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

Модели безопасности компьютерных систем

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 **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	24	24	24	24
Практические	24	24	24	24
Иная контактная работа	0,25	0,25	0,25	0,25
Итого ауд.	48,25	48,25	48,25	48,25
Контактная работа	48,25	48,25	48,25	48,25
Сам. работа	51	51	51	51
Часы на контроль	8,75	8,75	8,75	8,75
Итого	108	108	108	108

г. Рязань

Программу составил(и):
к.ф.-м.н., доц., Ильин Михаил Евгеньевич

Рабочая программа дисциплины

Модели безопасности компьютерных систем

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	(1) Приобретение базовых знаний и умений в соответствии с Федеральным государственным образовательным стандартом.
1.2	(2) Формирование у студентов способности к логиче-скому мышлению, анализу и восприятию информации, воспитание математической культуры, посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС, в части представленных ниже знаний, умений и навыков.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Модели безопасности автоматизированных систем
2.1.2	Моделирование
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Обеспечение информационной безопасности создания и эксплуатации автоматизированных систем
2.2.2	Практика по получению профессиональных умений и опыта профессиональной деятельности
2.2.3	Производственная практика
2.2.4	Теория информации
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-8: Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах;

ОПК-8.1. Применяет методы научных исследований при формировании математических моделей безопасности компьютерных систем

Знать
методы научных исследований при формировании математических моделей безопасности компьютерных систем
Уметь
применять методы научных исследований при формировании математи-ческих моделей безопасности компьютерных систем
Владеть

ОПК-8.2. Обосновывает необходимость защиты информации в автоматизированных системах на основе научных исследований

Знать
обоснования необходимости защиты информации в автоматизированных системах на основе научных исследований
Уметь
обосновывать необходимость защиты информации в автоматизированных системах на основе научных исследований
Владеть
обоснованием необходимости защиты информации в автоматизированных системах на основе научных иссле-дований

ОПК-8.4. Участвует в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем

Знать
методы участия в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем
Уметь
участвовать в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем
Владеть
методами участия в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем

ОПК-8.10. Разрабатывает формальные модели политик безопасности компьютерных систем

Знать
методы разработки формальных моделей политик безопасности компьютерных систем
Уметь
разрабатывать формальные модели политик безопасности компьютерных систем
Владеть
методами разработки формальных моделей политик безопасности компьютерных систем

ОПК-8.11. Разрабатывает формальные модели управления доступом и информационными потоками в компьютерных системах
Знать формальные модели управления доступом и информационными потоками в компьютерных системах **Уметь** разрабатывать формальные модели управления доступом и информационными потоками в компьютерных системах **Владеть** методами разработки формальных моделей управления доступом и информационными потоками в компьютерных системах

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	методы научных исследований при формировании математических моделей безопасности компьютерных систем
3.1.2	обоснования необходимости защиты информации в автоматизированных системах на основе научных исследований
3.1.3	методы участия в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем
3.1.4	методы разработки формальных моделей политик безопасности компьютерных систем
3.1.5	формальные модели управления доступом и информационными потоками в компьютерных системах
3.2	**Уметь:**
3.2.1	применять методы научных исследований при формировании математических моделей безопасности компьютерных систем
3.2.2	обосновывать необходимость защиты информации в автоматизированных системах на основе научных исследований
3.2.3	участвовать в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем
3.2.4	разрабатывать формальные модели политик безопасности компьютерных систем
3.2.5	разрабатывать формальные модели управления доступом и информационными потоками в компьютерных системах
3.3	**Владеть:**
3.3.1	методами научных исследований при формировании математических моделей безопасности компьютерных систем
3.3.2	обоснованием необходимости защиты информации в автоматизированных системах на основе научных исследований
3.3.3	методами участия в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем
3.3.4	методами разработки формальных моделей политик безопасности компьютерных систем
3.3.5	методами разработки формальных моделей управления доступом и информационными потоками в компьютерных системах

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	Введение /Тема/	8	0			Проверка полноты и уровня усвоения компетенций темы

1.2	Сущность, субъект, доступ, информационный поток. Основная аксиома. Проблема построения защищенной КС Политика безопасности /Лек/	8	4	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.1 Л1.3Л2.7Л3.1 Э1 Э3	Проверка конспекта лекиций, опрос по то теме
1.3	Сущность, субъект, доступ, информационный поток. Основная аксиома. Проблема построения защищенной КС Политика безопасности /Пр/	8	2	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.1 Л1.3Л2.2 Л2.6Л3.1 Э1 Э3	Опрос по теме занятия, решение стандартных задач
1.4	Сущность, субъект, доступ, информационный поток. Основная аксиома. Проблема построения защищенной КС Политика безопасности /Ср/	8	11	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л2.1Л3.1 Э1 Э3	Работа с методическими материалами, конспектами лекций и практических занятий
	Раздел 2. Модели компьютерных систем с дискреционным управлением доступом					
2.1	Модели компьютерных систем с дискреционным управлением доступом /Тема/	8	0			Проверка полноты и уровня усвоения компетенций темы

