Лекция 8. Компьютерная безопасность

- *8.1. Основы противодействия нарушению конфиденциальности информации*
- *8.2. Методы разграничения доступа*
- *8.3. Криптографические методы защиты данных*
- *8.4. Принцип достаточности защиты*
- *8.5. Использование хэш-функций*
- *8.6. Электронная цифровая подпись*

Комплекса мероприятий, предотвращения несанкционированного доступа

- идентификация и аутентификация пользователей;
- мониторинг несанкционированных действий - аудит;
- разграничение доступа к компьютерным системам;
- криптографические методы сокрытия информации;
- защита при работе в сети.

Задачи администратора по поддержанию средств защиты

- постоянный контроль корректности функционирования КС и ее защиты:
- регулярный просмотр журналов регистрации событий;
- организация и поддержание адекватной политики безопасности;
- инструктирование пользователей ОС об изменениях в системе защиты, правильного выбора паролей и т. д.;
- регулярное создание и обновление резервных копий программ и данных;
- постоянный контроль изменений конфигурационных данных и политики безопасности отдельных пользователей, чтобы вовремя выявить взлом защиты.

Организации доступа субъектов к объектам

- идентификация и аутентификация субъекта доступа;
- проверка прав доступа субъекта к объекту;
- ведение журнала учета действий субъекта.

Идентификация и аутентификация пользователей

- Эти две операции обычно выполняются вместе, т.е., пользователь сначала сообщает сведения, позволяющие выделить его из множества субъектов (идентификация) – вводит ***имя пользователя*** (login), а затем сообщает секретные сведения, подтверждающие, что он тот, за кого себя выдает.
- Обычно данные, идентифицирующие пользователя, не засекречены, но для усложнения проведения атак по несанкционированному доступу желательно хранить эти данные в файле, доступ к которому возможен только администратору системы.

Категории атрибутивных идентификаторов

- пароли;
- съемные носители информации;
- электронные жетоны;
- пластиковые карты;
- механические ключи.

Понятие пароля

- ***Паролем*** называют комбинацию символов, которая известна только владельцу пароля или, возможно, администратору системы безопасности.
- Обычно пароль вводится со штатной клавиатуры после включения питания.
- Возможен ввод пароля с пульта управления или специального наборного устройства.

Рекомендации при организации парольной защиты

- Пароль необходимо запоминать, а не записывать.
- Длина пароля должна быть не менее девяти символов.
- Пароли должны периодически меняться.
- Должны фиксироваться моменты времени успешного получения доступа и неудачного ввода пароля. Информация о попытках неверного ввода пароля должны подвергаться статистической обработке и сообщаться администратору.
- Пароли должны храниться так, чтобы доступ к ним был затруднен. Это достигается двумя способами:
  - пароли хранятся в специальном ЗУ, запись в которое осуществляется в специальном режиме;
  - пароли подвергаются криптографическому преобразованию (шифрованию).
- При вводе пароля не выдавать никаких сведений на экран, чтобы затруднить подсчет введенных символов.
- Не использовать в качестве паролей имена и фамилии, дни рождения и географические или иные названия. Желательно менять при вводе пароля регистры, использовать специальные символы, набирать русский текст на латинском регистре, использовать парадоксальные сочетания слов.

Методы ограничения доступа к информации

- Существует несколько моделей разграничения доступа. Наиболее распространенными являются:
- дискреционная модель разграничения доступа;
- полномочная (мандатная) модель разграничения доступа.

Дискреционная модель

- Характеризуется следующим набором правил:
- для любого объекта существует владелец;
- владелец может произвольно ограничивать доступ субъектов к данному объекту;
- для каждой тройки субъект–объект–метод возможность доступа определена однозначно;
- существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу доступа.

Полномочная (мандатная) модель

- Характеризуется следующим набором правил:
- каждый объект имеет гриф секретности. Чем выше его числовое значение, тем секретнее объект;
- каждый субъект доступа имеет уровень допуска.

