ПРОГРАММА ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА
в аспирантуру
по направлению 10.06.01
" Информационная безопасность "

1. Проблемы защиты информации в информационных системах, информационных сетях. Сохранность информации и обеспечение ее безопасности в информационных системах, информационных сетях. Защита локальных сетей. Защита операционных систем. Защита баз данных. Интеграция систем защиты.

2. Принципы построения систем защиты информации, их основы, законодательная база, нормативно-правовая база. Требования к содержанию нормативно-методических документов по защите информации.

3. Политика информационной безопасности. Организационно-технические меры обеспечение информационной безопасности, средства ограничения доступа к компонентам системы и сети. Защита от локального несанкционированного доступа.

4. Аппаратно-программные средства криптографической защиты компьютерной информации. Основные элементы средств защиты сети от несанкционированного доступа. Способы встраивания защитных механизмов в программное обеспечение. Понятие разрушающего программного воздействия.

5. Комплексная защита процесса обработки информации в компьютерных системах на основе интеллектуальных информационных технологий. Принятие решений в условиях информационных конфликтов. Методы выявления, идентификации и классификации угроз нарушения информационной безопасности объектов.

6. Электронный документооборот. Электронный архив. Электронные конференции, Электронное правительство - организация работы, организация защиты. Аутентификация пользователей, аутентификация информации. Электронная подпись, коллективная электронная подпись.

7. Понятие несанкционированного доступа. Способы несанкционированного доступа к информации в компьютерных сетях. Классификации несанкционированного доступа. Обобщенный алгоритм подготовки и реализации несанкционированного доступа. Нападения на постоянные компоненты и сменные элементы систем защиты. Нападения на протоколы информационного взаимодействия.

8. Противодействие несанкционированному межсетевому доступу. Функции межсетевого экранирования. Фильтрация трафика. Политика межсетевого взаимодействия. Требования к классам защищенности.

9. Понятия уязвимости и открытости. Классификация уязвимостей. Реестры уязвимостей. Классификации дефектов программного обеспечения. Классификации вредоносных программ.

10. Обманные системы, назначение, классификация, недостатки и достоинства. Аудит уровня защищенности информационных систем.

11. Проблема обнаружения компьютерных вирусов. Определение и концепции вредоносного программного обеспечения. Классификация вредоносного программного обеспечения. Вычислительная сложность задач обнаружения вирусов. Определение вирусного множества.

12. Виды вредоносного программного обеспечения. программного обеспечения. Подходы к классификации вредоносного программного обеспечения. Основные стратегии заражения информационной системы (файловые вирусы, буткиты).

13. Методы исследования вредоносного кода и механизмы противодействия им (антидеббагинг, антиэвристика, антиэмуляция, обфускация кода, использование упаковщиков).

14. Ботнеты и компьютерные черви. Общая структура. Основные схемы и техники рассылки кода. Методы удаленного управления. Взаимодействие между червями.

15. Антивирусное программное обеспечение: назначение, структура, основные критерии выбора и принципы функционирования. Сканеры безопасности: назначение, классификация, принципы функционирования. Системы обнаружения атак: классификации, уровни функционирования, принципы реализации. Особенности

реализации на уровне сети, недостатки и достоинства. Поведенческие блокираторы: назначение, принципы реализации.

16. Классические криптосистемы с открытым ключом. Доказуемо стойкие криптосистемы. Схемы электронной цифровой подписи. Алгоритмы электронной цифровой подписи.

17. Механизмы формирования подписи в схемах электронной цифровой подписи. Схемы подписи с открытым ключом. Схемы подписи с секретным ключом. Протоколы формирования коллективной электронной цифровой подписи.

18. Традиционные симметричные криптосистемы. Шифры перестановки. Шифрующие таблицы. Шифры замены. Шифрование методом гаммирования, блочные и порточные шифры.

19. Симметричные криптосистемы для защиты компьютерной информации. Стандарты шифрования данных. Режимы шифрования данных простой замены, гаммирования, гаммирования с обратной связью, блочные и поточные шифры, имитовставка.

20. Асимметричные криптосистемы для защиты компьютерной информации. Процедуры шифрования и расшифрования данных. Безопасность и быстродействие криптосистем. Основные схемы шифрования. Комбинированный метод шифрования.

Литература

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2002. - 480 с.
2. Анин Б.Ю. Защита компьютерной информации.- СПб: БХВ - Петербург, 2000.-384 с.
3. Вайнштейн Ю.В., Демин С.Л., Кирко И.Н и др. Основы информационной безопасности. Красноярск, 2007. - 303 с.
4. Венбо Мао. Современная криптография. Теория и практика. -М., СПб., Киев: Издательский дом «Вильямс», 2005. - 763 с.
5. ГОСТ Р 50922-2006 – Защита информации. Основные термины и определения.
6. Гошко С.В. Технология борьбы с компьютерными вирусами. Практическое пособие. - М.: СОЛОН-ПРЕСС, 2009. - 352 с.
7. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. - М.:СИНТЕГ, 1999. - 232 с.
8. Дернова Е.С., Молдовян Д.Н., Молдовян Н.А. Криптографические протколы.- СПб., Изд. СПбГЭТУ, 2009. - 100 с.
9. Дернова Е.С., Молдовян Н.А., Молдовяну П.А. Элементы теоретических основ криптографии.- СПб., Изд. СПбГЭТУ, 2009. - 92 с.
10. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий.- СПб: БХВ - Петербург, 2003. - 368 с.
11. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. - 368 с.
12. Касперски К. Компьютерные вирусы изнутри и снаружи. - СПб.: ПИТЕР, 2006 .- 526 с.
13. Котенко И.В., Котухов М.М., Марков А.С. и др. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности АС и ИВС.- СПб:ВУС им. С.М. Буденого, 2000. - 190 с.
14. Лукацкий А. Обнаружение атак.- СПб: БХВ - Петербург, 2003. - 608 с.
15. Мельников В.П. Информационная безопасность и защита информации. - М.: Издательский центр «Академия», 2008. - 336с..
16. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография: скоростные шифры. - СПб: БХВ - Петербург, 2002. - 496 с.
17. Молдовян Н.А. Практикум по криптосистемам с открытым ключом.- СПб: БХВ-Петербург, 2007. - 298 с.
18. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - СПб: БХВ - Петербург, 2010.- 304 с.
19. Молдовян А.А., Молдовян Н.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов.- СПб: Петербург - БХВ, 2002, - 450 с.

20. Молдовян А.А., Молдовян Н.А., Советов Б.Я,.Криптография.- СПб.,. Лань, 2001.- 218 с.
21. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи.- СПб.: Петербург-БХВ, 2010, - 304 с.
22. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. - С-Петербург, Петербург - БХВ, 2005, - 288 с.
23. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. - М.: Научный мир, 2004.-173 с.
24. Сенкевич Г. Искусство восстановления данных.- СПб: БХВ - Петербург, 2010.- 305 с.
25. Скляров Д.В. Искуство защиты и взлома информации.- СПб: БХВ - Петербург, 2004.- 288 с.
26. Столлингс В. Криптография и защита сетей: принципы и практика.- М., Издательский дом «Вильямс», 2001.- 672 с.
27. Фомичев В.М. Дискретная математика и криптология. - М.: ДИАЛОГ-МИФИ, 2003.- 397 с.
28. Чмора А.Л. Современная прикладная криптография. М.: Гелиос - АРВ, 2002.-256 с.
29. Шнайдер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: Триумф, 2002.- 816 с.