МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Национальный исследовательский ядерный университет «МИФИ»

Саровский физико-технический институт -

филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»

(**СарФТИ НИЯУ МИФИ**)

ФИЗИКО-ТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра «Радиофизика и электроника»

УТВЕРЖДАЮ
Декан ФТФ,
член-корреспондент РАН

_____А.К. Чернышев

«___» _____ 2022 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптография и специсследования

наименование дисциплины

Направление подготовки (специальность) 11.04.04 Электроника и наноэлектроника

Наименование образовательной программы Электронные приборы и устройства

Квалификация (степень) выпускника магистр

Форма обучения очная

Программа одобрена на заседании кафедры

протокол № 3 от 17.12.2021г.

Зав. кафедрой РФ
д.т.н., доцент
_____ Д.Б. Николаев

«____» _____ 2022г.

г. Саров, 2022 г.

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ на 202____/202_____ учебный год.
Заведующий кафедрой РФ, д.т.н., доцент Д.Б. Николаев

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ на 202____/202_____ учебный год.
Заведующий кафедрой РФ, д.т.н., доцент Д.Б. Николаев

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ на 202____/202_____ учебный год.
Заведующий кафедрой РФ, д.т.н., доцент Д.Б. Николаев

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ на 202____/202_____ учебный год.
Заведующий кафедрой РФ, д.т.н., доцент Д.Б. Николаев

Семестр	В форме практической подготовки	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	КР/ КП	Форма(ы) контроля, экз./зач./ЗсО/
1	16	2	72	16	16	-	40	-	З
2	16	3	108	32	32	-	8	-	Э
ИТОГО	**32**	**5**	**180**	**48**	**48**	**-**	**48**	**-**	**36**

АННОТАЦИЯ

Учебная дисциплина «Криптография и специсследования» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления. Основной целью дисциплины «Криптография и специсследования» является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями и задачами дисциплины «Криптография и специсследования» являются:

- изучение основополагающих принципов защиты информации;
- изучение и исследование криптографических методов обеспечения безопасности данных;
- практическая реализация методов защиты информации на практике.

Дисциплина «Криптография и специсследования» является базовой (общепрофессиональной) частью профессиональной компетенции и базируется на таких дисциплинах как, «Информатика», «Информационные технологии», «Алгоритмические языки», «Программирование».

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Освоение дисциплины «Криптография и специсследования» необходимо для успешного изучения дисциплин, связанных с проектированием и эксплуатацией информационных систем с применением современных методов защиты информации. Знание основ защиты информации в рамках информационных систем необходимо для успешного выполнения производственной практики и научно-исследовательской работы магистра.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	З-УК-1 Знать: методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации У-УК-1 Уметь: применять методы системного подхода и критического анализа проблемных ситуаций; разрабатывать стратегию действий, принимать конкретные решения для ее реализации В-УК-1 Владеть: методологией системного и критического анализа проблемных ситуаций; методиками постановки цели, определения способов ее достижения, разработки стратегий действий

Профессиональные компетенции в соответствии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции**	**Код и наименование индикатора достижения профессиональной компетенции**
научно-исследовательский			
Компьютерное моделирование исследуемых физических процессов, приборов, схем и устройств, относящихся к профессиональной сфере	Материалы, компоненты, электронные приборы, устройства, установки, методы их исследования, проектирования и конструирования, математические модели, алгоритмы решения типовых задач, современное программное и информационное обеспечение процессов моделирования и проектирования изделий электроники и наноэлектроники	ПК-2 Способен разрабатывать эффективные алгоритмы решения сформулированных задач с использованием современных языков программирования и обеспечивать их программную реализацию Профессиональный стандарт «06.001. Программист»	З-ПК-2 Знать современные языки программирования, компьютерных технологий, математических методов моделирования и прикладных программных макетов, основ информационной безопасности. У-ПК-2 Уметь: разрабатывать эффективные алгоритмы компьютерного моделирования в области электроники и наноэлектроники. В-ПК-2 Владеть: навыками программной реализации алгоритмов решения задач электроники и

