

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  
**Национальный исследовательский ядерный университет «МИФИ»  
(НИЯУ МИФИ)**

УТВЕРЖДАЮ  
Проректор НИЯУ МИФИ  
\_\_\_\_\_ В.В. Ужва

СОГЛАСОВАНО  
Председатель Совета по подготовке  
научно-педагогических кадров  
\_\_\_\_\_ Н.А. Кудряшов

Ответственный секретарь  
приемной комиссии  
\_\_\_\_\_ В.И. Скрытный

**Программа вступительного испытания**  
по направлению подготовки научно-педагогических кадров  
в аспирантуре

**10.06.01 «Информационная безопасность»**

Форма обучения  
очная, заочная

**Москва, 2016**

Программа вступительного испытания сформирована на основе федеральных государственных образовательных стандартов высшего образования.

**Форма проведения испытания:**

Вступительное испытание по направлению подготовки аспирантов «Информационная безопасность» проводится в виде собеседования с обязательным оформлением ответов на вопросы билета в письменном виде. Собеседование проводится с целью выявления у абитуриента объема научных знаний, научно-исследовательских компетенций, навыков системного и критического мышления, необходимых для обучения в аспирантуре. Абитуриент должен показать профессиональное владение теорией и практикой в предметной области, продемонстрировать умение вести научную дискуссию.

**Структура испытания:**

Испытание состоит из ответов на вопросы билета и дополнительные вопросы в рамках программы вступительного испытания.

**Критерии оценки результатов испытания:**

Оценка «отлично» ставится при следующем условии:

даны исчерпывающие и обоснованные ответы на вопросы, поставленные экзаменационной комиссией;

Оценка «хорошо» ставится при следующих условиях:

1. даны полные, достаточно глубокие и обоснованные ответы на вопросы, поставленные экзаменационной комиссией;
2. ответы на вопросы даются полно, но логическая последовательность не всегда соблюдается.

Оценка «удовлетворительно» ставится при следующих условиях:

1. даны в основном правильные ответы на вопросы, поставленные экзаменационной комиссией;
2. ответы на вопросы даются в основном полно, но при слабом логическом оформлении высказываний.

Оценка «неудовлетворительно» ставится в случае, когда не выполнены условия, позволяющие поставить оценку «удовлетворительно».

Решения экзаменационной комиссии принимаются большинством голосов.

**Вопросы для подготовки к вступительному испытанию  
Направление 10.06.01 «Информационная безопасность»**

**Профиль (направленность): 05.13.19 Методы и системы защиты информации, информационная безопасность**

1. НАУЧНО-ПРАКТИЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
  - 1.1. Понятие национальной безопасности; виды безопасности; информационная безопасность в системе национальной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации. Органы государственной власти, регулирующие деятельность в области обеспечения информационной безопасности.
  - 1.2. Основные термины и определения в области информационной безопасности. Информационная безопасность и защита информации. Понятие угрозы безопасности информации. Основные аспекты информационной безопасности: конфиденциальность, целостность, доступность. Классификация угроз конфиденциальности, целостности и доступности информации; классификация источников угроз. Модели оценки ущерба от реализации угроз информационной безопасности.
  - 1.3. Понятие уязвимости в информационной безопасности. Базы уязвимостей. Классификация каналов утечки и искажения информации.
  - 1.4. Классификация и краткая характеристика методов и средств защиты информации. Защита объектов информатизации.
  - 1.5. Организационная структура международной системы стандартизации. Стандарты де-юре и де-факто. Организации, разрабатывающие стандарты. Основные международные стандарты в области информационной безопасности и защиты информации.
  - 1.6. Структура нормативной правовой базы Российской Федерации в области обеспечения информационной безопасности. Деятельность государственных органов РФ, контролирующей деятельность в области информационной безопасности, их роль в формировании и актуализации государственной системы защиты информации в РФ.
  - 1.7. Государственная система технического регулирования и стандартизации в Российской Федерации. Основные нормативно-технические документы Российской Федерации в области обеспечения информационной безопасности.
  - 1.8. Система сертификации средств защиты информации по требованиям безопасности информации. Органы сертификации. Испытательные лаборатории (центры).
  - 1.9. Лицензирование деятельности в области защиты информации в Российской Федерации.
  - 1.10. Управление информационной безопасностью. Процессный подход. Понятие системы управления информационной безопасностью (СУИБ). Стандарты серии ISO 27000. Понятие риска информационной безопасности. Анализ рисков. Основные процессы СУИБ. Документирование СУИБ.
  - 1.11. Обеспечение информационной безопасности информационных систем. Политика безопасности. Структура документов, разрабатываемых для документирования требований политики безопасности к информационным системам. Событие и инцидент информационной безопасности. Управление инцидентами информационной безопасности.

