

# АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)/ПРАКТИКИ

## Б1.В.06 Защита информации в организационных структурах

(индекс и наименование дисциплины (модуля), в соответствии с учебным планом)

**Автор:** канд. эконом. наук, доцент кафедры \_\_\_\_\_ Федосеев А.И.

**Направление, программа магистратуры:** 38.04.02 Менеджмент "Digital design в менеджменте (информационно-аналитический менеджмент)"

**Квалификация выпускника:** Магистр

**Форма обучения:** очная

### **Цель освоения дисциплины:**

Сформировать следующие компетенции:

- способностью управлять организациями, подразделениями, группами (командами) сотрудников, проектами и сетями (ПК-1);

### **План курса:**

Тема 1. Введение. Безопасность функционирования современной организации и технологий.

Введение. Предмет и задачи дисциплины. Значение и место дисциплины в подготовке специалистов в области прикладных аспектов информатики и информационных технологий по защите информации от несанкционированных воздействий и обеспечения достоверности и целостности при ее обработке в информационно-телекоммуникационных системах. Научная и учебная взаимосвязь дисциплины с другими дисциплинами, изучаемыми в высшем учебном заведении.

Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения практических и семинарских занятий. Состав и методика самостоятельной работы студентов по изучению дисциплины. Форма проверки знаний. Анализ нормативных источников, научной и учебной литературы. Знания и умения студентов, которые должны быть получены в результате изучения дисциплины.

Актуальность проблемы обеспечения информационной безопасности в торгово-экономических структурах, потенциально возможные несанкционированные воздействия на информационную инфраструктуру торгово-экономической деятельности, информационный криминал. Статистические показатели состояния информационной безопасности информационной инфраструктуры торгово-экономической деятельности, динамика ее развития.

Составляющие воздействия на информационную инфраструктуру государства: информационная война, информационный терроризм, информационный криминал. Понятие конкурентной разведки.

Тема 2. Современная доктрина информационной безопасности Российской Федерации.

Понятие и назначение Доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Значение информационной безопасности и ее место в системе национальной безопасности. Значение информационной безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации.

Международные стандарты информационного обмена, правовые основы защиты государственной, коммерческой, служебной, процессуальной, профессиональной тайны и информации персонального характера. Федеральные Законы Российской Федерации по

обеспечению информационной безопасности в информационных технологиях, Доктрина Информационной безопасности Российской Федерации, Концепция Национальной Безопасности Российской Федерации, нормативные и руководящие документы, Постановления Правительства Российской Федерации по проблемам обеспечения информационной безопасности, Руководящие документы и инструкции Федеральной службы по техническому и экспортному контролю (ФСТЭК), Приказы и распоряжения ФСБ РФ, Ведомственные приказы и распоряжения.

Тема 3. Международные стандарты информационного обмена. Модели безопасности и их применение.

Безопасность в сетях Internet и Intranet. Технология безопасности: межсетевые экраны (Межсетевые экраны прикладного уровня, межсетевые экраны с пакетной фильтрацией, гибридные межсетевые экраны). Разработка конфигурации межсетевого экрана: Архитектура 1 – системы за пределами; архитектура 2 – один межсетевой экран; архитектура 3 – двойные межсетевые экраны. Безопасность виртуальных частных сетей (VPN).

Модели безопасности: модели разграничения доступа; модели разграничения доступа, построенные по принципу предоставления прав; модели дискретного доступа; модели мандатного доступа; модель Белла и Лападула; специализированные модели; вероятностные модели; информационные модели; модели контроля целостности; Модель Биба; модель Кларка-Вилсона. Модели анализа безопасности программного обеспечения.

Тема 4. Сущность и задачи обеспечения информационной безопасности.

Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Агрегация информационных ресурсов с точки зрения информационной безопасности. Классификация угроз информационной безопасности. Информационная безопасность компьютерных систем. Основные понятия и определения. Безопасность автоматизированных систем обработки информации. Доступ к информации (санкционированный, несанкционированный), разграничение доступа, конфиденциальность данных, угрозы безопасности, защита информации, политика безопасности

Основные виды угроз безопасности компьютерным системам: нарушения конфиденциальности информации, нарушения целостности информации, нарушения работоспособности системы. Каналы несанкционированного доступа. Способы несанкционированного доступа: перехват паролей, «маскарад», незаконное использование привилегий.

Тема 5. Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.

«Врожденные слабости» наиболее распространенных служб Internet. Основные компоненты межсетевых экранов: фильтрующие маршрутизаторы, шлюзы сетевого уровня, шлюзы прикладного уровня. Аутентификация пользователей как основной компонент межсетевых экранов. Схема защиты компьютерных сетевых технологий на основе межсетевых экранов: фильтрующий маршрутизатор, межсетевой экран на основе двупортового шлюза, межсетевой экран на основе экранированного шлюза, экранированная подсеть, межсетевые экраны для организации виртуальных корпоративных сетей. Программные методы защиты сетевых технологий в Internet структурах.

Тема 6. Состав, структура и назначение Удостоверяющих центров в системах защиты и аутентификации электронных документов в интернет.

Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования, Разновидности задач защиты от копирования. Подходы к задаче защиты от копирования. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования. Привязка к внешним (добавляемым) элементам ПЭВМ. Привязка к портовым ключам. Использование дополнительных плат расширения. Методы

«водяных знаков» и методы «отпечатков пальцев».

В результате освоения дисциплины у студентов должны быть сформированы:

| ОТФ/ТФ<br><br>(при наличии профстандарта)/<br>профессиональные действия | Код этапа освоения компетенции | Планируемые результаты обучения  |
|---|--------------------------------|--|
| Управление группой менеджеров продуктов - С/05.6                        | ПК-1.2                         | на уровне знаний:<br>знать особенности управления организациями, подразделениями и группами сотрудников  |
|   |                                | на уровне умений:<br>уметь сравнивать различные стратегии и программы управления организациями, подразделениями и группами (командами) сотрудников |
|   |                                | на уровне навыков:<br>владеть навыками управления проектами и сетями   |

**Формы и методы текущего контроля и промежуточной аттестации:**

В ходе реализации дисциплины Б1.В.06 «Защита информации в организационных структурах» используются следующие методы текущего контроля успеваемости обучающихся:

- при проведении занятий лекционного типа (аудиторно): опрос, дискуссия;
- при проведении занятий практического (лабораторного) типа (аудиторно): опрос, дискуссия (устные ответы на вопросы преподавателя по теме занятия, групповое обсуждение вопросов); преподаватель, реализующий дисциплину, определяет самостоятельно планы занятий;
- при контроле результатов самостоятельной работы студентов (с использованием ДОТ): эссе, тестирование.

Форма промежуточной аттестации: зачет

**Основная литература**

- 1.Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 261 с. — (Высшее образование). — ISBN 978-5-534-01678-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/414082> (дата обращения: 24.01.2021).