МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

**Одобрена**
на заседании кафедры

05.12.2022 г.

протокол № 4

Зав. кафедрой Назаров Д.М.

**Утверждена**
Советом по учебно-методическим вопросам и качеству образования

14 декабря 2022 г.

протокол № 4

Председатель _____ Карх Д.А.
*(подпись)*

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

| | |
|---|---|
| Наименование дисциплины | Защита информации в корпоративных информационных системах |
| Направление подготовки | 10.03.01 Информационная безопасность |
| Профиль | Информационно-аналитические системы финансового мониторинга |
| Форма обучения | очная |
| Год набора | 2023 |

Разработана:
Доцент, к.э.н.
Буценко Е.В.

Екатеринбург
2022 г.

**СОДЕРЖАНИЕ**

## ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

| | |
|---|---|
| ФГОС ВО | Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427) |
| ПС | |

## 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование у студентов компетенций, направленных на изучение теоретических основ и практическое освоение методики обеспечения защиты информации в корпоративных системах при решении задач, связанных с автоматизацией управленческих, финансовых, экономических и бухгалтерских аспектов деятельности предприятия.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к вариативной части учебного плана.

## 3. ОБЪЕМ ДИСЦИПЛИНЫ

| Промежуточный контроль | Часов | | | | | З.е. |
|---|---|---|---|---|---|---|
| | Всего за семестр | Контактная работа .(по уч.зан.) | | | Самостоятельная работа в том числе подготовка контрольных и курсовых | |
| | | Всего | Лекции | Лабораторные | | |
| Семестр 6 | | | | | | |
| Экзамен | 180 | 108 | 36 | 72 | 36 | 5 |

## 4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Профессиональные компетенции (ПК)

| Шифр и наименование компетенции | Индикаторы достижения компетенций |
|---|---|
| эксплуатационный | |

| | |
|---|---|
| ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных | ИД-1.ПК-3 Знать:<br>Архитектура подсистем защиты информации в операционных системах<br>Принципы построения систем управления базами данных<br>Основные средства и методы анализа программных реализаций<br>Принципы построения антивирусного программного обеспечения<br>Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению<br>Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению<br>Уязвимости используемого программного обеспечения и методы их эксплуатации<br>Виды и формы функционирования вредоносного программного обеспечения<br>Характерные признаки наличия вредоносного программного обеспечения<br>Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения<br>Принципы функционирования программных средств криптографической защиты информации<br>Порядок обеспечения безопасности информации при эксплуатации программного обеспечения<br>Нормативные правовые акты в области защиты информации<br>Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации<br>Организационные меры по защите информации |
| | ИД-2.ПК-3 Уметь:<br>Анализировать угрозы безопасности информации программного обеспечения<br>Формулировать правила безопасной эксплуатации программного обеспечения<br>Обосновывать правила безопасной эксплуатации программного обеспечения<br>Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия<br>Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации<br>Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения<br>Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации<br>Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения |

| | |
|---|---|
| ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных | ИД-3.ПК-3 Иметь практический опыт:<br>Определение порядка установки программного обеспечения с целью соблюдения требований по защите информации<br>Контроль над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение<br>Формулирование требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения<br>Выполнение работ по обнаружению вредоносного программного обеспечения<br>Ликвидация обнаруженного вредоносного программного обеспечения и последствий его функционирования<br>Формулирование требований к встроенным средствам защиты информации программного обеспечения |

