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**)

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЭЛЕКТРОНИКИ
Кафедра «Вычислительной и информационной техники»

УТВЕРЖДАЮ
Декан ФИТЭ, к.ф-м.н., доцент
_____В.С. Холушкин
«___» _____ 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

КРИПТОГРАФИЯ
наименование дисциплины

Направление подготовки (специальность)	09.03.01 Информатика и вычислительная техника
Наименование образовательной программы	Вычислительные машины, комплексы, системы и сети
Квалификация (степень) выпускника	бакалавр
Форма обучения	очная

Программа одобрена на заседании кафедры
Протокол № от 2020

Зав. кафедрой ВИТ
_____ В.С. Холушкин
«____» _____ 2020 г.

г. Саров, 2020 г.

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ, ФИТЭ на 202____/202_____ учебный год.

Заведующий кафедрой ВИТ В.С. Холушкин

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ, ФИТЭ на 202____/202_____ учебный год.

Заведующий кафедрой ВИТ В.С. Холушкин

Программа переутверждена на 202____/202___учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ, ФИТЭ на 202____/202_____ учебный год.

Заведующий кафедрой ВИТ В.С. Холушкин

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с Семестровыми учебными планами академических групп ФТФ, ФИТЭ на 202____/202_____ учебный год.

Заведующий кафедрой ВИТ В.С. Холушкин

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/
7	32	3	108	16	-	32	60	-	Зач.
ИТОГО	**32**	**3**	**108**	**16**	**-**	**32**	**60**	**-**	**Зач.**

АННОТАЦИЯ

Курс посвящен изучению теоретических и практических основ криптографии и защиты информации. Изучаются способы и методы разработки современных инструментальных и программных средств защиты криптографии и информации и их применение при решении научно-исследовательских и производственных задач из различных предметных областей. Главная цель преподавания дисциплины – подготовка специалиста, владеющего фундаментальными знаниями и практическими навыками в области криптографии.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основная цель дисциплины:

обеспечить комплексность и полноту подготовки бакалавриата по направлению «Информатика и вычислительная техника» путем формирования у студентов знаний и навыков в области современной криптографии и ее приложениям для обеспечения безопасности новых информационных технологий.

Задачи дисциплины:

ознакомить студентов с основными проблемами в области создания и анализа средств криптографической защиты информации, а также с методами и средствами их решения;

обеспечить необходимыми сведениями и навыками для последующего обучения по направлению подготовки «Информатика и вычислительная техника».

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

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

Освоение дисциплины «Криптография» 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 бакалавра.

3.ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные компетенции

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УКЕ-1 Способен использовать знания естественнонаучных дисциплин, применять методы математического анализа и моделирования, теоретического и экспериментального исследования в поставленных задачах	**З-УКЕ-1** знать: основные законы естественнонаучных дисциплин, методы математического анализа и моделирования, теоретического и экспериментального исследования **У-УКЕ-1** уметь: использовать математические методы в технических приложениях, рассчитывать основные числовые характеристики случайных величин, решать основные задачи математической статистики; решать типовые расчетные задачи **В-УКЕ-1** владеть: методами математического анализа и моделирования; методами решения задач анализа и расчета характеристик физических систем, основными приемами обработки экспериментальных данных, методами работы с прикладными программными продуктами

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
Типы задач профессиональной деятельности: Производственно-технологический, научно-исследовательский и инновационный			
применение современных инструментальных средств при разработке программного обеспечения;	высокопроизводительные вычислительные системы, комплексы и сети; системное и прикладное программное обеспечение на современной аппаратной платформе высокопроизводительных вычислительных систем; многофункциональные компьютерные сети на современной аппаратной платформе; автоматизированные системы обработки информации и управления; системы автоматизированного проектирования и информа-	ПК-3 Способен разрабатывать модели и компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии *Основание:* Профессиональный стандарт «06.001 Программист» Профессиональный стандарт «06.011 Администратор баз данных»	З-ПК-3 Знать: схемотехнику логических схем, цифровых и запоминающих устройств, принципы построения и элементы микропроцессоров и микроконтроллеров, принципы работы программируемых логических матриц и программируемой матричной логики, основы объектно-ориентированного подхода к программированию,

