МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
"РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА"

СОГЛАСОВАНО
Зав. выпускающей кафедры

УТВЕРЖДАЮ

Управление информационной безопасностью

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационной безопасности**

Учебный план 10.05.03_24_00.plx

Квалификация **специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**9 (5.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Иная контактная работа	0,25	0,25	0,25	0,25
Итого ауд.	64,25	64,25	64,25	64,25
Контактная работа	64,25	64,25	64,25	64,25
Сам. работа	62	62	62	62
Часы на контроль	17,75	17,75	17,75	17,75
Итого	144	144	144	144

г. Рязань

Программу составил(и):
к.т.н., доцент, Кузьмин рий Михайлович

Рабочая программа дисциплины

Управление информационной безопасностью

разработана в соответствии с ФГОС ВО:

ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

составлена на основании учебного плана:

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

утвержденного учёным советом вуза от 26.01.2024 протокол № 8.

Рабочая программа одобрена на заседании кафедры

Информационной безопасности

Протокол от 17.06.2024 г. № 12
Срок действия программы: 2024-2030 уч.г.
Зав. кафедрой Пржегорлинский Виктор Николаевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2025 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2026 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2027 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2028 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью дисциплины является получение обучающимися знаний, формирование у них умений и навыков, необходимых при разработке политик безопасности организации и администрирования систем обеспечения информационной безопасности для решения задач в профессиональной деятельности.
1.2	Задачами дисциплины являются:
1.3	− получение знаний об основных уязвимостях и угрозах безопасности информации, моделях угроз и нарушителя в автоматизированных системах, принципах формирования политики информационной безопасности в автоматизированных системах; рисках информационной безопасности в автоматизированных системах; методах и мерах по управлению информационной безопасностью в автоматизированных системах и оценке эффективности принятых мер;
1.4	− приобретение умения выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; проводить мониторинг угроз безопасности автоматизированных систем; разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; разрабатывать корпоративную и частные политики информационной безопасности автоматизированных систем; оценивать информационные риски в автоматизированных системах; составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; разрабатывать предложения по совершенствованию системы управления ин-формационной безопасностью автоматизированных систем; определять информаци-онную инфраструктуру и информационные ресурсы организации, подлежащие защите; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем;
1.5	− приобретение практических навыков управления информационной безопасностью автоматизированных систем; разработки политик информационной безопасности, анализа информационной инфраструктуры автоматизированной системы и степени ее текущей безопасности, участия в экспертизе состояния защищенности информации на объекте защиты; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.
2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Компьютерные сети
2.1.2	Спецдисциплина 3
2.1.3	Государственные стандарты по защите информации
2.1.4	Нормативное обеспечение информационной безопасности компьютерных систем
2.1.5	Правовое регулирование в сфере информационно-коммуникационных технологий
2.1.6	Нормативное обеспечение информационной безопасности компьютерных систем
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита государственной тайны в Российской Федерации
2.2.2	Практика по получению профессиональных умений и опыта профессиональной деятельности
2.2.3	Производственная практика
2.2.4	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
2.2.5	Преддипломная практика
3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	
ОПК-5.7. Разрабатывает частные политики информационной безопасности автоматизированных систем	
Знать Требования к разработке политик информационной безопасности автоматизированных систем (АС), порядок проведения анализа АС, порядок разработки и типовую структуру разрабатываемой политики информационной безопасности АС **Уметь** Проводить анализ безопасности АС и разрабатывать политики информационной безопасности АС **Владеть** Навыками проведения анализа безопасности АС и разработки политики информационной безопасности АС	
ОПК-5.8. Разрабатывает предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	

Знать
Критерии оценки эффективности и направления совершенствования системы управления информационной безопасностью
Уметь
Проводить оценку эффективности системы управления информационной безопасностью АС и определять направление совершенствования системы управления информационной безопасностью АС
Владеть
Навыками оценки эффективности системы управления информационной безопасностью АС и определения направление ее совершенствования

ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах 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. Анализирует и оценивает риски информационной безопасности

Знать
Методы и средства анализа и оценки рисков информационной безопасности
Уметь
Анализировать и оценивать риски информационной безопасности
Владеть
Навыками анализа и оценки рисков информационной безопасности

ОПК-6.6. Контролирует эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем

Знать
Показатели эффективности мер по реализации частных политик информационной безопасности автоматизированных систем
Уметь
Контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем
Владеть
Навыками контроля эффективности принятых мер по реализации частных политик информационной безопасности

ОПК-15: Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;

ОПК-15.1. Определяет информационную инфраструктуру и информационные ресурсы автоматизированных систем, подлежащие защите

Знать
Основные информационную инфраструктуру и информационные ресурсы автоматизированных систем, подлежащие защите
Уметь
Определять информационную инфраструктуру и информационные ресурсы автоматизированных систем, подлежащие защите
Владеть
Навыками определения информационной инфраструктуры и информационных ресурсов автоматизированных систем,

ОПК-15.2. Выявляет угрозы безопасности автоматизированных систем в защищенном исполнении

Знать
Основные угрозы безопасности автоматизированных систем в защищенном исполнении
Уметь
Выявлять угрозы безопасности автоматизированных систем в защищенном исполнении
Владеть
Навыками выявления угроз безопасности автоматизированных систем в защищенном исполнении

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	Требования к разработке политик информационной безопасности автоматизированных систем (АС), порядок проведения анализа АС, порядок разработки и типовую структуру разрабатываемой политики информационной безопасности АС
3.1.2	Критерии оценки эффективности и направления совершенствования системы управления информационной безопасностью
3.1.3	Методы и средства анализа и оценки рисков информационной безопасности
3.1.4	Показатели эффективности мер по реализации частных политик информационной безопасности автоматизированных систем
3.1.5	Основные информационную инфраструктуру и информационные ресурсы автоматизированных систем, подлежащие защите

3.1.6	Основные угрозы безопасности автоматизированных систем в защищенном исполнении
3.2	**Уметь:**
3.2.1	Проводить анализ безопасности АС и разрабатывать политики информационной безопасности АС
3.2.2	Проводить оценку эффективности системы управления информационной безопасностью АС и определять направление совершенствования системы управления информационной безопасностью АС
3.2.3	Анализировать и оценивать риски информационной безопасности
3.2.4	Контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем
3.2.5	Определять информационную инфраструктуру и информационные ресурсы автоматизированных систем, подлежащие защите
3.2.6	Выявлять угрозы безопасности автоматизированных систем в защищенном исполнении
3.3	**Владеть:**
3.3.1	Навыками проведения анализа безопасности АС и разработки политики информационной безопасности АС
3.3.2	Навыками анализа и оценки рисков информационной безопасности
3.3.3	Навыками контроля эффективности принятых мер по реализации частных политик информационной безопасности автоматизированных систем
3.3.4	Навыками определения информационной инфраструктуры и информационных ресурсов автоматизированных систем, подлежащие защите
3.3.5	Навыками выявления угроз безопасности автоматизированных систем в защищенном исполнении

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Форма контроля
	Раздел 1. Введение в дисциплину. Базовая терминология					
1.1	/Тема/	9	0			
1.2	Цели, задачи, содержание дисциплины, планируемые результаты обучения по дисциплине. Система. Системный подход. Процесс. Процессный подход. Управление. Циклическая модель улучше-ния процессов. Системный подход к управлению организацией. Процессный подход к управлению организацией. /Лек/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
1.3	Изучение конспекта лекций /Ср/	9	9	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).

