РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

Митюшин Дмитрий
Алексеевич

Защита информации от несанкционированного доступа

Тема 3. Методы идентификации и аутентификации пользователя

Вопросы:

1. *Требования к идентификации и аутентификации*
2. *Классификация задач, решаемых механизмами идентификации и аутентификации*
3. *Парольная защита*

Литература

1. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от НСД к информации. — Москва, 1992.
2. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Москва, 1992.

1. Требования к идентификации и аутентификации

1.1. Понятие идентификации и аутентификации. Процедура авторизации

Идентификация призвана каждому пользователю (группе пользователей) сопоставить соответствующую ему разграничительную политику доступа на защищаемом объекте. Для этого пользователь должен себя идентифицировать – указать своё «имя» (идентификатор).

Таким образом проверяется, относится ли регистрирующийся пользователь к пользователям, идентифицируемым системой. В соответствии с введённым идентификатором пользователю будут сопоставлены соответствующие права доступа.

Аутентификация предназначена для контроля процедуры идентификации. Для этого пользователь должен ввести секретное слово – пароль. Правильность вводимого пароля подтверждает однозначное соответствие между регистрирующимся пользователем и идентифицированным пользователем.

В общем случае, как будет показано далее, идентифицируются и аутентифицируются не только пользователи, но и другие субъекты доступа к ресурсам.

1. Требования к идентификации и аутентификации

1.1. Понятие идентификации и аутентификации. Процедура авторизации

Совокупность выполнения процедур идентификации и аутентификации принято называть процедурой **авторизации**. При этом заметим, что иногда не требуется идентифицировать пользователя, а достаточно только выполнения процедуры аутентификации.

Например, это происходит когда требуется подтвердить текущего (уже зарегистрированного) пользователя при выполнении каких-либо действий, требующих дополнительной защиты. В свою очередь, не всегда требуется осуществлять контроль идентификации, то есть в некоторых случаях аутентификация может не производиться.

Процедура авторизации имеет ключевое значение при защите компьютерной информации, т.к. вся разграничительная политика доступа к ресурсам реализуется относительно идентификаторов пользователей. То есть, войдя в систему с чужим идентификатором, злоумышленник получает права доступа к ресурсу того пользователя, идентификатор которого был им предъявлен при входе в систему.

1. Требования к идентификации и аутентификации

1.2. Формализованные требования

Формализованные требования к данным механизмам защиты состоят в следующем:

- Должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов (для АС классов защищённости 1Г и 1В).
- Система защиты должна требовать от пользователей идентифицировать себя при запросах на доступ.
- Система защиты должна подвергать проверке подлинность идентификации – осуществлять аутентификацию. Для этого она должна располагать необходимыми данными для идентификации и аутентификации.
- Система защиты должна препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась (для 5 класса защищённости по классификации СВТ). Для 3 класса защищённости по классификации СВТ вводится дополнительное требование: система защиты должна обладать способностью надёжно связывать полученную идентификацию со всеми действиями данного пользователя.

1. Требования к идентификации и аутентификации

1.2. Формализованные требования

Очевидно, что кроме ограничения «...паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов...» данные требования никак не формализуют подходы к реализации механизмов парольной защиты.

Кроме того, данные требования не определяют, каким образом должны быть реализованы механизмы парольной защиты, а также не накладывают дополнительных ограничений, связанных с повышением стойкости пароля к подбору.

В частности, они не регламентируют использование внешних носителей парольной информации – дискет, смарт-карт и т.д.

1. Требования к идентификации и аутентификации

1.3. Дополнительные требования

Как отмечалось ранее, существует целая группа угроз, связанная с некорректностью реализации процедуры авторизации в современных ОС, а также с наличием ошибок в реализации соответствующих механизмов защиты. Это обусловливает целесообразность рассмотрения механизмов авторизации с целью их добавочной защиты. Кроме того, механизмы идентификации и аутентификации являются важнейшими для противодействия НСД к информации, а значит, следует рассматривать возможные варианты их резервирования (как «горячего», так и «холодного»).

Кроме того, в рамках декларируемого системного подхода к проектированию системы защиты (рассмотренного нами в четвертой главе), при раз-работке механизмов авторизации следует рассматривать как явные, таки скрытые угрозы преодоления защиты.

И ещё: в рамках системного подхода следует рассматривать не отдельно механизм авторизации как таковой, а необходимую и достаточную совокупность механизмов защиты, призванных в комплексе решать рассматриваемую задачу защиты. Далее мы покажем, что как бы хорошо не был исполнен механизм авторизации, в отдельности он не позволяет обеспечить надёжную защиту от несанкционированного входа пользователя в систему.

1. Требования к идентификации и аутентификации

1.4. Авторизация в контексте количества и вида зарегистрированных пользователей. Кого следует воспринимать в качестве потенциального злоумышленника

В системе зарегистрирован один пользователь

В общем случае в системе может быть зарегистрирован один либо несколько пользователей.

Случай, когда в системе зарегистрирован только один пользователь, характеризуется тем, что данный пользователь является и прикладным пользователем, и администратором безопасности.

Здесь источником потенциальной угрозы является только сторонний сотрудник предприятия, а вся задача защиты сводится к контролю доступа в компьютер (либо в систему), т.е. к парольной защите.

Данный случай нами не рассматривается, т.к. в соответствии с формализованными требованиями к защите информации от НСД даже при защите конфиденциальной информации предполагается обязательное наличие администратора безопасности.

