

Аннотация рабочей программы дисциплины (модуля)

Б1.В.ДВ.09.01 Сетевая безопасность

Цель дисциплины

Целью изучения дисциплины является предоставление обучаемым знаний об основных типах и способах защиты информации в компьютерных сетях, а также навыков по проектированию системы защиты информации и анализу защищенности вычислительных сетей.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- изучение основных принципов информационной безопасности сетевого оборудования;
- ознакомление с техническими и технологическими решениями, используемыми в данной области;
- выработка практических навыков аналитического и экспериментального исследования основных методов и средств, используемых в области, изучаемой в рамках данной дисциплины.

Формируемые компетенции и индикаторы их достижения по дисциплине

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ОПК-2	– способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии;	ОПК-2.1 Обладать базовыми знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий. ОПК-2.2 Уметь находить, формулировать и решать стандартные задачи, используя современные образовательные и информационные технологии. ПК-2.3. Иметь практический опыт использования современных образовательных и информационных технологий для решения задач профессиональной деятельности.
ОПК- 4	– способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК-4.1 Знать основные методы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-4.2 Уметь использовать методы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-4.3 Иметь навыки решения стандартных задач

		<p>профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p>
ПК-4	<p>– способностью работать в составе научно-исследовательского и производственного коллектива и решать задачи профессиональной деятельности</p>	<p>ПК - 4.1 Обладать способностью работать в составе научно-исследовательского и производственного коллектива и решать задачи профессиональной деятельности</p> <p>ПК - 4.2 Уметь решать стандартные задачи в научно-исследовательской и профессиональной деятельности в составе научно-исследовательского и производственного коллектива</p> <p>ПК - 4.3 Иметь практические навыки в области решения стандартных задач в научно-исследовательской и профессиональной деятельности в составе научно-исследовательского и производственного коллектива</p>
ПК-5	<p>– способностью осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети "Интернет" (далее – сеть "Интернет") и в других источниках;</p>	<p>ПК-5.1 Знать, как осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети Интернет и в других источниках.</p> <p>ПК -5.2 Уметь осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети Интернет и в других источниках.</p> <p>ПК-5.3 Иметь навыки осуществления целенаправленного поиска информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети Интернет и в других источниках.</p>
ПК-7	<p>– способностью к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения</p>	<p>ПК - 7.1 Знать основные методы разработки и применения алгоритмических и программных решений в области системного и прикладного программного обеспечения</p> <p>ПК - 7.2 Уметь разрабатывать, и применять алгоритмические и программные решения в области системного и прикладного программного обеспечения</p> <p>ПК - 7.3 Иметь практические навыки в области разработки, и применения алгоритмических и программных решений в области системного и прикладного программного обеспечения</p>

Содержание разделов дисциплины

8 семестр

Тема 1. Виды атак. Модель сетевой безопасности

Обобщенный сценарий атаки. Пассивная разведка. Активная разведка. Взлом целевой системы. Сокрытие следов взлома. Классификация атак. Модель сетевой безопасности.

Тема 2. Криптография и системы шифрования.

Криптография. Структура шифрования Фейстеля. Алгоритмы стандартного шифрования. Режимы работы блочных шифровальщиков. Расположение устройств шифрования. Распределение ключей. Криптография и аутентификация сообщений на основе общего ключа.

Тема 3. Механизмы обеспечения безопасности коммутируемых локальных сетей.

Ограничение количества управляющих компьютеров. Настройка безопасности индивидуального порта. Фильтрация MAC-адресов. Технология фильтрации IP-MAC Binding. Списки контроля доступа. Сегментация трафика. Протокол IEEE 802.1x. Виртуальные сети. Аудит безопасности протокола связующего дерева STP.

Тема 4. Механизмы обеспечения безопасности беспроводных локальных сетей.

Классификация механизмов безопасности в сетях Wi-Fi. Механизмы шифрования. Принцип аутентификации абонента. Открытая аутентификация. Аутентификация с общим ключом. Аутентификация по MAC-адресу. Дополнительные механизмы защиты.

Тема 5. Механизмы межсетевой безопасности.

Межсетевые экраны. Фильтры пакетов. Фильтры инспекции состояний. Транслятор адресов. Транспортные шлюзы. Шлюзы приложений. Системы обнаружения атак и вторжений.

Тема 6. Системы тунелирования.

Протокол PPPoE. Виртуальные частные сети. Протокол IPSEC. Протокол SSL/TLS.

Тема 7. Безопасность удаленного управления.

Аудит безопасности протокола SNMP. Версии протокола SNMP. Протокол SNMPv3. Протокол SSH. Рекомендации по безопасности использования протокола SSH.