# АНАЛІЗ КЛІЄНТСЬКОГО ТА СЕРВЕРНОГО ШИФРУВАННЯ

Бєльський О.Ю., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

**Метою доповіді** є дослідження різниці між клієнтським та серверним шифруванням, а також розгляд їх сильних та слабких сторін.

Клієнтське шифрування - це процес захисту даних на стороні користувача (клієнта). У цьому методі дані шифруються на пристрої користувача перед відправкою на сервер. Один із основних прикладів цього - HTTPS (SSL/TLS) шифрування, яке застосовується в браузерах під час з'єднання з веб-сервером [1]. Але на цьому використання клієнтського шифрування не обмежене і може бути використано як основа архітектури проекту.

Серед сильних сторін клієнтського шифрування можна відзначити конфіденційність - дані шифруються ще до відправлення на сервер, що запобігає зловмисним атакам на дані під час передачі. Контроль користувача - користувач має контроль над шифруванням своїх даних, що дозволяє йому забезпечити додатковий рівень безпеки. зменшення обсягу даних - зашифровані дані важко читати для незаконних осіб, що робить їх менш придатними для крадіжки чи зламу [2]. Але подібне шифрування має і свої недоліки: обмежене застосування - клієнтське шифрування не може захистити дані на сервері, коли вони розшифровуються для обробки. Потребує обслуговування на клієнтському боці - підтримка та налагодження шифрування на клієнтському боці може бути складнішою задачею. Серверне шифрування передбачає, що дані надсилаються на сервер у незашифрованому вигляді, і шифруються та розшифровуються лише на стороні сервера [2].

Щодо серверного шифрування то виділяють такі переваги: зручність - всі дані розшифровуються централізовано на сервері, що полегшує обслуговування та моніторинг шифрування. Захист від зловмисних клієнтів - серверний шифр захищає дані від недостовірних клієнтів. Але також очевидні і деякі недоліки: потенційна незахищеність під час передачі - дані надсилаються на сервер у незашифрованому вигляді, що може створювати ризик під час передачі на сервер. Збільшена залежність від сервера - при використанні серверного шифрування, сервер стає однією точкою вразливості.

Обираючи між клієнтським та серверним шифруванням, розробники повинні ретельно розглядати потреби проекту та дотримуватися найкращих практик забезпечення конфіденційності та безпеки даних. Комбінування обох методів також може бути варіантом, щоб забезпечити максимальну захищеність даних в веб-застосунках.

**Список літератури**

1. Rescorla, E. (2001). "SSL and TLS: Designing and Building Secure Systems." Addison-Wesley Professional.

2. Schneier, B. (2015). "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." W. W. Norton & Company..