Ключи. Организация хранения ключей (с примерами реализации). Распределение ключей. Использование комбинированной криптосистемы. Метод распределения ключей Диффи-Хеллмана. Протокол вычисления ключа парной связи ЕСКЕР.

Любая криптографическая система основана на использовании криптографических ключей. Под ключевой информацией понимают совокупность всех действующих в информационной сети или системе ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации в сети или системе. Управление ключами включает реализацию таких функций, как генерация, хранение и распределение ключей. Распределение ключей - самый ответственный процесс в управлении ключами.

1. Ключи. Организация хранения ключей

При работе с открытыми КС необходимо обеспечить защиту аутентифицирующей информации, хранимой в КС. В открытых КС часто отсутствуют внешние максимально защищенные от НСД устройства, хранящие аутентифицирующую информацию, и данную информацию, используемую для аутентификации, приходится хранить в реальном объекте файловой системы (БД аутентификации).

Эту информацию необходимо защищать от 2 основных видов угроз:

- угроза непосредственного доступа злоумышленника к БД аутентификации с целью ее копирования, модификации, удаления;
- угроза несанкционированного изучения БД аутентификации.

Защита от первого вида угрозы реализуется, как правило, на уровне ядра ОС путем ограничения доступа к той БД аутентификации всех субъектов, за исключением привилегированных. Либо защита от данного вида угроз реализуется путем определения дискреционной политики безопасности. Однако, как правило, способы защиты от угроз первого вида не работают корректно и их можно обойти, используя существующие уязвимости.

Поэтому при защите БДА большее внимание уделяется защите от несанкционированного исследования их содержимого.

Методы:

1). Шифрование

Такой подход к закрытию содержимого БД аутентификации не является стойким, так как:

1. Шифрование должно быть на ключах, которые необходимо хранить. Хранение в операционной системе недопустимо.
2. При аутентификации пользователя необходимо расшифровать пароль, тем самым нарушить его секретность. Такой способ также уязвим к атакам, например, к атакам, заключенным в пошаговом исследовании процесса аутентификации с помощью известных отладчиков.

2). Хэширование

Для защиты от исследования БДА используется две типовых схемы хранения ключевой информации:

Схема 1

Пусть пользователь с N i имеет идентификатор ID_i и ключ идентификации K_i, тогда первая типовая схема предполагает наличие в БД аутентификации двух основных полей:

№	Информация для идентификации	Информация для аутентификации
1	ID1	E1
2	ID2	E2
…		
n	IDn	En

$Et = F(IDt, Kt)$, F – функция хэширования. Функция F должна удовлетворять следующим свойствам:

1). Необратимостью: восстановить Kt возможно было бы только полным перебором

2). Вероятность совпадения хэшей 2 произвольно взятых сообщений должна быть чрезмерно мала, если длина сообщения меньше длины хэша, то вероятность должна быть равна нулю.

3) Рассеивание – при малейшем изменении сообщения его хэш должен существенным образом изменяться.

При использовании такой схемы хранения ключевой информации, ОС в явном виде не знает те ключи, пароли, которые используются пользователем для входа в систему.

Алгоритм аутентификации пользователя будет выглядеть следующем образом:

Пользователь вводит идентификатор при входе в систему. Подсистема аутентификации ищет наличие данного идентификатора в БД аутентификации. Если данный идентификатор не найден, то идентификация отклоняется. Если же введенный идентификатор равен некому IDt, то подсистема аутентификации извлекает Et, соответствующий ему. Далее пользователь вводит пароль k. Подсистема аутентификации вычисляет $y = F(IDt, kt)$. Если $y = Et$, то аутентификация принимается.

Недостатком данной схемы является то, что достаточно часто закрытые образы паролей формируются как $Et = F(kt)$. Тогда пользователи, имеющие одинаковые пароли, будут иметь одни и те же хэши. Злоумышленник, обнаружив подобную ситуацию, может сделать вывод, что пользователи используют одинаковые пароли.

Для устранения этого вводится вторая схема аутентификации.

Схема 2

Вторая типовая схема предполагает хранение вместе с идентификатором ID_iслучайной информации S_i, формирующейся при создании учетной записи. S_i называется символом привязки.

$Ei = F(S_i, ki)$

Информация для идентификации	Информация для аутентификации
ID1 , S1	E1
ID2, S2	E2
IDn, Sn	En

В этом случае хэши будут различны. Данная схема используется в системах класса Unix.

Утверждение о подмене эталона

Если злоумышленник имеет доступ на запись в БД аутентификации, то он может пройти аутентификацию как любой пользователь КС, отраженный в ней, в том числе и как администратор. Следовательно, доступ на запись в БД аутентификации должны иметь только привилегированные субъекты.

Защита баз данных аутентификации операционных систем класса Windows NT.

