

image not found or type unknown



При рассмотрении вопросов, связанных с получением информации, хранящейся и обрабатываемой в компьютерных системах, под основными способами несанкционированного доступа предполагались следующие:

- преодоление программных средств защиты;
- несанкционированное копирование информации;
- перехват информации в каналах связи;
- использование программных закладок;
- использование аппаратных закладок;
- перехват побочных электромагнитных излучений и наводок (ПЭМИН).

При рассмотрении методов защиты мы не будем разделять их по вышеперечисленным способам, так как во многих случаях одни и те же методы оказываются эффективным средством предотвращения различных видов несанкционированного доступа.

Основными способами защиты являются следующие:

- аутентификация пользователей на этапе регистрации их полномочий;
- физическая защита компьютерных систем
- выявление программных и аппаратных закладок;
- кодирование информации.

А. Средства защиты информации в информационных сетях

В так называемой группе А к наиболее известным программно-аппаратным средствам относятся:

- >• система защиты от НСД «Спектр-Z»;

- > • система Secret Net;
- > • программно-аппаратный комплекс защиты **DAALLAS LOCK**;
- > • программно-аппаратная система «Криптон-Вето»;
- > • система криптографической защиты информации «Верба-0»;
- > • криптографический комплекс «Шифратор IP потоков» (**ШИП**).

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА «СПЕКТР-Z»

Спектр-Z — это комплексная система защиты, устанавливаемая на различные по классу ПЭВМ типа IBM PC (настольные, портативные, переносные), работающие под управлением операционных систем Windows'95 или Windows'98 всех версий.

Спектр-Z по своим характеристикам соответствует требованиям руководящих документов (РД) Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» по 3-му классу защищенности и «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации!») классу защищенности 1В, а также требованиям технических условий № ТУ 4012-001-13194780-99.

Система сертифицирована в 1999 г. Гостехкомиссией при Президенте РФ. Сертификат соответствия №251. Основные возможности системы **Спектр-Z**

Система Secret Net Win предназначена для обеспечения защиты информации в локальных вычислительных сетях на основе Windows'95. Secret Net Win обеспечивает:

- > • аутентификацию пользователей при помощи специальных аппаратных средств (Touch Memory и Smart Card);
- > • избирательное (дискреционное) разграничение доступа пользователям к каталогам, файлам и системам, в том числе и в одноранговой сети;
- > • полномочное управление доступом пользователей к данным;

- > • поддержку централизованного управления доступом пользователей к совместно используемым данным;
- > • оперативный контроль (мониторинг) за работой пользователей;
- > • подключение средств криптографической защиты данных;
- > • оповещение администратора безопасности о событиях НСД;
- > • подробную регистрацию событий, происходящих в системе и имеющих отношение к ее безопасности, а также гибкое управление регистрацией.

Существует клиентский вариант Secret Net Win для работы с серверами управления доступом на платформах Windows NT и Novell NetWare.

Secret Net Remote Tools — специальное программное средство, предназначенное для управления удаленными рабочими станциями в сети Novell NetWare, оснащенными системой Secret Net. Она позволяет:

- > • с разрешения администратора системы устанавливать удаленное соединение с рабочими станциями как собственной локальной сети, так и любой другой локальной сети на основе ОС Novell NetWare, с которой есть связь по протоколу TCP/IP и в которой присутствует сервер управления доступом системы Secret Net;
- > • подключать средства криптографической защиты для шифрования данных, передаваемых по каналу связи;
- > • просматривать содержимое экрана (только текстовые режимы) и управлять клавиатурой рабочей станции сети.

Данное программное средство функционирует в среде ОС MS-DOS и Novell NetWare.

Осуществление аутентификации пользователей осуществляется с помощью аппаратных средств:

Net Card — обеспечивает ввод имени и пароля пользователя до загрузки ОС, а также управление загрузкой компьютера с гибких магнитных дисков.

Net TM Card — выполняет функции Secret Net Card, а также обеспечивает аутентификацию пользователя при помощи Touch Memory.

Secret Net Smart Card — выполняет функции Secret Net Card, а также обеспечивает аутентификацию пользователя при помощи Smart Card.

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ЗАЩИТЫ DAALLAS LOCK

Версия DAALLAS LOCK 4.1. Предназначена для работы в операционной среде Windows'95. Система защиты сертифицирована Государственной технической комиссией по 3-му классу защищенности (сертификат № 181 от 02.06.98).

Программное обеспечение содержит:

- > • модуль контроля целостности;
- > • встроенную антивирусную защиту;
- > • возможность назначения пользователю списка разрешенных и запрещенных задач;
- > • регистрация событий, относящихся к доступу к компьютерной информации;
- > • блокировка экрана и клавиатуры в отсутствие пользователя.

Аппаратная часть содержит:

- > • в качестве основного средства идентификации — электронную карту iButton (Touch Memory*);
- > • контроллер КТ-331, содержащий собственный процессор, флэш-память и ROM-BIOS; он позволяет обеспечивать выполнение процедуры опознавания пользователя на любом ПК, независимо от типа ОС и совместимость с любым ПО.

Особенности сетевой версии:

- > • вход в сеть по электронной карте Touch Memory;
- > • удаленная работа с матрицами доступа: сравнение, изменение, обновление базы;
- > • просмотр на мониторе администратора безопасности экранов подключенных рабочих станций в режиме реального времени;
- > • графическое отображение топологии сети;

- > • эмуляция клавиатуры удаленной рабочей станции;
- > • просмотр списков пользователей и журналов любых рабочих станций с установленным комплексом DAALLAS LOCK;
- > • оперативная блокировка действий пользователей рабочих станций в критических ситуациях.

Версия DAALLAS LOCK 5.0. Система предназначена для работы на любом IBM-совместимом компьютере под управлением ОС Windows NT Workstation. Позволяет поддерживать работу до 32 зарегистрированных пользователей.

Основное отличие от версии 4.1. — наличие инструмента Secure File Deletion, позволяющего гарантированно стирать уничтоженные файлы путем затирания их места на диске нулевым кодом.

ПРОГРАММНО-АППАРАТНАЯ СИСТЕМА «КРИПТОН-ВЕТО»

Система «Криптон-Вето» предназначена для защиты ПК с процессором не ниже 386 под управлением MS DOS и выше. Windows 3.1, Windows'95. Персональный компьютер при этом может использоваться в качестве:

- > • абонентского пункта;
- > • центра коммутации пакетов;
- > • центра выработки ключей.

Принцип работы программно-аппаратной системы заключается в следующем.

Жесткий диск разбивается на логические диски. Первый логический диск (С) отводится для размещения системных программ и данных. Последний — под систему защиты от НСД и доступен только администратору. Остальные логические диски предназначены для хранения информации и программ пользователей. Эти диски можно разделить по степени конфиденциальности защищаемой информации. Функции администратора заключаются в определении степени конфиденциальности информации на каждом из логических дисков и определении круга лиц, имеющих доступ к этим дискам.

По форме хранения информации диски подразделяются на открытые и шифруемые; по виду доступа;

> • доступные для чтения и записи;

> • доступные только для чтения;

> • недоступные (заблокированные)

Подпись:

Юрьева Ксения Олеговна