



|  |  |  |
| --- | --- | --- |
| УП: v15.04.04\_20\_00.plx |  | стр. 4 |
|  |  |  |  |
|  |
|  |  |  |  |
|  |
|  |  |  |  |
| **Визирование РПД для исполнения в очередном учебном году** |
|  |  |  |  |
| Рабочая программа пересмотрена, обсуждена и одобрена дляисполнения в 2021-2022 учебном году на заседании кафедры |
| **Автоматизация информационных и технологических процессов** |
|  |  |  |  |
|  | Протокол от \_\_ \_\_\_\_\_\_\_\_\_\_ 2021 г. № \_\_Зав. кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |  |
|  |
|  |  |  |  |
|  |
|  |  |  |  |
| **Визирование РПД для исполнения в очередном учебном году** |
|  |  |  |  |
| Рабочая программа пересмотрена, обсуждена и одобрена дляисполнения в 2022-2023 учебном году на заседании кафедры |
| **Автоматизация информационных и технологических процессов** |
|  |  |  |  |
|  | Протокол от \_\_ \_\_\_\_\_\_\_\_\_\_ 2022 г. № \_\_Зав. кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |  |
|  |
|  |  |  |  |
|  |
|  |  |  |  |
| **Визирование РПД для исполнения в очередном учебном году** |
|  |  |  |  |
| Рабочая программа пересмотрена, обсуждена и одобрена дляисполнения в 2023-2024 учебном году на заседании кафедры |
| **Автоматизация информационных и технологических процессов** |
|  |  |  |  |
|  | Протокол от \_\_ \_\_\_\_\_\_\_\_\_\_ 2023 г. № \_\_Зав. кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |  |
|  |
|  |  |  |  |
|  |
|  |  |  |  |
| **Визирование РПД для исполнения в очередном учебном году** |
|  |  |  |  |
| Рабочая программа пересмотрена, обсуждена и одобрена дляисполнения в 2024-2025 учебном году на заседании кафедры |
|  |  |  |  |
| **Автоматизация информационных и технологических процессов** |
|  |  |  |  |
|  | Протокол от \_\_ \_\_\_\_\_\_\_\_\_\_ 2024 г. № \_\_Зав. кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |  |
| --- | --- | --- |
| УП: v15.04.04\_20\_00.plx |  | стр. 5 |
| **1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)** |
| 1.1 | Целью освоения дисциплины «Основы информационной безопасности» является приобретение навыков защиты данных в автоматизированных информационных системах (АИС) и разработки политики безопасности информации, изучение видов политики безопасности и основных направлений защиты информации. |
|  |  |  |  |  |
| **2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ** |
| Цикл (раздел) ОП: | Б1.Б |
| **2.1** | **Требования к предварительной подготовке обучающегося:** |
| 2.1.1 | Знать: |
| 2.1.2 | - принципы организации и планирования автоматизированных производств; |
| 2.1.3 | - состав информационного и программного обеспечения автоматизированных производств; |
| 2.1.4 | - основы моделирования информационных систем. |
| 2.1.5 | Уметь: |
| 2.1.6 | - обследовать и формализовать информационные потоки на предприятии. |
| 2.1.7 | Владеть: |
| 2.1.8 | -программными средствами, используемыми для построения систем защиты информации. |
| **2.2** | **Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:** |
| 2.2.1 | Автоматизация научных исследований |
| 2.2.2 | Базы данных |
| 2.2.3 | Практика по получению профессиональных умений и опыта профессиональной деятельности (технологическая практика) |
| 2.2.4 | Автоматизация технологических процессов |
| 2.2.5 | Диагностика и надежность систем и устройств |
| 2.2.6 | Проектная деятельность в информационных технологиях |
| 2.2.7 | Научно-исследовательская работа (часть 2) |
| 2.2.8 | Подготовка к защите и процедура защиты выпускной квалификационной работы |
| 2.2.9 | Преддипломная практика |
|  |  |  |  |  |
| **3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)** |
| **ОК-2: готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения** |
| **.** |
