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.
_____
«01» 07 20 19 г.

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 - очная
Институт, факультет - Институт управления, автоматизации и информационных технологий, Факультет управления и автоматизации
Кафедра-разработчик рабочей программы - Интеллектуальных систем и управления информационными ресурсами
Курс 3, семестр 6

	Часы	Зачетные единицы
Лекции	18	0,5
Практические занятия		
Лабораторные занятия	36	1
Контроль самостоятельной работы		
Самостоятельная работа	54	1,5
Форма аттестации экзамен	36	1
Всего	144	4

Казань, 2019 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования (№ 929 от 19.09.2017) по направлению 09.03.01 «Информатика и вычислительная техника» на основании учебного плана набора обучающихся 2019 г.

Разработчик программы:
Профессор А.П. Кирпичников

Рабочая программа рассмотрена и одобрена на заседании кафедры «Интеллектуальных систем и управления информационными ресурсами», протокол от 1.07.2019 г. № 11

Зав. кафедрой, профессор А.П. Кирпичников

СОГЛАСОВАНО

Протокол заседания кафедры АССОИ, реализующей подготовку основной образовательной программы от 17.06.2019 г. № 20

Зав. кафедрой Р.Н. Гайнуллин

УТВЕРЖДЕНО

Начальник УМЦ, доцент 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 (модуля) в структуре основной образовательной программы

Дисциплина «Защита информации» относится к части ООП обязательной и формирует у бакалавров по направлению подготовки 09.03.01 набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Защита информации» бакалавр по направлению подготовки 09.03.01 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 является предшествующей и необходима для успешного усвоения последующих дисциплин:

а) защита информации

б) моделирование

в) сетевые технологии

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

ОПК-2 Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности;

ОПК-2.1 Знает современные информационные технологии и программные средства, 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

1) Знать:

а) основания криптографической защиты информации в организации;

б) основные понятия и требования криптографической защиты информации

2) Уметь:

а) выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации;

б) выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации;

3) Владеть:

а) навыками определения криптографической стойкости шифрсистем;

б) навыками обоснования выбора криптографических средств для защиты информации.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 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	Теоретический раздел		18				24	Контрольная работа
2	Практический раздел				36		30	Контрольная работа
ИТОГО			18		36		54	
Форма аттестации			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	1	Исторический очерк развития криптографии Рассматривается ряд конкретных примеров шифров и их применения, известных начиная с античных времен и до современного периода времени. Краткая характеристика рассматриваемых шифров.	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
2	Математические основы криптографии. Основные понятия криптографии	1	Математические основы криптографии. Основные понятия криптографии 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.	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3

			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.	
3	Классификация шифров по различным признакам	2	Классификация шифров по различным признакам Математическая модель шифра простой замены. Классификация шифров замены.	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
4	Шифры перестановки	1	Шифры перестановки Маршрутные перестановки. Элементы криптоанализа шифров перестановки.	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
5	Шифры замены	2	Шифры замены Поточные шифры простой замены. Элементы криптоанализа поточного шифра простой замены. Блочные шифры простой замены. Многоалфавитные шифры замены. Многоалфавитные шифры замены.	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
6	Шифры гаммирования	1	Шифры гаммирования Табличное гаммирование. О возможности восстановления вероятностей знаков гаммы. Восстановление текстов, зашифрованных неравновероятной гаммой. Повторное использование гаммы. Элементы криптоанализа шифра Виженера. Ошибки шифровальщика.	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
7	Надежность шифров	2	Надежность шифров Энтропия и избыточность языка. Расстояние единственности. Стойкость шифров. Теоретическая стойкость шифров. Практическая	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3

			стойкость шифров. Вопросы имитостойкости шифров. Шифры, не распространяющие искажений.	
8	Блочные системы шифрования	1	Блочные системы шифрования 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	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
9	Поточные системы шифрования	1	Поточные системы шифрования Синхронизация поточных шифрсистем. Принципы построения поточных шифрсистем. Примеры поточных шифрсистем – шифрсистема А5, шифрсистема Гиффорда. Линейные регистры сдвига. Алгоритм Берлекемпа-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.	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
10	Системы шифрования с открытыми ключами	1	Системы шифрования с открытыми ключами Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиса. Шифрсистемы	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3

