

Министерство просвещения Российской Федерации  
Федеральное государственное автономное образовательное учреждение  
высшего образования  
«Российский государственный профессионально-педагогический университет»  
Институт инженерно-педагогического образования  
Кафедра информационных систем и технологий

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
Б1.О.07.05 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

Направление подготовки 09.03.03 Прикладная информатика

Профиль программы «Прикладная информатика (по элективным модулям)»

Автор(ы): ст. преп. С.В. Ченушкина

Одобрена на заседании кафедры информационных систем и технологий. Протокол от «20» января 2022 г. №5.

Рекомендована к использованию в образовательной деятельности научно-методической комиссией института ИПО РГППУ. Протокол от «26» января 2022 г. №6.

Екатеринбург  
2022

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины «Информационная безопасность»: формирование у студентов профессиональных знаний и умений в области информационной безопасности на предприятиях.

Задачи:

- овладение теорией и методологией информационной безопасности в современном информационном обществе;
- изучение отечественных и международных стандартов в области информационной безопасности, в том числе защиты государственной тайны;
- изучения технологий проектирования политики безопасности с использованием программных, технических и криптографических средств;
- ознакомление с правовой базой и законодательством Российской Федерации в области информационной безопасности, а также анализ научно-технической информации, отечественного и зарубежного опыта.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность» относится к обязательной части учебного плана.

Для изучения учебной дисциплины необходимы знания, умения и владения, формируемые следующими дисциплинами:

1. Базы данных.
2. Компьютерные коммуникации и сети.
3. Web-программирование.

Перечень учебных дисциплин, для которых необходимы знания, умения и владения, формируемые данной учебной дисциплиной:

1. Сетевое администрирование.
2. Управление IT-проектами.
3. Разработка клиент-серверных приложений.

## 3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина направлена на формирование следующих компетенций:

- ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;



- ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;
- ОПК-5 Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем.

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

31. Теорию информационной безопасности, методологию защиты информации;
32. Правовое обеспечение информационной безопасности, законодательную базу, систему государственного контроля и управления в области информационной безопасности;
33. Организационное обеспечение информационной безопасности;
34. Основные программные средства защиты информации;
35. Криптографические методы и средства обеспечения информационной безопасности.

Уметь:

- У1. Оценивать состояние организационной защиты информации на объекте;
- У2. Определять рациональные меры по обеспечению организационной защите на объекте;
- У3. Организовать работу с персоналом с секретной (конфиденциальной) информацией.

Владеть:

- В1. Методами выявления угроз информационной безопасности объекта;
- В2. Способами обеспечения режима и секретности на объекте.

#### 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

##### 4.1 Объем дисциплины и виды контактной и самостоятельной работы

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 час.), семестр изучения – 5, распределение по видам работ представлено в табл. № 1.

Таблица 1. Распределение трудоемкости дисциплины по видам работ

Вид работы	Форма обучения
	очная
	Семестр изучения
	5 сем.
	Кол-во часов
Общая трудоемкость дисциплины по учебному плану	108



Контактная работа, в том числе:	50
Лекции	16
Лабораторные работы	34
Самостоятельная работа студента	58
Промежуточная аттестация, в том числе:	
Экзамен	5 сем.

*\*Распределение трудоемкости по видам контактной работы для заочной формы обучения (при наличии) корректируется в соответствии с учебным планом заочной формы обучения.*

## 4.2 Содержание и тематическое планирование дисциплины

Таблица 2. Тематический план дисциплины

Наименование разделов и тем дисциплины (модуля)	Сем.	Всего, час.	Вид контактной работы, час.			СРС
			Лекции	Практ. занятия	Лаб. работы	
1. Основные цели и задачи информационной безопасности	5	16	2	-	2	12
2. Угрозы информационной безопасности на предприятии	5	18	2	-	4	12
3. Основные программные средства защиты информации	5	31	6	-	14	11
4. Организационное обеспечение информационной безопасности	5	24	4	-	8	12
5. Правовые аспекты информационной безопасности	5	19	2	-	6	11