- 1.12. Аудит информационной безопасности организаций. Внешний и внутренний аудит. Стандарты аудита. Программа аудита. Методы и инструментальные средства проведения аудита информационной безопасности.
- 1.13. Оценка защищенности продуктов и систем информационных технологий. Стандарт ISO/IEC 15408 – «Общие критерии». Функциональные требования и требования доверия к безопасности.
- 1.14. Аттестация объектов информатизации по требованиям безопасности информации: аттестация автоматизированных систем, средств связи, обработки и передачи информации; аттестация помещений; аттестация технических средств, установленных в выделенных помещениях.
- 1.15. Контроль защищенности информации ограниченного доступа: выявление технических каналов утечки информации и способов несанкционированного доступа к ней; контроль эффективности применяемых средств защиты информации.
- 1.16. Технические каналы утечки информации. Защита информации от утечки по техническим каналам. Специальные исследования технических средств на наличие технических каналов утечки информации.
- 1.17. Основные вехи истории возникновения и развития защиты информации как самостоятельной отрасли человеческой деятельности. Этапы формирования современных научно-практических основ защиты информации.

## 2. ОСНОВЫ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

### 2.1. Информатика и информационные технологии

- 2.1.1. Классификация и краткая характеристика типов современной компьютерной техники. Архитектура и структура современной компьютерной техники.
- 2.1.2. Элементная база современной компьютерной техники. Микропроцессоры. Понятие микропроцессорной системы. Обобщённая структура микропроцессорной системы. Системная магистраль. Организация и структура памяти, системы прерывания; системы ввода-вывода; периферийные устройства.
- 2.1.3. Классификация систем хранения данных: локальные дисковые накопители, RAID-массивы, сети хранения данных (SAN), ленточные библиотеки. Модели управления хранением данных. Международные стандарты в области хранения данных.
- 2.1.4. Программное обеспечение современной компьютерной техники. Системное и прикладное программное обеспечение (ПО). Основные семейства операционных систем: UNIX-подобные (AIX, Solaris, FreeBSD, Linux, Android, MAC OS X и пр.), Windows, OS X. Специализированные операционные системы. ПО с открытым исходным кодом и проприетарное ПО.
- 2.1.5. Типология системного ПО: СУБД, мониторы виртуальных машин, ПО среднего слоя (middleware) и др. Типология прикладного ПО: CRM, CMS, CAD и др.
- 2.1.6. Концепция виртуализации вычислительных средств. Понятие монитора виртуальных машин. Облачные среды. Сервисы, предоставляемые облачными провайдерами для пользователей. Интерфейсы прикладного программирования (API) облачных сервисов для разработчиков прикладного ПО
- 2.1.7. Понятие открытой информационной системы. Предпосылки возникновения концепции открытых систем. Классификация информационных систем по назначению и сфере применения. Исторические пути развития вычислительной техники, операционных систем, прикладного ПО, интернета, распределенных систем. Проблемы обеспечения совместимости информационных систем. Требования к совместимости систем. Переносимость и способность к

- взаимодействию. Модели открытых систем. Системный подход к описанию функциональности.
- 2.1.8. Коммуникационные архитектуры. Системообразующие стандарты: модель ISO/OSI, профили взаимосвязи открытых систем ISO/IEC 10000, другие системообразующие стандарты ISO и ITU, модель POSIX/OSE, модель TCP/IP. Модели распределенных вычислений; «клиент-сервер» и др.
  - 2.1.9. Языки программирования. Процедурное, объектно-ориентированное и функциональное программирование. Краткая характеристика основных языков программирования: C, C++, C#, Java, Python и др. Интегрированные среды разработки системного и прикладного ПО.
  - 2.1.10. Веб-сервисы. Веб-разработка. Архитектуры ПО на стороне сервера и на стороне клиента. Средства веб-разработки. Технические аспекты веб-разработки: хостинг сайтов, поддержка доменных имен. Системы управления контентом.
  - 2.1.11. Инфраструктура безопасности открытых систем. Архитектура безопасности ISO/OSI. Стандарты ISO/IEC по защите информации. Концепция инфраструктуры управления ключами (PKI и KMI).
- 2.2. Алгоритмы и структуры данных. Теория алгоритмов. Анализ данных и машинное обучение
- 2.2.1. Структуры данных и абстракции данных; элементарные и простые структуры данных: стеки и очереди, связные списки, деревья и пр.
  - 2.2.2. Сложные структуры данных: деревья, В-деревья, леса и пр.
  - 2.2.3. Хеширование и хеш-таблицы. Распределенные хеш-таблицы.
  - 2.2.4. Оценка сложности алгоритмов. Классификация задач по сложности. Труднорешаемые задачи.
  - 2.2.5. Алгоритмы сортировки. Поиск максимального и минимального элементов массива. Оценки сложности алгоритмов сортировки.
  - 2.2.6. Алгоритмы поиска. Поиск подстрок. Обработка поисковых запросов. Построение индекса.
  - 2.2.7. Алгоритмы на графах: поиск на графах, построение минимального остовного дерева, поиск кратчайших путей, задача о максимальном потоке.
  - 2.2.8. Генерация случайных и псевдослучайных двоичных последовательностей. Наиболее распространенные конструкции псевдослучайных генераторов.
  - 2.2.9. Матричные алгоритмы. Алгоритмы решения систем линейных алгебраических уравнений.
  - 2.2.10. Алгоритмы оптимизации. Поиск локального минимума функции. Линейное программирование.
  - 2.2.11. Представление полиномов. Быстрое преобразование Фурье.
  - 2.2.12. Теоретико-числовые алгоритмы. Модульная арифметика. Решение модульных линейных уравнений.
  - 2.2.13. Приближенные алгоритмы. Задача о коммивояжере. Задача о покрывании множества.
  - 2.2.14. Параллельная обработка данных. Параллельные алгоритмы: примеры, оценки их сложности. Поддержка параллельного программирования в языках программирования.
  - 2.2.15. Элементарная статистическая обработка данных: гистограмма, среднее значение, дисперсия, среднееквадратическое отклонение.
  - 2.2.16. Построение линейной регрессии по выборочным данным. Расчёт выборочного коэффициента корреляции.
  - 2.2.17. Классификация задач анализа данных. Deskриптивные и предиктивные модели. Этапы анализа данных: предварительный анализ данных, построение модели,

