

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Петренко Вячеслав Иванович
 Должность: и.о. директора Института цифрового развития
 Дата подписания: 05.07.2024 09:35:26
 Уникальный программный ключ:
 b47f96eea65a20e275f94abf1bb0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Основы построения защищенных компьютерных сетей
Содержание	Проблемы безопасности в компьютерных сетях. Обобщенный сценарий атаки. Классификация атак. Модель сетевой безопасности. Криптография и аутентификация сообщений на основе общего ключа. Области применения криптографии с открытым ключом. Методы аутентификации сообщений. Безопасные кэш функции. 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. Роли устройств. Процесс аутентификации. Состояние портов коммутатора. Методы контроля доступа при использовании протокола IEEE 802 1x. Виртуальные сети. Сети на базе MAC-адресов. Сети на базе портов. Сеть на базе маркированных кадров. Аудит безопасности протокола связующего дерева STP. Обзор протокола Spanning Tree. Протокол STP и виртуальные сети VLAN. Возможные схемы атак. Получение дополнительной информации о сети при помощи STP. Механизмы обеспечения безопасности беспроводных локальных сетей. Классификация механизмов безопасности в сетях Wi-Fi. Механизм шифрования WEP (IEEE 802 11). Спецификация WPA. Стандарт сети 802 с повышенной безопасностью (WPA2). утентификация в беспроводных Wi-Fi сетях. Принцип аутентификации абонента в IEEE 802. Открытая аутентификация. Аутентификация с общим ключом. Аутентификация по MAC-адресу. Стандарт IEEE 802 1x/EAP. Дополнительные механизмы защиты SSID. Общие механизмы обеспечения безопасности локальных сетей. Механизмы межсетевой безопасности. Межсетевые экраны. Архитектура межсетевого экрана. Фильтр пакетов. Фильтр инспекции состояний. Транслятор адресов. Транспортные шлюзы. Шлюзы приложений (прокси-сервера). Системы обнаружения атак и вторжений. Классификация COB. Системы тунелирования. Протокол PPPoE. Обзор протокола PPPoE. Обзор протокола PPP. Виртуальные частные сети. Обзор протоколов PPTP и L2TP. Протокол IPSEC. Протокол SSL/TLS. Безопасность удалённого управления. Аудит безопасности протокола SNMP. Версии протокола SNMP. Модель протокола SNMP. Протокол SNMPv3. Безопасность протокола SNMPv3. Протокол SSH. Протокол SSH. Существующее программное обеспечение. Рекомендации по безопасности использования протокола SSH.
Реализуемые компетенции	ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей. ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

	ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях. ПК-1. Способен разрабатывать требования по защите информации для формирования политик безопасности компьютерных систем и сетей. ПК-2. Способен проводить анализ безопасности компьютерных систем.
Результаты освоения дисциплины (модуля)	ОПК-8 Знать: основные положения теории помехоустойчивого кодирования; принципы разработки алгоритмов и устройств помехоустойчивого кодирования; базовые методы статистического анализа помехоустойчивости кодеров в современных технических системах передачи информации; фундаментальные понятия теории кодирования и сжатия информации, а также основные методы и алгоритмы кодирования и сжатия; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений. Уметь: использовать алгоритмы кодирования и сжатия информации основных классов в задачах анализа информационной безопасности; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем; умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. Владеть: основными понятиями и навыками теории алгоритмов кодирования и сжатия информации; способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах; навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств;

навыками настройки межсетевых экранов; методиками анализа сетевого трафика.

ОПК-10

Знать: базовые понятия теории эллиптических кривых; основные задачи, решаемые криптографическими методами; математические модели шифров, подходы к оценке их стойкости; зарубежные и российские криптографические стандарты; типовые криптопротоколы, используемые в сетях связи; основные типы криптопротоколов и принципов их построения с использованием шифрсистем; средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях TCP/IP; знает основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений; фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации; основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума; основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга); понятие пропускной способности канала связи, прямую и обратную теоремы кодирования.

Уметь: корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность); решать типовые задачи кодирования и декодирования; работать с научно-технической литературой по тематике дисциплины.

Владеть: навыками использования типовых криптографических алгоритмов; подходами к разработке и анализу безопасности криптографических протоколов; навыками настройки межсетевых экранов; методиками анализа сетевого трафика; основами построения математических моделей текстовой информации и моделей систем передачи информации; навыками применения математического аппарата для решения прикладных теоретико-информационных задач.

ОПК-16

Знать: средства и методы хранения и передачи

	аутентификационной информации; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений. Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. Владеть: навыками настройки межсетевых экранов; владеет методиками анализа сетевого трафика. ПК-1 Знать: принципы построения компьютерных систем и сетей; модели безопасности компьютерных систем; виды политик безопасности компьютерных систем и сетей; принципы построения средств криптографической защиты информации; национальные, межгосударственные и международные стандарты в области защиты информации; возможности используемых и планируемых к использованию средств защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации Уметь: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации. Владеть: навыками разработки технических заданий на создание средств защиты информации; классификации информационной системы по требованиям защиты информации. ПК-2 Знать: уязвимости компьютерных систем и сетей; криптографические методы защиты информации; принципы построения систем управления базами данных; средства анализа конфигураций; национальные, межгосударственные и международные стандарты в области защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации Уметь: анализировать компьютерную систему с целью определения уровня защищенности и доверия; прогнозировать возможные пути развития действий нарушителя информационной безопасности; производить анализ политики безопасности на предмет адекватности; проводить мониторинг, анализ и сравнение
--	---

	эффективности программно-аппаратных средств защиты информации в операционных системах; составлять и оформлять аналитический отчет по результатам проведенного анализа; разрабатывать предложения по устранению выявленных уязвимостей. Владеть: навыками определения уровня защищенности и доверия в компьютерных системах; оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; оценки соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам; подготовки аналитического отчета по результатам проведенного анализа; формулирования предложений по устранению выявленных уязвимостей.
Трудоемкость, з.е.	5
Форма отчетности	Экзамен, семестр 10. Курсовая работа, 10 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Столлинкс, В. Основы защиты сетей. Приложения и стандарты: Пер. с англ. – М.: Изд. дом "Вильямс", 2002. – 430 с.: ил. – Парал. тит. л.англ. – ISBN 5-8459-0298-3 (рус.), экземпляров 19 2. Олифер, В. Г. Компьютерные сети: принципы, технологии, протоколы: [учебник] / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб.: Питер, 2011. – 944 с.: ил. – (Учебник для вузов). – На учебнике гриф: Рек.МО. – Библиогр.: с. 917. – ISBN 978-5-469-00920-0, экземпляров 10
Дополнительная литература	3. Практикум по дисциплине Сетевая безопасность и ее планирование Электронный ресурс / сост.: В. А. Докучаев [и др.] / ред. В. А. Докучаев. – Практикум по дисциплине Сетевая безопасность и ее планирование, 2022-04-04. – Москва: Московский технический университет связи и информатики, 2016. – 28 с. – Книга находится в премиум-версии ЭБС IPR BOOKS. – ISBN 2227-8397, экземпляров неограниченно 4. Защита от хакеров корпоративных сетей / Дэвид М. Ахмад, Идо Дубравский, Хал Флинн и др.; пер. с англ. А. А. Петренко. – 2-е изд., (обновленное и доп. новыми фактами, ставшими известными по прошествии года после 1-го изд.). – М.: Компания АйТи: ДМК-Пресс, 2005. – 863 с.: ил. – (Информационная безопасность). – ISBN 5-98453-015-5. – ISBN 1-928994-70-9, экземпляров 1