**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»**

**Факультет вычислительной техники**

**Кафедра «Информационная безопасность»**

|  |  |
| --- | --- |
| **«СОГЛАСОВАНО»**  **Декан ФВТ**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.А. Перепелкин**  **«\_\_» \_\_\_\_\_\_\_\_ 2020 г.** | **«УТВЕРЖДАЮ»**  **Проректор по РОПиМД**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Корячко А.В.**  **«\_\_» \_\_\_\_\_\_\_ 2020 г.** |
| **Руководитель ОПОП**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.Н. Пржегорлинский**  **«\_\_» \_\_\_\_\_\_\_\_ 2020 г.** |  |

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Б1.Б.38 «Защита программ и данных »**

Специальность: 10.05.01 Компьютерная безопасность

Специализация: № 8 Информационная безопасность объектов информатизации

на базе компьютерных систем в защищенном исполнении

ОПОП по специальности:

Компьютерная безопасность

Квалификация выпускника: специалист по защите информации

Форма обучения - очная

Срок обучения — 5,5 лет

Рязань 2020

1. **ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ СПЕЦИАЛИТЕТА**

Рабочая программа по дисциплине «Защита программ и данных» является составной частью основной профессиональной образовательной программы (ОПОП) по специальности 10.05.01 «Компьютерная безопасность», разработанной в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности 10.05.01 «Компьютерная безопасность» (уровень специалитета), утвержденным приказом Минобрнауки России от 01.12.2016 г. №1512.

**Целью изучения дисциплины** является получение обучающимися знаний, формирование у них умений и навыков, необходимых при анализе и разработке защищенных программных средств и защите данных в компьютерных системах для решения задач в профессиональной деятельности.

**Задачами дисциплины** являются:

− получение знаний об основных уязвимостях и угрозах безопасности в программном обеспечении (ПО), основных угрозах безопасности данных в компьютерных системах, основных средствах и методах анализа программных реализаций и средствах и методах защиты программ от изучения, основных направлениях, средствах и методах защиты программ, основных направлениях, средствах и методах защиты данных;

− приобретение умения оценивать защищенность программ и защищенность данных в компьютерных системах, применять инструментальные средства отладки и дизассемблирования программного кода, средства и методы защиты программ, в том числе от анализа, применять средства и методы защиты данных, в том числе средства восстановления данных и программ после сбоев;

− приобретение практических навыков оценки защищенности программ и защищенности данных в компьютерных системах, применения инструментальных средств отладки и дизассемблирования программного кода для анализа, применения основных средств и методов защиты программ, в том числе для защиты от анализа, применения основных средств и методов защиты данных, в том числе средств восстановления данных и программ после сбоев.