1. Требования к идентификации и аутентификации

1.4. Авторизация в контексте количества и вида зарегистрированных пользователей. Кого следует воспринимать в качестве потенциального злоумышленника

В системе зарегистрированы администратор безопасности и один прикладной пользователь

Общий случай функционирования системы с одним прикладным пользователем – это наличие в системе администратора безопасности и только одного прикладного пользователя. В задачи администратора безопасности здесь входит ограничение прав прикладного пользователя по доступу к системным и иным ресурсам компьютера. В частности, может ограничиваться набор задач, разрешённых для решения на компьютере, набор устройств, которые могут быть подключены к компьютеру (например, внешний модем, принтер и т.д.), способ сохранения обрабатываемых данных (например, на дискетах только в шифрованном виде) и т.д.

В данном случае потенциальным злоумышленником в части несанкционированного использования ресурсов защищаемого объекта может являться как сторонний сотрудник предприятия, так и собственно прикладной пользователь. Заметим, что прикладной пользователь здесь может выступать в роли сознательного нарушителя, либо стать «инструментом» в роли стороннего нарушителя, например, запустив по чьей-либо просьбе какую-нибудь программу.

1. Требования к идентификации и аутентификации

1.4. Авторизация в контексте количества и вида зарегистрированных пользователей. Кого следует воспринимать в качестве потенциального злоумышленника

В системе зарегистрированы администратор безопасности и несколько прикладных пользователей

Кроме администратора безопасности, в системе может быть заведено несколько прикладных пользователей. При этом ресурсами защищаемого компьютера могут пользоваться несколько сотрудников, решая различные задачи.

Ввиду этого информационные и иные ресурсы защищаемого объекта должны между ними разграничиваться.

В данном случае к потенциальным нарушителям добавляется санкционированный прикладной пользователь, целью которого может служить НСД к информации, хранимой на защищаемом объекте другим пользователем.

1. Требования к идентификации и аутентификации

1.4. Авторизация в контексте количества и вида зарегистрированных пользователей. Кого следует воспринимать в качестве потенциального злоумышленника

При использовании компьютера (прежде всего, рабочей станции) в составе ЛВС, помимо локальных ресурсов защищаемого объекта, защите подлежат сетевые ресурсы.

В этом случае между пользователями могут разграничиваться права по доступу к серверам, сетевым службам, разделённым сетевым ресурсам (общим папкам и устройствам, например, к сетевым принтерам) и т.д.

Здесь злоумышленник (санкционированный пользователь) может осуществлять попытку получить НСД к сетевому ресурсу, к которому ему доступ неразрешён, с целью осуществления на него атаки с рабочей станции.

1. Требования к идентификации и аутентификации

1.5. Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей

Отметим, что наиболее простой в реализации защитой является защита от стороннего сотрудника. В этом случае все мероприятия по защите возлагаются на использование механизма парольного входа.

Простота же состоит в том, что, как увидим далее, в этом случае следует оказывать противодействие только явным угрозам преодоления парольной защиты, от которых защититься не представляет большого труда.

Однако основной угрозой служат преднамеренные или неумышленные действия санкционированного пользователя, который обладает возможностью осуществления скрытой атаки на защищаемый ресурс (например, запустив какую-либо программу собственной разработки).

Очевидно, что механизмы идентификации и аутентификации должны предусматривать противодействие всем потенциальным злоумышленникам, т.е. как сторонним по отношению к защищаемому объекту, так и санкционированным пользователям, зарегистрированным на компьютере.

1. Требования к идентификации и аутентификации

1.5. Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей

При этом речь идёт о прикладных пользователях, т.к. осуществить какую-либо защиту от НСД к информации от администратора безопасности невозможно, даже включая применение механизмов криптографической защиты (он сумеет снять информацию до момента её поступления в драйвер шифрования).

С учётом сказанного в этом разделе мы можем сделать следующие выводы:

1. На защищаемом объекте, как правило, зарегистрированы, по крайней мере, два пользователя – прикладной пользователь и администратор безопасности. Поэтому в качестве потенциального злоумышленника при реализации механизмов парольной защиты в общем случае следует рассматривать не только стороннее по отношению к защищаемому объекту лицо, но и санкционированного пользователя, который преднамеренно либо неумышленно может осуществить атаку на механизм парольной защиты.
2. Рассматривая атаки на парольную защиту, следует учитывать, что по сравнению со сторонним лицом, которое может характеризоваться явными угрозами парольной защите, защита от атак санкционированного пользователя качественно сложнее, т.к. им могут быть реализованы скрытые угрозы.

