

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
ФТД.03 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА
ИНФОРМАЦИИ»**

Направление подготовки 46.03.02 Документоведение и архивоведение

Профиль программы «Правовое и документационное обеспечение
управления персоналом»

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 и защита информации»: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи:

- изучение концепции инженерно-технической защиты информации;
- изучение теоретических основ инженерно - технической защиты информации;
- изучение физических основ инженерно-технической защиты информации;
- изучение технических средств добывания и защиты информации;
- изучение организационных основ инженерно-технической защиты информации;
- изучение методического обеспечения инженерно-технической защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность и защита информации» относится к факультативным дисциплинам учебного плана.

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

1. Организация работы с электронными документами.
2. Информационные технологии в документационном обеспечении управления и архивном деле.
3. Правовое обеспечение управленческой деятельности.
4. Документирование системы менеджмента качества.
5. Организационно-информационное обеспечение деятельности руководителя.

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина направлена на формирование следующих компетенций:

- УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;



- ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;
- ОПК-5 Способен самостоятельно работать с различными источниками информации и применять основы информационно-аналитической деятельности при решении профессиональных задач;
- ПКС-1 Способен осуществлять организационное, документационное и информационное обеспечение деятельности организации.

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 1 зач. ед. (36 час.), семестр изучения – 8, распределение по видам работ представлено в табл. № 1.

Таблица 1. Распределение трудоемкости дисциплины по видам работ

Вид работы	Форма обучения
	очная
	Семестр изучения



	8 сем.
	Кол-во часов
Общая трудоемкость дисциплины по учебному плану	36
Контактная работа, в том числе:	18
Лабораторные работы	18
Самостоятельная работа студента	18
Промежуточная аттестация, в том числе:	
Зачет	8 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	8	4	-	-	2	2
2. Угрозы информационной безопасности на предприятии	8	8	-	-	4	4
3. Основные программные средства защиты информации	8	8	-	-	4	4
4. Организационное обеспечение информационной безопасности	8	8	-	-	4	4
5. Правовые аспекты информационной безопасности	8	8	-	-	4	4

**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. Традиционные образовательные технологии, которые ориентируются на организацию образовательного процесса, предполагающую прямую трансляцию



знаний от преподавателя к студенту (преимущественно на основе объяснительно-иллюстративных методов обучения). Учебная деятельность студента носит в таких условиях, как правило, репродуктивный характер.

2. Информационно-коммуникационные образовательные технологии, при которых организация образовательного процесса, основывается на применении специализированных программных сред и технических средств работы с информацией. Используются для поддержки самостоятельной работы обучающихся с использованием электронной информационно-образовательной среды (ЭИОС), телекоммуникационных технологий, педагогических программных средств и др.

3. Технология обучения в сотрудничестве применяются при проведении семинарских, практических и лабораторных занятий, нацелены на совместную работу в командах или группах и достижение качественного образовательного результата.

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. Скабцов Н. Аудит безопасности информационных систем / Н. Скабцов. - Санкт-Петербург : Питер, 2018. - 272 с. - ISBN 978-5-4461-0662-2. - URL: <https://ibooks.ru/bookshelf/356717/reading>

2. Брюхомицкий, Ю. А. Безопасность информационных технологий. В 2 частях. Ч.1 : учебное пособие / Ю. А. Брюхомицкий. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 171 с. — ISBN 978-5-



9275-3571-2 (ч.1), 978-5-9275-3526-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/107943.html>

3. Скрыпников А. В., Родин С. В., Перминов Г. В., Чернышова Е. В. Безопасность систем баз данных : учебное пособие. - Воронеж : Воронежский государственный университет инженерных технологий, 2015. - 144 с. - Режим доступа: <http://www.iprbookshop.ru/50628>.

4. Защита Web-приложений : учебное пособие / А. В. Скрыпников, Д. В. Арапов, В. В. Денисенко, Т. Д. Герасимова. — Воронеж : Воронежский государственный университет инженерных технологий, 2020. — 76 с. — ISBN 978-5-00032-469-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/106438.html>

5. Бисюков В. М. Защита и обработка конфиденциальных документов : практикум. - Ставрополь : Северо-Кавказский федеральный университет, 2016. - 116 с. - Режим доступа: <http://www.iprbookshop.ru/66060>.

6. Тумбинская М. В. Защита информации на предприятии : учебное пособие / Тумбинская М. В., Петровский М. В. — Санкт-Петербург : Лань, 2020. — 184 с. — Режим доступа: <https://e.lanbook.com/book/130184>.

7. Никифоров С. Н. Защита информации. Защита от внешних вторжений : учебное пособие. - Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, 2017. - 84 с. - Режим доступа: <http://www.iprbookshop.ru/74381>.

8. Никифоров С. Н. Защита информации. Защищенные сети : учебное пособие. - Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, 2017. - 80 с. - Режим доступа: <http://www.iprbookshop.ru/74382>.

9. Петренко В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / Петренко В. И., Мандрица И. В. — Санкт-Петербург : Лань, 2020. — 108 с. — Режим доступа: <https://e.lanbook.com/book/149364>.

10. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/108227.html>

11. 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. Никифоров С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие для вузов / Никифоров С. Н. — Санкт-Петербург : Лань, 2020. — 124 с. — Режим доступа: <https://e.lanbook.com/book/146885>.

2. Никифоров С. Н. Методы защиты информации. Защищенные сети: учебное пособие / Никифоров С. Н. — Санкт-Петербург : Лань, 2018. — 96 с. — Режим



доступа: <http://e.lanbook.com/book/110935>.

3. Краковский Ю. М. Методы защиты информации : учебное пособие / Краковский Ю. М. — Санкт-Петербург : Лань, 2021. — 236 с. — Режим доступа: <https://e.lanbook.com/book/156401>.

4. 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>.

5. Гилязова Р. Н. Информационная безопасность. Лабораторный практикум : учебное пособие / Гилязова Р. Н. — Санкт-Петербург : Лань, 2020. — 44 с. — Режим доступа: <https://e.lanbook.com/book/130179>.

6.3 Программное обеспечение и Интернет-ресурсы

Интернет-ресурсы:

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

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

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

Программное обеспечение:

1. Операционная система Ubuntu.
2. Операционная система Windows.
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.