**Перечень планируемых результатов обучения по дисциплине**

|  |  |  |
| --- | --- | --- |
| **Коды**  **компетенций** | **Содержание**  **компетенции** | **Перечень планируемых результатов обучения** |
| **ОПК-5** | Способность ис­пользовать норма­тивные правовые акты в своей про­фессиональной де­ятельности | **Знать**   * основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации   **Уметь**   * применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;   **Владеть**   * навыками работы с нормативными правовыми актами в области защиты информации |
| **ПК-*5*** | Способность участвовать в раз­работке и конфи­гурировании про­граммно-аппарат­ных средств за­щиты информации, включая защищен­ные операционные системы | **Знать**   * требования к программным и про­грамм­но-техническим сред­ст­вам обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти; * виды и функции программных и про­грамм­но-технических сред­ст­в обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти; * основные угрозы безопасности информации и модели нарушителя в компьютерных системах и сетях; * основные направления, методы и способы защиты программ и данных с помощью программных и программно-технических средств; |
| **Уметь**   * анализировать программные, архитектурно-технические и схемотехнические решения компонентов компьютерных систем и сетей с целью выявления потенциальных уязвимостей информационной безопасности; * про­во­дить вы­бор программных и про­грамм­но-технических средств обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти с це­лью обес­пе­че­ния тре­буе­мо­го уров­ня за­щи­щен­но­сти компьютерных систем и сетей |
| **Владеть**   * навыками установки и настройки семейств Windows и Unix и локальных сетей на их основе с учетом требований по обеспечению информационной безопасности*;* * на­вы­ка­ми конфигурирования, настройки и ис­поль­зо­ва­ния программных и про­грамм­но-технических средств обес­пе­че­ния безо­пас­но­сти*;* |
| **ПК-1*7*** | Способность про­изводить уста­новку, наладку, тестирование и об­служивание со­временного об­щего и специаль­ного программного обеспечения, включая операци­онные системы, системы управле­ния базами дан­ных, сетевое про­граммное обеспе­чение | **Знать**   * требования к программным и про­грамм­но-техническим сред­ст­вам обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти*;* * виды и функции программных и про­грамм­но-технических сред­ст­в обес­пе­че­ния ин­фор­ма­ци­он­ной безо­пас­но­сти в опе­ра­ци­он­ных сис­те­мах, сис­те­мах управ­ле­ния ба­за­ми дан­ных, ком­пь­ю­тер­ных системах и се­тях; * основные угрозы безопасности информации и модели нарушителя в компьютерных системах и сетях; * основные меры по защите информации в компьютерных системах и сетях; * методы и программно-технические и программные средства защиты программного обеспечения от несанкционированного изучения, копирования и модификации; * методы и программно-технические и программные средства защиты данных утечки, несанкционированного удаления и модификации;   **Уметь**   * определять актуальные угрозы безопасности информации (программ и данных) в компьютерных системах и сетях; * определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения необходимого и достаточного уровня защищенности программ и данных в компьютерных системах и сетях; * развертывать, настраивать и использовать программные и программно-технические средства для защиты программ и данных в компьютерных системах и сетях;   **Владеть**   * на­вы­ка­ми определения актуальных угроз безопасности информации (программ и данных) в компьютерных системах и сетях; * на­вы­ка­ми конфигурирования, настройки и ис­поль­зо­ва­ния программных и про­грамм­но-технических средств обес­пе­че­ния безо­пас­но­сти; * инструментарием, обеспечивающим программно-техническую защиту программного обеспечения от изучения, модификации и копирования; * инструментарием, обеспечивающим программно-техническую защиту данных от утечки, несанкционированного удаления и модификации. |

**2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП СПЕЦИАЛИТЕТА**

Дисциплина Б1.Б.38 «Защита программ и данных» относится к базовой части блока «Дисциплины» учебного плана специальности 10.05.01 – «Компьютерная безопасность» со специализацией № 8 «Информационная безопасность объектов информатизации на базе компьютерных систем в защищенном исполнении» ФГБОУ ВО «РГРТУ им. В.Ф. Уткина».

Изучается дисциплина по очной форме обучения на 5 курсе в 9-ом семестре.

*Пререквизиты дисциплины*.

Для освоения дисциплины «Защита программ и данных» обучающиеся должны обладать компетенциями, полученными в результате освоения следующих дисциплин:

- «Спецдисциплина 1»;

- «Спецдисциплина 3»;

- «Операционные системы»

- «Защита в операционных системах»;

- «Криптографические протоколы»

*Взаимосвязь с другими дисциплинами*.

Дисциплина «Защита программ и данных» содержательно и методологически взаимосвязана с другими дисциплинами, такими как «Оценка и управление рисками при защите информации в КС».

*Постреквизиты дисциплины.*

Компетенции, полученные в результате освоения дисциплины «Защита программ и данных», необходимы обучающемуся при изучении следующих дисциплин:

- «Защищенные геоинформационные технологии и системы»;

- «Защита от компьютерных и сетевых атак»;

- «Научно-исследовательская работа»;

- «Производственная практика»;

- «Преддипломная практика»;

- «Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы».

1. **3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ**
2. Общая трудоемкость (объем) дисциплины составляет 4 зачетных единицы (ЗЕ), 144 часа для очной формы обучения, изучается на 5 курсе в 9 семестре обучения.

|  |  |
| --- | --- |
| **Вид учебной работы** | **Всего часов** |
| Общая трудоемкость дисциплины,  в том числе: | 144 |
| Контактная работа обучающихся с преподавателем (всего),  в том числе: | 50,35 |
| Лекции | 24 |
| Лабораторные работы (ЛР) | 24 |
| Практические занятия (ПЗ) |  |
| Иная контактная работа (ИКР) | 0,35 |
| Консультация (Кнс) | 2 |
| Самостоятельная работа обучающихся (всего),  в том числе: | 93,65 |
| Контроль, подготовка к экзамену | 44,65 |
| Иные виды самостоятельной работы | 49 |
| Форма промежуточной аттестации - экзамен |  |

