Приложение 10

ПРОГРАММА ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА В АСПИРАНТУРУ ПО СПЕЦИАЛЬНОСТИ 05.13.19 «Методы и системы защиты информации, информационная безопасность»

ОБЩИЕ ПОЛОЖЕНИЯ

Программа отражает современное состояние обеспечения информационной безопасности и включает важнейшие общенаучные разделы, знание которых необходимо специалисту в этой области.

Рассмотрение проблем защиты информации и информационной безопасности базируется на задачах ускорения научно-технического прогресса и в частности – на необходимости решения данных проблем в связи с интенсивной информатизацией современного общества и происходящими изменениями в стране.

СОДЕРЖАНИЕ

Раздел 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. ОСНОВНЫЕ ПОЛОЖЕНИЯ СОВРЕМЕННОЙ КОНЦЕПЦИИ КОМПЛЕКСНОЙ ЗАЩИТЫ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Информация, сообщения, информационные системы и процессы как объекты информационной безопасности. Основные понятия информации и сообщения как объектов защиты. Основные понятия информационных систем.

Защита информации в современных системах ее обработки. Понятийный аппарат. Основные подходы к организации защиты информации.

Угрозы информации в современных системах ее обработки. Условия функционирования современных информационно-телекоммуникационных систем (ИТКС). Угрозы ИТКС. Пути утечки и нарушения безопасности информации. Обобщенная модель канала утечки информации. Классификация каналов утечки информации. Классификация каналов утечки по физической сущности.

Современная постановка проблемы комплексной защиты информации. Основные положения. Общее содержание теоретических основ комплексной защиты информации. Общие подходы к формированию теоретических основ комплексной защиты информации. Структура теоретических и концептуальных основ комплексной защиты информации.

1.2. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Общее содержание методологических основ информационной безопасности. Определение и структура научно-методологических основ информационной безопасности. Система принципов формирования теоретических основ комплексной защиты информации. Системный подход к управлению защитой информации. Системные

принципы создания комплексной защиты информации.

Задачи и функции защиты информации. Формирование множества задач защиты информации. Формирование множества функций защиты информации. Системная классификация средств защиты информации.

Модели защиты информации. Основные понятия методов и средств моделирования систем и процессов защиты информации. Классификация системы моделей защиты информации. Модели анализа защищенности информации. Модели синтеза систем защиты информации. Модели управления защитой информации.

Обобщенная и частные модели защиты информации. Обобщенная модель систем и процессов защиты информации. Частные модели анализа базовых показателей. Статистические модели определения значений базовых показателей уязвимости информации. Модели определения значений обобщенных показателей уязвимости. Методические вопросы использования моделей защиты информации.

Классификация методов решения задач защиты информации. Классификационная структура и общие методы решения задач комплексной защиты информации. Методы решения задач анализа систем и процессов защиты информации. Методы решения задач синтеза систем защиты информации. Методы решения задач управления системой защиты информации.

1.3. АРХИТЕКТУРА СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Архитектура систем защиты информации. Требования к архитектуре систем защиты информации. Архитектура системы защиты информации.

Типизация и стандартизация систем защиты информации. Основные понятия типизации и стандартизации. Классификация систем защиты. Методы структуризации средств защиты информации. Типовая модель многорубежной системы защиты информации.

1.4. СОДЕРЖАНИЕ, ЗАДАЧИ, ФУНКЦИИ И ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Место правовой защиты конфиденциальной информации в системе организационного и правового обеспечения информационной безопасности. Информация как объект правовой защиты.

Степени важности и грифы секретности документов и изделий, составляющих государственную тайну. Содержание и функции правового обеспечения защиты информации.

1.5. КОНЦЕПЦИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Международный опыт правового обеспечения защиты информации и развитие организационно-правового регулирования защиты информации в России. Формирование государственной системы правового обеспечения защиты информации в Российской Федерации.

Концепция правового обеспечения в области информации и ее защиты. Правовое регулирование деятельности организаций в области защиты конфиденциальной информации.

1.6. ЮРИДИЧЕСКАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВОВЫХ НОРМ ПО ВОПРОСАМ ЗАЩИТЫ ИНФОРМАЦИИ

Понятие и виды юридической ответственности за нарушение правовых норм по защите информации.

Ответственность за нарушение правовых норм защиты государственной, служебной и коммерческой тайны.

Административная ответственность и проведение административного расследования правонарушений в сфере информационной безопасности.

1.7. ОПТИМИЗАЦИЯ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ КАК СПОСОБ ПРОТИВОДЕЙСТВИЯ ВРЕДОНОСНЫМ ПРОГРАММАМ

Особенности применения вредоносных программ для несанкционированного манипулирования информацией в информационно-телекоммуникационных системах.

Принципы оптимизации функционирования информационно-телекоммуникационных систем в условиях противодействия вредоносным программам.

Обоснование показателей для оценки эффективности противодействия вредоносным программам и эффективности функционирования информационно-телекоммуникационных систем в условиях противодействия вредоносным программам.

1.8. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОПТИМИЗАЦИИ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ ПРОТИВОДЕЙСТВИЯ ВРЕДОНОСНЫМ ПРОГРАММАМ

Основные теоремы теории оптимизации функционирования информационно-телекоммуникационных систем в условиях противодействия вредоносным программам.

Метод определения оптимального объема непополняемого временного резерва информационно-телекоммуникационной системы.

Метод оптимального распределения непополняемого временного резерва информационно-телекоммуникационной системы между модулями ее программного обеспечения.

Метод реализации непополняемого временного резерва информационно-телекоммуникационной системы управления с целью идентификации воздействий вредоносных программ.

Требования к объему пополняемого временного резерва информационно-телекоммуникационной системы.

1.9. МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ ПРОТИВОДЕЙСТВИЯ ВРЕДОНОСНЫМ ПРОГРАММАМ

Формализованное представление процессов функционирования типовой информационно-телекоммуникационной системы в условиях противодействия вредоносным программам.

Принципы построения аналитических моделей процессов функционирования информационно-телекоммуникационных систем в условиях противодействия вредоносным программам.

Типовые аналитические модели для оценки точечных и интервальных характеристик процессов функционирования информационно-телекоммуникационных систем в условиях противодействия вредоносным программам.

Особенности построения имитационной модели процессов функционирования типовой информационно-телекоммуникационных систем в условиях противодействия вредоносным программам.

1.10. ОСОБЕННОСТИ РЕАЛИЗАЦИИ АЛГОРИТМОВ ПРОТИВОДЕЙСТВИЯ ВРЕДОНОСНЫМ ПРОГРАММАМ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Особенности реализации алгоритмов идентификации фактов воздействия вредоносных программ в информационно-телекоммуникационных системах.

Особенности реализации алгоритмов идентификации следов воздействий вредоносных программ в информационно-телекоммуникационных системах. Особенности реализации средств идентификации злоумышленника.

Особенности алгоритмов формирования гарантированных наборов тестовых данных для анализа последствий воздействия вредоносных программ в информационно-телекоммуникационных системах.

1.11. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ РЕЧЕВОЙ СВЯЗИ И СОВРЕМЕННАЯ КОНЦЕПЦИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ОБЪЕКТА

Оценка угроз людским, материальным и информационным ресурсам объекта. Роль и место средств защиты акустической (речевой) информации среди комплекса технических средств защиты объекта.

Информативность речевого сигнала и способы оценивания речевой информации. Особенности распространения речевого сигнала по каналам речевой связи и утечки речевой информации.

Анализ существующих способов блокировки утечки речевой информации по телефонным линиям.

Способы речепреобразования при реализации технических и криптографических методов закрытия речевых сигналов. Аналоговое скремблирование. Цифровые методы закрытия речевых сообщений.