			наноэлектроники
сбор, обработка, анализ и систематизация научнотехнической информации по теме исследования, выбор методик и средств решения задачи	Материалы, компоненты, электронные приборы, устройства, установки, методы их исследования, проектирования и конструирования, математические модели, алгоритмы решения типовых задач, современное программное и информационное обеспечение процессов моделирования и проектирования изделий электроники и наноэлектроники	ПК-6 Способен использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического и компьютерного моделирования в теоретических и расчетно-экспериментальных исследованиях Профессиональный стандарт «40.008. Специалист по организации и управлению научно-исследовательскими и опытно-конструкторскими работами»	З-ПК-6 Знать: основные законы высшей математики, физики конденсированных сред и других естественнонаучных дисциплин. У-ПК-6 Уметь: использовать основные законы физики конденсированных сред, методы высшей математики в теоретических и расчетно-экспериментальных исследованиях по электронике и наноэлектронике. В-ПК-6 Владеть: навыками математического и компьютерного моделирования в исследованиях по электронике и наноэлектронике.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ*

№ п/п	Наименование раздела /темы дисциплины	№ недели	Виды учебной работы					
			Лекции	Практ. занятия/ семинары	Лаб. работы	СРС	Текущий контроль (форма)*	Максимальный балл (см. п. 6.3)
			48	**48**		**180**		
Семестр № 1								
1.	**Введение в криптографию**		8	8		16		
1.1.	Тема 1		2	2	-	2	УО	2
1.2.	Тема 2		2	2	-	2	УО	2
1.3	Тема 3		2	2	-	2	УО	3
1.4	Тема 4		2	2	-	2	УО	3
Рубежный контроль		**8**					**УО**	10
2.								
2.1.	Тема 5		2	2	-	2	УО	3
2.2.	Тема 6		2	2	-	2	УО	3
2.3.	Тема 7		2	2	-	2	УО	4
2.4.	Тема 8		2	2	-	2	УО	5
Рубежный контроль		**16 (15)**					**Тест**	10
Промежуточная аттестация			**Зачет**				**36 / 0**	**0 - 50**
Посещаемость								**5**
Итого:			**32**	**16**	**-**	**16**		**100**
Семестр № 2								
3.	**Асимметричные криптосистемы и ЭП**		32	32	-	32		
3.1.	Тема 19		2	2	-	2	УО	1
3.2.	Тема 10		2	2	-	2	УО	1
3.1.	Тема 11		2	2	-	2	УО	1
3.2.	Тема 12		2	2	-	2	УО	1
3.1.	Тема 13		2	2	-	2	УО	1

№ п/п	Наименование раздела /темы дисциплины	№ недели	Виды учебной работы					
			Лекции	Практ. занятия/ семинары	Лаб. работы	СРС	Текущий контроль (форма)*	Максимальный балл (см. п. 6.3)
			48	48		180		
3.2.	Тема 14		2	2	-	2	УО	1
3.1.	Тема 15		2	2	-	2	УО	1
3.2.	Тема 16		2	2	-	2	УО	2
Рубежный контроль		**8**					**УО**	10
4.	**Криптопротоколы**		16	16	-	16		
4.1	Тема 17		2	2	-	2	УО	1
4.2	Тема 18		2	2	-	2	УО	2
4.3	Тема 19		2	2	-	2	УО	2
4.4	Тема 20		2	2	-	2	УО	2
4.5	Тема 21		2	2	-	2	УО	2
4.6	Тема 22		2	2	-	2	УО	2
4.7	Тема 23		2	2	-	2	УО	2
4.8	Тема 24		2	2	-	2	УО	2
Рубежный контроль		**15**					**Контр.**	10
Промежуточная аттестация			**Экзамен**				**36**	**0 - 50**
Посещаемость								**5**
Итого:			**48**	**48**	**-**	**48**	**36**	**100**

***Сокращение наименований форм текущего, рубежного и промежуточного контроля:**

УО – устный опрос
Контр. – контрольная работа
Тест **– *тестирование (письменный опрос)***
ДЗ – домашнее задание
РГР – расчетно-графическая работа
Э/Зач/ЗсО – экзамен/зачет/зачет с оценкой и др.