**4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ**

1. 4.1. Содержание дисциплины, структурированное по темам (разделам)

|  |  |
| --- | --- |
| **Раздел дисциплины** | **Содержание** |
| 1. Модели распространения и лицензирования ПО | Лицензирование ПО. Свободное и несвободное ПО.  Программы и виды права (авторское, информационное, вещное).  Свободное ПО - признаки и разновидности свободного ПО. Несвободное, бесплатное, некоммерческое ПО.  Особенности защиты коммерческого ПО. |
| 2.Защита программ | 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 оnline-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 программы  2) затруднение дизассемблирования (статического анализа программ)  а) использование самогенерирующих кодов  б) динамическое изменение (мутация) кода программы  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  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:  - 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:  Защита ПО от разрушающих программных воздействий (РПВ) и программно-математических воздействий (ПМВ):  - 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 администрирования (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. |
| 3. Защита данных | 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;  - 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  Программные средства восстановления:  - данных  - разделов  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 данных:  - принципы работы DLP;  - основные функции DLP;  - состав DLP и их виды:  - хостовые DLP;  - шлюзовые DLP;  - универсализация систем DLP;  - примеры систем DLP;  Средства ОС для шифрования данных.  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 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  - Бесплатные программные средства удаления и затирания информации  - Сравнение программных средств гарантированного уничтожения информации |
| 4. Программные и программно-технические средства защиты программ и данных | Электронный замок (аппаратный модуль доверенной загрузки).  Средства безопасной аутентификации.  СЗИ SecretNet (SecretNet Studio) и Страж.  Программные средства контроля целостности программ и данных.  Программные средства генерации паролей. |

1. 4.2. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Раздел** | **Общая трудо­емкость, всего часов** | **Контактная работа**  **обучающихся с преподавателем** | | | | | | **Контроль** | **Само­стоятельная работа обу­чаю­щихся** |
| **Всего** | **Лекции** | **Практические занятия** | **Лабораторные работы** | **ИКР** | **Консультации** |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1 | Модели распространения и лицензирования ПО | ***7*** | ***2*** | ***2*** |  |  |  |  |  | ***5*** |
| 2 | Защита программного обеспечения | ***44*** | ***30*** | ***10*** |  | ***20*** |  |  |  | ***14*** |
| 3 | Защита данных | ***28*** | ***14*** | ***10*** |  | ***4*** |  |  |  | ***14*** |
| 4 | Программные и программно-технические средства защиты программ и данных | ***18*** | ***2*** | ***2*** |  |  |  |  |  | ***16*** |
|  | Иная контактная работа | ***0,35*** | ***0,35*** |  |  |  | ***0,35*** |  |  |  |
|  | Контроль | ***44,65*** |  |  |  |  |  |  | ***44,65*** |  |
|  | Консультации | ***2*** | ***2*** |  |  |  |  | ***2*** |  |  |
|  | Всего по дисциплине | ***144*** | ***50,35*** | ***24*** |  | ***24*** | ***0,35*** | ***2*** | ***44,65*** | ***49*** |