	ционной поддержки жизненного цикла промышленных изделий;		базы данных и системы управления базами данных для информационных систем различного назначения, принципы построения современных операционных систем и особенности их применения У-ПК-3 Уметь: строить логические схемы счетчиков, регистров сумматоров и запоминающих устройств, строить временные диаграммы работы интерфейсов и контроллеров, сопрягать Аппаратные и программные средства в составе аппаратно-программных комплексов, работать с современными системами программирования, включая объектно-ориентированные В-ПК-3 Владеть: современными инструментальными средствами проектирования цифровых устройств, языками процедурного и объектно-ориентированного программирования, навыками разработки и отладки программ

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. 5.3)
			16	-	32	60		
Семестр 7								
Раздел 1.								
1.1.	Тема 1. Введение. Понятие о шифрах.	**1,2**	**2**	**-**		**6**	**УО**	**4**
1.2	Тема 2. Блочные м поточные криптосистемы и их классификация. Криптографические свойства функций.	**3-4**	**2**	**-**	**8**	**6**	**Защита ЛР**	**4**
Раздел 2.								
2.1	Тема 1. Теория информации и криптография. Теория сложности вычислений и криптография.	**5-6**	**2**	**-**		**8**	**УО**	**4**
2.2	Тема 2. Основные понятия криптографии с открытым ключом. Цифровая подпись.	**7-8**	**2**	**-**	**4**	**8**	**Защита ЛР**	**4**
2.3	Тема 3. Разновидности протоколов электронной цифровой подписи. Функции хэширования. Управление ключами. Криптосистемы и протоколы на эллиптических кривых.	**9**	**2**	**-**		**8**	**УО**	**4**
2.4	Тема 4. Управление ключами. Разновидности протоколов электронной цифровой подписи. Протоколы идентификации и аутентификации. Протоколы честного обмена секретами	**10**	**2**	**-**	**4**	**8**	**Защита ЛР**	**4**

№ п/п	Наименование раздела /темы дисциплины	№ недели	Виды учебной работы					
			Лекции	Практ. занятия/ семинары	Лаб. работы	СРС	Текущий контроль (форма)*	Максимальный балл (см. п. 5.3)
			16	-	32	60		
	Рубежный контроль	**11**					**СР**	**8**
Раздел 3.								
3.1	Тема 1. Интерактивные схемы доказательств. Протоколы электронного тайного голосования Понятие о протоколах электронных платежей. Вопросы стандартизации и патентования	**12-13**	**2**	**-**	**8**	**8**	**УО**	**4**
3.2	Тема 2. Необходимые сведения из алгебры и теории чисел	**14-15**	**2**	**-**	**8**	**8**	**Защита ЛР**	**4**
	Рубежный контроль	**16**					**СР**	**5**
	Промежуточная аттестация					**З**	**-**	**50**
	Посещаемость							**5**
	Итого:		**16**		**32**	**60**	**-**	**100**

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

УО – устный опрос

СР – самостоятельная работа(решение задачи на заданную тему)

РГР – расчетно – графическая работа

4.2. Содержание дисциплины, структурированное по разделам (темам)

Лекционный курс

№	Наименование раздела /темы дисциплины	Содержание
	Раздел 1	
1.1	Тема 1.Введение. Понятие о шифрах	Основные понятия и определения. Криптография или криптология. Информационная безопасность и криптография. Различные аспекты безопасности информации (секретность, целостность, аутентичность, неотказуемость, неотслеживаемость, …) и методы криптографии, обеспечивающие их выполнение при хранении и передаче информации в телекоммуникационных системах. По-