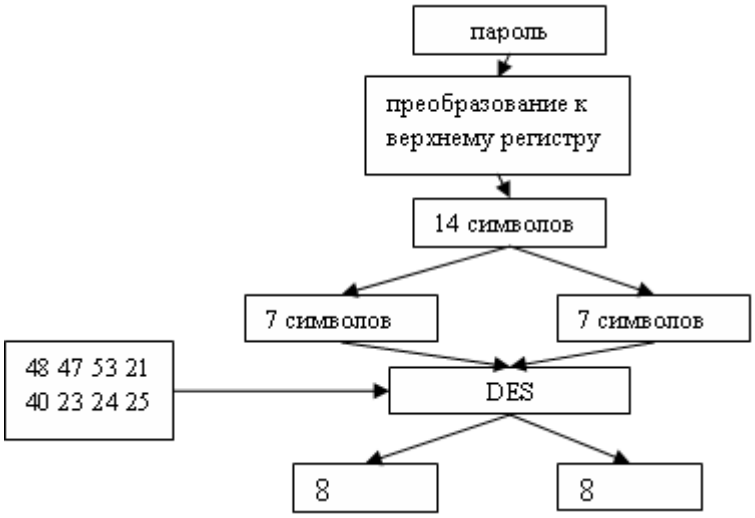
В данных ОС БД аутентификации хранится в каталоге: winnt\system32\config

БДА носит название SAM, а файл System, в котором хранится ключ шифрования БД аутентификации.

В данной БД аутентификации хранится 2 вида хэшей:

- LANMAN, используемый для удаленной сетевой аутентификации с ранних версий Windows;
- NTLM, используется для локальной аутентификации.

Алгоритм вычисления хэша LANMAN



Например, если пароль будет состоять из заглавных букв английского алфавита (26), прописных букв английского алфавита (26), цифр (10), специальных символов (13), то

$$A = 26 + 26 + 10 + 13 = 75$$

$$S = 75^{13}$$

Тогда время подбора $T = \frac{75^{13}}{10^7}$ сек

Используя хэш LANMAN, получим, что

$$A = 49$$

$$S = 49^7$$

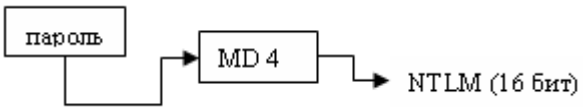
Время подбора пароля $T = \frac{49^7}{10^7} \approx 5^7$

Минусы:

- все символы пароля преобразуются в заглавные, что уменьшает энтропию паролей, сокращает пространство их перебора;
- пароль разбивается на две части, которые образуются независимо друг от друга;

При выборе паролей больше 14 символов хэши LANMAN из БД исчезают, следовательно, необходимо выбирать пароли из 15-16 символов.

Хэш NTLM



Хэш NTLM имеет длину 16 байт. Каждому из паролей длины меньшей или равной 16 символов соответствует единственный хэш NTLM, по которому ОС будет определять корректность его ввода пользователем. Однако если выбрать пароли больше 17 символов, то для них найдутся другие с длинной

меньше или равной 16 символам, которые будут иметь тот же самый хэш. В этом случае ОС будет пускать пользователя на пароле меньшей длины. Есть вероятность, что длина таких паролей будет очень мала. Поэтому в целях безопасности использование паролей длиной больше или равной 17 символов необходимо запретить. Для ОС, построенных на технологии NT, следует выбирать пароли 15-16 символов.

2. Распределение ключей

При использовании симметричной криптосистемы две вступающие в информационный обмен стороны должны сначала согласовать секретный сессионный ключ, то есть ключ для шифрования всех сообщений, передаваемых в процессе обмена. Этот ключ должен быть неизвестен всем остальным, и его необходимо периодически обновлять одновременно у отправителя и получателя. Процесс согласования сессионного ключа называют также обменом или распределением ключей.

Асимметричная криптосистема предполагает использование двух ключей -открытого и закрытого (секретного). Открытый ключ можно разглашать, а закрытый надо хранить в тайне. При обмене сообщениями необходимо пересылать только открытый ключ, обеспечив его подлинность.

К распределению ключей предъявляются следующие требования:

- оперативность и точность распределения;
- конфиденциальность и целостность распределяемых ключей.

Для распределения ключей между пользователями компьютерной сети используются следующие основные способы [95]:

1. Использование одного или нескольких центров распределения ключей.
2. Прямой обмен ключами между пользователями сети.

Проблемой первого подхода является то, что центру распределения ключей известно, кому и какие ключи распределены, и это позволяет читать все сообщения, передаваемые по сети. Возможные злоупотребления могут существенно нарушить безопасность сети. При втором подходе проблема состоит в том, чтобы надежно удостовериться в подлинности субъектов сети.

Задача распределения ключей сводится к построению такого протокола распределения ключей, который обеспечивает:

- взаимное подтверждение подлинности участников сеанса;
- подтверждение достоверности сеанса;
- использование минимального числа сообщений при обмене ключами.

Характерным примером реализации первого подхода является система аутентификации и распределения ключей Kerberos.

Остановимся подробнее на втором подходе - прямом обмене ключами между пользователями сети.

При использовании для защищенного информационного обмена криптосистемы с симметричным секретным ключом два пользователя, желающие обменяться криптографически защищенной информацией, должны обладать общим секретным ключом. Эти пользователи должны обменяться общим ключом по каналу связи безопасным образом. Если пользователи меняют ключ достаточно часто, то доставка ключа превращается в серьезную проблему.

Для решения этой проблемы можно применить два основных способа:

1. Использование асимметричной криптосистемы с открытым ключом для защиты секретного ключа симметричной криптосистемы.

2. Использование системы открытого распределения ключей Диффи-Хеллмана.

Реализация первого способа осуществляется в рамках комбинированной криптосистемы с симметричными и асимметричными ключами. При таком подходе симметричная криптосистема применяется для шифрования и передачи исходного открытого текста, а асимметричная криптосистема с открытым ключом - для шифрования, передачи и последующего расшифрования только секретного ключа симметричной криптосистемы.

