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

Информационная безопасность компьютерных систем объектов информатизации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационной безопасности**

Учебный план 10.05.01 _21_00.plx
10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Квалификация **специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	40	40	40	40
Практические	24	24	24	24
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	35	35	35	35
Часы на контроль	8,75	8,75	8,75	8,75
Итого	108	108	108	108

г. Рязань

Программу составил(и):
ст. преп., Колесенков Николай Александрович

Рабочая программа дисциплины
Информационная безопасность компьютерных систем объектов информатизации

разработана в соответствии с ФГОС ВО:
ФГОС ВО - специалитет по специальности 10.05.01 Компьютерная безопасность (приказ Минобрнауки России от 26.11.2020 г. № 1459)

составлена на основании учебного плана:
10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
утвержденного учёным советом вуза от 28.01.2022 протокол № 6.

Рабочая программа одобрена на заседании кафедры
Информационной безопасности

Протокол от 29.06.2022 г. № 12
Срок действия программы: 2021-2027 уч.г.
Зав. кафедрой Пржегорлинский Виктор Николаевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
Информационной безопасности

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
Информационной безопасности

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
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 _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	изучение основных понятий в области угроз безопасности информации компьютерных систем, формирование у будущих специалистов твердых теоретических знаний и практических навыков в части анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации компьютерных систем в защищенном исполнении.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Спецдисциплина 3
2.1.2	Государственные стандарты по защите информации
2.1.3	Нормативное обеспечение информационной безопасности компьютерных систем
2.1.4	Управление информационной безопасностью
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	Проектирование защищенных компьютерных сетей
2.2.2	Защита государственной тайны в Российской Федерации
2.2.3	Практика по получению профессиональных умений и опыта профессиональной деятельности
2.2.4	Производственная практика
2.2.5	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
2.2.6	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-5.5. Контролирует работы по выполнению режима защиты информации, в том числе ограниченного доступа

Знать
нормативные и методические документы по выполнению режима защиты информации, в том числе ограниченного доступа.
Уметь
контролировать выполнения режима защиты информации, в том числе ограниченного доступа.
Владеть
способами организации контроля защиты информации на объекте.

ОПК-5.1: Способен обосновывать необходимость, организовывать и проводить подготовительные работы по созданию систем защиты информации компьютерных систем объектов информатизации;

ОПК-5.1.1. Определяет угрозы информационной безопасности процесса создания систем защиты информации компьютерных систем объектов информатизации

Знать
потенциальные угрозы безопасности информации в компьютерных системах.
Уметь
определять средства и способы защиты от угроз безопасности информации в компьютерных системах.
Владеть
навыками определения средств и способов защиты от угроз безопасности информации в компьютерных системах.

ОПК-5.1.2. Разрабатывает требования к системе защиты информации при создании систем защиты информации компьютерных систем объектов информатизации

Знать
требования к системе защиты информации компьютерных систем.
Уметь
проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации компьютерных систем.
Владеть
навыками разработки требований к системе защиты информации компьютерных систем объектов информатизации.

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	потенциальные угрозы безопасности информации в компьютерных системах.
3.2	**Уметь:**

3.2.1	определять средства и способы защиты от угроз безопасности информации в автоматизированных системах.
3.3	**Владеть:**
3.3.1	разработки требований к системе защиты информации компьютерных систем объектов информатизации.

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. Состав и содержание угроз безопасности информации в компьютерных системах.					
1.1	Введение. Состав и содержание угроз безопасности информации в компьютерных системах. /Тема/	8	0			
1.2	Лекция 1. Введение. Термины и определения. Общая классификация угроз безопасности информации в компьютерных системах. Лекция 2. Классификация угроз безопасности информации компьютерных систем по виду защищаемой информации. Лекция 3. Классификация угроз безопасности информации компьютерных систем по видам возможных источников угроз безопасности. Лекция 4. Классификация угроз безопасности информации компьютерных систем по способам реализации угроз безопасности. /Лек/	8	8	ОПК-5.1.1-З ОПК-5.5-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Вопросы
1.3	Практическое занятие 1. Изучение классификации угроз безопасности информации компьютерных систем по виду защищаемой информации. Практическое занятие 2. Рассмотрение возможных источников и способов реализации угроз безопасности информации, обрабатываемой в компьютерных системах. /Пр/	8	4	ОПК-5.1.1-З ОПК-5.1.1-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Вопросы
1.4	Изучение конспекта лекций. Подготовка к практическим занятиям. /Ср/	8	12	ОПК-5.1.1-З ОПК-5.5-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Вопросы
	Раздел 2. Виды угроз безопасности информации в компьютерных системах.					
2.1	Виды угроз безопасности информации в компьютерных системах. /Тема/	8	0			