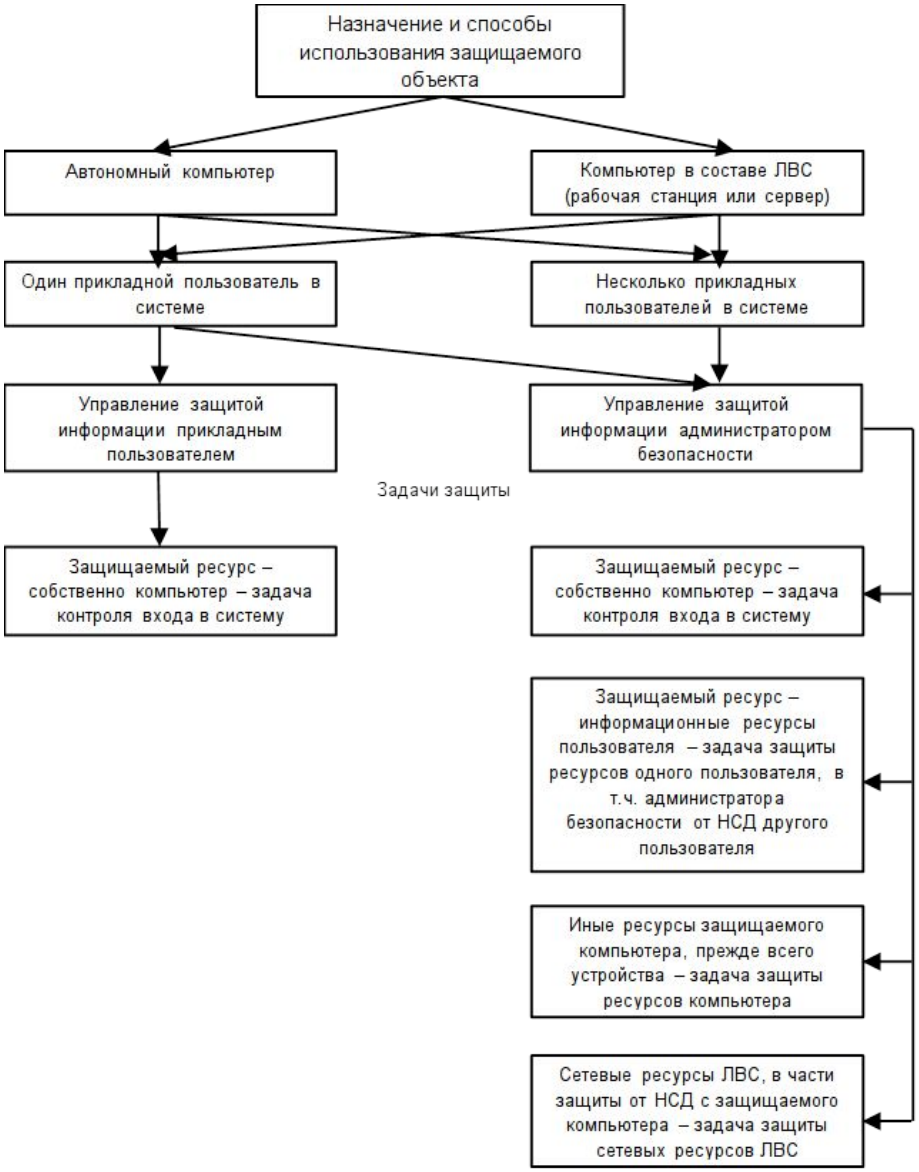
2. Классификация задач, решаемых механизмами идентификации и аутентификации

2.1. Классификация задач по назначению защищаемого объекта

Основу классификации задач, решаемых механизмами парольной защиты, составляет назначение защищаемого объекта (компьютера). Именно в соответствии с назначением объекта определяется перечень защищаемых ресурсов и источников угроз (потенциальных злоумышленников).

2. Классификация задач, решаемых механизмами идентификации и аутентификации

2.1. Классификация задач по назначению защищаемого объекта



2. Классификация задач, решаемых механизмами идентификации и аутентификации

2.1. Классификация задач по назначению защищаемого объекта

Кстати говоря, рассматриваемые процедуры парольной защиты могут устанавливаться на любые действия системы и пользователя (например, на запуск каждого процесса). Однако необходимо понимать, что это, как правило, не оправдано, поскольку приводит к существенной дополнительной загрузке вычислительного ресурса, т.к. данная процедура выполняется не автоматически.

2. Классификация задач, решаемых механизмами идентификации и аутентификации

2.2. Возможные классификации механизмов авторизации, реализованных в системах защиты

Рассмотрим возможные классификации механизмов идентификации и аутентификации, полученные на основе анализа применения механизмов парольной защиты в ОС (прежде всего семейства Windows), приложениях и современных добавочных средствах защиты ОС.

Классификация по функциональному назначению процедур идентификации и аутентификации, применяемых на практике в системах защиты (в том числе и в добавочных средствах защиты):

- Контроль загрузки
  - Доступ к загрузке системы
  - Доступ к заданию способа загрузки
  - Доступ к заданию режима загрузки
- Контроль функционирования
  - Доступ к системе
  - Доступ к запуску процесса (приложения)
  - Доступ к локальным ресурсам системы
  - Доступ к сетевым ресурсам

2. Классификация задач, решаемых механизмами идентификации и аутентификации

2.2. Возможные классификации механизмов авторизации, реализованных в системах защиты

- Блокировка
  - Загрузки системы
  - Доступа в систему
  - Учётной записи пользователя
  - Запуска приложения

Классификация по принадлежности идентификаторов и паролей:

- Пользователь
  - Прикладной
  - Администратор
- Ответственное лицо

Классификация по субъекту их задания:

- Администратором
- Пользователем
- Ответственным лицом

2. Классификация задач, решаемых механизмами идентификации и аутентификации

2.2. Возможные классификации механизмов авторизации, реализованных в системах защиты

Классификация по способу ввода идентификатора и пароля

- Ввод с клавиатуры
- Ввод с внешнего носителя:
  - Стандартные устройства ввода
  - Специализированные устройства аутентификации

Классификация по способу хранения идентификатора и пароля

- Локально на защищаемом объекте
- Удалённо на сервере.