Второй способ безопасного распространения секретных ключей основан на применении алгоритма открытого распределения ключей Диффи-Хеллмана. Этот алгоритм позволяет пользователям обмениваться ключами по незащищенным каналам связи.

Лекция 12
Использование комбинированной криптосистемы

Главным достоинством асимметричных криптосистем с открытым ключом является их потенциально высокая безопасность: нет необходимости ни передавать, ни сообщать кому бы то ни было значения секретных ключей, ни убеждаться в их подлинности. Однако быстродействие асимметричных криптосистем с открытым ключом обычно в сотни и более раз меньше быстродействия симметричных криптосистем с секретным ключом.

В свою очередь, быстродействующие симметричные криптосистемы страдают существенным недостатком: обновляемый секретный ключ симметричной криптосистемы должен регулярно передаваться партнерам по информационному обмену, и во время этих передач возникает опасность раскрытия секретного ключа.

Существует эффективный метод комбинированного использования симметричного и асимметричного шифрования.

Комбинированное применение симметричного и асимметричного шифрования позволяет устранить основные недостатки, присущие обоим методам. Комбинированный (гибридный) метод шифрования позволяет сочетать преимущества высокой секретности, предоставляемые асимметричными криптосистемами с открытым ключом, с преимуществами высокой скорости работы, присущими симметричным криптосистемам с секретным ключом.

При таком подходе симметричную криптосистему применяют для шифрования исходного открытого текста, а асимметричную криптосистему с открытым ключом - только для шифрования секретного ключа симметричной криптосистемы. В результате асимметричная криптосистема с открытым ключом не заменяет, а лишь дополняет симметричную криптосистему с секретным ключом, позволяя повысить в целом защищенность передаваемой информации. Такой подход иногда называют схемой *электронного цифрового конверта.*

Пусть пользователь А хочет применить комбинированный метод шифрования для защищенной передачи сообщения М пользователю В.

Тогда последовательность действий пользователей А и В будет следующей.

Действия пользователя А:

1. Создает (например, генерирует случайным образом) симметричный сеансовый секретный ключ Ks.
2. Шифрует сообщение М на симметричном сеансовом секретном ключе Ks.
3. Шифрует секретный сеансовый ключ Ks на открытом ключе Кв пользователя В (получателя сообщения).
4. Передает по открытому каналу связи в адрес пользователя В зашифрованное сообщение М вместе с зашифрованным сеансовым ключом Ks.

Действия пользователя А иллюстрируются схемой шифрования сообщения комбинированным методом (рис. 3.9).

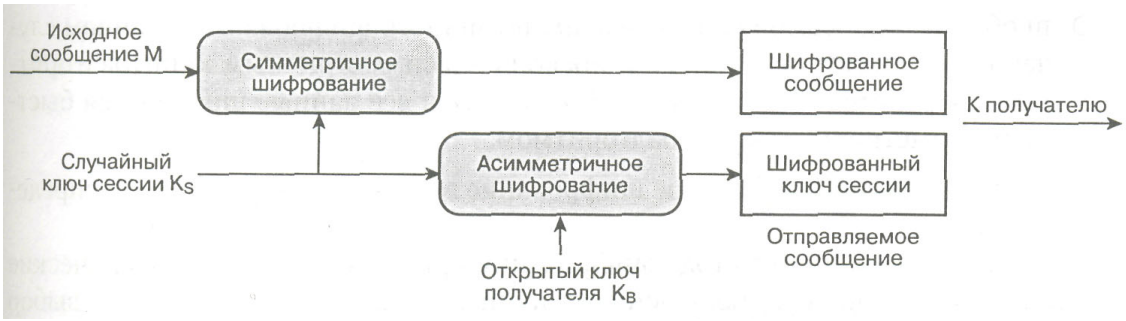


Рис. 3.9. Схема шифрования сообщения комбинированным методом

Действия пользователя В (при получении электронного цифрового конверта - зашифрованного сообщения М и зашифрованного сеансового ключа Ks):

5. Расшифровывает на своем секретном ключе kв сеансовый ключ Ks.
6. С помощью полученного сеансового ключа Ks расшифровывает принятое сообщение М.

Действия пользователя В иллюстрируются схемой расшифрования сообщения комбинированным методом (рис. 3.10).