Средства закрытия телефонных переговоров, представленные на зарубежном и отечественном рынках спецтехники. Пути совершенствования технологий закрытия речевых сигналов

Особенности применения компьютерных технологий закрытой телефонии. Принципы построения компьютерных систем закрытой телефонии и предъявляемые к ним требования.

1.12. ТЕНДЕНЦИИ РАЗВИТИЯ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ ЗАЩИТЫ РЕЧЕВЫХ СООБЩЕНИЙ

Представление речевых сигналов в виде графических образов. Системы цифрового динамического спектрального анализа-синтеза речи.

Анализ сонограмм, выявление следов фонообъектов. Требования к построению и обработке сонограмм. Возможные области применения новых компьютерных технологий безопасности речевой связи.

Раздел 2. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Структура теории компьютерной безопасности. Основные понятия и определения. Анализ угроз информационной безопасности. Структуризация методов обеспечения информационной безопасности. Основные методы реализации угроз информационной безопасности. Основные принципы обеспечения информационной безопасности в АС. Причины, виды и каналы утечки информации.

Методология построения систем защиты информации в АС. Построение систем защиты от угрозы нарушения конфиденциальности информации. Построение систем защиты от угрозы нарушения целостности информации. Построение систем защиты от угрозы отказа доступа к информации. Построение систем защиты от угрозы раскрытия параметров информационной системы. Методология построения защищенных АС.

Политика безопасности. Понятие политики безопасности. Понятия доступа и монитора безопасности. Основные типы политики безопасности. Разработка и реализация политики безопасности. Домены безопасности.

Модели безопасности. Модель матрицы доступов HRU. Модель распространения прав доступа Take-Grant. Модель системы безопасности Белла-Лападула. Модель безопасности информационных потоков.

Основные критерии защищенности АС. Классификация систем защиты АС. Руководящие документы Государственной технической комиссии России. Критерии оценки безопасности компьютерных систем Министерства обороны США ("Оранжевая книга"). Европейские критерии безопасности информационных технологий. Федеральные критерии безопасности информационных технологий.

Раздел 3. ЗАЩИТА ПРОГРАММ И ДАННЫХ

Средства защиты компьютеров. Средства защиты в MS-DOC, Windows, OS/2. Дополнительные программно-аппаратные средства, обеспечивающие повышенный уровень защиты. Средства идентификации, основанные на индивидуальных характеристиках человека.

Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера. Типы несанкционированного доступа и условия работы средств защиты. Вариант защиты от локального НСД. Вариант защиты от удаленного НСД. Средства защиты, управляемые модемом. Надежность средств защиты.

Защита от несанкционированного копирования программного обеспечения. Основные направления организационно-экономической и правовой защиты. Способы распространения программного обеспечения. Техническая защита от несанкционированного копирования. Базовые методы нейтрализации систем защиты от несанкционированного копирования. Идентификация параметров персонального компьютера. Идентификация жестких дисков. Идентификация гибких дисков. Оценка уникальности конфигурации компьютера.

Методы и средства хранения ключевой информации. Общие сведения о методах аутентификации. Магнитные диски. Магнитные и интеллектуальные карты. Уст-

ройство хранения ключей типа Touch Memory. Типовые решения в организации ключевых систем.

Анализ программных реализаций. Постановка задачи. Метод экспериментов. Статический метод. Пример применения статического метода. Проблемы автоматизации анализа при применении статистического метода. Программные отладочные средства. Динамический метод. Особенности анализа некоторых программ динамическим методом. Пример применения динамического метода.

Защита программ от изучения. Классификация способов защиты. Классификация способов защиты. Способы встраивания защитных механизмов в программное обеспечение.

Защита от разрушающих программных воздействий. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Классификация и методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от РПВ. Понятие изолированной программной среды.

Системные вопросы защиты программ и данных. Основные категории требований к средствам обеспечения информационной безопасности. Структура синтеза системы защиты.

Раздел 4. ЗАЩИТА ИНФОРМАЦИИ В ОПЕРАЦИОННЫХ СИСТЕМАХ

Общие вопросы обеспечения информационной безопасности. Угрозы безопасности операционной системы. Понятие защищенной операционной системы.

