

# **1. Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы магистратуры**

Рабочая программа дисциплины «Основы информационной безопасности» является составной частью основной образовательной программы (ООП) магистратуры «Системы автоматизации информационных и технологических процессов предприятия», разработанной в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 15.04.04 Автоматизация технологических процессов и производств (уровень магистратуры), утверждённым приказом Минобрнауки России от 21*.11.2014 г. № 1484.*

**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.

**Основные задачи** **освоения дисциплины**:

1. Изучение возможных угроз безопасности информации.

2. Изучение принципов построения и основных моделей политики безопасности.

3. Изучение основных направлений защиты информации и особенностей задач защиты информации в компьютерных системах.

4. Изучение основных методов обеспечения безопасности баз данных (БД).

5. Выработка навыков и умения создавать систему информационной безопасности на предприятии.

**Компетенции** студента, формируемые в результате освоения дисциплины «Основы информационной безопасности»

|  |  |  |
| --- | --- | --- |
| **Коды****компетенции** | **Содержание****компетенций** | **Перечень планируемых результатов обучения по дисциплине** |
| ОК-2 | Готовность 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 | Готовность 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 | Способность обеспечивать надёжность 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. Владеть методами и способами защиты информации от преднамеренных и непреднамеренных угроз.  |
| ПК-18 | Способность осуществлять управление результатами научно- исследовательской деятельности и коммерциализацией прав на объекты интеллектуальной собственности, осуществлять её 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. |

**2. Место дисциплины в структуре ООП бакалавриата**

Дисциплина «Основы информационной безопасности» является обязательной и относится к базовой части дисциплин блока №1 основной профессиональной образовательной программы магистратуры «Автоматизация технологических процессов и производств» по направлению подготовки 15.04.04 «Системы автоматизации информационных и технологических процессов предприятия» ФГБОУ ВО «РГРТУ».

Дисциплина изучается по очной и очно-заочной формам обучения на 1 курсе в 1 семестре.

*Пререквизиты дисциплины*. Для освоения дисциплины обучающийся должен иметь компетенции, полученные в результате освоения дисциплин бакалавриата «Информатика», «Программирование и алгоритмизация», «Математическая логика», «Базы данных и СУБД», «Автоматизация управления жизненным циклом продукции», «Вычислительные машины, системы и сети». Для освоения дисциплины обучающийся должен:

*Знать***:**

- высшую и прикладную математику;

- принципы организации и планирования автоматизированных производств;

- состав информационного и программного обеспечения автоматизированных производств;

- основы моделирования информационных систем.

*Уметь***:**

- обследовать и формализовать информационные потоки на предприятии.

*Владеть***:**

-программными средствами, используемыми для построения систем защиты информации.

*Взаимосвязь с другими дисциплинами.*

Дисциплина «Основы информационной безопасности» содержательно и методологически взаимосвязана с дисциплинами «Проектирование единого информационного пространства виртуальных предприятий», «Базы данных», «Распределённые системы обработки информации».

*Постреквизиты дисциплины.* Компетенции, полученные в результате освоения дисциплины необходимы обучающемуся при изучении следующих дисциплин: «Проектирование единого информационного пространства виртуальных предприятий», «Базы данных», «Распределённые системы обработки информации».

**3. Объем дисциплины и виды учебной работы**

1. *Общая трудоёмкость (объем) дисциплины составляет 4 зачётных единиц (ЗЕ),
144 часа.*

|  |  |
| --- | --- |
| **Вид учебной работы** | **Всего часов** |
| Общая трудоёмкость дисциплины, в том числе: | 144 |
| Контактная работа обучающихся с преподавателем (всего), в том числе: | 36 |
| Лекции  | 6 |
| Лабораторные работы | - |
| Практические занятия | 30 |
| Самостоятельная работа (всего), том числе | 108 |
| Курсовая работа  | - |
| Консультации в семестре  | 4 |
| Экзамены и консультации | 40,5 |
| Самостоятельные занятия | 63,5 |
| Вид аттестации обучающегося  | Экзамен |

**4. Содержание дисциплины**

#### Тема 1. Введение. Угрозы безопасности информации и их источники.

#### Роль информационного ресурса в обществе. Проблема обеспечения информационной безопасности.

Классификация источников безопасности. Характеристика угроз в зависимости от вида источника. Угрозы конфиденциальности и целостности информации. Внутренние и внешние угрозы безопасности.