		литика различных организаций в области защиты информации. Криптография и криптоанализ (дешифрование). Этапы развития криптографии. Роль математики в развитии методов защиты информации. Новые направления в криптографии. Криптографические примитивы и криптографические протоколы по защите информации. Классификация примитивов с открытым ключом. Протоколы с арбитром, с судьей, самодостаточные (self-enforcing) протоколы. Двухсторонние и многосторонние протоколы. Типы предполагаемых противников. Формальные методы оценки качества криптографических протоколов. Шифры перестановки и замены. Примеры. Стойкость шифра. Классификация методов дешифрования по информации, известной криптоаналитику. Ручные шифры. Электронные и механические реализации шифров. Модель предполагаемого нарушителя. Правила Керкхоффса. Понятие о криптографических протоколах. Конечные автоматы. Эквивалентность конечных автоматов и их состояний. Шифрующие автоматы. Регистры сдвига с обратной связью над различными алгебраическими структурами. Линейные последовательностные машины. Линейные рекуррентные последовательности.
1.2	Тема 2. Блочные м поточные криптосистемы и их классификация. Криптографические свойства	Определения. Примеры. Описание DES - AES, ГОСТ 28147-89, RC4 и др. Режимы использования и их сравнение (ECB,CBC, OFB, …). Некоторые методы криптоанализа. Равновероятность (равновесность). Свойство лавинного эффекта. Свойство строго лавинного эффекта порядка m. Совершенные нелинейные булевы функции. Множество булевых функций, обладающих линейными структурами. Понятие корреляционной независимости. Бент - функции. Свойство размазывания. Строение и свойства S-блоков.
Раздел 2		
2.1	Тема 1. Теория информации и криптография. Теория сложности вычислений и криптография.	Энтропия, условная энтропия. Совершенная секретность по Шеннону. Примеры. Шифр одноразового блокнота (Шифр Вернама). Практическая стойкость шифров. Рабочая характеристика. Расстояние единственности для не совершенно секретных шифров. Метод Хеллмана оценки расстояния единственности. Понятие об управлении ключами криптосистем. Краткое введение в теорию сложности. Вычислительные машины, задачи, алгоритмы и сложность. Временная, емкостная, асимптотическая сложность. Сложность в худшем случае, средняя сложность. Модели вычислений. Решаемые, трудные и алгоритмически неразрешимые задачи. Классификация задач по сложности. Классы P, NP, NP-полные, … . Полиномиальная сводимость. Теорема Кука. Используемые в криптографии задачи теории сложно-