*\*Распределение часов по разделам (темам) дисциплины для заочной формы обучения осуществляется научно-педагогическим работником, ведущим дисциплину.*

## 4.3 Содержание разделов (тем) дисциплин

### Раздел 1. Основные цели и задачи информационной безопасности

Актуальность информационной безопасности. Основные цели и задачи системы защиты. Источники угроз и атак. Основные классификации атак. Системы критериев оценки защищенности среды.

### Раздел 2. Угрозы информационной безопасности на предприятии



Виды угроз информационной безопасности и их характеристика. Модели нарушителей информационной безопасности на предприятии. Формы преступного посягательства. Оценка ущерба вследствие организационных нарушений информационной безопасности на предприятии.

### **Раздел 3. Основные программные средства защиты информации**

Программные средства защиты информации. Задачи обеспечения конфиденциальности, целостности и задачи обеспечения наблюдаемости, решаемые программными средствами защиты информации. Изучение основных технологий в области аутентификации данных, криптографии и обеспечении целостности данных. Управление доступом к ресурсам автоматизированной системы.

Технические мероприятия, призванные обеспечить физическую и информационную безопасность. Технические средства для реализации мероприятий данной группы.

Обеспечение безопасности электронного документооборота. Электронная подпись. Методы и средства защиты информации при работе с удаленными базами данных. Стеганография. Компьютерные вирусы и программы типа «Троянский конь». Средства обнаружения и уничтожения компьютерных вирусов.

### **Раздел 4. Организационное обеспечение информационной безопасности**

Корпоративная политика норм и требований, предъявляемых к сотрудникам на предприятии в отношении защиты корпоративной информации. Подходы к реализации мероприятий по обеспечению информационной безопасности. Построение модели защищенной системы. Обеспечение целостности и конфиденциальности. Примеры реализации политик безопасности информации на различных предприятиях.

### **Раздел 5. Правовые аспекты информационной безопасности**

Требования к защите информации, изложенные в соответствующих Законах РФ, стандартах и нормативных документах. Сравнение с нормативными документами о защите информации и мер наказания нарушителей законов о защите информации в развитых странах.

## **5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ**

Для изучения дисциплины используются различные образовательные технологии:

1. Для поддержки самостоятельной работы обучающихся использованы информационно-коммуникационные образовательные технологии, в частности, облачные технологии, электронная информационно-образовательная среда (ЭИОС), электронные средства обучения и электронно-библиотечные системы.



При этом результативность организации самостоятельной работы обучающихся существенно повышается за счет доступности материалов, упорядоченности работ и возможности получения консультации преподавателя.

2. Организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

3. Кейс-технологии применяются как способ обучать решению практико-ориентированных неструктурированных образовательных научных или профессиональных проблем. Применяется как при чтении лекций, так и при проведении семинарских, практических и лабораторных занятий.

4. При реализации образовательной программы с применением дистанционных образовательных технологий и электронного обучения:

- состав видов контактной работы по дисциплине (модулю), при необходимости, может быть откорректирован в направлении снижения доли занятий лекционного типа и соответствующего увеличения доли консультаций (групповых или индивидуальных) или иных видов контактной работы;

- информационной основой проведения учебных занятий, а также организации самостоятельной работы обучающихся по дисциплине (модулю) являются представленные в электронном виде методические, оценочные и иные материалы, размещенные в электронной информационно-образовательной среде (ЭИОС) университета, в электронных библиотечных системах и открытых Интернет-ресурсах;

- взаимодействие обучающихся и педагогических работников осуществляется с применением ЭИОС университета и других информационно-коммуникационных технологий (видеоконференцсвязь, облачные технологии и сервисы, др.);

- соотношение контактной и самостоятельной работы по дисциплине (модулю) может быть изменено в сторону увеличения последней, в том числе самостоятельного изучения теоретического материала.

