МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Казанский национальный исследовательский
технологический университет»
(ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ
Проректор по учебной работе
Д.Ш. Султанова
«07» июня 2021 г.

Рабочая программа дисциплины в виде электронного документа выгружена из информационной системы управления университетом и соответствует оригиналу
Простая электронная подпись, ID подписи: 1060
Подписал Проректор по учебной работе Д.Ш. Султанова
Дата 07.06.2021

РАБОЧАЯ ПРОГРАММА
по дисциплине **«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»**

Направление подготовки:	10.03.01 Информационная безопасность
Профиль:	Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника:	Бакалавр
Форма обучения:	Очно-заочная
Институт:	Инжиниринговый центр в области химии и технологии энергонасыщенных материалов"Спецхимия"
Факультет:	Инжиниринговый центр в области химии и технологии энергонасыщенных материалов"Спецхимия"
Кафедра-разработчик:	Казанский межвузовский инженерный центр "Новые технологии" федерального государственного бюджетного образовательного учреждения высшего образования "Казанский национальный исследовательский технологический университет"
Курс; семестр	4; 7

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Лабораторная работа	36	1
Контроль самостоятельной работы	63	1,75
Самостоятельная работа	72	2
Форма аттестации: Зачет (7 сем), Курсовой проект (7 сем), Экзамен (7 сем)	27	0,75
Всего	216	6

Казань, 2021

Рабочая программа составлена с учётом требований Федерального государственного образовательного стандарта (приказ № 1427 от 17.11.2020) по направлению подготовки 10.03.01 Информационная безопасность для профиля «Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)» на основании учебных планов набора обучающихся 2021 года.

Разработчик программы:

Доцент А.Ю. Сенцова

С О Г Л А С О В А Н О

Рабочая программа рассмотрена и одобрена на заседании Казанского межвузовского инженерного центра "Новые технологии" федерального государственного бюджетного образовательного учреждения высшего образования "Казанский национальный исследовательский технологический университет", протокол от 19.05.2021 г. № 6.

Директор ***Согласовано*** А.Ф. Махоткин

У Т В Е Р Ж Д Е Н О

Начальник центра УМЦ ***Утверждаю*** Л.А. Китаева

1. Цели освоения дисциплины

Целями освоения дисциплины «Методы и средства криптографической защиты информации» являются:

-изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Методы и средства криптографической защиты информации» относится к обязательной части ООП и формирует у обучающихся по профилю «Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Методы и средства криптографической защиты информации» обучающийся по направлению подготовки 10.03.01 «Информационная безопасность» должен освоить материал предшествующих дисциплин:

1. Защита информационных процессов в телекоммуникациях
2. Информационные технологии в информационной безопасности
3. Основы информационной безопасности
4. Работа с конфиденциальной информацией
5. Сети и системы передачи информации
6. Теория вероятностей и математическая статистика

Дисциплина «Методы и средства криптографической защиты информации» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Защита информации от утечки по техническим каналам
2. Комплексная система защиты информации
3. Организация автоматизированных систем
4. Подготовка к процедуре защиты и защита выпускной квалификационной работы
5. Проектирование защищенных телекоммуникационных систем
6. Производственная практика (преддипломная практика)

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

ОПК-9.1. Знает современные достижения науки и техники в области защиты информации, современные принципы рационального выбора средств защиты в зависимости от вида объекта защиты, системный подход к выполнению и организации

ОПК-9.2. Умеет проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации

ОПК-9.3. Владеет навыками эффективного применения средств криптографической защиты информации, средств технической защиты информации, сетей и систем передачи информации при решении задач профессиональной деятельности

В результате освоения дисциплины обучающийся должен

Знать:

принципы устройства и функционирования средств криптографической и технической защиты информации

Уметь:

интегрировать средства криптографической и технической защиты информации в автоматизированные системы при решении задач профессиональной деятельности

Владеть:

методами установки и настройки криптографических и технических средств защиты информации

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 6 зачетных единиц, 216 часов.

№ п/п	Раздел дисциплины	Семе-стр	Виды учебной работы (в часах)					Оценочные средства для проведения текущей и промежу-точной аттестации
			Лекция	Практические занятия	Лабора-торные	КСР	СРС	
1	2	3	4	5	6	7	8	9
1.	Теория и практика симметричной криптографии	7	10		16	20	18	Лабораторная работа; Реферат; Экзамен
2.	Теория и практика ассиметричной криптографии	7	8		20	33	18	
3.	Курсовой проект	7				10	36	Курсовой проект
	Итого по семестру	**7**	**18**		**36**	**63**	**72**	**Зачет, Курсовой проект, Экзамен**