| **Знать** роль информационного ресурса в обществе. Законы Российской Федерации в области информационной безопасности, а также требования правовой защиты на международном уровне.  |
| **Уметь** оценивать внутренние и внешние угрозы конфиденциальности и целостности информации.  |
| **Владеть** методами и способами защиты информации от преднамеренных и непреднамеренных угроз.  |
|  |  |  |  |  |
| **ОК-3: готовностью к саморазвитию, самореализации, использованию творческого потенциала** |
| **.** |
| **Знать** основные тенденции развития программных и технических средств хранения и обработки информации  |
| **Уметь** пользоваться научной литературой и другими источниками информации для повышения своей компетентности.  |
| **Владеть** навыками использования своего научного и творческого потенциала для решения поставленных задач.  |
|  |  |  |  |  |
| **ПК-9: способностью обеспечивать надежность и безопасность на всех этапах жизненного цикла продукции, выбирать системы экологической безопасности производства** |
| **.** |
| **Знать** требования к уровням защиты на всех этапах жизненного цикла продукции.  |
| **Уметь** контролировать надёжность каждого уровня защиты.  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| УП: v15.04.04\_20\_00.plx |  |  |  |  |  |  | стр. 6 |
| **Владеть** методами и способами защиты информации от преднамеренных и непреднамеренных угроз.  |
|  |  |  |  |  |  |  |  |  |  |
| **ПК-18: способностью осуществлять управление результатами научно-исследовательской деятельности и коммерциализацией прав на объекты интеллектуальной собственности, осуществлять ее фиксацию и защиту** |
| **.** |
| **Знать** основные законы РФ. нормативы и стандарты, обеспечивающие правовую защиту информации.  |
| **Уметь** организовать мероприятия, парирующие внутренние и внешние угрозы безопасности информации.  |
| **Владеть** методами и приёмами защиты информации в компьютерных системах от несанкционированного доступа, хищения и разрушения.  |
|  |  |  |  |  |  |  |  |  |  |
| **В результате освоения дисциплины (модуля) обучающийся должен** |
| **3.1** | **Знать:** |
| 3.1.1 | Понятие информационной безопасности. Распространение объектно-ориентированного подхода на информационную безопасность. Наиболее распространённые угрозы. |
| **3.2** | **Уметь:** |
| 3.2.1 | Пользовать информационными системами для анализа уровня информационной безопасности. |
| **3.3** | **Владеть:** |
| 3.3.1 | Законодательной базой информационной безопасности. Уметь применять стандарты и спецификации в области информационной безопасности |
|  |  |  |  |  |  |  |  |  |  |
| **4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)** |
| **Код занятия** | **Наименование разделов и тем /вид занятия/** | **Семестр / Курс** | **Часов** | **Компетен-****ции** | **Литература** | **Форма контроля** |
|  | **Раздел 1. Основы информационной безопасности** |  |  |  |  |  |
| 1.1 | Введение. Угрозы безопасности информации и их источники. /Тема/ | 1 | 0 |  |  |  |
| 1.2 | Роль информационного ресурса в обществе. Проблема обеспечения информационной безопасности. Классификация источников безопасности. Характеристика угроз в зависимости от вида источника. Угрозы конфиденциальности и целостности информации. /Лек/ | 1 | 1 | ОК-2 ОК-3 | Л1.1Л2.1Э1 Э2 Э3 |  |
| 1.3 | Внутренние и внешние угрозы безопасности. /Пр/ | 1 | 3 | ПК-9 ПК-18 | Л1.3Л3.1Э1 Э2 Э3 |  |
| 1.4 | Угрозы информационной безопасности Российской Федерации /Ср/ | 1 | 8 | ОК-2 ОК-3 ПК-9 ПК-18 | Л1.2Э1 Э2 Э3 |  |
| 1.5 | Политика безопасности информации. /Тема/ | 1 | 0 |  |  |  |
| 1.6 | Понятие политики безопасности. Задачи, решаемые политикой безопасности. Основные принципы политики безопасности: усиление самого слабого звена, недопустимость перехода в открытое состояние, минимизация привилегий, многоуровневая защита, разнообразие защитных средств. /Лек/ | 1 | 1 | ОК-2 ОК-3 | Л1.1Л2.1Э1 Э2 Э3 |  |