- визуализация результатов и др. Основная терминология в области анализа данных: объекты, признаки, типы данных, типы признаков.
- 2.2.18. Понятие машинного обучения. Этапы обучения и построения модели. Типы задач, решаемых с помощью машинного обучения. Понятие нейронной сети.
  - 2.2.19. Задача поиска ассоциативных правил. Алгоритмы Apriori и FP-Growth.
  - 2.2.20. Задачи классификации. Построение решающих деревьев. Байесовская классификация. Метрические методы классификации.
  - 2.2.21. Задачи кластеризации. Метод k средних.
  - 2.2.22. Задачи поиска аномалий (outlier detection).
- 2.3. Компьютерные сети
- 2.3.1. Основные сетевые понятия и определения. Основные сетевые стандарты и стандартизирующие организации. Задача распределенной обработки данных. Области применения.
  - 2.3.2. Различные типы сетей. LAN и WAN сети. Классификация и сравнительная характеристика различных типов сетей. Основные модели взаимодействия открытых систем: модель OSI и модель TCP/IP.
  - 2.3.3. Локальные вычислительные сети: архитектура, топология, общие подходы к проектированию и построению. Передача данных на различных уровнях модели OSI. Технологии пакетной коммутации. Технологии построения локальных сетей на основе общей шины доступа. Технология Ethernet. Стандарты Ethernet. Требования к физической среде передачи данных технологии Ethernet. Безопасность технологии и принципы построения локальных сетей на ее основе.
  - 2.3.4. Оборудование локальных сетей: концентраторы (hub), мосты (bridge), коммутаторы (switch). Коммутация пакетов в локальных сетях. Бриджинг и свитчинг: сходства и различия двух понятий.
  - 2.3.5. Резервирование на канальном уровне. Алгоритм STA. Формулировка задачи. Протокол построения покрывающего дерева STP. Особенности реализации.
  - 2.3.6. Построение безопасных доменов на канальном уровне. Технология VLAN: основные понятия, принципы использования и области применения. Различные типы VLAN-ов. Технологии MLT, SMLT, IST. Транковые соединения, стандарт 802.1q/p. Обеспечения надежности и проблемы безопасности.
  - 2.3.7. Маршрутизируемые протоколы. Понятие маршрутизации пакетов сетевого уровня. Протоколы сетевого уровня модели OSI (TCP/IP). Опции IP (IP source routing, time stamps, security). Протокол IPX. Протокол SPX.
  - 2.3.8. Транспортные протоколы. Протокол TCP, механизмы управления и контроля потока. Протокол UDP.
  - 2.3.9. Глобальные вычислительные сети. Основы организации и функционирования, принципы построения. Протокол ICMP.
  - 2.3.10. Современные архитектуры WAN сетей. Понятие плоских и иерархических сетей. Структура сети Internet. Автономные системы и области. Понятие динамической и статической маршрутизации. Понятие IGP и EGP протоколов маршрутизации. Дистанционно-векторные протоколы и протоколы состояния связей.
  - 2.3.11. Протоколы динамической маршрутизации. Протокол RIP. Механизмы предотвращения петель маршрутизации (poisoned reverse, split horizon, hop-count limit), сравнение RIP и IGRP. Алгоритм SPF. Протокол OSPF, механизм установки соединения. Безопасность протокола.
  - 2.3.12. Протоколы маршрутизации в Интернет. Протоколы EGP. Протокол BGPv4. IBGP и EBGP. Атрибуты BGP, механизм принятия решения. Протоколы EGP. Конфедерации BGP, отражатели маршрутов (route reflectors), кластеры. Damping & flapping, балансировка нагрузки, multihop и multilink (multipath) соединения. BGP.

