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

Программа вступительного испытания
по научной специальности

2.3.6. «Методы и системы защиты информации, информационная безопасность»

Форма обучения
очная

Москва, 2023

Общие положения

Форма проведения испытания:

Вступительное испытание по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» проводится в виде собеседования с обязательным оформлением ответов на вопросы билета в письменном виде. Собеседование проводится с целью выявления у абитуриента объёма 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.

Оценка испытания:

Оценка за собеседование выставляется по 100-балльной шкале. Минимальный балл, необходимый для успешного прохождения собеседования и дальнейшего участия в конкурсе – 60 баллов.

Критерии оценки результатов испытания:

100-90 баллов - даны исчерпывающие и обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует глубокие теоретические знания, умение сравнивать и оценивать различные научные подходы, пользоваться современной научной терминологией.

89-80 баллов - даны полные, достаточно глубокие и обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует хорошие знания, умение пользоваться современной научной терминологией.

79-70 баллов - даны обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует хорошие знания.

69-60 баллов - даны в целом правильные ответы на вопросы, поставленные экзаменационной комиссией, при этом абитуриент недостаточно аргументирует ответы.

59-0 баллов – абитуриент демонстрирует непонимание основного содержания теоретического материала, поверхностность и слабую аргументацию суждений или допущены значительные ошибки.

Вопросы для подготовки к вступительному испытанию

Научная специальность: 2.3.6 Методы и системы защиты информации, информационная безопасность

1. ОСНОВЫ ТЕОРИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Информационная безопасность в системе национальной безопасности Российской Федерации. Критическая информационная инфраструктура Российской Федерации. Субъекты и объекты критической информационной инфраструктуры. Государственная система защиты информации.
1.2. Место проблем защиты информации в общей совокупности информационных проблем современного общества. Информационное противоборство в современных условиях.
1.3. Виды и категории информации. Классификация методов и средств обеспечения безопасности информации.
1.4. Методы оценки параметров защищаемой информации. Факторы, влияющие на требуемый уровень защиты информации.
1.5. Определение и общеметодологические принципы построения систем защиты информации. Основы архитектурного построения систем защиты. Типизация и стандартизация систем защиты.
1.6. Риски, уязвимости и угрозы безопасности информации, их взаимосвязь. Методы и модели оценки уязвимости информации.
1.7. Классификация угроз конфиденциальности, целостности и доступности информации. Классификация источников угроз.
1.8. Объект защиты. Системность и комплексность защиты информации.
1.9. Макроструктурные компоненты комплексной системы зашиты информации (функциональные и обеспечивающие подсистемы). Подсистемы обеспечения информационной безопасности.
1.10. Процессный подход к обеспечению информационной безопасности.
1.11. Политики обеспечения информационной безопасности.
1.12. Управление системой обеспечения информационной безопасностью.

2. ОСНОВЫ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

2.1. Информатика и системы передачи данных

2.1.1. Информация, данные, сигналы. Источники информации и ее носители. Жизненный цикл информации.
2.1.2. Количество информации и энтропия. Формула Шеннона.
2.1.3. Математические модели каналов связи. Помехоустойчивость каналов.
2.1.4. Типы сигналов, их дискретизация и восстановление.
2.1.5. Спектральная плотность сигналов. Теорема Котельникова.
2.1.6. Частотное представление дискретных сигналов. Ортогональные преобразования дискретных сигналов. Задачи интерполяции и прореживания сигналов.
2.1.7. Характеристики процесса передачи информации. Математические модели каналов связи и их классификация.
2.1.8. Аналого-цифровое и цифро-аналоговое преобразование. Быстрые преобразования. Цифровые фильтры.
2.1.9. Нелинейное и параметрическое преобразование сигналов. Модуляция и демодуляция; преобразование частоты.

2.2. Теория вероятностей и математическая статистика

2.2.1. Случайные величины, функции распределения, их свойства.
2.2.2. Типовые распределения: биномиальное, пуассоновское, нормальное.
2.2.3. Независимость событий. Условные вероятности, формулы Байеса.
2.2.4. Математическое ожидание и дисперсия случайной величины.
2.2.5. Цепи Маркова, их свойства.
2.2.6. Задача проверки статистических гипотез. Статистические критерии. Ошибки 1-го и 2-го родов при проверке гипотез. Метод статистических испытаний.
2.2.7. Оценка результатов измерений. Точечные оценки и их определение. Надёжность оценки, доверительная вероятность и доверительный интервал.

