МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

УТВЕРЖДАЮ
Проректор по учебной работе

_____ Василенко В. Н.
(подпись) (Ф.И.О.)

«25» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ
(наименование в соответствии с РУП)

Направление подготовки (специальность)

38.05.01 Экономическая безопасность
(шифр и наименование направления подготовки/специальности)

Направленность (профиль)

Экономико-правовое обеспечение экономической безопасности
(наименование профиля/специализации)

Квалификация выпускника

экономист

(в соответствии с Приказом Министерства образования и науки РФ от 12 сентября 2013 г. N 1061 "Об утверждении перечней специальностей и направлений подготовки высшего образования" (с изменениями и дополнениями)

1. Цели и задачи дисциплины

Целью освоения дисциплины «Информационная безопасность организации» является освоение специалистами актуальных изменений в вопросах правоохранительной деятельности, обновление их теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению безопасности информации при обработке в информационных системах в условиях существования угроз безопасности информации.

Задачи дисциплины:

реализация мер, обеспечивающих нейтрализацию факторов, способных дестабилизировать экономическую ситуацию;

изучение методов и процедур выявления угроз безопасности информации в информационных системах и оценки степени их опасности;

практическая отработка способов и порядка проведения работ по обеспечению безопасности информации при обработке в информационных системах организаций различной ведомственной принадлежности.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

№ п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ОПК- 3	способностью применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов	понятие и сущность информационной безопасности, ее место в системе экономической безопасности; концепцию информационной безопасности Российской Федерации; принципы построения и элементы систем безопасности; основные направления и особенности проектирования систем защиты информации, ее роль и место в порядке документооборота организаций	применять основные закономерности создания и принципы функционирования систем обеспечения информационной безопасности организаций в интересах обеспечения экономической безопасности	навыками разработки нормативно-распорядительных документов в области обеспечения информационной безопасности, подготовки проведения аттестационных и сертификационных испытаний.
2	ПК-20	способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области	понятие государственной тайны и иных охраняемых законом сведений, составляющих государственную тайну и сведений конфиденциального характера; организационно-правовые основы режима секретности; нормативные правовые документы в области защи-	применять организационные и технические мероприятия по обеспечению информационной безопасности в	навыками электронного документооборота в условиях реализации угроз информационной безопасности в интересах выполнения требования правовых

		защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	ты государственной тайны, обеспечения режима секретности	интересах выполнения требований в области защиты государственной тайны и соблюдения режима секретности	актов в области защиты государственной тайны и информационной безопасности, обеспечение соблюдения режима секретности

3. Место дисциплины в структуре ОП ВО

Дисциплина относится к вариативной части обязательных дисциплин и изучается в 9 семестре 5 года обучения.«Входными» знаниями, умениями и компетенциями обучающегося, необходимыми для изучения дисциплины, служат базовые знания, умения и навыки, полученные при изучении таких дисциплин как Управление организацией (предприятием), прохождении производственной практики. Знания, умения, навыки и компетенции, сформированные при изучении дисциплины будут полезны при освоении таких дисциплин как Научные методы исследования экономической безопасности, прохождении преддипломной практики и ГИА.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 5 зачетных единиц.

Виды учебной работы	**Всего акад. часов**	**Семестр 9**
Общая трудоемкость дисциплины	180	180
Контактная работа в т.ч. аудиторные занятия:	**79**	**79**
Лекции	30	30
Лабораторные занятия	15	15
в том числе в форме практической подготовки	15	15
Практические занятия (ПЗ)	30	30
Консультации текущие	30	30
Вид аттестации (экзамен)	**33,8**	**33,8**
Самостоятельная работа:	**67,5**	**67,5**
Доклад	34,2	34,2
Выполнение домашнего задания	33,3	33,3

5. Содержание дисциплины, структурированное по разделам с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела	Трудоемкость раздела, часы
1	Информационная безопасность в организации	Основные понятия в области защиты государственной тайны и информационной безопасности . Законодательные и иные правовые акты, регулирующие вопросы области защиты государственной тайны и информационной безопасности. Система документов по информационной безопасности и краткая характеристика ее основных составляющих. Структура и направления деятельности системы защиты государственной тайны и информационной безопасности в субъектах Российской Федерации. Система органов в области защиты госу-	135

		дарственной тайны и информационной безопасности в Российской Федерации, их задачи, распределение полномочий по обеспечению технической защиты информации. Лицензирование деятельности в области защиты государственной тайны и информационной безопасности. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации. Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности государственной тайны при обработке в информационных системах. Основные типы актуальных угроз безопасности информации при обработке в информационных системах, порядок их определения. Угрозы несанкционированного доступа к информации в информационных системах. Угрозы утечки информации по техническим каналам. Основные принципы обеспечения безопасности информации при их обработке. Основные направления деятельности по обеспечению безопасности информации при обработке в информационных системах. Общий порядок организации обеспечения безопасности информации в информационных системах. Оценка достаточности и обоснованности запланированных мероприятий. Состав мер по обеспечению безопасности информации. Порядок выбора мер по обеспечению безопасности информации, подлежащих реализации в информационной системе. Содержание мер по обеспечению безопасности информации, реализуемых в рамках системы защиты. Организация обеспечения безопасности информации в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности информации. Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке информации. Обязанности оператора, осуществляющего обработку персональных данных.	

