

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:
 b47f96eea65a2d6e27b94abf7db0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Методы и средства криптографической защиты информации
Содержание	Общие сведения о криптографических методах защиты информации. Классификация шифров. Криптографическая стойкость шифров. Подходы к моделированию криптосистем. Принципы построения и функционирования блочных шифров. Симметричные криптоалгоритмы. Принципы построения и функционирования поточных шифров. Принципы построения криптоалгоритмов с открытым ключом. Современные криптоалгоритмы с открытым ключом. Имитостойкость и помехоустойчивость шифров. Основные методы криптоанализа. Криптоанализ симметричных алгоритмов. Криптоанализ асимметричных алгоритмов Криптографические хэш-функции. Электронная цифровая подпись. Управление криптографическими ключами. Реализации криптографических алгоритмов: программная, аппаратная, программно-аппаратная. Композиция криптографических методов в систему защиты информации. Криптографические стандарты.
Реализуемые компетенции	ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности. ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности. ПК-4. Способен проводить инструментальный анализ защищенности компьютерной системы и осуществлять поиск уязвимостей программного обеспечения
Результаты освоения дисциплины (модуля)	ОПК-9 Знать: типовые криптопротоколы, используемые в сетях связи; основные типы криптопротоколов и принципов их построения с использованием шифрсистем; технические каналы утечки информации; возможности технических средств перехвата информации; знает основные характеристики сигналов электросвязи, спектры и виды модуляции; принципы построения и функционирования систем и сетей передачи информации; способы передачи и распределения информации в телекоммуникационных системах и сетях; основные телекоммуникационные протоколы. Уметь: разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств; пользоваться нормативными документами в области технической защиты информации;

	анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи. Владеть: навыками использования типовых криптографических алгоритмов; подходами к разработке и анализу безопасности криптографических протоколов. 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 ТСП/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-13

Знать: средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; основы физической защиты объектов информатизации; общие принципы построения и использования современных языков программирования высокого уровня; язык программирования высокого уровня (объектно-ориентированное программирование); язык ассемблера персонального компьютера; современные технологии программирования; показатели качества программного обеспечения; базовые структуры данных; основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки вычислительной сложности.

Уметь: формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем; пользоваться нормативными документами в области технической защиты информации; анализировать и оценивать угрозы информационной безопасности объекта; формализовать поставленную задачу; работать с интегрированными средами разработки программного обеспечения; разрабатывать эффективные алгоритмы и программы; проводить оценку вычислительной сложности алгоритма; планировать разработку сложного программного обеспечения.

Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей эффективности технической защиты информации; навыками разработки, отладки, документирования и тестирования программ; навыками использования инструментальных средств отладки и дизассемблирования программного кода; методами оценки качества готового программного обеспечения; навыками разработки алгоритмов для решения типовых профессиональных задач.

ПК-4

Знать: принципы построения компьютерных систем и сетей; формальные модели безопасности компьютерных систем и сетей; принципы построения систем обнаружения компьютерных атак; методы обработки данных мониторинга безопасности компьютерных систем и сетей; порядок создания и структура

	отчета, создаваемого по результатам проверок; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; криптографические протоколы, применяемые в компьютерных сетях; 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: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет. Владеть: навыками выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнения анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составления отчетов по результатам проверок.
Трудоемкость, з.е.	7
Формы отчетности	Зачет, 5 семестр; зачет с оценкой, 6 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Рябко, Борис Яковлевич. Криптографические методы защиты информации: учеб. пособие для вузов / Б. Я. Рябко, А. Н. Фионов. – М.: Горячая линия – Телеком, 2012. – 229 с.: ил., табл. – Гриф: Рек. УМО. – Библиогр.: с. 218-221. – Предм. указ.: с. 222-226. – 500 экз. – ISBN 978-5-9912-0286-2. 2. Бабенко, Л.К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. – М: Гелиос АРВ, 2012. 3. Шанкин, Г.П. Криптография / Г.П. Шанкин, А.В. Бабаш. – М.: Солон-Р, 2012. 4. Мао, В. Современная криптография: теория и практика / В. Мао. – М.: Издательский дом «Вильямс», 2011. 5. Сمارт, Н. Криптография / Н. Смарт. – М.: Техносфера, 2010.
Дополнительная литература	1. Гашков, Сергей Борисович. Криптографические методы защиты информации: [учеб. пособие*]. – М.: Академия, 2010. – 299 с. – (Высшее проф. образование). – На обл.: Информационная безопасность. – Предм. указ.: с. 285-286. – Библиогр.: с. 287-294. – ISBN 978-5-7695-4962-5. 2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер. – М.: Триумф, 2003. 3. Грушо, А.А. Анализ и синтез криптоалгоритмов. Курс лекций / А.А. Грушо, Е.Е. Тимонина, Э.А. Применко. – Йошкар-Ола: МФ МОСУ, 2000. 4. Фомичев, В.М. Дискретная математика и криптология. Курс лекций / Под общ.ред. д-ра физ.-мат. наук Н.Д. Подуфалова. – М.: ДИАЛОГ-МИФИ, 2003.

	5. Осипян, В.О. Криптография в упражнениях и задачах / В.О. Осипян, К.В. Осипян. – М.: Гелиос-АРВ, 2004. 6. Болотов, А.А. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М.: КомКнига, 2006. 7. Фергюсон, Н. Практическая криптография / Н. Фергюсон, Б. Шнайер. – М.: Издательский дом «Вильямс», 2005. 8. Курсы «Математика криптографии и теория шифрования», «Стандарты информационной безопасности», «Криптографические основы безопасности», «Управление ключами шифрования и безопасность сети», «Инфраструктуры открытых ключей». www.intuit.ru 9. ГОСТ 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». М.: Издательство стандартов, 2003. 10. ГОСТ Р 34.11-94. «Информационная технология. Криптографическая защита информации. Функции хэширования». М.: Издательство стандартов, 2001. 11. ГОСТ Р 34.10-2001.» Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». М.: Издательство стандартов, 2005. 12. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005). // Бюллетень нормативных актов федеральных органов исполнительной власти. – №11. – 14.03.2005. 13. Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. // «Бюллетень нормативных актов федеральных органов исполнительной власти». – №34. – 20.08.2001. 14. ГОСТ Р 52069.0-2003. Защита информации. Система стандартов. Основные положения. М.: ИПК Издательство стандартов, 2003 15. ГОСТ Р ИСО/МЭК 15408-2008. Критерии оценки безопасности информационных технологий. М.: ИПК Издательство стандартов, 2009 ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. М., ИПК Издательство стандартов, 2004
--	---