3. Парольная защита

3.1. Механизмы парольной защиты

Функциональное назначение механизмов парольной защиты

По функциональному назначению парольный вход, как правило, используется для контроля загрузки системы, контроля функционирования и с целью блокировки.

С целью контроля загрузки может устанавливаться процедура идентификации и аутентификации пользователя перед началом загрузки системы, например, встроенными средствами BIOS. В этом случае выполнить загрузку системы сможет только санкционированный пользователь.

Доступ к заданию режима загрузки контролируется штатными средствами BIOS, где после аутентификации пользователь может установить, откуда загружается система – с жёсткого диска или с внешнего носителя, а также указать очерёдность выбора средств загрузки. В качестве контроля доступа к заданию режима загрузки может устанавливаться парольный вход на возможность загрузки в безопасном режиме. Например, для загрузки в режиме Safe Mode для ОС Windows NT/2000/XP пользователю необходимо пройти авторизацию. Загрузиться в аналогичном безопасном режиме в ОС семейства UNIX после авторизации может только пользователь с правами «root».

3. Парольная защита

3.1. Механизмы парольной защиты

Для решения задачи контроля функционирования вычислительной системы выделяются:

- **Контроль пользователя при доступе в систему**. Реализуется в том числе штатными средствами ОС.
- **Контроль при запуске процесса**. Благодаря этому при запуске некоторых приложений может быть установлена парольная защита. Прежде всего, здесь интерес представляет установка пароля ответственного лица, например, начальника подразделения.
- **Контроль при доступе к локальным ресурсам**. Например, при доступе к локальному принтеру и т.д. также может использоваться аутентификация ответственного лица.
- **Контроль при доступе к сетевым ресурсам**. Реализуется в том числе штатными средствами ОС. Например, доступ к ресурсам можно разделить паролем. Так осуществляется сетевой доступ к общим ресурсам по протоколу NETBIOS для ОС семейства Windows.

3. Парольная защита

3.1. Механизмы парольной защиты

В качестве реакции на несанкционированные действия пользователя системой защиты может устанавливаться блокировка некоторых функций: загрузки системы, доступа в систему, учётных записей пользователя, запуска определённых приложений.

Для снятия блокировки необходима авторизация администратора безопасности или ответственного лица.

Кроме того, пользователь может сам выставить блокировку на доступ к системе и к приложениям и т.д., чтобы доступ в систему и к этим приложениям в его отсутствии был блокирован.

Для разблокировки приложения необходимо авторизоваться текущему пользователю. При этом администратор безопасности может блокировать учётные записи пользователей для входа в систему в нерабочее время.

3. Парольная защита

3.1. Механизмы парольной защиты

Особенности парольной защиты, исходя из принадлежности пароля

С точки зрения принадлежности пароля в классификации выделены «пользователь», к которому относится прикладной пользователь системы и администратор, а также «ответственное лицо», в качестве которого может выступать начальник подразделения.

Авторизация ответственного лица может устанавливаться для реализации физического контроля доступа пользователя к ресурсам, прежде всего, к запуску процесса. При этом особенностью здесь является то, что авторизация ответственного лица осуществляется не при доступе в систему, а в процессе функционирования текущего пользователя.

Рассмотрим пример. Пусть требуется обеспечить физически контролируемый доступ к внешней сети, например, Internet. На запуск соответствующего приложения устанавливается механизм авторизации ответственного лица (его учётные данные хранятся в системе защиты). Тогда при запуске соответствующего приложения появится окно авторизации ответственного лица, и приложение может быть запущено только после его успешной авторизации. При этом приложение запускается только на один сеанс.

3. Парольная защита

3.1. Механизмы парольной защиты

Таким образом, приложение физически запускается ответственным лицом с локальной консоли защищаемого объекта. В результате ответственное лицо будет знать, кто и когда запросил доступ в Internet, так как сам принимает решение о разрешении доступа. Если доступ разрешён, ответственное лицо может полностью контролировать данный доступ, т.к. запуск приложения возможен только в его присутствии.

В соответствии с классификацией принадлежности учётной записи введена и классификация способов задания учётных данных. Соответственно назначение учётных данных могут осуществлять как владелец учётной записи, так и администратор (принудительно).

Реализация механизмов парольной защиты

Ввод идентификатора и пароля может осуществляться, как с применением штатных средств компьютера – клавиатуры, устройств ввода (например, дисковод – с дискеты), так и с использованием специализированных устройств аутентификации – всевозможных аппаратных ключей, биометрических устройств ввода параметров и т.д.

Естественно, что для сравнения вводимой и эталонной информации, эталонные учётные данные пользователей должны где-то храниться. Возможно хранение эталонных учётных данных непосредственно на защищаемом объекте. Тогда

3. Парольная защита

3.1. Механизмы парольной защиты

Эталонные данные могут располагаться на сервере. Тогда вводимые данные передаются на сервер, где и сравниваются с эталоном.

И с сервера разрешается или запрещается доступ субъекту, который ввёл учётные данные.

Очевидно, что хранить эталонный пароль как на защищаемом объекте, так и на сервере в открытом виде недопустимо.

Поэтому для хранения пароля используется необратимое преобразование (Хеш-функция), позволяющая создавать некий образ пароля – прямое преобразование.

