**Задание на 27.01.2022**

МДК 03.02 Программно-аппаратные средства защиты информации

1. **Сделать конспект лекции**
2. **Сделать практическую работу №3** Настройка защиты ОС. Защитные механизмы операционных систем.
3. **Сделать практическую работу №4** Доступ к элементам системы. Способы управления доступом.
4. **Отчет отправить на почту svebalch@mail.ru**

**Лекция 5**

**Идентификации субъекта. Понятие протокола идентификации. Идентифицирующая информация. Пароли.**

**Программно-аппаратные средства идентификации и аутентификации пользователей**

Угроза несанкционированного доступа к информационным ресурсам КС представляется достаточно опасной с точки зрения Возможных последствий. Для несанкционированного доступа злоумышленник обычно использует:

— знания о КС и умения работать с ней;

— сведения о системе защиты информации;

сбои и отказы технических и программных средств.

Для защиты информации от НСД создается система разграничения доступа, контролирующая любые запросы к информационным ресурсам КС со Стороны пользователей (или их программ) по установленным для них правилам и видам доступа.

В системе разграничения доступа по отношению к любому субъекту доступа (пользователю, программе, техническому средству) должны быть предусмотрены следующие этапы доступа к КС:

- идентификация субъектов и объектов доступа;

- установление подлинности (аутентификация);

- определение полномочий для последующего контроля и разграничения доступа к компьютерным ресурсам.

**Идентификация и аутентификация.**

**Основные понятия и классификация**

Применение при межсетевом взаимодействии открытых каналов передачи данных создает потенциальную угрозу проникновения злоумышленников (нарушителей). Если пассивный нарушитель имеет возможность только просматривать доступные ему сообщения, то активный наряду с прослушиванием может перехватывать, искажать и уничтожать их. Поэтому одной из важных задач обеспечения информационной безопасности при межсетевом взаимодействии является использование методов и средств, позволяющих одной (проверяющей) стороне убедиться в подлинности другой (проверяемой) стороны. Обычно для решения данной проблемы применяются специальные приемы, дающие возможность проверить корректность сообщений о том, что проверяемая сторона владеет определенным секретом.

С каждым зарегистрированным в компьютерной системе субъектом (пользователем или процессом, действующим от Имени пользователя) связана некоторая информация, однозначно идентифицирующая его. Это может быть число или строка символов, именующие данный субъект. Такую информацию называют идентификатором субъекта. Имея идентификатор, зарегистрированный в сети пользователь считается легальным (заданным); остальные субъекты относятся к нелегальным.

Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает две стадии идентификацию и аутентификацию.

*Идентификация* — это процедура распознавания пользователя по его идентификатору (имени). Эта функция выполняется в первую очередь, когда пользователь делает попытку войти в сеть. Он сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

*Аутентификация* — процедура проверки подлинности, позволяющая достоверно убедиться, что пользователь является именно тем, кем он себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны; при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация — взаимосвязанные процессы распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу.

После того как субъект идентифицирован и аутентифицирован, выполняется его *авторизация*. Это процедура предоставления субъекту определенных прав и ресурсов в данной системе; иными словами, авторизация устанавливает сферу его действия и доступные ему ресурсы КС.

Перечисленные три процедуры инициализации являются процедурами защиты и относятся к одному субъекту КС.

При защите каналов передачи данных выполняется *взаимная аутентификация субъектов*, то есть взаимное подтверждение подлинности субъектов, связывающихся между собой по линиям связи Процедура подтверждения подлинности выполняется обычно в начале сеанса при установлении соединения абонентов; термин «соединение» указывает на логическую связь (потенциально двустороннюю) между двумя субъектами сети. Цель данной процедуры — обеспечить уверенность, что соединение установлено с законным субъектом и вся информация дойдет до места назначения.

