Защита от несанкционированного изменения структур КС в процессе эксплуатации

Разграничение доступа к оборудованию

Несанкционированный доступ к аппаратным и программным средствам может быть исключен или существенно затруднен при выполнении следующего комплекса мероприятий:

• охрана помещений, в которых находятся аппаратные средства КС;

• разграничение доступа к оборудованию;

• противодействие несанкционированному подключению оборудования;

• защита внутреннего монтажа, средств управления и коммутации от несанкционированного вмешательства;

• противодействие внедрению вредительских программ.

Под *доступом к оборудованию* понимается предоставление субъекту возможности выполнять определенные разрешенные ему действия с использованием указанного оборудования.

Так, пользователю ЭВМ разрешается включать и выключать ЭВМ, работать с программами, вводить и выводить информацию.

Обслуживающий персонал имеет право в установленном порядке тестировать ЭВМ, заменять и восстанавливать отказавшие блоки.

При организации доступа к оборудованию пользователей, операторов, администраторов выполняются следующие действия:

• идентификация и аутентификация субъекта доступа;

• разблокирование устройства;

• ведение журнала учета действий субъекта доступа.

Для идентификации субъекта доступа в КС чаще всего используются атрибутивные идентификаторы.

Биометрическая идентификация проще всего осуществляется по ритму работы на клавиатуре.

Из **атрибутивных идентификаторов, как правило,** используются:

• пароли;

• съемные носители информации;

• электронные жетоны;

• пластиковые карты (рассмотрены ранее);

• механические ключи.

Практически во всех КС, работающих с конфиденциальной информацией, аутентификация пользователей осуществляется с помощью паролей.

Паролем называют комбинацию символов (букв, цифр, специальных знаков), которая должна быть известна только владельцу пароля и, возможно, администратору системы безопасности.

После подачи питания на устройство пароль вводится субъектом доступа в систему с помощью штатной клавиатуры, пульта управления или специального наборного устройства, предназначенного только для ввода пароля.

В КС, как правило, используется штатная клавиатура.

В современных операционных системах ПЭВМ заложена возможность использования пароля.

Пароль хранится в специальной памяти, имеющей автономный источник питания. Сравнение паролей осуществляется до загрузки ОС. Защита считалась эффективной, если злоумышленник не имеет возможности отключить автономное питание памяти, в которой хранится пароль.

Однако оказалось, что кроме пароля пользователя для загрузки ОС ПЭВМ можно использовать некоторые ≪технологические≫ пароли, перечень которых представлен в Internet.

В настоящее время разработаны средства защиты от несанкционированного доступа (НСД) к ПЭВМ, которые проверяют пароль до загрузки ОС. Для этого изменяются участки программ, осуществляющих загрузку ОС. Эти изменения позволяют прервать процесс загрузки до ввода правильного пароля.

При использовании паролей в момент загрузки ОС должно выполняться условие: в ЭВМ невозможно изменить установленный порядок загрузки ОС. Для этого жестко определяется ВЗУ, с которого осуществляется загрузка ОС. Желательно для этой цели использовать запоминающее устройство с несъемным носителем.

Если загрузка ОС осуществляется со съемного носителя, то необходимо предусмотреть ряд дополнительных мер.

Например, ВЗУ, с которого осуществляется загрузка ОС, настраивается таким образом, что оно может работать только с определенными носителями. В ПЭВМ это может быть достигнуто изменением порядка форматирования магнитных дисков. Отключение на время загрузки ОС всех ВЗУ, кроме выделенного для загрузки, осуществляется настройками программ загрузки ОС.

При организации парольной защиты необходимо выполнять следующие рекомендации:

1. Пароль должен запоминаться субъектом доступа. Запись пароля значительно повышает вероятность его компрометации (нарушение конфиденциальности).

2. Длина пароля должна исключать возможность его раскрытия путем подбора. Рекомендуется устанавливать длину пароля $S > 9$ символов.