Этот образ однозначно соответствует паролю, но не позволяет осуществить обратное преобразование – из образа восстановить пароль. Для реализации необратимого преобразования наиболее часто используется алгоритм хеширования MD5.

3. Парольная защита

3.2. Угрозы преодоления парольной защиты

Рассмотрим обобщённую классификацию основных угроз парольной защите. Данная классификация вводится как в соответствии со статистикой известных угроз, так и в соответствии с потенциально возможными угрозами.

Кроме того, при построении данной классификации учитывался анализ принципов работы механизмов идентификации и аутентификации.

Рассмотрим представленные угрозы.

Наиболее очевидными **явными** угрозами являются **физические** – **хищение носителя** (например, дискеты с паролём, электронного ключа с парольной информацией и т.д.), а также **визуальный съём пароля при вводе** (с клавиатуры, либо с монитора).

Кроме того, при использовании длинных сложных паролей пользователи подчас записывают свой пароль, что также является объектом физического хищения.

3. Парольная защита

3.2. Угрозы преодоления парольной защиты

К **техническим явным** угрозам можно отнести **подбор пароля** – либо **автоматизированный** (**вручную пользователем**), либо **автоматический**, предполагающий запуск пользователем специальной программы.

Известно, для сравнения вводимого и эталонного значений пароля, эталонное значение пароля должно храниться на защищаемом объекте (либо на сервере), которое без соблюдения **соответствующих мер по хранению паролей** (хеширование, разграничение доступа к области памяти или реестра, где хранятся пароли), может быть похищено злоумышленником.

Естественно, что наиболее опасными являются скрытые угрозы, например:

- технический съём пароля при вводе;
- модификация механизма парольной защиты;
- модификация учётных данных на защищаемом объекте.

3. Парольная защита

3.2. Угрозы преодоления парольной защиты

Первая группа скрытых угроз наиболее очевидна. Пароль должен быть каким-либо образом введён в систему – с клавиатуры, со встроенного или дополнительного устройства ввода, из сети (по каналу связи). При этом злоумышленником может быть установлена соответствующая программа, позволяющая перехватывать поступающую на защищаемый объект информацию.

Развитые подобные программы позволяют автоматически фильтровать перехватываемую информацию по определённым признакам – в том числе, с целью обнаружения паролей. Примером таких программ могут служить **сниферы клавиатуры** и **канала связи**.

Например, снифер клавиатуры позволяет запоминать все последовательности нажатий кнопок на клавиатуре (здесь пароль вводится в явном виде), а затем фильтровать события по типам приложений.

Злоумышленник, установив подобную программу, и задав режим её запуска при входе в систему какого-либо пользователя, получит его пароль в открытом виде. Затем, например, троянская программа может выдать этот пароль по сети на другую рабочую станцию. Таким образом, если в системе зарегистрировано несколько пользователей, то один пользователь может узнать пароль другого

3. Парольная защита

3.2. Угрозы преодоления парольной защиты

Второй тип скрытых угроз предполагает возможность отключить механизм парольной защиты злоумышленником, например, загрузить систему с внешнего носителя (дисковода или CD-ROM). Если механизм парольной защиты представляет собой некий процесс (в добавочной системе защиты), то выполнение данного процесса можно остановить средствами системного монитора, либо монитора приложений, например, встроенными средствами в оболочку Far.

Третья группа скрытых угроз заключается в модификации учётных данных на защищаемом объекте. Это осуществляется либо путём их **замены**, либо путём **сброса в исходное состояние** настроек механизма защиты. Примером может служить известная программная атака на BIOS – сброс настроек BIOS в исходное состояние посредством изменения контрольных сумм BIOS.

Из сказанного может быть сделан весьма важный вывод: каким бы надёжным ни был механизм парольной защиты, он сам по себе в отдельности, без применения иных механизмов защиты, не может обеспечить сколько-нибудь высокого уровня безопасности защищаемого объекта.

Другой вывод состоит в том, что невозможно сравнивать между собою альтернативные подходы к реализации механизма защиты (в частности, механизма парольной защиты), так как можно оценивать лишь уровень защищённости, обеспечиваемый всей системой защиты в целом, то есть обеспечиваемый совокупностью механизмов защиты (с учётом их реализации),

3. Парольная защита

3.3. Способы усиления парольной защиты

Основные механизмы ввода пароля

Наиболее очевидный способ ввода пароля, который реализован практически во всех ОС, состоит в **вводе пароля с клавиатуры**.

Недостатком данного способа является возможность визуального съёма пароля злоумышленником.

При этом в меньшей степени опасность представляет набор пароля пользователем на клавиатуре – этому можно противодействовать организационными мерами. В большей степени угроза состоит в том, что при задании сложного пароля пользователь стремится его куда-нибудь записать, чтобы не забыть.

В качестве противодействия угрозе визуального съёма пароля могут использоваться **внешние носители** информации. При этом могут использоваться как стандартные средства ввода информации (например, дискета), так и средства, предполагающие подключение специальных средств ввода парольной информации – всевозможные электронные ключи, «таблетки» и т.д.

3. Парольная защита

3.3. Способы усиления парольной защиты

На этих носителях записывается пароль, который считывается системой при аутентификации пользователя. Здесь может задаваться достаточно большая длина пароля без угрозы его визуального съёма.

Применение для ввода пароля стандартного или специального носителя с точки зрения обеспечиваемого уровня безопасности практически равноценно. Вопрос выбора носителя определяется его ценой, долговечностью, удобством хранения.

