Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Казанский национальный исследовательский технологический университет»
(ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ
Проректор по УР
Бурмистров А.В.
_____
«_1_» _____04_____ 2019 г.

РАБОЧАЯ ПРОГРАММА

По дисциплине «Методы защиты компьютерной информации»
Направление подготовки - 02.03.03 «Математическое обеспечение и администрирование информационных систем»
Профиль/специализация - Информационные системы и базы данных
Квалификация выпускника - бакалавр
Форма обучения - очная
Институт, факультет - Нефти, химии и нанотехнологий, Наноматериалов и нанотехнологий
Кафедра-разработчик рабочей программы - Интеллектуальных систем и управления информационными ресурсами
Курс 4, семестр 7,8

	Часы	Зачетные единицы
Лекции	36	1
Практические занятия		
Лабораторные занятия	72	2
Контроль самостоятельной работы		
Самостоятельная работа	108	3
Форма аттестации зачёт,экзамен	36	1
Всего	252	7

Казань, 2019 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования (№ 809 от 23.08.2017) по направлению 02.03.03 «Математическое обеспечение и администрирование информационных систем» на основании учебного плана набора обучающихся 2019 г.

Разработчик программы:
Доцент А.С. Титовцев

Рабочая программа рассмотрена и одобрена на заседании кафедры ИСУИР, протокол от 1.07. 2019 г. № 11

Зав. кафедрой А.П. Кирпичников

УТВЕРЖДЕНО

Начальник УМЦ, доцент Л.А. Китаева

1. Цели освоения дисциплины

Целями освоения дисциплины «Методы защиты компьютерной информации» являются

а) формирование знаний о методах построения алгоритмов криптографической защиты данных,

б) обучение способам применения криптосистем с открытым ключом,

в) раскрытие сущности процессов, происходящих при зашифровании и расшифровании данных.

2. Место дисциплины (модуля) в структуре основной образовательной программы

Дисциплина «Методы защиты компьютерной информации» относится к части ООП формируемой участниками образовательных отношений и формирует у бакалавров по направлению подготовки 02.03.03 набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Методы защиты компьютерной информации» бакалавр по направлению подготовки 02.03.03 должен освоить материал предшествующих дисциплин должен освоить материал предшествующих дисциплин:

а) математический анализ

б) общая, линейная и высшая алгебра

в) теория вероятностей и математическая статистика

г) теория чисел

д) математическая логика

е) дискретная математика

Дисциплина «Методы защиты компьютерной информации» является предшествующей и необходима для успешного усвоения последующих дисциплин:

а) теория принятия решений

б) проектирование защищенных телекомуникационных систем

Знания, полученные при изучении дисциплины могут быть использованы при прохождении практик и выполнении выпускной квалификационной работы.

3. Компетенции и индикаторы достижения компетенции обучающегося, формируемые в результате освоения дисциплины

ПК-5 - Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования

ПК-5.1 - Знает современные методы разработки и реализации алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования

ПК-5.2 - Умеет разрабатывать и реализовывать алгоритмы математических моделей на базе языков программирования и пакетов прикладных программ моделирования

ПК-5.3 - Владеет навыками разработки и реализации алгоритмов на

базе языков программирования и пакетов прикладных программ моделирования

В результате освоения дисциплины обучающийся должен

1) Знать:

а) историю развития криптографической защиты данных;

б) методы построения основных алгоритмов зашифрования и расшифрования данных.

2) Уметь:

а) решать задачи синтеза криптографических алгоритмов зашиты данных;

б) применять криптографические методы для построения алгоритмов электронной цифровой подписи.

3) Владеть:

а) современными методами построения симметричных алгоритмов шифрования данных;

б) основными методами построения криптосистем с открытым ключом;

в) методами построения безопасных протоколов передачи данных

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 7 зачетных единиц, 252 часов.