- 2.3.13. Технологии свитчинга. Технологии “tag switching” на примере технологии MPLS. Коммутация третьего уровня, принципы работы, используемые протоколы, преимущества и недостатки, проблемы безопасности.
- 2.3.14. Базовые прикладные сервисы вычислительных сетей. Протоколы идентификации (ARP (RARP), BOOTP, ICMP, DHCP, WINS, DNS). Принцип действия, спецификация, базовые команды, коды возврата. Особенности применения. Проблемы безопасности.
- 2.3.15. Протоколы прикладного уровня: прием/передача почтовых сообщений (SMTP, POP3, IMAP). Принцип действия, спецификация, базовые команды, коды возврата. Особенности применения. Проблемы безопасности.
- 2.3.16. Протоколы прикладного уровня: протоколы передачи данных (FTP, TFTP, SSH). Принцип действия, спецификация версий, базовые команды, коды возврата. Особенности применения. Проблемы безопасности.
- 2.3.17. Протоколы прикладного уровня: протокол обмена гипертекстовой информацией (HTTP). Принцип действия, спецификация версий, базовые команды, методы передачи, коды возврата. Особенности применения. Проблемы безопасности.
- 2.3.18. Протоколы прикладного уровня: протоколы управления (SNMP), TELNET. Принцип действия, спецификация версий, базовые команды, коды возврата. Особенности применения. Проблемы безопасности.
- 2.3.19. Сервисные протоколы LAN: NETBIOS/SMB, NTP, LDAP, NFS, NIS, RPC. Принцип действия, спецификация версий, базовые команды, коды возврата. Особенности применения. Проблемы безопасности.
- 2.3.20. Основы сетевого программирования. Стандарты программирования: «Sockets» и «XTIs». Основы построения клиент-серверных приложений с использованием Sockets и XTIs. Интерфейсы прикладного сетевого программирования. Блокируемая и неблокируемая модели, «ленивые сокет».
- 2.3.21. Межсетевые экраны. Типы межсетевых экранов. Выбор и адаптация межсетевых экранов к практическим задачам. Внутренняя архитектура межсетевых экранов, пакетные фильтры, шлюзы уровня сеанса, посредники прикладного уровня, инспекторы состояний.
- 2.3.22. Схемы применения и работы различных типов межсетевых экранов. Системы анализа сетевой защиты. Различные варианты и уровни сетевого анализа. Сравнительные характеристики, достоинства и недостатки.
- 2.3.23. Системы контроля содержания сетевого трафика. Схемы применения и работы. Обманные сетевые системы («Honeypot»). Возможности, сравнительные характеристики, достоинства и недостатки.
- 2.3.24. Подходы к проектированию и построению распределенных информационных систем. «Вертикальная» и «горизонтальная» сетевые инфраструктуры, «последняя миля». Архитектура системы защиты локальной сети, основные методы и средства ее реализации. Сетевая безопасность распределенных корпоративных систем.
- 2.3.25. Подходы к проектированию WAN-сетей. Методы обеспечения надежности и резервирования. Подходы к обеспечению сетевой безопасности распределенных систем.
- 2.3.26. Виртуальные сети, классификация, схемы и методы построения (VLAN, MPLS VPN). Возможности, сравнительные характеристики, достоинства и недостатки различных подходов.

## 2.4. Базы данных

- 2.4.1. Общие принципы построения баз данных (БД): реляционные и нереляционные БД. Общая характеристика, назначение и возможности систем управления базами данных (СУБД).

- 2.4.2. Реляционные СУБД. Реляционная алгебра. Нормальные формы. Язык манипулирования данными SQL. Первичные и внешние ключи в таблицах реляционной БД.
- 2.4.3. Обработка транзакций в реальном масштабе времени (OLTP) и оперативная аналитическая обработка данных (OLAP). Краткая характеристика программных средств поддержки OLTP и OLAP.
- 2.4.4. Нереляционные СУБД (технология NoSQL): модель «ключ – значение», документ-ориентированные, графовые СУБД. Запросы к нереляционным СУБД.
- 2.4.5. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных.
- 2.4.6. Оптимизация производительности и характеристик доступа к базам данных.
- 2.4.7. Большие данные (big data). Характерные черты больших данных. Программные средства обработки больших данных. Модель MapReduce.