Для подтверждения своей подлинности субъект может предъявлять системе разные сущности. В зависимости от предъявляемых субъектом сущностей процессы аутентификации могут быть разделены на следующие категории:

• *на основе знания чего-либо*. Примером могут служить стандартные пароли, персональные идентификационные номера (Personal Identification Numbers PIN), а также секретные и открытые ключи, знание которых демонстрируется в протоколах типа «запрос-ответ»;

• *на основе обладания чем-либо*. Обычно это магнитные карты, смарт-карты, сертификаты, устройства touch- memory и персональные генераторы, которые используются для создания одноразовых паролей;

• *на основе каких-либо неотъемлемых характеристик.* данная категория включает методы, базирующиеся на проверке биометрических характеристик пользователя (голос, сетчатка глаза, отпечатки пальцев). В этой категории не используются криптографические методы и средства. Аутентификация на ос- ноне биометрических характеристик применяется для контроля доступа в помещения или к какой-либо технике.

Для взаимной аутентификации участников взаимодействия быть организован обмен паролями между ними. *Пароль* — то, что знает пользователь и что также знает другой участник взаимодействия. Персональный идентификационный номер PIN является испытанным способом аутентификации держателя пластиковой карты и смарт-карты. Секретное значение PIN - должно быть известно только держателю карты.

*Динамический (одноразовый) пароль* — это пароль, который после однократного применения никогда больше не используется. На практике обычно выбирают регулярно меняющееся значение, которое базируется на постоянном пароле или ключевой фразе.

*Система «запрос-ответ»* — одна из сторон инициирует аутентификацию с помощью посылки другой стороне уникально, и непредсказуемого значения «запрос», а другая сторона посылат ответ, вычисленный с помощью запроса и секрета. Так как обе стороны владеют одним секретом, то первая из них может проверить правильность ответа второй.

*Сертификаты и цифровые подписи* — если для аутентификации используются сертификаты, то требуется применение и цифровых подписей на них. Сертификаты выдаются ответственным лицом в организации пользователя, сервером сертификатов или внешней доверенной организацией. В рамках Internet появилось несколько коммерческих инфраструктур РКI для распространения сертификатов электронных подписей. Пользователи могут получить сертификаты различных уровней.

Процессы аутентификации можно также классифицировать по уровню обеспечиваемой безопасности. В соответствии с данным подходом процессы аутентификации разделяются на следующие типы:

• *простая аутентификация* (на основе использования паролей);

• *строгая аутентификация* (на основе использования криптографических методов и средств);

• процессы (протоколы) аутентификации, обладающие Свойством *доказательства с нулевым знанием*.

С точки зрения безопасности каждый из перечисленных типов способствует решению определенных задач, поэтому процессы и протоколы аутентификации активно используются на практике. В то же время следует отметить, что интерес к протоколам аутентификации, обладающим свойством доказательства с нулевым знанием, носит пока скорее теоретический, нежели практический характер, но, возможно, в недалеком будущем их начнут активно использовать для защиты информационного обмена.

Основными атаками на протоколы аутентификации являются:

• *маскарад* (impersonation). Пользователь пытается выдать себя за другого с целью получения привилегий и возможности действий от лица другого пользователя;

• *подмена* *стороны аутентификационного обмена* (interleaving attack). Злоумышленник в ходе данной атаки участвует в процессе аутентификационного обмена между двумя сторонами с целью модификации проходящего через него трафика. Существует разновидность атаки подмены: после успешного прохождения аутентификации между двумя пользователями и установления соединения нарушитель исключает какого- либо пользователя из соединения и продолжает работу от его имени;

• *повторная передача* (replay attack). Заключается в повторной передаче аутентификационных данных каким-либо пользователем;

• *отражение передачи* (reflection attack). Один из вариантов предыдущей атаки, в ходе которой злоумышленник в рамках данной сессии протокола пересылает обратно перехваченную информацию;

• *вынужденная задержка* (forced delay). Злоумышленник перехватывает некоторую информацию и передает ее спустя некоторое время;

• *атака с выборкой текста* (chosen- text attack). Злоумышленник перехватывает аутентификационный трафик и пытается получить информацию о долговременных криптографических ключах.