2.3. Технологии программирования, алгоритмы и структуры данных

2.3.1. Жизненный цикл программного обеспечения. Тестирование программ.
2.3.2. Параллельные методы программирования.
2.3.3. Основные алгоритмы поиска данных, их временная сложность.
2.3.4. Алгоритмы сортировки, их временная сложность и практическое значение для решения задач обработки данных.
2.3.5. Временная сложность алгоритмов. Оценка времени выполнения программ.
2.3.6. Основные абстрактные типы данных: списки, стеки, очереди, деревья, ориентированные и неориентированные.

2.4. Вычислительные сети

2.4.1. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей; основы организации и функционирования сетей.
2.4.2. Распределенная обработка информации в системах клиент-сервер; одноранговые сети.
2.4.3. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения прав доступа.
2.4.4. Глобальная сеть Internet: основные службы и предоставляемые услуги, основные протоколы, особенности реализации на различных платформах, стандарты.
2.4.5. Глобальная сеть Internet: технологии обеспечения безопасности, функционирование, разработка и сопровождение приложений.
2.4.6. Современные виды информационного обслуживания; электронная почта; телеконференция; видеотекс; сети связи; структура, топология и архитектура сетей связи.
2.4.7. Методы коммутации информации; особенности сетей с коммутацией каналов, сообщений и пакетов.
2.4.8. Глобальные и локальные сети; особенности современных сетевых архитектур; архитектурные особенности современных локальных сетей; протоколы физического и канального уровней.

2.5. Базы данных

2.5.1. Общие принципы построения баз данных: реляционная, иерархическая и сетевая модели.
2.5.2. Общая характеристика, назначение и возможности систем управления базами данных (СУБД).
2.5.3. Языковые средства СУБД для различных моделей данных; языковые средства манипулирования данными в реляционных СУБД; языковые средства описания данных реляционных СУБД.

2.5.4. Особенности языковых средств управления и обеспечения безопасности данных в реляционных СУБД.
2.5.5. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных.
2.5.6. Базовые структурные компоненты модели данных: домены и атрибуты, отношение сущности, схема отношения.
2.5.7. Средства обеспечения безопасности баз данных: средства идентификации и аутентификации объектов баз данных, языковые средства разграничения доступа, концепция и реализация механизма ролей.
2.5.8. Организация аудита событий в системах баз данных; средства контроля целостности информации, организация взаимодействия СУБД и базовой ОС, журнализация, средства создания резервных копии и восстановления баз данных.

3. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Основы криптографической защиты информации

3.1.1. Определение криптографической системы, виды криптосистем.
3.1.2. Базовые криптографические примитивы. Шифры перестановки и замены.
3.1.3. Блочные и поточные шифры.
3.1.4. Вычислительно сложные задачи и однонаправленные функции, используемые в криптографии.
3.1.5. Модели шифров. Основные требования к шифрам. Совершенные шифры, криптографические хеш-функции.
3.1.6. Криптографические параметры узлов и блоков шифраторов. Синтез шифров.
3.1.7. Методы получения случайных и псевдослучайных последовательностей; программные реализации шифров.
3.1.8. Суть криптографических методов защиты информации (ЗИ). Основные задачи по ЗИ, решаемые с использованием криптографических методов. Значение криптографических методов в комплексной системе ЗИ. Базовые понятия криптологии (шифр, ключи, протоколы, шифрсистема).
3.1.9. Криптографическая стойкость шифров. Активные и пассивные атаки на шифрсистемы, задачи криптоаналитика. Теоретически стойкие шифры. Практическая стойкость шифров, её основные характеристики (трудоёмкость и надёжность дешифрования, количество необходимого материала).
3.1.10. Классификация шифрсистем с секретным ключом. Шифрсистемы поточного шифрования (синхронные и асинхронные).
3.1.11. Системный подход к построению практически стойких шифров. Характеристики случайности и непредсказуемости выходных последовательностей генераторов (периодичность, линейная сложность, статистические характеристики).
3.1.12. Криптография с открытым ключом. Основные принципы. Сравнение криптосистем с открытым и секретным ключом.