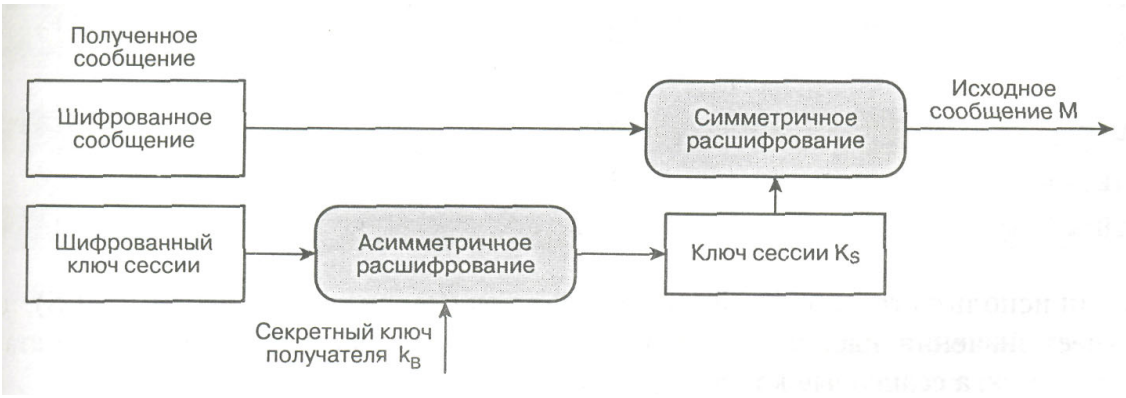


Рис. 3.10. Схема расшифрования сообщения комбинированным методом

Полученный электронный цифровой конверт может раскрыть только законный получатель - пользователь В. Только пользователь В, владеющий личным секретным ключом кв, сможет правильно расшифровать секретный сеансовый ключ Ks и затем с помощью этого ключа расшифровать и прочитать полученное сообщение М.

При методе цифрового конверта недостатки симметричного и асимметричного криптоалгоритмов компенсируются следующим образом:

- проблема распространения ключей симметричного криптоалгоритма устраняется тем, что сеансовый ключ Ks, на котором шифруются собственно сообщения, передается по открытым каналам связи в

зашифрованном виде; для зашифрования ключа Ks используется асимметричный криптоалгоритм;

- проблемы медленной скорости асимметричного шифрования в данном случае практически не возникает, поскольку асимметричным криптоалгоритмом шифруется только короткий ключ Ks, а все данные шифруются быстрым симметричным криптоалгоритмом.

В результате получают быстрое шифрование в сочетании с удобным распределением ключей.

При комбинированном методе шифрования применяются криптографические ключи как симметричных, так и асимметричных криптосистем. Очевидно, выбор длин ключей для криптосистемы каждого типа следует осуществлять таким образом, чтобы злоумышленнику было одинаково трудно атаковать любой механизм защиты комбинированной криптосистемы.

В табл. 3.1 приведены распространенные длины ключей симметричных и асимметричных криптосистем, для которых трудность атаки полного перебора примерно равна трудности факторизации соответствующих модулей асимметричных криптосистем [95, 157].

Таблица 3.1

Длина ключа симметричной криптосистемы, битов	Длина ключа асимметричной криптосистемы, битов
56	384
64	512
80	768
112	1792
128	2304

Если используется короткий сеансовый ключ (например, 40-битовый DES), то не имеет значения, насколько велики асимметричные ключи. Хакеры будут атаковать не их, а сеансовые ключи.

Метод распределения ключей Диффи-Хеллмана

Метод открытого распределения ключей, изобретенный У. Диффи и М. Хеллманом, позволяет пользователям обмениваться ключами по незащищенным каналам | связи. Его безопасность обусловлена трудностью вычисления дискретных логарифмов в конечном поле, в отличие от легкости решения прямой задачи дискретного возведения в степень в том же конечном поле. Суть метода Диффи-Хеллмана заключается в следующем (рис. 3.11).

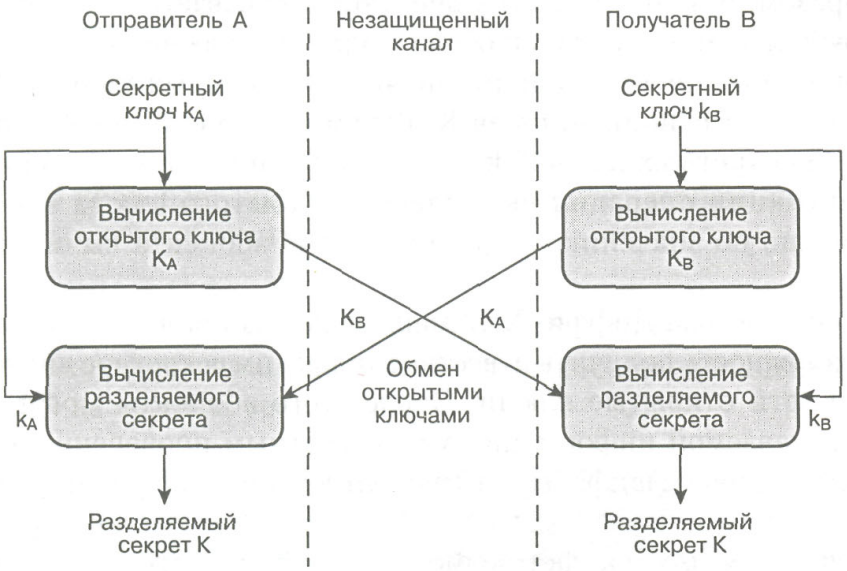


Рис. 3.11. Схема открытого распределения ключей Диффи–Хеллмана

Пользователи А и В, участвующие в обмене информации, генерируют независимо друг от друга свои случайные секретные ключи kA и kв (ключи kA и kв - случайные большие целые числа, которые хранятся пользователями А и В в секрете).

Затем пользователь А вычисляет на основании своего секретного ключа kA открытый ключ:

KA=gkA(mod N).

Одновременно "пользователь В вычисляет на основании своего секретного ключа kв открытый ключ:

KB=gkB(mod N).

Здесь N и g - большие целые простые числа. Арифметические действия выполняются с приведением по модулю N [95]. Числа N и g могут не храниться в секрете. Как правило, эти значения являются общими для всех пользователей сети или системы.

