператора и уполномоченного лица;

г) обладателя информации (заказчика), оператора, уполномоченного лица, а также политик обеспечения информационной безопасности привлекаемой организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации;

3. **Требования к системе защиты информации государственной информационной системы определяются в зависимости от:**

а) банка данных угроз безопасности информации (bdu.fstec.ru), а также результатов анализа уязвимостей информационной системы;

б) модели угроз безопасности информации, а также результатов анализа уязвимостей информационной системы;

в) класса защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации;

г) от значимости обрабатываемой в ней информации и масштаба информационной системы;

4. **Разработка системы защиты информации информационной системы организуется:**

а) обладателем информации (заказчиком);
б) оператором информационной системы;
в) уполномоченным лицом;
г) привлекаемой организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации;

5. **В каких информационных системах в целях защиты информации предусмотрено обязательное применение средств криптографической защиты информации?**

а) в государственных информационных системах;
б) в информационных системах персональных данных;
в) в информационных системах общего пользования;
г) в информационных системах персональных данных, если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации и осуществляется

передача таких персональных данных по не защищенным каналам связи и/или осуществляется хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов;

6. В каких информационных системах в целях защиты информации предусмотрено обязательное применение квалифицированной электронной подписи?

а) в государственных информационных системах;

б) в информационных системах персональных данных;

в) в информационных системах общего пользования;

г) во всех перечисленных выше информационных системах;

7. Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы и включает следующие стадии:

а) классификацию информационной системы по требованиям защиты информации; определение угроз безопасности информации; определение требований к системе защиты информации;

б) разработку модели угроз; определение требований к системе защиты информации; определение видов и типов средств защиты информации, обеспечивающих реализацию технических мер защиты информации; разработку эксплуатационной документации;

в) разработку модели угроз; определение требований к системе защиты информации; определение необходимых средств защиты информации; разработку организационно-распорядительной и эксплуатационной документации;

г) проектирование системы защиты информации; разработку эксплуатационной документации; макетирование и тестирование системы защиты информации (при необходимости);

8. Эксплуатационная документация на систему защиты информации информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 и должна в том числе содержать:

а) руководство пользователя; руководство оператора; руководство администратора; описание правил эксплуатации системы защиты информации информационной системы;

б) описание структуры системы защиты информации информационной системы; описание состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств; описание правил эксплуатации системы защиты;

в) руководство администратора информационной системы; описание правил развертывания и эксплуатации системы защиты информации информационной системы;

г) порядок развертывания и настройки средств защиты информации; описание правил эксплуатации системы защиты; правила и требования по реализации установленных мер защиты информации;

9. Внедрение системы защиты информации информационной системы организуется:

а) обладателем информации (заказчиком);

б) оператором информационной системы;

в) уполномоченным лицом;

г) привлекаемой организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации;

10.Внедрение системы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

а) настройку средств защиты; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; приемочные испытания; аттестацию информационной системы;

б) развертывание средств защиты; разработку организационных мер защиты информации; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; анализ уязвимостей и принятие мер защиты информации по их устранению; приемочные испытания;

в) установку и настройку средств защиты; разработку организационно-распорядительных документов по защите информации; внедрение организационных мер защиты информации; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; анализ уязвимостей и принятие мер защиты информации по их устранению; приемочные испытания;

г) установку и настройку средств защиты; разработку организационно-распорядительных документов по защите информации; внедрение организационных мер защиты информации; обучение пользователей; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; приемочные испытания;

Задания открытого типа

1. Сколько установлено классов для средств криптозащиты информации?
2. Сколько установлено классов для информационных систем общего пользования?

Задания с развёрнутым ответом

1. **Какие основные мероприятия защиты информации проводятся в государственной информационной системе (от создания до вывода из эксплуатации).**

Критерии оценивания	Шкала оценок
Обучающийся приводит основные мероприятия защиты информации в государственных информационных системах. Подробно описан каждый из этапов.	Отлично (90-100 баллов)
Обучающийся приводит основные мероприятия защиты информации в государственных информационных системах. Подробно описан каждый из этапов. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Обучающийся допускает ошибку в последовательности основных мероприятий защиты информации в государственных информационных системах. Частично описан каждый из этапов. Ответ не содержит грубых ошибок.	Удовлетворительно (50-70 баллов)
Не представлены этапы жизненного цикла государственных информационных систем. Присутствуют грубые ошибки или неточности.	Неудовлетворительно

