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
Проректор по УР

А.В. Корячко

Защита информации специальных организационно-технических объектов

рабочая программа дисциплины (модуля)

Закреплена за кафедрой	**Электронные вычислительные машины**
Учебный план	27.05.01_22_00.plx 27.05.01 Специальные организационно-технические системы
Квалификация	**Инженер-системотехник**
Форма обучения	**очная**
Общая трудоемкость	**5 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		**8 (4.2)**		Итого	
Недель	16		16			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	16	16	16	16	32	32
Лабораторные	16	16			16	16
Практические			16	16	16	16
Иная контактная работа	0,25	0,25	0,35	0,35	0,6	0,6
Консультирование перед экзаменом и практикой			2	2	2	2
Итого ауд.	32,25	32,25	34,35	34,35	66,6	66,6
Контактная работа	32,25	32,25	34,35	34,35	66,6	66,6
Сам. работа	31	31	47	47	78	78
Часы на контроль	8,75	8,75	26,65	26,65	35,4	35,4
Итого	72	72	108	108	180	180

г. Рязань

Программу составил(и):
к.т.н., доц., Бабаев Сергей Игоревич

Рабочая программа дисциплины
Защита информации специальных организационно-технических объектов

разработана в соответствии с ФГОС ВО:
ФГОС ВО - специалитет по специальности 27.05.01 Специальные организационно-технические системы (приказ Минобрнауки России от 12.08.2020 г. № 951)

составлена на основании учебного плана:
27.05.01 Специальные организационно-технические системы
утвержденного учёным советом вуза от 28.01.2022 протокол № 6.

Рабочая программа одобрена на заседании кафедры
Электронные вычислительные машины

Протокол от 02.06.2022 г. № 11
Срок действия программы: уч.г.
Зав. кафедрой Костров Борис Васильевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
Электронные вычислительные машины

Протокол от __ _____ 2023 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры
Электронные вычислительные машины

Протокол от __ _____ 2024 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Электронные вычислительные машины

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

Электронные вычислительные машины

Протокол от __ _____ 2026 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью освоения дисциплины является формирование у обучающихся твердых теоретических знаний и практических навыков в части защиты информации, обрабатываемой в специальных организационно-технических системах.
1.2	Основные задачи освоения учебной дисциплины:
1.3	- усвоение знаний об основных механизмах, методах и средствах защиты информации;
1.4	- усвоение знаний об основных типах угроз информационной безопасности, характерных для современных информационных систем;
1.5	- усвоение знаний о требованиях законодательства РФ по защите информации в информационных системах;
1.6	- усвоение и закрепление практических навыков и умений по применению основных методов и средств защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Базы данных специальных организационно-технических систем
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-2: Способен осуществлять инсталляцию, сопровождение и работу с СУБД с учетом регламентов обеспечения информационной безопасности

ПК-2.1. Выполняет инсталляцию и первоначальную настройку СУБД

Знать
способы оценки и прогнозирования требований к информационной системе, в том числе с точки зрения информационной безопасности
Уметь
прогнозировать и оценивать требования информационной безопасности к информационным системам
Владеть
навыками прогнозирования и оценки требований к коммуникационной системы с точки зрения соблюдения требований информационной безопасности

ПК-2.3. Обеспечивает соблюдение требований регламентов информационной безопасности

Знать
основные требования информационной безопасности, предъявляемые к информационно-коммуникационным системам
Уметь
применять на практике методы и подходы по защите информации
Владеть
практическими навыками разработки дизайна информационно-коммуникационных систем с учетом требований информационной безопасности

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	нормативные правовые акты по защите информации.
3.2	**Уметь:**
3.2.1	применять на практике требования законодательства РФ по защите информации.
3.3	**Владеть:**
3.3.1	навыками работы с программными, техническими и программно-техническими средствами /

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Форма контроля
	Раздел 1. Защита информации, ее составляющие и виды					
1.1	Защита информации, ее составляющие и виды /Тема/	7	0			Беседа по материалу

