Управление доступом в ИС

- Существует два направления контроля и управления доступом в ИС: физическое и логическое.

- Физическое управление доступом применяется к техническим и аппаратным средствам ИС, а также к информации, представленной в печатной, визуальной и аудиоформе.

- Логическое управление доступом – к программным средствам и информации, представленной в электронной форме. Оно реализуется программными средствами.
- Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, в некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

- В основе управления доступом лежит идентификация и аутентификация.
- Если субъект и СИБ территориально разнесены, то с точки зрения безопасности необходимо рассмотреть два аспекта:
  - что служит аутентификатором;
  - как организован (и защищен) обмен данными идентификации и аутентификации.

- Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) 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.

- Существуют следующие концептуальные механизмы ИБ:
- Идентификация и аутентификация;
- Контроль и управление доступом;
- Протоколирование и аудит;
- Шифрование:
- Контроль целостности;
- Экранирование.

- Для надежной ЗИ необходима комплексная реализация всех перечисленных механизмов. Некоторые из них могут быть реализованы в более полной мере, другие – нет. Защита ИС в первую очередь зависит от реализации механизма идентификации и аутентификации.
- Идентификатор –уникальный набор символов, однозначно соответствующий объекту или субъекту в данной системе .
- Идентификация – распознавание участника процесса информационного взаимодействия (ИВ) перед тем, как к нему будут применены какие-либо аспекты ИБ.
- Пароль – секретный набор символов, позволяющий подтвердить соответствие субъекта предъявленному им идентификатору.
- Аутентификация – обеспечение уверенности в том, что участник ИВ идентифицирован верно.
- Профиль – набор установок и конфигураций для данного субъекта или объекта и определяющий его работу в ИС.
- Авторизация – формирование профиля прав для конкретного участника ИВ.

- Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:
- нечто, что он знает (пароль, криптографический ключ и т.п.);
- нечто, чем он владеет (электронный ключ, смарт-карта и т.п.);
- нечто, что есть часть его самого (свои биометрические характеристики).
- Аутентификация бывает односторонней (обычно субъект доказывает свою подлинность системе) и двусторонней (взаимной).
- Надежная идентификация и аутентификация затруднена по целому ряду причин.

- В ИС между сторонами может не существовать доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности.
- Почти все аутентификационные сущности можно узнать, украсть или подделать.
- Имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами субъекта с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию.
- Чем надежнее средство защиты, тем оно дороже.

Парольная аутентификация

- Главное достоинство парольной аутентификации – простота. Недостаток – это самое слабое средство проверки подлинности.
- Основные нарушения при создании и использовании паролей:
- простой пароль,
- использование стандартных значений из какой-либо документации, которые никогда не изменяют,
- запись пароля на тех предметах, где его можно прочитать, подсмотреть и т.д.
- сообщение пароля другому сотруднику.
- Меры, позволяющие повысить надежность парольной защиты:
- наложение технических ограничений (длина, использование букв, цифр, знаков);
- управление сроком действия паролей;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему;
- обучение пользователей;
- использование программных генераторов паролей, которые основываясь на некоторых правилах, могут порождать сложные, но запоминающиеся пароли,
- одноразовые пароли.