**Тема 13: "ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ, УПРАВЛЕНИЕ ДОСТУПОМ"**

***13.1 Основные программно-технические меры.***

По данным статистики главную угрозу информационным системам представляют легальные пользователи, а точнее их некомпетентность и неаккуратность при выполнении служебных обязанностей. Физическая защита в данном случае малоэффективна, и только программно-технические меры способны им противостоять.

Программно-технические меры обеспечения информационной безопасности ИС – это меры, направленные на защиту аппаратных, программных ресурсов и данных, хранящихся в ИС. В данном случае эта задача возлагается на саму информационную систему. Компьютеры помогли автоматизировать многие области человеческой деятельности. Почему бы не возложить на них обеспечение собственной безопасности.

В рамках современных информационных систем известны следующие меры или **сервисы безопасности:**

* идентификация и аутентификация;
* управление доступом;
* протоколирование и аудит;
* шифрование;
* контроль целостности;
* экранирование;
* анализ защищенности;
* обеспечение высокой доступности;
* туннелирование;
* управление.

Среди этих мер можно выделить меры, направленные на:

* предупреждение нарушений ИБ;
* обнаружение нарушений ИБ;
* меры по локализации зоны действия нарушений;
* меры по выявлению нарушителя;
* меры по восстановлению режима безопасности.

***Задачи сервисов безопасности***

Большинство сервисов безопасности направлено на *предупреждение нарушений*. Это идентификация, аутентификация, управление доступом, шифрование, экранирование.

Протоколирование, аудит и контроль целостности помогут в *обнаружении нарушений*, (о которых, часто даже не знают). Активный аудит позволяет обеспечить *реакцию системы на нарушения* и отследить его.

Анализ защищенности необходим для *выявления уязвимых мест ИС* с целью их оперативной ликвидации.

Меры обеспечения высокой доступности направлены на *повышение отказоустойчивости системы и обеспечение безопасного восстановления* (например «откат операционной системы»).

Туннелирование – это конвертирование одних протоколов передачи пакетов через сеть, в другие протоколы. Оно позволяет реализовать такое защитное средство, как *частные виртуальные сети* (VPN) поверх других сетей, например, сети Интернет.

И, наконец, задача управления – *обеспечение нормальной работы* всех компонентов и средств безопасности.

Рассмотрим несколько подробнее основные сервисы безопасности.

***13.2 Идентификация и аутентификация. Основные понятия***

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности. Идентификация и аутентификация – это первая линия обороны, «проходная» информационного пространства организации.

*Идентификация* позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством *аутентификации* вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова «аутентификация» иногда используют словосочетание «проверка подлинности».

Рассмотрим конкретный пример. Перед началом интерактивного сеанса работы большинство операционных систем запрашивают у пользователя его имя (логин) и пароль. Введенное имя является *идентификатором* пользователя, а его пароль – *аутентификатором*. Это пример односторонней аутентификации, когда клиент доказывает свою подлинность серверу. Аутентификация бывает и двусторонней (взаимной).

Существуют различные варианты реализации данного сервиса безопасности. Их разнообразие определяется 2-мя аспектами:

1) аутентификатором (то есть что используется для подтверждения подлинности субъекта);

2) организацией обмена данными идентификации/аутентификации.

Субъект может подтвердить свою подлинность, предъявив, один из следующих аутентификаторов:

* нечто, **что он знает** (пароль, личный идентификационный номер, криптографический ключ и т.д.)
* нечто, **чем он владеет** (личную карточку или иное устройство аналогичного назначения);
* нечто, **что есть часть его самого** (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

Существуют некоторые особенности, которые необходимо учесть.

1. В открытой сетевой среде между сторонами идентификации/аутентификации не существует доверенного маршрута. Это значит, что данные, переданные субъектом, могут быть искажены злоумышленником. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от перехвата, изменения или воспроизведения данных. Передача паролей в открытом виде, очевидно, недопустима. Не спасает положение и шифрование паролей, так как оно не защищает от воспроизведения. Нужны более сложные протоколы аутентификации.

2. Надежная идентификация и аутентификация затруднена не только из-за сетевых угроз, но и по целому ряду других причин. Во-первых, почти все аутентификаторы можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

3. Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть - это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации.

