вычислительных сетей для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы сетей на всех этапах их жизненного цикла (строительство помещений, проектирование сети, монтаж и наладка оборудования, испытания и эксплуатация). Подобные мероприятия хорошо известны, достаточно многочисленны. Обсуждение данного вопроса выходит за рамки статьи.

Подводя итог проведенному обзору, следует отметить, что защита информации может решаться разными методами, но наибольшего эффекта и требуемой надежности можно достигнуть только реализацией ряда комплексных мероприятий.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

А.С. Овсянников, В.В. Камышников, Ю.М. Казаченко, Н.Н. Мошак

Необходимой, а точнее, центральной составной частью мероприятий по защите информации в вычислительных системах и сетях являются внутренние эффективные системы защиты отдельных ПЭВМ от несанкционированного доступа (НСД). Основными направлениями защиты от НСД являются:

- идентификация и аутентификация пользователей средств вычислительной техники (СВТ) и АС (автоматизированных систем);
- реализация правил разграничения доступа;
- регистрация действий пользователей и их процессов;
- предоставление возможностей по изменению конфигурации системы защиты: введение новых пользователей, изменение их полномочий, и т.д.;
- реакция на попытки НСД;
- очистка оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователей с защищаемыми данными;
- учет выходных печатных и графических форм и твердых копий в АС;
- контроль целостности программной и информационной части как системы разграничения доступа, так и обеспечивающих ее средств.

Сравнение систем защиты проводилось с учетом следующих факторов:

• наличие в них тех или иных функций защиты и удобство их реализации для пользователей;

• имеющиеся сведения о механизмах реализации функций защиты, возможности их взлома потенциальным нарушителем.

В процессе анализа рассмотрены следующие системы защиты:

• программно-аппаратный комплекс защиты от НСД ассоциации "Конфидент" с использованием ключей touch memory "Dallas Lock";

• программно-аппаратный комплекс "Аккорд" с использованием ключей touch memory, поставляемый акционерным обществом "Атлас-контракт";

• комплекс программных средств на базе использования платы "Криптон-3", поставляемый малым предприятием Ancud;

• система защиты от НСД входящая в систему криптографической защиты "Маскарад";

• комплекс обеспечения безопасности работ "КОБРА".

Полноту функций систем защиты кратко можно задавать с учетом требований РД Гостехкомиссии РФ, которые классифицируются по 7 классам защищенности СВТ. Наиболее незащищенным является 7 класс, а 1 класс характеризуется максимальными требованиями по защите.

В системе "Dallas Lock" реализована система разграничения доступа к внешним устройствам дисководам, принтеру, логическим устройствам "винчестера" и разграничение доступа пользователей во времени. Система регистрирует время получения к компьютеру, а также действия зарегистрированных пользователей, связанные с попыткой превысить свои полномочия. Если оценивать полноту функций защиты, реализованных в системе "Dallas Lock" ассоциации "Конфидент", то можно сослаться на сертификат Гостехкомиссии РФ, удостоверяющий, что система удовлетворяет требованиям 6-го класса защищенности и по основным показателям требованиям 5-го класса (не удовлетворяются требования по регистрации).

Принципы построения системы защиты от НСД, реализованные в программно-аппаратном комплексе "Аккорд", также использующем электронные ключи touch memory, базируются на исходном предположении, что НСД к информации, обрабатываемой ПЭВМ, гарантированно невозможен, если:

1. На ПЭВМ с проверенным BIOS установлена проверенная операционная среда.

2. Достоверно установлена неизменность DOS и BIOS для данного сеанса работы.

3. Кроме проверенных программ в данной программно-аппаратной среде не запускалось и не запускается никаких иных программ, проверенные программы перед запуском контролируются на целостность.

4. Исключен запуск проверенных программ в какой-либо иной ситуации, т.е. вне проверенной среды.

5. Условия 1-4 выполняются в любой момент времени для всех пользователей, аутентифицированных защитным механизмом.

Аппаратно-программный комплекс "Аккорд" реализует алгоритм ступенчатого контроля целостности в DOS для создания изолированной программной среды. Этот алгоритм заключается в следующем. Процесс аутентификации проводится в одном из расширений BIOSa (чтобы минимизировать число ранее запущенных программ). Далее при загрузке программной среды предварительно фиксируется неизменность программ в основном, и расширенных BIOS, затем, используя функцию чтения в BIOS (для DOS int 13h), читаются программы обслуживания чтения (драйверы DOS), рассматриваемые как последовательность секторов, и фиксируется их целостность; в последнюю очередь, используя уже файловые операции, проверяются необходимые исполняемые модули (командный интерпретатор, драйверы дополнительных устройств, .EXE и .COM - модули и т.д.). Контроль запуска программ включается уже после загрузки DOS (иначе DOS определяет эту функцию на себя).

Комплекс "Аккорд" реализует разграничение доступа к исполняемым модулям. Разграничение доступа к другим объектам (устройствам, директориям, файлам) может быть реализовано как в самой системе защиты при ее развитии за счет введения контроля соответствующих функций операционной системы, так и возложено на прикладные задачи (такая возможность существует, поскольку число таких задач для каждого конкретного пользователя жестко ограничено).

Общим недостатком систем защиты от НСД, использующих ключи touch memory, является то, что если вынуть плату расширения, обслуживающую считы-

ватель ключа (или в случае кражи "винчестера"), то доступ к винчестеру ничем не ограничивается.

