Межрегиональное общественное учреждение
"Институт инженерной физики"

УТВЕРЖДАЮ
Председатель приёмной комиссии Института
Президент Института –
Председатель Правления Института
Заслуженный деятель науки РФ
д.т.н., профессор А.Н. Царьков
«23» 09 2019 г.

ПРОГРАММА

вступительного испытания в аспирантуру по специальной дисциплине, соответствующей направлению подготовки

10.06.01 – «Информационная безопасность»

Направленность (профиль) программы –
«Методы и системы защиты информации, информационная безопасность»

Программа вступительного испытания рассмотрена и рекомендована к утверждению на заседании учебно-методического Совета МОУ «ИИФ», протокол № 14 от 20.09.2019 г.

Серпухов, 2019

1. ЦЕЛЬ И ЗАДАЧИ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Целью вступительного испытания является аттестация поступающего в аспирантуру по 100-балльной системе – для последующего зачисления в аспирантуру на конкурсной основе. Минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания устанавливается в Институте равным 40 баллам.

Задачей вступительного испытания является выявление уровня подготовки поступающего в аспирантуру по соответствующим разделам специальной дисциплины, соответствующей направлению подготовки 10.06.01 – Информационная безопасность.

Аттестация поступающего в аспирантуру оформляется протоколом и проводится в устной форме на комиссионной основе по двум вопросам из тематического плана.

2. ТЕМАТИЧЕСКИЙ ПЛАН И ВОПРОСЫ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

Тематический план вступительного испытания включает в себя разделы:

1. Научные основы защиты информации.
2. Методы и средства обеспечения информационной безопасности.
3. Проектирование защищённых автоматизированных систем.

Раздел I. Научные основы защиты информации

1.1. Понятие национальной безопасности; виды безопасности; информационная безопасность (ИБ) в системе национальной безопасности Российской Федерации.

1.2. Общеметодологические принципы теории ИБ, анализ угроз ИБ.

1.3. Проблемы информационного противоборства; государственная политика в информационной сфере; региональные проблемы информационной безопасности.

1.4. Виды категорий информации; классификация методов и средств обеспечения ИБ.

1.5. Классификация угроз конфиденциальности, целостности и доступности информации; классификация каналов утечки и искажения информации.

1.6. Архитектура электронных систем обработки данных; формальные модели.

1.7. Модели безопасности.

1.8. Политика безопасности.

1.9. Критерии и классы защищённости средств вычислительной техники и автоматизированных информационных систем.

1.10. Характеристика стандартов по оценке защищенных систем.

1.11. Построение парольных систем, примеры практической реализации.

1.12. Особенности применения криптографических методов; способы реализации криптографической подсистемы.

1.13. Особенности реализации систем с симметричными и несимметричными ключами; концепция защищённого ядра.

1.14. Классификация методов верификации и исследования корректности систем защиты.

1.15. Классификация методов построения защищённых автоматизированных систем.

1.16. Методология обследования и проектирования систем защиты.

1.17. Особенности управления процессами функционирования систем защиты.

1.18. Определение и место проблем информационной безопасности в общей совокупности информационных проблем современного общества. Анализ развития подходов к защите информации. Современная постановка задачи защиты информации.

1.19. Особенности и состав научно-методологического базиса решения задач защиты информации. Общеметодологические принципы формирования теории защиты информации. Основное содержание теории защиты информации. Модели систем и процессов защиты информации.

1.20. Определение и содержание понятия угрозы информации в современных системах ее обработки. Системная классификация угроз. Система показателей уязвимости информации. Методы и модели оценки уязвимости информации.

1.21. Постановка задачи определения требований к защите информации. Методы оценки параметров защищаемой информации. Факторы, влияющие на требуемый уровень защиты информации.

1.22. Определение и общеметодологические принципы построения систем защиты информации. Основы архитектурного построения систем защиты. Типизация и стандартизация систем защиты.

1.23. Основные выводы из истории развития теории и практики защиты информации. Перспективы развития теории и практики защиты. Трансформация проблемы защиты информации в проблему обеспечения информационной безопасности.

