

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

26 мая 2020 г.

Кафедра «Управление и защита информации»

Автор Стряпкин Леонид Игоревич

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Криптографические методы защиты информации»

Специальность:	<u>10.05.01 – Компьютерная безопасность</u>
Специализация:	<u>Информационная безопасность объектов информатизации на базе компьютерных систем</u>
Квалификация выпускника:	<u>Специалист по защите информации</u>
Форма обучения:	<u>очная</u>
Год начала подготовки	<u>2020</u>

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии</p>  <p style="text-align: right;">С.В. Володин</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p style="text-align: center;">Протокол № 16 21 мая 2020 г. Заведующий кафедрой</p>  <p style="text-align: right;">Л.А. Баранов</p>
---	--

Москва 2020 г.

1. Цели освоения учебной дисциплины

Основной целью изучения дисциплины «Криптографические методы защиты информации» является формирование у обучающегося компетенций для следующих видов деятельности:

? научно-исследовательская;

? проектная;

? контрольно-аналитическая;

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Научно-исследовательская деятельность:

- сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности;

Проектная деятельность:

- разработка технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов;

- разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием.

Контрольно-аналитическая деятельность:

- предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей; применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;

- подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей.

Задачи дисциплины:

- изложение основополагающих принципов защиты информации с помощью криптографических методов и изучение их практического применения.

- развитие у обучаемых системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами с помощью методов криптографии;

- изучение принципов синтеза и анализа криптосистем, математических методов оценки их стойкости.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Криптографические методы защиты информации" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОПК-2	Способен применять программные средства системного и прикладного назначения для решения профессиональных задач
ОПК-7	Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей
ОПК-8	Способен проводить анализ корректности реализации эффективных комбинаторных, теоретико-числовых и криптографических алгоритмов и протоколов применительно к конкретным условиям
ОПК-12	Способен участвовать в разработке программно-аппаратных средств

	защиты информации компьютерных систем и сетей
ПКО-4	Способен участвовать в разработке подсистемы информационной безопасности компьютерной (в том числе автоматизированной) системы включая разработку программно-аппаратных средств защиты информации, защищенных операционных систем, систем управления базами данных, компьютерных сетей, систем антивирусной защиты, средств криптографической защиты информации
ПКО-6	Способен проводить оценку эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации

4. Общая трудоемкость дисциплины составляет

5 зачетных единиц (180 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Криптографические методы защиты информации» осуществляется в форме лекций и практических занятий. Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 30 % являются традиционными классическими лекционными (объяснительно-иллюстративными), и на 70 % с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа лекция. Практические занятия организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач). Остальная часть практического курса проводится с использованием интерактивных (диалоговых) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения. Часть практических работ, выполняемых с использованием ПЭВМ, подразумевает оформление соответствующего отчёта. Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относятся отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях. .

6. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1

Основы криптографии

Тема: Введение в криптографию

Структурная схема защищённой системы передачи информации. Роль криптографических методов защиты в её структуре. Понятия модуляции, кодирования, шифрования. Основные задачи защиты информации криптографическими методами. Понятие симметричной шифросистемы и её структурная схема. Понятие асимметричной шифросистемы и её структурная схема. Исторические шифры, их примеры.

Тема: Теоретические положения криптографии

Понятия алфавита, стандартной кодировки и шифротекста. Лавинный эффект в шифровании.

Частотный криптоанализ

Классификация атак в криптографии. Основные понятия.

Вычислительно сложные задачи математики. Понятие «односторонней» функции и «односторонней функции с секретом».

Элементы теории чисел. Функция Эйлера и её особенности, теоремы Эйлера и Ферма.

РАЗДЕЛ 2

Криптосистемы с открытым ключом

Тема: Криптосистемы на базе задачи дискретного логарифмирования

Криптосистема Диффи — Хеллмана

Криптосистема (бесключевой протокол) Шамира

Криптосистема Эль-Гамала.

Тема: Криптосистемы на базе задачи факторизации

Криптосистема RSA.

РАЗДЕЛ 3

Электронно-цифровая подпись (ЭЦП)

Тема: Общие сведения об ЭЦП

Назначение и классификация (НЭП, ПЭП, КЭП)

Тема: Алгоритмы ЭЦП

Алгоритм ЭЦП Эль-Гамала

Алгоритм ЭЦП RSA

Тема: Хеш-функции

Понятие и основные свойства хеш-функции. Коллизии первого и второго рода.

РАЗДЕЛ 4

Криптосистемы на эллиптических кривых

Тема: Общие сведения об эллиптических кривых

Экспоненциальная и субэкспоненциальная сложность алгоритмов

Эллиптические кривые. Понятие дискриминанта и сингулярности.

Операция композиции точек на кривой.

Свойства точек на эллиптической кривой.

Тема: Алгоритмы на эллиптических кривых

Выбор параметров кривой.

Построение криптосистем на эллиптических кривых.

Шифр Эль-Гамала на эллиптической кривой.

Стандарт ЭЦП ГОСТ Р 34.10

РАЗДЕЛ 5

Обзор криптографических алгоритмов и средств

Тема: Введение

Классификация криптографических алгоритмов и средств защиты информации

Тема: Блочные шифры

Основные особенности построения блочных шифров с использованием SP-сетей и сетей Фейстеля

Тема: Алгоритм DES и его вариации

Описание алгоритма DES

Тема: Алгоритм AES

Описание алгоритма AES

Тема: Поточные шифры.

Основные особенности построения поточных шифров

Тема: Аппаратное шифрование и скремблирование.

Виды скремблирования, особенности аппаратного шифрования

Тема: Управление ключами

Распределение ключей на базе алгоритма Диффи-Хеллмана

Тема: Стеганография: история и современность

Обзор стеганографических методов защиты информации

Тема: Аутентификация и идентификация.

Криптографические основы аутентификации пользователей компьютерных систем.

Тема: Применение криптографии в радиосвязи

Системы радиосвязи с ППРЧ и с использованием шумоподобных сигналов, расширение спектра, стандарт ARCO25.

Тема: Помехоустойчивость шифров.

Шифры, не размножающие искажений

Тема: Современные криптосистемы с открытым ключом

Асимметричные криптосистемы, их особенности.

Тема: Современные криптосистемы с секретным ключом

Симметричные криптосистемы, их особенности.

РАЗДЕЛ 6

Генераторы псевдослучайных последовательностей

Тема: Общие сведения о генераторах псевдослучайных последовательностей.

Основные понятия и свойства генераторов ПСП.

Тема: Программные и аппаратные генераторы ПСП

Принципы построения программных и аппаратных генераторов ПСП

Тема: Регистры РСЛОС

Регистры сдвига с линейными обратными связями как генераторы псевдослучайных

последовательностей

Тема: Структуры генераторов ПСП на базе РСЛОС
Каскадирование РСЛОС и мажори-тарная структура на их базе.

Тема: Характеристики генераторов ПСП.
Вероятностные характеристики РСЛОС, предсказуемость ПСП.

РАЗДЕЛ 7
Курсовая работа

Экзамен