3.2. Основы защиты информации от утечки по техническим каналам

3.2.1. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения и сигналов. Опасные сигналы и их источники.

3.2.2. Структура, классификация и основные характеристики технических каналов утечки информации. Основные методы и средства защиты информации от утечки по техническим каналам.

3.2.3. Технические каналы утечки акустической (речевой) информации. Основные характеристики. Основные методы и средства защиты речевой информации в помещениях.

3.2.4. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информативных сигналов.

3.2.5. Обнаружение и локализация закладных устройств, подавление их сигналов. Подавление опасных сигналов акустоэлектрических преобразователей.

3.2.6. Экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания.

3.2.7. Технические каналы утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН). Основные характеристики. Основные методы и средства защиты информации от утечки за счет ПЭМИН.

3.2.8. Технические каналы утечки информации при передаче по каналам связи. Основные характеристики. Основные методы и средства защиты информации в каналах связи.

3.2.9. Технические каналы утечки информации средств вычислительной техники. Основные характеристики.

3.2.10. Построение модели технических каналов утечки информации и оценка возможностей нарушителя по их использованию.

3.3. Программно-аппаратные методы защиты информации от несанкционированного доступа

3.3.1. Основные принципы создания программно-аппаратных средств защиты информации. Концепция диспетчера доступа.

3.3.2. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение.

3.3.3. Защита от разрушающих программных воздействий. Защита программ от изменения и контроль целостности. Построение изолированной программной среды.

3.3.4. Программно-аппаратные средства защиты информации в сетях передачи данных.

3.3.5. Организация управления доступом и защиты ресурсов ОС. Основные механизмы безопасности: средства и методы аутентификации в ОС.

3.3.6. Модели разграничения прав доступа, организация и использование средств аудита.

3.3.7. Методы идентификации и аутентификации. Общая характеристика функции аутентификации.

3.3.8. Методы реализации контроля и разграничения прав доступа. Функции контроля и разграничения прав доступа.

3.3.9. Модель нарушителя доступа при защите автоматизированных систем от несанкционированного доступа.

3.3.10. Методы контроля защищенности автоматизированных систем от несанкционированного доступа.

3.4. Защита информации от вредоносного программного обеспечения.

3.4.1. Общее описание компьютерных вирусов. Видовая классификация компьютерных вирусов.

3.4.2. Методы и средства антивирусной защиты.

3.4.3. Организационно-правовые методы защиты от вирусов

3.4.4. Защита от вирусов в статике процессов.

3.4.5. Защита от вирусов в динамике процессов.
3.4.6. Антивирусная политика на объекте информатизации.
3.4.7. Основные направления антивирусной борьбы в компьютерных и телекоммуникационных системах.
3.4.8. Основные механизмы внедрения компьютерных вирусов в поражаемую систему.

4. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Основные положения Доктрины информационной безопасности Российской Федерации.
4.2. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы.
4.3. Основные положения Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
4.4. Основные положения Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4.5. Основные положения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».
4.6. Анализ и оценка угроз информационной безопасности объекта управления. Методология оценки ущерба от злоумышленных и неумышленных противоправных нарушений безопасности информации.
4.7. Понятие секретного (конфиденциального) делопроизводства. Общие принципы его организации. Механизм и процедуры установления степени секретности (конфиденциальности).
4.8. Особенности организации электронного документооборота. Система удостоверения ЭЦП. Цели, задачи и особенности функционирования удостоверяющих центров.
4.9. Обеспечение безопасности при осуществлении научно-технического, экономического и международного сотрудничества.
4.10. Система защиты государственной тайны. Правовой режим защиты государственной тайны. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации. Правовые режимы конфиденциальной информации.
4.11. 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.
4.12. Правовые основы защиты информации с использованием технических средств (защита от технических разведок, применение шифровальных средств, электронная цифровая подпись и т.д.).
4.13. Защита интеллектуальной собственности. Основные положения Федерального закона от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне».
4.14. Международное законодательство в области защиты информации.
4.15. Преступления в области защиты информации (Уголовный кодекс РФ, Гражданский кодекс РФ, Кодекс об административных правонарушениях РФ).

