**Лекция 6**

**Тема: «Методы аутентификации информации в электронной коммерции»**

**1. Идентификация, аутентификация и авторизация**

#### 2 Аутентификация объекта электронной коммерции

С целью исключения возможного несанкционарованного вмешательства в работу информационной системы необходима процедура распознавания системой каждого законного пользователя (или групп пользователей). Для этого в защищенном месте система обязана хранить информацию, по которой можно опознать пользователя, а пользователь, входя в систему, выполняет определенные действия, позволяющие его идентифицировать, т.е. указывает идентификатор **ID**, присвоенный ему в данной системе. Получив идентификатор, система проверяет его содержательность (подлинность) - принадлежность множеству идентификаторов. Обычно устанавливается ограничение на число попыток предъявления некорректного идентификатора.

Если бы идентификация не дополнялась аутентификацией, то сама идентификация теряла бы всякий смысл. Аутентификация пользователя может быть основана на следующих принципах:

* предъявлении пользователем пароля;
* предъявлении пользователем доказательств, что он обладает секретной ключевой информацией;
* ответах на некоторые тестовые вопросы;
* предъявлении пользователем некоторых неизменных признаков, неразрывно связанных с ним;
* предоставлении доказательств того, что он находится в определенном месте в определенное время;
* установлении подлинности пользователя некоторой третьей доверенной стороной.

Процесс распознавания законного пользователя в схематичном виде представлен на рисунке 6.1

 

**Рис. 6.1**Процессы идентификации, аутентификации и авторизации

Процедуры аутентификации должны быть устойчивы к подлогу, подбору и подделке.

После распознавания пользователя система должна выяснить, какие права предоставлены этому пользователю, какую информацию он может использовать и каким образом (читать, записывать, модифицировать или удалять), какие программы может выполнять, какие ресурсы ему доступны, а также другие вопросы подобного рода. Этот процесс называется авторизацией. Таким образом, вход пользователя в систему состоит из идентификации, аутентификации и авторизации. В процессе дальнейшей работы иногда может появиться необходимость дополнительной авторизации в отношении каких-либо действий.

Существуют различные механизмы реализации разграничения доступа. Например, каждому ресурсу (или компоненту) системы может быть сопоставлен список управления доступом ACL (Access Control List), в котором указаны идентификаторы всех пользователей, которым разрешен доступ к данному ресурсу, а также определено, какой именно доступ разрешен. При обращении пользователя к конкретному ресурсу система проверяет наличие у данного ресурса списка управления доступом и, если он существует, выясняет, разрешено ли этому пользователю работать с данным ресурсом в запрошенном режиме. Другим примером реализации механизма авторизации пользователя является профиль пользователя - список, ставящий в соответствие всем идентификаторам пользователей перечень объектов, к которым разрешен доступ данному пользователю с указанием типа доступа. Может быть организована системная структура данных, так называемая матрица доступа, которая представляет собой таблицу, столбцы которой соответствуют идентификаторам всех системных ресурсов, а строки - идентификаторам всех зарегистрированных пользователей. На пересечении i-го столбца и j-й строки таблицы администратор системы указывает разрешенный тип доступа владельца i-го идентификатора к j-му ресурсу.

Доступ к механизмам авторизации должны иметь только специальные системные программы, обеспечивающие безопасность системы, а также строго ограниченный круг пользователей, отвечающих за безопасность системы. Рассматриваемые механизмы должны быть тщательно защищены от случайного или преднамеренного доступа неавторизованных пользователей. Многие атаки на информационные системы нацелены именно на вывод из строя или обход средств разграничения доступа.

Аналогичные действия осуществляются в системе и при аутентификации других субъектов взаимодействия (претендентов), например прикладных процессов или программ, с системой (*верификатором*).

В отличие от аутентификации субъекта взаимодействия процедура аутентификации объекта, устанавливая подлинность электронной почты, банковского счета и т.п., проверяет факт принадлежности данного объекта владельцу указанного идентификатора.

#### 2 Аутентификация объекта электронной коммерции

В процессе аутентификации объекта, иногда называемой *аутентификацией источника данных*, проверяется подлинность идентификатора, представленного с некоторыми данными. В отличие от аутентификации субъекта в этой ситуации претенденту не нужно быть активным участником процесса аутентификации. Данный тип аутентификации по сути ничем не отличается от процедуры контроля целостности. Для аутентификации объекта применяются шифрование симметричным алгоритмом, выработка кода МАС или НМАС, формирование электронной подписи. Первые два варианта применяются в том случае, когда претендент и верификатор доверяют друг другу. Если необходимо иметь возможность доказательства подлинности идентификатора третьей стороне (при условии, что верификатор не имеет возможности изменить массив данных М), например необходима юридическая значимость пересылаемых электронных документов, требуется электронная подпись.

Процедуры аутентификации должны быть устойчивы к подлогу, подбору и подделке.

После распознавания пользователя система должна выяснить, какие права предоставлены этому пользователю, какую информацию он может использовать и каким образом (читать, записывать, модифицировать или удалять), какие программы может выполнять, какие ресурсы ему доступны, а также другие вопросы подобного рода. Этот процесс называется авторизацией. Таким образом, вход пользователя в систему состоит из идентификации, аутентификации и авторизации. В процессе дальнейшей работы иногда может появиться необходимость дополнительной авторизации в отношении каких-либо действий.

Существуют различные механизмы реализации разграничения доступа. Например, каждому ресурсу (или компоненту) системы может быть сопоставлен список управления доступом ACL (Access Control List), в котором указаны идентификаторы всех пользователей, которым разрешен доступ к данному ресурсу, а также определено, какой именно доступ разрешен. При обращении пользователя к конкретному ресурсу система проверяет наличие у данного ресурса списка управления доступом и, если он существует, выясняет, разрешено ли этому пользователю работать с данным ресурсом в запрошенном режиме. Другим примером реализации механизма авторизации пользователя является профиль пользователя - список, ставящий в соответствие всем идентификаторам пользователей перечень объектов, к которым разрешен доступ данному пользователю с указанием типа доступа. Может быть организована системная структура данных, так называемая матрица доступа, которая представляет собой таблицу, столбцы которой соответствуют идентификаторам всех системных ресурсов, а строки - идентификаторам всех зарегистрированных пользователей. На пересечении i-го столбца и j-й строки таблицы администратор системы указывает разрешенный тип доступа владельца i-го идентификатора к j-му ресурсу.

Доступ к механизмам авторизации должны иметь только специальные системные программы, обеспечивающие безопасность системы, а также строго ограниченный круг пользователей, отвечающих за безопасность системы. Рассматриваемые механизмы должны быть тщательно защищены от случайного или преднамеренного доступа неавторизованных пользователей. Многие атаки на информационные системы нацелены именно на вывод из строя или обход средств разграничения доступа.

Аналогичные действия осуществляются в системе и при аутентификации других субъектов взаимодействия (претендентов), например прикладных процессов или программ, с системой (*верификатором*).

В отличие от аутентификации субъекта взаимодействия, процедура аутентификации объекта, устанавливая подлинность электронной почты, банковского счета и т.п., проверяет факт принадлежности данного объекта владельцу указанного идентификатора.