Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Сирота Александр Анатольевич

Кафедра технологий обработки и защиты информации

01.07.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.40 Организационное и правовое обеспечение информационной безопасности

1. Код и наименование направления подготовки/специальности:

10.03.01 Информационная безопасность

2. Профиль подготовки/специализация:

Безопасность компьютерных систем

3. Квалификация (степень) выпускника:

Бакалавриат

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Степанцов Вячеслав Алексеевич, кандидат технических наук, доцент

7. Рекомендована:

протокол Ученого совета ФКН №6 от 07.06.2021

8. Учебный год:

2022-2023

9.Цели и задачи учебной дисциплины:

формирование профессиональных навыков, связанных со структурой правового обеспечения информационной безопасности и соответствующего законодательства в области информации, информационных технологий и защиты информации.

Основные задачи дисциплины:

формирование у студентов профессиональных навыков, связанных

− со структурой правового обеспечения информационной безопасности и соответствующего законодательства в области информации;

− информационных технологий и защиты информации;

− обучение применению основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации.

10. Место учебной дисциплины в структуре ООП:

Блок Б1.О обязательные дисциплины.

Входные знания в области основ информационной безопасности. Дисциплина является предшествующей для дисциплины «Методы и средства криптографической защиты информации».

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

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-5 Способен 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 власти в Российской Федерации;	знает основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.2 знает основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации;	знает основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	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 характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации;	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 характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.4 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности;	знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.5 умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав;	умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	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;	умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.7 умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации;	умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.8 умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;	умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-6 Способен 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;	ОПК-6.1 знает 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;	знает 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

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-6 Способен 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;	ОПК-6.2 знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях;	знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-6 Способен 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;	ОПК-6.3 знает систему организационных мер, направленных на защиту информации ограниченного доступа	знает систему организационных мер, направленных на защиту информации ограниченного доступа

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-6 Способен 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;	ОПК-6.4 умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-6 Способен 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;	ОПК-6.5 умеет определить политику контроля доступа работников к информации ограниченного доступа	умеет определить политику контроля доступа работников к информации ограниченного доступа

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-6 Способен 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;	ОПК-6.6 умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации	умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Зачет с оценкой,Контрольная работа

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 4	Всего
Аудиторные занятия	50	50
Лекционные занятия	16	16
Практические занятия	34	34
Лабораторные занятия		0
Самостоятельная работа	58	58
Курсовая работа		0
Промежуточная аттестация	0	0
Часы на контроль		0
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
	Лекции		
1	Назначение и структура правого обеспечения информационной безопасности	1. Основы правового регулирования отношений в информационной сфере.	Создан электронный онлайн - курс, размещены материалы к лекциям и практическим занятиям
2	Федеральные нормативные акты по обеспечению защиты информации и персональных данных	2. Информационная сфера как сфера обращения информации и правового регулирования. Информационное законодательство как основной источник информационного права. 3. Юридические особенности и свойства информации.	Создан электронный онлайн - курс, размещены материалы к лекциям и практическим занятиям
3	Правовые основы защиты тайны и персональных данных	4. Структура и направленность правовых мер обеспечения информационной безопасности. 5. Особенности ведомственного и корпоративного нормативного регулирования обеспечения информационной безопасности. 6. Правовые основы защиты государственной, коммерческой, служебной, профессиональной и личной тайны, персональных данных.	Создан электронный онлайн - курс, размещены материалы к лекциям и практическим занятиям
4	Организационное обеспечение информационной безопасности	7. Политика безопасности. Требования действующих международных стандартов по вопросам менеджмента информационной безопасности. Принципы организационного обеспечения информационной безопасности.	Создан электронный онлайн - курс, размещены материалы к лекциям и практическим занятиям