4.2. Содержание дисциплины, структурированное по разделам (темам)

Лекционный курс

№	Наименование раздела /темы дисциплины	Содержание
1.	**Введение в криптографию**	
1.1.	Тема 1	Основные понятия и определения криптографии.
1.2.	Тема 2	Этапы развития криптографии. Роль математики в развитии методов защиты информации. Новые направления в криптографии.
1.3	Тема 3	Криптографические примитивы и криптографические протоколы по защите информации.
1.4	Тема 4	Двухсторонние и многосторонние протоколы. Типы предполагаемых противников. Формальные методы оценки качества криптографических протоколов.
2.	**Основные шифры**	
2.1.	Тема 5	Шифры. Примеры. Стойкость шифра. Классификация методов дешифрования. Шифрующие автоматы. Типовые узлы. Регистры сдвига с обратной связью. Линейные последовательностные машины.
2.2.	Тема 6	Блочные и поточные криптосистемы и их классификация. Описание DES - AES, ГОСТ 28147-89, RC4 и др. Режимы использования и их сравнение (ECB,CBC, OFB, …).
2.3.	Тема 7	Криптографические свойства функций.
2.4.	Тема 8	Теория информации и криптография. Совершенная секретность по Шеннону.
3.	**Асимметричные криптосистемы и ЭП**	
3.1.	Тема 19	Теория сложности вычислений и криптография. Используемые в криптографии задачи теории сложности и их оценка.
3.2.	Тема 10	Основные понятия криптографии с открытым ключом. Сравнение криптосистем с открытым и секретным ключом.
3.1.	Тема 11	Однонаправленные (односторонние) функции по Нидхэму. Однонаправленные функции, основанные на сложности задачи дискретного логарифмирования. Применения в современных технологиях.
3.2.	Тема 12	Однонаправленные (односторонние) функции с секретом и их применение для цели шифрования информации. Схемы RSA, Рабина, Эль Гамаля, МакЭлайса, Меркля – Хеллмана.
3.1.	Тема 13	Понятия о цифровой подписи на основе однонаправленной функции с секретом. Классификация атак на схемы цифровой подписи.
3.2.	Тема 14	Некоторые методы быстрой модульной арифметики и их применение для ускорения криптографических алгоритмов.
3.1.	Тема 15	Сравнение стандартов цифровой подписи США (FIPS PUB 186) и России (ГОСТ Р 34.10-94). Стандарт цифровой подписи ГОСТ Р 34.10-2001 на основе эллиптических кривых.
3.2.	Тема 16	Схемы подписи Фиата-Шамира, Файге-Фиата-Шамира и др. Схема Шнорра.
4.	**Криптопротоколы**	
4.1	Тема 17	Управление ключами. Доказуемо безопасные генераторы ключей. Некоторые способы сокращения объемов хранимых ключей.
4.2	Тема 18	Протоколы распределения криптографических ключей.
4.3	Тема 19	Криптографическая инфраструктура на основе механизма открытых ключей (PKI). Модели криптографической инфраструктуры.
4.4	Тема 20	Протоколы, основанные на идентификационной информации (ID-based cryptosystems).
4.5	Тема 21	Протоколы с разделением секрета. Пороговые схемы.
4.6	Тема 22	Криптосистемы и протоколы на эллиптических кривых.
4.7	Тема 23	Протоколы идентификации и аутентификации.
4.8	Тема 24	Протоколы честного обмена секретами.