| 1.7 | Анализ периодических источников информации. /Пр/ | 1 | 3 | ПК-9 ПК-18 | Л1.3Л3.1Э1 Э2 Э3 |  |
| 1.8 | Разработка правил физической безопасности /Ср/ | 1 | 8 | ОК-2 ОК-3 ПК-9 ПК-18 | Л1.2Э1 Э2 Э3 |  |
| 1.9 | Модели политики безопасности. /Тема/ | 1 | 0 |  |  |  |
| 1.10 | Цель создания политики безопасности. Субъектно-объектная модель информационной системы. Понятие состояния системы. Понятие потока информации. Правила разграничения доступа. /Лек/ | 1 | 1 | ОК-2 ОК-3 | Л1.1Л2.1Э1 Э2 Э3 |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| УП: v15.04.04\_20\_00.plx |  |  |  |  |  |  | стр. 7 |
| 1.11 | Анализ данных из Интернет-источников. /Пр/ | 1 | 3 | ПК-9 ПК-18 | Л1.3Л3.1Э1 Э2 Э3 |  |
| 1.12 | Аутентификация и безопасность Интернет сети /Ср/ | 1 | 8 | ОК-2 ОК-3 ПК-9 ПК-18 | Л1.2Э1 Э2 Э3 |  |
| 1.13 | Виды политики безопасности. /Тема/ | 1 | 0 |  |  |  |
| 1.14 | Политика избирательного доступа. Матрица управления доступом. Принудительное управление доступом. Добровольное управление доступом. Достоинства и недостатки политики избирательного доступа. Политика полномочного доступа. Метки секретности, уровень прозрачности. Текущее значение уровня безопасности. /Лек/ | 1 | 1 | ОК-2 ОК-3 | Л1.1Л2.1Э1 Э2 Э3 |  |
| 1.15 | Политика ролевого доступа. Пользователи, роли, операции над защищаемыми объектами. Преимущества и недостатки политики ролевого доступа. /Пр/ | 1 | 3 | ПК-9 ПК-18 | Л1.3Л3.1Э1 Э2 Э3 |  |
| 1.16 | Вредоносное программное обеспечение и виды защиты /Ср/ | 1 | 8 | ОК-2 ОК-3 ПК-9 ПК-18 | Л1.2Э1 Э2 Э3 |  |
| 1.17 | Основные направления защиты информации. /Тема/ | 1 | 0 |  |  |  |
| 1.18 | Правовая защита. Правовая защита на международном уровне и на уровне Российской Федерации. Законы Российской Федерации в области информационной безопасности. Организационная защита. Инженерно- техническая защита. Физические средства защиты. Аппаратные, программные и криптографические средства защиты. Комбинированные средства защиты. /Лек/ | 1 | 1 | ОК-2 ОК-3 | Л1.1Л2.1Э1 Э2 Э3 |  |
| 1.19 | Идентификация и аутентификация. Атрибутивные и биометрические средства защиты. /Пр/ | 1 | 3 | ПК-9 ПК-18 | Л1.3Л3.1Э1 Э2 Э3 |  |
| 1.20 | Роль шифрования в информационной безопасности /Ср/ | 1 | 8 | ОК-2 ОК-3 ПК-9 ПК-18 | Л1.2Э1 Э2 Э3 |  |
| 1.21 | Угрозы безопасности информации в компьютерных системах. /Тема/ | 1 | 0 |  |  |  |
| 1.22 | Случайные угрозы. Класс преднамеренных угроз. Шпионаж и диверсии. Несанкционированный доступ к информации. Электромагнитное излучение и наводки. Несанкционированная модификация структуры. Вредительские программы. /Лек/ | 1 | 1 | ОК-2 ОК-3 | Л1.1Л2.1Э1 Э2 Э3 |  |
| 1.23 | Программное обеспечение для защиты информации. /Пр/ | 1 | 3 | ПК-9 ПК-18 | Л1.3Л3.1Э1 Э2 Э3 |  |
| 1.24 | Законы Российской Федерации в сфере информационной безопасности /Ср/ | 1 | 8 | ОК-2 ОК-3 ПК-9 ПК-18 | Л1.2Э1 Э2 Э3 |  |
| 1.25 | Защита информации от случайных угроз. /Тема/ | 1 | 0 |  |  |  |
| 1.26 | Задачи защиты информации от случайных угроз. Дублирование информации. Повышение надёжности компьютерных систем (КС). Создание отказоустойчивых КС. Блокировка ошибочных операций. Оптимизация взаимодействия пользователей и обслуживающего персонала. Минимизация ущерба от аварий и стихийных бедствий. /Лек/ | 1 | 1 | ОК-2 ОК-3 | Л1.1Л2.1Э1 Э2 Э3 |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| УП: v15.04.04\_20\_00.plx |  |  |  |  |  |  |  | стр. 8 |
| 1.27 | Защита информации от вредоносных программ. Виды вредительских программ. Характеристика и классификация компьютерных вирусов. Методы защиты от компьютерных вирусов. /Пр/ | 1 | 3 | ПК-9 ПК-18 | Л1.3Л3.1Э1 Э2 Э3 |  |
| 1.28 | Стандарты и спецификации в области информационной безопасности. /Ср/ | 1 | 8 | ОК-2 ОК-3 ПК-9 ПК-18 | Л1.2Э1 Э2 Э3 |  |
