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

Модели угроз и нарушителей безопасности информации объектов информатизации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационная безопасность**

Учебный план 10.05.01 _20_00.plx
10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Квалификация **специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Иная контактная работа	0,55	0,55	0,55	0,55
Итого ауд.	64,55	64,55	64,55	64,55
Контактная работа	64,55	64,55	64,55	64,55
Сам. работа	59	59	59	59
Часы на контроль	8,75	8,75	8,75	8,75
Письменная работа на курсе	11,7	11,7	11,7	11,7
Итого	144	144	144	144

г. Рязань

Программу составил(и):

к.т.н., доц., Конкин Юрий Валериевич

Рабочая программа дисциплины

Модели угроз и нарушителей безопасности информации 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

Информационная безопасность

Протокол от 29.06.2022 г. № 12
Срок действия программы: 2020-2026 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

Информационная безопасность

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

Информационная безопасность

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

Информационная безопасность

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

Информационная безопасность

Протокол от __ _____ 2026 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины «Модели угроз и нарушителей безопасности информации объектов информатизации» является теоретическая и практическая подготовка специалистов к деятельности, связанной с исследованием объектов информатизации на предмет выявления угроз и уязвимостей. Дисциплина обеспечивает приобретение знаний и умений в области обнаружения прогнозирования действий злоумышленников при их воздействии на объекты информатизации, способствует освоению принципов корректного применения современных средств защиты информации.
1.2	Задачи дисциплины:
1.3	- получение знаний об угрозах и нарушителях безопасности информации компьютерных систем;
1.4	- получение знаний о методах выявления и оценки актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Объекты защиты информации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная практика
2.2.2	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
2.2.3	Преддипломная практика

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

ПК-3: Способен оценивать уровень безопасности компьютерных систем и сетей

ПК-3.1. Разрабатывает требования по защите, формирование политик безопасности компьютерных систем и сетей

Знать
основы проведения научных исследований
Уметь
разрабатывать типовые нормативные документы по оценке угроз информационной безопасности компьютерных систем и их формальному представлению
Владеть
навыками администрирования компьютерных сетей, систем баз данных и ОС

ПК-3.2. Проводит анализ безопасности компьютерных систем

Знать
основы построения защищенных компьютерных сетей
Уметь
разрабатывать типовые нормативные акты по обеспечению информационной безопасности на предприятии
Владеть
навыками работы с нормативными документами по определению требований о защите информации компьютерных систем

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	основы законодательства РФ в области обеспечения информационной безопасности компьютерных систем
3.2	**Уметь:**
3.2.1	разрабатывать типовые модели угроз информационной безопасности
3.3	**Владеть:**
3.3.1	современными информационными технологиями работы над проектами

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					
1.1	Описание информационной системы и особенностей ее функционирования /Тема/	8	0			

1.2	Общие положения. Описание информационной системы и особенностей ее функционирования. Цель и задачи, решаемые информационной системой /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
1.3	Описание структурно-функциональных характеристик информационной системы. Описание технологии обработки информации /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
1.4	Описание информационной системы /Пр/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Устный опрос по теме. Решение задач. Проверка домашнего задания.
1.5	Изучение конспекта лекций. Изучение литературы /Ср/	8	10	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Подготовка конспекта по вопросам темы.
	Раздел 2. Модели нарушителей информационной безопасности					
2.1	Модели нарушителей информационной безопасности /Тема/	8	0			
2.2	Возможности нарушителей (модель нарушителя) /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
2.3	Типы и виды нарушителей /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
2.4	Возможные цели и потенциал нарушителей /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
2.5	Типовые модели нарушителей /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
2.6	Классификация угроз информационной безопасности объектов информатизации /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.

