Юрин Игорь Юрьевич

Блокчейн — это распределенная база данных, которая хранит информацию в виде непрерывной последовательной цепочки блоков. Каждый блок содержит данные и хеш предыдущего блока, что делает систему устойчивой к изменениям и атакам. Блокчейн используется для финансовых операций, идентификации пользователей и других приложений

Криптография — это наука и практика защиты информации от несанкционированного доступа. Она обеспечивает конфиденциальность, целостность и аутентификацию данных путем преобразования открытого текста в зашифрованный формат, доступный только авторизованным сторонам

Файервол — это программное или аппаратное средство, которое контролирует и фильтрует входящий и исходящий сетевой трафик на основе заранее определенных правил безопасности. Он помогает защитить компьютеры и сети от вредоносных атак и несанкционированного доступа.

Троян — это тип вредоносного ПО, которое маскируется под полезную программу, но на самом деле позволяет злоумышленникам получить несанкционированный доступ к компьютеру или сети. Трояны часто используются для кражи данных или установки других вредоносных программ.

Компьютерный вирус — это вредоносная программа, которая может реплицироваться и распространяться на другие компьютеры. Вирусы могут повреждать файлы, крадить данные или нарушать работу системы.

Майнинг — это процесс подтверждения транзакций в блокчейне с помощью мощных вычислительных ресурсов. В обмен на подтверждение транзакций майнеры получают вознаграждение в виде криптовалюты, например, биткоинов.

Flipper zero — это портативное устройство для хакеров и энтузиастов, которое позволяет исследовать и взаимодействовать с различными беспроводными протоколами, RFID, инфракрасными устройствами и другими технологиями.

Аутентификация — это процесс проверки личности пользователя или системы для обеспечения доступа к определенным ресурсам или данным. Это может включать пароли, биометрические данные или другие методы идентификации.

Брутфорс — это метод взлома пароля или криптографического ключа путем последовательного перебора всех возможных комбинаций. Этот метод часто используется злоумышленниками для получения несанкционированного доступа к системам или данным.

DDoS-атака (Distributed Denial of Service) — это тип кибератаки, при которой злоумышленники используют множество компьютеров для перегрузки системы или сайта трафиком, что приводит к его недоступности для легитимных пользователей.