		сти: задача о коммивояжере, задача о рюкзаке, задача о выполнимости, задача о факторизации больших целых чисел, задача о дискретном логарифмировании, и др. Современные оценки сложности решения этих задач.
2.2	Тема 2.Основные понятия криптографии с открытым ключом. Цифровая подпись.	Предпосылки появления криптографии с открытым ключом. Сравнение криптосистем с открытым и секретным ключом. Однонаправленные (односторонние) функции по Нидхэму. Связь с NP-полными задачами. Примеры однонаправленных функций на основе блочных шифров. Применение в протоколах аутентификации. Программный продукт S/KEY фирмы Bellcore. Однонаправленные функции, основанные на сложности задачи дискретного логарифмирования. Схема открытого распределения ключей Диффи и Хеллмана. Шарады Меркля. Однонаправленные (односторонние) функции с секретом и их применение для цели шифрования информации. Понятия о цифровой подписи на основе однонаправленной функции с секретом. Классификация атак на схемы цифровой подписи. Схемы шифрования с открытым ключом. Основные принципы. Схемы RSA и Рабина и их применение. Схемы открытого шифрования Эль Гамаля, МакЭлайса, Меркля – Хеллмана и др. Атаки, выбор безопасных параметров. Некоторые методы быстрой модульной арифметики и их применение для ускорения криптографических алгоритмов. Алгоритм Монтгомери и его модификации. Подходы к конструированию криптосистем: теоретико-информационный, теоретико - сложностной и теоретико-системный. **Цифровая подпись.** Основные понятия. Типы атак на схемы подписи. Схема Лампорта одноразовой подписи. Схемы цифровой подписи RSA и Рабина. Схема цифровой подписи Эль Гамаля и ее модификации. Способы ускорения процедур подписи и проверки. Сравнение стандартов цифровой подписи США (FIPS PUB 186) и России (ГОСТ Р 34.10-94). Новый стандарт цифровой подписи ГОСТ Р 34.10-2001 на основе эллиптических кривых. Методы генерации секретных параметров для стандартов цифровой подписи. Схемы подписи Фиата-Шамира, Файге-Фиата-Шамира и др. Схема Шнорра.
2.3	Тема 3. Разновидности протоколов электронной цифровой подписи. Функции хэширования. Управление ключами. Криптосистемы и протоколы на эллиптических кривых.	Подпись вслепую (blind signature) и ее применения. Схемы конфиденциальной подписи (undeniable signature) и их применение. Протоколы проверки и отвержения как примеры протоколов доказательств с нулевым разглашением. Схемы Шаума. Схемы подписи, в которых подделка подписи может быть доказана. Схемы мультиподписи (multisignature scheme). Групповая подпись (group signature scheme). Схемы подписи с восстановлением сообщения (message recovery). Подпись по доверенности

		(proxy signature). Подписи с обнаружением подделки (fail-stop digital signature). Подписи, подтверждаемые доверенным лицом (designated confirmer signature). Ring signature. **Функции хэширования.** Классификация. Слабые и сильные функции хэширования. Функции хэширования без ключа (MDC) и с ключом (MAC). Атаки на функции хэширования. Принципы построения. Слабости функций хэширования Ривеста: MD2, MD4, MD5. Американский стандарт функции хэширования (SHS) и его изменения. Российский стандарт функции хэширования (ГОСТ Р 34.11-94). Применение функции хэширования в схемах цифровой подписи и при построении криптосистем. **Управление ключами.** Классификация ключей по типу алгоритма и использованию. Генерация и хранение ключей. Требования к генераторам псевдослучайных последовательностей. Тестирование генераторов. Доказуемо безопасные генераторы ключей. Некоторые способы сокращения объемов хранимых ключей. Протоколы распределения криптографических ключей. Виды протоколов распределения. Протоколы типа Диффи-Хеллмана. Протоколы выработки и распределения сеансовых ключей. Kerberos. Особенности реализации в ОС Windows 2000. Криптографическая инфраструктура на основе механизма открытых ключей(PKI). Модели криптографической инфраструктуры. Стандарт X.509, SPKI – Simple Public Key Infrastructure, PGP – Pretty Good Privacy. Протоколы, основанные на идентификационной информации (ID-based cryptosystems). Протоколы для конференц- связи. Протокол Ингемарссона-Танга-Вонга. Иерархические схемы распределения ключей. Протоколы с разделения секрета. Пороговые схемы. Депонирование ключей (Key Escrow). **Криптосистемы и протоколы на эллиптических кривых.** Представление открытого текста. Аналог схемы открытого распределения ключей Диффи- Хеллмана, аналоги схем шифрования с открытым ключом Месси-Омуры, Эль-Гамаля и др. Примеры реализации.
2.4	Тема 4. Управление ключами Разновидности протоколов электронной цифровой подписи. Протоколы идентификации и аутентификации. Протоколы честного обмена секретами	**Протоколы идентификации и аутентификации.** Слабая и сильная аутентификация. Методы аутентификации на основе криптосистем с секретным или открытым ключом. Протоколы Файге-Фиата-Шамира, GQ протокол идентификации (Guillou-Quisquater). Протокол Шнорра. Протоколы, основанные на идентификационной информации (identity-based). Атаки на протоколы идентификации. **Протоколы честного обмена секретами** Честный обмен секретами. Двусторонние и много-

