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

Программно-аппаратные средства защиты информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационная безопасность**

Учебный план 10.05.03_20_00.plx
10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Квалификация **специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **6 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	32	32	32	32	64	64
Лабораторные			16	16	16	16
Практические	16	16	16	16	32	32
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.	48,25	48,25	66,35	66,35	114,6	114,6
Контактная работа	48,25	48,25	66,35	66,35	114,6	114,6
Сам. работа	51	51	6	6	57	57
Часы на контроль	8,75	8,75	35,65	35,65	44,4	44,4
Итого	108	108	108	108	216	216

г. Рязань

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

Рабочая программа дисциплины

Программно-аппаратные средства защиты информации

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 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 дисциплины «Программно-аппаратные средства защиты информации» является получение обучающимися знаний, формирование у них умений и навыков, необходимых при эксплуатации и администрирования программно-аппаратных средств защиты информации с учетом требований по обеспечению информационной без-опасности для решения задач в профессиональной деятельности.
1.2	Задачами дисциплины являются:
1.3	− получение знаний об основных уязвимостях и угрозах безопасности в программном обеспечении автоматизированных систем; основных угрозах безопасности данных в автома-тизированных системах; основных направлениях, средствах и методах защиты программного обеспечения автоматизированных систем; основных средствах и методах защиты данных в автоматизированных системах; программных средствах обеспечения информационной без-опасности в защищенных операционных системах;
1.4	− приобретение умения оценивать защищенность программного обеспечения и за-щищенность данных в автоматизированных системах; проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в со-ставе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; применять основные средства и методы аутентификации поль-зователей в автоматизированных системах; применять основные средства и методы защиты программного обеспечения в автоматизированных системах; применять основные средства и методы защиты данных в автоматизированных системах, в том числе средства восстановле-ния данных и программного обеспечения автоматизированных систем после сбоев;
1.5	− приобретение практических навыков эксплуатации и администрирования (настройка разграничения доступа, аутентификации и аудита) программно-аппаратных средств защиты информации в автоматизированных системах.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
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)

ОПК-11: Способен разрабатывать компоненты систем защиты информации автоматизированных систем;

ОПК-11.1. Выбирает программные и программно-технические средства обеспечения ИБ для использования их в составе АС с целью обеспечения требуемого уровня защищенности АС

Знать
Программно-аппаратные средства защиты информации, используемые в составе автоматизированных систем
Уметь
Выбиратьпрограммно-аппаратные средства защиты информации для использования в составе автоматизированных систем
Владеть
Навыками выбора программно-аппаратных средств защиты информации для использования в составе автоматизированных систем

ОПК-11.2. Применяет программные и программно-технические сред-ства обеспечения ИБ для защиты информации в АС

Знать
Программно-аппаратные средства защиты информации для обеспечения безопасности информации в автоматизированных системах
Уметь
Применять программно-аппаратные средства защиты информации для обеспечения безопасности информации в автоматизированных системах
Владеть
Навыками применения программно-аппаратных средств защиты информации для обеспечения безопасности информации в автоматизированных системах

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	Программно-аппаратные средства защиты информации, используемые в составе автоматизированных систем
3.1.2	Программно-аппаратные средства защиты информации для обеспечения безопасности информации в автоматизированных системах

3.2	**Уметь:**
3.2.1	Выбирать и применять программно-аппаратные средства защиты информации для использования в составе автоматизированных систем
3.2.2	Применять программно-аппаратные средства защиты информации для обеспечения безопасности информации в автоматизированных системах
3.3	**Владеть:**
3.3.1	Навыками выбора и применения программно-аппаратных средств защиты информации для использования в составе автоматизированных систем
3.3.2	Навыками применения программно-аппаратных средств защиты информации для обеспечения безопасности информации в автоматизированных 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. Общие вопросы ОБИ и дисциплины ПАСЗИ					
1.1	/Тема/	7	0			
1.2	Связь дисциплины с другими дисциплинами учебного плана. Взаимосвязь понятий: защищенность, уязвимость, угроза, нарушитель, атака, ущерб, риск. Виды программно-аппаратных (программно-технических) средств защиты информации. Отличия их от технических средств защиты информации. Каналы утечки компьютерной информации: защищаемые элементы; источники угроз; основные каналы утечки информации и средства их образования. /Лек/	7	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
1.3	Изучение литературы по вопросам: - виды программно-аппаратных (программно-технических) средств защиты /Ср/	7	3	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 2. Защита от РПВ (ПМВ)					
2.1	/Тема/	7	0			