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Теория и практика симметричной криптографии	4	Основы симметричной криптографии	ОПК-9.1 ОПК-9.2 ОПК-9.3
2.		2	Введение в криптографию	ОПК-9.1 ОПК-9.2 ОПК-9.3
3.		2	СКЗИ на симметричной криптографии	ОПК-9.1 ОПК-9.2 ОПК-9.3
4.		2	Контроль целостности	ОПК-9.1 ОПК-9.2 ОПК-9.3
5.	Теория и практика ассиметричной криптографии	4	Основы ассиметричной криптографии	ОПК-9.1 ОПК-9.2 ОПК-9.3
6.		2	Электронная подпись	ОПК-9.1 ОПК-9.2 ОПК-9.3
7.		2	Инфраструктура открытых ключей	ОПК-9.1 ОПК-9.2 ОПК-9.3
	ВСЕГО	**18**		

6. Содержание практических/семинарских занятий

Проведение практических/семинарских занятий не предусмотрено учебным планом

7. Содержание лабораторных занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Теория и практика симметричной криптографии	10	Шифрование симметричными алгоритмами	ОПК-9.1 ОПК-9.2 ОПК-9.3
2.		6	Контроль целостности с помощью хеш и имитовставки	ОПК-9.1 ОПК-9.2 ОПК-9.3
3.	Теория и практика ассиметричной криптографии	10	Генерация ассимметричных ключей. Создание запроса и сертификата	ОПК-9.1 ОПК-9.2 ОПК-9.3
4.		10	Удостоверяющий центр	ОПК-9.1 ОПК-9.2 ОПК-9.3
	ВСЕГО	**36**		

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Контроль целостности	9	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-9.1 ОПК-9.2 ОПК-9.3
2.	Симметричная криптография	9	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-9.1 ОПК-9.2 ОПК-9.3
3.	Электронная подпись	6	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-9.1 ОПК-9.2 ОПК-9.3
4.	Инфраструктура открытых ключей	6	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-9.1 ОПК-9.2 ОПК-9.3
5.	Ассиметричная криптография	6	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-9.1 ОПК-9.2 ОПК-9.3
6.	Курсовой проект	36	выполнение курсового проекта	ОПК-9.1 ОПК-9.2 ОПК-9.3
	ВСЕГО	**72**		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Контроль целостности	10	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-9.1 ОПК-9.2 ОПК-9.3
2.	Симметричная криптография	10	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-9.1 ОПК-9.2 ОПК-9.3
3.	Электронная подпись	11	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-9.1 ОПК-9.2 ОПК-9.3
4.	Инфраструктура открытых ключей	12	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-9.1 ОПК-9.2 ОПК-9.3

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
5.	Ассиметричная криптография	10	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-9.1 ОПК-9.2 ОПК-9.3
6.	Курсовой проект	10	проверка курсового проекта	ОПК-9.1 ОПК-9.2 ОПК-9.3
	ВСЕГО	**63**		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Методы и средства криптографической защиты информации» используется рейтинговая система. 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.

Рейтинговая оценка формируется на основании текущего и промежуточного контроля. За контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

Оценочные средства	Кол-во	Мин.баллов	Макс.баллов
7-й семестр			
Лабораторная работа	4	28	48
Реферат	1	8	12
Экзамен	1	24	40
Итого		**60**	**100**
7-й семестр			
Курсовой проект	1	60	100
Итого		**60**	**100**

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

Оценочные средства для проведения текущего контроля успеваемости, промежуточной аттестации и 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 и средства криптографической защиты информации» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
Б. А. Фороузан,, Криптография и безопасность сетей [Прочее] учебное пособие: Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021	http://www.iprbookshop.ru/102017.html Режим доступа: по подписке КНИТУ
Бабаш А.В., Баранова Е.К., Криптографические методы защиты информации [Прочее] Учебник: Москва : КноРус, 2020	https://www.book.ru/book/933943 Режим доступа: по подписке КНИТУ
В. М. Фомичёв, Д. А. Мельников, Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты [Прочее] Учебник для вузов: Москва : Юрайт, 2020	https://urait.ru/bcode/451486 Режим доступа: по подписке КНИТУ

