Федеральное агентство научных организаций

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
САНКТ-ПЕТЕРБУРГСКИЙ ИНСТИТУТ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ
РОССИЙСКОЙ АКАДЕМИИ НАУК (СПИИРАН)

УТВЕРЖДАЮ

Директор СПИИРАН

член-корреспондент РАН

_____ Р.М. Юсупов

«09» 06 2015 г.

ПРОГРАММА

вступительного экзамена по специальности

Направление подготовки:

10.06.01 Информационная безопасность

Программа (профиль) подготовки:

05.13.19 Методы и системы защиты информации, информационная безопасность

Квалификация:

Исследователь. Преподаватель-исследователь

ОДОБРЕНО Ученым советом СПИИРАН
09.06.2015 г., протокол № 5

Санкт-Петербург 2015

1. Методы и системы защиты информации

Законодательные и правовые основы защиты компьютерной информации информационных технологий. Безопасность информационных ресурсов и документирование информации; государственные информационные ресурсы; персональные данные о гражданах; права на доступ к информации; разработка и производство информационных систем; вычислительные сети и защита информации; нормативно-правовая база функционирования систем защиты информации; компьютерные преступления и особенности их расследования; российское законодательство по защите информационных технологий; промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.

Проблемы защиты информации в информационных системах. Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах; основные задачи обеспечения безопасности информации в информационных системах; защита локальных сетей и операционных систем; интеграция систем защиты; Internet в структуре информационно-аналитического обеспечения информационных систем; рекомендации по защите информации в Internet.

Содержание системы средств защиты компьютерной информации в информационных системах. Защищенная информационная система и система защиты информации; принципы построения систем защиты информации и их основы; законодательная, нормативно-методическая и научная база системы защиты информации.

Требования к содержанию нормативно-методических документов по защите информации; научно-методологический базис, стратегическая направленность и инструментальный базис защиты информации; структура и задачи (типовой перечень) органов, выполняющих защиту информации.

Организационно-правовой статус службы информационной безопасности; организационно-технические и режимные меры; политика безопасности: организация секретного делопроизводства и мероприятий по защите информации; программно-технические методы и средства защиты информации; программно-аппаратные методы и средства ограничения доступа к компонентам компьютера; типы несанкционированного доступа и условия работы средств защиты; вариант защиты от локального несанкционированного доступа и от удаленного ИСД.

Средства защиты, управляемые модемом, надежность средств защиты.

2 . Информационная безопасность

Изучение традиционных симметричных криптосистем. Основные понятия и определения; шифры перестановки; шифр перестановки «скитала»; шифрующие таблицы; применение магических квадратов; шифры простой замены; полибианский квадрат; система шифрования Цезаря; система шифрования Вижинера; шифр «двойной квадрат» Уитстона; одноразовая система шифрования; шифрование методом Вернама; роторные машины; шифрование методом гаммирования; методы генерации псевдослучайных последовательностей чисел.

Применение симметричных криптосистем для защиты компьютерной информации в информационных системах. Изучение американского стандарта шифрования данных DES; основные режимы работы алгоритма DES; отечественный стандарт шифрования данных; режим простой замены; режим гаммирования; режим гаммирования с обратной связью; режим выработки имитовставки; блочные и поточные шифры.

Применение асимметричных криптосистем для защиты компьютерной информации в информационных ситемах. Концепция криптосистемы с открытым ключом; однонаправленные функции; криптосистема шифровывания данных RSA (процедуры

шифрования и расшифрования в этой системе); безопасность и быстродействие криптосистемы RSA; схема шифрования Полига—Хеллмана; схема шифрования эль-Гамаля, комбинированный метод шифрования.

Методы идентификации и проверки подлинности пользователей компьютерных систем. Основные понятия и концепции; идентификация и механизмы подтверждения подлинности пользователя; взаимная проверка подлинности пользователей; протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний; проблема аутентификации данных и электронная цифровая подпись; однонаправленные хэш-функции; алгоритм безопасного дешифрования SHA; однонаправленные хэш-функции на основе симметричных блочных алгоритмов; отечественный стандарт хэш-функции; алгоритм цифровой подписи RSA; алгоритм цифровой подписи эль-Гамаля (EGSA); алгоритм цифровой подписи DSA; отечественный стандарт цифровой подписи.

Защита компьютерных систем от удаленных атак через сеть Internet

Режим функционирования межсетевых экранов и их основные компоненты; маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация; основные схемы сетевой защиты на базе межсетевых экранов; применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты.

Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН. Основные элементы средств защиты сети от несанкционированного доступа; устройства криптографической защиты данных; контроллер смарт-карт SCAT-200; программно-аппаратная система защиты от несанкционированного доступа (НСД) КРИПТОН-ВЕТО; защита от НСД со стороны сети; абонентское шифрование и ЭЦП; шифрование пакетов; аутентификация; защита компонентов ЛВС от НСД; защита абонентского пункта, маршрутизаторов и устройств контроля; технология работы с ключами.

Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Классификация способов защиты; защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение; понятие разрушающего программного воздействия; модели взаимодействия прикладной программы и программной закладки; методы перехвата и навязывания информации; методы внедрения программных закладок; компьютерные вирусы как особый класс разрушающих программных воздействий; защита от РПВ; понятие изолированной программной среды.

Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии. Возможности СИИТ для обеспечения комплексной защиты программ в момент их выполнения и данных при их обработке в компьютере; метод верификации программного обеспечения для контроля корректности, реализуемости и защиты от закладок.

Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов.

Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации; защита арифметических вычислений в компьютерных системах; основные направления создания защищенных компьютерных систем нового поколения на основе СИИТ.

Основная литература

Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: Руководящий документ Гостехкомиссии России. М.: ГТК РФ, 1992.

Безопасность информационных технологий / Госкомитет РФ по высшему образованию. М.: МИФИ. 1994. Вып. 1.

Безопасность информационных технологий / Московский государственный инженерно-физический институт (технический университет), 1995. Вып. 3.

ГОСТ 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: Руководящий документ Гостехкомиссии России. М.: ГТК РФ, 1992.

Насыпный В.В. Метод защиты арифметических вычислений в компьютерных системах. М.: Прометей, 1999.

Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.

Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. М.: ГТК РФ, 1992.

Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2 кн. М.: Радио и связь, 1999.