2.2	Понятие РПВ. Виды РПВ. Программные закладки (ПЗ): понятие ПЗ; виды ПЗ; модели работы (воздействия на компьютерные системы) ПЗ на компьютеры; защита от программных закладок (поиск недокументированных (недекларированных) возможностей); понятие изолированной программной среды и изолированного компьютера; контроль отсутствия НДВ. Защита от троянов и вредоносных утилит: утилиты скрытого ад-министрирования (backdoor), exploit'ы, rootkit'ы и просто трояны; кейлоггеры; руткиты (руткиты уровня пользователя, руткиты уровня ядра). Защита от троянов и руткитов. Защита от вирусов: понятие вируса; классификация вирусов; файловые вирусы; макро-вирусы; сетевые вирусы (черви); почтовые вирусы; загрузочные вирусы; методы защиты вирусов от обнаружения; вредоносные утилиты, специальные упаковщики и парольные взломщики; антивирусное ПО; методы защиты от вирусов и ПЗ; белый и черный ящики (Blacklisting и Whitelisting). Вредоносные программы для мобильных устройств. Внедрение вредоносного ПО через автозагрузку (реестр и Планировщик Windows): как устроен реестр; ключи автозагрузки; описание (определение) возможностей разных вариантов автозапуска программ; планировщик заданий в Windows. /Лек/	7	10	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
2.3	Изучение литературы по вопросам: - виды РПВ. /Ср/	7	6	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
2.4	Изучение литературы по вопросам: - модели работы (воздействия на компью-терные системы) ПЗ на компьютеры. /Ср/	7	6	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
2.5	Изучение литературы по вопросам: - трояны и руткиты; - защита от троянов и руткитов. /Ср/	7	6	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).

2.6	Изучение литературы по вопросам: - вредоносные программы для мобильных устройств; - белый и черный ящики (Blacklisting и Whitelisting); - внедрение вредоносного ПО через автоза-грузку (реестр и Планировщик Windows) /Ср/	7	6	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 3. Защита данных					
3.1	/Тема/	8	0			

3.2	Направления и методы защиты данных: - контроль доступа к локальным портам, внешним носителям и принтерам; - разграничение доступа к ресурсам ПК; - антивирусная защита; - защита данных от утечки (DLP); - резервное копирование и восстановление (данных и разделов) - шифрование данных: - использование RAID-массивов (RAID 1 - зеркало); - архивирование с паролем (WinRar); - устранение потенциальных опасностей хищения данных: - отслеживание временных файлов; - контроль записи на переносные носители; - отключение службы «Сервер»; - отключение удаленного доступа (RDP или терминальный сервер); - устранение потенциальных опасностей потери данных: - стабильное электропитание; - резервное копирование; - завершение транзакции записи «нового» перед удалением «старого» (чтобы не потерять «старое»); - контроль целостности программ и данных; - гарантированное уничтожение (затирание) данных. Программные средства резервного копирования (Acronis Backup). Программные средства восстановления: - данных - EasyRecovery - RStudio - GetDataBack - разделов - Acronis Partition Expert (в составе Acronis Disk Director) Программные средства защиты данных от утечки: - статистика состояния проблемы утечек информации; - задачи системы защиты от утечек данных; - классификация внутренних нарушителей; - использование DLP-систем для предотвращения утечки дан-ных: - принципы работы DLP; - основные функции DLP; - состав DLP и их виды: - хостовые DLP; - шлюзовые DLP; - универсализация систем DLP; - примеры систем DLP; Средства шфрования данных: - EFS (можно зашифровывать отдельные папки) - BitLocker + TPM (зашифровывает весь раздел) Средства гарантированного уничтожения (затирания) данных: - Требования стандартов и руководящих документов к гарантированному уничтожению информации - Удаление информации - Виды остаточной информации - Восстановление удаленной информации - Виды гарантированного уничтожения	8	20	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.

	информации - Достоинства и недостатки аппаратного и программного способов гарантированного уничтожения информации - Аппаратные средства уничтожения информации - Средства, использующие физический принцип воздействия магнитным полем - Средства, использующие механический принцип воздействия - Программное гарантированное уничтожение информации - Наиболее известные алгоритмы затирания информации - Особенности гарантированного уничтожения информации с различных носителей - Сертифицированные программные средства удаления и затирания информации - Программа Terrier 3.0 - СЗИ Secret Net - СЗИ Dallas Lock 8.0 - СЗИ Страж NT - Бесплатные программные средства удаления и затирания информации - Программа Eraser - Программа CCleaner - Mem Reduct - Сравнение программных средств гарантированного уничтожения информации Программные средства контроля целостности программ и дан-ных. /Лек/					
3.3	Изучение литературы по вопросам: - средства шифрования данных - использование RAID-массивов - архивирование с паролем - устранение (отключение) потенциальных опасностей хищения данных - устранение опасностей потери данных. /Ср/	7	4	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
3.4	Изучение литература по вопросам: - примеры систем DLP; - сравнение систем DLP. /Ср/	7	4	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
3.5	Изучение литература по вопросам: - средства шифрования данных в ОС Windows; - сертифицированные и бесплатные программные средства гарантированного уни-чтожения данных /Ср/	7	4	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).