2.2	Классическая модель распространения прав доступа Take-Grant. Де-юре правила преобразования графов доступов. Условия передачи прав доступа в графе доступов, состоящем только из субъектов. Остров, мост, пролеты моста /Лек/	8	5	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.1Л2.2Л3.1 Э1 Э3	Проверка конспекта лекиций, опрос по то теме
2.3	Классическая модель распространения прав доступа Take-Grant. Де-юре правила преобразования графов доступов. Условия передачи прав доступа в графе доступов, состоящем только из субъектов. Остров, мост, пролеты моста /Пр/	8	6	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.1Л2.3Л3.2 Э1 Э3	Опрос по теме занятия, решение стандартных задач
2.4	Классическая модель распространения прав доступа Take-Grant. Де-юре правила преобразования графов доступов. Условия передачи прав доступа в графе доступов, состоящем только из субъектов. Остров, мост, пролеты моста /Ср/	8	10	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.3Л2.2 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э3	Работа с методическими материалами, конспектами лекций и практических занятий
	Раздел 3. Модели компьютерных систем с мандатным управлением доступом.					
3.1	Модели компьютерных систем с дискреционным управлением доступом /Тема/	8	0			Проверка полноты и уровня усвоения компетенций темы

3.2	Классическая модель Белла-ЛаПадулы. Свойства безопасности. Безопасный доступ, состояние, система. Базовая теорема безопасности. Примеры реализации запрещенных информационных потоков. /Лек/	8	5	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.2Л2.2 Л2.4Л3.1 Э1 Э3	Проверка конспекта лекиций, опрос по то теме
3.3	Классическая модель Белла-ЛаПадулы. Свойства безопасности. Безопасный доступ, состояние, система. Базовая теорема безопасности. Примеры реализации запрещенных информационных потоков. /Пр/	8	6	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.2Л3.1 Э1 Э3	Опрос по теме занятия, решение стандартных задач
3.4	Классическая модель Белла-ЛаПадулы. Свойства безопасности. Безопасный доступ, состояние, система. Базовая теорема безопасности. Примеры реализации запрещенных информационных потоков. /Ср/	8	10	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.4Л2.3Л3.1 Э1 Э4	Работа с методическими материалами, конспектами лекций и практических занятий
	Раздел 4. Модели компьютерных систем с ролевым управлением доступом					
4.1	Модели компьютерных систем с дискреционным управлением доступом /Тема/	8	0			Проверка полноты и уровня усвоения компетенций темы

4.2	Модели компьютерных систем с ролевым управлением доступом /Лек/	8	5	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.1Л2.7Л3.2 Э1 Э3	Проверка конспекта лекиций, опрос по то теме
4.3	Понятие ролевого доступа. Ролевой доступ к управлению /Пр/	8	5	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.2Л3.2 Э1 Э3	Опрос по теме занятия, решение стандартных задач
4.4	Понятие ролевого доступа. Ролевой доступ к управлению /Ср/	8	10	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.4Л2.6 Э1 Э3	Работа с методическими материалами, конспектами лекций и практических занятий
	Раздел 5. Развитие формальных моделей безопасности компьютерных систем					
5.1	Развитие формальных моделей безопасности компьютерных систем /Тема/	8	0			Проверка полноты и уровня усвоения компетенций темы

5.2	Понятие формальной политики безопасности. Реализация формальной политики безопасности различный уровней /Лек/	8	5	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.1Л2.2 Э1 Э3	Проверка конспекта лекиций, опрос по то теме
5.3	Понятие формальной политики безопасности. Реализация формальной политики безопасности различный уровней /Пр/	8	5	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.3Л2.1Л3.2 Э1 Э3	Опрос по теме занятия, решение стандартных задач
5.4	Понятие формальной политики безопасности. Реализация формальной политики безопасности различный уровней /Ср/	8	10	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.4Л2.5Л3.2 Э1 Э3	Работа с методическими материалами, конспектами лекций и практических занятий
	Раздел 6. Промежуточная аттестация					
6.1	Зачет /Тема/	8	0			Проверка полноты и уровня усвоения компетенций дисциплины