Недостаток применения внешних носителей для ввода пароля – потенциальная угроза его хищения злоумышленником.

Для противодействия хищению могут рассматриваться следующие альтернативные способы защиты:

- Использование биометрических характеристик пользователя – подход, позволяющий отказаться от внешнего носителя с паролем как такового. При этом идентификатором пользователя становятся его биометрические параметры. Причём ввиду их однозначного соответствия пользователю эти параметры служат одновременно и паролем.
- Комбинирование способа ввода пароля с клавиатуры и способа ввода пароля с внешнего носителя. Например, механизм ввода пароля с клавиатуры может рассматриваться как дополнение к механизму ввода пароля с внешнего

3. Парольная защита

3.3. Способы усиления парольной защиты

- Комбинированный способ осуществляется двумя механизмами, один из который является основным, а другой – дополнительным. При защите компьютеров имеет смысл использовать следующий комбинированный способ ввода пароля:
- основной – с внешнего носителя (целесообразно реализовать добавочными средствами защиты),
- дополнительный – с клавиатуры (для этого могут использоваться встроенные в ОС механизмы авторизации пользователя).

Таким образом, можно выделить следующие приоритеты в использовании механизмов ввода пароля (расположены в порядке убывания):

1. Биометрический способ идентификации пользователя.
2. Комбинированный способ (консольный ввод + использование внешнего носителя).
3. Ввод пароля с внешнего носителя.
4. Консольный ввод (ввод пароля с клавиатуры).

3. Парольная защита

3.3. Способы усиления парольной защиты

Основные способы усиления парольной защиты

Все способы призваны воспрепятствовать подбору пароля злоумышленником.

К ним относятся.

- Посредством задания дополнительных требований к параметрам пароля:
  - Увеличение длины пароля;
  - Увеличение алфавита набором символов одного типа для задания пароля;
  - Увеличение алфавита набором типов символов для задания пароля
- Посредством включения ограничений на процедуру аутентификации:
  - Ограничение на число неверно введённых значений пароля (самое эффективное)
  - Ограничение на число типов символов в пароле
  - Ограничение на повторяемость пароля (история паролей)
  - Ограничение на возможность задания простых паролей
  - Ограничение на периодичность смены пароля пользователем

3. Парольная защита

3.4. Задачи и методы добавочных механизмов в рамках усиления парольной защиты

Требования к добавочным механизмам в рамках усиления парольной защиты

Как отмечалось ранее, важнейшими способами усиления парольной защиты является комплексное использование механизмов, так как сам по себе механизм парольной защиты не может обеспечить гарантированной защиты от несанкционированного входа в систему.

Добавочной защитой в рамках противодействия скрытым угрозам преодоления механизма парольной защиты должны решаться следующие задачи:

- обеспечение замкнутости программной среды, не позволяющей запускать пользователю в системе программы с целью осуществления нерегламентированных действий, например, запуск программ-сниферов (канала связи, каналов ввода с внешних устройств и с клавиатуры) и иных потенциально опасных программ, в частности, позволяющих модифицировать механизм парольной защиты;
- обеспечение разграничения прав доступа к реестру (для ОС Windows), к каталогам и файлам, хранящим учётные данные механизмов парольной защиты для ОС UNIX;

3. Парольная защита

3.4. Задачи и методы добавочных механизмов в рамках усиления парольной защиты

- обеспечение контроля целостности (с возможностью автоматического восстановления из эталонной копии) ключей и ветвей реестра, а также файлов, хранящих учётные данные механизмов парольной защиты, применяемый в предположении, что разграничение прав доступа к реестру ОС, каталогам и файлам злоумышленником преодолены.
- обеспечение защиты от возможности отключения механизма защиты, в частности, возможности загрузки системы с внешних устройств, останова процесса или драйвера, реализующего парольную защиту добавочными средствами;
- обеспечение хеширования паролей, применяемое в предположении, что разграничение прав доступа к реестру ОС, каталогами файлам злоумышленником преодолены, в том числе с использованием ошибок и закладок в ПО.

3. Парольная защита

3.4. Задачи и методы добавочных механизмов в рамках усиления парольной защиты

С учётом сказанного можно выделить ряд механизмов, которые должны быть реализованы с целью усиления парольной защиты от скрытых угроз на защищаемом объекте.

Это:

- Механизм обеспечения замкнутости программной среды.
- Механизм разграничения прав доступа к настройкам ОС и приложений (к реестру для ОС Windows, к каталогам и файлам настроек для ОС Unix).
- Механизм контроля целостности с возможностью автоматического восстановления из резервной копии настроек ОС и приложений (ключей реестра для ОС Windows, файлов для ОС семейства Unix).
- Механизм защиты от возможности отключения парольной защиты, в частности, возможности загрузки системы с внешних устройств, останова процесса или драйвера, реализующего парольную защиту добавочными средствами.
- Механизм хеширования парольной информации и др.

3. Парольная защита

3.5. Двухуровневая авторизация

Двухуровневая авторизация на уровне ОС

Ранее отмечалось, что целесообразно усилить парольную защиту за счёт включения в механизм идентификации и аутентификации возможности ввода пароля с внешнего носителя.

Реализация данной возможности имеет смысл, прежде всего, для однопользовательских ОС, к которым относятся ОС семейства Windows (под однопользовательской здесь понимаем систему, в которой в каждый момент времени может присутствовать только один прикладной пользователь).