Виды практических, лабораторных и самостоятельных работ

| Раздел | Вид работы | Наименование и содержание работы | Трудоемкость, часов |
| --- | --- | --- | --- |
| Раздел 1. Модели распространения и лицензирования ПО | Самостоятельная работа обучающегося | Изучение литературы по вопросам:  - свободное ПО - признаки и разновидности свободного ПО;  - особенности защиты коммерческого ПО. | 5 |
| Раздел 2. Защита программ | Самостоятельная работа обучающегося  Самостоятельная работа обучающегося  Самостоятельная работа обучающегося  Лабораторная работа  Лабораторная работа  Лабораторная работа  Лабораторная работа  Лабораторная работа | Изучение литературы по вопросам:  Методы защиты от несанкционированного исследования, анализа и восстановления алгоритмов: структурные методы защиты от анализа (искусственное усложнение алгоритмов; искусственное усложнение структуры программы); затруднение дизассемблирования (использование самогенерирующих кодов; динамическое изменение (мутация) кода программы; архивация кода программы; шифрование кода программы); обнаружение и затруднение отладки (выявление 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.  Изучение литературы по вопросам:  защита программ от 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; недостатки защиты с помощью протекторов. Защита 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.  Изучение литературы по вопросам:  - виды РПВ.  - модели работы (воздействия на компьютерные системы) ПЗ на компьютеры.  - трояны и руткиты;  - защита от троянов и руткитов.  - вредоносные программы для мобильных устройств;  - белый и черный ящики (Blacklisting и Whitelisting);  - внедрение вредоносного ПО через автозагрузку (реестр и Планировщик Windows)  Исследование программ статическим методом. Изучение общих принципов дизассемблирования и работы в IDA  Исследование программ статическим методом. Возможные уязвимости парольной защиты программ  Исследование программ статическим методом. Защита программ от исследования статическим методом  Исследование программ динамическим методом. Изучение упакованных программ с помощью отладчика OllyDbg  Исследование программ динамическим методом. Защита программ от исследования динамическим методом | 5  5  4  4  4  4  4  4 |
| Раздел 3. Защита данных | Самостоятельная работа обучающегося  Самостоятельная работа обучающегося  Самостоятельная работа обучающегося  Самостоятельная работа обучающегося  Самостоятельная работа обучающегося  Лабораторная работа | Изучение литературы по вопросам:  - средства шифрования данных  - использование RAID-массивов  - архивирование с паролем  - устранение (отключение) потенциальных опасностей хищения данных  - устранение опасностей потери данных.  Изучение литература по вопросам:  - примеры систем DLP;  - сравнение систем DLP.  Изучение литература по вопросам:  - средства шифрования данных в ОС Windows;  - сертифицированные и бесплатные программные средства гарантированного уничтожения данных  Изучение документации по программным средствам резервного копирования  Изучение документации по программным средствам восстановления данных и разделов  Защита данных с использованием средств, встроенных в редакторы текста | 2  2  2  2  4  4 |
| Раздел 4. Программные и программно-технические средства обеспечения безопасности (не защита программ и данных) | Самостоятельная работа обучающегося  Самостоятельная работа обучающегося  Самостоятельная работа обучающегося  Самостоятельная работа обучающегося  Самостоятельная работа обучающегося | Изучение литературы электронным замкам  Изучение литературы по СЗИ SecretNet и  Страж.  Изучение литературы по средствам безопасной аутентификации.  Изучение литературы по программным средствам контроля целостности программ  и данных  Изучение литературы по средствам генерации паролей | 4  4  4  2  2 |
| Подготовка к экзамену в течение семестра | Контроль |  | 44,65 |

Выбор форм и видов работы с обучающимися с ограниченными возможностями здоровья и инвалидов осуществляется с учетом их способностей, особенностей восприятия и готовности к освоению учебного материала.