2.2	Лекция 1. Угрозы несанкционированного доступа к информации в компьютерных системах. Лекция 2. Общая характеристика источников угроз несанкционированного доступа в компьютерных системах. Лекция 3. Угрозы непосредственного доступа в операционную среду компьютерных систем. Лекция 4. Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия. Лекция 5. Угрозы программно-математических воздействий. Лекция 6. Угрозы утечки информации по нетрадиционным информационным каналам. Лекция 7. Общая характеристика результатов несанкционированного или случайного доступа к ресурсам компьютерных систем. Лекция 8. Угрозы утечки информации по техническим каналам. Лекция 9. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок. /Лек/	8	18	ОПК-5.1.1-З ОПК-5.1.2-У ОПК-5.5-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Вопросы
2.3	Практическое занятие 1. Анализ угроз несанкционированного доступа к информации компьютерных систем. Практическое занятие 2. Изучение угроз программно-математических воздействий. Практическое занятие 3. Изучение угроз утечки информации по техническим каналам. Практическое занятие 4. Электромагнитные и электрические каналы утечки информации. Практическое занятие 5. Общая характеристика уязвимостей компьютерных систем. Практическое занятие 6. Уязвимости компьютерных систем. /Пр/	8	12	ОПК-5.1.1-З ОПК-5.1.2-У ОПК-5.5-З ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Вопросы
2.4	Изучение конспекта лекций. Подготовка к практическим занятиям. /Ср/	8	10	ОПК-5.1.1-З ОПК-5.1.2-У ОПК-5.5-З ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Вопросы
	Раздел 3. Методы и средства обеспечения безопасности компьютерных систем в защищенном исполнении.					
3.1	Методы и средства обеспечения безопасности компьютерных систем в защищенном исполнении. /Тема/	8	0			
3.2	Лекция 1. Компьютерные системы в защищенном исполнении. Система защиты информации компьютерных систем. Лекция 2.Требования обеспечения информационной безопасности компьютерных систем. Лекция 3. Меры обеспечения информационной безопасности создания компьютерных систем в защищенном исполнении. Лекция 4. Оценка информационной безопасности компьютерных систем. Лекция 5. Обеспечение безопасности компьютерных систем. Методы и средства обеспечения безопасности. /Лек/	8	10	ОПК-5.1.1-У ОПК-5.1.1-В ОПК-5.1.2-З ОПК-5.1.2-У ОПК-5.1.2-В ОПК-5.5-З ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Вопросы

3.3	Практическое занятие 1. Требования обеспечения информационной безопасности компьютерных систем. Практическое занятие 2. Меры обеспечения информационной безопасности создания компьютерных систем в защищенном исполнении. Практическое занятие 3. Требования к техническим средствам защиты компьютерных систем в защищенном исполнении. /Пр/	8	6	ОПК-5.1.1-У ОПК-5.1.1-В ОПК-5.1.2-З ОПК-5.1.2-У ОПК-5.1.2-В ОПК-5.5-З ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Вопросы
3.4	Изучение конспекта лекций. Подготовка к практическим занятиям. /Ср/	8	8	ОПК-5.1.1-У ОПК-5.1.2-З ОПК -5.1.2-У ОПК-5.5-З ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Вопросы
	Раздел 4. Нарушители безопасности информации в компьютерных системах.					
4.1	Нарушители безопасности информации в компьютерных системах. /Тема/	8	0			
4.2	Лекция 1. Модель нарушителя безопасности информации в компьютерных системах. Лекция 2. Модель угроз безопасности информации в компьютерных системах. /Лек/	8	4	ОПК-5.1.1-З ОПК-5.1.1-У ОПК-5.1.2-У ОПК-5.5-З ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Вопросы
4.3	Упражнение 1. Нарушители безопасности информации в компьютерных системах. /Пр/	8	2	ОПК-5.1.1-З ОПК-5.1.1-У ОПК-5.1.1-В ОПК-5.1.2-З ОПК-5.1.2-У ОПК-5.1.2-В ОПК-5.5-З ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Вопросы
4.4	Изучение конспекта лекций. Подготовка к практическим занятиям. /Ср/	8	5	ОПК-5.1.1-З ОПК-5.1.1-У ОПК-5.1.1-В ОПК-5.1.2-У ОПК-5.5- З ОПК-5.5- У ОПК-5.5- В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	Вопросы
	Раздел 5. Контроль.					
5.1	Контроль. /Тема/	8	0			

5.2	Зачет с оценкой. /ЗаО/	8	8,75	ОПК-5.1.1-З ОПК-5.1.1-У ОПК-5.1.1-В ОПК-5.1.2-З ОПК-5.1.2-У ОПК-5.1.2-В ОПК-5.5-З ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Вопросы
5.3	Иная контактная работа. /ИКР/	8	0,25	ОПК-5.1.1-З ОПК-5.1.1-В ОПК-5.1.2-З ОПК -5.1.2-У ОПК-5.1.2-В ОПК-5.5- З ОПК-5.5- У ОПК-5.5- В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Вопросы

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине "Информационная безопасность компьютерных систем объектов информатизации".

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	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019, 702 с.	978-5-4488-0070-2, http://www.iprbookshop.ru/87995.html
Л1.2	Кияев В. И., Граничин О. Н.	Безопасность информационных систем	Москва: ИНТУИТ, 2016, 191 с.	, https://e.lanbook.com/book/100580

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Шаньгин В. Ф.	Защита компьютерной информации. Эффективные методы и средства	Саратов: Профобразование, 2019, 543 с.	978-5-4488-0074-0, http://www.iprbookshop.ru/87992.html
Л2.2	Гультяева Т. А.	Основы защиты информации : учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2018, 83 с.	978-5-7782-3641-7, http://www.iprbookshop.ru/91638.html

6.1.3. Методические разработки

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	Пржегорлинский В.Н.	Объекты защиты информации. Ч.2 Комплексные объекты защиты информации : Учебное пособие	Рязань: РИЦ РГРТУ, 2014,	, https://elib.rsreu.ru/ebs/download/937
Л3.2	Пржегорлинский В.Н.	Объекты защиты информации. Ч.1. Элементарные объекты защиты информации : Учебное пособие	Рязань: РИЦ РГРТУ, 2012,	, https://elib.rsreu.ru/ebs/download/938

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. 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
LibreOffice	Свободное ПО

6.3.2 Перечень информационных справочных систем

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1	264 учебно-административный корпус. учебная аудитория для проведения учебных занятий Специализированная мебель (16 посадочных мест), 5 рабочих мест (стол), магнитно-маркерная доска.
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)

Методическое обеспечение дисциплины приведено в приложении к рабочей программе дисциплины (см. документ «Методические указания дисциплины "Информационная безопасность компьютерных систем объектов информатизации".