		сторонние протоколы. Асинхронные протоколы честного обмена. Честный обмен с доверенной или с почти доверенной стороной. Протоколы без доверенной стороны. Одновременное подписание контракта. Применение протоколов честного обмена в платежных системах. Заказная электронная почта.
Раздел 3		
3.1	Тема 1. Интерактивные схемы доказательств. Протоколы электронного тайного голосования Понятие о протоколах электронных платежей. Вопросы стандартизации и патентования	**Интерактивные схемы доказательств** Интерактивные схемы доказательств с нулевым разглашением. Доказательство знания. Доказательство идентичности. Практические применения теории доказательств с нулевым разглашением. **Протоколы электронного тайного голосования .** Требования к идеальному протоколу. Использование схем подписи вслепую. Голосование с одной и двумя Центральными Избирательными Комиссиями (ЦИК). Использование Центрального Управления Регистрации (ЦУР). Голосование без ЦИК, схема Меррита (Merritt M.). Классификация протоколов голосования. Протоколы с перемешиванием и протоколы с разделением. Протоколы секретного многостороннего вычисления. **Понятие о протоколах электронных платежей** Общие требования к платежным системам. Неотслеживаемость. Анонимность. Централизованные и автономные системы. Схемы Шаума, Якоби, Брандса, Шнорра. Идентификация повторной траты “электронных денег”. Переводимые монеты. Примеры. Платежи в Интернет. Протоколы SSL, SET,3D Secure, SEPP, STT. Микроплатежи. Протокол iKP, DigiCash, PayCash и др. Платежные системы в мобильной коммерции.PayBox, GiSMo, и др. Классификация, характеристика и примеры протоколов электронной коммерции. Методы обеспечения честности и неотказуемости участников криптографического протокола. Методы конструирования и анализа робастных протоколов. Доказательность действий участников протокола. Безопасность протоколов электронных игр, лотерей, аукционов. **Вопросы стандартизации и патентования** Стандарты Интернет и RFCs. Политика различных организаций в области защиты информации.
3.2	Тема 2. Необходимые сведения из алгебры и теории чисел	Алгебраические структуры с одной и двумя бинарными операциями. Теория делимости в кольце целых чисел и многочленов. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Расширенный алгоритм Евклида. Теорема Чезаро. Простые числа. Попарно взаимно простые числа. Китайская теорема об остатках. Функция Эйлера и ее свойства. Теорема Эйлера-Ферма. Теорема Кармайкла. Псевдопростые числа. Вероятностные тесты на простоту целых чисел. Сведение сравнений n-ой степени по произвольному модулю к системе сравнений по попарно взаимно простым

		модулям, к сравнениям по примарному и простому модулю. Сравнения первой и второй степени. Символы Лежандра и Якоби. Критерий Эйлера. Метод Берлекемпа решения сравнений второй степени по простому модулю. Теорема эквивалентности Рабина. Основные факты об эллиптических кривых над полями. Эллиптические кривые и факторизация больших целых чисел. Дискретный логарифм на эллиптической кривой над полем.

Лабораторные занятия

№	Примерные темы лабораторных занятий
1.	Генератор паролей с заданными требованиями
2.	Генератор паролей и оценка стойкости полученных паролей по отношению к атакам методом прямого перебора
3.	Шифрование входного потока информации по заданному алгоритму с обязательным дешифрованием
4.	Стеганография: метод незначащих младших разрядов (Least Significant Bit). Использование контейнеров формата Bitmap

4.3 Перечень учебно-методического обеспечения для самостоятельной работы студентов

При изучении дисциплины используются следующие виды самостоятельной работы:

- самостоятельный поиск литературы по разделам и темам курса;
- изучение материала по дополнительным разделам дисциплины;
- изучение литературы и подготовка к выполнению лабораторных работ, курсовых работ;
- подготовка к тестированию, контрольным работам, написанию рефератов;
- подготовка к зачету, экзаменам.