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
5	Планирование и проведение мероприятий по защите информации в организации	8. Порядок деятельности по осуществлению требований организационно-распорядительной документации, периоды проверок, составы комиссий, привлечение аттестованных организаций.	Создан электронный онлайн - курс, размещены материалы к лекциям и практическим занятиям
	Практические занятия		
1	Назначение и структура правого обеспечения информационной безопасности	1. Информационные отношения как объект правового регулирования. Виды нормативно-правовых актов, их иерархия.	Создан электронный онлайн - курс, размещены материалы к лекциям и практическим занятиям
2	Федеральные нормативные акты по обеспечению защиты информации и персональных данных	2. Государственное регулирование деятельности в области защиты информации. 3. Законодательство РФ в области информационной безопасности и защиты государственной тайны. 4. Законодательство РФ в области информационной безопасности и защиты тайны в различных сферах деятельности. 5. Правовые основы защиты информации с использованием технических средств. 6. Ответственность за правонарушения в области информационной безопасности и ее виды.	Создан электронный онлайн - курс, размещены материалы к лекциям и практическим занятиям
3	Правовые основы защиты тайны и персональных данных	7. Правовой режим защиты государственной тайны. 8. Порядок обращение с документами, содержащими сведения, составляющие государственную тайну. 9. Правовой режим защиты информации конфиденциального характера. 10. Институт правовой защиты персональных данных.	Создан электронный онлайн - курс, размещены материалы к лекциям и практическим занятиям

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
4	Организационное обеспечение информационной безопасности	11. Понятие и сущность организационной защиты информации. 12. Организация режима секретности. 13. Организация работ по обеспечению безопасности персональных данных в информационных системах персональных данных.	Создан электронный онлайн - курс, размещены материалы к лекциям и практическим занятиям
5	Планирование и проведение мероприятий по защите информации в организации	14. Разработка политики безопасности предприятия 15. Организация режимных мероприятий. 16. Организация работ по выстраиванию режима защиты коммерческой тайны. 17. Организация работы службы безопасности предприятия.	Создан электронный онлайн - курс, размещены материалы к лекциям и практическим занятиям

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Назначение и структура правого обеспечения информационной безопасности	2	2		8	12
2	Федеральные нормативные акты по обеспечению защиты информации и персональных данных	4	10		16	30
3	Правовые основы защиты тайны и персональных данных	6	8		14	28

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
4	Организационное обеспечение информационной безопасности	2	6		10	18
5	Планирование и проведение мероприятий по защите информации в организации	2	8		10	20
		16	34	0	58	108

14. Методические указания для обучающихся по освоению дисциплины

1) При освоении дисциплины рекомендуется использовать следующие средства:

- изучение рекомендуемой основной и дополнительной литературы методических указаний и пособий;
- работа с текстом конспекта лекций;
- систематическая подготовка к практическим занятиям;
- выполнение контрольных заданий для закрепления теоретического материала;
- работа с электронными версиями 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 лабораторных работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.
3) При проведении практических занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.
4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций онлайн и проведения лабораторно- практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.
5) При использовании дистанционных образовательных технологий и электронного обучения обучающиеся должны выполнять все указания преподавателей, вовремя подключаться к онлайн - занятиям, ответственно подходить к заданиям для самостоятельной работы.

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

№ п/п	Источник
1	Ажмухамедов, И. М. Основы организационно-правового обеспечения информационной безопасности : учебное пособие / И. М. Ажмухамедов, О. М. Князева. — Санкт-Петербург : Интермедия, 2017. — 264 с. — ISBN 978-5-4383-0160-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103196 (дата обращения: 30.06.2021). — Режим доступа: для авториз. пользователей.
2	Мельников, Владимир Павлович. Информационная безопасность : [учебник для студ. вузов, обучающихся по направлениям подготовки "Конструкторско-технологическое обеспечение машиностроительных производств", "Автоматизация технологических процессов и производств"] / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева ; под ред. В.П. Мельникова .— 2-е изд., перераб. и доп. — Москва : КноРус, 2018 .— 371 с. : ил., цв. ил., табл. — (Бакалавриат) .— Библиогр.: с. 369-371.