## 2.5. Системы передачи данных

- 2.5.1. Информация, данные, сигналы. Источники информации и ее носители. Количество информации и энтропия. Формулы Хартли и Шеннона.
- 2.5.2. Характеристики процесса передачи информации. Математические модели каналов связи и их классификация.
- 2.5.3. Помехоустойчивость передачи информации. Пропускная способность каналов связи. Теорема Шеннона для каналов без помех и с ними.
- 2.5.4. Типы сигналов, их дискретизация и восстановление. Спектральная плотность сигналов. Частота Найквиста, теорема Котельникова.
- 2.5.5. Частотное представление дискретных сигналов. Ортогональные преобразования дискретных сигналов. Задачи интерполяции и прореживания сигналов.
- 2.5.6. Классификация кодов. Линейные коды. Оптимальное кодирование.
- 2.5.7. Геометрический подход к кодированию. Неравномерные коды Хемминга.
- 2.5.8. Циклические коды. Помехоустойчивое кодирование. Корректирующие коды.
- 2.5.9. Аналого-цифровые и цифро-аналоговые преобразователи; быстрые преобразования. Цифровые фильтры.
- 2.5.10. Нелинейное и параметрическое преобразование сигналов; модуляция и демодуляция; преобразование частоты.
- 2.5.11. Классификация систем связи; кодирование информации в системах связи.
- 2.5.12. Методы модуляции в системах связи; основные типы модемов; уплотнение информации в системах связи; дискретные вокодеры.
- 2.5.13. Особенности цифровых систем многоканальных передач сообщений: способы объединения цифровых потоков; особенности передачи дискретных сообщений по цифровым каналам.
- 2.5.14. Системы телефонной связи; цифровая телефония.
- 2.5.15. Коротковолновые и ультракоротковолновые системы связи; радиорелейные системы связи; телевизионные системы; спутниковые системы связи; волоконно-оптические системы связи.
- 2.5.16. Маршрутизация и управление потоками в сетях связи; сети интегрального обслуживания.

## 3. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

### 3.1. Основы криптографии

- 3.1.1. Классическая криптография. Шифры замены и шифры перестановки. Шифры полиалфавитной замены.



- 3.1.2. Определение поточного шифра. Требования к стойкости поточного шифра. Конструкции поточных шифров. Синхронные и самосинхронизирующиеся поточные шифры. Групповые шифры гаммирования, шифры модульного гаммирования. Шифр Вернама. Одноразовый блокнот. Примеры. Применение поточных шифров. Слабые ключи поточных шифров.
- 3.1.3. Генераторы случайных и псевдослучайных чисел. Основные принципы построения. Равномерно распределенные случайные последовательности, псевдослучайные последовательности. Требования к управляющей гамме генератора псевдослучайных чисел: длина периода, линейная сложность и т.д.
- 3.1.4. Конструкции криптографических генераторов случайных и псевдослучайных двоичных последовательностей: фильтрующие и комбинирующие генераторы, схемы с внешним управлением, схемы с самоуправлением, генераторы с дополнительной памятью. Примеры.
- 3.1.5. Критерии оценки качества криптографических генераторов. Постулаты Голомба, пакет статистических тестов NIST. Критерий хи-квадрат.
- 3.1.6. Симметричные блочные шифры. Принципы построения подстановки итеративного симметричного блочного шифра. Конструкции блочных шифров: шифры, основанные на схеме Фейстеля, SP-сети. Примеры.
- 3.1.7. Алгоритмы блочного шифрования AES, DES, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015 Слабые ключи итеративных симметричных блочных шифров.
- 3.1.8. Режимы шифрования: простая замена, сцепление блоков шифртекста, гаммирование с обратной связью по шифртексту, гаммирование с внутренней обратной связью.
- 3.1.9. Симметричные схемы аутентификации сообщений на основе блочных шифров. Криптографические хэш-функции (бесключевые).
- 3.1.10. Симметричные схемы аутентификации сообщений на основе криптографических хэш-функций.
- 3.1.11. Симметричные схемы аутентичного шифрования.
- 3.1.12. Симметричные схемы шифрования с расширенными свойствами и с дополнительной функциональностью.
- 3.1.13. Вычислительно сложные задачи, используемые в асимметричной криптографии. Арифметические алгоритмы, используемые в асимметричной криптографии. Генерация параметров и ключей асимметричных криптосхем.
- 3.1.14. Открытое распределение ключей. Протокол Диффи-Хеллмана.
- 3.1.15. Определение схемы открытого шифрования. Стойкость схем открытого шифрования. Сравнительная оценка симметричных шифров и схем открытого шифрования.
- 3.1.16. Схемы открытого шифрования на основе однонаправленной функции с потайной дверью (схемы RSA, Рабина и др.).
- 3.1.17. Схемы открытого шифрования на основе дискретного логарифмирования (схема Эль-Гамала и др.).
- 3.1.18. Определение схемы электронной подписи. Стойкость схем электронной подписи. Сравнительная оценка симметричных и асимметричных методов аутентификации сообщений.
- 3.1.19. Схемы электронной подписи на основе задачи RSA.
- 3.1.20. Схемы электронной подписи на основе задачи дискретного логарифмирования.
- 3.1.21. Математические основы криптографии на эллиптических кривых. Асимметричные криптосхемы на основе математического аппарата эллиптических кривых.
- 3.1.22. Асимметричные криптосхемы на основе математического аппарата билинейных спариваний. Схема открытого распределения ключей Joux. Схема шифрования Boneh- Franklin.