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)					Оценочные средства для проведения промежуточной аттестации по разделам
			Лекции	Практические занятия	Лабораторные работы	КСР	СРС	
1	Исторический очерк развития криптографии	7	3		6		9	
2	Математические основы криптографии. Основные понятия криптографии	7	3		6		9	
3	Классификация шифров по различным признакам	7	3		6		9	Контрольная работа
4	Шифры перестановки	7	3		6		9	
5	Шифры замены	7	3		6		9	
6	Шифры гаммирования	7	3		6		9	
7	Надежность шифров	8	2		4		6	Контрольная работа
8	Блочные системы шифрования	8	2		4		6	
9	Поточные системы шифрования	8	2		4		6	
10	Системы шифрования с открытыми ключами	8	2		4		6	Контрольная работа
11	Идентификация	8	2		4		6	
12	Криптографические хеш-функции	8	2		4		6	
13	Цифровые подписи	8	2		4		6	
14	Протоколы распределения ключей	8	2		4		6	
15	Управление ключами	8	2		4		6	Контрольная работа
ИТОГО			36		72		108	
Форма аттестации			зачет/экзамен (36 ч)					

5. Содержание лекционных занятий по темам с указанием формируемых компетенций

№	Раздел дисциплины	Часы	Тема лекционного занятия, краткое содержание	Индикаторы достижения компетенции
1	Исторический очерк развития криптографии	3	Рассматривается ряд конкретных примеров шифров и их применения, известных начиная с античных времен и до современного периода времени. Краткая характеристика рассмат-риваемых шифров.	ПК-5.1, ПК-5.2, ПК-5.3
2	Математические основы криптографии. Основные понятия криптографии	3	Операции над множествами. Бинарные отношения на множестве Бинарные операции на множестве. Алгебраические структуры (группы, кольца и т.д.). Криптография. Конфиден-циальность. Целостность. Аутентификация. Цифровая подпись. Управление секретными ключами. Предварительное распределение ключей. Пересылка ключей. Открытое распространение ключей. Схема разделения секрета. Инфраструктура открытых ключей. Сертификаты. Центры сертификации. Формальные модели шифров. Модели открытых текстов. Математические модели открытого текста. Критерии распо-знавания открытого текста.	ПК-5.1, ПК-5.2, ПК-5.3
3	Классификация шифров по различным признакам	3	Математическая модель шифра простой замены. Классификация шифров замены.	ПК-5.1, ПК-5.2, ПК-5.3
4	Шифры перестановки	3	Маршрутные перестановки. Элементы криптоанализа шифров перестановки.	ПК-5.1, ПК-5.2, ПК-5.3
5	Шифры замены	3	Поточные шифры простой замены. Элементы криптоанализа поточного шифра простой	ПК-5.1, ПК-5.2, ПК-5.3

			замены. Блочные шифры простой замены. Многоалфавитные шифры замены. Многоалфавитные шифры замены.	
6	Шифры гаммирования	3	Табличное гаммирование. О возможности восстановления вероятностей знаков гаммы. Восстановление текстов, зашифрованных неравновероятной гаммой. Повторное использование гаммы. Элементы криптоанализа шифра Виженера. Ошибки шифровальщика.	ПК-5.1, ПК-5.2, ПК-5.3
7	Надежность шифров	2	Энтропия и избыточность языка. Расстояние единственности. Стойкость шифров. Теоретическая стойкость шифров. Практическая стойкость шифров. Вопросы имитостойкости шифров. Шифры, не распространяющие искажений.	ПК-5.1, ПК-5.2, ПК-5.3
8	Блочные системы шифрования	2	Принципы построения блочных шифров. Примеры блочных шифров – американский стандарт шифрования данных DES, стандарт шифрования данных ГОСТ 28147-89. Режимы использования блочных шифров. Комбинирование алгоритмов блочного шифрования. Элементы криптоанализа алгоритмов блочного шифрования. Рекомендации по использованию алгоритмов блочного шифрования.	ПК-5.1, ПК-5.2, ПК-5.3
9	Поточные системы шифрования	2	Синхронизация поточных шифрсистем. Принципы построения поточных шифрсистем. Примеры поточных шифрсистем – шифрсистема А5, шифрсистема Гиффорда. Линейные регистры сдвига. Алгоритм Берлекемпа-	ПК-5.1, ПК-5.2, ПК-5.3

			Месси. Усложнение линейных рекуррентных последовательностей. Фильтрующие генераторы. Комбинирующие генераторы. Композиции линейных регистров сдвига. Схемы с динамическим изменением закона рекурсии. Схемы с элементами памяти. Элементы криптоанализа поточных шифров.	
10	Системы шифрования с открытыми ключами	2	Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиса. Шифрсистемы на основе «проблемы рюкзака».	ПК-5.1, ПК-5.2, ПК-5.3
11	Идентификация	2	Фиксированные пароли (слабая идентификация). Правила составления паролей. Усложнение процедуры проверки паролей. «Подсоленные» пароли. Парольные фразы. Атаки на фиксированные пароли. Повторное использование паролей. Тотальный перебор паролей. Атаки с помощью словаря. Личные идентификационные номера. Одноразовые пароли. «Запрос-ответ» (сильная идентификация). «Запрос-ответ» с использованием симметричных алгоритмов шифрования. «Запрос-ответ» с использованием асимметричных алгоритмов шифрования. Протоколы с нулевым разглашением. Атаки на протоколы идентификации.	ПК-5.1, ПК-5.2, ПК-5.3
12	Криптографические хеш-функции	2	Функции хеширования и целостность данных. Ключевые функции хеширования. Бесключевые функции хеширования. Целостность данных и аутентификация сообщений. Возможные атаки на	ПК-5.1, ПК-5.2, ПК-5.3