			на основе «проблемы рюкзака»	
11	Идентификация	1	Идентификация 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.	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
12	Криптографические хеш-функции	1	Криптографические хеш-функции Функции хеширования и целостность данных. Ключевые функции хеширования. Бесключевые функции хеширования. Целостность данных и аутентификация сообщений. Возможные атаки на функции хеширования.	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
13	Цифровые подписи	1	Цифровые подписи Общие положения. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Одноразовые цифровые подписи.	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
14	Протоколы распределения ключей	1	Протоколы распределения ключей Передача ключей с использованием симметричного	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2,

			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.	ОПК-3.3
15	Управление ключами	1	Управление ключами Жизненный цикл ключей. Услуги, предоставляемые доверенной третьей стороной. Установка временных меток. Нотаризация цифровых подписей.	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3

6. Содержание практических занятий

Учебным планом не предусмотрено.

7. Содержание лабораторных занятий

Целью проведения лабораторных работ является закрепление теоретического материала на наглядном примере, а также приобретение практических навыков постановки и решения задач компьютерной графики.

№ п/п	Раздел дисциплины	Часы	Наименование лабораторной работы	Индикаторы достижения компетенции
1	Практический раздел	6	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	Практический	6	Многоалфавитные шифры	ОПК-2.1,

	раздел		замены. Многоалфавитные шифры замены.	ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
3	Практический раздел	6	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	Практический раздел	6	Системы шифрования с открытыми ключами	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
5	Практический раздел	6	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	Практический раздел	6	Управление ключами	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	Теоретический раздел	12	Проработка теоретического материала	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
2	Теоретический раздел	12	Проработка теоретического материала	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
3	Практический раздел	6	Подготовка к лабораторным работам, подготовка к контрольной работе	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
4	Практический раздел	6	Подготовка к лабораторным работам,	ОПК-2.1, ОПК-2.2,

			подготовка к контрольной работе	ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
5	Практический раздел	6	Подготовка к лабораторным работам, подготовка к контрольной работе	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
6	Практический раздел	6	Подготовка к лабораторным работам, подготовка к контрольной работе	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3
7	Практический раздел	6	Подготовка к лабораторным работам, подготовка к контрольной работе	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности, обучающихся в рамках дисциплины «Защита 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 выполнение двух контрольных работ с максимальным количеством баллов 15 за каждую.

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 семестр.

Оценочные средства	***Кол-во***	***Min, баллов***	***Max, баллов***
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 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 «Защита информации» в качестве основных источников информации рекомендуется использовать следующую литературу.

Основные источники информации	**Кол-во экз.**
Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. – Москва; Берлин: Директ-Медиа, 2015. – 253 с. ISBN 978-5-4475-3946-7	ЭБС «Университетская библиотека онлайн»: http://biblioclub.ru/index.php?page=book_red&id=276557 доступ после регистрации с IP-адресов КНИТУ
Смирнов, В.И. Защита информации: лабораторный практикум / В.И. Смирнов; Поволжский государственный технологический университет. – Йошкар-Ола: Поволжский государственный технологический университет, 2017. – 67 с. ISBN 978-5-8158-1866-8	ЭБС «Университетская библиотека онлайн»: http://biblioclub.ru/index.php?page=book_red&id=476512 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.**
Аверченков, В.И. Служба защиты информации: организация и управление: / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стер. – Москва: Флинта, 2016. – 186 с. ISBN 978-5-9765-1271-9	ЭБС «Университетская библиотека онлайн»: http://biblioclub.ru/index.php?page=book_red&id=93356 доступ после регистрации с IP-адресов КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Защита 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).

Лабораторный практикум проводится в компьютерном классе. Требования к аппаратному обеспечению следующие:

1. Персональный компьютер на платформе Intel (AMD или аналогичной)
2. Локальная и глобальная сети

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 18 часов лабораторных занятий проводится в интерактивной форме. При проведении подобных занятий используется интерактивная электронная доска, персональный компьютер, проектор, комплект электронных презентаций.