1.2	Защита информации как деятельность. Виды защиты информации. Информационная безопасность и компьютеризация информационной среды. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг /Лек/	7	4		Л1.1 Л1.2Л2.1 Л2.2 Л2.3	Беседа по материалу лекционных занятий
1.3	Виды защищаемой информации. Классификация и виды тайны /Лаб/	7	2			Сдача и защита лабораторной работы
1.4	Определение видов защищаемой информации на объекте защиты /Лаб/	7	2			Сдача и защита лабораторной работы
1.5	Изучение методических указаний к лабораторным работам /Ср/	7	2			Устный опрос по самостоятельно изученному материалу
1.6	Изучение литературы. Изучение конспекта лекций. Изучение документов по категориям защищаемой информации /Ср/	7	7		Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4	Устный опрос по самостоятельно изученному материалу
	Раздел 2. Цели и направления защиты информации					
2.1	Цели и направления защиты информации /Тема/	7	0			Беседа по материалу
2.2	Цели защиты информации. Направления защиты информации. Защита информации от утечки. Защита информации от несанкционированного воздействия. Защита информации от непреднамеренного воздействия. /Лек/	7	8		Л1.1 Л1.2Л2.1 Л2.2 Л2.3	Беседа по материалу лекционных занятий
2.3	Направления защиты информации (утрата и утечка, «КЦД») /Лаб/	7	2			Сдача и защита лабораторной работы
2.4	Основные способы защиты информации от НСД /Лаб/	7	2			Сдача и защита лабораторной работы
2.5	Изучение методических указаний к лабораторным работам /Ср/	7	2			Устный опрос по самостоятельно изученному материалу
2.6	Изучение литературы. Изучение конспекта лекций. Защита от непреднамеренных воздействий и не декларированные возможности ПО /Ср/	7	8		Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4	Устный опрос по самостоятельно изученному материалу
	Раздел 3. Объекты защиты информации					
3.1	Объекты защиты информации /Тема/	8	0			Беседа по материалу

3.2	Определение понятия объект защиты информации. Информация как объект защиты. Сущность и определение понятия информация как объекта защиты. Свойства информации как объективного явления. Информация как объект правовых отношений. Носитель информации как объект защиты. Определение понятия носитель информации и классификация носителей информации. /Лек/	7	4		Л1.1 Л1.2Л2.1 Л2.2 Л2.3	Беседа по материалу лекционных занятий
3.3	Виды объектов защиты. Подходы к защите информации на различных видах ОЗ /Лаб/	7	4			Сдача и защита лабораторной работы
3.4	АС как объект ЗИ /Лаб/	7	4			Сдача и защита лабораторной работы
3.5	Изучение методических указаний к лабораторным работам /Ср/	7	4			Устный опрос по самостоятельно изученному материалу
3.6	Изучение литературы. Изучение конспекта лекций. Руководящие документы ФСТЭК, ФСБ в области ЗИ на ОЗ /Ср/	7	8		Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4	Устный опрос по самостоятельно изученному материалу
3.7	Документированная информация и информационные ресурсы. Информационный процесс как объект защиты. Информационный процесс и информационная технология. Информационная система как средство реализации информационного процесса и комплексный объект защиты информации. Автоматизированная система как комплексный объект защиты информации. Определение понятия автоматизированная система. Классификация автоматизированных систем. /Лек/	8	4		Л1.1 Л1.2Л2.1 Л2.2 Л2.3	Беседа по материалу лекционных занятий
	Раздел 4. Промежуточная аттестация					
4.1	Промежуточная аттестация /Тема/	7	0			
4.2	Иная контактная работа /ИКР/	7	0,25			Беседа
4.3	Зачет /Зачёт/	7	8,75			Подготовка к зачету
	Раздел 5. Условия, в которых осуществляется защита информации					
5.1	Условия, в которых осуществляется защита информации /Тема/	8	0			
5.2	Явления, действия, процессы, объекты и субъекты, характеризующие условия защиты информации. Вредоносные воздействия на объекты информационной инфраструктуры и угрозы безопасности информации. Нарушители безопасности информации. /Лек/	8	4		Л1.1 Л1.2Л2.1 Л2.2 Л2.3	Беседа по материалу лекционных занятий
5.3	Вредоносные воздействия и их идентификация /Пр/	8	4			Сдача и защита материалов практического занятия

