**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**

**ФТД.В.02 «Управление**

**информационной безопасностью»**

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 «Управление информационной безопасностью» 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 дисциплины** является получение обучающимися знаний, формирование у них умений и навыков, необходимых при разработке политик безопасности организации и администрирования систем обеспечения информационной безопасности для решения задач в профессиональной деятельности..

**Задачами дисциплины** являются:

− получение знаний об основных уязвимостях и угрозах безопасности информации, моделях угроз и нарушителя в автоматизированных системах, принципах формирования политики информационной безопасности в автоматизированных системах; рисках информационной безопасности в автоматизированных системах; методах и мерах по управлению информационной безопасностью в автоматизированных системах и оценке эффективности принятых мер;

− приобретение умения выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; проводить мониторинг угроз безопасности автоматизированных систем; разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; разрабатывать корпоративную и частные политики информационной безопасности автоматизированных систем; оценивать информационные риски в автоматизированных системах; составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем;

− приобретение практических навыков управления информационной безопасностью автоматизированных систем; разработки политик информационной безопасности, анализа информационной инфраструктуры автоматизированной системы и степени ее текущей безопасности, участия в экспертизе состояния защищенности информации на объекте защиты; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.

**Перечень планируемых результатов обучения по дисциплине**

|  |  |  |
| --- | --- | --- |
| **Коды**  **компетенций** | **Результаты освоения ООП.**  **Содержание**  **компетенции** | **Перечень планируемых результатов**  **обучения по дисциплине** |
| 1 | 2 | 3 |
| **ОПК-5** | Способность использовать нормативные правовые акты в своей профессиональной деятельности | **Знать**:  - нормативно-правовые акты и принципы формирования политики информационной безопасности в компьютерных системах;  - принципы формирования политики информационной безопасности в автоматизированных системах.  **Уметь**:  - применять нормативные правовые акты при разработке политик информационной безопасности компьютерных системах;  - разрабатывать предложения по совершенствованию системы управления информационной безопасностью акомпьютерных систем.  **Владеть**:  - навыками поиска необходимых нормативных актов в профессиональной деятельности;  - навыками разработки и анализа документации по системе управления информационной безопасностью компьютерных систем. |
| **ПК-8** | Способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы | **Знать**:  - основные угрозы безопасности информации и модели нарушителя в компьютерных системах;  - принципы формирования политики информационной безопасности в компьютерных системах и контроля эффективности ее реализации.  **Уметь**:  - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;  - разрабатывать модели угроз и нарушителей информационной безопасности компьютерных систем;  - оценивать информационные риски в компьютерных системах;  - определять комплекс мер для обеспечения информационной безопасности в компьютерных системах;  - разрабатывать политики информационной безопасности информационной безопасности компьютерных систем;  - строить системы управления информационной безопасностью в различных условиях функционирования защищаемых компьютерных систем;  **Владеть**:  - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;  - определения комплекса мер для обеспечения информационной безопасности в компьютерных системах. |
| **ПК-10** | Способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации | **Знать**:  - основные угрозы безопасности информации и модели нарушителей безопасности информации в компьютерных системах;  - основные механизмы информационной безопасности и типовые процессы управления этими механизмами в компьютерных системах;  - особенности защиты информации на предприятиях различных форм собственности;  - методы и средства оценки эффективность реализации систем защиты информации и действующих политик безопасности;  - принципы разработки предложений по совершенствованию системы систем защиты информации, действующих политик безопасности и системы управления информационной безопасности в компьютерных системах.  **Уметь**:  - проводить анализ и оценку эффективность реализации систем защиты информации и действующих политик безопасности;  - строить системы управления информационной безопасностью в различных условиях функционирования защищаемых компьютерных систем;  - оценивать и контролировать эффективность принятых мер по реализации политик информационной безопасности компьютерных систем.  - разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем.  **Владеть**:  - методами и средствами выявления угроз безопасности компьютерных систем;  - навыками анализа информационной инфраструктуры компьютерной системы и ее безопасности;  - навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем. |

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

Дисциплина ФТД.В.02 «Управление информационной безопасностью» относится к вариативной 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 3-ом курсе в 5-ом семестре.

*Пререквизиты дисциплины*.

Для освоения дисциплины «Управление информационной безопасностью» обучающиеся должны обладать компетенциями, полученными в результате освоения следующих дисциплин:

- «Правовое регулирование в сфере информационно-коммуникационных технологий»;

*Взаимосвязь с другими дисциплинами*.

Дисциплина «Управление информационной безопасностью» содержательно и методологически взаимосвязана с другими дисциплинами, такими как «Криптографические методы защиты информации».