  Форма контроля: отчет по лабораторным работам и их защита, защита курсовых работ.

Учебно-методические пособия:

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.

Рекомендуемый перечень тем самостоятельного углубленного изучения материала дисциплины:

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.

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
1	Тема 1.Введение. Понятие о шифрах	УКЕ-1, ПК-3	З-УКЕ-1;У-УКЕ-1;В-УКЕ-1 З-ПК-3;У-ПК-3;В-ПК-3	УО2,
	Тема 2. Блочные м поточные криптосистемы и их классификация. Криптографические свойства	УКЕ-1, ПК-3	З-УКЕ-1;У-УКЕ-1;В-УКЕ-1 З-ПК-3;У-ПК-3;В-ПК-3	Защита ЛР4
Рубежный контроль		УКЕ-1, ПК-3	З-УКЕ-1;У-УКЕ-1;В-УКЕ-1 З-ПК-3;У-ПК-3;В-ПК-3	СР11
2	Тема 1. Теория информации и криптография. Теория сложности вычислений и криптография.	УКЕ-1, ПК-3	З-УКЕ-1;У-УКЕ-1;В-УКЕ-1 З-ПК-3;У-ПК-3;В-ПК-3	УО6
	Тема 2.Основные понятия криптографии с открытым ключом. Цифровая подпись.	УКЕ-1, ПК-3	З-УКЕ-1;У-УКЕ-1;В-УКЕ-1 З-ПК-3;У-ПК-3;В-ПК-3	Защита ЛР8
	Тема 3. Разновидности протоколов электронной цифровой подписи. Функции хэширования. Управление ключами. Криптосистемы и протоколы на эллиптических кривых.	УКЕ-1, ПК-3	З-УКЕ-1;У-УКЕ-1;В-УКЕ-1 З-ПК-3;У-ПК-3;В-ПК-3	УО9
	Тема 4. Управление ключами. Разновидности протоколов электронной цифровой подписи. Протоколы идентификации и аутентификации. Протоколы честного обмена секретами	УКЕ-1, ПК-3	З-УКЕ-1;У-УКЕ-1;В-УКЕ-1 З-ПК-3;У-ПК-3;В-ПК-3	Защита ЛР10
3	Тема 1. Интерактивные схемы доказательств. Протоколы электронного тайного голосования Понятие о протоколах электронных платежей. Вопросы стандартизации и патентования	ПК-12.1, ПК-12.2	З-УКЕ-1;У-УКЕ-1;В-УКЕ-1 З-ПК-3;У-ПК-3;В-ПК-3	УО13

	Тема 2. Необходимые сведения из алгебры и теории чисел	ПК-12.1, ПК-12.2	З З-УКЕ-1;У-УКЕ-1;В-УКЕ-1 З-ПК-3;У-ПК-3;В-ПК-3	Защита ЛР15
Рубежный контроль		ПК-12.1, ПК-12.2	З-УКЕ-1;У-УКЕ-1;В-УКЕ-1 З-ПК-3;У-ПК-3;В-ПК-31	СР16
Промежуточная аттестация		ПК-12.1, ПК-12.2	З-УКЕ-1;У-УКЕ-1;В-УКЕ-1 З-ПК-3;У-ПК-3;В-ПК-3	**Зачет**

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. Оценочные средства для текущего контроля

5.2.1.1. Примерные вопросы для устного опроса (УО)

- Виды паролей и их надежность
- Атаки на пароли методом прямого перебора
- Нестандартные пароли
- Электронные ключи
- Надежность биометрических идентификаторов
- Простейшие криптоалгоритмы
- Комплексные СЗИ
- Правила и требования безопасности в организации и на предприятии

5.2.1.2. Примерные темы и вопросы для самостоятельной работы (СР)

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.