6.2	Подготовка к зачету /ЗаО/	8	8,75	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1	Работа с методическими материалами дисуиплины
6.3	Зачет /ИКР/	8	0,25	ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.10-З ОПК-8.10-У ОПК-8.10-В ОПК-8.11-З ОПК-8.11-У ОПК-8.11-В	Э1	Проверка полноты и уровня усвоения компетенций дисциплины

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Фонд оценочных средств для проведения промежуточной аттестации обущающихся по дисциплине "Модели безопасности компьютерных систем" приведен в файле "10.05.03 МБКС ОМ Набор2022 20221019", ссылка на который размещена на вкладке "Приложения"

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	Галатенко В. А.	Основы информационной безопасности	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, 266 с.	978-5-94774-821-5, http://www.iprbookshop.ru/52209.html
Л1.2	Трушин В. А., Котов Ю. А., Левин Л. С., Донской К. А.	Введение в информационную безопасность и защиту информации : учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2017, 132 с.	978-5-7782-3233-4, http://www.iprbookshop.ru/91329.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.3	Дронов В. Ю.	Международные и отечественные стандарты по информационной безопасности : учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2016, 34 с.	978-5-7782-3112-2, http://www.iprbookshop.ru/91395.html
Л1.4	Червяков Н. И., Бабенко М. Г., Гладков А. В.	Вероятностные методы оценки состояния информационной безопасности : учебное пособие	Ставрополь: Северо-Кавказский федеральный университет, 2017, 182 с.	2227-8397, http://www.iprbookshop.ru/92536.html

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Рогозин В. Ю., Галушкин И. Б., Новиков В. К., Вепрев С. Б.	Основы информационной безопасности : учебник для студентов вузов, обучающихся по направлению подготовки «правовое обеспечение национальной безопасности»	Москва: ЮНИТИ-ДАНА, 2017, 287 с.	978-5-238-02857-6, http://www.iprbookshop.ru/72444.html
Л2.2	Жидко Е. А.	Логико-вероятностно-информационный подход к моделированию информационной безопасности объектов защиты : монография	Воронеж: Воронежский государственный архитектурно-строительный университет, ЭБС АСВ, 2016, 121 с.	978-5-89040-614-9, http://www.iprbookshop.ru/72917.html
Л2.3	Смирнов А. А.	Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза : монография	Москва: ЮНИТИ-ДАНА, 2017, 159 с.	978-5-238-02259-8, http://www.iprbookshop.ru/81515.html
Л2.4	Гультяева Т. А.	Основы информационной безопасности : учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2018, 79 с.	978-5-7782-3640-0, http://www.iprbookshop.ru/91640.html
Л2.5	Лагоша О. Н.	Сертификация информационных систем	Санкт-Петербург: Лань, 2020, 112 с.	978-5-8114-4668-1, https://e.lanbook.com/book/139268
Л2.6	Громов Ю.Ю., Драчев В.О., Иванова О.Г., Шахов Н.Г.	Основы информационной безопасности : учеб. пособие	Старый Оскол: ТНТ, 2019, 381с.; прил.	978-5-94178-216-1, 1
Л2.7	Краковский Ю. М.	Методы защиты информации	Санкт-Петербург: Лань, 2021, 236 с.	978-5-8114-5632-1, https://e.lanbook.com/book/156401

6.1.3. Методические разработки

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	Галатенко, В. А.	Основы информационной безопасности : учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020, 266 с.	978-5-4497-0675-1, http://www.iprbookshop.ru/97562.html
Л3.2	сост., Кирколуп, Скурыдина, Е. М.	Информационная безопасность : учебное пособие	Барнаул: Алтайский государственный педагогический университет, 2017, 313 с.	978-5-88210-898-3, http://www.iprbookshop.ru/102889.html

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Сайт кафедры Информационная безопасность РГРТУ
Э2	Единое окно доступа к образовательным ресурсам
Э3	Электронная библиотека РГРТУ, режим доступа с любого компьютера без пароля
Э4	Дистанционный электроный ресурс "Модели безопасности компьютерных систем"

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
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
6.3.2.3	Справочная правовая система «КонсультантПлюс» (договор об информационной поддержке №1342/455-100 от 28.10.2011 г.)

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1	266 а учебно-административный корпус. компьютерный класс для проведения учебных занятий, самостоятельной работы обучающихся Специализированная мебель (14 компьютерных столов), 14 персональных компьютеров. Возможность подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ.
2	267 учебно-административный корпус. Учебная аудитория для проведения учебных занятий лекционного и семинарского типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Специализированная мебель. 80 мест, доска. Мультимедийное оборудование, компьютер.
3	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.
4	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)

Методические указания для обучающихся по освоению дисуиплины "Модели безопасности компьютерных систем" приведены в файле "10.05.03 МБКС МО Набор2022 2021019", ссылка на который размещена на вкладке "Приложения"