1.4	Изучение схемы взаимосвязи основных поня-тий, изучаемых в дисциплине /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
	Раздел 2. Стандартизация систем и процессов управления информа-ционной безопасностью					
2.1	/Тема/	9	0			
2.2	Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Стандарты на отдельные процессы управлении ИБ и оценку без-опасности ИТ: ISO/IEC 13335 - методы и средства обеспечения безопасности информационных технологий, ISO/IEC 15408 и ISO/IEC 18045 - Общие критерии и методология оценки безопас-ности информационных технологий, ISO 19011:2018 и ГОСТ Р ИСО 19011-2012 - Рекомендации по аудиту систем менеджмента, BS 25999 и ГОСТ Р 53647 - Управление непрерывностью бизнеса. Законы о Банке Росии - Федеральный закон от 10 июля 2002 г. N 86-ФЗ "О Центральном банке Российской Федерации (Банке Рос-сии)" и Федеральный закон от 27 июня 2011 г. N 161-ФЗ «О национальной платежной системе». ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базо-вый состав организационных и технических мер (уровни защиты). ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия (оценка соответствия уровней защиты). Отраслевые стандарты в области управления ИБ - стандарты Бан-ка России, рекомендации Банка России и положения Банка Рос-сии по защите информации. /Лек/	9	6	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.

2.3	Изучение конспекта лекций /Ср/	9	9	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
2.4	Анализ основных руководящих документов по управлению ИБ /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
2.5	Анализ основных руководящих документов Банка России по защите информации /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
	Раздел 3. Политика информационной безопасности					
3.1	/Тема/	9	0			

3.2	Понятия политики обеспечения ИБ и политики ИБ организации. Причины выработки политики ИБ. Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ. Содержание политики ИБ: содержание корпоративной политики ИБ, содержание частных политик ИБ, примеры частных политик ИБ. Жизненный цикл политики ИБ: разработка политики ИБ, внедре-ние политики ИБ, применение политики ИБ, аннулирование по-литики ИБ, ответственность за исполнение политики ИБ. /Лек/	9	4	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
3.3	Изучение конспекта лекций /Ср/	9	9	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
3.4	Составление списка активов организации и выбор средств их защиты. /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.

3.5	Изучение требований к разработке модели угроз информационной безопасности автоматизированной системы в защищенном исполнении (АСЗИ). /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.6	Изучение требований к разработке модели нарушителей информационной безопасности автоматизированной системы в защищенном исполнении (АСЗИ). /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.7	Разработка политик информационной безопасности организации. /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
	Раздел 4. Управление и система управления информационной безопасностью					
4.1	/Тема/	9	0			

4.2	Необходимость управления обеспечением ИБ организации. Дея-тельность по обеспечению ИБ организации как процесс. Опреде-ление управления ИБ организации. Управление ИБ информаци-онно-телекоммуникационных технологий организации. Система управления ИБ организации: область действия СУИБ, документальное обеспечение СУИБ, политика СУИБ, поддержка СУИБ со стороны руководства организации. Процессный подход в рамках управления ИБ: планирование СУ-ИБ, реализация СУИБ, проверка СУИБ, совершенствование СУ-ИБ. Работа с процессами СУИБ организации: задание процесса СУ-ИБ, идентификация процессов СУИБ организации, документиро-вание и описание процесса СУИБ, мониторинг и измерение пара-метров процесса СУИБ. Стратегии построении и внедрения СУИБ: построение и внедре-ние СУИБ в целом, построение и внедрение процессов СУИБ по отдельности. /Лек/	9	4	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
4.3	Изучение конспекта лекций /Ср/	9	9	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
4.4	Изучение основных компонентов СУИБ /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.

4.5	Этапы разработки и внедрения системы управления ИБ. Содержание этапов разработ-ки и внедрения системы управления ИБ. /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
	Раздел 5. Оценка и управление рисками информационной безопасности					
5.1	/Тема/	9	0			
5.2	Основные определения. Нормативное обеспечение управления рисками информационной безопасности. Оценка рисков информационной безопасности. Обработка рисков информационной безопасности. Принятие и мониторинг рисков информационной безопасности. Обеспечение управления рисками информационной безопасно-сти. /Лек/	9	6	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
5.3	Изучение конспекта лекций /Ср/	9	9	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).