3.6	Изучение документации по программному средству резервного копирования Acronis Backup /Ср/	7	4	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
3.7	Изучение возможностей и настроек про-грамм семейства Acronis для резервного ко-пирования (ч.1) /Пр/	7	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.8	Изучение возможностей и настроек про-грамм семейства Acronis для резервного ко-пирования (ч.2) /Пр/	7	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.9	Изучение возможностей и настроек про-грамм семейства Acronis для резервного ко-пирования (ч.3) /Пр/	7	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.10	Работа с программами семейства Acronis (резервное копирование) /Лаб/	8	4	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
3.11	Изучение документации по программным средствам восстановления: - данных - EasyRecovery - RStudio - GetDataBack - разделов - Acronis Partition Expert (в составе Acronis Disk Director) /Ср/	7	4	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).

3.12	Изучение возможностей и настроек про-граммных средств восстановления данных /Пр/	7	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.13	Восстановление данных с помощью про-граммно-аппаратных средств /Лаб/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
3.14	Изучение возможностей и настроек про-грамм семейства Acronis по восстановлению разделов (ч.1) /Пр/	7	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.15	Изучение возможностей и настроек про-грамм семейства Acronis по восстановлению разделов (ч.2) /Пр/	7	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.16	Изучение возможностей и настроек про-грамм семейства Acronis по восстановлению разделов (ч.3) /Пр/	7	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.17	Работа с программами семейства Acronis (восстановление разделов) /Лаб/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.

3.18	Изучение литературы по программным средствам контроля целостности программ /Ср/	7	4	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
3.19	Изучение типовых настроек программно-аппаратного средства контроля целостности «ФИКС 2.0.1» /Пр/	7	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.20	Работа с программно-аппаратным средством «ФИКС 2.0.1» /Лаб/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
3.21	Сдача (прием) зачета /ИКР/	7	0,25	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Ответы на Контрольные вопросы Результаты решения задач. Ответы на дополнительные вопросы. Результаты тестирования.
3.22	Подготовка к зачету /ЗаО/	7	8,75	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Задачи к зачету. Билеты к зачету. Тесты к зачету.
	Раздел 4. Защита программ					
4.1	/Тема/	8	0			

4.2	Направления защиты программ. Классификация средств атаки на средства защиты ПО. Классификация методов защиты ПО: - методы защиты от НСД к ПО: - защита с помощью регистрационных кодов; - защита на основе ключевого файла; - защита методом online регистрации; - защита на основе аппаратных (электронных) ключей; - защита с помощью протекторов («навесная» защита); - защита с помощью криптографических методов: - использование шифрования; - использование стеганографии (сокрытие информации в файлах с другой информацией); - методы защиты от НСК (ПО на носителе или самого носителя) - методы, затрудняющие считывание копируемой информации с материального носителя (стандартными методами копирования): - нестандартная разбивка (форматирование) носителя; - нанесение на поверхность носителя специальных меток; - преднамеренная порча (искажение) оглавления защищаемого носителя; - методы, препятствующие использованию скопированной информации; - привязка защищаемого ПО к уникальным характеристикам компьютера или носителя; - скрытое хранение данных или ПО (стеганография) или шифрование данных или ПО; - методы защиты от несанкционированного исследования, анализа и восстановления алгоритмов: 1) структурные методы защиты от анализа (усложнения анализа) а) искусственное усложнение (запутывание) (англ. obfuscation, обфускация) алгоритмов обработки данных б) искусственное усложнение структуры програм-мы 2) затруднение дизассемблирования (статического анализа программ) а) использование самогенерирующих кодов б) динамическое изменение (мутация) кода про-граммы в) архивация кода программы г) шифрование кода программы 3) обнаружение и затруднение отладки (динамического анализа программ) а) выявление факта выполнения программы под отладчиком б) затруднение отладки - навязывание отладчику ложных точек останова - засорение консоли отладчика - использование своего отладчика для работы защищаемого ПО - использование (провоцирование) известных программных ошибок конкретных отладчиков	7	20	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.