Система криптографической защиты информации "Маскарад" является чисто программным средством. В этой системе реализована фактически только защита от загрузки с системной дискеты и парольный вход в операционную систему. Эта защита сводится к модификации MBR и может быть обойдена, например, по следующей схеме. Производится загрузка с системной дискеты, вследствие действия системы защиты "винчестер" при этом операционной системе недоступен. Однако он виден для таких программ как, например, diskedit.exe из набора утилит Нортона. С помощью этой утилиты обнуляется MBR, а затем с помощью ndd.exe производится "лечение" "винчестера", диск-доктор ищет разделы (это возможно, поскольку диск не зашифрован) и сам создает таблицу разделов. Возможны и другие способы взлома. На модификации MBR построены и некоторые другие известные системы защиты от НСД: "Снег", Adm; система защиты, имеющаяся в операционной системе DR DOS или Novell DOS 7.0.

Из изложенного выше можно сделать вывод, что защита от НСД, основанная на модификации MBR, не обладает достаточной степенью надежности. В то же время, если система защиты использует криптографические преобразования в "прозрачном" режиме, даже если используемый алгоритм криптозащиты не обладает существенной криптостойкостью, описанный выше подход не применим.

Наиболее известным устройством шифрования, реализующим отечественный стандарт и широко используемым для защиты информации в сетях ПЭВМ, является "Криптон-3", которое реализовано на одной печатной плате расширения для ПЭВМ. Устройство изготовлено на базе специализированных заказных БИС "Блюминг-1". Стойкость шифрования обеспечивается при сохранении в тайне действующего ключа. Устройство вырабатывает с использованием встроенного физического датчика случайных чисел свыше 10^{75} различных ключей. Конструкция платы обеспечивает защиту от компрометирующих излучений. Скорость шифрования до 70 Кбит/с.

Пакет программ CR TOOLS позволяет зашифровывать и расшифровывать отдельные файлы и группы файлов на индивидуальном ключе пользователя, а также осуществлять генерацию таких ключей. Работа ведется в режиме "Меню". Имеется поддержка устройства "Мышь".

Пакет программ CR LINK позволяет обмениваться конфиденциальной информацией между ПЭВМ по обычному телефонному каналу с помощью стандартных модемов. Шифрование информации производится "на проходе" и не требует от пользователя дополнительных действий. Пакет позволяет осуществлять как непосредственную связь между пользователями, так и обмен предварительно подготовленными файлами. Скорость передачи информации зависит от типа модема и качества телефонного канала.

В составе пакета имеется программный драйвер, заменяющий прерывание BIOS 13h, который контролирует обращения к внешним накопителям и производит шифрование информации при всех операциях ввода/вывода, что позволяет хранить информацию на устройстве в зашифрованном виде практически незаметно для пользователя (прозрачный режим).

Основными недостатками платы "Криптон-3" являются:

- недостаточно высокая скорость работы (70 Кбит/с),
- существенно более высокие цены, причем программное обеспечение должно приобретаться отдельно.

Программная система для защиты ПЭВМ "КОБРА" обеспечивает широкие возможности по реализации различных стратегий защиты с помощью оригинального алгоритма, создает для каждого пользователя системы "сейфа с двумя ключами", обеспечивает разграничение доступа пользователей к файлам и функциональным клавишам и полную защиту от программных "закладок", а также аутентификацию пользователей по ключевой дискете и паролю. При этом шифруются все разделы жесткого диска (в том числе и диск С), что исключает возможность получения информации третьими лицами даже в случае кражи компьютера, дискет и других носителей информации. Система предусматривает установку защиты с двумя "замками" (один пользователь имеет ключевую дискету, а другой знает пароль входа). Система обнаруживает и отражает атаку любых типов вирусов.

Произведенный анализ отечественных систем защиты от НСД позволяет сделать однозначный вывод, что по совокупности оцениваемых показателей, в число которых входят: наличие функций защиты, удобство реализации этих функций для пользователей, возможность взлома потенциальным нарушителем и

стоимость системы защиты, - предпочтение должно быть отдано программному комплексу защиты "КОБРА".

ИМИТАЦИОННЫЕ МОДЕЛИ В ОТЛАДКЕ СИСТЕМ УПРАВЛЕНИЯ РОСПУСКОМ ЖЕЛЕЗНОДОРОЖНЫХ СОСТАВОВ НА СОРТИРОВОЧНЫХ ГОРКАХ

А.Ю. Павлов, М.А. Шамашов

Отладка программного обеспечения (ПО) систем реального времени (СРВ) - это процесс, трудоемкость которого может превышать 50-60% общего объема работ по созданию таких систем. Если же рассматривать отладку в широком смысле не только как процесс выявления ошибок в уже разработанном программном продукте, а в первую очередь, как процесс проверки правильности решений, принимаемых на различных стадиях проектирования системы, то приведенные цифры можно рассматривать, по-видимому, как нижнюю границу такой трудоемкости. Отладка в широком смысле - это непрерывный процесс, который желательно начинать на самых ранних стадиях проектирования системы.

В общем случае существует два метода отладки ПО СРВ: отладка с использованием реальных устройства связи с объектом (УСО) и объекта управления и исследования (ОУИ) (натурные испытания) и отладка на базе имитационных моделей этих устройств и объекта. Применение первого способа во многих случаях невозможно или нецелесообразно. Наиболее важным аргументом в пользу применения имитационных моделей при отладке ПО СРВ является принципиальная способность подобной системы справится с самыми важными и разнообразными проблемами отладки: доступность ко всем моделируемым элементам, разнообразие методов управления, повторяемость, возможность введения аварийных ситуаций и обеспечения параллельных разработок аппаратуры и ПО СРВ [1]. В рамках методологии моделирования, используемой при втором методе отладки, УСО и ОУИ заменяются моделями, функционирующими в соответствии со строгими временными и логическими закономерностями, свойственными реальным устройствам и объекту.