Для предотвращения таких атак при построении протоколов аутентификации применяются следующие приемы:

• использование механизмов типа «запрос-ответ», меток времени, случайных чисел, идентификаторов, цифровых подписей;

• привязка результата аутентификации к последующим действиям пользователей в рамках системы. Примером подобного подхода может служить осуществление в процессе аутентификации обмена секретными сеансовыми ключами, которые используются при дальнейшем взаимодействии пользователей;

• периодическое выполнение процедур аутентификации в рамках уже установленного сеанса связи и т.п.

Механизм запроса-ответа состоит в следующем. Если пользователь А хочет быть уверенным, что сообщения, получаемые им от пользователя В, не являются ложными, он включает в посылаемое для В сообщение непредсказуемый элемент — запрос Х (например, некоторое случайное число). При ответе пользователь В должен выполнить над этим элементом определенную операцию (например, вычислить некоторую функцию f (Х)). Это невозможно осуществить заранее, так как пользователю В неизвестно, какое случайное число Х придет в запросе. Получив от- нет с результатом действий В, пользователь А может быть уверен в подлинности В. Недостаток этого метода — возможность установления закономерности между запросом и ответом.

Механизм отметки времени подразумевает регистрацию времени для каждого сообщения. В этом случае каждый пользователь сети может определить, насколько устарело пришедшее сообщение, и не принять его, поскольку оно может быть ложным.

В обоих случаях для защиты механизма контроля следует применять шифрование, чтобы быть уверенным, что ответ послан не злоумышленником.

При использовании отметок времени возникает *проблема допустимого временного интервала задержки* для подтверждения подлинности сеанса. Ведь сообщение с «временным штемпелем» в принципе не может быть передано мгновенно. Кроме того, компьютерные часы получателя и отправителя могут не быть абсолютно синхронизированы.

При сравнении и выборе протоколов аутентификации необходимо учитывать следующие характеристики:

• наличие *взаимной аутентификации* — это свойство отражает необходимость обоюдной аутентификации между сторонами аутентификационного обмена;

• *вычислительная эффективность* — количество операций, необходимых для выполнения протокола;

• *коммуникационная эффективность* — данное свойство отражает количество сообщений и их длину, необходимую для осуществления аутентификации;

• *наличие третьей стороны* — примером третьей стороны может служить доверенный сервер распределения симметричных ключей или сервер, реализующий дерево сертификатов для распределения открытых ключей;

• *основа гарантий безопасности* — примером могут служить протоколы, обладающие свойством доказательства с нулевым знанием;

• *хранение секрета* — имеется в виду способ хранения критичной ключевой информации.

Аутентификация должна применяться не только для установления подлинности пользователей, но и для проверки целостности сообщений и подлинности их источника. После того как произошла успешная взаимная аутентификация абонентов, приходит очередь аутентификации передаваемых по защищенному каналу данных. Каждый получатель информации (устройство, приложение или пользователь) должен иметь подтверждение, что полученные им данные были сформированы и отправлены именно тем отправителем (устройством, приложением или пользователем), легальность которого была доказана во время предшествующей процедуры аутентификации.

Таким образом, необходимо обеспечить выполнение следующих требований защиты при обмене сообщениями:

• получатель должен быть уверен в подлинности источника данных; получатель должен быть уверен в подлинности передаваемых данных;

• отправитель должен быть уверен в доставке данных получателю;

• отправитель должен быть уверен в подлинности доставленных данных.

Применительно к первому и второму требованиям в качестве средства защиты выступает цифровая подпись. Для выполнения последних двух условий отправитель должен получить уведомление о вручении. Средством защиты в такой процедуре является цифровая подпись подтверждающего ответного сообщения, которое, в свою очередь, служит доказательством пересылки исходного сообщения.

Если четыре вышеназванных требования реализованы в КС, то гарантируется защита целостности данных и подлинности их источника при передаче информации по каналу связи, а также обеспечивается функция защиты, называемая функцией неоспоримости (неотрицаемости) передачи. В этом случае отправитель не может отрицать ни факта посылки сообщения, ни его содержания, а получатель не может отрицать ни факта получения сообщения, ни подлинности его содержания.

Существует особая разновидность процессов (протоколов) аутентификации сообщений и/или аутентификации источника данных, которые реализуются с использованием алгоритмов электронной цифровой подписи.