- 3.1.23. Гомоморфные схемы шифрования. Полностью гомоморфное шифрование. Частично гомоморфное шифрование. Схема открытого шифрования Paillier. Возможности применения гомоморфного шифрования в криптографии.
  - 3.1.24. Основные принципы конструирования и анализа криптографических протоколов. Основные понятия и определения. Свойства протоколов. Классификация нарушителей. Типичные атаки. Принципы доказательной криптографии (provable security).
  - 3.1.25. Вероятностные доказательства. Интерактивные доказательства. Доказательства с нулевым разглашением (zero-knowledge proofs). Примеры.
  - 3.1.26. Протоколы аутентификации. Базовые конструкции протоколов аутентификации. Аутентификация по паролю (списки паролей, протокол Лампорта). Аутентификация «запрос – ответ» (ISO/IEC 9798). Принцип аутентификации, основанный на нулевом разглашении (протоколы Фиата – Шамира, Файге – Фиата – Шамира).
  - 3.1.27. Протоколы распределения ключей. Основные понятия и определения. Свойства протоколов распределения ключей. Защищенная конференц-связь.
  - 3.1.28. Протоколы распределения ключей, основанные на симметричных криптографических методах (двухраундовые и трёхраундовые протоколы, ЗРКД, Needham – Schroeder, Otway – Rees, Kerberos).
  - 3.1.29. Протоколы распределения ключей, основанные на асимметричных криптографических методах. Транспортировка ключей (Needham – Schroeder, X.509, Beller – Yacobi). Обмен ключами (Diffie – Hellman, MTI, STS).
  - 3.1.30. Защищенные каналы передачи данных. Способы и средства установления защищенных соединений.
  - 3.1.31. Спецификация SSH.
  - 3.1.32. Спецификация SSL/TLS.
  - 3.1.33. Спецификация IPSec.
  - 3.1.34. Схемы разделения секрета. Пороговые схемы разделения секрета. Схема Шамира. Схемы проверяемого разделения секрета Фельдмана и Педерсена. Принцип пороговой криптографии.
  - 3.1.35. Криптография в недоверенных средах. Обзор задач: обеспечение стойкости к утрате части носителей данных, доказательство обладания данными (proof-of-possession), верификация вычислений, гомоморфное шифрование. Пример –
- 3.2. Основы защиты информации от утечки по техническим каналам и физическая защита
    - 3.2.1. Виды, источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники.
    - 3.2.2. Побочные электромагнитные излучения и наводки; структура, классификация и основные характеристики технических каналов утечки информации; классификация технической разведки; основные этапы и процедуры добывания информации технической разведкой; возможности видов технической разведки.
    - 3.2.3. Методы и средства инженерной защиты и технической охраны объектов; скрытие объектов наблюдения.
    - 3.2.4. Скрытие речевой информации в каналах связи; энергетическое скрытие акустических информативных сигналов; обнаружение и локализация закладных устройств, подавление их сигналов; подавление опасных сигналов акустоэлектрических преобразователей.
    - 3.2.5. Экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания; подавление опасных сигналов.

- 3.2.6. Основные положения методологии инженерно-технической защиты информации. Виды контроля эффективности защиты информации, методы расчета и инструментального контроля показателей защиты информации.
- 3.2.7. Средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа.
- 3.2.8. Основные методы и средства защиты информации от утечки по техническим каналам.
- 3.2.9. Основные методы и средства инженерной защиты и технической охраны объектов.

### 3.3. Программно-аппаратные методы защиты от НСД

- 3.3.1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности, концепция монитора доступа.
- 3.3.2. Методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации.
- 3.3.3. Защита программ от изучения, способы встраивания средств защиты в программное обеспечение.
- 3.3.4. Защита от вредоносного программного обеспечения, защита программ от изменения и контроль целостности, построение изолированной программной среды.
- 3.3.5. Организация управления доступом и защиты ресурсов ОС; основные механизмы безопасности: средства и методы аутентификации пользователей.
- 3.3.6. Краткая характеристика моделей разграничения доступа: дискреционной, мандатной, ролевой, атрибутной.
- 3.3.7. Модели нарушителей и угроз информационной безопасности. Сетевые атаки. Классификация типовых удаленных атак на информационные системы.
- 3.3.8. Классификация и краткая характеристика средств обеспечения информационной безопасности в компьютерных сетях. Системы анализа защищенности. Организация и использование средств доказательной регистрации событий (аудита).
- 3.3.9. Межсетевые экраны. Фильтрация трафика. Системы обнаружения и предотвращения вторжений (IDS/IPS). SIEM-системы.
- 3.3.10. Аналитические системы безопасности. Использование аналитики больших данных для реализации аппаратно-программных средств обеспечения информационной безопасности: обнаружение ботнетов, активная аутентификация, обнаружение вторжений, обнаружение фишинга, мониторинг транзакций и др.
- 3.3.11. Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС; основные стандарты ОС.
- 3.3.12. Средства обеспечения безопасности баз данных: средства идентификации и аутентификации объектов баз данных, языковые средства разграничения доступа, концепция и реализация механизма ролей.
- 3.3.13. Средства контроля целостности информации в СУБД, организация взаимодействия СУБД и базовой ОС, журнализация, средства создания резервных копии и восстановления баз данных. Задачи и средства администратора безопасности баз данных.

