пропустить или блокировать движение пакетов в определенном направлении. У некоммутируемых протоколов (например, Internet Control Message Protocol (ICMP)) нет входа в таблицы соединения, поэтому по спискам контроля доступа проверяются все пакеты, решение пропускать или блокировать принимается по каждому из них индивидуально.

Проверка установления подлинности пользователя. МСЭ может подтвердить подлинность пользователей, когда они начинают связи через него. После подтверждения подлинности пользователя МСЭ сохраняет данные пользователя и последующие дополнительные связи могут быть быстро установлены.

Установление подлинности пользователя происходит путем запросов-ответов между МСЭ и соответствующим AAA сервер, например, RADIUS или TACACS+.

После подтверждения пользователя МСЭ может запросить информацию авторизации от сервера, которая используется для ограничения доступа пользователей к определенным ресурсам через МСЭ, и санкционировать доступ пользователей посредством одного из следующих методов:

вызывая из AAA соответствующий атрибут для пользователя;

управляя связями пользователя путем применения ACL, хранящегося в AAA;

управляя связями пользователя путем применения ACL, загружаемого из AAA.

Механизм инспектирования. МСЭ проверяет каждое соединение и применяет правила используемых протоколов. Этот процесс называется инспекцией протокола прикладного уровня.

Некоторые протоколы просты и имеют слабые правила для управления трафиком между источником и получателем. К ним относятся некоммутируемые протоколы, например ICMP и UDP. Напротив, коммутируемые протоколы, такие, как TCP очень строги в подтверждении связи и обмена пакета между источником и назначением.

Н.М. Бобович, А.В. Макеров, А.Е. Снегиревич

О ЗАЩИТЕ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ СЛЕДОВАТЕЛЯ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Защищенность от несанкционированного доступа и использования является одним из наиболее важных требований, предъявляемых к автоматизированной информационной системе (АИС) следователя, с помощью которой обрабатывается информация с ограниченным доступом (конфиденциальная). Основу современных АИС составляют структурированные данные (базы данных или базы знаний) и информационные технологии, реализующие информационные процессы. Поэтому обеспечение эффективной защиты от несанкционированного доступа к специализированным базам данных (БД) посторонних лиц является главным условием информационной безопасности деятельности следователя в условиях применения компьютерных технологий.

В АИС следователя, которые разрабатывались на основе БД Flint, основными средствами защиты конфиденциальной информации являлись пароль и гашение экрана монитора (дисплея). В последнее время наибольшее распространение получили АИС следователя на основе реляционной СУБД MS Access, которая располагает всеми необходимыми средства для определения и обработки данных, а также для управления ими при работе с большими объемами информации. Система управления БД позволяет контролировать задание структуры и описания своих данных, работу с ними и организацию коллективного пользования этой информацией.

Несомненным достоинством АИС следователя на основе MS Access является обеспечение достаточно высокого уровня защиты конфиденциальной информации. Это достигается за счет применения следующих средств защиты:

1. Кодирование и декодирование БД. Кодирование позволяет сжимать файл БД, что делает его недоступным для чтения с помощью служебных программ или текстовых редакторов. Применяется при электронной передаче БД или сохранении ее на магнитные носители информации. Кодирование БД возможно ее владельцем либо членом группы «Admins» в файле рабочей группы, который содержит учетные записи, используемые для защиты БД.

2. Отображение и скрытие объектов в окне БД (наименее надежный способ защиты, так как относительно просто можно отобразить любые скрытые объекты).

3. Использование параметров запуска (стартовая форма, которая автоматически открывается при открытии БД; заголовок и значок приложения БД; возможность скрытия окна БД и установления собственной кнопочной формы).

4. Использование пароля. Каждое открытие БД сопровождается появлением диалогового окна, в которое необходимо ввести пароль. Открытие БД возможно только для тех пользователей, которые введут правильный пароль.

5. Использование защиты на уровне пользователя. Позволяет устанавливать различные уровни доступа пользователей к важной информации в БД. Для этого в файле рабочей группы каждый пользователь идентифицируется уникальным кодом. Уровень доступа и объекты,

доступ к которым получает пользователь, зависят от кода и пароля. С помощью мастера защиты можно создавать собственные группы пользователей и определять разрешения на работу с БД и ее объектами для различных пользователей (групп пользователей). Кроме того, могут быть установлены разрешения на доступ, по умолчанию присваиваемые вновь создаваемым объектам БД. Группам и пользователям предоставляются разрешения, определяющие возможность их доступа к каждому объекту базы данных.