**Тема 2.** **Политика безопасности информации**.

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.

**Тема 3. Модели политики безопасности.**

Цель создания политики безопасности. Субъектно-объектная модель информационной системы. Понятие состояния системы. Понятие потока информации. Правила разграничения доступа.

**Тема 4. Виды политики безопасности**.

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.

Политика ролевого доступа. Пользователи, роли, операции над защищаемыми объектами. Преимущества и недостатки политики ролевого доступа.

**Тема 5. Основные направления защиты информации**.

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. Идентификация и аутентификация. Атрибутивные и биометрические средства защиты.

**Тема 6.У грозы безопасности информации в компьютерных системах**.

Случайные угрозы. Класс преднамеренных угроз. Шпионаж и диверсии. Несанкционированный доступ к информации. Электромагнитное излучение и наводки. Несанкционированная модификация структуры. Вредительские программы.

**Тема 7. Защита информации от случайных угроз**.

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.

**Тема 8. Защита информации от преднамеренных угроз**.

Защита информации от шпионажа и диверсий.

Защита информации от несанкционированного доступа. Идентификация и аутентификация. Метод паролей. Виды паролей. Противодействие угрозам съема паролей. Использование паролей в сетях ЭВМ Защита баз данных.

Защита от электромагнитного излучения и наводок. Защита от несанкционированной модификации структуры.

**Тема 9. Защита информации от вредоносных программ.**

Виды вредительских программ. Характеристика и классификация компьютерных вирусов. Методы защиты от компьютерных вирусов.

**Тема 10**. Криптографические методы защиты информации.

Терминология. Методы моноалфавитной подстановки. Полиалфавитная подстановка. Метод перестановок. Обзор других методов криптографии

**4.2. Разделы дисциплины (модуля) и трудоёмкость по видам учебных занятий (в академических часах)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Тема** | **Общая трудоёмкость, всего часов** | **Контактная работа****обучающихся**с преподавателем | **Самостоятельная работа обучающихся** |
| **всего** | **лекции** | **лабораторные работы** | **упражнения** |
| 1. | Введение. Угрозы безопасности информации и их источники. Введение. Угрозы безопасности информации и их источники | 6 | - | - | - | - | 6 |
| 2. | Политика безопасности информации | 6 | - | 2 | - | 4 | 6 |
| 3. | Модели политики безопасности | 12 | 6 | - | - | 2 | 6 |
| 4. | Виды политики безопасности | 10 | 4 | - | *-* | 4 | 7 |
| 5. | Основные направления защиты информации | 10 | 4 | - | - | 4 | 6 |
| 6. | Угрозы безопасности информации в компьютерных системах | 14 | 6 | 2 |  | 2 | 7 |
| 7. | Защита информации от случайных угроз | 16 | 10 | - | - | 4 | 6 |
| 8. | Защита информации .от преднамеренных угроз | 14 | 6 | 2 | *-* | 2 | 7,5 |
| 9. | Защита информации от вредоносных программ |  |  |  |  | 4 | 6 |
| 10. | Криптографические методы защиты информации | 16 | **-** | - | *-* | 4 | 6 |
|  | Консультации в семестре | 4 | **-** | - | *-* | **-** | 4 |
|  | Экзамены и консультации |  |  |  |  |  | 40,5 |
|  | Всего | **144** | **36** | **6** | - | **30** | **108** |