**5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

1. Защита программ и данных. Часть 1: методические указания к лабораторным работам / Рязан. гос. радиотехн. ун-т; сост.: Ю.М. Кузьмин, Т.И. Калинкина. Рязань, 2019. 64 с. (№ 5486).
2. Защита программ и данных. Часть 2. Исследование программ динамическим методом: методические указания к лабораторным работам / Рязан. гос. радиотехн. ун-т; сост.: Ю.М. Кузьмин, Т.И. Калинкина; под ред. В.Н. Пржегорлинского. - Рязань, 2020. - 48 с.
3. Проскурин В.Г. Защита программ и данных: уч. пособие для студ. учреждений высш. проф. образования. - М.: Издательский центр «Академия», 2011. 208 с.
4. Казарин О.В. Программно-аппаратные средства ЗИ. Защита ПО. - М.: Изд-во Юрайт, 2017. - 312 с.
5. Юричев Д. Reverse Engineering для начинающих. - Электрон. текстовые данные.— Режим доступа: https://beginners.re/RE4B-RU.pdf
6. Методы и средства защиты информации : метод. указ. к лаб. работам / Белай К.Ю., Сухов В.Е. ; РГРТУ. - Рязань, 2013. - 16с. - 48 экз.
7. Евдокимова Л.М. Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учеб. пособие / РГРТУ. - М. : КУРС : ИНФРА-М, 2017. - 294с. - 40 экз.
8. Швечков В.А., Швечкова О.Г. Методы контроля, обеспечения достоверности и защиты информационного и программного обеспечения. Защита от разрушающих программных средств : метод. указ. к лаб. работе. - РГРТУ, Рязань, 2014. - 16с. - 20 экз.
9. Программно-аппаратные средства обеспечения информационной безопасности: методические указания к лабораторным работам. / Рязан. гос. радиотехн. ун-т.; сост. Ю.М. Кузьмин, В.А. Кураксин, В.Н. Прежегорлинский Рязань, 2018. 48 с. (60 экз.)
10. Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс] : учебно-методическое пособие / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 218 c. — 978-5-4487-0297-6. — Режим доступа: http://www.iprbookshop.ru/77317.html.
11. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html.
12. Помешкин А.А. Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса «SECRET NET 5.0» [Электронный ресурс] : учебно-методическое пособие / А.А. Помешкин, И.В. Коротких. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2012. — 47 c. — 978-5-7782-1990-8. — Режим доступа: http://www.iprbookshop.ru/45015.html.
13. Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. — Электрон. текстовые данные. — Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. — 224 c. — 978-5-9515-0305-3. — Режим доступа: http://www.iprbookshop.ru/60959.html.
14. Джонс К.Д. Инструментальные средства обеспечения безопасности [Электронный ресурс] / К.Д. Джонс, М. Шема, Б.С. Джонсон. — 2-е изд. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 914 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/73679.html.
15. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс] : учебное пособие / Ю.Н. Сычев. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 195 c. — 978-5-4487-0128-3. — Режим доступа: http://www.iprbookshop.ru/72345.html.
16. Ермаков Д.Г. Применение антивирусных программ для обеспечения информационной безопасности [Электронный ресурс] / Д.Г. Ермаков, А.В. Присяжный. — Электрон. текстовые данные. — Екатеринбург: Уральский федеральный университет, ЭБС АСВ, 2013. — 64 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66577.html.
17. Антивирусная защита компьютерных систем [Электронный ресурс] / НОУ «Интуит», URL: http://www.intuit.ru/studies/courses/2259/155/info.
18. Калмыков И.А. Компьютерная криминалистика [Электронный ресурс] : лабораторный практикум / И.А. Калмыков, В.С. Пелешенко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2017. — 84 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/69392.html.
19. Соколов В.П. Кодирование в системах защиты информации [Электронный ресурс] : учебное пособие / В.П. Соколов, Н.П. Тарасова. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 94 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61485.html.
20. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 544 c. — 978-5-4488-0074-0. — Режим доступа: http://www.iprbookshop.ru/63592.html.
21. VipNet Генератор паролей. Руководство пользователя. - Электрон. текстовые данные.— Режим доступа: https://docplayer.ru/41755058-Vipnet-generator-paroley.html.
22. [Сертифицированный программный генератор надежных паролей](https://npo-echelon.ru/news/7317/) «Генератор» (НПО «Эшелон») - Электрон. текстовые данные.— Режим доступа: https://npo-echelon.ru/news/7317/.
23. Знакомство с InfoWatch Traffic Monitor - Электрон. текстовые данные.— Режим доступа: https://www.infowatch.ru/sites/default/files/products/tme/6d5/TM\_6\_5\_300916.pdf.

Для обеспечения самостоятельной работы разработаны и предоставляются студентам демонстрационные материалы лекций.

**6. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

Оценочные материалы по данной дисциплине приведены в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Защита программ и данных»).