	4) эмуляция процессоров и операционных систем 5) нестандартные методы работы с аппаратным обеспечением 6) нестандартные обращения к функциям ОС Построение технической защиты ПО от несанкционированного копирования (НСК): а) Структура системы технической защиты от НСК. б) Подсистема внедрения управляющих механизмов. в) Подсистема противодействия нейтрализации защитных механизмов. г) Блок ответной реакции д) Блок сравнения характеристик среды. е) Блок установки характеристик среды Защита программ от НСД и НСК с помощью регистрационных кодов: - требования к защите ПО от НСК и классификация методов защиты; - методы проверки регистрационных кодов: - «черный» ящик; - решение сложной математической задачи; - табличные методы; - достоинства и недостатки защиты ПО от НСК. Защита программ от НСД и НСК с помощью навесных защит (протекторов): - какую защиту обеспечивают протекторы; - как работают протекторы; - сценарии атаки (- действия взломщика этой защиты); - защита от взлома протектора; - примеры протекторов: - ASProtect - Armadillo - VMProtect - Themida/WinLicense - HASP Envelope - StarForce - недостатки защиты с помощью протекторов. Защита ПО от НСД и НСК с помощью электронных ключей: - виды электронных ключей; - состав ключа; - Аппаратная часть - блок логики, - блок памяти) - Программная часть - драйвер - модуль, встраиваемый в защищаемое ПО - варианты реализации электронных ключей: - Ключи с неизвестным алгоритмом - Ключи с известным алгоритмом - Ключи с программируемым алгоритмом - Ключи с таймером - Сетевые ключи - приемы защиты ключей от взлома - достоинства и недостатки использования ключей для защиты ПО; - производители электронных ключей: - ЗАО «Аладдин Р.Д.» - Rainbow security (WibuKey) - ЗАО "Актив-софт" (Guardant)					

	- «МультиСофт» (Rockey, раньше Feitian Rockey) - «Компания "Эримекс"» (Sentinel (HASP) HL) /Лек/					
4.3	Изучение литературы по вопросам: Методы защиты от несанкционированного исследования, анализа и восстановления алгоритмов: структурные методы защиты от анализа (искусственное усложнение алго-ритмов; искусственное усложнение струк-туры программы); затруднение дизассем-блирования (использование самогенериру-ющих кодов; динамическое изменение (му-тация) кода программы; архивация кода программы; шифрование кода программы); обнаружение и затруднение отладки (выяв-ление факта выполнения программы под отладчиком; затруднение отладки - навязывание отладчику ложных точек останова; засорение консоли отладчика; использование своего отладчика для работы защищаемого ПО; использование (провоцирование) известных программных ошибок конкретных отладчиков); эмуляция процессоров и операционных систем; нестандартные методы работы с аппаратным обеспечением; нестандартные обращения к функциям ОС. защита программ от НСК с помощью навес-ных защит (протекторов): какую защиту обеспечивают протекторы; как работают протекторы; сценарии атаки - действия взломщика этой защиты; защита от взлома протектора; примеры протекторов; недо-статки защиты с помощью протекторов. За-щита ПО с помощью электронных ключей: виды электронных ключей; состав ключа; варианты реализации электронных ключей; достоинства и недостатки использования ключей для защиты ПО; производители электронных ключей. /Ср/	8	4	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
4.4	Изучение защиты программ от изучения статическим методом /Пр/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
4.5	Изучение защиты программ от изучения статическим методом /Лаб/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.

4.6	Изучение защиты программ от изучения ди-намическим методом /Пр/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
4.7	Изучение защиты программ от изучения ди-намическим методом /Лаб/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
	Раздел 5. Программные и программно-технические средства обеспечения безопасности (не относящиеся к защите программ и данных)					
5.1	/Тема/	8	0			
5.2	Электронный замок (аппаратный модуль доверенной загрузки) «Соболь». Средства безопасной аутентификации типа RuToken. СЗИ SecretNet (SecretNet Studio) и Страж. Программные средства генерации паролей. Программные средства анализа защищенности сети (Ревизор). /Лек/	8	12	ОПК-11.1-З ОПК-11.1-У ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
5.3	Изучение литературы по разделу средствам из раздела 5 /Ср/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
5.4	Изучение СЗИ SecretNet /Пр/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.

5.5	Изучение СЗИ Страж /Пр/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
5.6	Изучение СЗИ SecretNet и Страж /Лаб/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Отчет по ЛР Защита ЛР.
5.7	Изучение средств безопасной аутентифика-ции типа RuToken (ч.1) /Пр/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
5.8	Изучение средств безопасной аутентифика-ции типа RuToken (ч.2) /Пр/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
5.9	Изучение сканера сети «Ревизор 2.0». /Пр/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
5.10	Изучение программы «Ревизор Сети 2.0 /Пр/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.

