Идентификация и установление подлинности

Идентификация – это присвоение какому-либо объекту или субъекту уникального образа, имени или числа.

Аутентификация – проверка подлинности объекта или субъекта, т.е. является ли проверяемый объект на самом деле тем, за кого себя выдает.

Конечная цель идентификации и установления подлинности объекта в автоматизированной системе – допуск его к информации ограниченного пользования в случае положительного исхода проверки или отказ в допуск к информации в случае отрицательного исхода проверки.

Объекты идентификации и установления подлинности:

- ✔отпечатки пальцев;
- ✔рисунок сетчатки или радужной оболочки глаза;
- ✔тепловой рисунок кисти руки;
- ✔фотография или тепловой рисунок лица;
- ✔почерк (роспись);
- ✔голос

Методы:

1. Метод «запрос-ответ».

Суть: в ВС заблаговременно создается и особо защищается массив вопросов, относящиеся к конкретному пользователю.

2. Использование паролей.

Достоинства: простота и привычность.

Недостатки:

1. Необходимость помнить пароль и хранить его в тайне.
2. Ввод пароля можно подсмотреть.
3. Пароль можно угадать методом перебора.
4. Пароли уязвимы по отношению к электронному перехвату.

Угрозы безопасности парольных систем

1. За счёт использования слабостей человеческого фактора.

2. Путём подбора.

- ✔Полный перебор.
- ✔Подбор с использованием сведений о пользователе.
- ✔Подбор по словарю.

3. За счёт использования недостатков реализации парольных систем.

Правила организации парольных систем:

- ✔Установление минимальной длины пароля.
- ✔Увеличение мощности алфавита паролей.
- ✔Проверка и отбраковка паролей по словарю.
- ✔Установка максимального срока действия пароля.
- ✔Установка минимального срока действия пароля.
- ✔Отбраковка по журналу истории паролей.

Правила организации парольных систем:

- ✔Соответствующий механизм
- ✔затрудняет интерактивный подбор паролей.
- ✔Ограничение числа попыток ввода пароля.
- ✔Принудительная смена пароля при первом входе пользователя в систему.
- ✔Задержка при вводе неправильного пароля.
- ✔Запрет на выбор пароля пользователем и автоматическая генерация пароля.

3. Использование токенов (смарт-карт).

Токен – это предмет или устройство, владение которым подтверждает подлинность пользователя.

Виды токенов:

1. Токены с памятью (пассивные, которые только хранят, но не обрабатывают информацию).
2. Интеллектуальные токены (активные).

Карточки с магнитной полосой.

Категории интеллектуальных токенов по принципу действия:

1.Статический обмен паролями.

2.Динамическая генерация паролей.

3.Запросно-ответные системы.

4. Биометрические методы

Биометрия – это наука, занимающаяся измерением характеристик человеческого организма.

Физические характеристики, используемые для идентификации:

- ✔отпечатки пальцев,
- ✔рисунок сетчатки и радужной оболочки глаза,
- ✔отпечатки ладоней,
- ✔лицо и голос.

Достоинства:

1. Биометрическая характеристика не может быть потеряна, похищена или воспроизведена.
2. Применение биометрии обеспечивает аутентификацию без передачи информации.

Режимы работы механизмов распознавания по биометрическим характеристикам:

1. Регистрация.
2. Верификация.