Затем пользователи А и В обмениваются своими открытыми ключами КА и Кв по незащищенному каналу и используют их для вычисления общего сессионного ключа К (разделяемого секрета):

пользователь А: К = (Кв)kA (mod N) = (gkB) kA (mod N),

пользователь В: К' = (KA)kB(mod N) = (gkA)кв (mod N),

при этом К = К', так как (gkB)kA =(gkA)kB(mod N).

Таким образом, результатом этих действий оказывается общий сессионный ключ, который является функцией обоих секретных ключей kA и kв.

Злоумышленник, перехвативший значения открытых ключей КА и Кв, не может вычислить сессионный ключ К, потому что он не имеет соответствующих значений секретных ключей kA и kв. Благодаря использованию однонаправленной функции операция вычисления открытого ключа необратима, то есть

невозможно по значению открытого ключа абонента вычислить его секретный ключ.

Уникальность метода Диффи-Хеллмана заключается в том, что пара абонентов имеет возможность получить известное только им секретное число, передавая по открытой сети открытые ключи. После этого абоненты могут приступить к защите передаваемой информации уже известным проверенным способом -применяя симметричное шифрование с использованием полученного разделяемого секрета.

Схема Диффи-Хеллмана дает возможность шифровать данные при каждом сеансе связи на новых ключах. Это позволяет не хранить секреты на дискетах или других носителях. Не следует забывать, что подобное хранение секретов повышает вероятность попадания их в руки конкурентов или злоумышленников.

Схема Диффи-Хеллмана позволяет также реализовать *метод комплексной защиты конфиденциальности и аутентичности передаваемых данных.* Алгоритм предоставляет пользователю возможность сформировать и использовать одни и те же ключи для выполнения цифровой подписи и симметричного шифрования передаваемых данных.

Для одновременной защиты целостности и конфиденциальности данных целесообразно применять шифрование и электронную цифровую подпись в комплексе. Промежуточные результаты работы схемы Диффи-Хеллмана могут быть использованы в качестве исходных данных для реализации метода комплексной защиты целостности и конфиденциальности передаваемых данных [53]. Действительно, согласно данному алгоритму пользователи А и В сначала генерируют свои секретные ключи kA и kв и вычисляют свои открытые ключи КА и Кв. Затем абоненты А и В используют эти промежуточные результаты для одновременного вычисления общего разделяемого секретного ключа К, который может использоваться для симметричного шифрования данных.

Метод комплексной защиты конфиденциальности и аутентичности передаваемых данных работает по следующей схеме:

- абонент А подписывает сообщение М с помощью своего секретного ключа kA, используя стандартный алгоритм цифровой подписи;
- абонент А вычисляет совместно разделяемый секретный ключ К по алгоритму Диффи-Хеллмана из своего секретного ключа kA и открытого ключа Кв абонента В;
- абонент А зашифровывает сообщение М на полученном совместно разделяемом секретном ключе К, используя согласованный с партнером по обмену алгоритм симметричного шифрования;
- абонент В при получении зашифрованного сообщения М вычисляет по алгоритму Диффи-Хеллмана совместно разделяемый секретный ключ К из своего секретного ключа kв и открытого ключа КА абонента А;
- абонент В расшифровывает полученное сообщение М на ключе К;

- абонент B проверяет подпись расшифрованного сообщения M с помощью открытого ключа абонента KA.

На основе схемы Диффи-Хеллмана функционируют протоколы управления криптоключами SKIP (Simple Key management for Internet Protocols) и IKE (Internet Key Exchange), применяемые при построении защищенных виртуальных сетей VPN на сетевом уровне.

Протокол вычисления ключа парной связи ECKEP

В *протоколе вычисления ключа эллиптической кривой ECKEP* (Elliptic Curve Key Establishment Protocol) определение параметров системы и генерация ключей аналогичны алгоритму асимметричного шифрования ECES.

Предположим, что общий ключ вычисляется пользователями A и B.

Пользователь A имеет секретный ключ a и открытый ключ QA = aP = (xA, yA). Аналогично пользователь B имеет секретный ключ b и открытый ключ QB = bP = = (xB, yB).

Вычисление ключа парной связи проводится в четыре этапа:

Этап 1. Действия пользователя A:

- выбирается случайное целое число kA, $1 \leq kA \leq n - 1$;
- вычисляется точка RA = kAP;
- вычисляется точка (x1, y1)= kAQB;
- вычисляется sA = kA + axAx1 mod n;
- RA отправляется пользователю B.

Этап 2. Действия пользователя B:

- выбирается случайное целое число kв, $1 \leq kв \leq n - 1$;
- вычисляется точка RB = kBP;
- вычисляется точка (x2, y2) = kвQA;
- вычисляется sB = kв + bxBx2 mod n;
- RB отправляется пользователю A.

Этап 3. Действия пользователя A:

- вычисляется (x2, y2) = aRB;
- вычисляется ключ парной связи K = sA(RB + xBx2QB).

Этап 4. Действия пользователя B:

- вычисляется (x1, y1) = bRA;
- вычисляется ключ парной связи K = sB(RA + xAx1QA) значению sA(RB + xBx2QB).

Важным достоинствами схемы распределения ключей Диффи-Хеллмана и протокола вычисления ключа парной связи ECKEP является то, что они позволяют обойтись без защищенного канала для передачи ключей. Однако необходимо иметь гарантию того, что пользователь A получил открытый ключ именно от пользователя B, и наоборот. Эта проблема решается с помощью сертификатов открытых ключей, создаваемых и распространяемых центрами сертификации CA (Certification Authority) в рамках инфраструктуры управления открытыми ключами PKI (Public Key Infrastructure).