5.2.2. Оценочные средства для рубежного контроля

5.2.2.1. Примерные задания для решения задач по заданной теме

ЛР. №1 Генератор паролей с заданными требованиями
ЛР. №2 Генератор паролей и оценка стойкости полученных паролей по отношению к атакам методом прямого перебора
ЛР. №3 Шифрование входного потока информации по заданному алгоритму с обязательным дешифрованием
ЛР. №4 Стеганография: метод незначащих младших разрядов (Least Significant Bit). Использование контейнеров формата Bitmap

5.2.3. Оценочные средства для промежуточной аттестации

5.2.3.1. Примерные вопросы к зачету:

Вопросы к зачету:

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

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:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню осво-ению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>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.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td><td rowspan="2">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.</td></tr>
<tr><td>60-64</td><td>E</td></tr>
</table>

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 ДИСЦИПЛИНЫ

6.1. Рекомендуемая литература

Обязательная литература для преподавателей:

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.

25. Болотов А.А., Гашков С.Б., Фролов А.Б. Протоколы криптографии на эллиптических кривых: Элементарное введение в эллиптическую криптографию. 2006. - 280 с.

26. Handbook of elliptic and hyperelliptic curve cryptography, Taylor & Francis Group, Scientific editors Henri Cohen & Gerard Frey, 2006. – 808 стр.

27. Зубов А.Ю. Математика кодов аутентификации. – М.: Гелиос АРБ, 2007.- 480с.

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.

7. Сердюк В.А. Новое в защите от взлома корпоративных систем. М.: Техносфера, 2007.- 360 с.(2.1.1. Средства криптографической защиты информации, 66-70 стр.)

Список обязательной и дополнительной литературы для студентов.

Обязательная:

1. Русский перевод: Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.- М.: Триумф, 2002. – 816 с.

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

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

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

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

Дополнительная:

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

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

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

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

.

7. **МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Изучение дисциплины проводится в лабораториях кафедры «Вычислительная и информационная техника». Лабораторные работы проводятся с использованием ресурсов компьютерных классов, позволяющих работать в различных инструментальных средах.

Класс ПЭВМ не ниже Intel Pentium 4, 512M RAM, 40G HDD с установленным программным обеспечением: MS WindowsXP, MS Office Pro, Borland Delphi 7.0, Microsoft Visual Studio 6.0, интерпретатор PHP 5.0, интерпретатор PERL 5.0
Из расчета одна ПЭВМ на одного человека.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Дисциплина «Современные операционные системы» изучается на четвертом курсе (в седьмом семестре). Основными видами занятий при изучении дисциплины являются: лекции, лабораторные работы и самостоятельная работа студентов.

В соответствии с требованиями ОС ВО по направлению подготовки 09.03.01 «Информатика и вычислительная техника» реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках учебного курса студенты работают с лекциями, рекомендованной литературой, выполняют лабораторные работы, готовятся к экзамену и зачету. В процессе подготовки студенты используют программные продукты, инструментальные среды, информационно-справочные системы, информационные источники, размещенные в сети Интернет (официальные сайты, веб-порталы, тематические форумы и телекоммуникации), электронные учебники и учебно-методические пособия.

9. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ СТУДЕНТАМ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Предлагается

- Самостоятельно прорабатывать лекционный материал для более полного усвоения материала;
- В учебном процессе при выполнении лабораторного практикума эффективно использовать методические пособия и методический материал по темам лабораторных работ;
- 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.

Программа составлена в соответствии с требованиями ОС ВО НИЯУ МИФИ к обязательному минимуму содержания основной образовательной программы по направлению подготовки 09.03.01 Информатика и вычислительная техника.

Автор(ы) _____ М.Д.Романова

Рецензенты _____ Д.Б.Николаев

Согласовано:

Зав. кафедрой ВИТ _____ В.С.Холушкин

Руководитель ОП _____ В.С.Холушкин