**7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

* + - * 1. **основная учебная литература**

1. Защита программ и данных. Часть 1: методические указания к лабораторным работам / Рязан. гос. радиотехн. ун-т; сост.: Ю.М. Кузьмин, Т.И. Калинкина. Рязань, 2019. 64 с. (№ 5486).
2. Защита программ и данных. Часть 2. Исследование программ динамическим методом: методические указания к лабораторным работам / Рязан. гос. радиотехн. ун-т; сост.: Ю.М. Кузьмин, Т.И. Калинкина; под ред. В.Н. Пржегорлинского. - Рязань, 2020. - 48 с.
3. Проскурин В.Г. Защита программ и данных: уч. пособие для студ. учреждений высш. проф. образования. - М.: Издательский центр «Академия», 2011. 208 с.
4. Казарин О.В. Программно-аппаратные средства ЗИ. Защита ПО. - М.: Изд-во Юрайт, 2017. - 312 с.
5. Юричев Д. Reverse Engineering для начинающих. - Электрон. текстовые данные.— Режим доступа: https://beginners.re/RE4B-RU.pdf
6. Методы и средства защиты информации : метод. указ. к лаб. работам / Белай К.Ю., Сухов В.Е. ; РГРТУ. - Рязань, 2013. - 16с. - 48 экз.
7. Евдокимова Л.М. Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учеб. пособие / РГРТУ. - М. : КУРС : ИНФРА-М, 2017. - 294с. - 40 экз.
8. Швечков В.А., Швечкова О.Г. Методы контроля, обеспечения достоверности и защиты информационного и программного обеспечения. Защита от разрушающих программных средств : метод. указ. к лаб. работе. - РГРТУ, Рязань, 2014. - 16с. - 20 экз.
9. Программно-аппаратные средства обеспечения информационной безопасности: методические указания к лабораторным работам. / Рязан. гос. радиотехн. ун-т.; сост. Ю.М. Кузьмин, В.А. Кураксин, В.Н. Прежегорлинский Рязань, 2018. 48 с. (60 экз.)
10. Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс] : учебно-методическое пособие / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 218 c. — 978-5-4487-0297-6. — Режим доступа: http://www.iprbookshop.ru/77317.html.
11. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html.
12. Помешкин А.А. Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса «SECRET NET 5.0» [Электронный ресурс] : учебно-методическое пособие / А.А. Помешкин, И.В. Коротких. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2012. — 47 c. — 978-5-7782-1990-8. — Режим доступа: http://www.iprbookshop.ru/45015.html.
13. Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. — Электрон. текстовые данные. — Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. — 224 c. — 978-5-9515-0305-3. — Режим доступа: http://www.iprbookshop.ru/60959.html.
14. Джонс К.Д. Инструментальные средства обеспечения безопасности [Электронный ресурс] / К.Д. Джонс, М. Шема, Б.С. Джонсон. — 2-е изд. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 914 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/73679.html.
15. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс] : учебное пособие / Ю.Н. Сычев. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 195 c. — 978-5-4487-0128-3. — Режим доступа: http://www.iprbookshop.ru/72345.html.
16. Ермаков Д.Г. Применение антивирусных программ для обеспечения информационной безопасности [Электронный ресурс] / Д.Г. Ермаков, А.В. Присяжный. — Электрон. текстовые данные. — Екатеринбург: Уральский федеральный университет, ЭБС АСВ, 2013. — 64 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66577.html.
17. Антивирусная защита компьютерных систем [Электронный ресурс] / НОУ «Интуит», URL: http://www.intuit.ru/studies/courses/2259/155/info.
18. Калмыков И.А. Компьютерная криминалистика [Электронный ресурс] : лабораторный практикум / И.А. Калмыков, В.С. Пелешенко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2017. — 84 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/69392.html.
19. Соколов В.П. Кодирование в системах защиты информации [Электронный ресурс] : учебное пособие / В.П. Соколов, Н.П. Тарасова. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 94 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61485.html.
20. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 544 c. — 978-5-4488-0074-0. — Режим доступа: http://www.iprbookshop.ru/63592.html.
21. VipNet Генератор паролей. Руководство пользователя. - Электрон. текстовые данные.— Режим доступа: https://docplayer.ru/41755058-Vipnet-generator-paroley.html.
22. Сертифицированный программный генератор надежных паролей «Генератор» (НПО «Эшелон») - Электрон. текстовые данные.— Режим доступа: https://npo-echelon.ru/news/7317/.
23. Знакомство с InfoWatch Traffic Monitor - Электрон. текстовые данные.— Режим доступа: https://www.infowatch.ru/sites/default/files/products/tme/6d5/TM\_6\_5\_300916.pdf.
    * + - 1. **дополнительная учебная литература**
24. Скрипник Д.А. Обеспечение безопасности персональных данных [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 121 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52153.html.
25. Петренко В.И. Защита персональных данных в информационных системах [Электронный ресурс] : учебное пособие / В.И. Петренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 201 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66023.html.
26. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 424 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52161.html.
27. Иванов М., Михайлов Д., Чугунков И. Защита информации в электронных платежных системах [Электронный ресурс] / НОУ «Интуит», Режим доступа: http://www.intuit.ru/studies/courses/3580/822/info.

