

**Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное
учреждение высшего образования
«Казанский национальный исследовательский технический университет
им. А.Н. Туполева-КАИ»
(КНИТУ-КАИ)**

Институт **Компьютерных технологий и защиты информации**

Кафедра **Компьютерных систем**

АННОТАЦИЯ

к рабочей программе

«Криптографические методы и средства защиты информации»

Индекс по учебному плану: **Б1.В.ДВ.02.01**

Направление подготовки: **09.04.01 «Информатика и вычислительная техника»**

Квалификация: **магистр**

Магистерская программа: **Системное и сетевое администрирование
(информатика как вторая компетенция)**

Виды профессиональной деятельности: **научно-исследовательская**

Разработчик: к.т.н., доцент кафедры СИБ Корнилов Г.С.

Казань - 2017 г.

1. Цель и задачи учебной дисциплины

Цель изучения дисциплины: Овладение теоретической и практической базой по методам и средствам криптографической защиты информации.

Задачи изучения дисциплины:

- определение места криптографической защиты информации в различных сферах жизнедеятельности человека;
- приобретение знаний по наиболее известным симметричным и асимметричным криптографическим алгоритмам и функциям хэширования;
- ознакомление студентов с основными методами криптоанализа и условиями их применения;
- обучение методам выбора криптографических алгоритмов и их параметров, обеспечивающих необходимую стойкость защиты..

2. Перечень компетенций, которые должны быть реализованы в ходе освоения дисциплины

Перечень компетенций, которые должны быть реализованы в ходе освоения дисциплины: *ПК-7*.

3. Структура дисциплины и трудоемкость ее составляющих

Таблица. Распределение фонда времени по семестрам, неделям и видам занятий для очной формы обучения

Наименование раздела и темы	Всего часов	Виды учебной деятельности, включая самостоятельную работу студентов и трудоемкость (в часах / интерактивные часы)				Коды составляющих компетенций	Формы и вид контроля освоения составляющих компетенций (из фонда оценочных средств)
		лекции	ла. раб.	пр. зан.	сам. раб.		
Раздел 1. Введение, элементы теории чисел, классические симметричные методы шифрования							ФОС ТК-1
Тема 1.1. Задачи и программа курса. Место изучаемой дисциплины среди других математических и общепрофессиональных дисциплин	5/1	1/1	–	–	4	ПК-7.3	Тесты

Тема 1.2. Модулярная арифметика. Алгоритм Евклида для нахождения наибольшего общего делителя. Вычисление обратных величин. Квадратичные вычеты. Вычисления в конечных полях	5/1	1/1	–	–	4	ПК-7.3	Тесты
Тема 1.3. Шифры перестановки, шифрование методом гаммирования	6/1	2/1	–	–	4	ПК-7.3	Тесты
<i>Раздел 2. Симметричные криптосистемы, асимметричные криптосистемы, методы криптоанализа</i>							<i>ФОС ТК-2</i>
Тема 2.1. Американский стандарт шифрования данных DES, Алгоритм шифрования данных IDEA, ГОСТ 28147-89. Блочные и поточные шифры.	16/2	2/1	8/1	–	6	ПК-7.3 ПК-7.У	Тесты, отчет о выполнении лабораторной работы
Тема 2.2. Концепция криптосистемы с открытым ключом. Комбинированный метод шифрования	44/6	2/2	8/4	–	34	ПК-7.3 ПК-7.У ПК-7.В	Тесты, отчет о выполнении лабораторной работы
Тема 2.3. Основные методы дешифрования, методы анализа, сводящиеся к решению линейных систем уравнений, корреляционный метод криптоанализа, методы анализа поточных шифров	12/1	2/1	–	–	10	ПК-7.3	Тесты
<i>Раздел 3. Идентификация и проверка подлинности, Электронная цифровая подпись, управление криптографическими ключами</i>							<i>ФОС ТК-3</i>
Тема 3.1. Основные понятия и концепции. Идентификация и аутентификация пользователя. Протоколы идентификации с нулевой передачей знаний.	7/1	1/1	–	–	6	ПК-7.3	Тесты
Тема 3.2. Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Генерация ключей. Хранение ключей.	13/5	1/1	8/4	–	4	ПК-7.3 ПК-7.У	Тесты, отчет о выполнении лабораторной работы
Экзамен	36	–	–	–	36	ПК-7.3 ПК-7.У ПК-7.В	<i>ФОС ПА - комплексное задание</i>
ИТОГО:	144/18	12/9	24/9		108		

4. Учебно-методическое и информационное обеспечение дисциплины (модуля)

4.1. Основная литература

1. Мельников В.П. Защита информации: учебник / В.П. Мельников, А.И. Куприянов, А.Г. Схиртладзе – М.:Академия, 2014. – 304 с.
2. Платонов В.В. Программно-аппаратные средства защиты информации [Текст] : учеб. для студ. вузов / В. В. Платонов, 2013. – М.: Издательский центр «Академия», - 336 с.
3. Хорев П.Б. Криптографические методы и средства защиты информации : учеб. пособие / П. Б. Хорев. М.: Форум, 2012 - 352 с.

4.2. Основное информационное обеспечение дисциплины (модуля)

1. Корнилов Г.С. Криптографические методы и средства защиты информации [Электронный ресурс]: курс дистанц. обучения по направлению подготовки магистров 09.04.01 «Информатика и вычислительная техника» ФГОС3+ / КНИ-ТУ-КАИ, Казань, 2015 – Доступ по логину и паролю. URL: https://bb.kai.ru:8443/webapps/blackboard/execute/content/blankPage?cmd=view&content_id=_86247_1&course_id=_9577_1

5. Кадровое обеспечение дисциплины (модуля)

5.1. Базовое образование

Высшее образование в области информатики и вычислительной техники и /или наличие ученой степени и/или ученого звания в указанной области и /или наличие дополнительного профессионального образования – профессиональной переподготовки в области информатики и вычислительной техники и /или наличие заключения экспертной комиссии о соответствии квалификации преподавателя профилю преподаваемой дисциплины.

5.2. Профессионально-предметная квалификация преподавателей

Наличие научных и/или методических работ по организации или методическому обеспечению образовательной деятельности по направлению информатики и вычислительной техники, выполненных в течение трех последних лет.

5.3. Педагогическая (учебно-методическая) квалификация преподавателей

К ведению дисциплины допускаются кадры, имеющие стаж научно-педагогической работы (не менее 1года), практический опыт работы в области информатики и вычислительной техники на должностях руководителей или ведущих специалистов более 3 последних лет.

Обязательное прохождение повышения квалификации (стажировки) не реже чем один раз в три года соответствующее области информатики и вычислительной техники, либо в области педагогики.