б) дополнительная литература:

№ п/п	Источник
1	Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры: [для студентов высших учебных заведений, обучающихся по юридическим направлениям и специальностям] / под ред. Т.А. Поляковой, А.А. Стрельцова .— Москва : Юрайт, 2018 .— 324, [1] с. : ил. — (Бакалавр и магистр. Академический курс) .— Библиогр.: с. 324-[325].
2	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— Москва : ACADEMIA, 2006 .— 330 с. : ил. — (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с. 327-328.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
2	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
3	«Университетская библиотека online» - Контракт № 3010-06/05-20 от 28.12.2020 «Консультант студента» - Контракт № 3010-06/06-20 от 28.12.2020 ЭБС «Лань» - Контракт №3010-06/04-21 от 10.03.2021 ЭБС «Лань» - Контракт №3010-06/03-21 от 10.03.2021 «РУКОНТ» (ИТС Контекстум) - Договор ДС-208 от 01.02.2021
4	Организационные основы защиты информации на предприятии (http://content/osnovi-zasiti-informacii/osnovi_zasiti_informacii_part_1.html).

№ п/п	Источник
5	Правовое обеспечение системы защиты информации на предприятии (http://old.ci.ru/inform11_97/aiti1.htm)
6	Участие в планировании и организации работ по обеспечению защиты объекта (https://studref.com/651196/prochie/uchastie_v_planirovanii_i_organizatsii_rabot_po_obespecheniyu_zaschity_obekta)

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Справочно-информационная система «КонсультантПлюс» [Электронный ресурс]. – URL: http://www.consultant.ru.
2	Методические указания для подготовки и выполнения практических занятий.

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

Для реализации учебного процесса используются:
1. ПО Microsoft в рамках подписки "Imagine/Azure Dev Tools for Teaching", договор №3010-16/96-18 от 29 декабря 2018г.
2. ПО MATLAB Classroom ver. 7.0, 10 конкурентных бессрочных лицензий на каждый, компоненты: Matlab, Simulink, Stateflow, 1 тулбокс, N 21127/VRN3 от 30.09.2011 (за счет проекта ЕК TEMPUS/ERAMIS).
3. ПО Матлаб в рамках подписки "Университетская лицензия на программный комплекс для ЭВМ - MathWorks, Headcount – 25 ": лицензия до 31.01.2022, сублицензионный контракт 3010-07/01-19 от 09.01.19.
4. При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 381), ПК-Intel-i3, рабочее место преподавателя: проектор, видеокоммутатор, специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.
2) Компьютерный класс (один из №1-4 корп. 1а, ауд. № 382-385), ПК-Intel-i3 16 шт., 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	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Назначение и структура правого обеспечения информационной безопасности	ОПК-5	ОПК-5.1	Устный опрос. Контрольная работа или тест.
2	Федеральные нормативные акты по обеспечению защиты информации и персональных данных	ОПК-5	ОПК-5.2	Устный опрос. Контрольная работа или тест.
3	Федеральные нормативные акты по обеспечению защиты информации и персональных данных	ОПК-5	ОПК-5.3	Устный опрос. Контрольная работа или тест.
4	Правовые основы защиты тайны и персональных данных	ОПК-5	ОПК-5.4	Устный опрос. Контрольная работа или тест.
5	Правовые основы защиты тайны и персональных данных	ОПК-5	ОПК-5.5	Практическое задание
6	Организационное обеспечение информационной безопасности	ОПК-5	ОПК-5.6	Практическое задание
7	Планирование и проведение мероприятий по защите информации в организации	ОПК-5	ОПК-5.7	Практическое задание
8	Правовые основы защиты тайны и персональных данных	ОПК-5	ОПК-5.8	Устный опрос. Контрольная работа или тест.
9	Планирование и проведение мероприятий по защите информации в организации	ОПК-6	ОПК-6.1	Практическое задание
10	Правовые основы защиты тайны и персональных данных	ОПК-6	ОПК-6.2	Устный опрос. Контрольная работа или тест.

