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»**

Специальность:	10.05.05 Безопасность информационных технологий в правоохранительной сфере
Специализация:	Технологии защиты информации в правоохранительной сфере
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	Очная
Институт:	Инженерный химико-технологический институт
Факультет:	Факультет экологической, технологической и информационной безопасности
Кафедра-разработчик:	Кафедра «Информационная безопасность»
Курс; семестр	4; 7

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Лабораторная работа	45	1,25
Контроль самостоятельной работы	63	1,75
Самостоятельная работа	63	1,75
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 № 1461 от 22.11.2020) по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере для специализации «Технологии защиты информации в правоохранительной сфере» на основании учебных планов набора обучающихся 2021 года.

Разработчик программы:

Доцент В.А. Богомолов

С О Г Л А С О В А Н О

Рабочая программа рассмотрена и одобрена на заседании кафедры «Информационная безопасность», протокол от 26.05.2021 г. № 10.

Заведующий кафедрой ***Согласовано*** В.А. Богомолов

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 формируемой участниками образовательных отношений части ООП и формирует у обучающихся по специализации «Технологии защиты информации в правоохранительной сфере» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Методы и средства криптографической защиты информации» обучающийся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» должен освоить материал предшествующих дисциплин:

1. Алгебра и геометрия
2. Информатика
3. Языки программирования

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

1. Аудит информационной безопасности
2. Защита информационных процессов в компьютерных системах
3. Защита операционных систем
4. Комплексная система защиты информации на предприятии

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ПК -2 Способен обеспечить безопасность компьютерных сетей, в том числе с использованием программно-аппаратных средств защиты информации, обосновать и проконтролировать результаты управленческих решений в области безопасности информации автоматизированных систем

ПК -2.1. Знает принципы построения компьютерных сетей, порядок реализации методов и средств межсетевого экранирования, источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению, принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации

ПК -2.2. Умеет оценивать угрозы безопасности информации в компьютерных сетях, настраивать правила фильтрации пакетов в компьютерных сетях, оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях, обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях

ПК -2.3. Владеет навыками применения программно-аппаратных средств защиты информации в компьютерных сетях и управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях

В результате освоения дисциплины обучающийся должен

Знать:

как обеспечить безопасность компьютерных сетей, в том числе с использованием программно-аппаратных средств защиты информации, обосновать и проконтролировать результаты управленческих решений в области безопасности информации автоматизированных систем

Уметь:

обеспечивать безопасность компьютерных сетей, в том числе с использованием программно-аппаратных средств защиты информации, обосновать и проконтролировать результаты управленческих решений в области безопасности информации автоматизированных систем

Владеть:

способностью обеспечивать безопасность компьютерных сетей, в том числе с использованием программно-аппаратных средств защиты информации, обосновать и проконтролировать результаты управленческих решений в области безопасности информации автоматизированных систем

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	12	15	Лабораторная работа
2.	Теория и практика ассиметричной криптографии	7	8		29	21	18	
3.	Курсовой проект	7				30	30	Курсовой проект; Экзамен
	Итого по семестру	**7**	**18**		**45**	**63**	**63**	**Зачет, 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	2	Введение в криптографию	ПК -2.1 ПК -2.2 ПК -2.3
2.		4	Основы симметричной криптографии	ПК -2.1 ПК -2.2 ПК -2.3
3.		2	СКЗИ на симметричной криптографии	ПК -2.1 ПК -2.2 ПК -2.3
4.		2	Контроль целостности	ПК -2.1 ПК -2.2 ПК -2.3
5.	Теория и практика ассиметричной криптографии	4	Основы ассиметричной криптографии	ПК -2.1 ПК -2.2 ПК -2.3
6.		2	Электронная подпись	ПК -2.1 ПК -2.2 ПК -2.3
7.		2	Инфраструктура открытых ключей	ПК -2.1 ПК -2.2