## 5. ТЕМАТИЧЕСКИЙ ПЛАН

| Тема | Часов | | | | | | |
|---|---|---|---|---|---|---|---|
| | Наименование темы | Всего часов | Контактная работа .(по уч.зан.) | | | Самост. работа | Контроль самостоятельной работы |
| | | | Лекции | Лабораторные | Практические занятия | | |
| Семестр 6 | | 26 | | | | | |
| Тема 1. | Проблемы безопасности корпоративной информации | 26 | 6 | 4 | | 16 | |
| Семестр 6 | | 26 | | | | | |
| Тема 2. | Законодательные акты в области защиты информации | 26 | 6 | 4 | | 16 | |
| Семестр 6 | | 28 | | | | | |
| Тема 3. | Технологии защиты корпоративных данных. Криптографическая защита информации. Идентификация, аутентификация и управление доступом | 28 | 8 | 20 | | | |
| Семестр 6 | | 48 | | | | | |
| Тема 4. | Комплексная защита корпоративных информационных систем. Обнаружение и предотвращение вторжений. Межсетевой экран. Виртуальные защищенные сети VPN. Фильтрация трафика в корпоративных сетях | 48 | 10 | 34 | | 4 | |
| Семестр 6 | | 16 | | | | | |
| Тема 5. | Архитектура защищенных корпоративных систем. Ядро и ресурсы средств защиты информации. Стратегии защиты информации | 16 | 6 | 10 | | | |

## 6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

| Раздел/Тема | Вид оценочного средства | Описание оценочного средства | Критерии оценивания |
|---|---|---|---|
| Текущий контроль (Приложение 4) | | | |

| | | | |
|---|---|---|---|
| 2. Комплексная защита корпоративных информационных систем. Обнаружение и предотвращение вторжений. Межсетевой экран. Виртуальные защищенные сети VPN. Фильтрация трафика в корпоративных сетях | Тест (Приложение 4) | Тест состоит из 30 вопросов с вариантами ответов | 1-10 баллов |
| 1. Проблемы безопасности корпоративной информации | Тест (Приложение 4) | Тест состоит из 30 вопросов с вариантами ответов | 1-10 баллов |
| 3. Архитектура защищенных корпоративных систем. Ядро и ресурсы средств защиты информации. Стратегии защиты информации | Тест (Приложение 4) | Тест состоит из 30 вопросов с вариантами ответов | 1-10 баллов |
| Промежуточный контроль (Приложение 5) | | | |
| 6 семестр (Эк) | Экзаменационный билет (приложение 5) | 24 билета. 2 теоретических вопроса и 1 практическое задание | 1-100 баллов |

## ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущей и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущая аттестация. Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущей аттестации, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

| Показатель оценки | По 5-балльной системе | Характеристика показателя |
|---|---|---|
| 100% - 85% | отлично | обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне |
| 84% - 70% | хорошо | обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов.<br><br>Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.) |
| 69% - 50% | удовлетворительно | обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне.<br>Допускаются ошибки, которые студент затрудняется исправить самостоятельно. |
| 49 % и менее | неудовлетворительно | обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов.<br>Не сформированы умения и навыки для решения профессиональных задач |
| 100% - 50% | зачтено | характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно» |
| 49 % и менее | не зачтено | характеристика показателя соответствует «неудовлетворительно» |

## 7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

| |
|---|
| Тема 1. Проблемы безопасности корпоративной информации<br>Защита корпоративной информации. Несанкционированный доступ. Защита от физического доступа. Защита резервных копий. Защита от инсайдеров |
| Тема 2. Законодательные акты в области защиты информации<br>Роли и обязанности должностных лиц по проведению политики безопасности. Аудит информационной безопасности. Нормы и стандарты информационной безопасности на предприятии |
| Тема 3. Технологии защиты корпоративных данных. Криптографическая защита информации. Идентификация, аутентификация и управление доступом<br>Необходимость защиты корпоративных систем: тенденции и факты. Угрозы безопасности автоматизированных систем обработки информации. Особенности защиты информации в корпоративных системах |
| Тема 4. Комплексная защита корпоративных информационных систем. Обнаружение и предотвращение вторжений. Межсетевой экран. Виртуальные защищенные сети VPN. Фильтрация трафика в корпоративных сетях<br><br>Методы защиты информации в автоматизированных системах обработки данных. ЭЦП. Криптография. Голография. Принцип голографии. Полиграфические средства защиты |
| Тема 5. Архитектура защищенных корпоративных систем. Ядро и ресурсы средств защиты информации. Стратегии защиты информации<br>Структура распределенных систем. Проектирование хранилищ данных. Анализ корпоративных данных |

