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

«Утверждаю»
Заведующий кафедрой ТО и ЗИ

«22» июня 2021 г.  А.А. Сирота

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.46 Основы управления информационной безопасностью

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 № 5 от 10.03.2021 г.

8. Учебный год: 2024-2025 **Семестр(ы):** 7

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются:

изучение основ и овладение практическими навыками планирования, развертывания и поддержания комплекса регламентов и процедур, направленных на минимизацию рисков нарушения информационной безопасности при разработке, сопровождении и проектировании 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 системе управления информационной безопасностью в организации;
- овладение практическими навыками разработки системы документов, регламентирующих требования и меры, обеспечивающие информационную безопасность в информационных системах различного назначения, разработки модели угроз, выявления и анализа рисков информационной безопасности;
- формирование представления о процедурах планирования и практической реализации процессов, направленных на минимизацию рисков информационной безопасности и контроля выполнения мер по защите информационных систем, различного назначения.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к блоку Б1.О обязательных дисциплин.

Для успешного освоения дисциплины необходимы входные знания в области основ информационной безопасности, программно-аппаратных средств защиты информации, криптографических методов защиты информации, организационно и правовом обеспечении информационной безопасности.

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 -5	Способность применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1	знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной	Знать: основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характери-
		ОПК-5.2	знает основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации;	
		ОПК-5.3	знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую ха-	

			рактеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации;	стику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности.
		ОПК-5.4	знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности;	
		ОПК-5.5	умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать	Уметь: обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации. Владеть: практическими навыками формирования требований безопасности информации для различных классов и уровней защищенности информационных систем.
		ОПК-5.6	умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;	
		ОПК-5.7	умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по	
		ОПК-5.8	умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;	
ОПК-6	Способность при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому	ОПК-6.1	знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической	Знать: систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа;
		ОПК-6.2	знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях;	
		ОПК-6.3	знает систему организационных мер, направленных на защиту информации ограниченного доступа	
		ОПК-6.4	умеет разрабатывать проекты инструкций, регламентов, положений и приказов, ре-	Уметь: разрабатывать проекты инструкций, регламентов, положе-

	и экспортному контролю		гламентирующих защиту информации ограниченного доступа в организации	ний и приказов, регламентирующих защиту информации ограниченного доступа в организации;
		ОПК-6.5	умеет определить политику контроля доступа работников к информации ограниченного доступа	определить политику контроля доступа работников к информации ограниченного доступа;
		ОПК-6.6	умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации	формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации. Владеть: практическими навыками формирования комплексного подхода к обеспечению информационной безопасности объекта защиты.
ОПК-10	Способность в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.3	знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности	Знать: правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности;
		ОПК-10.4	знает принципы формирования политики информационной безопасности организации	принципы формирования политики информационной безопасности организации. Уметь: проводить разработку политики информационной безопасности для различных вариантов построения защищенных информационных систем; Владеть: навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требований.
ОПК-12	Способность 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;	Знать: принципы формирования политики информационной безопасности в информационных системах;
		ОПК-12.2	знает принципы организации информационных систем в соответствии с требованиями по защите информации;	принципы организации информационных систем в соответствии с требованиями по защите информации.
		ОПК-12.5	умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;	Уметь: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
		ОПК-12.6	умеет анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;	анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; Владеть: навыками контроля комплекса мер безопасности информации на защищаемом объекте с учетом требований руководящих и нормативных документов.

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

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра 7	№ семестра	…
Аудиторные занятия		68	68		
в том числе:	лекции	34	34		
	лабораторные	34	34		
	контроль	36	36		
Самостоятельная работа		40	40		
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(экзамен – __час.)*					
Итого:		144	144		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Система управления информационной безопасностью	1. Введение. Система управления информационной безопасностью. 2. Модель разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы управления информационной безопасности.	
1.2	Государственная информационная система, классы защищённости информационной системы	3. Государственная информационная система, классы защищённости информационной системы. 4. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.	
1.3	Обеспечение безопасности персональных данных при их обработке в информационных системах	5. Понятие категории персональных данных. И её нормативно-правовое регулирование. 6. Основные этапы организации обработки и обеспечения безопасности персональных данных. 7. Определение уровня защищенности персональных данных и классификация информационных систем персональных данных. 8. Формирование политики в отношении обработки персональных данных. 9. Формирование облика и внедрение системы защиты персональных данных. 10. Оценка эффективности принимаемых мер защиты персональных данных в информационных системах персональных данных. 11. Обеспечение защиты персональных данных в ходе эксплуатации и при выводе из эксплуатации информационной системы персональных данных.	
1.4	Требования безопасности информации при использовании криптографических средств защиты	12. Криптографические средства защиты информации. 13. 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».	
1.5	Модели угроз безопас-	14. Методика определения угроз безопасности	

