

КОМПЛЕКСНИЙ ПОКАЗНИК ЯКОСТІ ОБСЛУГОВУВАННЯ КЛІЄНТІВ ETHERNET-МЕРЕЖ НА ОСНОВІ ПОСТКВАНТОВИХ АЛГОРИТМІВ

д-р техн. наук, проф. С.П. Євсєєв, канд. екон. наук, доц.

*В.С. Хвостенко, Національний технічний університет "Харківський
політехнічний інститут", м. Харків; асп. К.О. Бондаренко,*

Харківський національний економічний університет ім. С. Кузнеця

Розвиток сучасних технологій дозволяє суттєво розширити цифрові послуги. Для забезпечення послуг в Інтернет-просторі як правило використовуються протоколи цілісності SSL, TLS. Однак стрімкий розвиток обчислювальних технологій дозволяє зловмисникам не тільки модифікувати кіберзагрози, а також розробляти нові цільові загрози. Крім того поява повномасштабного квантового комп'ютера, як стверджують спеціалісти НІСТ США, дозволить зламувати симетричні та несиметричні криптосистеми на основі алгоритмів Гровера та Шора за поліноміальний час.

Запропонована схема модифікованого протоколу TLS на основі модифікованих (гібридних) крипто-кодових конструкцій забезпечує необхідний рівень стійкості до сучасних загроз постквантового періоду. Проведені дослідження підтверджують, що застосування еліптичних кодів (модифікованих еліптичних кодів) забезпечує швидкодію на рівні швидкості криптоперетворень симетричних криптоалгоритмів, доказову криптостійкість на основі теоретико-складності задачі декодування випадкового коду (забезпечується $10^{30} - 10^{35}$ групових операцій), і достовірність на основі використання укороченого алгеброгеометричного коду (забезпечується $P_{\text{пом}} = 10^{-9} - 10^{-12}$). Для подальшого зменшення потужності алфавіту (поля Галуа до GF (24–26) пропонується використовувати системи на збиткових кодах, що дозволяють одночасно формувати багатоканальні криптосистеми. Для дослідження властивостей запропонованого підходу використовується метод багатокритеріального аналізу, який дозволяє сформулювати комплексний показник якості обслуговування. Представлені дослідження підтверджують, що використання постквантових алгоритмів в якості алгоритму стійкості в протоколі TLS забезпечують підвищення ефективності на 30% при використанні в мережі на основі Gigabit Ethernet, та в 2 рази при використанні 10 Gb Ethernet.