



Защита информации

- Защита информации – это комплекс мер, которые предназначены для безопасного хранения и **защиты информации** от нежелательных пользователей.



Защита с использованием паролей

- Пароли являются классическим средством защиты информации от чужих глаз. Чтобы пароль был эффективным , нужно соблюдать несколько простых правил :
- 1. пароль не должен содержать части пользовательского имени
- 2. для эффективности можно использовать символы латинского алфавита в разных регистрах
- 3.регулярная смена паролей. На чувствительных ресурсах раз в месяц, на остальных — раз в два месяца.
- 4.пароль не должен передаваться другим лицам .

Двухфакторная аутентификация

С развитием интернет-сервисов и глобального внедрения становится модной и актуальной двухфакторная аутентификация. Работает эта технология довольно просто. Ваш аккаунт сервиса привязывается к телефонному номеру, вводится логин/пароль и на указанный номер приходит дополнительный «уникальный пароль». Такое решение позволяет значительно усилить защиту аккаунта. Но если, под рукой не будет смартфона или резервных кодов на бумаге, то в доступе будет отказано.



Биометрические системы защиты

- Однако такие системы как использование паролей слишком уязвимы и могут легко пострадать от подделки, воровства и других факторов. Поэтому все больший интерес вызывают методы биометрической идентификации, позволяющие определить личность человека по его физиологическим характеристикам путем распознавания по заранее сохраненным образцам.



- Диапазон проблем, решение которых может быть найдено с использованием новых технологий, чрезвычайно широк:
- предотвратить проникновение злоумышленников на охраняемые территории и в помещения за счет подделки, кражи документов, карт, паролей;
- ограничить доступ к информации и обеспечить персональную ответственность за ее сохранность;
- обеспечить допуск к ответственным объектам только сертифицированных специалистов;
- И др.

- Биометрические данные являются очень удобным для людей способом аутентификации, так как их невозможно забыть или потерять. При этом, обеспечивается достаточно высокая степень защиты данных, так как подделать их очень сложно.
- Все методы биометрической аутентификации делятся на два класса. Это **статистические методы**, основанные на физиологических характеристиках человека, которые присутствуют в каждом из нас всю жизнь, их нельзя потерять, скопировать или украсть. **Второй класс – динамические методы**. Они основываются на поведенческих особенностях людей (это, как правило, подсознательные движения в процессе повторения или воспроизведения какого-то конкретного быденного действия).



Статистические методы:

- Аутентификация по отпечатку пальца
- Аутентификация по радужной оболочке глаза
- Аутентификация по сетчатке глаза
- Аутентификация по геометрии руки
- Аутентификация по геометрии лица

Динамические методы :

- Аутентификация по голосу
- Аутентификация по рукописному почерку



Физическая защита данных на дисках

- **RAID-массивы** (избыточные массивы независимых дисков) используются для обеспечения более высокой скорости чтения и записи, а также повышают надежность хранения данных на жестких дисках. Группа жестких дисков подключается к **RAID-контроллеру**, рассматривающему их в качестве единого логического носителя информации.



Способы реализации RAID-массивов

- **Аппаратный** – дисковый массив содержит группу жестких дисков, которые управляются с помощью специальной платы контроллера RAID-массива. **Программный** – RAID-массив реализован с помощью специального драйвера. Дисковые разделы, которые занимают весь диск или его часть, организуются в программный массив. Программные RAID-массивы зачастую оказываются менее надежными от аппаратных, но позволяют обеспечить лучшую скорость работы с данными.

Организация дисковых массивов

- **Уровень 0**

- Нулевой уровень является простым разделением потока данных между двумя или несколькими дисками. Преимуществом такого решения является увеличение скорости ввода и вывода, которая пропорциональна числу задействованных в массиве дисков. Но при таком решении невозможно восстановление информации при поломке хотя бы одного диска массива. Уровень

- **1 Первый**

- уровень состоит в организации «зеркальных» дисков. При записи данных происходит дублирование информации основного диска системы на второй – зеркальный диск, а при выходе из строя основного диска работу поддерживает «зеркальный».

- **Уровни 2 и 3**

- На втором и третьем уровнях создаются параллельные дисковые массивы. Данные при записи на такие дисковые массивы распределяются по дискам на битовом уровне. Избыточная информация, которая используется для восстановления данных при поломке одного из дисков массивов, хранится на специально выделенном диске.

- **Уровень 4**

- Четвертый уровень является модификацией нулевого уровня, на котором поток данных распределяется по дискам массива. Отличается четвертый уровень от нулевого тем, что на нем избыточная информация хранится на специально выделенном диске.

- **Уровень 5**

- Пятый уровень является модификацией уровня 0, на котором поток данных распределяется по дискам массива. На пятом уровне избыточная информация распределяется по всем дискам массива.

С помощью RAID-массивов обеспечивается наиболее высокая скорость записи или чтения данных, возможность полного их восстановления и замены дисков, которые вышли из строя, в режиме непрерываемой работы остальных дисков массива (без их отключения).