Здесь пользователь авторизуется при консольном входе в систему. Для многопользовательских ОС, к которым относятся ОС семейства UNIX, характерна удалённая работа на компьютере многих пользователей, поэтому рассматриваемая задача дополнительной авторизации здесь не столь актуальна.

В простейшем случае рассматриваемая возможность усиления парольной защиты достигается подключением внешних носителей пароля к встроенным механизмам идентификации и аутентификации. При этом средства разработчика, поставляемые изготовителем аппаратных носителей парольной

3. Парольная защита

3.5. Двухуровневая авторизация

Однако, как отмечалось ранее, имеет смысл реализовать режим двухуровневой авторизации – так называемый комбинированный режим. При этом авторизация производится сначала с внешнего устройства, а затем с клавиатуры. Это позволяет оказывать противодействие несанкционированному входу в систему при хищении носителя с парольной информацией.

Рассмотрим возможное техническое решение по комбинированию механизмов добавочной и встроенной парольной защиты входа в систему. На практике это решение реализовано, например, в КСЗИ «Панцирь». Работает схема следующим образом.

3. Парольная защита

3.5. Двухуровневая авторизация

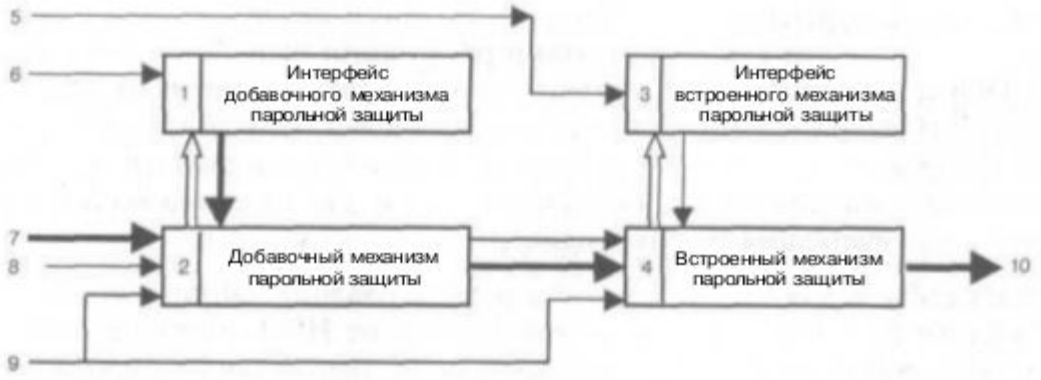


Рис. 9.1. Схема двухуровневой авторизации

Сначала со входа 8 задаётся пароль для аутентификации механизмом добавочной защиты (значение этого пароля записывается на внешний носитель, например, на флэшку). Затем со входа 9 задаётся пароль для аутентификации встроенным механизмом защиты. Этот пароль заносится и в блок 4, и в блок 2. При запросе доступа в систему (со входа 7) блок 2 запускает интерфейс для ввода пользователя пароля со входа 6 (с внешнего носителя).

3. Парольная защита

3.5. Двухуровневая авторизация

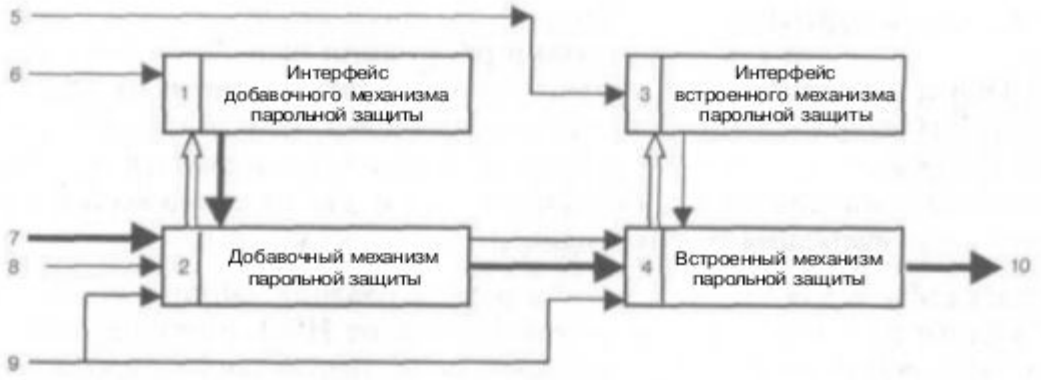


Рис. 9.1. Схема двухуровневой авторизации

При успешной аутентификации блоком 2 выдаётся в блок 4 запрос пользователя на доступ в систему и системный пароль. Причём системный пароль подставляется блоком 2 по запросу аутентификации пользователя блоком 4 без запуска интерфейса 3. Если пароль совпадает, то на выход 10 выдаётся сигнал об успешном прохождении пользователем процедуры аутентификации. В противном случае, блоком 4 запускается блок3, и пользователю предлагается пройти аутентификацию со входа 5 в стандартном окне системной аутентификации – в блоке 3. При успешной аутентификации вырабатывается сигнал на выходе 10.

3. Парольная защита

3.5. Двухуровневая авторизация

Таким образом, представленная схема позволяет реализовать два режима аутентификации – одноуровневый и двухуровневый.