Компетенция ОПК-1.4

Задания закрытого типа

1. **В государственной информационной системе как минимум подлежат регистрации следующие события:**

а) вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;

б) подключение машинных носителей информации и вывод информации на носители информации;

в) запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

г) попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

д) попытки удаленного доступа;

е) все вышеперечисленные события;

2. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

а) управления (администрирования) системой защиты информации; выявления инцидентов безопасности информации и реагирования на них; управления конфигурацией информационной системы и системы защиты информации; контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе; защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации;

б) управления (администрирования) системой защиты информации; управления конфигурацией информационной системы и системы защиты информации; контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе; защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации;

в) управления (администрирования) системой защиты информации; управления конфигурацией информационной системы и системы защиты информации; контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

г) выявления инцидентов безопасности информации и реагирования на них; управления конфигурацией информационной системы и системы защиты информации; контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

3. При внедрении организационных мер защиты информации осуществляются:

а) реализация правил разграничения доступа, установка и настройка средств защиты; разработка организационно-распорядительных документов по защите информации; обучение пользователей; предварительные испытания системы защиты информации; опытная эксплуатация системы защиты информации;

б) реализация правил разграничения доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения; проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов; отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации;

в) развертывание средств защиты; разработка организационных мер защиты информации; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; анализ уязвимостей и принятие мер защиты информации по их устранению; приемочные испытания;

г) обучение пользователей; предварительные испытания системы защиты информации; опытная эксплуатация системы защиты информации; анализ уязвимостей и принятие мер защиты информации по их устранению; реализация правил разграничения доступа, и введение ограничений на действия пользователей; проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов; отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации;

4. Анализ уязвимостей информационной системы включает:

а) тестирование на проникновение; установка обновлений программного обеспечения; подтверждение, что в информационной системе отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России;

б) сканирование сертифицированными средствами защиты информации; установка обновлений программного обеспечения; подтверждение, что в информационной системе отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России;

в) анализ уязвимостей программного обеспечения информационной системы; установка обновлений программного обеспечения; подтверждение, что в информационной системе отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России;

г) анализ уязвимостей средств защиты информации, технических средств и программного обеспечения информационной системы;

5. В случае выявления уязвимостей информационной системы, приводящих к возникновению дополнительных угроз безопасности информации, проводится:

а) уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей;

б) принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей;

в) установка обновлений программного обеспечения; принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей;

г) установка обновлений программного обеспечения; подтверждение, что в информационной системе отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России;

6. Аттестация информационной системы организуется:

а) обладателем информации (заказчиком);

б) оператором информационной системы;

в) обладателем информации (заказчиком) или оператором;

г) привлекаемой организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации;

7. Информационные системы, функционирующие на базе общей инфраструктуры (средств вычислительной техники, серверов телекоммуникационного оборудования) в качестве прикладных сервисов, подлежат аттестации:

а) в составе указанной инфраструктуры;

б) по отдельности; общая инфраструктура должна иметь свой аттестат соответствия требованиям безопасности информации;

в) в составе указанной инфраструктуры; допускается проведение аттестации таких информационных систем отдельно;

г) каждая такая информационная система должна иметь свой аттестат соответствия требованиям безопасности информации; аттестация общей инфраструктуры необязательна;

8. На какой срок выдается аттестат соответствия требованиям по защите информации на государственную информационную систему?

а) на 3 года;

б) на 5 лет;

в) на время эксплуатации государственной информационной системы;

г) бессрочно;

9. Правовой акт органа исполнительной власти о вводе системы в эксплуатацию включает мероприятия:

а) по разработке и утверждению организационно-распорядительных документов; по аттестации системы по требованиям защиты информации; по подготовке должностных лиц к эксплуатации системы;

б) по разработке и утверждению организационно-распорядительных документов; по аттестации системы по требованиям защиты информации; по подготовке к эксплуатации системы; по подготовке должностных лиц к эксплуатации системы;

в) по аттестации системы по требованиям защиты информации; по подготовке к эксплуатации системы; по подготовке должностных лиц к эксплуатации системы;

г) по подготовке к эксплуатации системы; по подготовке должностных лиц к эксплуатации системы;

10. Обязано ли лицо, осуществляющее обработку персональных данных по поручению оператора, получать согласие субъекта персональных данных на обработку его персональных данных?

