

Обеспечение конфиденциальности

Самое главное - это **следовать принципу наименьшего доступа (или принцип минимальных привилегий)**, он заключается в предоставлении каждому пользователю или системному компоненту только тех прав и возможностей, которые строго необходимы для выполнения конкретной задачи.

Технические меры обеспечения конфиденциальности

Технические меры обеспечения конфиденциальности включают в себя использование различных технологий и протоколов для защиты данных от несанкционированного доступа.

- **Шифрование**

Как работает: Текст или данные преобразуются в нечитаемый формат, доступный только тем, кто имеет ключ шифрования.

Простой пример: HTTPS в веб-браузере. Когда вы открываете сайт с HTTPS, данные между вашим браузером и сервером шифруются.

- **Маскирование\хеширование персональных и чувствительных данных**

Как работает: Текст или данные преобразуются в нечитаемый формат, доступный только системе-передатчику.

Простой пример: Пользователи могут менять пароли и сохранять его с помощью системы, но если сотрудник системы зайдет в базу данных - вместо паролей увидит строки символов (хеши), потому что пароли не хранятся в открытом виде в системе, а хешируются.

- **Аутентификация и авторизация**

Как работает: Аутентификация удостоверяет, что вы — это вы. Авторизация определяет, какие ресурсы вам доступны.

Простой пример: Вход в почтовый ящик с использованием пароля и SMS-кода (MFA).

- **Firewall и IDS/IPS**

Как работает: Firewall фильтрует трафик, IDS/IPS обнаруживает и блокирует вредоносные действия.

Простой пример: Запрет на доступ к определенным портам или IP-адресам.

- **VPN и прокси-серверы**

Как работает: VPN шифрует все данные перед их отправкой через интернет, прокси-сервер служит посредником между пользователем и целевым сервером.

Простой пример: Использование VPN для обхода геоблокировки.

- **Контроль доступа на уровне файловой системы**

Как работает: Устанавливаются права доступа к файлам и папкам.

Простой пример: Запрет на чтение/запись файла для всех, кроме администратора.

Организационные меры

Организационные меры — это набор правил и процедур, регулирующих доступ и обработку данных в организации.

- **Политики конфиденциальности**

Как работает: Описываются правила хранения, обработки и передачи данных.

Простой пример: Политика конфиденциальности на веб-сайте, где описано, как хранятся и используются персональные данные пользователей.

- **Обучение персонала**

Как работает: Персонал проходит обучение по правилам обработки данных и реагированию на инциденты.

Простой пример: Ежеквартальные тренинги по безопасности.

- **Логирование, аудит и мониторинг**

Как работает: Регулярная проверка соответствия действий сотрудников и систем политикам безопасности.

Простой пример: Ежемесячный аудит доступа к секретным файлам.

- **Физическая безопасность**

Как работает: Ограничение физического доступа к ресурсам.

Простой пример: Карточные системы доступа в серверную.

- **Процедуры реагирования на инциденты**

Как работает: Процедуры для быстрого и эффективного реагирования на инциденты безопасности.

Простой пример: Что делать, если обнаружена утечка данных.