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ЛЗ,час	ПЗ,час	СРО, час (акад. часы)
1	Информационная безопасность в организации	30	15	30	69

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, акад. час
1	Информационная безопасность в организации	Основные понятия в области защиты государственной тайны. Стратегия национальной безопасности Российской Федерации. Законодательство в области государственной тайны. Концептуальные основы технической защиты информации.	8
		Структура и направления деятельности системы защиты государственной тайны в субъектах Российской Федерации. Система органов по защите государственной тайны в Российской Федерации, их задачи, распределение полномочий по обеспечению техниче-	8

		ской защиты информации. Лицензирование деятельности в области государственной тайны. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации.	
		Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности государственной тайны при обработке в информационных системах.	6
		Основные принципы обеспечения безопасности государственной тайны при их обработке. Основные направления деятельности по обеспечению безопасности информации при обработке в информационных системах. Общий порядок организации обеспечения безопасности информации в информационных системах.	8

5.2.2 Практические занятия (ПЗ)

№ п/п	Наименование раздела дисциплины	Тематика ПЗ	Трудоемкость, акад. час
1	Информационная безопасность в организации	Организация обеспечения безопасности государственной тайны в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности государственной тайны.	10
		Порядок выбора мер по обеспечению безопасности информации, подлежащих реализации в информационной системе.	10
		Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера при организации защиты государственной тайны. Обязанности оператора, осуществляющего обработку персональных данных.	10

5.2.3 Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Тематика ЛЗ	Трудоемкость, акад. час
1	Информационная безопасность в организации	Классификация информационного ресурса при обработке государственной тайны. Разработка нормативно-распорядительного документа «Акт ввода в эксплуатацию»	4
		Определение класса защищенности объекта информатизации при обработке конфиденциальной информации. Разработка нормативно-распорядительного документа «Акт классификации в информационной системе»	4
		Актуализация модели угроз информационной безопасности при обработке государственной тайны. Разработка нормативно-распорядительного документа «Модель угроз информационной безопасности».	4
		Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты информации, развертываемой на объекте информатизации в процессе ее создания или модернизации. Разработка нормативно-распорядительного документа «План мероприятий по защите конфиденциальных данных.	3

5.2.4 Самостоятельная работа обучающихся

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, акад. час
1	Информационная безопасность в организации	Доклад	30
		Домашнее задание №1	12
		Домашнее задание №2	9
		Домашнее задание №3	9
		Домашнее задание №4	9

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Петренко, В. И. Защита персональных данных в информационных системах : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016. – 201 с. : схем. –– URL: https://biblioclub.ru/index.php?page=book&id=459205

2. Аверченков, В. И. Защита персональных данных в организации / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. – 3-е изд., стер. – Москва : ФЛИНТА, 2016. – 124 с. – – URL: https://biblioclub.ru/index.php?page=book&id=93260

3. Скрипник, Д. А. Обеспечение безопасности персональных данных: курс / Д. А. Скрипник ; Национальный Открытый Университет "ИНТУИТ". – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2011. – 109 с. : ил., схем. –– URL: https://biblioclub.ru/index.php?page=book&id=234794

6.2 Дополнительная литература

1. Кияев, В. Безопасность информационных систем: курс : [16+] / В. Кияев, О. Граничин. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. : ил. –– URL: https://biblioclub.ru/index.php?page=book&id=429032

2. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, К. В. Славнов, Е. В. Кравцов ; под ред. А. В. Душкина. – Москва : Горячая линия – Телеком, 2016. – 248 с. : схем., табл., ил. – URL: https://biblioclub.ru/index.php?page=book&id=483768

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

СкрыпниковА.В. Информационная безопасность в организации [Электронный ресурс] : методические указания и задания к самостоятельной работе для обучающихся по специальности 38.05.01 - «Экономическая безопасность», очной и заочной формы обучения / СкрыпниковА.В., В. А. Хвостов ; ВГУИТ, Кафедра информационной безопасности. - Воронеж: ВГУИТ, 2017. http://education.vsuet.ru

6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Сайт научной библиотеки ВГУИТ <http://cnit.vsuet.ru>.
2. Базовые федеральные образовательные порталы. <http://www.edu.ru/db/portal/sites/portal_page.htm>.
3. Государственная публичная научно-техническая библиотека. <www.gpntb.ru/>.
4. Федеральная служба государственной статистики. <http://www.gks.ru/>.
5. Национальная электронная библиотека. <www.nns.ru/>..
6. Поисковая система «Апорт». <www.aport.ru/>.