Практические/семинарские занятия

№	Наименование раздела /темы дисциплины	Содержание
1.	**Введение в криптографию**	
1.1.	Тема 1	Основные понятия и определения криптографии.
1.2.	Тема 2	Этапы развития криптографии. Роль математики в развитии методов защиты информации. Новые направления в криптографии.
1.3	Тема 3	Криптографические примитивы и криптографические протоколы по защите информации.
1.4	Тема 4	Двухсторонние и многосторонние протоколы. Типы предполагаемых противников. Формальные методы оценки качества криптографических протоколов.
2.	**Основные шифры**	
2.1.	Тема 5	Шифры. Примеры. Стойкость шифра. Классификация методов дешифрования. Шифрующие автоматы. Типовые узлы. Регистры сдвига с обратной связью. Линейные последовательностные машины.
2.2.	Тема 6	Блочные и поточные криптосистемы и их классификация. Описание DES - AES, ГОСТ 28147-89, RC4 и др. Режимы использования и их сравнение (ECB,CBC, OFB, …).
2.3.	Тема 7	Криптографические свойства функций.
2.4.	Тема 8	Теория информации и криптография. Совершенная секретность по Шеннону.
3.	**Асимметричные криптосистемы и ЭП**	
3.1.	Тема 9	Теория сложности вычислений и криптография. Используемые в криптографии задачи теории сложности и их оценка.
3.2.	Тема 10	Основные понятия криптографии с открытым ключом. Сравнение криптосистем с открытым и секретным ключом.
3.1.	Тема 11	Подпись вслепую (blind signature) и ее применения.
3.2.	Тема 12	Схемы конфиденциальной подписи (undeniable signature) и их применение. Протоколы проверки и отвержения как примеры протоколов доказательств с нулевым разглашением. Схемы Шаума.
3.1.	Тема 13	Схемы подписи, в которых подделка подписи может быть доказана.
3.2.	Тема 14	Схемы мультиподписи (multisignature scheme).
3.1.	Тема 15	Подпись по доверенности (proxy signature).
3.2.	Тема 16	Функции хэширования. Американский стандарт функции хэширования (SHS) и его изменения. Российский стандарт функции хэширования (ГОСТ Р 34.11-94).
4.	**Криптопротоколы**	
4.1	Тема 17	Управление ключами. Доказуемо безопасные генераторы ключей. Некоторые способы сокращения объемов хранимых ключей.
4.2	Тема 18	Протоколы распределения криптографических ключей.
4.3	Тема 19	Криптографическая инфраструктура на основе механизма открытых ключей (PKI). Модели криптографической инфраструктуры.
4.4	Тема 20	Протоколы, основанные на идентификационной информации (ID-based cryptosystems).
4.5	Тема 21	Интерактивные схемы доказательств.
4.6	Тема 22	Протоколы электронного тайного голосования.
4.7	Тема 23	Понятие о протоколах электронных платежей.
4.8	Тема 24	Вопросы стандартизации и патентования.

4.3. Перечень учебно-методического обеспечения для самостоятельной работы студентов

1 Захарова Н.А., Николаев Д.Б. Построение и анализ формирователей параметрической информации с заданными характеристиками. Учебно-методическое пособие. ФГБОУ ВПО НИЯУ МИФИ СарФТИ, Саров, 2010 г., 60 с.

2 Мартынов А.П., Николаев Д.Б., Седаков А.В. Современные направления развития симметричных криптографических систем. Учебно-методическое пособие. ФГБОУ ВПО НИЯУ МИФИ СарФТИ, Саров, 2010 г., 160 с.

3 Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем. Учебное пособие. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2011 г., 411 с.

4 Грибунин В.Г., Костюков В.Е., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Современные методы обеспечения безопасности информации в атомной энергетике. Монография. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2014 г., 636 с.

5 Волков К.О., Мартынов А.П., Николаев Д.Б., Марунин М.В. Аналитические исследования характеристик информационной составляющей автоматизированных систем управления и контроля. Учебно-методическое пособие. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2017 г., 197 с.