В. М. Фомичёв, Д. А. Мельников, Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты [Прочее] Учебник для вузов: Москва : Юрайт, 2020	https://urait.ru/bcode/450820 Режим доступа: по подписке КНИТУ
И. Н. Васильева, Криптографические методы защиты информации [Прочее] Учебник и практикум для вузов: Москва : Юрайт, 2020	https://urait.ru/bcode/450998 Режим доступа: по подписке КНИТУ
С. В. Запечников, О. В. Казарин, А. А. Тарасов, Криптографические методы защиты информации [Прочее] Учебник для вузов: Москва : Юрайт, 2020	https://urait.ru/bcode/450538 Режим доступа: по подписке КНИТУ
М. Масааки, С. Синъити, Занимательная информатика. Криптография. Манга [Электронный ресурс] : Москва : ДМК Пресс, 2019	https://e.lanbook.com/book/131685 Режим доступа: по подписке КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
А. Бехроуз, Криптография и безопасность сетей [Электронный ресурс] Учебное пособие: Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017	http://www.iprbookshop.ru/72337.html Режим доступа: по подписке КНИТУ
Ю. В. Косолапов, Криптографические протоколы на основе линейных кодов [Прочее] учебное пособие: Ростов-на-Дону|Таганрог : Южный федеральный университет, 2020	http://biblioclub.ru/index.php?page=book&id=598671 Режим доступа: по подписке КНИТУ
А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков, Криптографические методы защиты информации для изучающих компьютерную безопасность [Прочее] Учебник для вузов: Москва : Юрайт, 2020	https://urait.ru/bcode/450277 Режим доступа: по подписке КНИТУ
А. А. Набебин, С. М. Авдошин, Дискретная математика. Модулярная алгебра, криптография, кодирование [Электронный ресурс] : Москва : ДМК Пресс, 2017	https://e.lanbook.com/book/93575 Режим доступа: по подписке КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Методы и средства криптографической защиты информации» предусмотрено использование электронных источников информации:

1. Электронный каталог УНИЦ КНИТУ: Режим доступа: http://ruslan.kstu.ru/
2. ЭБС «Лань»:Режим доступа: https://e.lanbook.com
3. Образовательная платформа «Юрайт»: Режим доступа: https://urait.ru/
4. ЭБС «Znanium.com»: Режим доступа: http://znanium.com/
5. ЭБС Университетская библиотека онлайн: Режим доступа: http://biblioclub.ru/
6. ЭБС IPR SMART: Режим доступа: http://www.iprbookshop.ru/
7. ЭБС BOOK.ru : Режим доступа: https://www.book.ru/
8. Научная электронная библиотека https://elibrary.ru/

УНИЦ
Согласовано

11.4. Профессиональные базы данных и информационные справочные системы

Базы данных
Wiley Online Library: https://onlinelibrary.wiley.com/
Springer Nature: https://link.springer.com/
zbMath : https://zbmath.org/

Информационные справочные системы
Справочно-правовая система «ГАРАНТ» Доступ свободный: www.garant.ru
Справочно-правовая система «КонсультантПлюс» Доступ свободный: www.consultant.ru

12. Материально-техническое обеспечение дисциплины

Лицензированное программное обеспечение и свободно распространяемое программное обеспечение, в том числе отечественного производства, используемое в учебном процессе при освоении дисциплины «Методы и средства криптографической защиты информации»:

Офисные и деловые программы: ABBYY FineReader 9.0 проф;
Офисные и деловые программы: MS Office 2007 Russian;
Офисные и деловые программы: MS Office 2007 Professional Russian;
Офисные и деловые программы: MS Office 2010-2016 Standard
Архиватор 7 Zip
Блокнот Notepad
Яндекс Браузер

Учебные аудитории для проведения учебных занятий оснащены оборудованием и техническими средствами обучения:
Аудитория 351-А;
1. Виртуальные машины VirtualBOX (GNU GENERAL PUBLIC LICENSE)
2. Симулятор сетей GNS3 (GNU GENERAL PUBLIC LICENSE)
3. Операционная система Linux (Fedora, Ubuntu). (GNU GENERAL PUBLIC LICENSE)
4. RADIUS сервер (GNU GENERAL PUBLIC LICENSE)
5. Sendmail - SMTP сервер (Sendmail License)
6. POP3 сервер (BSD License)
7. IMAP4 сервер (BSD License)
8. NTP сервер (BSD License)
9. Межсетевой экран iptables (GNU GENERAL PUBLIC LICENSE)
10. Межсетевой экран Firewalld (GNU GENERAL PUBLIC LICENSE)
11. Сканер сетевой безопасности nmap (GNU GENERAL PUBLIC LICENSE)
12. Система обнаружения атак snort (GNU GENERAL PUBLIC LICENSE)
13. Система синхронизации данных rsync
14. компьютер/ноутбук
техническими средствами обучения:
1. Типовой комплект учебного оборудования «Глобальные компьютерные сети» ,
2. Типовой комплект учебного оборудования «Корпоративные компьютерные сети» .
Помещения для самостоятельной работы оснащены компьютерной техникой:
Аудитория Г-407, компьютер/ноутбук с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ.

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Методы и средства криптографической защиты информации» составляет 9 ч.

В процессе освоения дисциплины «Методы и средства криптографической защиты информации» используются следующие образовательные технологии:

• творческие задания;
• работа в малых группах;
• дискуссия;
• обучающие игры (ролевые игры, имитации, деловые игры и образовательные игры);
• изучение и закрепление нового материала на интерактивной лекции (лекция-беседа, лекция – дискуссия, лекция с разбором конкретных ситуаций, лекция с заранее запланированными ошибками, лекция- пресс-конференция, мини-лекция);