а) Соответствующее лицо не обязано получать согласие субъекта персональных данных на обработку его персональных данных;

б) соответствующее лицо обязано получать согласие субъекта персональных данных на обработку его персональных данных;

в) соответствующее лицо может получать согласие субъекта персональных данных на обработку его персональных данных в зависимости от желаний и возможностей данного лица;

г) соответствующее лицо обязано получать согласие субъекта персональных данных на обработку его персональных данных в случае, если обрабатываются специальные категории персональных данных субъекта;

д) нет правильного ответа;

11.Каков определяющий признак государственной информационной системы?

а) требования к защите информации в информационной системе определяют ФСБ России и ФСТЭК России;

б) информационная система создана за счет государственного бюджета;

в) информационная система эксплуатируется в государственной организации;

г) информационная система создана на основании федерального закона или правового акта государственного органа.

Задания открытого типа

1. Информация, доступ к которой ограничен федеральными законами называется информацией
2. Как часто необходимо проводить контроль защиты информации в государственных информационных системах 2 и 3 класса защищенности?

Задания с развёрнутым ответом

1. **Как определяется необходимость применения средств криптозащиты информации и их требуемый класс для заданной информационной системы?**

Критерии оценивания	Шкала оценок
Обучающийся приводит основные документы, регламентирующие применение средств криптозащиты информации. Подробно описаны критерии определяющие необходимость применения средств криптозащиты информации.	Отлично (90-100 баллов)
Обучающийся приводит основные документы, регламентирующие применение средств криптозащиты информации. Подробно описаны критерии определяющие необходимость применения средств криптозащиты информации. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Обучающийся допускает ошибку в критериях, определяющих необходимость применения средств криптозащиты информации. Не твердо знает нормативные документы, регламентирующие применение средств криптозащиты информации. Ответ не содержит грубых ошибок.	Удовлетворительно (50-70 баллов)
Обучающийся не знает нормативные документы, регламентирующие применение средств криптозащиты информации. Присутствуют грубые ошибки или неточности.	Неудовлетворительно

Компетенция ОПК-1.4

Задания закрытого типа

1. **В случае определения в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей**

а) применяется во всех случаях;
б) может применяться как дополнительная мера;
в) не применяется вообще;

2. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором

а) ежегодно;
б) не реже одного раза в 3 года;
в) при возникновении инцидента;

3. Какой реквизит наносится на документах, содержащих сведения, составляющие коммерческую тайну, в случае предоставления обладателем по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления?

а) «Для служебного пользования»;
б) никакой реквизит не наносится;
в) «Коммерческая тайна»;

4. Технические средства информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями,

а) должны размещаться на территории Российской Федерации;
б) могут размещаться на территории дружественных государств;
в) могут размещаться произвольно;

5. Деятельность по защите конфиденциальной информации лицензируется в соответствии с положениями:

а) Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

б) Федерального закона от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;

в) Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;

6. Для обеспечения какого уровня защищенности персональных данных необходимо в том числе создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности?

а) любого уровня защищенности;

б) третьего и выше;

в) второго и выше;

г) первого;

7. К чему может привести установка на рабочий компьютер несанкционированного ПО, скачанного из сети Интернет?

а) к необоснованному расходу компьютерных ресурсов;

б) к возникновению конфликтов при работе штатных программ;

в) к внедрению «троянских» и шпионских программ;

г) к неумышленному заражению компьютеров вирусами;

д) все из перечисленного.

8. Подлежат ли лицензированию услуги по мониторингу информационной безопасности средств и систем информатизации?

а) подлежат по отдельному решению руководства лицензиата;

б) не подлежат;

в) подлежат обязательно;

9. Особенности технического регулирования в части разработки и установления обязательных требований ФСБ России и ФСТЭК России определяются

а) Законодательством Российской Федерации;

б) Президентом Российской Федерации, Правительством Российской Федерации в соответствии с их полномочиями;

в) соответствующими федеральными органами исполнительной власти;

10. Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств устанавливает лицензионные требования к соответствующей деятельности со средствами, предназначенными

а) для защиты информации, содержащей персональные данные;

б) для защиты информации конфиденциального характера;

в) для защиты информации, обладатель которой осуществляет техническое обслуживание шифровальных (криптографических) средств для обеспечения собственных нужд;

11. К какой ответственности может быть привлечен работник за нарушение правил информационной безопасности, принятых в организации?