5.11	Прием (сдача) экзамена /ИКР/	8	0,35	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Ответы на Контрольные вопросы Результаты решения задач. Ответы на дополнительные вопросы. Результаты тестирования.
5.12	Консультирование перед экзаменом /Кнс/	8	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Вопросы к экзамену. Решение типовых задач. Ответы на вопросы.
5.13	Подготовка к экзамену /Экзамен/	8	35,65	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4 Э5 Э6	Задачи к экзамену. Билеты к экзамену. Тесты к экзамену.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы по данной дисциплине приведены в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Программно-аппаратные средства защиты информации»).

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	Помешкин А. А., Коротких И. В.	Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса «SECRET NET 5.0» : учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2012, 47 с.	978-5-7782-1990-8, http://www.iprbookshop.ru/45015.html
Л1.2	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, 368 с.	2227-8397, http://www.iprbookshop.ru/73732.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.3	Фомин Д. В.	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие	Саратов: Вузовское образование, 2018, 218 с.	978-5-4487-0297-6, http://www.iprbookshop.ru/77317.html
Л1.4	Астайкин А. И., Мартынов А. П., Николаев Д. Б., Фомченко В. Н.	Методы и средства обеспечения программно-аппаратной защиты информации : научно-техническое издание	Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015, 224 с.	978-5-9515-0305-3, http://www.iprbookshop.ru/60959.html
Л1.5	Соколов В. П., Тарасова Н. П., Шелухин О. И.	Кодирование в системах защиты информации : учебное пособие	Москва: Московский технический университет связи и информатики, 2016, 94 с.	2227-8397, http://www.iprbookshop.ru/61485.html
Л1.6	Петренко В. И.	Защита персональных данных в информационных системах : учебное пособие	Ставрополь: Северо-Кавказский федеральный университет, 2016, 201 с.	2227-8397, http://www.iprbookshop.ru/66023.html
Л1.7	Ермаков Д. Г., Присяжный А. В.	Применение антивирусных программ для обеспечения информационной безопасности	Екатеринбург: Уральский федеральный университет, ЭБС АСВ, 2013, 64 с.	2227-8397, http://www.iprbookshop.ru/66577.html
Л1.8	Калмыков И. А., Пелешенко В. С.	Компьютерная криминалистика : лабораторный практикум	Ставрополь: Северо-Кавказский федеральный университет, 2017, 84 с.	2227-8397, http://www.iprbookshop.ru/69392.html
Л1.9	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
Л1.10	Глотина И. М.	Средства безопасности операционной системы Windows Server 2008 : учебно-методическое пособие	Саратов: Вузовское образование, 2018, 141 с.	978-5-4487-0136-8, http://www.iprbookshop.ru/72538.html
Л1.11	Джонс К. Д., Шема М., Джонсон Б. С.	Инструментальные средства обеспечения безопасности	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, 914 с.	2227-8397, http://www.iprbookshop.ru/73679.html

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1		Администрирование ОС Unix	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, 303 с.	2227-8397, http://www.iprbookshop.ru/73659.html
Л2.2	Айвенс К.	Администрирование Microsoft Windows Server 2003	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, 486 с.	2227-8397, http://www.iprbookshop.ru/73725.html

6.1.3. Методические разработки

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	Денисов И. А.	Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации	Москва: Московский технический университет связи и информатики, 2016, 31 с.	2227-8397, http://www.iprbookshop.ru/61529.html
Л3.2	Кузьмин Ю.М., Кураксин В.А., Пржегорлинский В.Н.	Программно-аппаратные средства обеспечения информационной безопасности : Методические указания	Рязань: РИЦ РГРТУ, 2018,	, https://elib.rsreu.ru/ebs/download/1883
Л3.3	Кузьмин Ю.М., Калинкина Т.И.	Защита программ и данных. Ч.1 : Методические указания	Рязань: РИЦ РГРТУ, 2019,	, https://elib.rsreu.ru/ebs/download/2119
Л3.4	Кузьмин Ю.М., Калинкина Т.И.	Защита программ и данных. Часть 2. Исследование программ динамическим методом: метод. указ. к лаб. работам : Методические указания	Рязань: РИЦ РГРТУ, 2020,	, https://elib.rsreu.ru/ebs/download/2638

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

LibreOffice	Свободное ПО
VMware Player	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 «Программно-аппаратные средства защиты информации»).	