**Виды практических, лабораторных и самостоятельных работ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | Тема | Вид работы | **Наименование и содержание работы** | **Трудоемкость, часов** |
| 1. | Введение. Угрозы безопасности информации и их источники.  | Самостоятельная работа обучающегося | Изучение конспекта лекций | 6 |
| 2. | Политика безопасности информации | Самостоятельная работа обучающегося | Изучение конспекта лекций | 6 |
| Практические занятия | Основные направления защиты информации | 2 |
| Практические занятия | Основные принципы политики безопасности | 2 |
| 3. | Модели политики безопасности | Самостоятельная работа обучающегося | Изучение конспекта лекций | 6 |
| Практические занятия | Субъектно-объектная модель | 2 |
| 4. | Виды политики безопасности | Самостоятельная работа обучающегося | Изучение конспекта лекций | 7 |
| Практические занятия | Политика избирательного доступа | 2 |
| Практические занятия | Политика полномочного и ролевого доступа | 2 |
| 5. | Основные направления защиты информации | Самостоятельная работа обучающегося | Изучение конспекта лекций | 6 |
| Практические занятия | Правовая и организационная защита | 2 |
| Практические занятия | Инженерно-техническая защита | 2 |
| 6. | Угрозы безопасности информации в компьютерных системах | Самостоятельная работа обучающегося | Изучение конспекта лекций | 7 |
| Практические занятия | Виды угроз безопасности информации | 2 |
| 7. | Защита информации от случайных угроз | Самостоятельная работа обучающегося | Изучение конспекта лекций | 6 |
| Практические занятия | Виды случайных угроз | 2 |
| Практические занятия | Методы защиты информации от случайных угроз | 2 |
| 8. | Защита информации от преднамеренных угроз | Самостоятельная работа обучающегося | Изучение конспекта лекций | 7,5 |
| Практические занятия | Методы защиты информации от несанкционированного доступа | 2 |
| 9. | Защита информации от вредоносных программ | Самостоятельная работа обучающегося  | Изучение конспекта лекций | 6 |
| Практические занятия | Классификация компьютерных вирусов | 2 |
| Практические занятия | Методы защиты от компьютерных вирусов | 2 |
| 10. | Криптографические методы защиты информации | Самостоятельная работа обучающегося | Изучение конспекта лекций | 6 |
| Практические занятия | Криптографические методы защиты информации | 2 |
| Практические занятия | Контрольная работа по методам шифрования | 2 |
|  | Консультации в семестре | - | - | 4 |
|  | Экзамены и консультации |  |  | 40,5 |

**5. Перечень учебно-методического обеспечения для самостоятельной работы
 обучающихся по дисциплине**

1. Трофимова И.П., Сосулин Ю.А. Хранение и защита информации: Учеб. пособие.. – Рязань. РГРТУ, 2013. – 52 с.
2. Галатенко В. А. Основы информационной безопасности: Курс лекций / В. А. Галатенко ; Под ред. Бетелина В. Б.; Ун-т интернет. - М., 2003, 2004. – 280 с., 22 экземпляра.
3. Нестеров С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С. А. ‒ Электрон. текстовые данные. ‒ СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014. ‒ 322 c. ‒ Режим доступа: http://www.iprbookshop.ru/43960.html
4. Галатенко В. А. Основы информационной безопасности [Электронный ресурс] / В. А. Галатенко. ‒ М.: ИНТУИТ, 2016. ‒ 266 c. ‒ Режим доступа: http://www.iprbookshop.ru/52209.html

**6. Фонд оценочных средств для проведения промежуточной аттестации
 обучающихся по дисциплине**

Фонд оценочных средств приведён в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Основы информационной безопасности»»).

**7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

1. **Основная учебная литература:**
2. Сычёв Ю. Н. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Ю. Н. Сычёв. ‒ Электрон. текстовые данные. ‒ М.: Евразийский открытый институт, 2010. ‒ 328 c. ‒ Режим доступа: http://www.iprbookshop.ru/10746.html
3. Фаронов А. Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А. Е. Фаронов. ‒ Электрон. текстовые данные. ‒ М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. ‒ 154 c. ‒ Режим доступа: http://www.iprbookshop.ru/52160.html
4. Галатенко В. А. Основы информационной безопасности [Электронный ресурс] / В. А. Галатенко. ‒ М.: ИНТУИТ, 2016. ‒ 266 c. ‒ Режим доступа: http://www.iprbookshop.ru/52209.html
5. Нестеров С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С. А. ‒ Электрон. текстовые данные. ‒ СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014. ‒ 322 c. ‒ Режим доступа: http://www.iprbookshop.ru/43960.html

**Дополнительная учебная литература:**

1. Анин Б. Защита компьютерной информации. – СПт.: БХВ-Санкт-Петербург, 2000. - 368с.