| 1.29 | Защита информации от преднамеренных угроз /Тема/ | 1 | 0 |  |  |  |
| 1.30 | Защита информации от шпионажа и диверсий. Защита информации от несанкционированного доступа. Идентификация и аутентификация. Метод паролей. Виды паролей. Противодействие угрозам съёма паролей. Использование паролей в сетях ЭВМ Защита баз данных. Защита от электромагнитного излучения и наводок. Защита от несанкционированной модификации структуры. /Лек/ | 1 | 1 | ОК-2 ОК-3 | Л1.1Л2.1Э1 Э2 Э3 |  |
| 1.31 | Криптографические методы защиты информации. Терминология. Методы моноалфавитной подстановки. Полиалфавитная подстановка. Метод перестановок. Обзор других методов криптографии. /Пр/ | 1 | 3 | ПК-9 ПК-18 | Л1.3Л3.1Э1 Э2 Э3 |  |
| 1.32 | Риски работы на персональном компьютере /Ср/ | 1 | 9 | ОК-2 ОК-3 ПК-9 ПК-18 | Л1.2Э1 Э2 Э3 |  |
| 1.33 | Контактная работа с преподавателем во время промежуточной аттестации /ИКР/ | 1 | 0,35 | ОК-2 ОК-3 ПК-9 ПК-18 | Э1 Э2 Э3 |  |
| 1.34 | Консультирование перед экзаменом /Кнс/ | 1 | 2 | ОК-2 ОК-3 ПК-9 ПК-18 | Э1 Э2 Э3 |  |
| 1.35 | Промежуточная аттестация /Экзамен/ | 1 | 44,65 | ОК-2 ОК-3 ПК-9 ПК-18 | Э1 Э2 Э3 |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)** |
|  |
| Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Основы информационной безопасности»»). |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)** |
| **6.1. Рекомендуемая литература** |
| **6.1.3. Методические разработки** |
| № | Авторы, составители | Заглавие | Издательство, год | Количество/название ЭБС |
| Л3.1 | Сычев Ю. Н. | Основы информационной безопасности : учебно- методический комплекс | Москва: Евразийский открытый институт, 2012, 342 с. | 978-5-374- 00602-5, http://www.ipr bookshop.ru/1 4642.html |
| **6.1.2. Дополнительная литература** |
| № | Авторы, составители | Заглавие | Издательство, год | Количество/название ЭБС |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| УП: v15.04.04\_20\_00.plx |  |  |  | стр. 9 |
| № | Авторы, составители | Заглавие | Издательство, год | Количество/название ЭБС |
| Л2.1 | Гультяева Т. А. | Основы информационной безопасности : учебное пособие | Новосибирск: Новосибирский государственн ый технический университет, 2018, 79 с. | 978-5-7782- 3640-0, http://www.ipr bookshop.ru/9 1640.html |
| **6.1.1. Основная литература** |
| № | Авторы, составители | Заглавие | Издательство, год | Количество/название ЭБС |
| Л1.1 | Нестеров С. А. | Основы информационной безопасности : учебное пособие | Санкт- Петербург: Лань, 2019, 324 с. | 978-5-8114- 4067-2, https://e.lanbo ok.com/book/1 14688 |
| Л1.2 | Новиков В. К. | Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) | Москва: Горячая линия- Телеком, 2017, 176 с. | 978-5-9912- 0525-2, https://e.lanbo ok.com/book/1 11084 |
| Л1.3 | Галатенко В. А. | Основы информационной безопасности | Москва: ИНТУИТ, 2016, 266 с. | 978-5-94774- 821-5, https://e.lanbo ok.com/book/1 00295 |
| **6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"** |
| Э1 | Электронная библиотечная система Издательства Лань [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://e.lanbook.com/ |
| Э2 | Электронная библиотечная система «IPRbooks» [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.iprbookshop.ru/ |
| Э3 | Электронная библиотечная система РГРТУ [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://elib.rsreu.ru//ebs//ebs |
| **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 |
| Adobe Acrobat Reader | Свободное ПО |
| Chrome | Свободное ПО |
| K-Lite Codec Pack | Свободное ПО |
| **6.3.2 Перечень информационных справочных систем** |
| 6.3.2.1 | Информационно-правовой портал ГАРАНТ.РУ http://www.garant.ru |
| 6.3.2.2 | Система КонсультантПлюс http://www.consultant.ru |