5.4	Основные подходы и методы оценки инфор-мационных рисков на предприятии. Метод оценки рисков на основе модели информаци-онных потоков. /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
5.5	Расчет рисков по угрозе конфиденциально-сти. Расчет рисков по угрозе целостности. Табличные методы оценки рисков. Оценка рисков по двум факторам. Разделение рисков на приемлемые и неприемлемые. /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
	Раздел 6. Управление инцидентами ИБ и обеспечение непрерывности бизнеса					
6.1	/Тема/	9	0			
6.2	Нормативная база управления инцидентами ИБ и обеспечение непрерывности бизнеса. Стандарт ISO 27035. Идентификация, протоколирование, реагирование на инциденты ИБ. Влияние ин-цидентов ИБ на бизнес-процессы. Средства управления событиями ИБ. SOC-центры ИБ, SIEM-системы управления информацией о безопасности и событиями информационной безопасности, IRP-системы автоматизации реа-гирования на инциденты информационной безопасности Управление непрерывностью бизнеса организации. /Лек/	9	6	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.

6.3	Изучение конспекта лекций /Ср/	9	9	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
6.4	Изучение подходов к управлению инциден-тами информационной безопасности на пред-приятии /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
6.5	Изучение систем и средств управления инци-дентами информационной безопасности на предприятии /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.

6.6	Изучение принципов и средств управления непрерывностью бизнеса организации /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
	Раздел 7. Процессы проверки системы управления ИБ и оценка деятельности по управлению ИБ					
7.1	/Тема/	9	0			
7.2	Нормативное обеспечение проверки и оценки деятельности по управлению информационной безопасностью. Аудит СУИБ. Процесс аудита. Внутренний и внешний аудит. Аудит первой, второй и третьей сторонами. Подготовка к выпол-нению аудита. Подготовка и представление отчетов в устной и письменной форме о результатах аудита. Принятие решений о необходимости соответствующих последующих аудиторских проверок. Оценка деятельности по управлению информационной безопас-ностью. /Лек/	9	4	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
7.3	Изучение конспекта лекций /Ср/	9	8	ОПК-5.7-З ОПК-5.7-У ОПК-5.8-З ОПК-5.8-У ОПК-6.5-З ОПК-6.5-У ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.2-З ОПК-15.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).

7.4	Изучение методов и средств оценки деятельности предприятия по управлению ИБ /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
7.5	Изучение примера оценки деятельности предприятия по управлению ИБ /Пр/	9	2	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
7.6	Сдача (прием) зачета /ИКР/	9	0,25	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Ответы на Контрольные вопросы Результаты решения задач. Ответы на дополнительные вопросы. Результаты тестирования.

7.7	Подготовка к зачету /ЗаО/	9	17,75	ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Задачи к зачету. Билеты к зачету. Тесты к зачету.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы по данной дисциплине приведены в приложении к рабочей про-грамме дисциплины (см. документ «Оценочные материалы по дисциплине «Управление ин-формационной безопасностью»).

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.1	Пелешенко В. С., Говорова С. В., Лапина М. А.	Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие	Ставрополь: Северо-Кавказский федеральный университет, 2017, 86 с.	2227-8397, http://www.iprbookshop.ru/69405.html
Л1.2	Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.	Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1	Москва: Горячая линия-Телеком, 2012, 244 с.	978-5-9912-0271-8, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5178
Л1.3	Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.	Серия «Вопросы управление информационной безопасностью". Выпуск 2	Москва: Горячая линия-Телеком, 2012, 130 с.	978-5-9912-0272-5, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5179
Л1.4	Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.	Серия «Вопросы управление информационной безопасностью". Выпуск 3	Москва: Горячая линия-Телеком, 2013, 170 с.	978-5-9912-0273-2, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5180