## 4. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

- 4.1. Законодательство РФ в области информационной безопасности, защита государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации.
- 4.2. Понятие и виды защищаемой информации по законодательству РФ; государственная тайна как особый вид защищаемой информации; конфиденциальная информация.
- 4.3. Система защиты государственной тайны; правовой режим защиты государственной тайны; правовое регулирование взаимоотношений администрации и персонала в области защиты информации; правовые режимы конфиденциальной информации.
- 4.4. Лицензирование и сертификация в области защиты информации, в том числе государственной тайны. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
- 4.5. Правовые основы защиты информации от утечки по техническим каналам.
- 4.6. Основные нормативные правовые акты Российской Федерации, посвященные вопросам защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.
- 4.7. Правовые основы обеспечения безопасности информации в ключевых системах информационной инфраструктуры. Правовые основы обеспечения безопасности информационных систем общего пользования и информационных систем, входящих в единую систему межведомственного электронного взаимодействия.
- 4.8. Нормативные правовые акты Российской Федерации, регламентирующие обеспечение безопасности персональных данных в Российской Федерации: Федеральные законы, постановления Правительства РФ, документы ФСТЭК России, документы ФСБ России.
- 4.9. Нормативное правовое и нормативно-техническое регулирование обеспечения безопасности криптографическими методами в Российской Федерации. Государственные стандарты РФ, регламентирующие обеспечение безопасности информации криптографическими методами. Государственное регулирование разработки и применения средств криптографической защиты информации (СКЗИ) в Российской Федерации. Основные положения документов, определяющих особенности применения СКЗИ для защиты персональных данных. Функции Центра по лицензированию, сертификации и защите государственной тайны ФСБ России.
- 4.10. Нормативное правовое и нормативно-техническое регулирование использования электронной подписи для обеспечения безопасности электронного документооборота в РФ, создания удостоверяющих центров. Закон РФ «Об электронной подписи».
- 4.11. Правовые основы деятельности по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Функции Федеральной службы по финансовому мониторингу РФ.
- 4.12. Правовые основы защиты интеллектуальной собственности в Российской Федерации.
- 4.13. Преступления в сфере компьютерной информации; экспертиза преступлений в области компьютерной информации; криминалистические аспекты проведения расследований.
- 4.14. Организация защиты объектов информатизации. Цели и задачи службы безопасности объекта информации. Организация и обеспечение ограничения доступа, пропускного и внутриобъектового режима, физическая защита, защита информации при авариях, экстремальных ситуациях и в условиях чрезвычайного положения.

- 4.15. Понятие секретного (конфиденциального) делопроизводства. Общие принципы его организации. Механизм и процедуры установления степени секретности (конфиденциальности). Правила оформления документов с ограниченным доступом. Правила и формы регистрации документов. Обеспечение сохранности документов с ограниченным доступом. Организация хранения. Требования к помещениям и хранилищам. Правила и порядок уничтожения документов с ограниченным доступом. Контроль и методы проверки состояния делопроизводства с ограниченным доступом. Порядок проведения служебных расследований случаев нарушения порядка специального делопроизводства.
- 4.16. Кадровое обеспечение информационной безопасности. Методы и средства подбора и расстановки кадров. Особенности взаимодействия служб безопасности с персоналом предприятия. Система обеспечения психологической устойчивости к криминальным воздействиям. Методы психофизиологического тестирования.

#### ЛИТЕРАТУРА ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

По разделу 1:

1. Конституция Российской Федерации. – М. : Маркетинг, 2001. – 39 с.
2. Федеральный закон РФ от 28.12.2010 № 390-ФЗ «О безопасности» (принят Государственной Думой 07.12.2010 и одобрен Советом Федерации 15.12.2010).
3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. «Доктрина информационной безопасности Российской Федерации» (утверждена Президентом РФ 9 сентября 2000 г. № Пр-1895).
5. «Стратегия развития информационного общества в Российской Федерации» (утверждена Президентом Российской Федерации 07.02.2008 № Пр-212).
6. «Стратегия национальной безопасности Российской Федерации до 2020 года» (утверждена Указом Президента РФ от 12 мая 2009 г. № 537).
7. Федеральный закон «О техническом регулировании» от 27.12.2002 № 184-ФЗ (принят Государственной Думой 15.12.2002).
8. Малюк А.А. [и др.] Введение в информационную безопасность. – М.: «Горячая линия – Телеком», 2011. – 290 с.
9. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2004. – 280 с.
10. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001. – 148 с.
11. Горбатов В.С. Основы технологии РКІ / В.С. Горбатов, О.Ю. Полянская. – М.: Горячая линия – Телеком, 2004. – 248 с.

