

# МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В АС

## 1. Защита от угрозы нарушения конфиденциальности

Защита машинных носителей информации (МНИ).

Особенности:

- последовательный либо прямой метод доступа;
- различные физические принципы реализации;
- различие объемов хранимой информации;
- многообразие вариантов реализации фирмами.

Задача злоумышленника:

- 1) выбор соответствующего данному носителю привода;

- 2) запуск соответствующего комплекта программ (операционных средств, драйверов и т.п.);
- 3) осуществление (организация) считывания в память КС содержимого носителей.

Отсюда тактика защиты. Существуют носители (накопители) со встроенными средствами защиты, требующими специальных паролей.

## **Парольные системы для защиты от НСД.**

Под НСД в руководящих документах понимают доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств. НСД может быть случайным либо преднамеренным.

## **Категории методов защиты от НСД:**

- организационные ( мероприятия и регламентирующие инструкции);
- технологические (программно-аппаратные средства идентификации, аутентификации и охранной сигнализации);
- правовые (меры контроля за исполнением нормативных актов).

**Идентификация** - присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

**Аутентификация** - проверка принадлежности пользователю предъявленного им идентификатора.

**Безопасность** (стойкость) системы идентификации и аутентификации это степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя.

Методы **аутентификации** основаны на наличии у каждого пользователя:

- индивидуального объекта заданного типа (пропуск, магнитная карта и т.п.);
- знаний некоторой информации (пароля), известного только ему и проверяющей стороне;
- индивидуальных биометрических характеристик (тембра голоса, рисунка папиллярных линий, структуры радужной оболочки глаза и т.п.).

Если в процедуре аутентификации участвуют только две стороны, то это **непосредственная аутентификация** (direct password authentication).

Если в этой процедуре участвует третья *доверенная* сторона, то ее называют **сервером аутентификации**, а метод называют *с участием доверенной стороны* (trusted third party authentication).

# Общие подходы к построению парольных систем.

Наиболее распространенные методы аутентификации основаны на применении многоразовых и одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные системы часто становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

- по хранимой копии пароля или его свёртке (**plaintext- equivalent**);
- по некоторому проверочному значению (**verifier-based**) ;

- Без непосредственной передачи информации о пароле проверяющей стороне (zero-knowledge);
- С использованием пароля для получения криптографического ключа (cryptographic).

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

**Идентификатор пользователя** – некоторое уникальное количество информации позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификаторы также наз. именем пользователя или именем учетной записи пользователя .

**Пароль пользователя** – некоторое секретное кол-во информации известное только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена для прохождения процедуры аутентификации. **Одноразовый пароль** дает возможность пользователю однократно пройти аутентификацию. **Многоразовый пароль** может быть использован для проверки подлинности повторно.

**Учетная запись пользователя** – совокупность его идентификатора и его пароля.

**База данных пользователей** парольной системы содержит учетные записи всех пользователей данной парольной системы.

**Под парольной системой** будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многократных паролей. Как правило такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансов) криптографических ключей.

## **Основными компонентами парольной системы являются:**

- интерфейс пользователя;
- интерфейс администратора;
- модуль сопряжения с другими подсистемами безопасности;
- база данных учетных записей.

Парольная система представляет собой “передний край обороны” всей системы безопасности. Некоторые ее элементы( в частности реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику.

Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему.

## **Типы угроз безопасности парольных систем.**

### **1. Разглашение параметров учетной записи через :**

- Подбор в интерактивном режиме
- Подсматривание
- Преднамеренную передачу пароля ее владельцем другому лицу
- Захват базы данных парольной системы с дальнейшей дешифрацией

- Перехват переданной по сети информации о пароле
- Хранение пароля в доступном месте

## 2. Вмешательство в функционирование компонентов парольной системы через

- Внедрение программных закладок
- Обнаружение и использование ошибок, допущенных на стадии разработки
- Выведение из строя парольной системы

Некоторые из перечисленных типов угроз связаны с наличием так называемого **человеческого фактора**, проявляющегося в том, что пользователь может:

- Выбрать пароль, который легко запомнить и также легко подобрать,
- Записать пароль, который сложно запомнить, и положить запись в доступном месте,
- Ввести пароль так, что его смогут увидеть посторонние,
- Передать пароль другому лицу намеренно или под влиянием заблуждения

# Выбор паролей

Для уменьшения влияния человеческого фактора при выборе и использовании паролей необходимо выполнить ряд требований:

- установить оптимальную длину пароля;
- использовать в паролях различные группы СИМВОЛОВ;
- проверка и отбраковка паролей по словарю;
- установить максимальный и минимальный срок действия пароля;
- ведение журнала истории паролей;
- применять алгоритмы, бракующие пароли на основании данных журнала историй;

- ограничение числа попыток ввода пароля;
- поддержка режима принудительной смены пароля пользователя;
- использование вопросо-ответного диалога при вводе неправильного пароля (для замедления цикла подбора);
- запрет на выбор пароля самим пользователем и автоматическая генерация паролей;
- принудительная смена пароля при первой регистрации пользователя в системе (для защиты от неправомерных действий системного администратора, имеющего доступ к паролю в момент создания учетной записи).