Любопытно отметить, что сервис идентификации/аутентификации может стать **объектом атак на доступность.** Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации (такое, например, как терминал) блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.

***Парольная аутентификация***

Главное достоинство парольной аутентификации – простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать *самым слабым средством проверки подлинности*.

Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т.п.). Однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя. Известна классическая история про советского разведчика Рихарда Зорге, объект внимания которого через слово говорил «карамба» разумеется, этим же словом открывался сверхсекретный сейф.

Иногда пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена.

Ввод пароля можно подсмотреть. Иногда для подглядывания используются даже оптические приборы.

Пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля. Теоретически в подобных случаях более правильно задействовать средства управления доступом, но на практике так никто не поступает; а тайна, которую знают двое, это уже не тайна.

Пароль можно угадать «методом грубой силы», используя, скажем, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммирован полный перебор (предполагается, что алгоритм шифрования известен).

Тем не менее, *следующие меры позволяют значительно повысить надежность парольной защиты*:

* наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
* управление сроком действия паролей, их периодическая смена;
* ограничение доступа к файлу паролей;
* ограничение числа неудачных попыток входа в систему (это затруднит применение «метода грубой силы»);
* обучение пользователей;
* использование программных генераторов паролей (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации.

***Одноразовые пароли***

Рассмотренные выше пароли можно назвать многоразовыми; их раскрытие позволяет злоумышленнику действовать от имени легального пользователя. Гораздо более сильным средством, устойчивым к пассивному прослушиванию сети, являются одноразовые пароли.

Используют программные генераторы одноразовых паролей. Идея состоит в следующем. Пусть имеется односторонняя функция f (то есть функция, вычислить обратную к которой за приемлемое время не представляется возможным). Эта функция известна и пользователю, и серверу аутентификации. Пусть, далее, имеется секретный ключ К, известный только пользователю.

На этапе начального администрирования пользователя функция применяется к ключу К *n*-раз, после чего результат сохраняется на сервере. После этого процедура проверки подлинности пользователя выглядит следующим образом:

* сервер присылает на пользовательскую систему число (n- 1);
* пользователь применяет функцию к секретному ключу К (n- 1) раз и отправляет результат по сети на сервер аутентификации;
* сервер применяет функцию f к полученному от пользователя, значению и сравнивает результат с ранее сохраненной величиной. В случае совпадения подлинность пользователя считается установленной, сервер запоминает новое значение (присланное пользователем) и уменьшает на единицу счетчик (n).

Поскольку функция необратима, перехват пароля, равно как и получение доступа к серверу аутентификации, не позволяют узнать секретный ключ К и предсказать следующий одноразовый пароль.

Другой подход к надежной аутентификации состоит в генерации нового пароля через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться программы или специальные интеллектуальные карты (с практической точки зрения такие пароли можно считать одноразовыми). Серверу аутентификации должен быть известен алгоритм генерации паролей и ассоциированные с ним параметры; кроме того, часы клиента и сервера должны быть синхронизированы.

***Сервер аутентификации Kerberos***

Kerberos – это программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений. Клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем.

Kerberos предназначен для решения следующей задачи. Имеется открытая (незащищенная) сеть, в узлах которой сосредоточены субъекты – пользователи, а также клиентские и серверные программные системы Каждый пользователь С обладает секретным ключом. Чтобы пользователь С мог доказать свою подлинность серверу S (без этого S не станет обслуживать С), он должен не только назвать себя, но и продемонстрировать знание секретного ключа. Пользователь С не может просто послать S свой секретный ключ, во- первых, потому, что сеть открыта (доступна для пассивного и активного прослушивания), а, во-вторых, потому, что S не знает (и не должен знать) секретный ключ С. Требуется менее прямолинейный способ демонстрации знания секретного ключа.

Система Kerberos представляет собой доверенную третью сторону (то есть сторону, которой доверяют все), владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности.