Раздел II. Методы и средства обеспечения информационной безопасности

2.1. Основы криптографии

2.1. Шифры и их свойства; композиции шифров; системы шифрования.

2.2. Модели шифров; основные требования к шифрам; совершенные шифры, криптографические хеш-функции.

2.3. Теоретико-информационный подход к оценке криптостойкости шифров; имитостойкость и помехоустойчивость шифров; принципы построения криптографических алгоритмов; различие между программными и аппаратными реализациями.

2.4. Криптографические параметры узлов и блоков шифраторов; синтез шифров.

2.5. Методы получения случайных и псевдослучайных последовательностей; программные реализации шифров.

2.6. Особенности использования вычислительной техники в криптографии; организация сетей засекреченной связи; ключевые системы.

2.7. Криптографические протоколы и основные требования к ним; протоколы «рукопожатия»; протоколы установления подлинности; протоколы идентификации и аутентификации.

2.8. Парольные системы разграничения доступа.

2.9. Протоколы генерации ключей; протоколы распределения ключей; рекомендации X.509.

2.10. Протоколы разделения секретов; протоколы с нулевым разглашением; доказательства нулевого разглашения; протоколы «игры в покер».

2.11. Сложность основных целочисленных алгоритмов в кольце целых чисел, кольцах вычетов и конечных полях; дискретное преобразование Фурье для кольца целых чисел.

2.12. Квадратичные вычеты и невычеты, квадратичный закон взаимности Гаусса; цепные дроби.

2.13. Асимптотический закон распределения простых чисел; проверка чисел на простоту; построение больших простых чисел.

2.14. Методы разложения чисел на множители; алгоритмы дискретного логарифмирования в конечном поле, криптографическая система RSA, протокол Диффи-Хеллмана.

2.15. 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).

2.16. Этапы развития криптологии. Криптография с секретным (симметричная) и открытым ключом (асимметричная). Основные различия. Криптографические примитивы и криптографические протоколы по защите информации.

2.17. 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). Связь между временной и вычислительной сложностью дешифрования. Классификация методов криптографического анализа.

2.18. Классификация шифрсистем с секретным ключом. Шифрсистемы поточного шифрования (синхронные и асинхронные).

2.19. Итерационные системы блочного щифрования (шифры Фейстеля, IDEA, RIJNDAEL). Режимы шифрования. Автоматные модели шифров.

2.20. Системный подход к построению практически стойких шифров. Характеристики случайности и непредсказуемости выходных последовательностей генераторов (периодичность, линейная сложность, статистические характеристики).

2.21. Характеристики нелинейности отображений, реализуемых алгоритмами шифрования (сбалансированность, совершенность, строгий лавинный критерий,

совершенная нелинейность, корреляционный иммунитет). Генераторы на основе линейных регистров сдвига (фильтрующие, комбинирующие, с неравномерным движением).

2.22. Криптография с открытым ключом. Предпосылки появления. Однонаправленные и однонаправленные функции с секретом и их применения. Схемы шифрования с открытым ключом и цифровой подписи. Основные принципы. Схемы шифрования и подписи RSA и Рабина. Схемы открытого шифрования Эль Гамаля. Сравнение криптосистем с открытым и секретным ключом. Новые схемы шифрования.

2.23. Электронная цифровая подпись. Основные понятия. Схемы цифровой подписи RSA и Рабина и их применение. Схема цифровой подписи Эль Гамаля и ее модификации. Способы ускорения процедур подписи и проверки. Стандарты цифровой подписи США (DSA) и России (ГОСТ Р 34.10). Методы генерации секретных параметров для стандартов цифровой подписи. Разновидности схем электронной цифровой подписи и их применение.

2.2. Основы защиты информации от утечки по техническим каналам и физическая защита

2.2.1. Виды, источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники.

2.2.2. 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.

2.2.3. Методы и средства инженерной защиты и технической охраны объектов; скрытие объектов наблюдения.

2.2.4. Скрытие речевой информации в каналах связи; энергетическое скрытие акустических информативных сигналов; обнаружение и локализация закладных устройств, подавление их сигналов; подавление опасных сигналов акустоэлектрических преобразователей.

2.2.5. Экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания; подавление опасных сигналов.

