

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 «**ЗАЩИТА ИНФОРМАЦИИ**»

Направление подготовки:	09.03.01 Информатика и вычислительная техника
Профиль:	Автоматизированные системы обработки информации и управления
Квалификация выпускника:	Бакалавр
Форма обучения:	Заочная
Институт:	Институт управления, автоматизации и информационных технологий
Кафедра-разработчик:	Кафедра «Интеллектуальных систем и управления информационными ресурсами»
Курс; семестр	3-4; 11, 9

Вид нагрузки	Часы	Зачётные единицы
Лекция	6	0,17
Лабораторная работа	8	0,22
Контроль самостоятельной работы	4	0,11
Самостоятельная работа	117	3,25
Форма аттестации: Контрольная работа (11 сем), Экзамен (11 сем)	9	0,25
Всего	144	4

Рабочая программа составлена с учётом требований Федерального государственного образовательного стандарта (приказ № 929 от 19.09.2017) по направлению подготовки 09.03.01 Информатика и вычислительная техника для профиля «Автоматизированные системы обработки информации и управления» на основании учебных планов набора обучающихся 2021 года.

Разработчик программы:

Профессор

А.С. Титовцев

СОГЛАСОВАНО

Рабочая программа рассмотрена и одобрена на заседании кафедры «Интеллектуальных систем и управления информационными ресурсами», протокол от 07.06.2021 г. № 12.

Заведующий кафедрой *Согласовано* А.В. Герасимов

УТВЕРЖДЕНО

Начальник центра УМЦ

Утверждаю

Л.А. Китаева

1. Цели освоения дисциплины

Целями освоения дисциплины «Защита информации» являются:

- а) формирование фундаментальных знаний в области существующих криптографических систем
- б) обучение технологии создания криптографических систем
- в) обучение способам применения существующих алгоритмов шифрования
- г) раскрытие сущности процессов, происходящих в системах

2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации» относится к обязательной части ООП и формирует у обучающихся по профилю «Автоматизированные системы обработки информации и управления» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Защита информации» обучающийся по направлению подготовки 09.03.01 «Информатика и вычислительная техника» должен освоить материал предшествующих дисциплин:

1. Дискретная математика
2. Математический анализ
3. Теория вероятности и математическая статистика

Дисциплина «Защита информации» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Выполнение и защита выпускной квалификационной работы

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ОПК-2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решения задач профессиональной деятельности;

ОПК-2.1. Знает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности

ОПК-2.2. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности

ОПК-2.3. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

В результате освоения дисциплины обучающийся должен

Знать:

основные понятия и требования криптографической защиты информации

принципы работы современных информационных технологий и программных средств

Уметь:

выявлять специфику криптографических угроз информационной безопасности по ряду категорий

информации

использовать программные средства при решении задач в профессиональной деятельности

Владеть:

навыками определения криптографической стойкости шифрсистем

навыками применения программных средств при решении задач в профессиональной деятельности

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 4 зачетные единицы, 144 часа.

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)					Оценочные средства для проведения текущей и промежуточной аттестации
			Лекция	Практические занятия	Лабораторные	КСР	СРС	
1	2	3	4	5	6	7	8	9
1.	Теоретический раздел	9	6				12	Контрольная работа
	Итого по семестру	9	6				12	
1.	Практический раздел	11			8	4	105	Контрольная работа; Лабораторная работа; Экзамен
	Итого по семестру	11			8	4	105	Контрольная работа, Экзамен

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Теоретический раздел	2	Исторический очерк развития криптографии. Математические основы криптографии. Основные понятия криптографии. Классификация шифров по различным признакам. Шифры перестановки. Шифры замены	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3
2.		2	Шифры гаммирования. Надежность шифров. Блочные системы шифрования. Поточные системы шифрования. Системы шифрования с открытыми ключами	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3
3.		2	Идентификация. Криптографические хеш-функции. Цифровые подписи.	ОПК-2.1 ОПК-2.2 ОПК-2.3

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
			Протоколы распределения ключей. Управление ключами	ОПК-3.1 ОПК-3.2 ОПК-3.3
	ВСЕГО	6		

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	б
1.	Практический раздел	1	Маршрутные перестановки. Элементы криптоанализа шифров перестановки.	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3
2.		1	Многоалфавитные шифры замены. Многоалфавитные шифры замены.	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3
3.		1	Энтропия и избыточность языка. Расстояние единственности.	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3
4.		2	Системы шифрования с открытыми ключами	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3
5.		2	Цифровые подписи на основе шифрсистем с открытыми ключами.	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3
6.		1	Управление ключами	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3
	ВСЕГО	8		

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Теоретический раздел	12	подготовка к контрольной работе, подготовка к экзамену, проработка лекционного материала	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3
2.	Практический раздел	105	подготовка к контрольной работе, подготовка к лабораторной работе, подготовка к экзамену	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3
ВСЕГО		117		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Практический раздел	4	прием лабораторной работы, проверка контрольной работы	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3
ВСЕГО		4		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Защита 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
11-й семестр			
Контрольная работа	2	18	30
Лабораторная работа	6	18	30
Экзамен	1	24	40
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 «Защита информации» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
-------------------------------	------------------------

А. Ю. Щеглов, К. А. Щеглов, Защита информации: основы теории [Прочее] Учебник Для бакалавриата и магистратуры: Москва : Юрайт, 2020	https://urait.ru/bcode/449285 Режим доступа: по подписке КНИТУ
Е.К. Баранова, А.В. Бабаш, Информационная безопасность и защита информации [Прочее] Учебное пособие: Москва : Издательский Центр РИОР; Москва : ООО "Научно-издательский центр ИНФРА-М", 2016	http://znanium.com/go.php?id=495249 Режим доступа: по подписке КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
А. М. Голиков, Защита информации в инфокоммуникационных системах и сетях [Прочее] учебное пособие: Томск : Томский государственный университет систем управления и радиоэлектроники, 2015	http://biblioclub.ru/index.php?page=book&id=480637 Режим доступа: по подписке КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Защита 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 ВООК.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 «Защита 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

Microsoft Teams

Учебные аудитории для проведения учебных занятий оснащены оборудованием:

1. учебная мебель (столы, стулья);
2. аудиторная доска;

техническими средствами обучения:

1. аудиторная 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.

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Защита информации» составляет 6 ч.

В процессе освоения дисциплины «Защита 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).