Чтобы с помощью Kerberos получить доступ к серверу S, пользователь С посылает Kerberos запрос, содержащий сведения о нем (клиенте) и о запрашиваемой услуге. В ответ Kerberos возвращает так называемый билет, зашифрованный секретным ключом *сервера*, и копию части информации из билета, зашифрованную секретным ключом *клиента*. Клиент должен расшифровать вторую порцию данных и переслать ее вместе с билетом серверу. Сервер, расшифровав билет, может сравнить его содержимое с дополнительной информацией, присланной клиентом. Совпадение свидетельствует о том, что клиент смог расшифровать предназначенные ему данные (ведь содержимое билета никому, кроме сервера и Kerberos, недоступно), то есть продемонстрировал знание секретного ключа. Значит, клиент – именно тот, за кого себя выдает. Подчеркнем, что секретные ключи в процессе проверки подлинности не передавались по сети (даже в зашифрованном виде) они только использовались для шифрования. Как организован первоначальный обмен ключами между Kerberos и субъектами и как субъекты хранят свои секретные ключи – вопрос отдельный.

Проиллюстрируем описанную процедуру.



***Рис. 19 Проверка сервером S подлинности клиента С***

Здесь с и s – сведения (например, имя), соответственно, о клиенте и сервере, d1 и d2 – дополнительная (по отношению к билету) информация, Тс.s – билет для клиента С на обслуживание у сервера S, Кс и Кs – секретные ключи клиента и сервера.

***Идентификация/аутентификация с помощью биометрических данных***

Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик.

К числу физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной). На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

Биометрией во всем мире занимаются очень давно, однако долгое время все, что было связано с ней, отличалось сложностью и дороговизной. В последнее время спрос на биометрические продукты, в первую очередь в связи с развитием электронной коммерции, постоянно и весьма интенсивно растет. Это понятно, поскольку с точки зрения пользователя гораздо удобнее предъявить себя самого (свой палец или глаз), чем что-то запоминать. Спрос рождает предложение, и на рынке появились относительно недорогие аппаратно-программные продукты, ориентированные в основном на распознавание отпечатков пальцев.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается *база данных характеристик потенциальных пользователей*. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).

В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных (имя пользователя).

Иногда биометрическая аутентификация является лишь первым рубежом защиты и служит для активизации интеллектуальных карт, хранящих криптографические секреты. В таком случае биометрический шаблон хранится на той же карте.

На наш взгляд, к биометрии следует относиться весьма осторожно. Необходимо учитывать, что она подвержена тем же угрозам, что и другие методы аутентификации. Во-первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути... много чего может произойти. Во-вторых, биометрические методы не более надежны, чем база данных шаблонов. В- третьих, следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в «полевых» условиях, когда, например, к устройству сканирования роговицы могут поднести муляж и т.п. В-четвертых, биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов.

Но главная опасность состоит в том, что любая «пробоина» для биометрии оказывается *фатальной*. Пароли, при всей их ненадежности, в крайнем случае, можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить нельзя. Если биометрические данные окажутся скомпрометированы, придется, как минимум производить существенную модернизацию всей системы/

***13.3 Управление доступом. Основные понятия***

С традиционной точки зрения средства управления доступом позволяют контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами). В данном разделе речь идет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами. Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары «субъект-объект» определить множество допустимых операций и контролировать выполнение установленного порядка.

Отношение «субъекты-объекты» можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа.

К объектам относятся файлы, устройства и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения).

Права (профили) пользователей задаются системным администратором.

Контроль прав доступа производится разными компонентами программной среды – ядром операционной системы, сервисами безопасности, системой управления базами данных, программным обеспечением промежуточного слоя (таким, как монитор транзакций) и т.д.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

* идентификатор пользователя;
* атрибуты пользователя (метка безопасности, группа пользователя и т.п.). Метки безопасности – основа принудительного (мандатного) управления доступом.

Матрицу доступа обычно хранят по столбцам, то есть для каждого объекта поддерживается список «допущенных» пользователей вместе с их правами.

Списки доступа – исключительно гибкое средство. Посредством списков системный администратор может добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством *произвольного управления доступом*.

Подавляющее большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Основное достоинство произвольного управления гибкость. Вообще говоря, для каждой пары «субъект-объект» можно независимо задавать права доступа, если используются списки управления доступом.

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Например, у каждого пользователя может храниться на общем накопителе своя информация, доступ к которой имеет только он один. Файлы других пользователей он просто не видит.