При одноуровневом режиме со входа 9 в блоки 2 и 4 заносятся одинаковые значения системного пароля для пользователя, а пользователь аутентифицируется только в интерфейсе добавочного механизма парольной защиты. При этом системную аутентификацию за пользователя реализует уже собственно механизм добавочной парольной защиты. Делает он это без выдачи соответствующего окна системной аутентификации на экран монитора.

При двухуровневом режиме (со входа 9 в блоки 2 и 4 заносятся различные значения системного пароля для пользователя), пользователь сначала аутентифицируется в интерфейсе добавочного механизма парольной защиты с использованием внешнего носителя с паролём. Затем, при успешной аутентификации, ему предлагается пройти второй уровень – уровень системной аутентификации в окне ОС. Для этого ему нужно ввести пароль с клавиатуры.

3. Парольная защита

3.5. Двухуровневая авторизация

Таким образом, помимо ввода пароля с внешнего носителя, пользователю дополнительно предлагается ввести пароль с клавиатуры. При этом заметим, что требования к дополнительному паролю уже могут быть не столь жёсткими, как к основному.

Требованием к реализации данного механизма является отсутствие какой-либо общности как собственно в реализации основного (встроенного в ОС) и добавочного механизмов защиты, так и в способах хранения и преобразования учётных данных пользователей.

При выполнении данного требования добавочный механизм может использоваться не только в качестве усиления парольной защиты, но и для резервирования механизма идентификации и аутентификации.

Актуальность и даже необходимость резервирования данного механизма, как одного из основных механизмов защиты от НСД, очевидна. Напомним, что учётные данные пользователя, подтверждаемые паролем при входе пользователя в систему, являются основой задания разграничительной политики доступа к ресурсам.

3. Парольная защита

3.5. Двухуровневая авторизация

Двухуровневая авторизация на уровне BIOS

Альтернативный известный вариант реализации двухуровневой парольной защиты состоит в реализации добавочного механизма перед загрузкой системы (средствами расширения BIOS). При этом перед загрузкой системы добавочное средство защиты предлагает пользователю авторизоваться с использованием внешнего носителя пароля. Затем уже при входе в систему могут использоваться штатные средства авторизации ОС. Таким образом, в отличие от рассмотренного выше подхода, здесь заменяется (дополняется) не механизм парольной защиты входа в систему, а механизм парольной защиты контроля загрузки системы. Данный подход используется в специальных дополнительных программно-аппаратных средствах защиты, так называемых «Электронных замках». (При этом, несмотря на использование аппаратной компоненты, собственно защита осуществляется программно).

К достоинствам данного подхода, по сравнению с рассмотренным выше, можно от нести противодействие скрытым угрозам непосредственно в процессе загрузки системы. В частности, загрузочное меню ОС здесь уже может быть вызвано только санкционированным пользователем.

К очевидным недостаткам данного подхода можно отнести необходимость использования дополнительной аппаратной компоненты системы защиты – платы, реализующей функцию расширения BIOS.

3. Парольная защита

3.6. Сетевая авторизация

Описанные ранее способы двухуровневой авторизации могут быть реализованы как в локальном, так и в сетевом исполнении. Оба данных подхода могут осуществлять локальную авторизацию добавочным средством при использовании сетевой авторизации пользователя на контроллере домена встроенным в ОС механизмом. Кроме того, для двухуровневой авторизации на уровне ОС оба уровня защиты могут быть выполнены в виде сетевой авторизации. При этом дополнительная авторизация осуществляется на сервере безопасности.

В этом случае механизм добавочной защиты содержит клиентскую часть, устанавливаемую на защищаемый компьютер, и серверную часть, на сервере безопасности. Серверная часть содержит учётную запись пользователя, а также пароли для аутентификации пользователя добавочным механизмом защиты и на контроллере домена при выполнении процедуры авторизации, серверная часть функционирует аналогично контроллеру домена. При этом наряду с функциями контроллера домена она реализует собственно процедуру авторизации, выдавая на клиентскую часть окно ввода идентификатора и пароля пользователем. Клиентская же часть осуществляет сокрытие окна авторизации контроллера домена и подстановку пароля ОС, который поступает с серверной части при про хождении авторизации пользователем в добавочном механизме защиты.

3. Парольная защита

3.6. Сетевая авторизация

Отметим, что применение сетевой авторизации в данном случае, не давая каких-либо преимуществ по защите пароля (предполагаем, что на защищаемом компьютере установлено добавочное средство защиты, локально обеспечивающее надёжную защиту учётных и парольных данных пользователя), существенно сказывается на надёжности функционирования защищаемой сети. Т.к. выход из строя сервера безопасности приводит к отказу всей сети. При этом ни на одном компьютере сети не сможет быть осуществлён вход пользователя в систему. Таким образом, надёжность сети в целом (и всех информационных систем, реализованных на базе этой сети) в данном случае определяется надёжностью одного компьютера. Это недопустимо в большинстве приложений информационных систем. И прежде всего это касается тех из них, где осуществляется распределённая обработка данных.

С учётом сказанного можно сформулированы следующие рекомендации по реализации механизмов двухуровневой авторизации:

- дополнительный механизм защиты должен быть реализован локально. При этом системой защиты должно обеспечиваться надёжное хранение парольной информации на защищаемом компьютере.
- Встроенный в ОС механизм может быть настроен как в режиме локальной, так и в режиме сетевой авторизации, в зависимости от задач, решаемых в сети.