**Оценка стойкости парольных систем осуществляется по формуле:**

$$P = V * T / S, \text{ где } S = A^L$$

Здесь  $A$  - мощность алфавита паролей;

$L$  - длина пароля;

$S$  - мощность пространства паролей;

$V$  - скорость подбора паролей;

$T$  - срок действия пароля;

$P$  - вероятность подбора пароля в течение его срока действия.

## ПРИМЕР:

Пусть задано  $P = 0.000001$ . Найти минимальную длину пароля, обеспечивающую его стойкость в течение одной недели непрерывных попыток подобрать пароль. Пусть скорость интерактивного подбора паролей  $V = 10$  паролей/мин. Тогда в течение недели можно подобрать:

$$10 * 60 * 24 * 7 = 100800 \text{ паролей.}$$

Тогда из формулы 1 имеем:

$$S = 100800 / 0.000001 = 1.008 * E+11$$

Полученному значению  $S$  соответствуют пары:

$$A = 26, L = 8 \quad \text{и} \quad A = 36, L = 6.$$

# Хранение паролей

Важным аспектом стойкости парольной системы, является способ хранения паролей в базе данных учетных записей. Варианты хранения паролей:

- 1) в открытом виде;
- 2) в виде сверток (хеширование);
- 3) зашифрованными в некотором ключе.

*Особенности второго и третьего вариантов.*

**Хеширование** не обеспечивает защиту от подбора паролей по словарю в случае получения базы данных злоумышленником.

При выборе алгоритма хеширования необходимо: -  
гарантировать несовпадение значений сверток,  
полученных на основе различных паролей поль-  
зователей;

- предусмотреть механизм, обеспечивающий  
уникальность сверток в том случае, если два  
пользователя выбирают одинаковые пароли,  
предусмотрев некоторое количество “случайной”  
информации.

Варианты шифрования базы данных учетных  
записей:

1) ключ генерируется программно и хранится в  
системе, обеспечивая возможность ее автома-  
тической перезагрузки;

2) ключ генерируется программно и хранится на внешнем носителе, с которого считывается при каждом запуске;

3) ключ генерируется на основе выбранного администратором пароля, который вводится в систему при каждом запуске.

**Наиболее безопасное** хранение паролей обеспечивается при комбинации второго и третьего способов.

Стойкость парольной системы определяет ее способность противостоять атаке противника, а также зависит от криптографических свойств алгоритма шифрования или хеширования.

# Передача пароля по сети.

Если передаваемая по сети в процессе аутентификации информация не защищена надлежащим образом, возникает угроза ее перехвата и использования для нарушения защиты парольной системы.

Многие компьютерные системы позволяют переключать сетевой адаптер в режим прослушивания адресованного другим получателям сетевого трафика.

Основные виды защиты сетевого трафика:

- физическая защита сети;
- оконечное шифрование;
- шифрование пакетов.