			функции хеширования.	
13	Цифровые подписи	2	Общие положения. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Одноразовые цифро-вые подписи.	ПК-5.1, ПК-5.2, ПК-5.3
14	Протоколы распределения ключей	2	Передача ключей с использованием симметричного шифрования. Двусторонние протоко-лы. Трехсторонние протоколы. Передача ключей с использованием асимметричного шиф-рования. Протоколы без использования цифровой подписи. Протоколы с использованием цифровой подписи. Сертификаты открытых ключей.Открытое распределение ключей. Предварительное распределение ключей. Схемы предварительного распределения ключей в сети связи. Схемы разделения секрета. Способы установления ключей для конференц-связи. Возможные атаки на протоколы распределения ключей.	ПК-5.1, ПК-5.2, ПК-5.3
15	Управление ключами	2	Жизненный цикл ключей. Услуги, предоставляемые доверенной третьей стороной. Уста-новка временных меток. Нотаризация цифровых подписей.	ПК-5.1, ПК-5.2, ПК-5.3

6. Содержание практических занятий

Не предусмотрено учебным планом.

7. Содержание лабораторных занятий

Целью проведения лабораторных работ является закрепление теоретического материала на наглядном примере, а также приобретение практических навыков

№ п/п	Раздел дисциплины	Часы	Наименование лабораторной работы	Индикаторы достижения компетенции
1	Исторический очерк развития криптографии	6	Рассматривается ряд конкретных примеров шифров и их применения, известных начиная с античных времен и до современного периода времени. Краткая характеристика рассматриваемых шифров.	ПК-5.1, ПК-5.2, ПК-5.3
2	Математические основы криптографии. Основные понятия криптографии	6	Операции над множествами. Бинарные отношения на множестве Бинарные операции на множестве. Алгебраические структуры (группы, кольца и т.д.). Криптография. Конфиденциальность. Целостность. Аутентификация. Цифровая подпись. Управление секретными ключами. Предварительное распределение ключей. Пересылка ключей. Открытое распространение ключей. Схема разделения секрета. Инфраструктура открытых ключей. Сертификаты. Центры сертификации. Формальные модели шифров. Модели открытых текстов. Математические модели открытого текста. Критерии распознавания открытого текста.	ПК-5.1, ПК-5.2, ПК-5.3
3	Классификация шифров по различным признакам	6	Математическая модель шифра простой замены. Классификация шифров замены.	ПК-5.1, ПК-5.2, ПК-5.3
4	Шифры перестановки	6	Маршрутные перестановки. Элементы криптоанализа шифров перестановки.	ПК-5.1, ПК-5.2, ПК-5.3
5	Шифры замены	6	Поточные шифры простой замены. Элементы криптоанализа поточного шифра простой замены. Блочные шифры простой замены. Многоалфавитные шифры замены. Многоалфа-	ПК-5.1, ПК-5.2, ПК-5.3

			витные шифры замены.	
6	Шифры гаммирования	6	Табличное гаммирование. О возможности восстановления вероятностей знаков гаммы. Восстановление текстов, зашифрованных неравновероятной гаммой. Повторное исполь-зование гаммы. Элементы криптоанализа шифра Виженера. Ошибки шифровальщика.	ПК-5.1, ПК-5.2, ПК-5.3
7	Надежность шифров	4	Энтропия и избыточность языка. Расстояние единственности. Стойкость шифров. Теоретическая стойкость шифров. Практическая стойкость шифров. Вопросы имитостойкости шифров. Шифры, не распространяющие искажений.	ПК-5.1, ПК-5.2, ПК-5.3
8	Блочные системы шифрования	4	Принципы построения блочных шифров. Примеры блочных шифров – американский стандарт шифрования данных DES, стандарт шифрования данных ГОСТ 28147-89. Режи-мы использования блочных шифров. Комбинирование алгоритмов блочного шифрования. Элементы криптоанализа алгоритмов блочного шифрования. Рекомендации по использованию алгоритмов блочного шифрования.	ПК-5.1, ПК-5.2, ПК-5.3
9	Поточные системы шифрования	4	Синхронизация поточных шифрсистем. Принципы построения поточных шифрсистем. Примеры поточных шифрсистем – шифрсистема А5, шифрсистема Гиффорда. Линейные регистры сдвига. Алгоритм Берлекемпа-Месси. Усложнение линейных рекуррентных последовательностей.	ПК-5.1, ПК-5.2, ПК-5.3