*Постреквизиты дисциплины.*

Компетенции, полученные в результате освоения дисциплины «Управление информационной безопасностью», необходимы обучающемуся при изучении следующих дисциплин:

- «Спецдисциплина 5»;

- «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 2 зачетных единицы (ЗЕ), 72 часа для очной формы обучения, изучается на 3-ем курсе в 5 семестре обучения.

|  |  |
| --- | --- |
| **Вид учебной работы** | **Всего часов** |
| Общая трудоемкость дисциплины,  в том числе: | 72 |
| Контактная работа обучающихся с преподавателем (всего),  в том числе: | 32,25 |
| Лекции | 32 |
| Лабораторные работы (ЛР) |  |
| Практические занятия (ПЗ) |  |
| Иная контактная работа (ИКР) | 0,25 |
| Консультация (Кнс) |  |
| Самостоятельная работа обучающихся (всего),  в том числе: | 39,75 |
| Контроль, подготовка к зачету | 8,75 |
| Иные виды самостоятельной работы | 31 |
| Форма промежуточной аттестации - зачет |  |

**4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ**

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

|  |  |
| --- | --- |
| **Раздел дисциплины** | **Содержание** |
| 1. Введение в дисциплину. Базовая терминология | Цели, задачи, содержание дисциплины, планируемые результаты обучения по дисциплине. Система. Системный подход. Процесс. Процессный подход. Управление. Циклическая модель улучшения процессов. Системный подход к управлению организацией. Процессный подход к управлению организацией. Информационная безопасность. |
| 2. Стандартизация систем и процессов УИБ | Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности».  Стандарты на отдельные процессы управлении ИБ и оценку безопасности ИТ: ISO/IEC 13335 - методы и средства обеспечения безопасности информационных технологий, ISO/IEC 15408 и ISO/IEC 18045 - Общие критерии и методология оценки безопасности информационных технологий, ISO 19011:2018 и ГОСТ Р ИСО 19011-2012 - Рекомендации по аудиту систем менеджмента, BS 25999 и ГОСТ Р 53647 - Управление непрерывностью бизнеса.  Законы о Банке Росии - Федеральный закон от 10 июля 2002 г. N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)" и Федеральный закон от 27 июня 2011 г. N 161-ФЗ «О национальной платежной системе».  ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер (уровни защиты). ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия (оценка соответствия уровней защиты).  Отраслевые стандарты в области управления ИБ - стандарты Банка России, рекомендации Банка России и положения Банка России по защите информации. |
| 3. Политика информационной безопасности | Понятия политики обеспечения ИБ и политики ИБ организации. Причины выработки политики ИБ. Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ.  Содержание политики ИБ: содержание корпоративной политики ИБ, содержание частных политик ИБ, примеры частных политик ИБ.  Жизненный цикл политики ИБ: разработка политики ИБ, внедрение политики ИБ, применение политики ИБ, аннулирование политики ИБ, ответственность за исполнение политики ИБ. |
| 4.Управление и система управления информационной безопасностью | Необходимость управления обеспечением ИБ организации. Деятельность по обеспечению ИБ организации как процесс. Определение управления ИБ организации. Управление ИБ информационно-телекоммуникационных технологий организации.  Система управления ИБ организации: область действия СУИБ, документальное обеспечение СУИБ, политика СУИБ, поддержка СУИБ со стороны руководства организации.  Процессный подход в рамках управления ИБ: планирование СУИБ, реализация СУИБ, проверка СУИБ, совершенствование СУИБ.  Работа с процессами СУИБ организации: задание процесса СУИБ, идентификация процессов СУИБ организации, документирование и описание процесса СУИБ, мониторинг и измерение параметров процесса СУИБ.  Стратегии построении и внедрения СУИБ: построение и внедрение СУИБ в целом, построение и внедрение процессов СУИБ по отдельности. |
| 5. Оценка и управление рисками информационной безопасности | Основные определения.  Нормативное обеспечение управления рисками информационной безопасности.  Оценка рисков информационной безопасности.  Обработка рисков информационной безопасности.  Принятие и мониторинг рисков информационной безопасности.  Обеспечение управления рисками информационной безопасности. |
| 6. Управление инцидентами ИБ и обеспечение непрерывности бизнеса | Нормативная база управления инцидентами ИБ и обеспечение непрерывности бизнеса. Стандарт ISO 27035. Идентификация, протоколирование, реагирование на инциденты ИБ. Влияние инцидентов ИБ на бизнес-процессы.  Средства управления событиями ИБ. SOC-центры ИБ, SIEM-системы управления информацией о безопасности и событиями информационной безопасности, IRP-системы автоматизации реагирования на инциденты информационной безопасности  Управление непрерывностью бизнеса организации. |
| 7. Процессы проверки системы управления ИБ и оценка деятельности по управлению ИБ | Нормативное обеспечение проверки и оценки деятельности по управлению информационной безопасностью.  Аудит СУИБ. Процесс аудита. Внутренний и внешний аудит. Аудит первой, второй и третьей сторонами. Подготовка к выполнению аудита. Подготовка и представление отчетов в устной и письменной форме о результатах аудита. Принятие решений о необходимости соответствующих последующих аудиторских проверок.  Оценка деятельности по управлению информационной безопасностью. |