7.2 Содержание практических занятий и лабораторных работ

| |
|---|
| Тема 1. Проблемы безопасности корпоративной информации<br><br>Объекты защиты предприятия. Государственные акты и стандарты защиты информации. Функции системы имитационного моделирования по управлению предприятием в условиях рыночной экономики |
| Тема 2. Законодательные акты в области защиты информации<br><br>Методология защиты автоматизированных систем обработки информации. Безопасность АСОИ |
| Тема 3. Технологии защиты корпоративных данных. Криптографическая защита информации. Идентификация, аутентификация и управление доступом<br><br>Управленческие, финансовые, экономические и бухгалтерские операции и их защита. Объекты и назначение средств программной защиты |

| |
|---|
| Тема 4. Комплексная защита корпоративных информационных систем. Обнаружение и предотвращение вторжений. Межсетевой экран. Виртуальные защищенные сети VPN. Фильтрация трафика в корпоративных сетях<br><br>1. Подпись документов при помощи симметричных криптосистем<br>2. Хэш-функция<br>3. Хранение ключей<br>4. Распределение ключей<br>5. Стандарты криптографии<br>6. Требования пользователей<br>7. Атаки на цифровую подпись<br>8. Атаки на алгоритмы<br>9. Атаки на криптосистему<br>10. Атаки на реализацию<br>11. Атаки на пользователей<br>12. Электронные цифровые подписи<br>13. Алгоритмы электронной цифровой подписи |
| Тема 5. Архитектура защищенных корпоративных систем. Ядро и ресурсы средств защиты информации. Стратегии защиты информации<br><br>Стратегии защиты корпоративной информации. Разработка системы защиты информации в корпорации |

7.3. Содержание самостоятельной работы

| |
|---|
| Тема 1. Проблемы безопасности корпоративной информации<br>Изучение понятийного аппарата темы, методического материала, глав рекомендованных учебников и дополнительных источников |
| Тема 2. Законодательные акты в области защиты информации<br>Изучение понятийного аппарата темы, методического материала, глав рекомендованных учебников и дополнительных источников |
| Тема 4. Комплексная защита корпоративных информационных систем. Обнаружение и предотвращение вторжений. Межсетевой экран. Виртуальные защищенные сети VPN. Фильтрация трафика в корпоративных сетях<br><br>Изучение понятийного аппарата темы, методического материала, глав рекомендованных учебников и дополнительных источников |

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
Не предусмотрено

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
Материалы не предусмотрены

7.6 Методические рекомендации по выполнению курсовой работы
Материалы не предусмотрены

## 8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

***По заявлению студента***

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

## 9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Сайт библиотеки УрГЭУ**
http://lib.usue.ru/

**Основная литература:**

1. Гришина Н. В. Основы информационной безопасности предприятия [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 216 с. – Режим доступа: https://znanium.com/catalog/product/1784437

2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2022. - 592 с. – Режим доступа: https://znanium.com/catalog/product/1843022

**Дополнительная литература:**

1. Моргунов А. Ф. Информационные технологии в менеджменте [Электронный ресурс]:Учебник для вузов. - Москва: Юрайт, 2022. - 310 – Режим доступа: https://urait.ru/bcode/489923

2. Полякова Т. А., Стрельцов А. А., Чубукова С. Г., Ниесов В. А. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]:учебник и практикум для вузов. - Москва: Юрайт, 2022. - 325 с – Режим доступа: https://urait.ru/bcode/498844

## 10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

**Перечень лицензионного программного обеспечения:**

Astra Linux Common Edition. Договор № 1 от 13 июня 2018, акт от 17 декабря 2018. Срок действия лицензии - без ограничения срока.

Libre Office. Лицензия GNU LGPL. Срок действия лицензии - без ограничения срока.

Microsoft Windows 10 .Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020. Срок действия лицензии 30.09.2023.

Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии 30.09.2023.

Microsoft Visual Studio Community. Лицензия для образовательных учреждений. Срок действия лицензии - без ограничения срока.

**Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:**

Справочно-правовая система Консультант +. Срок действия лицензии до 31.12.2023

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

## 11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.