**Тема:** «Алгоритмы взаимной проверки подлинности пользователей»

1. Характеристика взаимной проверки подлинности, назначение:

Взаимная проверка подлинности – это процесс, при котором две или более стороны подтверждают свою идентичность друг перед другом. Назначение этого процесса состоит в обеспечении безопасности и защите информации, предотвращении несанкционированного доступа, аутентификации пользователей и обеспечении конфиденциальности.

2. Охарактеризовать следующие механизмы взаимной проверки подлинности пользователей:

Механизм запроса-ответа:

* Сторона, желающая получить доступ, отправляет запрос на проверку подлинности.
* Сторона, имеющая доступ, отвечает на запрос, предоставляя необходимую информацию для подтверждения подлинности.

Механизм отметки времени:

* Включает использование временных меток для определения времени проведения операции проверки подлинности.
* Предотвращает повторные запросы и атаки с использованием ранее полученных данных.

Механизм "рукопожатие" (Handshake):

* Включает обмен информацией между сторонами для установления безопасного соединения.
* Обычно включает этапы идентификации, подтверждения и установления безопасного канала связи.

Непрерывная проверка подлинности:

* Систематическая проверка подлинности в течение всего сеанса взаимодействия.
* Обеспечивает дополнительный уровень безопасности, предотвращая атаки, которые могут произойти после установки сеанса.

3. Охарактеризовать следующие протоколы:

Протоколы идентификации с нулевой передачей знаний:

* Позволяют сторонам проверить подлинность друг друга, не передавая секретные знания напрямую.
* Часто используют криптографические методы, такие как доказательства знаний.

Параллельная схема идентификации с нулевой передачей знаний:

* Включает процесс взаимной проверки, при котором обе стороны могут убедиться в подлинности друг друга, не раскрывая свои секреты.
* Эффективен для обеспечения безопасной и анонимной идентификации.