7. Поисковая система «Рамблер». <www.rambler.ru/>.
8. Поисковая система «Yahoo» . <www.yahoo.com/>.
9. Поисковая система «Яндекс». <www.yandex.ru/>.
10. Российская государственная библиотека. <www.rsl.ru/>.
11. Российская национальная библиотека. <www.nlr.ru/>.

6.5 Методические указания для обучающихся по освоению дисциплины

1. Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс] :методические указания для обучающихсяна всех уровнях высшего образования / М. М. Данылив, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. - Воронеж : ВГУИТ, 2016. – Режим доступа:http://biblos.vsuet.ru/. - Загл. с экрана

Порядок изучения курса:

- Объем трудоемкости дисциплины – 5 зачетных единиц (180 ак. ч.);
- Виды учебной работы и последовательность их выполнения:
- аудиторная: лекции, лабораторные, практические занятия – посещение в соответствии с учебным расписанием;
- самостоятельная работа: изучение теоретического материалы для сдачи тестовых заданий, подготовка к практическим занятиям, формирование каталога Интернет-ресурсов, подготовка и участие в диспуте, выполнение и сдача домашнего задания и курсовой работы – выполнение в соответствии с графиком контроля текущей успеваемости;
- График контроля текущей успеваемости обучающихся – рейтинговая оценка;
- Состав изученного материала для каждой рубежной точки контроля - рубежный контроль на практических занятиях (тестирование, каталог Интернет-ресурсов, участие в диспуте), домашнее задание, курсовая работа;
- Учебно-методическое и информационное обеспечение дисциплины: рекомендуемая литература, методические разработки, перечень ресурсов информационно-телекоммуникационной сети «Интернет»;
- Заполнение рейтинговой системы текущего контроля процесса обучения дисциплины – контролируется на сайте www.vsuet.ru;
- Допуск к сдаче экзамена – при выполнении графика контроля текущей успеваемости;
- Прохождение промежуточной аттестации –экзамен (собеседование).

6.6 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Используемые виды информационных технологий:

- «электронная»: персональный компьютер и информационно-поисковые (справочно-правовые) системы;
- «компьютерная» технология: персональный компьютер с программными продуктами разного назначения (ОС Windows; ОС ALT Linux; СЗИ "Страж -NT v. 3.0", СЗИ "DallasLock 8.0");
- «сетевая»: локальная сеть университета и глобальная сеть Internet.

7 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа (а. 240), практических занятий (а.420), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (а. 420), укомплектованные специальной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории; помещения для самостоятельной работы (а. 251), оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспеченные досту-

пом в электронную информационно-образовательную среду организации; помещение для хранения и профилактического обслуживания учебного оборудования (а. 249б). Для проведения занятий лекционного типа предусмотрены учебно-наглядные пособия, обеспечивающие тематические иллюстрации.

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

8.1 **Оценочные материалы** (ОМ) для дисциплины включают в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

8.2 Для каждого результата обучения по дисциплине (модулю) определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины (модуля)**.

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

ПРИЛОЖЕНИЕ
к рабочей программе

1. Организационно-методические данные дисциплины для очно-заочной или заочной форм обучения

1.1 Объемы различных форм учебной работы и виды контроля в соответствии с учебным планом

Общая трудоемкость дисциплины (модуля) составляет __5__ зачетных единиц

Виды учебной работы	**Всего академических часов**	**Распределение трудоемкости по семестрам, ак. ч**
		Акад. ч 11 семестр
Общая трудоемкость дисциплины (модуля)	180	180
Контактная работа в т. ч. аудиторные занятия:	26.2	26.2
Лекции	8	8
Практические/лабораторные занятия	14	14
в том числе в форме практической подготовки	14	14
Консультации текущие	4.2	4.2
Консультации перед экзаменом		
Вид аттестации (зачет/экзамен)	6.8	6.8
Самостоятельная работа:	147	147
Проработка материалов по лекциям, учебникам, учебным пособиям	70	70
Подготовка к практическим/лабораторным занятиям	40	40
Курсовой проект/работа		
Домашнее задание, реферат,	20	20
Другие виды самостоятельной работы	7	7
Подготовка к экзамену (контроль)	10	10

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ

1 Перечень компетенций с указанием этапов их формирования

п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
	ОПК- 3	способностью применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов	понятие и сущность информационной безопасности, ее место в системе экономической безопасности; концепцию информационной безопасности Российской Федерации; принципы построения и элементы систем безопасности; основные направления и особенности проектирования систем защиты информации, ее роль и место в порядке документооборота организаций	применять основные закономерности создания и принципы функционирования систем обеспечения информационной безопасности организаций в интересах обеспечения экономической безопасности	навыками разработки нормативно-распорядительных документов в области обеспечения информационной безопасности, подготовки проведения аттестационных и сертификационных испытаний.
	ПК-20	способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	понятие государственной тайны и иных охраняемых законом сведений, составляющих государственную тайну и сведений конфиденциального характера; организационно-правовые основы режима секретности; нормативные правовые документы в области защиты государственной тайны, обеспечения режима секретности	применять организационные и технические мероприятия по обеспечению информационной безопасности в интересах выполнения требований в области защиты государственной тайны и соблюдения режима секретности	навыками электронного документооборота в условиях реализации угроз информационной безопасности в интересах выполнения требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечение соблюдения режима секретности