| 6.3.2.3 | Справочная правовая система «КонсультантПлюс» (договор об информационной поддержке №1342/455-100 от 28.10.2011 г.) |
|  |  |  |  |  |  |  |  |  |
| **7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)** |
| 1 | 117 учебно-административный корпус. Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Всего 28 мест (без учёта места преподавателя и работников). 14 компьютеров (без учёта компьютера преподавателя и работников), из них: 2 компьютера FORMOZA на базе Core2 - 6700 6 компьютеров PERSONAL 4 компьютеров Intel Core i-3 1 компьютер Celeron 1 компьютер Pentium 4 с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду РГРТУ. 1 мультимедиа проектор NEC - NP 200 A, 1 экран. Посадочные места: студенты - 14 столов + 28 стульев. |

|  |  |  |
| --- | --- | --- |
| УП: v15.04.04\_20\_00.plx |  | стр. 10 |
| 2 | 117а учебно-административный корпус. Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Всего 50 место (без учёта места преподавателя). 1 мультимедиа проектор BenQ 721, 1 документ-камера Aver Visio 330, 1 экран, 1 компьютер FORMOZA на базе Core2 - 6700 с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду РГРТУ. Посадочные места: студенты - 25 столов + 50 стульев. преподаватель - 1 стол + 1 стул. 1 доска аудиторная. |
|  |  |  |  |
| **8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)** |
| Методическое обеспечение дисциплины приведено в приложении к рабочей программе дисциплины (см. документ «Методические указания дисциплины «Основы информационной безопасности»»). |

|  |
| --- |
| МИНИСТРЕСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ |
|  |  |  |  |  |  |  |  |  |  |  |
| **ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ****"РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА"** |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Аннотация |  |
|  |  |  |  |  |  |  |  |  |  |  |
| **Основы информационной безопасности** |
| рабочая программа дисциплины (модуля) |
|  |  |  |  |  |  |  |  |  |  |  |
|  | Закреплена за кафедрой |  | **Автоматизация информационных и технологических процессов** |
|  |  |  |  |  |  |  |  |  |  |  |
|  | Учебный план | v15.04.04\_20\_00.plx15.04.04 АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВИ ПРОИЗВОДСТВ |
|  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | Квалификация | **магистр** |
|  |  |  |  |  |  |  |  |  |  |  |
|  | Форма обучения | **очно-заочная** |
|  |  |  |  |  |  |  |  |  |  |  |
|  | Программу составил(и): | к.т.н., доц., Дятлов Роман Николаевич |
|  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| **Распределение часов дисциплины по семестрам** |  |  |
| Семестр(<Курс>.<Семестр на курсе>) | **1 (1.1)** | Итого |  |  |
| Недель | 16 |  |  |
| Вид занятий | УП | РП | УП | РП |  |  |
| Лекции | 8 | 8 | 8 | 8 |  |  |
| Практические | 24 | 24 | 24 | 24 |  |  |
| Иная контактная работа | 0,35 | 0,35 | 0,35 | 0,35 |  |  |
| Консультирование перед экзаменом и практикой | 2 | 2 | 2 | 2 |  |  |
| Итого ауд. | 34,35 | 34,35 | 34,35 | 34,35 |  |  |
| Кoнтактная рабoта | 34,35 | 34,35 | 34,35 | 34,35 |  |  |
| Сам. работа | 65 | 65 | 65 | 65 |  |  |
| Часы на контроль | 44,65 | 44,65 | 44,65 | 44,65 |  |  |
| Итого | 144 | 144 | 144 | 144 |  |  |

|  |  |  |
| --- | --- | --- |
| УП: v15.04.04\_20\_00.plx |  | стр. 2 |
| **1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ** |
| 1.1 | Целью освоения дисциплины «Основы информационной безопасности» является приобретение навыков защиты данных в автоматизированных информационных системах (АИС) и разработки политики безопасности информации, изучение видов политики безопасности и основных направлений защиты информации. |
|  |  |  |  |  |
| **2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП** |
| Цикл (раздел) ООП: | Б1.Б |
| **2.1** | **Требования к предварительной подготовке обучающегося:** |