Лекция 13

Основные подходы к защите данных от НСД. Защита ПЭВМ от несанкционированного доступа

Как показывает практика, несанкционированный доступ (НСД) представляет одну из наиболее серьезных угроз для злоумышленного завладения защищаемой информацией в современных АСОД. Как ни покажется странным, но для ПЭВМ опасность данной угрозы по сравнению с большими ЭВМ повышается, чему способствуют следующие объективно существующие обстоятельства:

1) подавляющая часть ПЭВМ располагается непосредственно в рабочих комнатах специалистов, что создаст благоприятные условия для доступа к ним посторонних лиц;

2) многие ПЭВМ служат коллективным средством обработки информации, что обезличивает ответственность, в том числе и за защиту информации;

3) современные ПЭВМ оснащены несъемными накопителями на ЖМД очень большой емкости, причем информация на них сохраняется даже в обесточенном состоянии;

4) накопители па ГМД производятся в таком массовом количестве, что уже используются для распространения информации так же, как и бумажные носи гели;

5) первоначально ПЭВМ создавались именно как персональное средство автоматизации обработки информации, а потому и по оснащались специально средствами защиты от НСД.

В силу сказанного те пользователи, которые желают сохранить конфиденциальность своей информации, должны особенно позаботиться об оснащении используемой ПЭВМ высокоэффективными средствами защиты от НСД.

Основные механизмы защиты ПЭВМ от НСД могут быть представлены следующим перечнем:

1) физическая защита ПЭВМ и носителей информации;

2) опознавание (аутентификация) пользователей и используемых компонентов обработки информации;

3) разграничение доступа к элементам защищаемой информации;

4) криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных);

5) криптографическое закрытие защищаемой информации в процессе непосредственной ее обработки;

6) регистрация всех обращений к защищаемой информации.

1. **Физическая защита ПЭВМ и носителей информации**. Содержание физической защиты общеизвестно потому детально обсуждать ее здесь нет необходимости. Заметим только, что ПЭВМ лучше размещать в надежно запираемом помещении, причем в рабочее время помещение должно быть

закрыто или ПЭВМ должна быть под наблюдением законного пользователя. При обработке же закрытой информации в помещении могут находиться только лица, допущенные к обрабатываемой информации. В целях повышения надежности физической защиты в нерабочее время 1 ГЭВМ следует хранить в опечатанном сейфе.

2. Опознавание (аутентификация) пользователей и используемых компонентов обработки информации. В концептуальном плане решение данной задачи принципиально не отличается от аналогичной задачи, решаемой в любой ЛС'ОД: система защиты должна надежно определять законность каждого обращения к ресурсам, а законный пользователь должен иметь возможность убедиться, что ему предоставляются именно те компоненты (аппаратура, программы, массивы данных), которые ему необходимы.

Для опознавания пользователей к настоящему времени разработаны и нашли практическое применение следующие способы:

1) с использованием простого пароля;

2) в диалоговом режиме с использованием нескольких паролей и/или персональной информации пользователей;

3) по индивидуальным особенностям и физиологическим характеристикам человека (отпечатки пальцев, геометрия руки, голос, персональная роспись, структура сетчатки глаза, фотография и некоторые другие);

4) с использованием радиокодовых устройств;

5) с использованием электронных карточек.

Рассмотрим коротко перечисленные способы.

Распознавание по простому паролю заключается в том, что каждому зарегистрированному пользователю выдается персональный пароль, который он должен держать в тайне и вводить в ЗУ ЭВМ при каждом обращении к ней . Специальная программа сравнивает введенный пароль с эталоном, хранящимся в ЗУ ЭВМ, и при совпадении паролей запрос пользователя принимаем си к исполнению. Простота способа очевидна, но очевидны неявные недостатки: пароль можем быть утерян или подобран перебором возможных комбинаций, а искусный злоумышленник можем проникнуть в ту область ЗУ, в которой хранятся эталонные пароли. Попытки преодолеть указанные недостатки, естественно, ведут к усложнению способа.

Опознавание в диалоговом режиме может быть осуществлено но следующей схеме. В файлах механизмов защиты заблаговременно создаются записи, содержащие персонифицирующие пользователи данные (цата рождения, рост, вес, имена и даты рождения родных и близких и т.п.) или достаточно большой и упорядоченный набор паролей. При обращении пользователи программа механизма защиты предлагает пользователю назвать некоторые данные из имеющейся записи, которые сравниваются с .хранящимися в файле. По результатам сравнения принимается решение о допуске. Для повышения надежности опознавания запрашиваемые у пользователя данные могут выбираться каждый раз разные. Достоинства и недостатки данного способа очевидны.

Опознавание по индивидуальным особенностям и физиологическим характеристикам может быть весьма надежным, но для его реализации необходима специальная аппаратура для съема и ввода соответствующих параметров и достаточно сложные программы их обработки и сравнении с эталоном. Все это в настоящее время вполне разрешимо, однако сопряжено с удорожанием и усложнением аппаратуры и программ ПЭВМ. В силу сказанного данный способ применительно к ПЭВМ пока не получил сколько-нибудь значительного распространения, Заманчивым но сравнительной простите и доступности может оказаться опознавание пользователя по параметрам его работы с клавиатурой ПЭВМ (скорость набора текста, интервалы между нажатием клавиш и др.), которые тоже носят сугубо индивидуальный характер.