2 Паспорт фонда оценочных средств по дисциплине

№ п/п	Разделы дисциплины	Индекс контролируемой компетенции	Оценочные средства		Технология/процедура оценивания (способ контроля)
			наименование	№№ заданий	
1	Информационная безопасность в организации	ОПК-3	Экзамен	1-34	Уровневая шкала
			Контрольные вопросы к текущим	62-95	Уровневая шкала

			опросам на практических работах		
			Доклад	124	Уровневая шкала
			Домашнее задание	125-129	Уровневая шкала
		ПК-20	Экзамен	35-61	Уровневая шкала
			Контрольные вопросы к текущим опросам на практических работах	96-123	Уровневая шкала
			Доклад	124	Уровневая шкала
			Домашнее задание	125-129	Уровневая шкала

3 Оценочные средства для промежуточной аттестации.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1 Вопросы для экзамена

3.1.1 ОПК- 3 способностью применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов

№ задания	Формулировка вопроса
1	Что такое защита информации?
2	Что является основным содержанием защиты информации?
3	Что такое защищаемая информация?
4	Что такое угроза безопасности информации?
5	Что такое естественная угроза безопасности информации?
6	Что такое искусственная угроза безопасности информации?
7	Какое отличие между непреднамеренными и преднамеренными угрозами безопасности информации?
8	Какие основные виды преднамеренных угроз безопасности информации?
9	Какими основными законами Российской федерации регламентирована защита конфиденциальных данных в организациях различной ведомственной принадлежности?
10	Какие основные категории конфиденциальных данных, обрабатываемых в информационных системах?
11	Какие объекты из состава информационных систем в учреждении требуют реализации организационных и технических мероприятий по защите конфиденциальных данных?
12	Какая информация о человеке должна быть отнесена к категории персональные данные?
13	Какая информация о сотрудниках должна быть отнесена к категории персональные данные?
14	Какая технологическая информация об информационных системах должна быть отнесена к категории персональные данные?
15	Какие данные требуют выполнения ряда мероприятий по защите информации в организации кроме конфиденциальных данных?
16	Что является информационным основанием функционирования организации различной ведомственной принадлежности?
17	Какой состав программного обеспечения типовой информационной системы?
18	Какой состав аппаратного обеспечения типовой информационной системы?
19	Какими особенностями функционирования обладают информационные системы с

	точки зрения решения задачи обеспечения защиты конфиденциальных данных?
20	Основные способы защиты информации при обработке персональных данных в информационных системах.
21	Основные средства защиты информации при обработке персональных данных в информационных системах.
22	Состав и основные функции систем защиты информации уровня отдельных ЭВМ.
23	Какие основные принципы построения и эксплуатации систем защиты информации?
24	Назовите основные типы систем защиты информации, используемые для защиты конфиденциальных данных в информационных системах?
25	Какими защитными функциями обеспечения безопасности информации наиболее распространенных операционных систем можно воспользоваться при построении защиты конфиденциальных?
26	Какой главный недостаток защитных функций обеспечения безопасности информации наиболее распространенных операционных систем с точки зрения защиты конфиденциальных данных?
27	Назовите основные защитные функции, реализуемые операционной системой WINDOWS XP.
28	Назовите основные защитные функции, реализуемые операционной системой LINUX.
29	Какой состав системы защиты информации уровня отдельной ЭВМ?
30	Назовите назначение подсистемы управления доступом системы защиты информации уровня отдельного ЭВМ.
31	Назовите назначение подсистемы регистрации и учета системы защиты информации уровня отдельного ЭВМ.
32	Назовите назначение криптографической подсистемы системы защиты информации уровня отдельного ЭВМ.
33	Назовите назначение подсистемы контроля целостности системы защиты информации уровня отдельного ЭВМ.
34	Назовите назначение межсетевого экрана.

3.1.2 ***ПК-20*** способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

№ задания	Формулировка вопроса
35	Какие параметры могут использоваться в качестве критериев анализа межсетевых экранов.
36	Назовите назначение системы обнаружения вторжений.
37	Назовите назначение средств построения виртуальных частных сетей.
38	Назовите назначение средств централизованного управления информационной безопасностью.
39	Назовите назначение средств анализа защищенности информационных систем.
40	Какие основные этапы и их содержание выполняемых действий руководителем учреждения при организации защиты персональных данных?
41	Какие основные этапы и их содержание выполняемых действий ответственным за обработку персональных данных сотрудником при организации защиты персональных данных?
42	Какие основные этапы и их содержание выполняемых действий ответственным за защиту персональных данных сотрудником при организации защиты?
43	Какие основные признаки классификации информационных систем при организации защиты персональных данных?
44	Какая последовательность действий при проведении классификации информационных систем?
45	Какие основные классы конфиденциальности информационных систем существуют?
46	Что такое акт классификации информационной системы?
47	Что такое политики безопасности персональных данных?
48	Что такое модель угроз безопасности персональных данных?

