Министерство образования и науки Российской Федерации

ПРОГРАММА-МИНИМУМ

кандидатского экзамена по специальности

05.13.19 «Методы и системы защиты информации, информационная безопасность»

по физико-математическим и техническим наукам

Программа-минимум

содержит 7 стр.

2007

Введение

В основу настоящей программы положены следующие дисциплины: «Основы информационной безопасности», «Технические средства и методы защиты информации», «Криптографические методы защиты информации», «Программно-аппаратные средства обеспечения информационной безопасности», «Защита от разрушающих программных воздействий».

Программа разработана экспертным советом Высшей аттестационной комиссии по управлению, вычислительной технике и информатике при участии Московского государственного горного университета, Московского энергетического института (технического университета) и Института системного анализа РАН.

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 ассиметричных криптосистем для защиты компьютерной информации в информационных ситемах.

Концепция криптосистемы с открытым ключом;
однонаправленные функции; криптосистема шифрования 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 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 защита 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.

Литература

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

2. Безопасность информационных технологий. Выпуск 1. М.: Госкомитет РФ по высшему образованию, МИФИ, 1994.

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

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

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

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

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

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

Термины и определения в области защиты от НСД к информации.

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