а) не может быть привлечен к ответственности;

б) гражданско-правовой и/или административной и/или уголовной;

в) гражданско-правовой и/или административной;

г) административной;

д) гражданско-правовой**;**

Задания открытого типа

1. На какой срок выдается Аттестат соответствия требованиям по защите информации на государственную информационную систему?
2. В каких информационных системах в целях защиты информации предусмотрено обязательное применение квалифицированной электронной подписи?

Задания с развёрнутым ответом

1. **Какие основные мероприятия проводятся в государственной информационной системе для формирование требований по защите информации.**

Критерии оценивания	Шкала оценок
Обучающийся приводит основные мероприятия защиты информации в государственных информационных системах. Подробно описан каждый из этапов.	Отлично (90-100 баллов)
Обучающийся приводит основные мероприятия защиты информации в государственных информационных системах. Подробно описан каждый из этапов. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Обучающийся допускает ошибку в последовательности основных мероприятий защиты информации в государственных информационных системах. Частично описан каждый из этапов. Ответ не содержит грубых ошибок.	Удовлетворительно (50-70 баллов)
Не представлены этапы формирования требований защиты информации в государственных информационных системах. Присутствуют грубые ошибки или неточности.	Неудовлетворительно

20.2. Промежуточная аттестация

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практические задания, позволяющие оценить степень сформированности умений и навыков.

При оценивании могут использоваться количественные или качественные шкалы оценок.

Для оценивания результатов обучения при проведении промежуточной аттестации используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание нормативных документов, основных определений, понятий и используемой терминологии;

2) умение проводить обоснование требований нормативных документов и практических мер их реализующих с использованием с использованием сертифицированных средств защиты информации;

3) умение связывать требования нормативных документов 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;

5) владение навыками программирования и администрирования компьютерных систем и средств защиты в рамках выполняемых лабораторных заданий;

6) владение навыками проведения компьютерного эксперимента, тестирования компьютерных моделей алгоритмов обработки информации.

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 государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на зачете

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

20.3. Примерный перечень практических заданий, тем рефератов, тем презентаций, докладов, вопросов к экзамену

№	Содержание
1	Система управления информационной безопасностью. Модель разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы управления информационной безопасности.
2	Государственная информационная система, классы защищённости информационной системы.
3	Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.
4	Понятие категории персональных данных. И её нормативно-правовое регулирование.
5	Основные этапы организации обработки и обеспечения безопасности персональных данных.
6	Определение уровня защищенности персональных данных и классификация информационных систем персональных данных
7	Формирование политики в отношении обработки персональных данных.
8	Формирование облика и внедрение системы защиты персональных данных.
9	Обеспечение защиты персональных данных в ходе эксплуатации и при выводе из эксплуатации информационной системы персональных данных
10	Требования безопасности информации при использовании криптографических средств защиты.
11	Модель угроз безопасности информации.
12	Модель нарушителя безопасности информации.
13	Банк данных угроз безопасности информации.
14	Возможные способы реализации угроз безопасности информации.
15	Виды ущерба безопасности информации и методы его оценки.

16	Контроль выполнения требований по обеспечению безопасности информации в государственных информационных системах.
17	Оценка эффективности принимаемых мер защиты персональных данных в информационных системах персональных данных.

20.4. Пример задания для выполнения лабораторной работы

Лабораторная работа №15

Контроль выполнения требований по обеспечению безопасности информации в государственных информационных системах. «Управление информационной безопасностью в операционной системе Windows 10 с использованием локальных политик безопасности»

Цель работы: практическое изучение методов управления информационной безопасностью в современных информационных системах.

Вариант №1. Настройка правил парольной защиты входа в информационную систему в соответствии с требованиями нормативных документов и контроль их выполнения.

20.5. Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2027

Направление подготовки / специальность 10.03.01 Информационная безопасность

Дисциплина Б1.О.46 Основы управления информационной безопасностью

Форма обучения Очное

Вид контроля экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Государственная информационная система, классы защищённости государственной информационной системы.
2. Базовые организационные и технические меры защиты информации, реализуемые в государственной информационной системе в рамках ее системы защиты.

Преподаватель _____ С.А. Вялых