Лекция 4
Программно-аппаратные средства технического контроля

1. Защита информации
2. Обзор методов защиты информации
3. Защита от несанкционированного доступа к информации
4. Аппаратно-программные комплексы защиты
5. Программные системы защиты
6. Криптографическое преобразование информации
7. Вопросы

Защита информации

Усложнение методов и средств организации машинной обработки информации, а также широкое использование вычислительных сетей приводит к тому, что информация становится все более уязвимой. В связи с этим защита информации в процессе ее сбора, хранения и обработки приобретает исключительно важное значение (особенно в коммерческих и военных областях).

Под защитой информации понимается совокупность мероприятий, методов и средств, обеспечивающих решение следующих основных задач:

− проверка целостности информации;

− исключение несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным (с целью сохранения трех основных свойств защищаемой информации: целостности, конфиденциальности, готовности);

− исключение несанкционированного использования хранящихся в ПЭВМ программ (т.е. защита программ от копирования).

Возможные каналы утечки информации, позволяющие нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации, принято классифицировать на три группы, в зависимости от типа средства, являющегося основным при получении информации.

Различают 3 типа средств:

- человек,
- аппаратура,
- программа.

С первой группой, в которой основным средством является человек, связаны следующие основные возможные утечки:

- чтение информации с экрана посторонним лицом;
- расшифровка программой зашифрованной информации;
- хищение носителей информации (магнитных дисков, дискет, лент и т. д.).

Ко второй группе каналов, в которых основным средством является аппаратура, относятся следующие возможные каналы утечки:

- подключение к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ.

В группе каналов, в которых основным средством является программа, можно выделить следующие возможные каналы утечки:

- несанкционированный доступ программы к информации;
- расшифровка программой зашифрованной информации;
- копирование программой информации с носителей.

Будем рассматривать средства защиты, обеспечивающие закрытие возможных каналов утечки, в которых основным средством является программа. Заметим, что такие средства в ряде случаев позволяют достаточно надежно закрыть некоторые возможные каналы утечки из других групп. Так, криптографические средства позволяют надежно закрыть канал, связанный с хищением носителей информации.

Обзор методов защиты информации

Проблемы защиты информации программного обеспечения имеют широкий диапазон: от законодательных аспектов защиты интеллектуальной собственности (прав автора) до конкретных технических устройств.

Средства защиты можно подразделить на следующие категории:

1 - средства собственной защиты;

2 - средства защиты в составе вычислительной системы;

3 - средства защиты с запросом информации;

4 - средства активной защиты;

5 - средства пассивной защиты.

Рисунок 1 - Классификация средств защиты информации

Защита от несанкционированного доступа к информации

В качестве примеров отдельных программ, повышающих защищенность КС от НСД, можно привести утилиты из пакета Norton Utilities, такие как программа шифрования информации при записи на диск Diskreet или Secret disk, программа стирания информации с диска WipeInfo, программа контроля обращения к дискам DiskMonitor и др.

Отечественными разработчиками предлагаются программные системы защиты ПЭВМ «Снег-1.0», «Кобра», «Страж-1.1» и др. В качестве примеров отечественных аппаратно-программных средств защиты, имеющих сертификат Гостехкомиссии, можно привести системы «Аккорд-4», «DALLAS LOCK 3.1», «Редут», «ДИЗ-1».

Аппаратно-программные комплексы защиты

Аппаратно-программные комплексы защиты реализуют максимальное число защитных механизмов:

• идентификация и аутентификация пользователей;

• разграничение доступа к файлам, каталогам, дискам;

• контроль целостности программных средств и информации;

• возможность создания функционально замкнутой среды пользователя;

• защита процесса загрузки ОС;

• блокировка ПЭВМ на время отсутствия пользователя;
• криптографическое преобразование информации;
• регистрация событий;
• очистка памяти.

Программные системы защиты

Программные системы защиты в качестве идентификатора используют, как правило, только пароль.

Пароль может быть перехвачен резидентными программами двух видов.

Программы первого вида перехватывают прерывания от клавиатуры, записывают символы в специальный файл, а затем передают управление ОС. После перехвата установленного числа символов программа удаляется из ОП.

Программы другого вида выполняются вместо штатных программ считывания пароля. Такие программы первыми получают управление и имитируют для пользователя работу со штатной программой проверки пароля. Они запоминают пароль, имитируют ошибку ввода пароля и передают управление штатной программе парольной идентификации. Отказ при первом наборе пароля пользователь воспринимает как сбой системы или свою ошибку и осуществляет повторный набор пароля, который должен завершиться допуском его к работе.

При перехвате пароля в обоих случаях пользователь не почувствует, что его пароль скомпрометирован. Для получения возможности перехвата паролей злоумышленник должен изменить программную структуру системы.

В некоторых программных системах защиты («Страж-1.1») для повышения достоверности аутентификации используются съемные магнитные диски, на которых записывается идентификатор пользователя. Значительно сложнее обойти блок идентификации и аутентификации в аппаратно-программных системах защиты от НСД. В таких системах используются электронные идентификаторы, чаще всего - Touch Memory.