	ности информации.	информации в информационных системах. 15. Модель нарушителя. 16. Модель угроз безопасности информации.	
1.6	Организация обработки персональных данных и обеспечение безопасности информации.	17. Организация обработки персональных данных в органах государственной власти и местного самоуправления.	
1.7	Контроль выполнения требований по обеспечению безопасности информации	18. 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	Государственная информационная система, классы защищённости информационной системы	1. Определение класса защищенности государственной информационной системы. 2. Формирование требований к мерам защиты информации для различных классов защищенности в государственных информационных системах.	
3.2	Обеспечение безопасности персональных данных при их обработке в информационных системах	3. Определение уровня защищенности информационной системы, обрабатывающей персональные данные. 4. Формирование требований к мерам защиты информации для различных уровней защищенности в информационных системах обрабатывающих персональные данные.	
3.3	Требования безопасности информации при использовании криптографических средств защиты	5. Формирование 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.	
3.4	Модели угроз безопасности информации	6. Определение источников угроз безопасности информации. 7. Оценка возможностей нарушителей по реализации угроз безопасности информации (разработка модели нарушителя). 8. Оценка возможных способов реализации угроз безопасности информации. 9. Оценка проектной защищенности информационной системы. 10. Оценка возможного ущерба от реализации угрозы безопасности. 11. Определение актуальных угроз безопасности информации в информационной системе. 12. Определение угроз безопасности информации при использовании средств криптографической защиты. 13. Разработка модели угроз безопасности информации в информационной системе.	
3.5	Организация обработки персональных данных и обеспечение безопасности информации.	14. Разработка комплекса организационных и технических мер обеспечения защиты информации в информационной системе с использованием сертифицированных средств защиты информации.	
3.6	Контроль выполнения требований по обеспечению без-опасности информации	15. Контроль выполнения требований по обеспечению безопасности информации в государственных информационных системах. 16. Контроль выполнения требований по обеспечению безопасности информации в информационных системах обрабатывающих персональные данные. 17. Контроль выполнения требований по обеспечению безопасности информации в информационных системах использующих средства криптозащиты.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Сам. работа	Всего
1	Система управления информационной безопасностью.	4	-	2	6
2	Государственная информационная система, классы защищённости информационной системы	4	6	4	14
3	Обеспечение безопасности персональных данных при их обработке в информационных системах.	10	6	6	24
4	Требования безопасности информации при использовании криптографических средств защиты.	4	6	8	16
5	Модели угроз безопасности информации	6	10	8	24
6	Организация обработки персональных данных и обеспечение безопасности информации	4	4	6	14
7	Контроль выполнения требований по обеспечению безопасности информации.	2	4	6	12
	Итого:	34	34	40	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	ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст)
7	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.
8	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.
9	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).
10	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.
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/

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

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)

№ п/п	Источник
1	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.

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) Лекционная аудитория, рабочее место преподавателя: ПК-Intel-i7, проектор, специализированная мебель: доска меловая 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., 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 1-5. Система управления информационной безопасностью. Классы и уровни защищенности информационных систем. Криптографические средства защиты. Методика определения угроз безопасности информации в информационных систе-	ОПК-5 Способность применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере	знать: базовые понятия, требования нормативных документов, методы анализа информационной безопасности при проектировании и эксплуатации информационных систем; уметь: анализировать и разрабатывать модели угроз для различных объектов защиты; владеть: практическими	Устный опрос. Лабораторные работы 1-13. Контрольная работа по соответствующим разделам или тест

	мах.	профессиональной деятельности	навыками формирования требований безопасности информации для различных классов и уровней защищенности информационных систем	
2.	Разделы 2-6 Организационные и технические меры обеспечения защиты информации в информационной системе с использованием сертифицированных средств защиты информации	ОПК-6 Способность при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	знать: типовые меры и требования информационной безопасности для различных вариантов построения защищенных информационных систем; уметь: организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности для различных вариантов построения защищенных информационных систем; владеть: практическими навыками формирования требований безопасности информации для различных классов и уровней защищенности информационных систем	Устный опрос. Лабораторные работы 1-13. Контрольная работа по соответствующим разделам или тест
3.	Разделы 2-4, 7 Требования по обеспечению безопасности информации в государственных информационных системах и информационных системах персональных данных	ОПК-10 Способность в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	знать: принципы формирования политики информационной безопасности организации; уметь: проводить разработку политики информационной безопасности для различных вариантов построения защищенных информационных систем; владеть: навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требований; навыками комплексного подхода к обеспечению информационной безопасности объекта защиты.	Устный опрос. Лабораторные работы 13-16. Контрольная работа по соответствующим разделам или тест
4.	Разделы 1-5. Система управления информационной безопасностью. Классы и уровни защищенности информационных систем. Криптографические средства защиты. Методика определения угроз безопасности ин-формации в информационных системах	ОПК-12 Способность проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих	знать: требования нормативных документов, методы анализа информационной безопасности при проектировании информационных систем; уметь: анализировать и разрабатывать модели угроз для различных объектов защиты; владеть: практическими навыками формирования требований безопасности информации для раз-	Устный опрос. Лабораторные работы 1-17. Контрольная работа по соответствующим разделам или тест

		проектных решений	личных классов и уровней защищенности информационных систем.	
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

20.2. Промежуточная аттестация

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 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 ис-

пользуемой 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 зачету с оценкой

№	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
__.__.2021

Направление подготовки / специальность 10.03.01 Информационная безопасность

Дисциплина Б1.О.46 Основы управления информационной безопасностью

Форма обучения Очное

Вид контроля зачет с оценкой

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