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
11	Правовые основы защиты тайны и персональных данных	ОПК-6	ОПК-6.3	Устный опрос. Контрольная работа или тест.
12	Планирование и проведение мероприятий по защите информации в организации	ОПК-6	ОПК-6.4	Практическое задание
13	Планирование и проведение мероприятий по защите информации в организации	ОПК-6	ОПК-6.5	Практическое задание
14	Планирование и проведение мероприятий по защите информации в организации	ОПК-6	ОПК-6.6	Практическое задание

Промежуточная аттестация

Форма контроля - Зачет с оценкой,Контрольная работа

Оценочные средства для промежуточной аттестации

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

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

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

Критерии оценивания компетенций и шкала оценок на экзамене (зачете с оценкой)

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 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплны	Критерии оценивания приведены выше
3	Тест	Теоретические вопросы по темам/разделам дисциплны	Содержит 4 тестовых вопроса, за правильный ответ на каждый из которых дается 1 балл
4	Практическое задание		Оценка «отлично» выставляется студенту, если он исчерпывающе и свободно справляется с практическими заданиями, дает правильное обоснование принятого решения; Оценка «хорошо» выставляется студенту, если он правильно, но недостаточно полно выполняет задания, не допускает существенных неточностей; Оценка «удовлетворительно» выставляется студенту, если он допускает неточности в ответе, испытывает затруднения в выполнении практических заданий, при указании на существенные ошибки может их исправить; Оценка «неудовлетворительно» выставляется студенту, если он допускает существенные ошибки и неправильно выполняет практические задания.

5	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 задания для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Критерии оценивания приведены выше

Комплект вопросов для контрольных работ

Контрольная работа № 1	
1	Понятие информационной безопасности.
2	Принципы построения систем защиты информации.
3	Актуальность проблемы обеспечения безопасности в информационном обществе.
4	Содержание объектов и субъектов безопасности.
5	Источники и классификация угроз информационной безопасности.
6	Нормативные правовые акты в области обеспечения информационной безопасности
7	Основные составляющие информационной инфраструктуры
8	Федеральный закон «Об информации, информатизации и защите информации» от 20.02.95 №24-ФЗ
9	ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»
10	Средства и способы обеспечения информационной безопасности
11	Система национальной безопасности Российской Федерации
Контрольная работа № 2	
1	Содержание интересов личности в информационной сфере.
2	Стратегия развития информационного общества в России.
3	Какую информацию относят к защищаемой?
4	Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
5	Содержание интересов общества в информационной сфере.
6	Классификация мер защиты информации.
7	Основные задачи в области обеспечения информационной безопасности.
8	Доктрина информационной безопасности РФ.
9	Содержание способов и средств обеспечения безопасности информации.
10	Организационные меры защиты информации и информационных систем
11	Содержание интересов государства в информационной сфере.
12	Правовые средства защиты информации и информационных систем.
13	Понятие угрозы. Анализ угроз информационной безопасности.
14	Содержание способов и средств обеспечения информационной безопасности.
15	Организационно-административные средства защиты информации.
16	Виды «нарушителей» информационной безопасности.
17	Основные причины утечки информации.
Контрольная работа № 3	
1	Политика безопасности. Основные типы политики безопасности.
2	Основные методы реализации угроз информационной безопасности.
3	Основные задачи обеспечения информационной безопасности.
4	Основные каналы утечки информации.
5	Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.
6	Нормативные методические документы ФСБ России в области защиты информации.
7	Противодействие иностранным техническим разведкам на территории РФ
8	Нормативные методические документы ФСТЭК России в области защиты информации.
9	Стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны.
10	Структура нормативной базы по вопросам информационной безопасности

11	Государственная система обеспечения информационной безопасности.
12	Стандарты информационной безопасности.

Пример практических заданий

Практическое задание №1

Тема: Разработка политики безопасности предприятия

Цель задания: Разработать политику безопасности для конкретного предприятия

Теоретические сведения

Политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. На практике политика безопасности трактуется несколько шире – как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса. Результатом политики является высокоуровневый документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Данный документ представляет методологическую основу практических мер (процедур) по реализации ОБИ и содержит следующие группы сведений:

1. Основные положения информационной безопасности.
2. Область применения.
3. Цели и задачи обеспечения информационной безопасности.
4. Распределение ролей и ответственности.
5. Общие обязанности.