Аппаратное обеспечение средств защиты. Задачи аппаратного обеспечения защиты информации. Аппаратная защита в процессорах семейства x86. Аппаратная защита в Windows NT, Windows 2000, Windows XP.

Типовая архитектура подсистемы защиты операционной системы. Основные функции подсистемы защиты операционной системы. Разграничение доступа к объектам операционной системы. Идентификация, аутентификация и авторизация субъектов доступа. Аудит.

Защита в операционной системе UNIX. Основные положения. Пароли. Защита файловой системы. Контроль целостности системы. Средства аудита. Безопасность системы UNIX при работе в сети.

Защита в операционной системе Windows XP. Объекты и субъекты доступа в Windows XP. Разграничение доступа в Windows XP. Идентификация, аутентификация и авторизация пользователей в Windows XP. Аудит в Windows XP. Процессы-серверы в Windows XP.

Защита в операционной системе IBM OS/390. Общий обзор средств безопасности OS/390. Сервер безопасности OS/390. Средство контроля доступа к ресурсам. Сервер безопасности для обеспечения распределенной обработки. Перспективы развития средств защиты в OS/390.

Раздел 5. ОСНОВЫ КРИПТОГРАФИИ

Исторический очерк развития криптографии. Основные понятия. Криптография. Конфиденциальность. Целостность. Аутентификация. Цифровая подпись. Управление секретными ключами. Предварительное распределение ключей. Пересылка ключей. Открытое распределение ключей. Схема разделения секрета. Инфра-

структура открытых ключей. Сертификаты. Центры сертификации. Формальные модели шифров. Модели открытых текстов. Математические модели открытого текста. Критерии распознавания открытого текста.

Классификация шифров по различным признакам. Математическая модель шифра замены. Классификация шифров замены.

Шифры перестановки. Маршрутные перестановки. Элементы криптоанализа шифров перестановки.

Шифры замены. Поточные шифры простой замены. Криптоанализ поточного шифра простой замены. Блочные шифры простой замены. Многоалфавитные шифры замены. Дисковые многоалфавитные шифры замены.

Шифры гаммирования. Табличное гаммирование. О возможности восстановления вероятностей знаков гаммы. Восстановление текстов, зашифрованных неравновероятной гаммой. Повторное использование гаммы. Криптоанализ шифра Виженера. Ошибки шифровальщика.

Надежность шифров. Энтропия и избыточность языка. Расстояние единственности. Стойкость шифров. Теоретическая стойкость шифров. Практическая стойкость шифров. Вопросы имитостойкости шифров. Шифры, не распространяющие искажений. Шифры, не распространяющие искажений типа "замены знаков". Шифры, не распространяющие искажений типа "пропуск-вставка знаков".

Блочные системы шифрования. Принципы построения блочных шифров. Примеры блочных шифров. Американский стандарт шифрования данных DES. Стандарт шифрования данных ГОСТ 28147-89. Режимы использования блочных шифров. Комбинирование алгоритмов блочного шифрования. Методы анализа алгоритмов блочного шифрования. Рекомендации по использованию алгоритмов блочного шифрования.

Поточные системы шифрования. Синхронизация поточных шифрсистем. Принципы построения поточных шифрсистем. Примеры поточных шифрсистем. Шифрсистема A5. Шифрсистема Гиффорда. Линейные регистры сдвига. Алгоритм Берлекемпа—Месси. Усложнение линейных рекуррентных последовательностей. Фильтрующие генераторы. Комбинирующие генераторы. Композиции линейных регистров сдвига. Схемы с динамическим изменением закона рекурсии. Схемы с элементами памяти. Методы анализа поточных шифров.

Шифрование в аналоговой телефонии. Особенности речевых сигналов. Скремблирование. Частотные преобразования сигнала. Временные преобразования сигнала. Стойкость систем временных перестановок. Системы цифровой телефонии.