51	Что такое сертификат ФСТЭК России на устанавливаемые системы защиты?
52	Назовите основное содержание проверки эффективности мероприятий по защите персональных данных?
53	На какие виды деятельности должна иметь лицензию организация, привлекаемая для проверки эффективности мероприятий по защите персональных данных?
54	В чем заключается процесс аттестации информационной системы?
55	Какие основные документы содержат основные результаты и выводы аттестационных испытаний информационной системы?
56	Какой срок действия Аттестата соответствия?
57	Каково содержание основных действий при эксплуатации аттестованной информационной системы?
58	В чем заключается управление подсистемой управления доступом?
59	В чем заключается управление подсистемой контроля целостности?
60	В чем заключается управление криптографической подсистемой?
61	В чем заключается управление подсистемой регистрации и учета?

3.2 Задания к практическим работам

3.2.1 ОПК- 3 способностью применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов

№ задания	Формулировка задания
62	Составить последовательность этапов действий руководителя организации по обеспечению информационной безопасности конфиденциальных данных, содержащих коммерческую тайну, и сформулировать их содержание.
63	Составить последовательность этапов действий должностного лица, ответственного за обработку конфиденциальной информации, по обеспечению информационной безопасности конфиденциальных данных, содержащих коммерческую тайну, и сформулировать их содержание.
64	Составить последовательность этапов действий должностного лица, ответственного за защиту конфиденциальной информации, по обеспечению информационной безопасности конфиденциальных данных, содержащих коммерческую тайну, и сформулировать их содержание.
65	Составить последовательность этапов действий руководителя организации по обеспечению информационной безопасности конфиденциальных данных, содержащих персональные данные, и сформулировать их содержание.
66	Составить последовательность этапов действий должностного лица, ответственного за обработку конфиденциальной информации, по обеспечению информационной безопасности конфиденциальных данных, содержащих персональные данные, и сформулировать их содержание.
67	Составить последовательность этапов действий должностного лица, ответственного за защиту конфиденциальной информации, по обеспечению информационной безопасности конфиденциальных данных, содержащих персональные данные, и сформулировать их содержание.
68	Составить последовательность этапов действий руководителя организации по обеспечению информационной безопасности конфиденциальных данных, содержащих банковскую тайну, и сформулировать их содержание.
69	Составить последовательность этапов действий должностного лица, ответственного за обработку конфиденциальной информации, по обеспечению информационной безопасности конфиденциальных данных, содержащих банковскую тайну, и сформулировать их содержание.
70	Составить последовательность этапов действий должностного лица, ответственного за защиту конфиденциальной информации, по обеспечению информационной безопасности конфиденциальных данных, содержащих банковскую тайну, и сформулировать их содержание.
71	Провести классификацию информационных систем персональных данных по исходным данным:

	Количество субъектов персональных данных менее 1000, персональные данные категории 1.
72	Провести классификацию информационных систем персональных данных по исходным данным: Количество субъектов персональных данных менее 1000, персональные данные категории 2
73	Провести классификацию информационных систем персональных данных по исходным данным: Количество субъектов персональных данных менее 1000, персональные данные категории 3
74	Провести классификацию информационных систем персональных данных по исходным данным: Количество субъектов персональных данных менее 1000, персональные данные категории 4
75	Провести классификацию информационных систем персональных данных по исходным данным: Количество субъектов персональных данных от 1000 до 100000, персональные данные категории 1.
76	Провести классификацию информационных систем персональных данных по исходным данным: Количество субъектов персональных данных от 1000 до 100000, персональные данные категории 2
77	Провести классификацию информационных систем персональных данных по исходным данным: Количество субъектов персональных данных от 1000 до 100000, персональные данные категории 2
78	Провести классификацию информационных систем персональных данных по исходным данным: Количество субъектов персональных данных от 1000 до 100000, персональные данные категории 3
79	Провести классификацию информационных систем персональных данных по исходным данным: Количество субъектов персональных данных от 1000 до 100000, персональные данные категории 4
80	Провести классификацию информационных систем персональных данных по исходным данным: Количество субъектов персональных данных более 100000, персональные данные категории 1
81	Провести классификацию информационных систем персональных данных по исходным данным: Количество субъектов персональных данных более 100000, персональные данные категории 2
82	Провести классификацию информационных систем персональных данных по исходным данным: Количество субъектов персональных данных более 100000, персональные данные категории 3
83	Провести классификацию информационных систем персональных данных по исходным данным: Количество субъектов персональных данных более 100000, персональные данные категории 4
84	Сформировать План мероприятий по обеспечению защиты конфиденциальных данных, содержащих коммерческую тайну
85	Сформировать План мероприятий по обеспечению защиты конфиденциальных данных коммерческого банка в соответствии с нормативной документацией Банка России
86	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Положение о защите конфиденциальных данных»