Для каждого пользователя устанавливаются его полномочия в отношении файлов, каталогов, логических дисков. Элементы, в отношении которых пользователю запрещены любые действия, становятся «невидимыми» для него, т. е. они не отображаются на экране монитора при просмотре содержимого внешних запоминающих устройств. Для пользователей может устанавливаться запрет на использование таких устройств, как накопители на съемных носителях, печатающие устройства. Эти ограничения позволяют предотвращать реализацию угроз, связанных с попытками несанкционированного копирования и ввода информации, изучения системы защиты.

В наиболее совершенных системах реализован механизм контроля целостности файлов с использованием хэш-функции. Причем существуют системы, в которых контрольная характеристика хранится не только в ПЭВМ, но и в автономном ПЗУ пользователя. Постоянное запоминающее устройство, как правило, входит в состав карты или жетона, используемого для идентификации пользователя.

Так в системе «Аккорд-4» хэш-функции вычисляются для контролируемых файлов и хранятся в специальном файле в ПЭВМ, а хэш-функция, вычисляемая для специального файла, хранится в Touch Memory. После завершения работы на ПЭВМ осуществляется запись контрольных характеристик файлов на карту или жетон пользователя. При входе в систему осуществляется считывание контрольных характеристик из ПЗУ карты или жетона и сравнение их с характеристиками, вычисленными по контролируемым файлам. Для того, чтобы изменение файлов осталось незамеченным, злоумышленнику необходимо изменить контрольные характеристики как в ПЭВМ, так и на карте или жетоне, что практически невозможно при условии выполнения пользователем простых правил.

Очень эффективным механизмом борьбы с НСДИ является создание функционально-замкнутых сред пользователей. Суть его состоит в следующем. Для каждого пользователя создается меню, в которое попадает пользователь после загрузки

ОС. В нем указываются программы, к выполнению которых допущен пользователь. Пользователь может выполнить любую из программ из меню. После выполнения программы пользователь снова попадает в меню. Если эти программы не имеют возможностей инициировать выполнение других программ, а также предусмотрена корректная обработка ошибок, сбоев и отказов, то пользователь не сможет выйти за рамки установленной замкнутой функциональной среды. Такой режим работы вполне осуществим во многих АСУ. Защита процесса загрузки ОС предполагает осуществление загрузки именно штатной ОС и исключение вмешательства в ее структуру на этапе загрузки. Для обеспечения такой защиты на аппаратном или программном уровне блокируется работа всех ВЗУ, за исключением того, на котором установлен носитель со штатной ОС. Если загрузка осуществляется со съемных носителей информации, то до начала загрузки необходимо удостовериться в том, что установлен носитель со штатной ОС. Такой контроль может быть осуществлен программой, записанной в ПЗУ ЭВМ.

Способы контроля могут быть разными: от контроля идентификатора до сравнения хэш-функций. Загрузка с несъемного носителя информации все же является предпочтительнее. Процесс загрузки ОС должен исключать возможность вмешательства до полного завершения загрузки, пока не будут работать все механизмы системы защиты. В КС достаточно блокировать на время загрузки ОС все устройства ввода информации и каналы связи. При организации многопользовательского режима часто возникает необходимость на непродолжительное время отлучиться от рабочего места, либо передать ЭВМ другому пользователю. На это время необходимо блокировать работу ЭВМ. В этих случаях очень удобно использовать электронные идентификаторы, которые при работе должны постоянно находиться в приемном устройстве блока идентификации ЭВМ.

При изъятии идентификатора гасится экран монитора и блокируются устройства управления. При предъявлении идентификатора, который использовался при доступе к ЭВМ, осуществляется разблокировка, и работа может быть продолжена. При смене пользователей целесообразно производить ее без выключения ЭВМ. Для этого необходим аппаратно-программный или программный механизм корректной смены полномочий. Если предыдущий пользователь корректно завершил работу, то новый пользователь получает доступ со своими полномочиями после успешного завершения процедуры аутентификации.

Криптографическое преобразование информации

Одним из наиболее эффективных методов разграничения доступа является криптографическое преобразование информации. Этот метод является универсальным. Он защищает информацию от изучения, внедрения программных закладок, делает операцию копирования бессмысленной.

Пользователи могут использовать одни и те же аппаратно-программные или программные средства криптографического преобразования или применять индивидуальные средства.

Для своевременного пресечения несанкционированных действий в отношении информации, а также для контроля за соблюдением установленных правил субъектами доступа, необходимо обеспечить регистрацию событий, связанных с защитой информации. Степень подробности фиксируемой информации может изменяться и обычно определяется администратором системы защиты.

Информация накапливается на ВЗУ. Доступ к ней имеет только администратор системы защиты. Важно обеспечивать стирание информации в ОП и в рабочих областях ВЗУ. В ОП размещается вся обрабатываемая информация, причем, в открытом виде. Если после завершения работы пользователя не осуществить очистку рабочих областей памяти всех уровней, то к ней может быть осуществлен несанкционированный доступ.

Вопросы

1. Что понимается под защитой информации?
2. Перечислите возможные каналы утечки информации (конкретно по каждой группе).
3. Приведите классификация средств защиты информации.
4. Приведите современные системы защиты ПЭВМ от несанкционированного доступа к информации.
5. Какие механизмы защиты реализуют аппаратно-программные комплексы защиты?