Системы шифрования с открытыми ключами. Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиса. Шифрсистемы на основе "проблемы рюкзака".

Идентификация. Фиксированные пароли (слабая идентификация). Правила составления паролей. Усложнение процедуры проверки паролей. "Подсоленные" пароли. Парольные фразы. Атаки на фиксированные пароли. Повторное использование паролей. Тотальный перебор паролей. Атаки с помощью словаря. Личные идентификационные номера. Одноразовые пароли. "Запрос-ответ" (сильная идентификация). "Запрос-ответ" с использованием симметричных алгоритмов шифрования. "Запрос-ответ" с использованием асимметричных алгоритмов шифрования. Протоколы с нулевым разглашением. Атаки на протоколы идентификации.

Криптографические хеш-функции. Функции хеширования и целостность данных. Ключевые функции хеширования. Бесключевые функции хеширования. Целостность данных и аутентификация сообщений. Возможные атаки на функции хеширования.

Цифровые подписи. Общие положения. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Фиата—Шамира. Цифровая подпись Эль-Гамаля. Одноразовые цифровые подписи.

Протоколы распределения ключей. Передача ключей с использованием симметричного шифрования. Двусторонние протоколы. Трехсторонние протоколы. Передача ключей с использованием асимметричного шифрования. Протоколы без использования цифровой подписи. Протоколы с использованием цифровой подписи. Сертификаты открытых ключей. Открытое распределение ключей. Предварительное распределение ключей. Схемы предварительного распределения ключей в сети связи. Схемы разделения секрета. Способы установления ключей для конференц-связи. Возможные атаки на протоколы распределения ключей.

Управление ключами. Жизненный цикл ключей. Услуги, представляемые доверенной третьей стороной. Установка временных меток. Нотаризация цифровых подписей.

Некоторые практические аспекты использования шифрсистем. Анализ потока сообщений. Ошибки операторов. Физические и организационные меры при использовании шифрсистем.

Квантово-криптографический протокол открытого распределения ключей. Квантовый канал и его свойства. Протокол открытого распределения ключей.

Раздел 6. ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

6.1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Телекоммуникационные системы. Основные понятия и определения в теории телекоммуникационных систем (ТКС). Особенности развития ТКС. Сети передачи данных. Мультиплексирование. Сети с коммутацией каналов и пакетов. Введение в протоколы и архитектуру сетей. Основные понятия. Функции уровней модели OSI. Сетезависимые протоколы и протоколы, ориентированные на приложения. Стандартные стеки коммуникационных протоколов. Линии связи сетей передачи данных.

Использование радиосредств в ТКС. Организация стационарного радиодоступа к телефонным сетям. Общие положения. Организация радиодоступа подвижных абонентов. Стандарты сотовых систем подвижной радиосвязи. Основные принципы построения систем сотовой связи. Перспективные системы сотовой подвижной связи.

Проблема защиты информации в ТКС. Защита информации. Основные понятия. Угрозы информационной безопасности. Классификация угроз информационной безопасности ТКС. Виды представления информации в ТКС и возможные каналы ее утечки. Модель вероятного нарушителя. Цели и возможные сценарии несанкционированного доступа к ТКС. Обеспечение защиты информации в телекоммуникационных системах. Информационная безопасность систем мобильной связи.

6.2. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Программная перестройка параметров сигнала. Программная перестройка параметров сигнала как мера защиты информации. Свойства числовых периодических последовательностей. Требования к используемым в широкополосных адресных сис-

темах передачи данных (ШАСПД) числовым последовательностям. Определение и основные свойства периодических числовых последовательностей. Корреляционные тождества и границы корреляционных функций.

Псевдослучайные последовательности, применяемые для формирования программ перестройки рабочих параметров в широкополосных адресных системах передачи данных. Линейные псевдослучайные последовательности. Нелинейные псевдослучайные последовательности. Многоуровневые числовые последовательности. Основы применения шумоподобных сигналов (ШПС) в системах связи. Определение шумоподобных сигналов и широкополосных систем связи. Основные типы шумоподобных сигналов. Общая характеристика режима ШПС как способа защиты информации в радиоканале.

