

## **Б1.В.ДВ.4.2 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА**

**Цели дисциплины:** обучение студентов современным технологиям в области информационных систем, создания и эксплуатации систем защиты информации.

### **Задачи дисциплины:**

- усвоение знаний по нормативно-правовым основам организации информационной безопасности, изучение стандартов и руководящих документов по защите информационных систем;
- ознакомление с основными угрозами информационной безопасности;
- правилами их выявления, анализа и определение требований к различным уровням обеспечения информационной безопасности;
- ознакомиться с угрозами информационной безопасности, создаваемыми компьютерными вирусами, изучить особенности этих угроз и характерные черты компьютерных вирусов.
- изучить особенности обеспечения информационной безопасности в компьютерных сетях и специфику средств защиты компьютерных сетей;
- изучить содержание и механизмы реализации сервисов безопасности «идентификация» и «аутентификация»;
- характеристика сетевой технологии Internet. Основные угрозы информационной безопасности организации при использовании Internet. Основные приёмы защиты корпоративных сетей при использовании Internet.

### **Место дисциплины в структуре ОПОП:**

Дисциплина относится к дисциплинам по выбору вариативной части учебного плана направлению подготовки: 38.03.01 Экономика профиль: Бухгалтерский учет, анализ и аудит.

Дисциплина основывается на знании следующих дисциплин: Б1.В.ОД.6 Информационные технологии и Б1.В.ОД.7 Информационные системы в экономике.

Для успешного освоения дисциплины, студент должен:

#### **Знать:**

- роли и значения информатики в современном обществе (ОПК-1);
- основы форм представления и преобразования информации в компьютере (ПК-8)

#### **Уметь:**

- применять математические методы, физические законы и вычислительную технику для решения практических задач (ОПК-1).

#### **Владеть:**

- базовыми основами алгоритмизации (ПК-8);
- навыками работы на персональном компьютере (ОПК-1).

### **Требования к результатам освоения дисциплины:**

В результате освоения дисциплины должны быть сформированы следующие компетенции:

***ОПК-1 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности***

В результате освоения компетенции ОПК-1 студент должен:

***знать:***

- виды угроз ИС и методы обеспечения информационной безопасности;
- задачи программно-технического обеспечения информационной безопасности;
- шифрование или криптографическое кодирование;
- организацию и политику безопасности в операционных системах;

***уметь:***

- проводить анализ предметной области, выявлять информационные потребности и разрабатывать требования к ИС;
- выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС;
- пользоваться основными методами и способами информационной безопасности;
- ориентироваться в видах вредоносных программ и способах борьбы с ними;
- настраивать политику безопасности современных операционных систем;
- решать задачи распределения ресурсов и прав доступа;

***владеть:***

- работы с инструментальными средствами проектирования баз данных и знаний, управления проектами ИС и защиты информации.
- теоретическими знаниями и практическими навыками, позволяющих ориентироваться в области информационных технологий;
- разрабатывать и применять системы безопасности;
- прикладными и инструментальными средствами создания систем информационной безопасности.

***ОПК-2 способность осуществлять сбор, анализ и обработку данных, необходимых для решения профессиональных задач***

В результате освоения компетенции ОПК-2 студент должен:

***знать:***

- виды угроз ИС и методы обеспечения информационной безопасности;

- задачи программно-технического обеспечения информационной безопасности;
  - шифрование или криптографическое кодирование;
  - организацию и политику безопасности в операционных системах;
- уметь:**
- проводить анализ предметной области, выявлять информационные потребности и разрабатывать требования к ИС;
  - выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС;
  - пользоваться основными методами и способами информационной безопасности;
  - ориентироваться в видах вредоносных программ и способах борьбы с ними;
  - настраивать политику безопасности современных операционных систем;
  - решать задачи распределения ресурсов и прав доступа;
- владеть:**
- работы с инструментальными средствами проектирования баз данных и знаний, управления проектами ИС и защиты информации.
  - теоретическими знаниями и практическими навыками, позволяющих ориентироваться в области информационных технологий;
  - разрабатывать и применять системы безопасности;
  - прикладными и инструментальными средствами создания систем информационной безопасности.

### **Содержание дисциплины:**

№ п/п	Наименование раздела дисциплины (темы)
1	Информационная безопасность и уровни ее обеспечения.
2	Компьютерные вирусы и защита от них.
3	Информационная безопасность вычислительных сетей.
4	Механизмы обеспечения "информационной безопасности".
5	Информационная безопасность при использовании Internet.
6	Безопасность операционных систем.

**Форма контроля - зачет**