| 2.1.1 | Знать: |
| 2.1.2 | - принципы организации и планирования автоматизированных производств; |
| 2.1.3 | - состав информационного и программного обеспечения автоматизированных производств; |
| 2.1.4 | - основы моделирования информационных систем. |
| 2.1.5 | Уметь: |
| 2.1.6 | - обследовать и формализовать информационные потоки на предприятии. |
| 2.1.7 | Владеть: |
| 2.1.8 | -программными средствами, используемыми для построения систем защиты информации. |
| **2.2** | **Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:** |
| 2.2.1 | Автоматизация научных исследований |
| 2.2.2 | Базы данных |
| 2.2.3 | Практика по получению профессиональных умений и опыта профессиональной деятельности (технологическая практика) |
| 2.2.4 | Автоматизация технологических процессов |
| 2.2.5 | Диагностика и надежность систем и устройств |
| 2.2.6 | Проектная деятельность в информационных технологиях |
| 2.2.7 | Научно-исследовательская работа (часть 2) |
| 2.2.8 | Подготовка к защите и процедура защиты выпускной квалификационной работы |
| 2.2.9 | Преддипломная практика |
|  |  |  |  |  |
| **3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)** |
| **ОК-2: готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения** |
| **.** |
| **Знать** |
| роль информационного ресурса в обществе. Законы Российской Федерации в области информационной безопасности, а также требования правовой защиты на международном уровне. |
| **Уметь** |
| оценивать внутренние и внешние угрозы конфиденциальности и целостности информации. |
| **Владеть** |
| методами и способами защиты информации от преднамеренных и непреднамеренных угроз. |
|  |  |  |  |  |
| **ОК-3: готовностью к саморазвитию, самореализации, использованию творческого потенциала** |
| **.** |
| **Знать** |
| основные тенденции развития программных и технических средств хранения и обработки информации |
| **Уметь** |
| пользоваться научной литературой и другими источниками информации для повышения своей компетентности. |
| **Владеть** |
| навыками использования своего научного и творческого потенциала для решения поставленных задач. |
|  |  |  |  |  |
| **ПК-9:способностью обеспечивать надежность и безопасность на всех этапах жизненного цикла продукции, выбирать системы экологической безопасности производства** |
| **.** |

|  |  |  |
| --- | --- | --- |
| УП: v15.04.04\_20\_00.plx |  | стр. 3 |
| **Знать** |
| требования к уровням защиты на всех этапах жизненного цикла продукции. |
| **Уметь** |
| контролировать надёжность каждого уровня защиты. |
| **Владеть** |
| методами и способами защиты информации от преднамеренных и непреднамеренных угроз. |
|  |  |  |  |
| **ПК-18:способностью осуществлять управление результатами научно-исследовательской деятельности и коммерциализацией прав на объекты интеллектуальной собственности, осуществлять ее фиксацию и защиту** |
| **.** |
| **Знать** |
| основные законы РФ. нормативы и стандарты, обеспечивающие правовую защиту информации. |
| **Уметь** |
| организовать мероприятия, парирующие внутренние и внешние угрозы безопасности информации. |
| **Владеть** |
| методами и приёмами защиты информации в компьютерных системах от несанкционированного доступа, хищения и разрушения. |
|  |  |  |  |
| **В результате освоения дисциплины обучающийся должен** |
| **3.1** | **Знать:** |
| Понятие информационной безопасности. Распространение объектно-ориентированного подхода на информационную безопасность. Наиболее распространённые угрозы.  |
| **3.2** | **Уметь:** |
| Пользовать информационными системами для анализа уровня информационной безопасности.  |
| **3.3** | **Владеть:** |
| Законодательной базой информационной безопасности. Уметь применять стандарты и спецификации в области информационной безопасности  |