Системы передачи информации с псевдослучайной перестройкой рабочих частот. Определение и классификация сигналов с псевдослучайной перестройкой рабочих частот. Структура алгоритмов формирования частотных последовательностей, используемых в линиях радиосвязи с псевдослучайной перестройкой рабочих частот. Общая характеристика режима псевдослучайной перестройки рабочей частоты как способа защиты информации в радиоканалах.

Кодирование. Теорема Шеннона о кодировании для канала с помехами. Блочные коды. Матричное кодирование. Групповые коды. Декодирование для групповых кодов. Геометрическая интерпретация двоичных кодов. Коды Хэмминга. Полиномиальные коды.

Шифрование. Основные положения криптографии. Шифрование с помощью датчика псевдослучайных чисел. Федеральный стандарт США на шифрование данных. Отечественный стандарт на шифрование данных. Шифрование с открытым ключом. Сравнение криптографических методов.

6.3. ПРАКТИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ СОТОВОЙ ПОДВИЖНОЙ РАДИОСВЯЗИ СТАНДАРТА GSM

Особенности построения и функционирования системы сотовой радиосвязи стандарта GSM. Общие характеристики стандарта GSM. Структурная схема и состав оборудования сетей связи. Сетевые и радиоинтерфейсы. Структура служб и передача данных в стандарте GSM. Терминальное оборудование и адаптеры подвижной станции. Структура TDMA кадров и формирование сигналов в стандарте GSM. Организация физических и логических каналов в стандарте GSM. Обработка речи в стандарте GSM.

Особенности защиты информации от ошибок в системе сотовой подвижной радиосвязи стандарта GSM. Защита информации от ошибок. Сверточное кодирование и перемежение в полноскоростном речевом канале. Кодирование и перемежение в полноскоростном канале передачи данных. Кодирование и перемежение в каналах управления.

Особенности обеспечения безопасности информации в системе сотовой подвижной радиосвязи стандарта GSM. Общая характеристика безопасности связи. Механизмы аутентификации. Секретность передачи данных. Обеспечение секретности абонента. Обеспечение секретности в процедуре корректировки местоположения. Общий состав секретной информации и ее распределение в аппаратных средствах GSM. Обеспечение секретности при обмене сообщениями между HLR, VLR и MSC. Модуль подлинности абонента.

ЛИТЕРАТУРА

1. Основы информационной безопасности: Учебник / В.А. Минаев, С.В. Скрыль, А.П. Фисун, В.Е. Потанин, С.В. Дворянкин. – Воронеж: Воронежский институт МВД России, 2001. – 464 с.

2. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков и др. – М.: Радио и связь, 2000. – 192 с.

3. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов / П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др. – М.: Радио и связь, 1999. – 168 с.

4. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов / Проскурин В.Г., Крутов С.В., Мацкевич И.В. – М.: Радио и связь, 2000. – 168 с.

5. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2001. – 480 с.

6. Защита информации в телекоммуникационных системах: Учебник / В.Г. Кулаков, А.Б. Андреев, А.В. Заряев и др. – Воронеж: Воронежский институт МВД России, 2002. – 300с.

7. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2-х кн.: Кн. 1. - М.: Энергоатомиздат, 1994. - 400 с.

8. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2-х кн.: Кн. 2. - М.: Энергоатомиздат, 1994. -176 с.

9. Герасименко В.А., Малюк А.А. Основы защиты информации. - М.: МОПО, МИФИ, 1997. - 537 с.

10. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Яхтсмен, 1996. - 192 с.

11. Теория и практика обеспечения информационной безопасности / Под ред. П. Д. Зегжды. - М.: Издательство агентства «Яхтсмен», 1996. - 192 с.

12. Хоффман Л.Дж. Современные методы защиты информации / Пер. с англ.; Под ред. В.А. Герасименко. - М.: Советское радио, 1980. - 363 с.