87	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Положение о подразделении по защите информации»
88	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Приказ о назначении ответственных лиц за обработку конфиденциальной информации»
89	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Концепция информационной безопасности ИС учреждения»
90	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Политика информационной безопасности ИСПДн учреждения»
91	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Перечень конфиденциальных данных, подлежащих защите»
92	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Приказ о проведении внутренней проверки»
93	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Положение о разграничении прав доступа к обрабатываемым персональным данным»
94	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Положение об Электронном журнале обращений пользователей информационной системы к конфиденциальным данным»
95	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Журнал по учету мероприятий по контролю состояния защиты информации»

3.2.2 ***ПК-20*** способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

№ задания	Формулировка задания
96	Составить последовательность этапов действий руководителя организации по обеспечению информационной безопасности конфиденциальных данных, содержащих государственную тайну, и сформулировать их содержание.
97	Составить последовательность этапов действий должностного лица, ответственного за обработку конфиденциальной информации, по обеспечению информационной безопасности конфиденциальных данных, содержащих государственную тайну, и сформулировать их содержание.
98	Составить последовательность этапов действий должностного лица, ответственного за защиту конфиденциальной информации, по обеспечению информационной безопасности конфиденциальных данных, содержащих государственную тайну, и сформулировать их содержание.
99	Составить последовательность этапов действий руководителя организации по обеспечению информационной безопасности конфиденциальных данных, содержащих служебную тайну, и сформулировать их содержание.
100	Составить последовательность этапов действий должностного лица, ответственного за обработку конфиденциальной информации, по обеспечению информационной безопасности конфиденциальных данных, содержащих служебную тайну, и сформулировать их содержание.
101	Составить последовательность этапов действий должностного лица, ответственного за защиту конфиденциальной информации, по обеспечению информационной безопасности конфиденциальных данных, содержащих служебную тайну, и сформулировать их содержание.
102	Сформировать перечень требований к средству вычислительной техники, предназначенному для обработки государственной тайны в соответствии с 1 классом защищенности (Руководящий документ Средства вычислительной

	техники Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации).
103	Сформировать перечень требований к средству вычислительной техники, предназначенному для обработки государственной тайны в соответствии с 2 классом защищенности (Руководящий документ Средства вычислительной техники Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации).
104	Сформировать перечень требований к средству вычислительной техники, предназначенному для обработки государственной тайны в соответствии с 3 классом защищенности (Руководящий документ Средства вычислительной техники Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации).
105	Сформировать перечень требований к средству вычислительной техники, предназначенному для обработки государственной тайны в соответствии с 4 классом защищенности (Руководящий документ Средства вычислительной техники Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации).
106	Сформировать перечень требований к средству вычислительной техники, предназначенному для обработки служебной тайны в соответствии с 5 классом защищенности (Руководящий документ Средства вычислительной техники Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации).
107	Сформировать перечень требований к средству вычислительной техники, предназначенному для обработки служебной тайны в соответствии с 6 классом защищенности (Руководящий документ Средства вычислительной техники Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации).
108	Сформировать перечень требований к автоматизированной системе, предназначенной для обработки государственной тайны, в соответствии с классом защищенности 3А (Руководящий документ Автоматизированные системы Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.).
109	Сформировать перечень требований к автоматизированной системе, предназначенной для обработки государственной тайны, в соответствии с классом защищенности 2А (Руководящий документ Автоматизированные системы Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.).
110	Сформировать перечень требований к автоматизированной системе, предназначенной для обработки государственной тайны, в соответствии с классом защищенности 1А (Руководящий документ Автоматизированные системы Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.).
111	Сформировать перечень требований к автоматизированной системе, предназначенной для обработки государственной тайны, в соответствии с классом защищенности 1Б (Руководящий документ Автоматизированные системы Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.).
112	Сформировать перечень требований к автоматизированной системе, предназначенной для обработки государственной тайны, в соответствии с классом защищенности 1В (Руководящий документ Автоматизированные системы Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.).

113	Сформировать перечень требований к автоматизированной системе, предназначенной для обработки государственной тайны, в соответствии с классом защищенности 1В (Руководящий документ Автоматизированные системы Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.).
114	Сформировать перечень требований к автоматизированной системе, предназначенной для обработки служебной тайны, в соответствии с классом защищенности 3Б (Руководящий документ Автоматизированные системы Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.).
115	Сформировать перечень требований к автоматизированной системе, предназначенной для обработки служебной тайны, в соответствии с классом защищенности 2Б (Руководящий документ Автоматизированные системы Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.).
116	Сформировать перечень требований к автоматизированной системе, предназначенной для обработки служебной тайны, в соответствии с классом защищенности 1Г (Руководящий документ Автоматизированные системы Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.).
117	Сформировать перечень требований к автоматизированной системе, предназначенной для обработки служебной тайны, в соответствии с классом защищенности 1Д (Руководящий документ Автоматизированные системы Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.).
118	Сформировать перечень требований к выделенным помещениям для ведения секретных переговоров 1 категории
119	Сформировать перечень требований к выделенным помещениям для ведения секретных переговоров 2 категории
120	Сформировать перечень требований к выделенным помещениям для ведения секретных переговоров 3 категории
121	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Акт ввода в эксплуатацию средства вычислительной техники (автоматизированной системы)»
122	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Список допущенных к проведению автоматизированных расчетов»
123	Разработать и определить порядок ввода в действие в организации нормативно распорядительного документа «Разрешение на проведение автоматизированных расчетов»