**8** ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ, **НЕОБХОДИМЫХ ДЛЯ** ОСВОЕНИЯ **ДИСЦИПЛИНЫ**

1. Электронно-библиотечная система «Лань». – Режим доступа: доступ из корпоративной сети РГРТУ – свободный (без пароля). URL: <https://e.lanbook.com/>
2. Электронно-библиотечная система «IPRbooks». – Режим доступа: доступ из корпоративной сети РГРТУ – свободный (без пароля), доступ из сети Интернет - по паролю. URL: <https://iprbookshop.ru/>.
3. Электронная библиотека РГРТУ. URL: http://elib.rsreu.ru/ . Режим доступа: из корпоративной сети РГРТУ – по паролю.
4. Научная электронная библиотека eLibrary. URL: http//e.lib/vlsu.ru/www.uisrussia.msu.ru/elibrary.ru.
5. Библиотека и форум по программированию. URL: <http://www.cyberforum.ru>
6. Национальный открытый университет ИНТУИТ. URL: <http://www.intuit.ru/>

**9 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ**

Успешное изучение дисциплины требует посещения лекций, активной работы на лабораторных работах и практических занятиях, выполнения всех учебных заданий преподавателя, ознакомления с основной и дополнительной литературой в рамках самостоятельной работы.

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

- посещение всех лекции и практических занятий;

- изучение конспекта лекции в тот же день, после лекции (10 – 15 минут);

- изучение конспекта лекции за день перед следующей лекцией (10 – 15 минут);

- изучение теоретического материала по учебнику и конспекту (1 час в неделю);

- прежде чем посетить следующую лекцию, добейтесь того, чтобы вам было полностью понятно содержание всего предыдущего материала;

- выполняйте все задания в установленный срок;

- работайте регулярно, не накапливайте не понятое и не сданное.

Кроме чтения учебной литературы из обязательного списка рекомендуется активно использовать информационные ресурсы сети Интернет по изучаемой теме.

Самостоятельное изучение тем дисциплины способствует:

- закреплению знаний, умений и навыков, полученных в ходе аудиторных занятий;

- углублению и расширению знаний по отдельным вопросам и темам дисциплины.

Самостоятельная работа как вид учебной работы может использоваться на лекциях, практических занятиях, а также иметь самостоятельное значение – внеаудиторная самостоятельная работа обучающихся – при подготовке к практическим занятиям, лабораторным работам, подготовке к зачету и экзамену.

Основными видами самостоятельной работы по дисциплине являются:

- изучение конспектов лекций при подготовке к практическим занятиям, лабораторным работам и при подготовке к экзамену;

- самостоятельное изучение отдельных вопросов дисциплины с применением учебников и дополнительной литературы;

- самостоятельная работа перед и при выполнении лабораторных работ.

**10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ**

В рамках реализации образовательной программы при проведении занятий по дисциплине используются следующие информационные технологии:

* удаленные информационные коммуникации между студентами и преподавателем, ведущим лекционные и практические занятия, посредством электронной почты, позволяющие осуществлять оперативный контроль графика выполнения и содержания лабораторных работ и практических занятий, решение организационных вопросов, удаленное консультирование;
* поиск актуальной информации для выполнения самостоятельной работы и практических заданий;
* доступ к информационным справочным системам.

**Перечень лицензионного программного обеспечения:**

|  |  |  |
| --- | --- | --- |
| **Название ПО** | **№ лицензии** | **Количество мест** |
| Справочная правовая система «Консультант Плюс» | договор №1342/455-100 | без ограничений |
| Операционная система Windows | номер подписки 700102019; ID 700565239 | бессрочно |
| Kaspersky Endpoint Security | №2304-180222-115814-600-1595 | На 1000 |
| Adobe Acrobat Reader | свободно распространяемая | без ограничений |
| LibreOffice | свободно распространяемая | без ограничений |
| Средство виртуализации VMware Player | свободно распространяемая | без ограничений |

**11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

|  |  |  |
| --- | --- | --- |
| **№** | **Наименование специальных помещений и помещений для самостоятельной работы** | **Перечень специализированного оборудования** |
| 1 | Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 270 главного учебного корпуса | Проектор – 1 шт.  Экран – 1 шт.  Доска магнитно-маркерная 120\*200 см |
| 2 | Учебная аудитория для проведения практических занятий, лабораторных работ и самостоятельной работы № 268 главного учебного корпуса | Персональный компьютер - 16 шт.  Возможность подключения к сети «Интернет» проводным или беспроводным способом и обеспечением доступа в электронную информационно-образовательную среду РГРТУ |

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по специальности 10.05.01 – Компьютерная безопасность.

Программу составил:

доцент кафедры

«Информационная безопасность» Ю.М. Кузьмин

Программа рассмотрена и одобрена на заседании кафедры «Информационная безопасность» «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2\_\_\_ г., протокол № \_\_\_.

Заведующий кафедрой

«Информационная безопасность» В.Н. Пржегорлинский