По разделу 2:

12. Кудряшов Б.Д, Теория информации. Учебник для вузов. – СПб.: Питер, 2009. – 320 с.
13. Запечников С.В. Стандартизация информационных технологий в аспекте защиты информации в открытых системах. – Москва : МИФИ, 2000. – 135 с.
14. Скляр Б. Цифровая связь. Теоретические основы и практическое применение: 2-е изд. – М.: ООО «И.Д. Вильямс», 2016. – 1104 с.
15. Кормен Т. [и др.] Алгоритмы: построение и анализ. 3-е изд.: пер. с англ. – М.: ООО «И.Д. Вильямс», 2013. – 1328 с.

16. Маннинг Д. [и др.] Введение в информационный поиск: пер. с англ. – М.: ООО «И.Д. Вильямс», 2011. – 528 с.
17. Барсегян А.А. [и др.] Анализ данных и процессов: учебное пособие: 3-е изд. – СПб.: БХВ-Петербург, 2009. – 512 с.
18. Олифер В.Г. Компьютерные сети. Олифер В.Г., Олифер Н.А. – СПб.: Питер, 2013. – 672 с.
19. Таненбаум Э. Компьютерные сети / пер. А. Гребенькова. Таненбаум Э., Уэзеролл Д. – СПб.: Питер, 2013. – 960 с.
20. Дейт, К. Дж. Введение в системы баз данных. 8-е изд.: пер. с англ. – М.: Издательский дом «Вильямс», 2008. – 1328 с.

По разделу 3:

21. Фомичев В.М. Методы дискретной математики в криптологии. Учебное пособие для вузов. – Москва : Диалог-МИФИ, 2010. – 424 с.
22. Алферов А.П. Основы криптографии. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Учебное пособие. – Москва : Гелиос АРВ, 2005. – 480 с.
23. Логачев О.А. Булевы функции в теории кодирования и криптологии. Логачев О.А., Сальников А.А., Смышляев С.В., Яценко В.В. – Москва : URSS, 2015. – 576 с.
24. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – Москва : Стандартинформ, 2015. – 21 с.
25. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – Москва: Стандартинформ, 2015. – 42 с.
26. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – Москва : Стандартинформ, 2012. – 29 с.
27. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.– Москва : Стандартинформ, 2012. – 34 с.
28. Мао В. Современная криптография: теория и практика.– Москва: Издательский дом Вильямс, 2005. – 768 стр.
29. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Москва: Триумф, 2002. – 816 с.
30. Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – Москва: Мир, 2006. – 471 с.
31. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. Учебное пособие для студентов вузов. – Москва: Горячая линия – Телеком, 2007. – 320 с.
32. Запечников С.В. Криптографические методы защиты информации. Учебное пособие. Запечников С.В., Казарин О.В., Тарасов А.А. – Москва: Юрайт Москва, 2015. – 309 с.
33. Информационная безопасность открытых систем: учебник для вузов в 2 тт. / С.В. Запечников [и др.]. – М.: Горячая линия–Телеком, Т. 1: Угрозы, уязвимости, атаки и подходы к защите.– 2006. – 536 с.
34. Информационная безопасность открытых систем: учебник для вузов в 2 тт. / С.В. Запечников [и др.]. – М.: Горячая линия–Телеком, Т. 2: Средства защиты в сетях. – 2008. – 558 с.
35. Запечников С.В. Основы построения виртуальных частных сетей: учеб. пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. – М.: Горячая линия–Телеком, 2003. – 249 с.

36. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2011. – 320 с.
37. Мельников Д.А. Информационная безопасность открытых систем. Учебник. – М.: Флинта, Наука, 2013. – 448 с.
38. Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем. Учебник. – М.: Университетская книга, 2012. – 598 с.
39. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2014. – 594 с.
40. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации. Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. - М.: Машиностроение, 2009. — 508 с.

По разделу 4:

41. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ "О персональных данных".
42. Северин В.А. Правовая защита информации в коммерческих организациях. – М: Academia, 2009. – 224 с.
43. Бабин С.А. Организационное обеспечение информационной безопасности. Бабин С.А., Жданов С.Г., Романов О.А. – М: Academia, 2008. – 192 с.
44. Борисов М.А. Основы организационно-правовой защиты информации. Борисов М.А., Романов О.А. – М: Ленанд, 2015. – 248 с.
45. Сайт Центра по лицензированию, сертификации и защите государственной тайны ФСБ России [электронный ресурс]. URL: <http://clsz.fsb.ru/>

Согласовано:

Председатель  
экзаменационной  
комиссии

Фомичёв Владимир  
Михайлович, д.ф.-м.н.,  
профессор

Заместитель  
председателя  
экзаменационной  
комиссии

Запечников Сергей  
Владимирович, д.т.н.,  
профессор