2. Завгородний В.И. Комплексная защита информации в компьютерных системах: учеб. пособие. - М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. -264 с: ил.

3. Галатенко В.А. Основы информационной безопасности. Курс лекций. Учебное пособие. М.: ИНТУИТ.РУ "Интернет-университет Информационных технологий», 2004.- 264 с.

4. Шаньгин В.Ф. Информационная безопасность [ Электронный ресурс]: учеб. пособие./ Шаньгин И.Ф. – М. Изд. "ДМК ПРЕСС",2014. – 702 с. Режим доступа: http://e.lanbook/com/books/element/php?pll id=50578

5. Барсуков В.С., Водолазкий С.В. Современные технологии безопасности. – М.: Нолидж, 2000. –495 с.

6. Андрианов В. В. Зефиров С. Л. и др. Обеспечение информационной безопасности бизнеса [ Электронный ресурс]. М.: Альпина Паблишерс, 2011. – 373 с.

7. Трофимова И.П., Сосулин Ю.А. Хранение и защита информации: учеб. Пособие. – Рязань: Рязан. гос. радиотехн. ун-т. 2013. - 52 с.

8. Расторгуев С. П. Основы информационной безопасности: учеб. пособие / Расторгуев Сергей Павлович. - 2-е изд., стер. - М.: Академия, 2009. – 187 с. - (Высш. проф. образ.).

# **8.Перечень ресурсов информационно–телекоммуникационной сети Интернет, необходимых для освоения дисциплины**

1. Электронная библиотечная система IPR BOOKS. Режим доступа: http://www.iprbookshop.ru/

2. Электронные библиотеки России. Полнотекстовые pdf-учебники. –Режим доступа: <http://www.gaudeamus.omskcity.com/PDF.html>

3. Национальная электронная библиотека [Электронный ресурс]. – Электрон. дан. – Режим доступа: p://www.nns.ru/

**9. Методические** указания для обучающихся по освоению дисциплины

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

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.

Перед выполнением заданий практических занятий и лабораторных работ необходимо изучить теоретический лекционный материал по заданной теме.

**Рекомендации по работе с конспектом и литературой**

Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги по соответствующей дисциплине. Литературу по курсу рекомендуется изучать в библиотеке. Полезно использовать несколько учебников по курсу. Рекомендуется после изучения очередного очередной темы или параграфа книги ответить на несколько простых вопросов по данной теме: Например полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): «О чем этот параграф?», «Как прочитанный материал связан с ранее изученным», «Какие новые понятия введены, каков их смысл?».

# 10. Перечень информационных технологий, используемых при осуществленииобразовательного процесса по дисциплине

Для освоения дисциплины «Основы информационной безопасности» применяется следующее материально-техническое обеспечение.

1. Лекционные и практические занятия:

-аудитория, оснащённая презентационной техникой (проектор, экран, компьютер).

# 11. Описание материально-технической базы, необходимой для осуществленияобразовательного процесса по дисциплине

Для освоения дисциплины необходимы:

1. Для проведения лекционных занятий необходима аудитория с достаточным количеством посадочных мест, соответствующая необходимым противопожарным нормам и санитарно-гигиеническим требованиям;

2. Для проведения лекционных и практических занятий аудитория должна быть оснащена проекционным оборудованием, компьютерами и соответствующим программным обеспечением.

Программу составил к.т.н., доцент Р. Н. Дятлов

Программа рассмотрена и одобрена на заседании кафедры АИТП

24.05.2019 г., протокол № «10».

Зав. кафедрой АИТП А. К. Мусолин