Требования к подсистеме аудита

- Только сама КС может добавлять записи в журнал аудита. Это исключит возможность компрометации аудитором других пользователей.
- Ни один субъект доступа, в том числе и сама КС, не может редактировать или удалять записи в журнале.
- Журнал могут просматривать только аудиторы, имеющие соответствующую привилегию.
- Только аудиторы могут очищать журнал. После очистки в него обязательно вносится запись о времени и имени пользователя, очистившего журнал. Должна поддерживаться страховая копия журнала, создаваемая перед очисткой. При переполнении журнала операционная система прекращает работу и дальнейшая работа может осуществляться до очистки журнала только аудитором.
- Для ограничения доступа должны применяться специальные средства защиты, которые предотвращают доступ администратора и его привилегии по изменению содержимого любого файла. Желательно страховую копию журнала сохранять на WORM-CD, исключающих изменение данных.

Что регистрируется в журнале аудита?

- попытки входа/выхода пользователей из системы;
- попытки изменения списка пользователей;
- попытки изменения политики безопасности, в том числе и политики аудита.

Криптографические методы защиты данных

- ***Криптографические*** методы являются наиболее эффективными средствами защиты информации, при передаче же по протяженным линиям связи они являются единственным реальным средством предотвращения несанкционированного доступа к ней.
- Важнейшим показателем надежности криптографического закрытия информации является его ***стойкость*** - тот минимальный объем зашифрованного текста, который можно вскрыть статистическим анализом.

Требования к криптографическому закрытию информации

- **Сложность и стойкость криптографического закрытия данных должны выбираться в зависимости от объема и степени секретности данных.**
- **Надежность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику становится известен метод шифрования.**
- **Метод закрытия, набор используемых ключей и механизм их распределения не должны быть слишком сложными.**
- **Выполнение процедур прямого и обратного преобразований должно быть формальным. Эти процедуры не должны зависеть от длины сообщений.**
- **Ошибки, возникающие в процессе преобразования, не должны распространяться по всему тексту.**
- **Вносимая процедурами защиты избыточность должна быть минимальной.**

Метод шифрования с секретным ключом.

- При этом важной задачей является безопасная передача ключа, который при этом обычно тоже шифруется. Учитывая короткую длину фразы, содержащей ключ, стойкость шифра ключа значительно выше, чем у основного текста.
- Основной недостаток симметричного процесса заключается в том, что, прежде чем начать обмен информацией, надо выполнить передачу ключа, а для этого опять-таки нужна защищенная связь, то есть проблема повторяется, хотя и на другом уровне.

Системы с открытым ключом или ***ассиметричный*** метод

- Наиболее перспективными системами криптографической защиты данных в настоящее время являются системы с открытым ключом. В таких системах для шифрования данных используется один ключ, а для дешифрования - другой.
- Первый ключ не является секретным и может быть опубликован для использования всеми пользователями системы, которые шифруют данные. Для дешифрования данных получатель использует второй ключ, который является секретным.
- Ключ дешифрования не может быть определен из ключа шифрования. В настоящее время наиболее развитым методом криптографической защиты информации с открытым ключом является алгоритм RSA.

Принцип достаточности защиты

- **Защиту информации принято считать достаточной, если затраты на ее преодоление превышают ожидаемую ценность самой информации.**
- Принцип предполагает, что защита не абсолютна, и приемы ее снятия известны, но она все же достаточна для того, чтобы сделать это мероприятие нецелесообразным.

Использование хэш-функций

- Функции ***хэширования*** широко используются для шифрования паролей пользователей КС и при создании электронной подписи.
- Получив в свое распоряжение файл, хранящий пароли пользователей, преобразованные хэш-функцией, злоумышленник не имеет возможности получить по ним сами пароли, а должен перебирать парольные комбинации символов, применять к ним хэш-функцию и проверять на соответствие полученной строки и строки из файла хэшированных паролей.

Электронная цифровая подпись

- Её основные достоинства:
- удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
- не дает лицу, подписавшему текст, отказаться от обязательств, связанных с подписанным текстом;
- гарантирует целостность подписанного текста.

Формирование цифровой подписи

- На этапе формирования цифровой подписи генерируются два ключа: секретный и открытый.
- Открытый ключ рассылается всем: абонентам, которым будет направлен электронный документ.
- Подпись, добавляемая к документу, содержит такие параметры отправителя, как дату подписи, информацию об отправителе письма и имя открытого ключа. С помощью хэш-функции, примененной ко всему документу, вычисляется небольшое число, характеризующее весь текст в целом.
- Это число, которое затем шифруется закрытым ключом, и является электронной цифровой подписью.