2.2.6. Характеристика государственной системы противодействия технической разведке; нормативные документы по противодействию технической разведке.

2.2.7. Основные положения методологии инженерно-технической защиты информации. Виды контроля эффективности защиты информации, методы расчета и инструментального контроля показателей защиты информации.

2.2.8. Средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа.

2.2.9. Концепция инженерно-технической защиты информации (ИТЗИ): характеристика ИТЗИ как области информационной безопасности; основные задачи, показатели эффективности и факторы, влияющие на эффективность ИТЗИ; базовые принципы и основные направления ИТЗИ.

2.2.10. Основные методы и средства защиты информации от утечки по техническим каналам.

2.2.11. Основные методы и средства инженерной защиты и технической охраны объектов.

2.2.12. Основные методы и средства защиты информации в каналах связи.

2.3. Программно-аппаратные методы защиты от НСД

2.3.1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности, концепция диспетчера доступа.

2.3.2. 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.

2.3.3. Защита программ от изучения, способы встраивания средств защиты в программное обеспечение.

2.3.4. Защита от разрушающих программных воздействий, защита программ от изменения и контроль целостности, построение изолированной программной среды.

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

2.3.6. Организация управления доступом и защиты ресурсов ОС; основные механизмы безопасности: средства и методы аутентификации в ОС.

2.3.7. Модели разграничения доступа, организация и использование средств аудита.

2.3.8. Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС; основные стандарты ОС.

2.3.9. Перспективы развития; основные механизмы обеспечения безопасности и управления распределенными ресурсами.

2.3.10. Основные положения критериев TCSEC («Оранжевая книга»). Фундаментальные требования компьютерной безопасности. Требования классов защищенности.

2.3.11. Основные положения Руководящих документов Гостехкомиссии России в области защиты информации. Определение и классификация нарушителя. Классы защищённости АС от НСД к информации.

2.3.12. Основные положения CCITCE («Единые критерии»). Структура профиля и проекта защиты. Структура и ранжирование функциональных требований. Требования доверия.

2.3.13. Языковые средства представления информации в Internet.

2.3.14. Организация защиты корпоративных сетей Intranet.

2.3.15. Средства обеспечения безопасности баз данных: средства идентификации и аутентификации объектов баз данных, языковые средства разграничения доступа, концепция и реализация механизма ролей.

2.3.16. 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.

2.3.17. Задачи и средства администратора безопасности баз данных.

2.3.18. Средства реализации диалогового интерфейса и подготовки отчётов в языках СУБД.

Раздел III. Проектирование защищённых автоматизированных систем

3.1. Постановка проблемы комплексного обеспечения информационной безопасности автоматизированных систем; состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ), функциональные и обеспечивающие подсистемы, технология, управление.

3.2. Методология формирования задач защиты; интеграция средств информационной безопасности в технологическую среду; этапы проектирования КСИБ и требования к ним: предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение.

3.3. Особенности проектирования на современном уровне и синтез КСИБ; типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД).

3.4. Методы и методики проектирования: методика выявления возможных каналов НСД, последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счёт ПЭМИН, моделирование как инструментарий проектирования.

3.5. Методы и методики оценки качества КСИБ: методы нормативного функционального наполнения, метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана, метод оценки риска Фишера.

3.6. Аттестация автоматизированных систем по требованиям безопасности информации.

3.7. Особенности эксплуатации КСИБ на объекте защиты, организационно-функциональные задачи службы безопасности, управление информационной безопасностью объекта.

3.8. Понятие сложной системы: элементы и подсистемы, управление и информация, самоорганизация; основные принципы системного подхода при создании сложных систем.

3.9. Понятие качества и эффективности: характеристики качества, показатели и критерии эффективности, методические вопросы оценки эффективности сложных систем.

3.10. Функциональная и обеспечивающая часть сложной системы; технология функционирования сложной системы; цели и задачи проектирования; структуризация предметной области; классификация объектов проектирования.

3.11. Жизненный цикл автоматизированной системы; этапы проектирования системы; организация работ, функции заказчиков и разработчиков.