6. Запрещение репликации БД, установки паролей и настройки параметров запуска пользователями. Запрещение репликации означает запрет на создание копии общей БД, а также запрет на добавление полей и внесения других изменений в текущую БД. Предусмотрены ситуации, когда может потребоваться запрещение установки пароля базы данных пользователями (если это произойдет, никто, не зная пароля, не сможет открыть БД), а также установка запрета на изменение параметров запуска, которые определяют такие свойства, как настраиваемые меню, настраиваемые панели инструментов и стартовую форму.

7. Защита программы на языке Visual Basic для приложений (VBA). Осуществляется с помощью пароля (вводится один раз за сеанс), который не позволяет несанкционированным пользователям редактировать, копировать, экспортировать, удалять программу VBA, а также вырезать из нее и вставлять в нее фрагменты текста.

8. Защита страниц доступа к данным (файл HTML) . Применяются средства защиты файловой системы компьютера, на котором хранятся файлы HTML. Защита данных, доступ к которым осуществляется со страницы, осуществляется либо с использованием средств защиты БД, к которой подключена страница, либо задаются настройки безопасности MS Internet Explorer для предотвращения несанкционированного доступа.

Анализ перечисленных средств защиты MS Access позволяет сделать следующие выводы. Пароль на открытие БД представляет собой средний уровень защиты конфиденциальной информации. Для БД, которая совместно используется небольшой группой пользователей в рамках локальной (корпоративной) компьютерной сети или на автономной (не сетевой) ПЭВМ, установка пароля обычно оказывается достаточной.

Однако после открытия БД все объекты становятся доступными для пользователя, поэтому следует также использовать наиболее гибкий способ защиты на уровне пользователей путем их разграничения по категориям доступа к определенным данным (документам) и операциям с компьютерной информацией. Группам и отдельным пользователям предоставляются разрешения на ознакомление и обработку лишь с той информации, которая не защищена вторым – внутрисистемным

паролем. Последний имеет две разновидности, определяющие возможность пользователя манипулировать информацией, а именно:

только ознакомление со сведениями определенного раздела БД,

ознакомление и определенные действия с информацией (изменение сведений, их запись на машинный носитель и т. д.).

В качестве программного средства защиты конфиденциальной информации, обрабатываемой в АИС следователя на автономном компьютере, и на компьютерах в составе корпоративной сети, может быть использована комплексная система защиты информации (КСЗИ) «Панцирь-К» для ОС Windows 2000/XP/2003, разработанная компанией ЗАО НПП «Информационные технологии в бизнесе». Система защиты содержит в своем составе, как механизмы защиты от несанкционированного доступа, так и механизмы криптографической защиты данных.

Основные возможности, предоставляемые системой «Панцирь-К» по защите конфиденциальной информации:

авторизация пользователей при входе в систему и при доступе к критичным файловым объектам (смарт-карта, AladdineToken, ruToken, Button);

разграничение и аудит работы пользователей и приложений с локальными и сетевыми ресурсами (файловые ресурсы – FAT/NTFS/DFS/ устанавливаемые ФС, ресурсы реестра ОС, сменные носители, принтеры, сервисы олицетворения, буфер обмена и т. д.);

разграничение и аудит работы пользователей и приложений с локальными и глобальными сетями;

разграничение и аудит работы пользователей с устройствами с использованием их серийных номеров (Flash-диски, CD/DVD, USB, WiFi, Bluetooth, IrDA, IEEE1394/ FireWire, PCMCIA, COM/LPT и т. д.);

шифрование данных, включая сетевые ресурсы, скрытие, разграничение доступа, а также гарантированное удаление остаточной информации, реализации коллективного доступа к зашифрованным данным;

контроль рабочего времени пользователя, в том числе средствами компьютерного видео наблюдения.

Анализ возможностей системы «Панцирь-К» показывает, что она может успешно использоваться для защиты как от внешних, так и от внутренних ИТ-угроз, обеспечивая эффективное противодействие атакам и со стороны хакеров, и со стороны инсайдеров (санкционированных пользователей, допущенных к обработке информации на защищаемом вычислительном средстве). Система также может использоваться для эффективного противодействия вирусным атакам, эксплойтам, вредоносным, шпионским и любым иным деструктивным программам, атакам на ошибки программирования в системном и прикладном программном обеспечении.