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» 10 2017 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.ОД.9 - «Методы защиты информации»

Направление подготовки 01.03.02 - «Прикладная математика и информатика»
Профиль подготовки – «Прикладная математика и информатика»
Квалификация (степень) выпускника - бакалавр
Форма обучения - очная
Институт, факультет – Институт нефти, химии и нанотехнологий, факультет наноматериалов и нанотехнологий
Кафедра-разработчик рабочей программы – кафедра интеллектуальных систем и управления информационными ресурсами
Курс 4, семестр 7, 8

	Часы	Зачетные единицы
Лекции	36	1
Практические занятия	-	-
Семинарские занятия	-	-
Лабораторные занятия	72	2
Самостоятельная работа	72	2
Форма аттестации - экзамен	36	1
Всего	216	6

Казань, 2017 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования (Приказ Минобрнауки России от 12.03.2015 № 228) по направлению 01.03.02 «Прикладная математика и информатика» по профилю «Прикладная математика и информатика», на основании учебного плана, утвержденного Учёным советом КНИТУ.

Годы набора обучающихся 2015, 2016, 2017.

Разработчик программы
профессор А.П. Кирпичников

Рабочая программа рассмотрена и одобрена на заседании кафедры ИСУИР, протокол от 10 октября 2017 г. № 2.

Зав. кафедрой профессор А.П. Кирпичников

УТВЕРЖДЕНО

Протокол заседания методической комиссии факультета Наноматериалов и нанотехнологий от 12 октября 2017 г. № 9.

Председатель комиссии профессор В.А. Сысоев

Начальник УМЦ доцент Л.А. Китаева

1. Цели освоения дисциплины

Целями освоения дисциплины «Методы защиты 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 «Методы защиты информации» относится к вариативной части ОП и формирует у бакалавров по направлению подготовки 01.03.02 набор знаний, умений, навыков и компетенций, необходимых для выполнения *научно-исследовательского, организационно-управленческого и социально-педагогического видов деятельности.*

Знания, полученные при изучении дисциплины «Методы защиты информации» могут быть использованы при прохождении преддипломной практики и выполнении выпускных квалификационных работ по направлению подготовки 01.03.02.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

1. ОК-4 - способность использовать основы правовых знаний в различных сферах жизнедеятельности;
2. ОК-6 - способность работать в команде, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия;
3. ОК-7 - способность к самоорганизации и самообразованию;
4. ПК-1 - способность собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов

по соответствующим научным исследованиям;

5. ПК-2 – способностью понимать, совершенствовать и применять современный математический аппарат;

6. ПК-3 - способность критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной деятельности.

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 зашиты 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 6 зачётных единиц, 216 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)	Лабораторные работы	СРС		
1	*Основные этапы истории развития крип-*	7	6		12	6	*Лекции в традиционной форме, лабораторные занятия с применением ПЭВМ*	*Коллоквиум*

	тографических методов защиты данных							
2	*Криптосистемы с секретным ключом*	7	6	-	12	6	*Лекции в традиционной форме, лабораторные занятия с применением ПЭВМ*	*Коллоквиум*
3	*Российский стандарт криптографической зашиты данных*	7	6	-	12	6	*Лекции в традиционной форме, лабораторные занятия с применением ПЭВМ*	*Коллоквиум*
4	*Криптосистемы с открытым ключом и их свойства*	8	9	-	18	27	*Лекции в традиционной форме, лабораторные занятия с применением ПЭВМ*	*Коллоквиум*
5	*Электронная цифровая подпись и защита целостности передачи данных*	8	9	-	18	27	*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*	6	*Основные понятия и исторический обзор развития криптографии. Классификация угроз противника. Классификация атак на систему кодирования данных с секретным ключом*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3
2	*Криптосистемы с секретным ключом*	6	*Основные типы симметричных криптосистем. Методы перестановки, методы простой и сложной замены и методы гаммиро-*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3

			вания	
3	*Российский стандарт криптографической защиты данных*	6	*Сети Х. Фейстеля и российский стандарт шифрования данных. Имитозащита и контроль целостности потока сообщений*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3
4	*Криптосистемы с открытым ключом и их свойства*	9	*Односторонние (однонаправленные) функции. Основные типы криптосистем с открытым ключом Открытое распределение ключей.*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3
5	*Электронная цифровая подпись и защита целостности передачи данных*	9	*Понятие электронной цифровой подписи. Решение проблемы аутентификации передаваемой информации при помощи ЭЦП*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3

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*	12	*Основные понятия и исторический обзор развития криптографии. Классификация угроз противника. Классификация атак на систему кодирования данных с секретным ключом*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3
2	*Криптосистемы с секретным ключом*	12	*Методы перестановки, методы простой и сложной замены и методы гаммирования*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3
3	*Российский стандарт криптографической защиты данных*	12	*Сети Х. Фейстеля и российский стандарт шифрования данных*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3
4	*Криптосистемы с открытым ключом и их свойства*	18	*Криптосистема, основанная на задаче об укладке рюкзака. Криптосистема RSA.Криптосистема*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3

			Эль Гамаля. Гибридные криптосистемы	
5	*Электронная цифровая подпись и защита целостности передачи данных*	18	*Решение проблемы аутентификации передаваемой информации при помощи ЭЦП*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3

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*	6	*Проработка теоретического материала, подготовка к лабораторным работам, подготовка к коллоквиуму по разделу*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3
2	*Криптосистемы с секретным ключом*	6	*Проработка теоретического материала, подготовка к лабораторным работам, подготовка к коллоквиуму по разделу*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3
3	*Российский стандарт криптографической зашиты данных*	6	*Проработка теоретического материала, подготовка к лабораторным работам, подготовка к коллоквиуму по разделу*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3
4	*Криптосистемы с открытым ключом и их свойства*	27	*Проработка теоретического материала, подготовка к лабораторным работам, подготовка к коллоквиуму по разделу*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3
5	*Электронная цифровая подпись и защита целостности передачи данных*	27	*Проработка теоретического материала, подготовка к лабораторным работам, подготовка к коллоквиуму по разделу*	ОК-4, ОК-6, ОК-7, ПК-1, ПК-2, ПК-3

9. Использование рейтинговой системы оценки знаний.

При оценке результатов деятельности студентов в рамках дисциплины «Методы защиты 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 указанной дисциплины 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 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., Зваенко 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 18 проводится в интерактивной форме, из них 9 часов лекций и 9 – 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.

Лист переутверждения рабочей программы

Рабочая программа по дисциплине «Методы защиты информации» пересмотрена на заседании кафедры Интеллектуальных систем и управления информационными ресурсами

(наименование кафедры)

№ п/п	Дата переутверждения РП (протокол заседания кафедры № 1 от 03.09.2018	Наличие изменений	Наличие изменений в списке литературы	Подпись разработчика РП	Подпись заведующего кафедрой	Подпись начальника УМЦ/ОМг/ОАиД
1		нет	нет			

**Если в списке литературы есть изменения, обновленный список необходимо утвердить у заведующей сектором комплектования УНИЦ и один экземпляр представить в УМЦ/ОМг/ОАиД.*