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

УТВЕРЖДАЮ
Проректор по УР
_____ А.В. Бурмистров
«_27_» _____09_____2018 г.

Р А Б О Ч А Я П Р О Г Р А М М А

по дисциплине Б1.В.ОД.3 - «Защита информации»

Направление подготовки 09.03.01 - «Информатика и вычислительная техника»
Профиль подготовки – «Автоматизированные системы обработки информации и управления»
Квалификация (степень) выпускника - бакалавр
Форма обучения - очная
Институт, факультет – Институт управления, автоматизации и информационных технологий, факультет управления и автоматизации
Кафедра-разработчик рабочей программы – кафедра интеллектуальных систем и управления информационными ресурсами
Курс 3, семестр 5

	Часы	Зачетные единицы
Лекции	18	
Практические занятия	-	-
Семинарские занятия	-	-
Лабораторные занятия	63	
Самостоятельная работа	72	
Форма аттестации - экзамен,зачет	27	0,75
Всего	180	5

Казань, 2018 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования (Приказ Минобрнауки России от 12.01.2016 № 5) по направлению 09.03.01 «Информатика и вычислительная техника» по профилю «Автоматизированные системы обработки информации и управления», на основании учебного плана, утвержденного Учёным советом КНИТУ.

Год набора обучающихся: 2018 г.

Разработчик программы
профессор кафедры ИСУИР А.П. Кирпичников

Рабочая программа рассмотрена и одобрена на заседании кафедры ИСУИР, протокол от 03.09.2018 г. №1 .

Зав. кафедрой профессор А.П. Кирпичников

СОГЛАСОВАНО

Протокол заседания методической комиссии факультета управления и автоматизации от 10.09.2018 г. №1 .

Председатель комиссии профессор Р.Н. Зарипов

УТВЕРЖДЕНО

Протокол заседания методической комиссии факультета наноматериалов и нанотехнологий от 10.09.2018 г. №19.

Председатель комиссии профессор В.А. Сысоев

Начальник УМЦ доцент Л.А. Китаева

1. Цели освоения дисциплины

Целями освоения дисциплины «Защита 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 образовательной программы

Дисциплина «Защита информации» относится к вариативной части ООП и формирует у бакалавров по направлению подготовки 09.03.01 набор знаний, умений, навыков и компетенций, необходимых для выполнения научно-исследовательской, проектно-конструкторской, проектно-технологической и монтажно-наладочной видов деятельности.

Знания, полученные при изучении дисциплины «Защита информации» могут быть использованы при прохождении преддипломной практики и выполнении выпускных квалификационных работ по направлению подготовки 09.03.01 «Информатика и вычислительная техника».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ОК-4 - способность использовать основы правовых знаний в различных сферах деятельности;

ОПК-2 - способностью осваивать методики использования программных средств для решения практических задач;

ОПК-5 - способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ПК-2 – способностью разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования.

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 защиты 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.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачётных единиц, 180 часов.

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)				Информационные и другие образовательные технологии, используемые при осуществлении образовательного процесса	Оценочные средства для проведения промежуточной аттестации по разделам
			Лекции	Семинар (Практические занятия)	Лабораторторные работы	СРС		
1	Основные этапы истории развития криптографических методов защиты данных	5	2		11	14	Лекции в традиционной форме, лабораторные занятия с применением ПЭВМ	Коллоквиум

2	Криптосистемы с секретным ключом	5	4	-	10	14	Лекции в традиционной форме, лабораторные занятия с применением ПЭВМ	Коллоквиум
3	Российский стандарт криптографической зашиты данных	5	4	-	10	14	Лекции в традиционной форме, лабораторные занятия с применением ПЭВМ	Коллоквиум
4	Криптосистемы с открытым ключом и их свойства	5	4	-	12	15	Лекции в традиционной форме, лабораторные занятия с применением ПЭВМ	Коллоквиум
5	Электронная цифровая подпись и защита целостности передачи данных	5	4	-	12	15	Лекции в традиционной форме, лабораторные занятия с применением ПЭВМ	Коллоквиум
Форма аттестации								Экзамен

5. Содержание лекционных занятий по темам с указанием формируемых компетенций и используемых инновационных образовательных технологий.

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Формируемые компетенции
1	Основные этапы истории развития криптографических методов защиты данных	2	Основные понятия и исторический обзор развития криптографии. Классификация угроз противника. Классификация атак на систему кодирования данных с секретным ключом	ОК-4, ОПК-2, ОПК-5, ПК-2
2	Криптосистемы с секретным ключом	4	Основные типы симметричных криптосистем. Методы перестановки, методы простой и сложной замены и методы гаммирования	ОК-4, ОПК-2, ОПК-5, ПК-2
3	Российский стандарт криптографической зашиты данных	4	Сети Х. Фейстеля и российский стандарт шифрования данных. Имитозащита и контроль целостности потока сообщений	ОК-4, ОПК-2, ОПК-5, ПК-2

4	Криптосистемы с открытым ключом и их свойства	4	Односторонние (однонаправленные) функции. Основные типы криптосистем с открытым ключом Открытое распределение ключей.	ОК-4, ОПК-2, ОПК-5, ПК-2
5	Электронная цифровая подпись и защита целостности передачи данных	4	Понятие электронной цифровой подписи. Решение проблемы аутентификации передаваемой информации при помощи ЭЦП	ОК-4, ОПК-2, ОПК-5, ПК-2

6. Содержание практических занятий

Практические занятия учебным планом не предусмотрены.