5.4	Уязвимости ПО и ОС /Пр/	8	4			Сдача и защита материалов практического занятия
5.5	Изучение методических указаний к лабораторным работам /Ср/	8	12			Устный опрос по самостоятельно изученному материалу
5.6	Изучение литературы. Изучение конспекта лекций. Изучение номенклатуры вредоносных воздействий и уязвимостей ОС /Ср/	8	12		Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4	Устный опрос по самостоятельно изученному материалу
	Раздел 6. Системы защиты информации для распространенных информационных систем					
6.1	Системы защиты информации для распространенных информационных систем /Тема/	8	0			Беседа по материалу
6.2	Обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов. Архитектура системы безопасности операционных систем. Механизм контроля доступа. Система защиты информации Secret Net. /Лек/	8	8		Л1.1 Л1.2Л2.1 Л2.2 Л2.3	Беседа по материалу лекционных занятий
6.3	Основные СЗИ от НСД /Пр/	8	4			Сдача и защита материалов практического занятия
6.4	Secret net /Пр/	8	4			Сдача и защита материалов практического занятия
6.5	Изучение методических указаний к лабораторным работам /Ср/	8	11			Устный опрос по самостоятельно изученному материалу
6.6	Изучение литературы. Изучение конспекта лекций. СЗИ от ПЭМИН /Ср/	8	12		Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4	Устный опрос по самостоятельно изученному материалу
	Раздел 7. Промежуточная аттестация					
7.1	Промежуточная аттестация /Тема/	8	0			
7.2	Иная контактная работа /ИКР/	8	0,35			Беседа
7.3	Консультации /Кнс/	8	2			Беседа
7.4	Экзамен /Экзамен/	8	26,65			Подготовка к сдаче экзамена

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Защита информации специальных организационно-технических объектов»).

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	Петров С. В., Кисляков П. А.	Информационная безопасность : учебное пособие	Саратов: Ай Пи Ар Букс, 2015, 326 с.	978-5-906-17271-6, http://www.iprbookshop.ru/33857.html
Л1.2	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019, 702 с.	978-5-4488-0070-2, http://www.iprbookshop.ru/87995.html

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Лапина М. А., Ревин А. Г., Лапин В. И., Килясханов И. Ш.	Информационное право : учебное пособие для студентов вузов, обучающихся по специальности 021100 «юриспруденция»	Москва: ЮНИТИ-ДАНА, 2017, 335 с.	5-238-00798-1, http://www.iprbookshop.ru/74890.html
Л2.2	Кияев В. И., Граничин О. Н.	Безопасность информационных систем	Москва: ИНТУИТ, 2016, 191 с.	, https://e.lanbook.com/book/100580
Л2.3	Хаулет, Т., Галатенко, В., Труфанова, О., Галатенко, В.	Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям : учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020, 607 с.	978-5-4497-0658-4, http://www.iprbookshop.ru/97544.html

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Электронно-библиотечная система «IPRbooks» [Электронный ресурс]. – Режим доступа: доступ из корпоративной сети РГРТУ – свободный, доступ из сети Интернет – по паролю. – URL: https://iprbookshop.ru/
Э2	Электронно-библиотечная система «Лань», режим доступа – с любого компьютера РГРТУ без пароля, из сети интернет по паролю. – URL: https://e.lanbook.com/
Э3	Электронная библиотека РГРТУ [Электронный ресурс]. – Режим доступа: из корпоративной сети РГРТУ – по паролю. – URL: https://elib.rsreu.ru/
Э4	Соколов, М. С. Информация как объект информационной безопасности [Электронный ресурс] / М.С. Соколов // Закон и право. – 2013. – № 12. – С. 27-33. – Режим доступа : http://elibrary.ru/item.asp?id=20780302

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
Apache OpenOffice	Свободный пакет офисных приложений. Лицензия Apache License 2.0
Операционная система Windows XP/Vista/7/8/10	Microsoft Imagine: Номер подписки 700102019, бессрочно
Microsoft SQL Server	Microsoft Imagine: Номер подписки 700102019, бессрочно
Kaspersky Endpoint Security	Коммерческая лицензия

6.3.2 Перечень информационных справочных систем

6.3.2.1	Информационно-правовой портал ГАРАНТ.РУ http://www.garant.ru
6.3.2.2	Система КонсультантПлюс http://www.consultant.ru

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1	122 учебно-административный корпус. Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, лабораторных работ, практических и самостоятельных занятий 10 компьютеров (CPU AMD Phenom II X4 955, 4 ГБ ОЗУ) (компьютерный класс) с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду РГРТУ, 56 мест, мультимедиа проектор, интерактивная доска, компьютер, специализированная мебель, доска
2	502 лабораторный корпус. Учебная аудитория для проведения учебных занятий Специализированная мебель (37 посадочных мест) ПК: Intel Celeron CPVJ1800 – 25 шт. Возможность подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ
3	503 лабораторный корпус. Учебная аудитория для проведения учебных занятий Специализированная мебель (37 посадочных мест) ПК: Intel Celeron CPVJ1800 – 25 шт. Возможность подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Методическое обеспечение дисциплины приведено в приложении к рабочей программе дисциплины (см. документ «Методические указания дисциплины «Защита информации специальных организационно-технических объектов»).