3. Пароли должны периодически меняться. Безопасное время использования пароля (Тб) может быть рассчитано по формуле:

$$T_б = (A^s \cdot t)/2,$$

где t - время, необходимое на ввод символа длиной s; s - длина пароля; A - количество символов, из которых может быть составлен пароль.

Время t определяется из соотношения: t=E/R,

где E - число символов в сообщении, содержащем пароль;

R - скорость передачи символов пароля (симв./мин.).

Величина E зависит от длины пароля и количества служебных символов.

В приведенной формуле расчета величины Тб считается, что злоумышленник имеет возможность непрерывно осуществлять подбор пароля. Если предусмотрена задержка в несколько секунд после неудачной попытки ввода пароля, то безопасное время значительно возрастает.

Период смены пароля не должен превышать Тб.
В любом случае использовать пароль свыше 1 года недопустимо.

4. В КС должны фиксироваться моменты времени успешного получения доступа и время неудачного ввода пароля. После трех ошибок подряд при вводе пароля устройство блокируется, и информация о предполагаемом факте подбора пароля поступает дежурному администратору системы безопасности.

5. Пароли должны храниться в КС таким образом, чтобы они были недоступны посторонним лицам. Этого можно достичь двумя способами:

• использовать для хранения паролей специальное запоминающее устройство, считанная информация из которого не попадает за пределы блока ЗУ (схема сравнения паролей находится в самом блоке). Запись в такое ЗУ осуществляется в специальном режиме;

• криптографическое преобразование пароля.

6. Пароль не выдается при вводе на экран монитора. Чтобы субъект доступа мог ориентироваться в количестве введенных символов на экран, взамен введенного выдается специальный символ (обычно звездочка).

7. Пароль должен легко запоминаться и в то же время быть сложным для отгадывания. Не рекомендуется использовать в качестве пароля имена, фамилии, даты рождения и т.п. Желательно при наборе пароля использование символов различных регистров, чередование букв, цифр, специальных символов.

Очень эффективным является способ использования парадоксального сочетания слов (≪книга висит≫, ≪плот летит≫ и т.п.) и набора русских
букв пароля на латинском регистре.
В результате получается бессмысленный набор букв латинского алфавита.

В качестве идентификатора во многих КС используется *съемный носитель информации,* на котором записан идентификационный код субъекта доступа.

В ПЭВМ для этой цели используется гибкий или иной магнитный диск.

Такой идентификатор обладает рядом достоинств:

• не требуется использовать дополнительные аппаратные средства;

• кроме идентификационного кода, на носителе может храниться другая информация, используемая для аутентификации, контроля целостности информации, атрибуты шифрования и т. д.

Для идентификации пользователей широко используются электронные *жетоны-генераторы* случайных идентификационных кодов.

Жетон - это прибор, вырабатывающий псевдослучайную буквенно-цифровую последовательность (слово). Это слово меняется примерно раз в минуту синхронно со сменой такого же слова в КС. В результате вырабатывается одноразовый пароль, который годится для использования только в определенный промежуток времени и только для однократного входа в систему.

Первый такой жетон SecurlD американской фирмы Security Dynamics появился в 1987 году.

Жетон другого типа внешне напоминает калькулятор. В процессе аутентификации КС выдает на монитор пользователя цифровую последовательность запроса, пользователь набирает ее на клавиатуре жетона. Жетон формирует ответную последовательность, которую пользователь считывает с индикатора жетона и вводит в КС.

В результате опять получается одноразовый неповторяющийся пароль. Без жетона войти в систему оказывается невозможным. Вдобавок ко всему, прежде чем воспользоваться жетоном, нужно ввести в него свой личный пароль.

Процесс аутентификации может включать также диалог субъекта доступа с КС. Субъекту доступа задаются вопросы, ответы на которые анализируются, и делается окончательное заключение о подлинности субъекта доступа.