6 Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и электроника. Учебное пособие. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2020 г., 552 с.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

5.1. Паспорт фонда оценочных средств по дисциплине

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Раздел	Темы занятий	Компетенция	Индикаторы освоения	Текущий контроль, неделя
Семестр 1				
Раздел 1	Тема 1.	УК-1 ПК-2 ПК-6	З-УК-1;У-УК-1; В-УК-1	УО - 1
	Тема 2.		З-ПК-2; У-ПК-2; В-ПК-2	УО - 3
	Тема 3.		З-ПК-6; У-ПК-6; В-ПК-6	УО - 5
	Тема 4.		З-ПК-6; У-ПК-6; В-ПК-6	УО - 7

Рубежный контроль		УК-1 ПК-2 ПК-6	З-УК-1;У-УК-1; В-УК-1	УО – 7
			З-ПК-2; У-ПК-2; В-ПК-2	
			З-ПК-6; У-ПК-6; В-ПК-6	
Раздел 2	Тема 5.	УК-1 ПК-2 ПК-6	З-УК-1;У-УК-1; В-УК-1	УО - 9
	Тема 6.		З-ПК-2; У-ПК-2; В-ПК-2	УО - 11
	Тема 7.		З-ПК-6; У-ПК-6; В-ПК-6	УО - 13
	Тема 8.		З-ПК-6; У-ПК-6; В-ПК-6	УО - 15
Рубежный контроль		УК-1 ПК-2 ПК-6	З-УК-1;У-УК-1; В-УК-1	Тест – 15 (16)
			З-ПК-2; У-ПК-2; В-ПК-2	
			З-ПК-6; У-ПК-6; В-ПК-6	
Промежуточная аттестация		УК-1 ПК-2 ПК-6	З-УК-1;У-УК-1; В-УК-1	**Зачет**
			З-ПК-2; У-ПК-2; В-ПК-2	
			З-ПК-6; У-ПК-6; В-ПК-6	
Семестр 2				
Раздел 3	Тема 9.	УК-1 ПК-2 ПК-6	З-УК-1;У-УК-1; В-УК-1	УО - 1
	Тема 10.		З-ПК-2; У-ПК-2; В-ПК-2	УО - 2
	Тема 11.		З-ПК-6; У-ПК-6; В-ПК-6	УО - 3
	Тема 12.		З-ПК-6; У-ПК-6; В-ПК-6	УО - 4
	Тема 13.		З-ПК-2; У-ПК-2; В-ПК-2	УО - 5
	Тема 14.		З-ПК-6; У-ПК-6; В-ПК-6	УО - 6
	Тема 15.		З-ПК-6; У-ПК-6; В-ПК-6	УО - 7
	Тема 16.		З-ПК-6; У-ПК-6; В-ПК-6	УО - 8
Рубежный контроль		УК-1 ПК-2 ПК-6	З-УК-1;У-УК-1; В-УК-1	УО –8
			З-ПК-2; У-ПК-2; В-ПК-2	
			З-ПК-6; У-ПК-6; В-ПК-6	
Раздел 4	Тема 17	УК-1 ПК-2 ПК-6	З-УК-1;У-УК-1; В-УК-1	УО - 9
	Тема 18		З-ПК-2; У-ПК-2; В-ПК-2	УО - 10

	Тема 19		З-ПК-6; У-ПК-6; В-ПК-6	УО - 11
	Тема 20		З-ПК-6; У-ПК-6; В-ПК-6	УО - 12
	Тема 21		З-ПК-2; У-ПК-2; В-ПК-2	УО - 13
	Тема 22		З-ПК-6; У-ПК-6; В-ПК-6	УО - 14
	Тема 23		З-ПК-6; У-ПК-6; В-ПК-6	УО - 15
	Тема 24		З-ПК-6; У-ПК-6; В-ПК-6	УО - 16
Рубежный контроль		УК-1 ПК-2 ПК-6	З-УК-1;У-УК-1; В-УК-1	Тест –15 (16)
			З-ПК-2; У-ПК-2; В-ПК-2	
			З-ПК-6; У-ПК-6; В-ПК-6	
Промежуточная аттестация		УК-1 ПК-2 ПК-6	З-УК-1;У-УК-1; В-УК-1	**Экзамен**
			З-ПК-2; У-ПК-2; В-ПК-2	
			З-ПК-6; У-ПК-6; В-ПК-6	

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

5.2.1. Примерные вопросы к экзамену или зачету

а) типовые вопросы (задания):

1. Основные понятия и определения криптографии.