			Фильтрующие генераторы. Комбинирующие генераторы. Композиции линейных регистров сдвига. Схемы с динамическим изменением закона рекурсии. Схемы с элементами памяти. Элементы криптоанализа поточных шифров.	
10	Системы шифрования с открытыми ключами	4	Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиса. Шифрсистемы на основе «проблемы рюкзака».	ПК-5.1, ПК-5.2, ПК-5.3
11	Идентификация	4	Фиксированные пароли (слабая идентификация). Правила составления паролей. Усложнение процедуры проверки паролей. «Подсоленные» пароли. Парольные фразы. Атаки на фиксированные пароли. Повторное использование паролей. Тотальный перебор паролей. Атаки с помощью словаря. Личные идентификационные номера. Одноразовые пароли. «Запрос-ответ» (сильная идентификация). «Запрос-ответ» с использованием симметричных алгоритмов шифрования. «Запрос-ответ» с использованием асимметричных алгоритмов шифрования. Протоколы с нулевым разглашением. Атаки на протоколы идентификации.	ПК-5.1, ПК-5.2, ПК-5.3
12	Криптографические хеш-функции	4	Функции хеширования и целостность данных. Ключевые функции хеширования. Бесключевые функции хеширования. Целостность данных и аутентификация сообщений. Возможные атаки на функции хеширования.	ПК-5.1, ПК-5.2, ПК-5.3
13	Цифровые подписи	4	Общие положения. Цифровые подписи на основе шифрсистем с	ПК-5.1, ПК-5.2, ПК-5.3

			открытыми ключами. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Одноразовые цифровые подписи.	
14	Протоколы распределения ключей	4	Передача ключей с использованием симметричного шифрования. Двусторонние протоколы. Трехсторонние протоколы. Передача ключей с использованием асимметричного шифрования. Протоколы без использования цифровой подписи. Протоколы с использованием цифровой подписи. Сертификаты открытых ключей.Открытое распределение ключей. Предварительное распределение ключей. Схемы предварительного распределения ключей в сети связи. Схемы разделения секрета. Способы установления ключей для конференц-связи. Возможные атаки на протоколы распределения ключей.	ПК-5.1, ПК-5.2, ПК-5.3
15	Управление ключами	4	Жизненный цикл ключей. Услуги, предоставляемые доверенной третьей стороной. Установка временных меток. Нотаризация цифровых подписей.	ПК-5.1, ПК-5.2, ПК-5.3

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	Исторический очерк развития криптографии	9	*Проработка теоретического материала*	ПК-5.1, ПК-5.2, ПК-5.3
2	Математические основы криптографии. Основные понятия криптографии	9	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3
3	Классификация шифров по	9	*Проработка*	ПК-5.1,

	различным признакам		*теоретического*	ПК-5.2, ПК-5.3
4	Шифры перестановки	9	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3
5	Шифры замены	9	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3
6	Шифры гаммирования	9	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3
7	Надежность шифров	6	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3
8	Блочные системы шифрования	6	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3
9	Поточные системы шифрования	6	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3
10	Системы шифрования с открытыми ключами	6	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3
11	Идентификация	6	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3
12	Криптографические хеш-функции	6	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3
13	Цифровые подписи	6	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3
14	Протоколы распределения ключей	6	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3
15	Управление ключами	6	*Проработка теоретического*	ПК-5.1, ПК-5.2, ПК-5.3

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности, обучающихся в рамках дисциплины «Методы защиты компьютерной информации» используется рейтинговая система. Рейтинговая оценка формируется на основании текущего и промежуточного контроля. Максимальное и минимальное количество баллов по различным видам учебной работы описано в «Положении о балльно-рейтинговой системе оценки знаний студентов и обеспечения качества учебного процесса» ФГБОУ ВО КНИТУ.