3.3 Тематика докладов и презентаций

3.3.1 ***ПК-3*** способностью применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов

3.3.2 ***ОПК-20*** способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

№ задания	Темы доклада
124	Система документов по защите персональных данных в Российской федерации

3.4 Домашнее задание №1

3.4.1 ***ПК-3*** способностью применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов

№ задания	Формулировка задания
125	Разработка нормативно распорядительного документа «Отчет о результатах проведения внутренней проверки». В качестве исходных данных при разработке документа используются информационные системы аудиторий 420 и 332а «Университета».

3.5 Домашнее задание №2

3.5.1 ***ПК-3*** способностью применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов

№ задания	Формулировка задания
126	Разработка нормативно распорядительного документа «Модель угроз безопасности конфиденциальных данных». В качестве исходных данных при разработке документа используются информационные системы аудиторий 420 и 332а «Университета».

3.6 Домашнее задание №3

3.6.1 ***ПК-3*** способностью применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов

№ задания	Формулировка задания
127	Разработка нормативно распорядительного документа «План мероприятий по обеспечению защиты конфиденциальных данных». В качестве исходных данных при разработке документа используются информационные системы аудиторий 420 и 332а «Университета».

3.6 Домашнее задание №4

3.6.1 ***ПК-3*** способностью применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов

№ задания	Формулировка задания
128	Разработка нормативно распорядительного документа «Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ». В качестве исходных данных при разработке документа используются информационные системы аудиторий 420 и 332а «Университета».

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

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

- П ВГУИТ 2.4.03 Положение о курсовых, экзаменах и зачетах;
- П ВГУИТ 4.1.02 Положение о рейтинговой оценке текущей успеваемости.

Для оценки знаний, умений, навыков обучающихся по дисциплине применяется рейтинговая система. Итоговая оценка по дисциплине определяется на основании определения среднеарифметического значения баллов по каждому заданию

5. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания для каждого результата обучения по дисциплине

Результаты обучения по этапам формирования компетенций	Предмет оценки (продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
ПК-12 способность применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов					
ЗНАТЬ: понятие и сущность информационной безопасности, ее место в системе национальной безопасности РФ; концепцию информационной безопасности Российской Федерации; принципы построения и элементы систем безопасности; основные направления и особенности проектирования систем защиты информации, ее роль и место в порядке документооборота организаций	Ответ на экзамене (тестовая часть)	Правильность ответов при тестировании	Обучающийся ответил на 85-100 % вопросов	отлично	освоена/повышенный
			Обучающийся ответил на 70-84 % вопросов	хорошо	освоена/повышенный
			Обучающийся ответил на 50-69 % вопросов	удовлетворительно	освоена/базовый
			Обучающийся ответил на 0-49 % вопросов	неудовлетворительно	не освоена (недостаточный)
	Результаты текущего тестирования	Правильность ответов при тестировании	Обучающийся ответил на 85-100 % вопросов	отлично	освоена/повышенный
			Обучающийся ответил на 70-84 % вопросов	хорошо	освоена/повышенный
			Обучающийся ответил на 50-69 % вопросов	удовлетворительно	освоена/базовый
			Обучающийся ответил на 0-49 % вопросов	неудовлетворительно	не освоена (недостаточный)
УМЕТЬ: применять основные закономерности создания и принципы функционирования систем обеспечения информационной безопасности организаций	Доклад	Правильность, лаконичность и полнота выполнения задания	В докладе проведен нормативной документации всех законодательных уровней по теме исследования в количестве не менее 10	отлично	освоена/повышенный
			Анализ нормативной документации менее 10, охвачены все законодательные уровни, доклад сформирован	хорошо	освоена/повышенный
			Анализ нормативной документации менее 10, охвачены не все законодательные уровни, доклад сформирован	удовлетворительно	освоена/базовый
			Перечень нормативной документации менее 10, охвачены не все законодательные уровни, доклад не сформирован	неудовлетворительно	не освоена (недостаточный)
ВЛАДЕТЬ: навыками разработки нормативно-распорядительных документов в области обеспечения информационной безопасности, подготовки проведения аттестационных и сертификационных испытаний	Домашнее задание	Качество представленного нормативно-распорядительного документа	Представлен подробный нормативно-распорядительный документ, в котором отражены вопросы регулирования требований по защите информации, подобраны и изучены основные источники по нормативному документу, грамотно составлены ссылки на нормативно-законодательную базу. Язык документа полностью соответствует проблемному направлению техническая защита информации.	отлично	освоена/повышенный

