

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:
 b47f96eea65a2dc27b94ab71bb0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Теория информации
Содержание	Энтропия и взаимная информация. Дискретные источники сообщений. Кодирование дискретных источников сообщений. Дискретные каналы связи. Теоремы кодирования для дискретных каналов без памяти. Коды, исправляющие ошибки.
Реализуемые компетенции	ОПК-10
Результаты освоения дисциплины (модуля)	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.
Трудоемкость, з.е.	5
Формы отчетности	Экзамен, 4 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Котенко, В. В. Теория информации: учебное пособие / В. В. Котенко, К. Е. Румянцев. – Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018. – 239 с. 2. Кудряшов Б. Д. Теория информации. Изд. Питер, 2009. – 320 с. 3. Яглом, А. М., Яглом, И. М. Вероятность и информация. – М.: КомКнига, 2007. – 512 с.
Дополнительная литература	1. Санников, В. Г. Теория информации и кодирования: учебное пособие / В. Г. Санников. – Москва: Московский технический университет связи и информатики, 2015. – 95 с. 2. Акулиничев, Ю. П. Теория и техника передачи информации: учебное пособие / Ю. П. Акулиничев, А. С. Бернагдт. – Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2012. – 210 с.