2. Этапы развития криптографии. Роль математики в развитии методов защиты информации. Новые направления в криптографии.

3. Криптографические примитивы и криптографические протоколы по защите информации.

4. Двухсторонние и многосторонние протоколы. Типы предполагаемых противников.

5. Формальные методы оценки качества криптографических протоколов.

6. Шифры. Примеры. Стойкость шифра.

7. Классификация методов дешифрования. Шифрующие автоматы. Типовые узлы. Регистры сдвига с обратной связью. Линейные последовательностные машины.

8. Блочные и поточные криптосистемы и их классификация. Описание DES - AES, ГОСТ 28147-89, RC4 и др. Режимы использования и их сравнение (ECB,CBC, OFB, …).

8. Криптографические свойства функций.

9. Теория информации и криптография. Совершенная секретность по Шеннону.

10. Теория сложности вычислений и криптография. Используемые в криптографии задачи теории сложности и их оценка.

11. Основные понятия криптографии с открытым ключом.

12. Сравнение криптосистем с открытым и секретным ключом.

13. Однонаправленные (односторонние) функции по Нидхэму. Однонаправленные функции, основанные на сложности задачи дискретного логарифмирования. Применения в современных технологиях.

14. Однонаправленные (односторонние) функции с секретом и их применение для цели шифрования информации.

15. Схемы RSA, Рабина, Эль Гамаля, МакЭлайса, Меркля – Хеллмана.

16. Понятия о цифровой подписи на основе однонаправленной функции с секретом. Классификация атак на схемы цифровой подписи.

17. Некоторые методы быстрой модульной арифметики и их применение для ускорения криптографических алгоритмов.

18. Сравнение стандартов цифровой подписи США (FIPS PUB 186) и России (ГОСТ Р 34.10-94). Стандарт цифровой подписи ГОСТ Р 34.10-2001 на основе эллиптических кривых.

19. Схемы подписи Фиата-Шамира, Файге-Фиата-Шамира и др. Схема Шнорра.

20. Подпись вслепую (blind signature) и ее применения.

21. Схемы конфиденциальной подписи (undeniable signature) и их применение.

22. Протоколы проверки и отвержения как примеры протоколов доказательств с нулевым разглашением. Схемы Шаума.

23. Схемы подписи, в которых подделка подписи может быть доказана.

24. Схемы мультиподписи (multisignature scheme).

25. Групповая подпись (group signature scheme).

26. Подпись по доверенности (proxy signature).

27. Функции хэширования.

28. Американский стандарт функции хэширования (SHS) и его изменения.

29. Российский стандарт функции хэширования (ГОСТ Р 34.11-94).

30. Управление ключами. Доказуемо безопасные генераторы ключей. Некоторые способы сокращения объемов хранимых ключей.

31. Протоколы распределения криптографических ключей.

32. Криптографическая инфраструктура на основе механизма открытых ключей(PKI).

33. Модели криптографической инфраструктуры.

34. Протоколы, основанные на идентификационной информации (ID-based cryptosystems).

35. Протоколы с разделением секрета. Пороговые схемы.

36. Криптосистемы и протоколы на эллиптических кривых.

37. Протоколы идентификации и аутентификации.

38. Протоколы честного обмена секретами.

39. Интерактивные схемы доказательств

40. Протоколы электронного тайного голосования .

41. Понятие о протоколах электронных платежей

42. Вопросы стандартизации и патентования

б) критерии оценивания компетенций (результатов):

балльно-рейтинговая система

в) описание шкалы оценивания:

приведено в п 5.3.

5.2.2. Примерные вопросы для устного опроса

а) типовые задания (вопросы) - образец:

1. Криптографические средства защиты информации в стандарте GSM и их стойкость.

2. Исследование алгоритма поточного шифрования RC4.

3. Особенности применения цифровой подписи вслепую в протоколах электронного тайного голосования.

4. Новые американские стандарты режимов шифрования с аутентификацией.