Опознавание по радиокодовым устройствам, как но следует из самого названия, заключаемся в том, что изготавливают специальные устройства, каждое из которых может генерировать радиосигналы, имеющие индивидуальные характеристики. ПЭВМ оснащается программно-аппаратными средствами приема (например, при приближении к экрану дисплея), регистрации и обработки сигналов. Каждому зарегистрированному пользователю выдается такое устройство, а его параметры заносятся в ЗУ механизмов защиты. Надежность опознавания по данному способу может быть высокой, однако такие устройства персонифицируют владельца, а не персону, полому похищение устройства дает злоумышленнику реальные шансы несанкционированного доступа.

Опознавание по специальным идентификационным карточкам заключается в том, что изготавливаются специальные карточки, на которые наносятся данные, персонифицирующие пользователя: персональный идентификационный номер, специальный шифр или код и т.п. Эти данные на карточку заносятся в зашифрованном виде, причем ключ шифрования может быть дополнительным идентифицирующим параметром, поскольку он может быть известен только пользователю, вводится им каждый раз при обращении к системе и уничтожается сразу же после использования. Опознавание по карточкам может быть очень надежным, однако для его реализации необходимы предприятия - изготовители карточек, а ПЭВМ должна быть оснащена устройством считывания данных с карточки. Поскольку все это сопряжено со значительными дополнительными расходами, то данный способ опознавания оказывается эффективным при его использовании в больших территориально распределенных сетях, где он в последнее время находит все большее применение, причем особенно в автоматизированных банковских системах. Более детально он будет рассмотрен в § 8.7.

Для опознавания компонентов обработки данных, т.е. ЭВМ, ОС, программ функциональной обработки, массивов данных (такое опознавание особенно актуально при работе в сети ЭВМ) используются следующие средства:

1) специальные аппаратные блоки-приставки 0с"я опознавания ЭВМ, терминалов, внешних устройств);

2) специальные программы, реализующие процедуру "запрос-ответ";

3) контрольные суммы (для опознавания щкмрамм и массивов данных).

Опознавание с помощью блоков-приставок заключается в том, что технические средства оснащаются специальными устройствами, генерирующими индивидуальные сигналы. В целях предупреждения перехвата этих сигналов и последующего их злоумышленного использования они могут передаваться в зашифрованном виде, причем периодически может меняться не только ключ шифрования, но и используемый способ (алгоритм) криптографического преобразования.

Программное опознавание по процедуре "запрос-ответ" заключается в ТОМ, что в ЗУ опознающего и опознаваемого объектов заблаговременно вносится достаточно развитые массивы идентифицируемых данных. Тогда опознающий объект в диалоговом режиме запрашивает те или иные данные из массива опознаваемого объекта и сравнивает их с соответствующими данными своего массива. Опять-таки в целях предупреждения перехвата и злоумышленного использования передаваемых идентифицирующих данных может осуществляться их кришографическос закрытие. *Опознавание по контрольной сумме* заключается в том, что для про-|рамм и массивов данных заблаговременно вычисляются их контрольные суммы (или другие величины, зависящие от содержания опознаваемых объектов). Дальнейшая процедура опознавания очевидна.

3. Разграничение доступа к злеменпшм защищаемой информации. Сущность указанного разграничения заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможности беспрепятственного доступа к информации в пределах его полномочий, и исключить возможности превышения своих полномочий. И лих целях разработаны и реализованы на практике методы и средства разграничения доступа к устройствам ЭВМ, к программам обработки информации, к нолям (областям ЗУ) и к массивам (базам) данных. Само разграничение можег осуществляться несколькими способами, а именно:

1) но уровням (кольцам) секретности;

2) по специальным спискам;

3) гго так называемым матрицам полномочий;

4) по специальным мандатам. .

Приведем краткую характеристику перечисленных способов.

Разграничение доступа по уровням (кольцам) секретности заключается в юм, что защищаемые данные распределяются по массивам (базам) таким образом, чтобы в каждом массиве (каждой базе) содержались данные одного уровня секретности (например, только с грифом "конфиденциально", или только "секретно", или только "совершенно секретно", ИЛИ каким-либо другим). Каждому зарегистрированному пользователю предоставляется вполне определенный уровень допуска (например, "секретно", "совершенно секретно" и т.н.). Тогда пользователю разрешается доступ к массиву (базе) своего уровня гг массивам (базам) низших уровней, и запрещается доступ к массивам (базам) более высоких уровней.

Разграничение доступа по специальным спискам заключается в том, что дня каждого элемента защищаемых данных (файла, базы, прсмрим мы) составляется список всех тех пользователей, которым предоставлено

право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа.

Разграничение доступа по матрицам полномочий предполагает формирование двумерной матрицы, по строкам которой содержатся идентификаторы зарегистрированных пользователей, а по столбцам - идентификаторы защищаемых элементов данных. Элементы матрицы содержат информацию об уровне полномочий соответствующего пользователя относительно соответствующего элемента. Например, при размерах элементов матрицы в два бита их содержание может быть следующим: 00 - доступ запрещен, 01 - разрешено только чтение, 10 - разрешена только запись, 11 - разрешены и чтение и запись.