7. Содержание лабораторных занятий

№ п/п	Раздел дисциплины	Часы	Наименование лабораторной работы	Формируемые компетенции
1	Основные этапы истории развития криптографических методов защиты данных	11	Основные понятия и исторический обзор развития криптографии. Классификация угроз противника. Классификация атак на систему кодирования данных с секретным ключом	ОК-4, ОПК-2, ОПК-5, ПК-2
2	Криптосистемы с секретным ключом	12	Методы перестановки, методы простой и сложной замены и методы гаммирования	ОК-4, ОПК-2, ОПК-5, ПК-2
3	Российский стандарт криптографической зашиты данных	12	Сети Х. Фейстеля и российский стандарт шифрования данных	ОК-4, ОПК-2, ОПК-5, ПК-2
4	Криптосистемы с открытым ключом и их свойства	14	Криптосистема, основанная на задаче об укладке рюкзака. Криптосистема RSA.Криптосистема Эль Гамаля. Гибридные криптосистемы	ОК-4, ОПК-2, ОПК-5, ПК-2
5	Электронная цифровая подпись и защита целостности передачи данных	14	Решение проблемы аутентификации передаваемой информации при помощи ЭЦП	ОК-4, ОПК-2, ОПК-5, ПК-2

Лабораторные работы проводятся в компьютерном классе с использованием специального оборудования – ПЭВМ.

8. Самостоятельная работа бакалавра

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Формируемые компетенции
1	Основные этапы истории развития криптографических методов защиты данных	14	Проработка теоретического материала, подготовка к лабораторным работам, подготовка к коллоквиуму по разделу	ОК-4, ОПК-2, ОПК-5, ПК-2
2	Криптосистемы с секретным ключом	14	Проработка теоретического материала, подготовка к лабораторным работам, подготовка к коллоквиуму по разделу	ОК-4, ОПК-2, ОПК-5, ПК-2
3	Российский стандарт криптографической зашиты данных	14	Проработка теоретического материала, подготовка к лабораторным работам, подготовка к коллоквиуму по разделу	ОК-4, ОПК-2, ОПК-5, ПК-2
4	Криптосистемы с открытым ключом и их свойства	15	Проработка теоретического материала, подготовка к лабораторным работам, подготовка к коллоквиуму по разделу	ОК-4, ОПК-2, ОПК-5, ПК-2
5	Электронная цифровая подпись и защита целостности передачи данных	15	Проработка теоретического материала, подготовка к лабораторным работам, подготовка к коллоквиуму по разделу	ОК-4, ОПК-2, ОПК-5, ПК-2

9. Использование рейтинговой системы оценки знаний.

При оценке результатов деятельности студентов 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 рейтинговой системе.

При изучении дисциплины «Защита информации» предусматривается сдача двух коллоквиумов с максимальным количеством баллов 30 баллов за каждый.

Коллоквиумы проводятся в форме блиц-опроса: короткий вопрос – короткий ответ. Каждый вопрос блица подразумевает конкретный ответ. Если студент

дает верный ответ по существу вопроса, то за каждый такой ответ он получает 5 баллов, в противном случае – 2 балла. Количество вопросов коллоквиума равно отношению его максимального балла к 5. Оценка за коллоквиум равна сумме баллов за все ответы. В результате максимальный текущий рейтинг за семестр составит 60 баллов.

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	**Количество**	**Минимум баллов**	**Максимум баллов**
Коллоквиум	2	36	60
Экзамен	1	24	40
Итого:		60	100

10. Информационно-методическое обеспечение дисциплины

10.1 Основная литература

При изучении дисциплины в качестве основных источников информации рекомендуется использовать следующую литературу.

Год набора обучающихся 2014:

Основные источники информации	**Кол-во экз.**
1. Басалова Г.В. Основы криптографии: курс лекций. — Национальный Открытый Университет «ИНТУИТ», 2011. — 253 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/177715 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
2. Гультяева Т.А. Основы теории информации и криптографии: конспект лекций. — Новосибирск: Изд-во НГТУ, 2010. — 88 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/186624 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
3. Кнауб Л.В., Новиков Е.А., Шитов Ю.А. Теоретико-численные методы в криптографии: учебное пособие. — Красноярск: Изд-во СФУ, 2011. — 160 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/180511 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
4. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. — М.: ДМК Пресс, 2012. — 592 с.	ЭБС «Лань» https://e.lanbook.com/book/3032?category_pk=1545#book_name Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ

Год набора обучающихся 2015:

Основные источники информации	**Кол-во экз.**
1. Долозов Н.Л., Гультяева Т.А. Программные средства защиты информации: конспект лекций. — Новосибирск: Изд-во НГТУ, 2015. — 63 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/185990 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ

2. Калмыков И.А. Науменко Д.О. Гиш Т.А. Криптографические методы защиты информации. — Ставрополь: Изд-во СКФУ, 2015. — 109 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/200528 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
3. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. — М.: ДМК Пресс, 2012. — 592 с.	ЭБС «Лань» https://e.lanbook.com/book/3032?category_pk=1545#book_name Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ

Год набора обучающихся 2016:

Основные источники информации	**Кол-во экз.**
1. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов, — М.: ДМК Пресс, 2016 г. — 296 с.	ЭБС «Лань» https://e.lanbook.com/book/82817?category_pk=1545#book_name Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
2. Долозов Н.Л., Гультяева Т.А. Программные средства защиты информации: конспект лекций. — Новосибирск: Изд-во НГТУ, 2015. — 63 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/185990 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
3. Калмыков И.А. Науменко Д.О. Гиш Т.А. Криптографические методы защиты информации. — Ставрополь: Изд-во СКФУ, 2015. — 109 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/200528 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
4. Лапонина О.Р. Криптографические основы безопасности. — Национальный Открытый Университет «ИНТУИТ», 2016. — 244 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/177261 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
5. Фороузан Б.А. Математика криптографии и теория шифрования. — Национальный Открытый Университет «ИНТУИТ», 2016. — 511 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/178747 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ

Год набора обучающихся 2017:

Основные источники информации	Кол-во экз.
1. Авдошин С.М., Набебин А.А. Дискретная математика. Модулярная алгебра, криптография, кодирование. — М.: ДМК Пресс, 2017 г. — 352 с.	ЭБС «Лань» https://e.lanbook.com/book/93575?category_pk=1548#authors Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
2. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов, — М.: ДМК Пресс, 2016 г. — 296 с.	ЭБС «Лань» https://e.lanbook.com/book/82817?category_pk=1545#book_name Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
3. Долозов Н.Л., Гультяева Т.А. Программные средства защиты информации: конспект лекций. — Новосибирск: Изд-во НГТУ, 2015. — 63 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/185990 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
4. Калмыков И.А. Науменко Д.О. Гиш Т.А. Криптографические методы защиты информации. — Ставрополь: Изд-во СКФУ, 2015. — 109 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/200528 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
5. Лапонина О.Р. Криптографические основы безопасности. — Национальный Открытый Университет «ИНТУИТ», 2016. — 244 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/177261 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
6. Фороузан Б.А. Математика криптографии и теория шифрования. — Национальный Открытый Университет «ИНТУИТ», 2016. — 511 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/178747 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ

В качестве дополнительных источников информации рекомендуется использовать следующую литературу.

Дополнительные источники информации	**Кол-во экз.**
1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: учеб. пособие для студ. вузов. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 480 с.	85 экз. в УНИЦ КНИТУ
2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. — М.: ДМК Пресс, 2008. — 448 с.	ЭБС «Лань» https://e.lanbook.com/book/3027?category_pk=1545#book_name Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
3. Фомичёв В.М**.** Методы дискретной математики в криптологии. — М.: Диалог-МИФИ, 2010. — 436 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/198429 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ
4. Шубович В.Г., Капитанчук В.В., Зыненко Н.С., Титаренко Ю.И. Разработка моделей криптографической защиты информации: монография. — Ульяновск: Изд-во УлГПУ, 2013. — 128 с.	ЭБС «Книгафонд» http://www.knigafund.ru/books/186948 Доступ из любой точки сети Интернет после регистрации по IP-адресам КНИТУ

10.3 Электронные источники информации

При изучении дисциплины допускается использование электронных источников информации:

1. Электронный каталог УНИЦ КНИТУ – режим доступа http://ruslan.kstu.ru
2. Научная электронная библиотека (НЭБ) – http://e.library.ru
3. ЭБС «ЮРАЙТ» - режим доступа http://biblio-online.ru
4. ЭБС «Лань» - режим доступа http://e.lanbook.com/books
5. ЭБС «Книгафонд» - режим доступа http://knigafund.ru
6. ЭБС «Znanium.com» - режим доступа http://znanium.com

Согласовано:

Зав.сектором ОКУФ

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

И.И. Усольцева

11. 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.

12. Материально-техническое обеспечение дисциплины (модуля).

В качестве материально-технического обеспечения дисциплины используются персональные компьютеры, раздаточный материал – учебные пособия; также могут быть использованы мультимедийные средства (проектор, экран, ноутбук) - для презентационных материалов.

13. Образовательные технологии

Из общего количества часов 24 проводится в интерактивной форме, из них 12 часов лекций и 12 – лабораторных занятий. При проведении подобных занятий используются персональные компьютеры и раздаточный материал. Интерактивные занятия реализуются с помощью компьютерной симуляции, исследовательского и проектного методов, а также мастер-классов приглашённых специалистов.