3.12. Практические методы реализации моделей безопасности; ядра безопасности; мониторинг взаимодействий в системе; архитектура защищенных систем.

3.13. Принципы построения защищенных информационных систем; технологический цикл реализации защищенной системы обработки и хранения информации.

3.14. Реализация систем контроля доступа; способы представления информации о правах доступа.

3. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

3.1. Основная литература

1. Бабенко Л.К., Ищукова Е.А. Криптографическая защита информации: симметричное шифрование. Учебное пособие для ВУЗов. – М.: Юрайт, 2018. – 220 с.

2. Грибунин В.Г. Комплексная система защиты информации на предприятии. – М.: Академия, 2009.

3. Гришина Н.В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007.

4. Зайцев А.П. Технические средства и методы защиты информации. – М.: Горячая линия – Телеком, 2009.

5. Партыка Т.Л. Информационная безопасность. – М.: Инфра-М, 2007.

6. Куприянов А.И. Основы защиты информации. – М.: Академия, 2006.

7. Торокин А.А. Инженерно-техническая защита информации.– М.: Аспект Пресс, 2006.

8. Основы защиты информации: Учебное пособие/А.И.Куприянов, А.В.Сахаров, В.А.Шевцов – М.: Издательский центр «Академия», 2006.

9. Коханович Г.Ф. и др. Защита информации в телекоммуникационных системах. – М.: Пресс, 2005.

10. Рябко Б.Я. Криптографические методы защиты информации. М.: Горячая линия – Телеком, 2005.

11. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия – Телеком, 2007.

12. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие. – М.: ИД Форум: НИЦ Инфра – М, 2012.

13. Фомичёв В.М. Криптографические методы защиты информации. В 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата / В.М. ФОМИЧЕВ, Д.А. Мельников. – М.: Юрайт, 2017. – 209 с.

14. Фомичёв В.М. Криптографические методы защиты информации. В 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата / В.М. Фомичёв, Д.А. Мельников. – М.: Юрайт, 2017. – 245 с.

15. Харин Ю.С. Математические и компьютерные основы криптологии. – М.: Новое знание, 2008. – 382 с.

16. Лидовский В.В. Основы теории информации и криптографии [Электронный ресурс], – https://biblioclub.ru/index.php?page=search_red.

17. Басалова Г.В. Основы криптографии [Электронный ресурс], – http://biblioclub.ru/index.php?page=book&id=233689.
18. Креопалов В.В. Технические средства и методы защиты информации [ресурс], – http://biblioclub.ru/index.php?page=book&id=90753.
19. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. – 2-е изд., испр. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book&id=428820.
20. Галатенко, В.А. Основы информационной безопасности: Курс лекций: учебное пособие / В.А. Галатенко ; под ред. В.Б. Бетелина. – Изд. 3-е. – М.: Интернет-Университет Информационных Технологий, 2006. – 208 с. [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book&id=233063.

3.2. Дополнительная литература

1. Внуков А.А. Защита информации: учебное пособие для бакалавриата и магистратуры. 2-е изд., испр. и доп. – М.: Юрайт, 2018. – 261 с.
2. Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие для вузов/ под. ред. А.В. Душкина. М.: Горячая линия – Телеком. 2018. – 248 с.
3. Белов Е.Б. Основы информационной безопасности. – «Телеком», 2006. – 544 с.
4. Сёмкин К.Н. и др. Основы организационного обеспечения информационной безопасности объектов информатизации. – М.: Гелиос АРВ, 2005. – 192 с.
5. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности. – М.: ИЦ Академия, 2008. – 192 с.
6. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. М.: Академия, 2006. – 256 с.
7 Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс], – http://biblioclub.ru/index.php?page=book&id=233065.
8. ГОСТ Р 51583-2000. Порядок создания автоматизированных систем в защищённом исполнении.
9. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии, Основные термины и определения в области технической защиты информации.

Программу вступительного испытания составил:

Первый Вице-президент Института – Главный конструктор

д.т.н., профессор _____ С.В. Смуров

Согласовано:

Вице-президент Института
по инновационным проектам,
руководитель аспирантуры

д.т.н., профессор _____ И. А. Бугаков

«20» 09 2019 г.