В качестве простого идентификатора часто используют *механические ключи.* Механический замок может быть совмещен с блоком подачи питания на устройство. На замок может закрываться крышка, под которой находятся основные органы управления устройством. Без вскрытия крышки невозможна работа с устройством.

Наличие такого замка является дополнительным препятствием на пути злоумышленника при попытке осуществить НСД к устройству.

Доступ к устройствам КС объекта может блокироваться дистанционно.

Так в ЛВС подключение к сети рабочей станции может блокироваться с рабочего места администратора.

Управлять доступом к устройствам можно и с помощью такого простого, но эффективного способа, как отключение питания.

В нерабочее время питание может отключаться с помощью коммутационных устройств, контролируемых охраной.

Комплекс мер и средств управления доступом к устройствам должен выполнять и функцию автоматической регистрации действий субъекта доступа. Журнал регистрации событий может вестись как на автономной ЭВМ, так и в сети. Периодически или при фиксации нарушений протоколов доступа, администратор просматривает журнал регистрации с целью контроля действий субъектов доступа.

Организация доступа обслуживающего персонала к устройствам отличается от организации доступа пользователей.

Прежде всего, по возможности, устройство освобождается от конфиденциальной информации и осуществляется отключение информационных связей.

Техническое обслуживание и восстановление работоспособности устройств выполняются под контролем должностных лиц.

Особое внимание обращается на работы, связанные с доступом к внутреннему монтажу и замене блоков.

Противодействие несанкционированному подключению устройств

Одним из возможных путей несанкционированного изменения технической структуры КС является подключение незарегистрированных устройств или замена ими штатных средств КС.

Для парирования такой угрозы используются следующие методы:

• проверка особенностей устройства;

• использование идентификаторов устройств.

Еще более надежным и оперативным методом контроля является использование специального кода-идентификатора устройства.

Этот код может генерироваться аппаратными средствами, а может храниться в ЗУ. Генератор может инициировать выдачу в контролирующее устройство (в вычислительной сети это может быть рабочее место администратора) уникального номера устройства. Код из ЗУ может периодически считываться и анализироваться средствами администратора КС.

Комплексное использование методов анализа особенностей конфигурации и использование идентификаторов устройств значительно повышают вероятность обнаружения попыток несанкционированного подключения или подмены.

Защита** внутреннего **монтажа,** средств **управления и коммутации от несанкционированного вмешательства

Для защиты от несанкционированных действий по изменению монтажа, замене элементов, переключению коммутирующих устройств необходимо выполнить условия:

• доступ к внутреннему монтажу, к органам управления и коммутации устройств блокируется имеющими замок дверями, крышками, защитными экранами и т. п.;

• наличие автоматизированного контроля вскрытия аппаратуры.

Создание физических препятствий на пути злоумышленника должно предусматриваться на этапе проектирования. Эти конструкции не должны создавать существенных неудобств при эксплуатации устройств.

Контроль вскрытия аппаратуры обеспечивается за счет использования несложных электрических схем, аналогичных системам охранной сигнализации. Контроль вскрытия обеспечивается путем использования датчиков контактного типа. Они устанавливаются на всех съемных и открывающихся конструкциях, через которые возможен доступ к внутреннему монтажу устройств, элементам управления и коммутации.

Датчики объединяются в единую систему контроля вскрытия устройств (СКВУ) с помощью проводных линий. Известно множество вариантов объединения датчиков в систему. При построении таких систем решаются две взаимосвязанные задачи:

обеспечение максимальной информативности системы и

минимизация числа проводных линий.

Максимум информативности автоматизированной СКВУ достигается в системах, позволяющих определить факт вскрытия конкретной защитной конструкции на определенном устройстве.

Однако во многих случаях достаточно получить дежурному администратору системы безопасности сигнал о вскрытии устройства, чтобы принять адекватные меры. Конкретное нарушение внешней целостности устройства определяется на месте.

Контроль целостности программной структуры в процессе эксплуатации

Контроль целостности программ и данных выполняется одними и теми же методами.