Основные положения определяют важность ОБИ, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.

Областью применения политики безопасности являются основные активы и подсистемы АС, подлежащие защите. Типовыми активами являются программно-аппаратное и информационное обеспечение АС, персонал, в отдельных случаях – информационная инфраструктура предприятия.

Цели, задачи, критерии ОБИ вытекают из функционального назначения предприятия. Например, для режимных организаций на первое место ставится соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности (оперативной готовности) подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и т. д. Здесь указываются законы и правила организации, которые следует учитывать при проведении работ по ОБИ.

Типовыми целями могут быть следующие:

- обеспечение уровня безопасности, соответствующего нормативным документам предприятия;

- следование экономической целесообразности в выборе защитных мер;

- обеспечение соответствующего уровня безопасности в конкретных функциональных областях АС;

- обеспечение подотчетности всех действий пользователей с информационными ресурсами и анализа регистрационной информации;

- выработка планов восстановления после критических ситуаций и обеспечения непрерывности работы АС и др.

Если предприятие не является изолированным, цели и задачи рассматриваются в более широком контексте: должны быть оговорены вопросы безопасного взаимного влияния локальных и удаленных подсистем.

В рассматриваемом документе могут быть конкретизированы некоторые стратегические принципы безопасности (вытекающие из целей и задач ОБИ). Таковыми являются стратегии действий в случае нарушения политики безопасности предприятия и сторонних организаций, взаимодействия с внешними организациями, правоохранительными органами, прессой и др.

В качестве примера можно привести две стратегии ответных действий на нарушение безопасности:

- «выследить и осудить», когда злоумышленнику позволяют продолжить действия с целью его компрометации и наказания (данную стратегию одобряют правоохранительные органы);

- «защититься и продолжить», когда организация опасается за уязвимость информационных ресурсов и оказывает максимальное противодействие нарушению.

Задание: Составить политику безопасности предприятия, придерживаясь вышеизложенного плана.

Вопросы для проверки знаний и умений:

1. Что такое политика безопасности?
2. Перечислите цели и задачи политики безопасности на предприятии.
3. Дайте определение понятию объект и субъект политики безопасности.
4. Назовите основное назначение политики информационной безопасности.

Пример вариант теста

1. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

A. Владельцы данных

B. Пользователи

C. Администраторы

D. Руководство

2. Что такое политика безопасности?

A. Пошаговые инструкции по выполнению задач безопасности

B. Общие руководящие требования по достижению определенного уровня безопасности.

C. Широкие, высокоуровневые заявления руководства.

D. Детализированные документы по обработке инцидентов безопасности.

3. Эффективная программа безопасности требует сбалансированного применения:

A. Технических и нетехнических методов.

B. Контрмер и защитных механизмов.

C. Физической безопасности и технических средств защиты.

D. Процедур безопасности и шифрования.

20.2 Промежуточная аттестация

Примерный перечень вопросов к зачету с оценкой

1	Состав сведений конфиденциального характера.
2	Понятие тайны. Виды тайн (государственная, коммерческая, банковская, налоговая, нотариальная, адвокатская, служебная).
3	Понятие тайны. Виды тайн (связи, личной жизни, врачебная, усыновления, страхования, персональные данные (ПДн), голосования, исповеди).