ЛИТЕРАТУРА ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

Нормативные акты

1. Конституция Российской Федерации.
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
4. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»
5. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ
6. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005). [Электронный документ]. Режим доступа: URL: http://www.27000.org/
7. Международный стандарт. ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью. [Электронный документ]. Режим доступа: URL: http://www.27000.org/
8. Международный стандарт. ISO/IEC 27004:2005 Информационные технологии. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью. [Электронный документ]. Режим доступа: URL: http://www.27000.org/
9. Международный стандарт. ISO/IEC 27005:2005 Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности. [Электронный документ]. Режим доступа: URL: http://www.27000.org/
10. Международный стандарт. ISO/IEC 27006:2005 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью. [Электронный документ]. Режим доступа: URL: http://www.27000.org/
11. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – Москва: Стандартинформ, 2015. – 21 с.
12. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – Москва: Стандартинформ, 2015. – 42 с.
13. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – Москва: Стандартинформ, 2012. – 29 с.

Основная литература

1. Информационная безопасность: концептуальные и методологические основы защиты информации / Малюк А.А. – М. Горячая линия-Телеком, 2004. – 280 с.
2. Кудряшов Б.Д. Теория информации. Учебник для вузов. – СПб.: Питер, 2009. – 320 с.
3. Основы управления информационной безопасностью / Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - М. Горячая линия-Телеком, 2014. – 244 с.
4. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.: (Высшее образование) ISBN 978-5-369-01450-9.
5. Шустова Лариса Ивановна Шустова Л.И. Базы данных: учебник / Л.И. Шустова, О.В. Тараканов. — М.: ИНФРА-М, 2017. — 304 с. + Доп. материалы [Электронный ресурс; Режим доступа http://www.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/11549.

6. Комплексная система защиты информации на предприятии / Грибунин В.Г - М.: Академия, 2009.
7. Математические и компьютерные основы криптологии / Харин Ю.С.- М.: Новое знание, 2008.
8. Фомичёв В. М., Мельников Д.А. Криптографические методы защиты информации в 2 ч.: учебник для вузов / под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2022. — 245 с.
9. Запечников С.В. Криптографические методы защиты информации. Учебное пособие. Запечников С.В., Казарин О.В., Тарасов А.А. – Москва: Юрайт Москва, 2015. – 309 с.
10. 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.
11. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2011. – 320 с.
12. Мельников Д.А. Информационная безопасность открытых систем. Учебник. – М: Флинта, Наука, 2013. – 448 с.
13. Основы защиты информации: Учебное пособие / А.И.Куприянов, А.В.Сахаров, В.А.Шевцов. -М.: Издательский центр «Академия», 2006.
14. Защита информации в телекоммуникационных системах / Коханович Г.Ф. и др. - М.: Пресс, 2005.
15. 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.
16. Борисов М.А. Основы организационно-правовой защиты информации. Борисов М.А., Романов О.А. – М: Ленанд, 2015. – 248 с.
17. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2014. – 594 с.

Дополнительная литература

1. Безопасность глобальных сетевых технологий / Игнатов В.Г. - СПб.: Питер, 2007.
2. Методы и средства защиты информации в компьютерных системах / Хорев П.Б. - М.: Академия, 2006.
3. Защита информации в системах мобильной связи / Чекалин А. А.- М.: Горячая линия-Телеком, 2005.
4. Дискретная математика и криптология / Фомичев В.М.. 2-е изд. -М,: ДИАЛОГ-МИФИ, 2009.
5. Комплексная защита информации в корпоративных системах / Шаньгин В.Ф. - М.: ИД Форум: НИЦ Инфра-М, 2012.
6. Информационная безопасность / Ярочкин В. И. - М.: Академия - проспект, 2006.
7. Основы информационной безопасности / Белов Е.Б. - М.: Горячая линия-Телеком, 2006.
8. Защита компьютерной информации от несанкционированного доступа / Щеглов Ю.А. - М.: Наука и техника, 2004.
9. Теоретико-числовые методы в криптографии / Маховенко Е.Б. - М.: Гелиос, 2006
10. . Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации (Учебное пособие) / Горбатов В.С., Дворянкин С.В., Дураковский А.П., Енгалычев Р.С. и др. Под общей редакцией Лаврухина Ю.Н. - М: НИЯУ МИФИ, 2014. -560 с.
11. Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем. Учебник. – М: Университетская книга, 2012. – 598 с.