При изучении указанной дисциплины предусматривается сдача 1 контрольной работы с максимальным количеством баллов 30 в седьмом

семестре и 3 контрольные работы с максимальным количеством баллов 10 за каждую в восьмом семестре.

Экзамен проводится в устной форме по билетам. Оценка за экзамен выставляется по пятибалльной шкале, затем умножается на 8. В результате за экзамен студент может получить максимальное количество баллов – 40. При оценке ниже 24 баллов экзамен считается несданным.

В итоге максимальный рейтинг за изучение дисциплины составляет 100 баллов за седьмой семестр и 100 баллов за восьмой семестр.

Оценочные средства	***Кол-во***	***Min, баллов***	***Max, баллов***
Лабораторная работа	***6***	***42***	***70***
Контрольная работа	***1***	***18***	***30***
Итого за 7 семестр:		***60***	***100***
Лабораторная работа	***9***	***18***	***30***
Контрольная работа	***3***	***18***	***30***
Экзамен	***1***	***24***	***40***
Итого за 8 семестр:		***60***	***100***

10. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Оценочные средства для проведения текущего контроля успеваемости, промежуточной аттестации обучающихся и итоговой (государственной итоговой) аттестации разрабатываются согласно положению о Фондах оценочных средств, рассматриваются как составная часть рабочей программы и оформляются отдельным документом.

11.Информационно-методическое обеспечение дисциплины

11.1. Основная литература

При изучении дисциплины «Методы защиты компьютерной информации» в качестве основных источников информации рекомендуется использовать следующую литературу.

Основные источники информации	**Кол-во экз.**
Кирпичников, Александр Петрович. Криптографические методы защиты компьютерной информации [Учебники] : учеб. пособие / А.П. Кирпичников, З.М. Хайбуллина ; Казанский нац. исслед. технол. ун-т .— Казань : Изд-во КНИТУ, 2016 .— 99, [1] с.	66 экз. в УНИЦ http://ft.kstu.ru/ft/Kirpichnikov-Kriptograficheskie_metody_zashchity.pdf доступ с ip-адресов КНИТУ
Грошев А.С. Информатика:	ЭБС «Университетская библиотека

учебник для вузов / А.С. Грошев. – Москва; Берлин: Директ-Медиа, 2015. – 484 с. ISBN 978-5-4475-5064-6	онлайн»: http://biblioclub.ru/index.php?page=book_red&id=428591 доступ после регистрации с IP-адресов КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Кол-во экз.
Прохорова О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова; Самарский государственный архитектурно-строительный университет. – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с. ISBN 978-5-9585-0603-3	ЭБС «Университетская библиотека онлайн»: http://biblioclub.ru/index.php?page=book_red&id=438331 доступ после регистрации с IP-адресов КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Методы защиты компьютерной информации» в качестве электронных источников информации, рекомендуется использовать следующие источники:

Электронный каталог УНИЦ КНИТУ – режим доступа: http://ruslan.kstu.ru/

ЭБС «Университетская библиотека онлайн» -режим доступа http://biblioclub.ru

ЭБС «IPRBooks» -режим доступа http://www.iprbookshop.ru

Согласовано:
Зав.сектором ОКУФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «КАЗАНСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ» Учебно-научный информационный центр

11.4. Современные профессиональные базы данных и информационные справочные системы.

1. eLIBRARY.ru - крупнейший российский информационный портал в области науки, технологии, медицины и образования. Доступ свободный: www.elibrary.ru

2. zbMATH – самая полная математическая база данных, охватывающая материалы с конца 19 века. zbMath содержит около 4 000 000 документов, из более 3 000 журналов и 170 000 книг по математике, статистике, информатике, а также машиностроению, физике, естественным наукам и др. Доступ свободный: zbmath.org

3. Архив журналов РАН. Доступ свободный: elibrary.ru и libnauka.ru

12. Материально-техническое обеспечение дисциплины (модуля).

Учебные аудитории для проведения учебных занятий оснащены оборудованием:

1. smart-доска

Помещения для самостоятельной работы оснащены компьютерной техникой:

1. персональный компьютер с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ. Допускается замена оборудования его виртуальными аналогами.

Лицензированное программное обеспечение и свободно распространяемое программное обеспечение, используемое в учебном процессе при освоении дисциплины:

1. MS Visual Studio.

13. Образовательные технологии

Из общего количества часов 18 проводится в интерактивной форме. Интерактивные занятия реализуются с помощью дискуссий и лекций-дискуссий.