5. Схемы криптосистем на основе парных отображений.

6. Методы эффективной реализации схем электронной цифровой подписи на основе группы точек эллиптических кривых.

7. Возможности преобразования отечественного стандарта цифровой подписи в схему цифровой подписи вслепую.

8. Сравнение криптографических средств различных протоколов мобильных платежей.

9. Исследование свойств подстановок на двоичных векторах при малых размерностях и их применение при построении узлов алгоритмов шифрования.

10. Решение проблемы повторной траты криптографическими методами в схемах электронных платежей.

б) критерии оценивания компетенций (результатов):

балльная система

в) описание шкалы оценивания:

правильный ответ – весовой коэффициент оценки в баллах, неправильный ответ – 0 баллов.

5.2.3. Наименование оценочного средства (тест**)**

а) типовые задания (вопросы) - образец:

1. Шифрование – это…

А) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого

Б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств

В) удобная среда для вычисления конечного пользователя

б) критерии оценивания компетенций (результатов):

балльная система

в) описание шкалы оценивания:

правильный ответ – весовой коэффициент оценки в баллах, неправильный ответ – 0 баллов.

5.3. Шкалы оценки образовательных достижений

Рейтинговая оценка знаний является интегральным показателем качества теоретических и практических знаний и навыков студентов по дисциплине и складывается из оценок, полученных в ходе текущего контроля и промежуточной аттестации.

Результаты текущего контроля и промежуточной аттестации подводятся по шкале балльно-рейтинговой системы.

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает
75-84		C	

70-74		D	материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
65-69	3 – «*удовлетворительно*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. Русский перевод: Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Вильямс, 2001. – 672 с.

2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.:ДМК, 2000. – 448 с.

3. Ростовцев А.Г. Алгебраические основы криптографии. – СПб: Мир и Семья, 2000.

4. Ростовцев А.Г., Маховенко Е.А. Введение в криптографию с открытым ключом. – СПб.: Мир и Семья, 2000.

5. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРБ, 2001. –480 с.

6. Burnet S., Paine S. RSA Security`s Official Guide to Cryptography.- NY.: The McGraw-Hill Companies, 2001.

7. Русский перевод: Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security.- М.: Бином-Пресс, 2002. –384 с.

8. Харин Ю.С., Агиевич С.В. Компьютерный практикум по математическим методам защиты информации. – Мн.:БГУ, 2001. – 190 с.

9. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. – М.: Гелиос АРБ, 2002. – 432 с.

10.Smith R. Authenticaton: From Passwords to Public Keys. – NY: Addison-Wesley Publishing Company, Inc., 2002.

11. Русский перевод: Смит Р. Аутентификация: от паролей до открытых ключей. –М.: Вильямс, 2002. – 432 с.

12. Чмора А.Л. Современная прикладная криптография. 2-е изд., стер. – М.: Гелиос АРБ, 2002. – 256 с.

13. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.

14. Масленников М.Е., Практическая криптография, -СПб.: БХВ-Петербург, 2003.-464 с.

15. Фомичев В.М., Дискретная математика и криптология. - М.: ДИАЛОГ - МИФИ, 2003.

16. Болотов А.А., Гашков С.Б., Фролов А.Б. Алгоритмические основы эллиптической криптографии, 2003.-526 стр.

17. Вельшенбах М., Криптография на Си и Си++ в действии. -М.: Триумф, 2004.

18. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. – М.: Гелиос АРВ, 2005.

19. Фергюссон Н., Шнайер Б. Практическая криптография. – Издательский дом «Вильямс», 2005.-424 с.

20. Венбо Мао. Современная криптография: теория и практика.: Пер. с англ.- М.: Вильямс, 2005. 768 с.

21. Смарт Н. Криптография. М.: Техносфера, 2005.- 528 с.

22. Земор Ж. Курс криптографии.- М.-Ижевск: НИЦ”Регулярная и хаотическая динамика”; Институт компьютерных исследований, 2006.-256.

23. Тилборг Ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.; Мир, 2006, 471 с.