2.7	Типовые модели нарушителей ИБ ОИ на базе компьютерных систем /Пр/	8	8	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Устный опрос по теме. Решение задач. Проверка домашнего задания.
2.8	Изучение конспекта лекций. Изучение литературы. Классификация нарушителей информационной безопасности /Ср/	8	20	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Подготовка конспекта по вопросам темы.
	Раздел 3. Угрозы информационной безопасности и уязвимости объектов информатизации					
3.1	Угрозы информационной безопасности и уязвимости объектов информатизации /Тема/	8	0			
3.2	Угрозы и уязвимости /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
3.3	Возможные способы реализации угроз безопасности информации /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
3.4	Актуальные угрозы безопасности информации /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
3.5	Типовые модели угроз информационной безопасности. Часть 1. /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
3.6	Типовые модели угроз информационной безопасности. Часть 2. /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
3.7	Типовые модели угроз информационной безопасности Уязвимости объектов информатизации /Пр/	8	12	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.8	Изучение конспекта лекций. Изучение литературы. Методики определения угроз информационной безопасности /Ср/	8	9	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Подготовка конспекта по вопросам темы.
	Раздел 4. Анализ рисков реализации угроз информационной безопасности					
4.1	Анализ рисков реализации угроз информационной безопасности /Тема/	8	0			

4.2	Разработка модели угроз /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
4.3	Способы оценки рисков реализации угроз информационной безопасности /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
4.4	Методические рекомендации по оценке рисков реализации угроз информационной безопасности /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
4.5	Методика определения угроз безопасности информации в информационных системах /Лек/	8	2	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Конспект лекций.
4.6	Анализ актуальности реализации угроз информационной безопасности /Пр/	8	10	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Устный опрос по теме. Решение задач. Проверка домашнего задания.
4.7	Изучение конспекта лекций. Изучение литературы. Методики оценки рисков реализации угроз информационной безопасности /Ср/	8	20	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Подготовка конспекта по вопросам темы.
	Раздел 5.					
5.1	/Тема/	8	0			
5.2	Сдача зачета /ИКР/	8	0,55	ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Ответы на Контрольные вопросы. Результаты решения зачач. Ответы на дополнительны е вопросы. Результаты тестирования.
5.3	Подготовк к зачету /ЗаО/	8	8,75	ПК-3.1-З ПК-3.2-З ПК-3.2-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Задачи к зачету. Билеты к зачету. Тесты к зачету.

5.4	/КПКР/	8	11,7	ПК-3.1-З ПК-3.1-У ПК-3.1-В	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	Оценка качества подготовки ПЗ к КР. Оценка качества и полноты выполнения задания к КР.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Модели угроз и нарушителей безопасности информации 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	Пакин А. И.	Информационная безопасность информационных систем управления предприятием : учебное пособие по части курса	Москва: Московская государственна я академия водного транспорта, 2009, 41 с.	2227-8397, http://www.ipr bookshop.ru/4 6462.html
Л1.2	Фомина К.Ю., Кураксин В.А.	Методы и средства защиты информации : метод. указ. к лаб. работам	Рязань, 2018, 48с.; прил.	, 20

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Артемов А. В.	Информационная безопасность : курс лекций	Орел: Межрегиональ ная Академия безопасности и выживания (МАБИВ), 2014, 256 с.	2227-8397, http://www.ipr bookshop.ru/3 3430.html
Л2.2	Конкин Ю.В., Кузьмин Ю.М., Пржегорлинский В.Н.	Основы информационной безопасности : учеб. пособие	Рязань, 2021, 96с.	, 20

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.ipr bookshop.ru/6 2945.html

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Менеджмент в сфере информационной безопасности
Э2	Алексеев А.П. Многоуровневая защита информации

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
LibreOffice	Свободное ПО
Adobe Acrobat Reader	Свободное ПО
VirtualBox	Свободное ПО

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	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.
2	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.

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Методическое обеспечение дисциплины приведено в приложении к рабочей программе дисциплины (см. документ «Методические указания дисциплины «Модели угроз и нарушителей безопасности информации объектов информатизации»).