

**Аннотация рабочей программы дисциплины (модуля)**  
**Б1.О.32 Безопасность компьютерных сетей**

**Цель дисциплины (модуля)** Целями освоения дисциплины *«Безопасность компьютерных сетей»* являются формирование общепрофессиональных компетенций будущих специалистов в области информационной безопасности, формирование у студентов базовых знаний, умений и навыков по принципам администрирования систем защиты информации компьютерных сетей достаточных для освоения основной профессиональной образовательной программы направления 10.03.01 Информационная безопасность.

**Задачи дисциплины**

Основными задачами изучения дисциплины являются:

- основные меры по защите информации в компьютерных сетях, а также содержание эксплуатационной документации компьютерных сетей;
- критерии оценки защищенности компьютерных сетей, средства контроля эффективности мер защиты информации;
- выработка практических навыков по решению задач защиты компьютерных сетей, исходя из задач, стоящих перед вычислительной системой.

**Формируемые компетенции и индикаторы их достижения по дисциплине:**

| <b>Коды компетенции</b> | <b>Содержание компетенций</b>                                                                                                                                                                                                                                           | <b>Код и наименование индикатора достижения компетенции</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ОПК-4.3                 | ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем | ОПК-4.3.1 - Знает основные меры по защите информации в автоматизированных системах, а также содержание эксплуатационной документации автоматизированной системы;<br>ОПК-4.3.2 - Умеет устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств;<br>ОПК-4.3.3 - Владеет навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы |
| ОПК-4.4                 | ОПК-4.4. Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем                                                                                                                                                                         | ОПК-4.4.1 - Знает критерии оценки защищенности автоматизированной системы, технические средства контроля эффективности мер защиты информации;<br>ОПК-4.4.2 - Умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, контролировать события безопасности и действия                                                                                                                                                                                                                                                                                                                                                  |

|  |  |                                                                                                                                                                                                                                                                                                         |
|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p>пользователей автоматизированных систем, а также документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы;</p> <p>ОПК-4.4.3 - Владеет навыками оценки защищенности автоматизированных систем с помощью типовых программных средств.</p> |
|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Содержание дисциплины

### **Раздел 1 Основы безопасности компьютерных сетей**

Тема 1. Основные понятия и терминология, угрозы, уязвимости, атаки

Тема 2. Нормативно-правовое обеспечение информационной безопасности КС

Тема 3. Классификация угроз и уязвимостей, банки угроз и уязвимостей, Банк данных угроз ФСТЭК, MITRE ATT&CK

Тема 4 Сетевые атаки, модель Cyber-Kill Chain

### **Раздел 2 Средства обеспечения безопасности компьютерных сетей**

Тема 5. Фильтрация сетевого трафика, межсетевые экраны, NGFW

Тема 6 Средства обеспечения безопасности компьютерных сетей. Технологии обнаружения сетевых атак, системы обнаружения и предотвращения вторжений

Тема 7. Средства обеспечения безопасности компьютерных сетей. Технологии построения защищенных каналов связи, средства построения виртуальных защищенных сетей

Тема 8. Средства обеспечения безопасности компьютерных сетей. Инструменты для исследования сети, снифферы и сканеры безопасности, инструменты мониторинга состояния сети

Тема 9 Средства обеспечения безопасности компьютерных сетей. Предотвращение утечек информации, DLP-системы

Тема 10 Средства обеспечения безопасности компьютерных сетей. Защита конечных устройств КС, технологии Endpoint Security, системы защиты конечных точек (Endpoint Protection Platform)

Тема 11. Современные тенденции в обеспечении безопасности компьютерных сетей  
Основы тестирования на проникновение, этапы проведения тестирования на проникновение, инструменты. XDR-системы

## **Темы и планы лабораторных занятий**

Тема 1. Межсетевые экраны Фильтрация сетевого трафика, межсетевые экраны, NGFW

Тема 2. Системы обнаружения вторжений

Технологии обнаружения сетевых атак. Виды систем обнаружения вторжений.

Использование систем для предотвращения вторжений.

Тема 3. Виртуальные защищенные сети

Технологии построения защищенных каналов связи, средства построения виртуальных защищенных сетей

Тема 4. Средства обеспечения безопасности компьютерных сетей. Инструменты для исследования сети, снифферы и сканеры безопасности, инструменты мониторинга состояния сети

Тема 5. DLP-системы. Системы защиты конечных точек (EPP-решения)

Тема 6. Средства обеспечения безопасности компьютерных сетей. Защита конечных устройств КС, технологии Endpoint Security, системы защиты конечных точек (Endpoint Protection Platform)

Тема 7. Современные тенденции в обеспечении безопасности компьютерных сетей. Этапы проведения тестирования на проникновение, инструменты. XDR-системы  
Инструменты тестирования на проникновение