## **Способы передачи паролей по сети :**

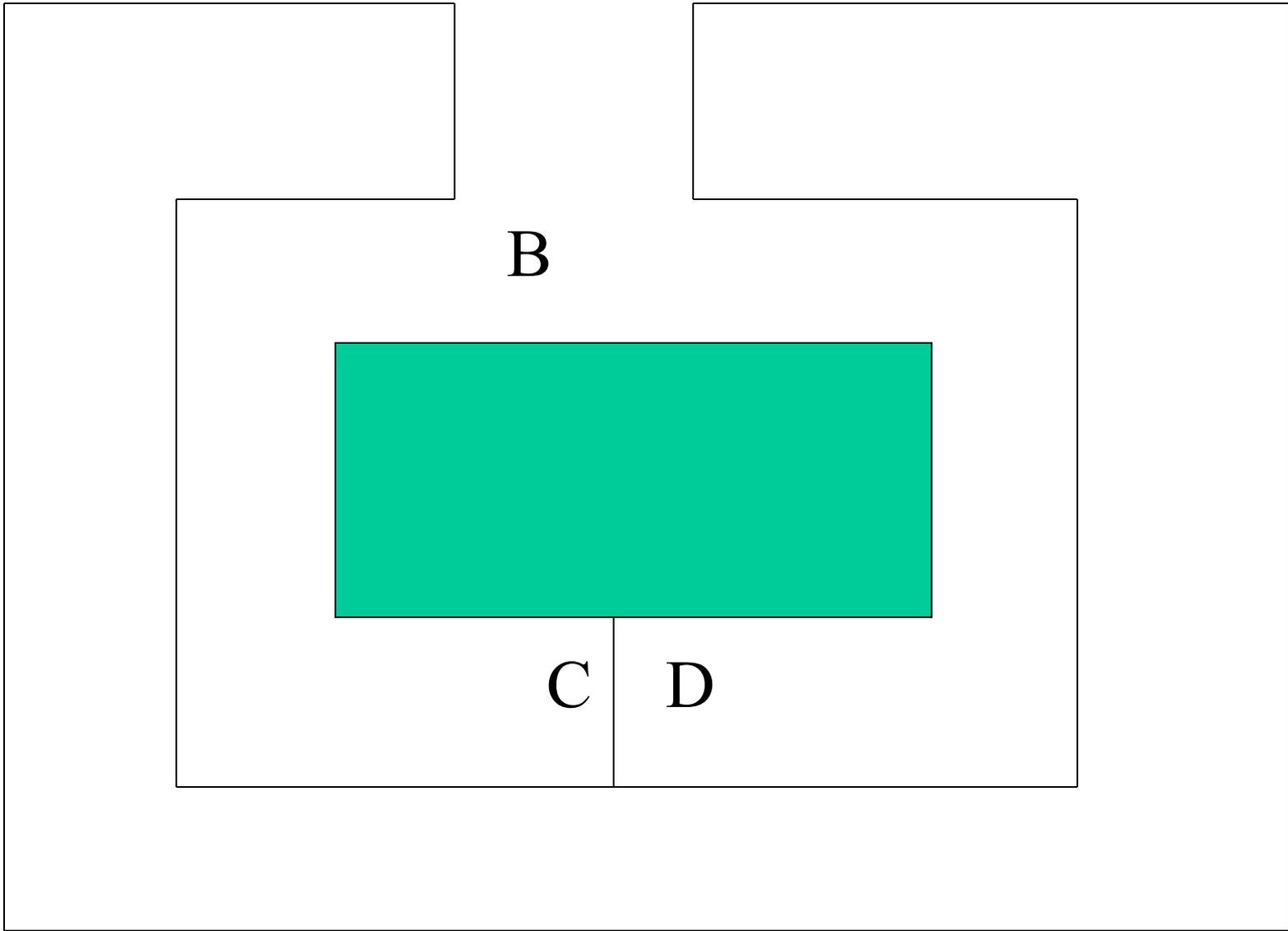
- 1) в открытом виде; (TELNET, FTP и других)
- 2) зашифрованными;
- 3) в виде сверток;
- 4) без непосредственной передачи информации о пароле (“доказательство с нулевым разглашением”).

При передаче паролей в зашифрованном виде или в виде сверток по сети с открытым физическим доступом возможна реализация следующих угроз безопасности парольной системы.

•

- - перехват и повторное использование информации;
- - перехват и восстановление паролей;
- - модификация информации с целью введения в заблуждение проверяющей стороны;
- - имитация злоумышленником действий проверяющей стороны для введения в заблуждение пользователя.
- **Схемы с нулевым разглашением** впервые появились в на рубеже 80-90-х годов. **Идея:** обеспечить возможность одному из пары субъектов доказать истинность некоторого утверждения второму, умалчивая при этом о содержании самого утверждения.

- **Общая схема процедуры аутентификации с нулевым разглашением** состоит из последовательности информационных обменов (итераций) между двумя участниками процедуры, по завершению которой проверяющий **с заданной вероятностью** делает правильный вывод об истинности проверяемого утверждения. С увеличением числа итераций возрастает вероятность правильного распознавания истинности (или ложности) утверждения.
- Классическим примером неформального описания системы аутентификации с нулевым разглашением служит так называемая пещера **АЛИ-БАБЫ**.



Пещера имеет один вход, путь от которого разветвляется в глубине пещеры на два коридора, сходящихся затем в одной точке, где установлена дверь с замком. Каждый, кто имеет ключ от замка, может переходить из одного коридора в другой в любом направлении. Одна итерация алгоритма состоит из последовательности шагов:

1. Проверяющий становится в точку А.
2. Доказывающий проходит пещеру и добирается до двери (оказывается в точке С или D). Проверяющий не видит, в какой из двух коридоров тот свернул.

3. Проверяющий приходит в точку В и в соответствии со своим выбором просит доказывающего выйти из определенного коридора.

4. Доказывающий, если нужно, открывает дверь ключом и выходит из названного проверяющим коридора.

Итерация повторяется столько раз, сколько требуется для распознавания истинности утверждения «доказывающий владеет ключом от двери» с заданной вероятностью. После  $i$ -той итерации вероятность того, что проверяющий попросит доказывающего выйти из того же коридора, в который вошел доказывающий, равна  $(1/2)^i$ .

Еще один способ повышения стойкости парольных систем в сети - применение одноразовых **(one-time)** паролей. Общий подход к их применению основан на последовательном использовании **хеш-функции** для вычисления **одноразового пароля на основе предыдущего:**

Вначале пользователь получает упорядоченный список одноразовых паролей, последний из которых также сохраняется в системе аутентификации. При каждой регистрации пользователь вводит очередной пароль, а система вычисляет его свойства и сравнивает с хранимым у себя эталоном.