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
				ПК -2.3
	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	4	Шифрование симметричными алгоритмами	ПК -2.1 ПК -2.2 ПК -2.3
2.		4	Контроль целостности с помощью хеш и имитовставки	ПК -2.1 ПК -2.2 ПК -2.3
3.		4	Контроль целостности данных (tripwire/aide)	ПК -2.1 ПК -2.2 ПК -2.3
4.		4	Шифрованная файловая система	ПК -2.1 ПК -2.2 ПК -2.3
5.	Теория и практика ассиметричной криптографии	6	Генерация ассимметричных ключей. Создание запроса и сертификата	ПК -2.1 ПК -2.2 ПК -2.3
6.		6	Удостоверяющий центр	ПК -2.1 ПК -2.2 ПК -2.3
7.		9	Электронная цифровая подпись	ПК -2.1 ПК -2.2 ПК -2.3
8.		8	Удостоверяющий центр с поддержкой протокола OCSP	ПК -2.1 ПК -2.2 ПК -2.3
	ВСЕГО	**45**		

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Симметричная криптография	9	подготовка к лабораторной работе	ПК -2.1 ПК -2.2 ПК -2.3
2.	Контроль целостности	6	подготовка к лабораторной работе	ПК -2.1 ПК -2.2 ПК -2.3
3.	Ассиметричная криптография	6	подготовка к лабораторной работе	ПК -2.1 ПК -2.2 ПК -2.3
4.	Инфраструктура открытых ключей	6	подготовка к лабораторной работе	ПК -2.1 ПК -2.2 ПК -2.3
5.	Электронная подпись	6	подготовка к лабораторной работе	ПК -2.1 ПК -2.2

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
				ПК -2.3
6.	Курсовой проект	30	выполнение курсового проекта	ПК -2.1 ПК -2.2 ПК -2.3
	ВСЕГО	**63**		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Симметричная криптография	6	прием лабораторной работы	ПК -2.1 ПК -2.2 ПК -2.3
2.	Контроль целостности	6	прием лабораторной работы	ПК -2.1 ПК -2.2 ПК -2.3
3.	Ассимметричная криптография	6	прием лабораторной работы	ПК -2.1 ПК -2.2 ПК -2.3
4.	Инфраструктура открытых ключей	8	прием лабораторной работы	ПК -2.1 ПК -2.2 ПК -2.3
5.	Электронная подпись	7	прием лабораторной работы	ПК -2.1 ПК -2.2 ПК -2.3
6.	Курсовой проект	30	проверка курсового проекта	ПК -2.1 ПК -2.2 ПК -2.3
	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	8	36	60
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
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 IPRbooks: 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

Scopus Доступ свободный: www.scopus.com
Web of Science Доступ свободный: apps.webofknowledge.com

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
Среда виртуализации VirtualBOX (GNU GENERAL PUBLIC LICENSE)
Симулятор сетей GNS3 (GNU GENERAL PUBLIC LICENSE)
Операционная система Linux (Fedora, Ubuntu). (GNU GENERAL PUBLIC LICENSE)
АРМ Центр Генерации Ключей - ЦГК. (Фактор-ТС)
Модуль Генерации Ключей - МГК. (Фактор-ТС)
Абонентский пункт ЭЦП – DiSignCA. (Фактор-ТС)
Автоматизированное рабочее место абонента электронной почты – DiPost. (Фактор-ТС)
Клиент криптографического сервера доступа - DioNIS Security (Фактор-ТС)
Блокхост-МДЗ (Доверенная загрузка) (ГАЗИНФОРМСЕРВИС)
Блокхост-сеть К (НСД) (ГАЗИНФОРМСЕРВИС)
Блокхост-ЭЦП 2.0 (ИОК) (ГАЗИНФОРМСЕРВИС)
ЭФРОС Config Inspector v.2.5 (Аудит) (ГАЗИНФОРМСЕРВИС)

Учебные аудитории для проведения учебных занятий оснащены оборудованием:

1. Аудитория П-7 ;
техническими средствами обучения:

1. Типовой комплект учебного оборудования «Криптографические системы» ,
2. Типовой комплект учебного оборудования «Глобальные компьютерные сети» ,
3. Типовой комплект учебного оборудования «Корпоративные компьютерные сети» . ;

Помещения для самостоятельной работы оснащены компьютерной техникой:

1. Аудитория И1-107 , ;
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 18 ч.

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

• творческие задания;
• работа в малых группах;
• обучающие игры (ролевые игры, имитации, деловые игры и образовательные игры);
• системы дистанционного обучения.