

Аннотация дисциплины

Наименование дисциплины	Персональная кибербезопасность
Содержание	<p>Основные понятия персональной кибербезопасности. Информационная безопасность и кибербезопасность. Свойства оцифрованной информации. Причины киберпреступлений. Проблемы кибербезопасности. Моделирование угроз персональной кибербезопасности. Анализ рисков как основа управления персональной кибербезопасностью. Модель угроз STRIDE. Инструменты анализа и контроля информационных рисков. Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: CIA, Гексада Паркера, 5A, STRIDE. Криптографические алгоритмы. Обзор алгоритмов шифрования и тенденций развития криптографии. Круг задач, на решение которых ориентированы криптографические методы. Основные понятия и определения криптографии. Рекомендации Microsoft по применению криптографических алгоритмов. Отечественный стандарт шифрования данных ГОСТ 28147-89. Американский стандарт шифрования данных AES. Концепция криптосистемы с открытым ключом. Классификация криптографических алгоритмов. Алгоритмы шифрования с секретным ключом (симметричные). Блочные шифры. Поточные шифры. Алгоритмы шифрования с открытым ключом (асимметричные). Криптоалгоритмы с секретным ключом. Методы криптоанализа. Обзор современных методов криптоанализа. Классические методы. Новый вид криптоанализа – атаки по побочным каналам. Квантовый криптоанализ. Исходы криптоанализа. Методы криптоанализа и их влияние на развитие криптографии. Предельные возможности по взлому шифров методом полного перебора ключей. Применимость различных типов криптоатак к симметричным и асимметричным криптосистемам и хеш-функциям. Перспективные технологии криптоанализа. Экономическая эффективность средств обеспечения персональной кибербезопасности. Оценка средств криптозащиты. Экономическое обоснование расходов на обеспечение персональной кибербезопасности. Обоснованный выбор мер и средств обеспечения персональной кибербезопасности. Преимущества и недостатки существующих методов обоснования инвестиций в средства обеспечения персональной кибербезопасности. Набор финансово-экономических показателей для оценки эффективности средств обеспечения персональной кибербезопасности с экономических позиций. Методика оценки экономической эффективности средств обеспечения персональной кибербезопасности. Инструменты организации персональной кибербезопасности. Обзор антивирусных средств защиты при организации системы персональной кибербезопасности. Антивирусная защита персональных компьютеров и мобильных устройств. Брандмауэры. Средства аппаратной защиты информации. Организация программно-аппаратных средств персональной кибербезопасности. Персональная кибербезопасность в интернет-банкинге. Технологии интернет-банкинга. Технологии биржевой торговли. Правила организации персональной кибербезопасности в интернет-банкинге. Программно-аппаратные</p>

	<p>средства защиты данных в процессах интернет-банкинга и биржевой торговли. Современные методы защищенной аутентификации. Методы авторизации пользователя при работе в сети Интернет. Авторизация и аутентификация. Методы создания и хранения паролей. Электронная цифровая подпись. Методы формирования электронной цифровой подписи.</p>
Реализуемые компетенции	ОПК-2. Способен вести обработку, анализ и представление информации в профессиональной деятельности с использованием информационных и компьютерных технологий
Результаты освоения дисциплины (модуля)	<p>Код компетенции ОПК-2:</p> <p>Знать: основные причины выявления киберугроз; методы выявления угроз информационной безопасности; правила первичного блокирования киберугроз; методы проведения профилактических работ по устранению киберугроз.</p> <p>Уметь: проводить первичный анализ на предмет выявления киберугроз; осуществлять первичное блокирование киберугроз.</p> <p>Владеть: навыком работы со стандартным набором инструментов пользователя, для выявления угроз информационной безопасности автоматизированного рабочего места; техниками выявления методов социальной инженерии.</p>
Трудоемкость, з.е.	1 з.е.
Форма отчетности	Зачет – 2 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	<p>1. Петренко В.И. Защита персональных данных в информационных системах [Электронный ресурс] : учебное пособие / В.И. Петренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 201 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66023.html</p> <p>2. Макаров А.М. Организация защиты персональных данных [Электронный ресурс] : лабораторный практикум / А.М. Макаров, И.В. Калиберда, К.О. Бондаренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 92 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/62971.html</p>
Дополнительная литература	<p>1. Скрипник Д.А. Обеспечение безопасности персональных данных [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 121 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52153.html</p> <p>2. Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» [Электронный ресурс] / А.И. Савельев. — Электрон. текстовые данные. — М. : Статут, 2017. — 320 с. — 978-5-8354-1365-2. — Режим доступа: http://www.iprbookshop.ru/65895.html</p>