

Информационная безопасность — это область, связанная с защитой информации от несанкционированного доступа, использования, раскрытия, модификации или уничтожения. Методы информационной безопасности разрабатываются для предотвращения утечки данных, защиты конфиденциальности и целостности информации, а также обеспечения доступности информационных активов. В данном обзоре представлены основные методы информационной безопасности, применяемые для защиты информации.

### ### 1. Криптография

Криптография — это метод шифрования данных таким образом, чтобы они могли быть прочитаны только теми, кто имеет ключ для расшифровки. Криптоалгоритмы делятся на симметричную и асимметричную криптографию. Симметричная криптография использует один и тот же ключ для шифрования и дешифрации, тогда как асимметричная криптография предполагает использование двух ключей: открытого ключа для шифрования и закрытого ключа для расшифровки.

### ### 2. Аутентификация

Аутентификация — это процесс подтверждения подлинности пользователей, устройств или сервисов. Аутентификационные методы включают пароли, токены, биометрические данные и одноразовые пароли (ОТР). Многофакторная аутентификация сочетает несколько методов для повышения безопасности.

### ### 3. Контроль доступа

Контроль доступа регулирует доступ к информационным ресурсам на основании ролей и привилегий пользователей. Политики контроля доступа определяют, какие пользователи имеют право выполнять те или иные операции с данными. Контролируемые списки доступа (ACL) и ролевой доступ (RBAC) являются распространёнными методами контроля доступа.

### ### 4. Файрволы и прокси-серверы

Файрволы фильтруют сетевые пакеты, блокируя нежелательный трафик. Прокси-серверы действуют как посредники между пользователями и внешними серверами, контролирующие доступ к Интернет-ресурсам. Эти методы защищают сеть от атак, блокируют вредоносный контент и ограничивают доступ к запрещённым сайтам.

### ### 5. Антивирусное ПО

Антивирусы обнаруживают и устраняют вредоносное ПО, предотвращая заражение системы. Антивирусы используют сигнатурные базы данных для распознавания вирусов, черви и троянские программы. Современные антивирусы также используют эвристические методы для обнаружения неизвестных угроз.

### ### 6. Интрузивные детекторы

Интрузивные детекторы выявляют подозрительную активность в сети, анализируя сетевой трафик. IDS (Intrusion Detection System) классифицирует события как атаки, отказы в обслуживании или нормальную деятельность. IPS (Intrusion Prevention System) предотвращает дальнейшую эксплуатацию уязвимости, блокировку трафика и изоляцию злоумышленников.

### ### 7. Виртуализация и контейнеризация

Виртуализация изолирует приложения и операционные системы, снижая риск компрометации всей системы. Контейнеры запускаются внутри виртуальной машины, создавая безопасную среду для тестирования и развертывания приложений. Docker и Kubernetes являются популярными инструментами для контейнеризации и оркестрации контейнеров.