Исполняемые программы изменяются крайне редко на этапе их эксплуатации. Существует достаточно широкий класс программ, для которых все исходные данные или их часть также изменяются редко.

Поэтому контроль целостности таких файлов выполняется так же, как и контроль программ.

Контроль целостности программных средств и данных осуществляется путем получения (вычисления) характеристик и сравнения их с контрольными характеристиками.

Контрольные характеристики вычисляются при каждом изменении соответствующего файла.

Характеристики вычисляются по определенным алгоритмам. Наиболее простым алгоритмом является ***контрольное суммирование.*** Контролируемый файл в двоичном виде разбивается на слова, обычно состоящие из четного числа байт. Все двоичные слова поразрядно суммируются с накоплением по mod2, образуя в результате контрольную сумму. Разрядность контрольной суммы равняется разрядности двоичного слова.

Алгоритм получения контрольной суммы может отличаться от приведенного, но, как правило, не является сложным и может быть получен по имеющейся контрольной сумме и соответствующему файлу.

Другой подход к получению характеристик целостности связан с использованием ***циклических*** *кодов*

При контроле целостности информации контролируемая последовательность (сектор на диске, файл и т. д.), сдвинутая на m разрядов, делится на выбранный порождающий полином, и запоминается полученный остаток, который называют синдромом.

Синдром хранится как эталон. При контроле целостности к полиному контролируемой последовательности добавляется синдром и осуществляется деление на порождающий полином. Если остаток от деления равен нулю, то считается, что целостность контролируемой последовательности не нарушена. Обнаруживающая способность метода зависит от степени порождающего полинома и не зависит от длины контролируемой последовательности.

Использование контрольных сумм и циклических кодов, как и других подобных методов, имеет существенный недостаток.

Алгоритм получения контрольных характеристик хорошо известен, и поэтому злоумышленник может произвести изменения таким образом, чтобы контрольная характеристика не изменилась (например, добавив коды).

Задача злоумышленника усложнится, если использовать переменную длину двоичной последовательности при подсчете контрольной характеристики, а характеристику хранить в зашифрованном виде или вне КС (например, в ЗУ Touch Memory).

Существует метод, который позволяет практически исключить возможность неконтролируемого изменения информации в КС.

Для этого необходимо использовать хэш-функцию. Под *хэшфункцией* понимается процедура получения контрольной характеристики двоичной последовательности, основанная на контрольном суммировании и криптографических преобразованиях.

Алгоритм хэш-функции приведен в ГОСТ Р34.11-94. Алгоритм не является секретным, так же как и алгоритм используемого при получении хэш-функции криптографического преобразования, изложенного в ГОСТ 28147-89.

Исходными данными для вычисления хэш-функции являются исходная двоичная последовательность и стартовый вектор хэширования. Стартовый вектор хэширования представляет собой двоичную последовательность длиной 256 бит. Он должен быть недоступен злоумышленнику.

Вектор либо подвергается зашифрованию, либо хранится вне КС.

Итерационный процесс вычисления хэш-функции H предусматривает:

• генерацию четырех ключей (слов длиной 256 бит);

• шифрующее преобразование с помощью ключей текущего значения H методом простой замены (ГОСТ 28147-89);

• перемешивание результатов;

• поразрядное суммирование по mod2 слов длиной 256 бит исходной последовательности;

• вычисление функции H.

В результате получается хэш-функция длиной 256 бит. Значение хэш-функции можно хранить вместе с контролируемой информацией, т. к., не имея стартового вектора хэширования, злоумышленник не может получить новую правильную функцию хэширования после внесения изменений в исходную последовательность.

А получить стартовый вектор по функции хэширования практически невозможно.

Для каждой двоичной последовательности используются две контрольные характеристики:

стартовый вектор и хэш-функция.

При контроле по стартовому вектору и контролируемой последовательности вычисляется **значение хэш-функции** и

сравнивается с контрольным значением.