

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:
 b47f96eea65a2d6e27b94abf7bb0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Криптографические протоколы
Содержание	Введение в криптографические протоколы. Протоколы подбрасывания монеты по телефону. Протоколы привязки к биту. Разделение секрета. Интерактивные системы доказательства. Интерактивные системы доказательства с нулевым разглашением. Протоколы идентификации и аутентификации. Покер по телефону. Слепая подпись. Скрытый канал.
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. ПК-3. Способен проводить сертификацию программно-аппаратных средств защиты информации и анализ результатов.
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 ТСР/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.

ПК-3

Знать: национальные, межгосударственные и международные стандарты в области защиты информации; национальные стандарты на проведение научно-исследовательских и опытно-конструкторских работ, сертификационных испытаний и создание систем защиты информации; способы организации работ при проведении сертификации программно-аппаратных средств защиты; принципы построения средств криптографической защиты информации; нормативные

	<p>правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации.</p> <p>Уметь: анализировать компьютерную систему с целью определения уровня защищенности и доверия; использовать профили защиты и задания по безопасности; применять инструментальные средства проведения сертификационных испытаний; составлять и оформлять аналитический отчет по проведенным сертификационным испытаниям; делать выводы по оценке защищенности на основании аналитического отчета.</p> <p>Владеть: навыками проведения теоретических исследований уровней защищенности компьютерных систем и сетей; проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; проведения сертификационных испытаний с использованием инструментальных средств; подготовки аналитического отчета по результатам проведенных сертификационных испытаний; формулирования выводов по оценке защищенности.</p>
Трудоемкость, з.е.	4
Формы отчетности	Зачет с оценкой, 7 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	<p>1. Акиншина Г.В. Криптографические протоколы: учеб. пособие: специальности: 090301 – Компьютерная безопасность, 090103 – Организация и технология защиты информации / Г. В. Акиншина, Ю. В. Быков; М-во образования и науки Рос. Федерации, ГОУ ВПО "Ставроп. гос. ун-т". – Ставрополь: Изд-во СГУ, 2011. – 174 с.</p>
Дополнительная литература	<p>1. Агibalов Г.П. Избранные теоремы начального курса криптографии: Учебное пособие. – Томск: Изд-во НТЛ, 2005. – 116 с.</p> <p>2. Анохин М.И., Варновский Н.П., Сидельников В.М., Яценко В.В. Криптография в банковском деле. – М.: МИФИ, 1997.</p> <p>3. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2005. – 229 с.: ил.</p> <p>4. Черемушкин, Александр Васильевич. Криптографические протоколы: основные свойства и уязвимости: учеб. пособие / А. В. Черемушкин. – М.: Академия, 2009. – 272 с.</p> <p>5. Шнайер Б., Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Изд-во ТРИУМФ, 2009. – 816 с.</p>