

## **Б1.Б.18 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

**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 ВО (основной профессиональной образовательной программы высшего образования)**

Дисциплина относится к базовой части учебного плана.

Дисциплина основывается на знании следующих дисциплин: Информатика и программирование и Вычислительные системы, сети и телекоммуникации.

Для успешного освоения дисциплины, студент должен:

#### **1. Знать:**

- базовые понятия информатики и вычислительной техники (ОК-4);
- роли и значения информатики в современном обществе (ОПК-1);
- современные тенденции развития информатики и вычислительной техники, компьютерных технологий (ОПК-4);
- основы форм представления и преобразования информации в компьютере (ПК-7)

#### **2. Уметь:**

- решать простейшие задачи вычислительного характера (ПК-12);

- применять математические методы, физические законы и вычислительную технику для решения практических задач (ПК-15).

### **3. Владеть:**

- базовыми основами алгоритмизации (ПК-6);
- навыками работы на персональном компьютере (ПК-14).

### **Требования к результатам освоения содержания дисциплины**

В результате освоения дисциплины должны быть сформированы следующие компетенции:

### **ОК-4 способность использовать основы правовых знаний в различных сферах деятельности**

#### **1. 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;

#### **2. 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;

#### **3. 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-1 способность использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий**

#### **1. 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;

## **2. 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;

## **3. 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-4 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности**

## **1. 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;

## **2. 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;

### **3. 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.

## **ПК-2 способность разрабатывать, внедрять и адаптировать прикладное программное обеспечение**

### **1. 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;

### **2. 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;

### **3. 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.

## **ПК-6 способность собирать детальную информацию для формализации требований пользователей заказчика**

### **1. 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;

### **2. 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;

### **3. 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.

## **ПК-7 способность проводить описание прикладных процессов и информационного обеспечения решения прикладных задач**

### **1. 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;

### **2. 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;

### **3. 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.

## **ПК-10 способность принимать участие во внедрении, адаптации и настройке информационных систем**

### **1. 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;

### **2. 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;

### **3. 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.

## **ПК-12 способность проводить тестирование компонентов программного обеспечения ИС**

### **1. 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;

### **2. 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;

### **3. 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.

## **ПК-14 способность осуществлять ведение базы данных и поддержку информационного обеспечения решения прикладных задач**

### **1. 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;

## **2. 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;

## **3. 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.

## **ПК-15 способность осуществлять тестирование компонентов информационных систем по заданным сценариям**

### **1. 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;

### **2. 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;

### **3. 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 - экзамен**