

Аннотация рабочей программы дисциплины (модуля)
Б1.В.ДВ.09.02 Сетевая безопасность

Цель дисциплины (модуля) Целями освоения дисциплины *«Безопасность компьютерных сетей»* являются формирование профессиональных компетенций будущих специалистов в области Информационных систем и технологий, формирование у студентов базовых знаний, умений и навыков по принципам управления системами защиты информации компьютерных сетей достаточных для освоения основной профессиональной образовательной программы направления 09.03.02 Информационные системы и технологии

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- основные меры по защите информации в компьютерных сетях;
- 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:

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ПКС-2	ПКС-2. Способен проводить формализацию предметной области с целью создания информационной системы	ПКС-2.1 - Знает требования к компьютерному программному обеспечению; виды технической спецификации на программные компоненты и их взаимодействие; методы проектирования компьютерного программного обеспечения ПКС-2.2 – Умеет применять требования к компьютерному программному обеспечению; разрабатывать технические спецификации на программные компоненты и их взаимодействие; применять методы проектирования компьютерного программного обеспечения; ПКС-2.3 – Владеет методами разработки требований к компьютерному программному обеспечению, технических спецификаций на программные компоненты, методами проектирования компьютерного программного обеспечения.
ПКС-3	ПКС-3 - Способен осуществлять организацию взаимодействия с заказчиком, планирования проекта ИС; руководить разработкой программного кода, верификацией и тестированием ИС	ПКС-3.1 - Знает методы организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС; ПКС-3.2 - Умеет применять методы организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС; ПКС-3.3 - Владеет методами организации взаимодействия с заказчиком,

		планирования проекта, разработки, верификации и тестирования ИС.
--	--	--

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