24. Словарь криптографических терминов/ Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006.- 94 с.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

1. Конеев И., Беляев А. Информационная безопасность предприятия. - СПб.: БХВ-Петербург, 2003.-752с.(Часть 5. Криптография, 209-364 стр.)

2. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. - СПб: 2003. http://lib.aldebaran.ru/author/shnaier_bryus/shnaier_bryus_sekrety_i_lozh_bezopasnost_dannyh_v_cifrovom_mire/

3. Скляров Д.В., Искусство защиты и взлома информации.- СПб.: БХВ-Петербург, 2004.- 288 с.

4. Максим М., Полино Д. Безопасность беспроводных сетей. – М.: Компания АйТи, ДМК Пресс, 2004. – 288 с.(пер. книги 2002 изд.)

5. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов, М.: Горячая линия – Телеком, 2006.- 544 с.

6. Mangard S., Oswald E., Popp T., Power Analysis attacks, Revealing the Secrets of Smart Cards, Springer, 2007, - 337 стр.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. Национальная платформа открытого образования

7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Освоение дисциплины производится на базе учебных лабораторий кафедры в СарФТИ НИЯУ МИФИ. Лаборатории оснащены современным оборудованием, позволяющим проводить практические и лабораторные занятия. Выполнение лабораторных работ, а также самостоятельной работы студентов осуществляется на рабочих местах, оснащенных макетами.

В качестве материально-технического обеспечения используются также ресурсы и программно-аппаратное обеспечение компьютерного класса (комплекс LabVIEW).

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При чтении лекционного материала используется электронное сопровождение курса: справочно-иллюстративный материал воспроизводится и озвучивается в аудитории с использованием проектора и переносного компьютера в реальном времени.

По дисциплине «Криптография и специсследования» в рабочем учебном плане предусмотрены интерактивные часы для проведения практических занятий.

Данный вид деятельности реализуется с помощью видео лекций ведущих специалистов в области информационной безопасности.

9. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ СТУДЕНТАМ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Изучение данного курса обеспечивает студента сведениями о современном состоянии в области криптографии. Курс существенно расширяет и углубляет знания, полученные студентами при изучении дисциплины «Криптография и специсследования». Материал курса основан на последних достижениях зарубежных и отечественных специалистов – криптографов как в классических областях применения криптографии, так и в новых, связанных с новыми информационными технологиями.

Существенное место в курсе уделено и стандартным методам и рекомендациям криптографической защиты информации, позволяющим существенно ускорить разработку и внедрение новых систем.

Рекомендации преподавателю

Предлагается:

В дисциплине необходимо уделить большое внимание рассмотрению и изложению материала, связанного со следующими темами:

- блочные и поточные криптосистемы и их классификация;
- криптографические свойства функций;
- криптографические применения теории сложности вычислений;
- основные понятия криптографии с открытым ключом;
- разновидности протоколов электронной цифровой подписи;
- функции хэширования;
- проблемы управления ключами;
- криптосистемы и протоколы на эллиптических кривых;
- протоколы идентификации и аутентификации;
- протоколы честного обмена секретами;
- интерактивные схемы доказательств с нулевым разглашением;
- протоколы электронного тайного голосования;
- протоколы электронных платежей;
- вопросы стандартизации и патентования;
- необходимые сведения из алгебры и теории чисел.

Рекомендации студенту

Предлагается:

- Самостоятельно прорабатывать лекционный материал для более полного усвоения материала;
- В учебном процессе при выполнении практикума эффективно использовать методические пособия и методический материал;

- Активно использовать Интернет-ресурсы для получения актуального материала по изучаемой дисциплине;
- Активно использовать Интернет-ресурсы для обновления инструментальной базы (систем программирования, инструментальных сред и т.д.) при выполнении лабораторных работ.

Рабочая программа дисциплины составлена в соответствии с ОС НИЯУ МИФИ (ФГОС) и учебным планом основной образовательной программы (программ).

Автор(ы): профессор кафедры РФ А.П. Мартынов

Рецензент(ы): профессор кафедры РФ В.Н. Фомченко