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.5	Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.	Серия «Вопросы управление информационной безопасностью". Выпуск 4	Москва: Горячая линия-Телеком, 2012, 214 с.	978-5-9912-0274-9, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5181
Л1.6	Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.	Серия «Вопросы управление информационной безопасностью". Выпуск 5	Москва: Горячая линия-Телеком, 2012, 166 с.	978-5-9912-0275-6, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5182
Л1.7	Капгер И. В., Шабуров А. С.	Управление информационной безопасностью : учебное пособие	Пермь: ПНИПУ, 2023, 91 с.	978-5-398-02866-9, https://e.lanbook.com/book/328889

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Сычев Ю. Н.	Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие	Саратов: Вузовское образование, 2018, 195 с.	978-5-4487-0128-3, http://www.iprbookshop.ru/72345.html

6.1.3. Методические разработки

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	Лапина М. А., Марков Д. М., Гиш Т. А., Песков М. В., Меденец В. В.	Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум	Ставрополь: Северо-Кавказский федеральный университет, 2016, 242 с.	2227-8397, http://www.iprbookshop.ru/62945.html

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	1. Электронно-библиотечная система «Лань». – Режим доступа: доступ из корпоративной се-ти РГРТУ – свободный (без пароля). URL: https://e.lanbook.com/
Э2	2. Электронно-библиотечная система «IPRbooks». – Режим доступа: доступ из корпоратив-ной сети РГРТУ – свободный (без пароля), доступ из сети Интернет - по паролю. URL: https://iprbookshop.ru/
Э3	3. Электронная библиотека РГРТУ. URL: http://elib.rsreu.ru/ . Режим доступа: из корпоратив-ной сети РГРТУ – по паролю
Э4	4. Научная электронная библиотека eLibrary. URL: http//e.lib/vlsu.ru/www.uisrussia.msu.ru/elibrary.ru
Э5	5. Библиотека и форум по программированию. URL: http://www.cyberforum.ru
Э6	6. Национальный открытый университет ИНТУИТ. URL: http://www.intuit.ru/

6.3 Перечень программного обеспечения и информационных справочных систем

6.3.1 Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование	Описание
Операционная система Windows	Коммерческая лицензия
Kaspersky Endpoint Security	Коммерческая лицензия
Adobe Acrobat Reader	Свободное ПО
VM VirtualBox	Свободно распространяемое программное обеспечение под лицензиями
LibreOffice	Свободное ПО

6.3.2 Перечень информационных справочных систем	
6.3.2.1	Система КонсультантПлюс http://www.consultant.ru
7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1	270 учебно-административный корпус. учебная аудитория для проведения учебных занятий. Специализированная мебель (42 посадочных места), магнитно-маркерная доска. Мультимедиа проектор, 1 экран. Рабочее место (2 стола), 1 персональный компьютер, 1 ноутбук.
2	268 учебно-административный корпус. компьютерный класс для проведения учебных занятий Специализированная мебель (20 компьютерных столов), 20 персональных компьютеров. Возможность подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ.
8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)	
Методические материалы по данной дисциплине приведены в Приложении 2 к рабочей про-грамме дисциплины (см. документ «Методическое обеспечение дисциплины «Управление информа-ционной безопасностью»).	

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДПИСАНО ЗАВЕДУЮЩИМ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**15.09.24** 17:57 (MSK)	Простая подпись
ПОДПИСАНО ЗАВЕДУЮЩИМ ВЫПУСКАЮЩЕЙ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**15.09.24** 17:57 (MSK)	Простая подпись
ПОДПИСАНО НАЧАЛЬНИКОМ УРОП	**ФГБОУ ВО "РГРТУ", РГРТУ,** Ерзылёва Анна Александровна, Начальник УРОП	**17.09.24** 09:58 (MSK)	Простая подпись