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 | 1. Введение в дисциплину. Базовая терминология | ***7*** | ***4*** | ***4*** |  |  |  |  |  | ***3*** |
| 2 | 2. Стандартизация систем и процессов УИБ | ***8*** | ***4*** | ***4*** |  |  |  |  |  | ***4*** |
| 3 | 3. Политика информационной безопасности | ***8*** | ***4*** | ***4*** |  |  |  |  |  | ***4*** |
| 4 | 4.Управление и система управления информационной безопасностью | ***10*** | ***5*** | ***5*** |  |  |  |  |  | ***5*** |
| 5 | 5. Оценка и управление рисками информационной безопасности | ***10*** | ***5*** | ***5*** |  |  |  |  |  | ***5*** |
| 6 | 6. Управление инцидентами ИБ и обеспечение непрерывности бизнеса | ***10*** | ***5*** | ***5*** |  |  |  |  |  | ***5*** |
| 7 | 7. Процессы проверки системы управления ИБ и оценка деятельности по управлению ИБ | ***10*** | ***5*** | ***5*** |  |  |  |  |  | ***5*** |
| 9 | Иная контактная работа | ***0,25*** | ***0,25*** |  |  |  | ***0,25*** |  |  |  |
| 10 | Контроль | ***8,75*** |  |  |  |  |  |  | ***8,75*** |  |
| 11 | Консультации |  |  |  |  |  |  |  |  |  |
| 12 | Всего по дисциплине | ***72*** | ***32,25*** | ***32*** |  |  | ***0,25*** |  | ***8,75*** | ***31*** |

Виды практических, лабораторных и самостоятельных работ

| Раздел | Вид работы | Наименование и содержание работы | Трудоемкость, часов |
| --- | --- | --- | --- |
| 1. Введение в дисциплину. Базовая терминология | Самостоятельная работа обучающегося | Изучение литературы и конспекта лекций | 3 |
| 2. Стандартизация систем и процессов УИБ | Самостоятельная работа обучающегося | Изучение литературы и конспекта лекций. | 4 |
| 3. Политика информационной безопасности | Самостоятельная работа обучающегося | Изучение литературы и конспекта лекций. | 4 |
| 4.Управление и система управления информационной безопасностью | Самостоятельная работа обучающегося | Изучение литературы и конспекта лекций. | 5 |
| 5. Оценка и управление рисками информационной безопасности | Самостоятельная работа обучающегося | Изучение литературы и конспекта лекций. | 5 |
| 6. Управление инцидентами ИБ и обеспечение непрерывности бизнеса | Самостоятельная работа обучающегося | Изучение литературы и конспекта лекций. | 5 |
| 7. Процессы проверки системы управления ИБ и оценка деятельности по управлению ИБ | Самостоятельная работа обучающегося | Изучение литературы и конспекта лекций. | 5 |
| Подготовка к зачету в течение семестра | Контроль |  | 8,75 |

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. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : лабораторный практикум / М.А. Лапина [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 242 c. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/62945.html>
2. Пелешенко В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления [Электронный ресурс] : учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2017. — 86 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/69405.html
3. Информационная безопасность при управлении техническими системами [Электронный ресурс] : учебное пособие / С.Ф. Баркалов [и др.]. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 528 c. — 978-5-4383-0133-2. — Режим доступа: <http://www.iprbookshop.ru/68589.html>
4. Программно-аппаратные средства защиты информации [Электронный ресурс] : учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность» / Л.Х. Мифтахова [и др.] – Электрон. текстовые данные. – СПб. : Интермедия, 2018 – 408 с. – 978-5-4383-0157-8. – Режим доступа: <http://www.iprbookshop.ru/736443.html>
5. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 212 c. — 978-5-9963-0237-6. — Режим доступа: <http://www.iprbookshop.ru/52182.html>
6. 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

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 «Управление информационной безопасностью»).

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

**а) основная литература:**

1. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : лабораторный практикум / М.А. Лапина [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 242 c. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/62945.html>
2. Пелешенко В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления [Электронный ресурс] : учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2017. — 86 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/69405.html
3. Информационная безопасность при управлении техническими системами [Электронный ресурс] : учебное пособие / С.Ф. Баркалов [и др.]. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 528 c. — 978-5-4383-0133-2. — Режим доступа: <http://www.iprbookshop.ru/68589.html>
4. Программно-аппаратные средства защиты информации [Электронный ресурс] : учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность» / Л.Х. Мифтахова [и др.] – Электрон. текстовые данные. – СПб. : Интермедия, 2018 – 408 с. – 978-5-4383-0157-8. – Режим доступа: <http://www.iprbookshop.ru/736443.html>

**б) дополнительная литература**

1. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 212 c. — 978-5-9963-0237-6. — Режим доступа: <http://www.iprbookshop.ru/52182.html>
2. 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

**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;

- 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, а также иметь самостоятельное значение – внеаудиторная самостоятельная работа обучающихся – при подготовке к зачету.

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.

**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