			Представлен краткий нормативно-распорядительный документ, в котором отражены вопросы регулирования требований по защите информации, подобраны и изучены основные источники по нормативному документу, грамотно составлены ссылки на нормативно-законодательную базу. Допущены некоторые ошибки. Язык документа не полностью соответствует проблемному направлению техническая защита информации.	хорошо	освоена/повышенный
			Представлен сжатый нормативно-распорядительный документ, в котором отражены вопросы регулирования требований по защите информации, подобраны и изучены основные источники по нормативному документу, грамотно составлены ссылки на нормативно-законодательную базу. Допущены существенные ошибки. Язык документа не соответствует проблемному направлению техническая защита информации.	удовлетворительно	освоена/базовый
			Не представлен нормативно-распорядительный документ, в котором отражены вопросы регулирования требований по защите информации. Допущены некоторые ошибки. Язык документа не соответствует проблемному направлению техническая защита информации.	неудовлетворительно	не освоена (недостаточный)
ПК-23 способность соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности					
ЗНАТЬ: понятие государственной тайны и иных охраняемых законом сведений, составляющих государственную тайну и сведений конфиденциального характера; организационно-правовые основы режима секретности; нормативные правовые документы в области защиты государственной тайны, обеспечения режима секретности	Ответ на экзамене (кейс-задача)	Знание правовых основ в области защиты государственной тайны, информационной безопасности и обеспечения соблюдения режима секретности	Обучающийся ответил на все вопросы, выбрал верную методику анализа, допустил не более 1 ошибки в ответе, решил задачу	отлично	освоена/повышенный
			Обучающийся ответил на все вопросы, выбрал верную методику анализа, допустил более 1, но менее 3 ошибок, решил задачу	хорошо	освоена/повышенный
			Обучающийся выбрал верную методику анализа, ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки, решил задачу	удовлетворительно	освоена/базовый
			Обучающийся ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки, или ответил на все вопросы верно, но не решил задачу	неудовлетворительно	не освоена (недостаточный)
	Результаты текущего тестирования	Правильность ответов при тестировании	Обучающийся ответил на 85-100 % вопросов	отлично	освоена/повышенный
			Обучающийся ответил на 70-84 % вопросов	хорошо	освоена/повышенный
			Обучающийся ответил на 50-69 % вопросов	удовлетворительно	освоена/базовый
			Обучающийся ответил на 0-49 % вопросов	неудовлетво-	не освоена (недос-

				рительно	таточный)
УМЕТЬ: применять организационные и технические мероприятия по обеспечению информационной безопасности в интересах выполнения требований в области защиты государственной тайны и соблюдения режима секретности	Доклад	Правильность, лаконичность и полнота выполнения задания	В докладе проведен нормативной документации всех законодательных уровней по теме исследования в количестве не менее 10	отлично	освое-на/повышенный
			Анализ нормативной документации менее 10, охвачены все законодательные уровни, доклад сформирован	хорошо	освое-на/повышенный
			Анализ нормативной документации менее 10, охвачены не все законодательные уровни, доклад сформирован	удовлетвори-тельно	освоена/базовый
			Перечень нормативной документации менее 10, охвачены не все законодательные уровни, доклад не сформирован	неудовлетво-рительно	не освоена (не-достаточный)
ВЛАДЕТЬ: навыками электронного документооборота в условиях реализации угроз информационной безопасности в интересах выполнения требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечение соблюдения режима секретности	Домашнее задание	Качество представленного нормативно-распорядительного документа	Представлен подробный нормативно-распорядительный документ, в котором отражены вопросы регулирования требований по защите информации, подобраны и изучены основные источники по нормативному документу, грамотно составлены ссылки на нормативно-законодательную базу. Язык документа полностью соответствует проблемному направлению техническая защита информации.	отлично	освое-на/повышенный
			Представлен краткий нормативно-распорядительный документ, в котором отражены вопросы регулирования требований по защите информации, подобраны и изучены основные источники по нормативному документу, грамотно составлены ссылки на нормативно-законодательную базу. Допущены некоторые ошибки. Язык документа не полностью соответствует проблемному направлению техническая защита информации.	хорошо	освое-на/повышенный
			Представлен сжатый нормативно-распорядительный документ, в котором отражены вопросы регулирования требований по защите информации, подобраны и изучены основные источники по нормативному документу, грамотно составлены ссылки на нормативно-законодательную базу. Допущены существенные ошибки. Язык документа не соответствует проблемному направлению техническая защита информации.	удовлетвори-тельно	освоена/базовый

			Не представлен нормативно-распорядительный документ, в котором отражены вопросы регулирования требований по защите информации. Допущены некоторые ошибки. Язык документа не соответствует проблемному направлению техническая защита информации.	неудовлетворительно	не освоена (недостаточный)