## **6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ**

### ***6.1 Основная литература***

1. Артемов А. В. Информационная безопасность : учебное пособие. - Орел : Межрегиональная Академия безопасности и выживания, 2014. - 256 с. - Режим доступа: <http://www.iprbookshop.ru/33430>.

2. Петров С. В., Кисляков П. А. Информационная безопасность : учебное пособие. - Саратов : Ай Пи Эр Медиа, 2015. - 326 с. - Режим доступа: <http://www.iprbookshop.ru/33857>.

3. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт [Электронный ресурс] : монография / Л.Л. Ефимова, С.А. Кочерга. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2015. — 239 с.



— 978-5-238-02405-9. — Режим доступа: <http://www.iprbookshop.ru/52672.html>. — ЭБС «IPRbooks»

4. Прохорова О. В. Информационная безопасность и защита информации : учебное пособие / Прохорова О. В. — Санкт-Петербург : Лань, 2020. — 124 с. — Режим доступа: <https://e.lanbook.com/book/133924>.

## **6.2 Дополнительная литература**

1. Шаньгин В. Ф. Информационная безопасность и защита информации : учебное пособие. - Саратов : Профобразование, 2017. - 702 с. - Режим доступа: <http://www.iprbookshop.ru/63594>.

2. Морозов А. В., Филатова Л. В., Полякова Т. А. Информационное право и информационная безопасность. Часть 1 : учебник. - Москва : Всероссийский государственный университет юстиции, 2016. - 436 с. - Режим доступа: <http://www.iprbookshop.ru/72395>.

3. Морозов А. В., Филатова Л. В., Полякова Т. А. Информационное право и информационная безопасность. Часть 2 : учебник. - Москва : Всероссийский государственный университет юстиции, 2016. - 604 с. - Режим доступа: <http://www.iprbookshop.ru/66771>.

4. Петров А. А. Компьютерная безопасность. Криптографические методы защиты : монография. - Саратов : Профобразование, 2017. - 446 с. - Режим доступа: <http://www.iprbookshop.ru/63800>.

5. Рябко Б. Я. Криптографические методы защиты информации / Рябко Б. Я., Фионов А. Н. — Москва : Горячая линия-Телеком, 2017. — 230 с. — Режим доступа: <http://e.lanbook.com/book/111097>.

6. Лапони́на О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс] / О.Р. Лапони́на. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 242 с. — 5-9556-00020-5. — Режим доступа: <http://www.iprbookshop.ru/52217.html>. — ЭБС «IPRbooks»

7. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс] : монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2013. — 232 с. — Режим доступа: <https://e.lanbook.com/book/63244>. — Загл. с экрана.

## **6.3 Программное обеспечение и Интернет-ресурсы**

Интернет-ресурсы:

1. Конституция Российской Федерации. Режим доступа: <http://www.constitution.ru/>

2. SQL.ru - все про SQL, базы данных, программирование и разработку информационных систем. Режим доступа: <http://www.sql.ru/>

3. ITSec.Ru - портал для профессионалов информационной безопасности. Режим доступа: <http://www.itsec.ru/>



Программное обеспечение:

1. Операционная система Windows.
2. Операционная система Ubuntu.
3. Офисная система Office Professional Plus.
4. Web-сервер Open Server.

Информационные системы и платформы:

1. Система дистанционного обучения «Moodle».
2. Информационная система «Таймлайн».
3. Платформа для организации и проведения вебинаров «Mirapolis Virtual Room».

## **7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Перечень материально-технического обеспечения для реализации образовательного процесса по дисциплине:

1. Компьютерный класс.
2. Помещения для самостоятельной работы.
3. Учебная аудитория для проведения занятий лекционного типа с мультимедийным оборудованием.
4. Помещения для самостоятельной работы.