4	Основные свойства информации в форме сведений. Основные свойства информации в форме сообщений.
5	Обеспечение информационной безопасности. Деятельность. Средства. Субъекты.
6	Обеспечение информационной безопасности РФ. Доктрина информационной безопасности РФ.
7	Основные виды организационных средств обеспечения информационной безопасности.
8	Основные направления защиты информации.
9	Основные направления организационной защиты информации.
10	Основные принципы организационной защиты информации.
11	Основные условия организационной защиты информации.
12	Структура системы защиты информации.
13	Основные требования к организации системы защиты информации.
14	Роль руководства в организации защиты информации
15	Основные виды структурных подразделений по защите информации
16	Виды средств защиты конфиденциальной информации
17	Виды методов защиты информации и их содержание
18	Задачи правовых методов защиты информации
19	Классы организационных методов защиты информации
20	Основные понятия при осуществлении права на поиск, получение, передачу, производство и распространение информации и обеспечение ее защиты
21	Основные принципы правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации в России
22	Отнесение сведений к различным видам конфиденциальной информации
23	Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну
24	Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну
25	Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей
26	Сведения, не подлежащие к отнесению к государственной тайне и засекречиванию
27	Основания и порядок рассекречивания сведений и их носителей, составляющих государственную тайну
28	Отнесение сведений к коммерческой тайне. Сведения конфиденциального характера
29	Отнесение сведений к коммерческой тайне. Сведения составляющие коммерческую тайну
30	Основные положения допуска персонала предприятия к конфиденциальной информации
31	Порядок оформления и переоформления допуска к государственной тайне. Формы допуска
32	Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска
33	Организация доступа персонала предприятия к сведениям, составляющим государственную тайну
34	Порядок доступа к конфиденциальной информации командированных лиц
35	Факторы и обстоятельства, приводящие к разглашению конфиденциальной информации персоналом предприятия
36	Основные направления работы с персоналом предприятия, допущенным к конфиденциальной информации
37	Основные методы работы с персоналом предприятия, допущенным к конфиденциальной информации
38	Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии. Режим секретности
39	Основные цели, подходы и принципы организации внутриобъектового режима. Основные мероприятия
40	Силы и средства, используемые при организации внутриобъектового режима
41	Функции и задачи руководителя, заместителя руководителя предприятия
42	Структурные подразделения предприятия, участвующие в организации внутриобъектового режима, их функции и задачи
43	Цели и задачи пропускного режима
44	Основные элементы системы организации пропускного режима, используемые силы и средства
45	Организация системы охраны предприятия
46	Цели и задачи охраны
47	Технические средства охраны

48	Обязанности сотрудников охраны
49	Причины нарушений системы охраны объектов
50	Планирование мероприятий по защите информации при подготовке к проведению совещания
51	Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания
52	Порядок проведения совещания и использования его материалов
53	Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия
54	Основные направления защиты конфиденциальной информации в ходе осуществления предприятием рекламной деятельности
55	Основные направления защиты информации при осуществлении предприятием издательской деятельности
56	Организация подготовки материалов к открытому опубликованию
57	Основы организации защиты информации в ходе взаимодействия со средствами массовой информации
58	Порядок передачи различных видов конфиденциальной информации иностранным государствам
59	Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам
60	Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу
61	Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам
62	Основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну
63	Порядок работы лицензирующего органа по лицензированию деятельности предприятий
64	Организация проведения государственной аттестации руководителей предприятий
65	Организация аналитической работы состояния защиты конфиденциальной информации. Основные функции аналитического подразделения
66	Основные задачи контроля состояния защиты конфиденциальной информации на предприятии
67	Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений
68	Основания, цели и задачи внутреннего (служебного) расследования
69	Процедура внутреннего (служебного) расследования
70	Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну
71	Уголовно-правовая защита в сфере компьютерной информации
72	Уголовно-правовая защита сведений, составляющих государственную тайну
73	Административно-правовая защита информации с ограниченным доступом
74	Гражданско-правовая защита служебной и коммерческой тайны
75	Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений
76	Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений
77	Условия обработки персональных данных и категории персональных данных
78	Согласие субъекта персональных данных на обработку персональных данных
79	Обеспечение выполнения оператором обязанностей. Обеспечению безопасности персональных данных при их обработке
80	Уровни защищенности персональных данных. Требования к защите персональных данных при их обработке в информационных системах

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.40 Организационное и правовое обеспечение информационной безопасности

Форма обучения Очное

Вид контроля Зачет с оценкой

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Состав сведений конфиденциального характера.
2. Уровни защищенности персональных данных. Требования к защите персональных данных при их обработке в информационных системах

Преподаватель _____ В.А. Степанцов

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

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

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

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

При оценивании используется количественная шкала. Критерии оценивания приведены выше.