Разграничение доступа по мандатам есть способ разового разрешения на допуск к защищаемому элементу данных. Заключается он в том, что каждому защищаемому элементу присваивается персональная уникальная метка, после чего доступ к этому элементу будет разрешен только тому пользователю, который в своем запросе предъявит метку элемента (мандат), которую ему может выдать администратор защиты или владелец элемента.

4. Криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных). Данный механизм, как следует из самого названия, предназначается для обеспечения защиты информации, которая подлежит продолжительному хранению на машинньгх носителях. Но при разработке методов его реализации имелась в виду и еще одна весьма важная цель - уменьшение объемов ЗУ, занимаемых хранимой информацией. Указанные цели и выступают в качестве основных критериев при поиске оптимальных вариантов решения задачи архивации данных.

Для предупреждения несанкционированного доступа к хранимой информации могут и должны использоваться все три рассмотренных выше механизма. Но особенно эффективными оказались методы криптографического преобразования информации, поэтому они составляют основу практически всех известных механизмов архивации. Уменьшение объемов ЗУ достигается применением так называемых методов сжатия данных, сущность которых заключается в использовании таких систем кодирования архивируемых данных, которые при сохранении содержания информации требуют меньшего объема носителя. Но тогда естественной представляется идея вьгбора такого способа кодирования, который удовлетворял бы обоим гребованиям: обеспечивал бы уменьшение объема ЗУ и обладал бьг требуемой надежностью криптографической защиты.

Классическим примером такого способа кодирования может служить достаточно известный код Хоффмана, сугь которого заключается в том, что для кодирования часто встречающихся символов (букв) используются более короткие кодовые комбинации, чем для кодирования редко встречающихся.

Нетрудно видеть, что если таблицу кодирования держать а секрете, го ^кодированный гаким образом'текст будет не только короче исходного, но и недоступен для чтения посторонними лицами.

5. Криптографическое закрытие защищаемой информации в процессе непосредственной ее обработки. Назначение указанного закрытия очевидно, а целесообразность применения определяется возможностями несанкционированного доступа к защищаемой информации в процессе непосредственной обработки. Если же обработка информации осуществляется в сетевой среде, то без применения криптографических средств надежное предотвращение несанкционированного доступа к ней практически не может быть обеспечено. Этим и обусловлено то достаточно большое внимание, которое уделяется разработке криптографических средств, ориентированных на применение в ПЭВМ

Рассмотрим краткое описание одной из серий криптографических устройств, получившей название "КРИПТОН".

КРИПТОН - это ряд выполненных в виде одноплатных устройств программно-аппаратных комплексов, обеспечивающих шифрование и дешифрование информации в ЭВМ и в информационно-вычислительных сетях. Устройства содержат датчики случайных чисел для генерации ключей и узлы шифрования, реализованные аппаратно в специализированных однокристальных микроЭВМ. Открытый интерфейс позволяет внедрять устройства КРИПТОН в любые системы и дополнять программным обеспечением специального назначения.

Устройства КРИПТОН позволяют осуществлять:

1) шифрование и дешифрование файлов, групп файлов и разделов дисков;

2) разграничение и контроль доступа к компьютеру;

3) защиту информации, передаваемой но открытым каналам связи и сетям межмашинного обмена;

4) электронную подпись документов;

5) прозрачное шифрование жестких и гибких дисков.

Для криптографического преобразования защищаемых данных использован алгоритм отечественного стандарта ГОСТ 28147-89. Длина ключа - 256 бит, причем предусмотрено 7 типов ключевых систем, любую из которых пользователь может выбрать по своему усмотрению. Конкретные ключи в пределах выбранного типа ключевой системы пользователь может изготовить самостоятельно или заказать в специализированном центре.

КРИПТОН работает в среде MS DOS версии 3.0 и выше.

На базе устройств КРИПТОН разработана и серийно выпускается система КРИПТОН-ИК, обеспечивающая дополнительно к перечисленным выше функциям также чтение, запись и защиту данных, хранящихся на так называемых интеллектуальных идентификационных карточках, получающих в последнее время широкое применение как в виде дебетно-кредитных карточек при безналичных расчетах, так и в виде средства хранения прав доступа, ключей шифрования и другой конфиденциальной информации.

6. Регистрация всех обращений к защищаемой информации. Регистрация обращений к защищаемой информации позволяет решать ряд важных задач, способствующих существенному повышению эффективности защиты, поэтому оно непременно присутствует во всех системах защиты информации.

Основные задачи, при решении которых заметную роль играет регистрация обращений, могут быть представлены следующим перечнем:

1) контроль использования защищаемой информации;

2) выявление попыток несанкционированного доступа к защищаемой информации;

3) накопление статистических данных о функционировании систем защиты.

Вообще говоря, регистрация обращений может быть осуществлена серийными средствами операционных систем ПЭВМ. Однако учитывая специфичность и избирательность необходимой регистрации в системах защиты, разработчики этих систем предпочитают создавать свои версии программ регистрации.

Таким образом, даже такое беглое рассмотрение вопросов предупреждения несанкционированного доступа достаточно убедительно показывает, что они, во-первых, составляют основу систем защиты инфорнации в ПЭВМ, а во-вторых, что их реализация сопряжена с решением широкою спектра разноплановых задач. Теоретические исследования и практический опыт показали, что наиболее эффективным способом их решения является создание комплексных систем защиты ПЭВМ от несанкционированного доступа.