УДК 004. 056.5 (043) **doi: 10.26906/SUNZ.2021.3.082**

С. П. Євсеєв, В. С. Хвостенко, К. О. Бондаренко

Харківський національний економічний університет імені С. Кузнеця, Харків, Україна

РОЗРОБКА КОМПЛЕКСНОГО ПОКАЗНИКА ЯКОСТІ ОБСЛУГОВУВАННЯ НА ОСНОВІ ПОСТКВАНТОВИХ АЛГОРИТМІВ

Анотація. 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. В роботі пропонується модифікація протоколу TLS на основі використання, в якості алгоритма, який забезпечує стійкість протоколу TLS, використання постквантових алгоритмів на основі крипто-кодових конструкцій Мак-Еліса та Нідеррайтера на еліптичних кодах. Для дослідження властивостей запропонованого підходу використовується метод багатокритеріального аналізу, який дозволяє сформувати 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.

Ключові слова: постквантовий період, протокол цілісності, крипто-кодові конструкції Нідеррайтера, еліптичні коди.

Вступ

Формулювання проблеми. Розвиток сучасних технологій, обчислювальних систем суттєво поширив спектр цифрових послуг практично у всіх галузях людства. Це дозволило за останні п'ять років поширити використання кіберпростору щодо створення е-послуг, використання IoT-речей, значного поширення мобільних технологій "G", створення умов переходу на NGN-мережі, з одного боку. З іншого поширення кіберзагроз, щорічну зміну векторів загроз, придбання ними ознак гібридності та синергізму. В таких умовах висуваються більш жорсткі вимоги щодо систем забезпечення вірогідності та конфіденційності інформаційних потоків, що своєю чергою вимагає модифікації механізмів, що існують та/або розробку нових підходів щодо забезпечення необхідного рівня надійності та безпеки якості обслуговування та працездатності відповідних систем та мереж в цілому.

Однак з ростом обчислювальних можливостей зростає кількість кібератак на інформаційно-комунікаційні системи та мережі (ІКСМ), кіберфізичні системи (CPS) та системи IoT. Вектор загроз в кіберпросторі постійно змінюється, загрози набувають ознак гібридності на синергізму, що дозволяє формувати цільові атаки, створювати нові та/або модифікувати застарілі загрози. Для забезпечення безпеки як правило використовуються симетричні та несиметричні криптосистеми. Однак з появою повномасштабного квантового комп'ютера з використанням алгоритмів Гровера та Шора, вони можуть бути зламані, що може привести до хаосу в кіберпросторі. Тому на сьогоднішній час висуваються більш жорсткі вимоги щодо протоколів забезпечення послуг безпеки – конфіденційності та цілісності. Прикладом такого протоколі є протокол *Transport layer security* (*TLS*), який забезпечує шляхом симетричних алгоритмів послуги безпеки – цілісність та автентичність. Таким чином в умовах постквантового періоду стає актуальним науково-прикладним завданням створення нового або модифікація даного протоколу.

Аналіз літератури. Проведений аналіз показника якості обслуговування мережі визначає два підходи до його забезпечення [1–5]. Перший підхід, полягає в гарантованому забезпеченні користувачеві дотримання деякої числової величини показника якості обслуговування (забезпечення встановленого показника середньої пропускної здатності, показника часу затримки передачі і т.д.). Другий підхід полягає в пріоритетному обслуговуванні користувачів відповідно до встановленої ієрархією мережі. Таким чином, якість обслуговування залежить від ступеня привілейованості користувача або групи користувачів, до якої він належить. Для уповноважених користувачів інформаційно-комунікаційних систем та мереж (ІКСМ) якість обслуговування не гарантується, а гарантується тільки рівень їх привілеїв. Таким чином основними критеріями якості обслуговування є надійність та безпека, при цьому роль останнього критерію зростає з поширенням цифрових послуг та зростанням рівня обчислювальних технологій.

Проведений аналіз загроз [6–10] показав, що на сьогодні на перше місце виходять цільові загрози з характерними рисами гібридності та синергізму, які забезпечують зловмисникові емерджентні властивості.

Крім того, вектор загроз суттєво залежить від обчислювальних можливостей, і як показав аналіз [6–10] бурхливе зростання обчислювальних можливостей, можливість появи повномасштабного квантового комп'ютера дозволяє створювати не тільки гібридні загрози, а також цільові атаки, які мають ознаки синергізму та дозволяють зловмисникам домагатися свої мети в найкоротші строки. В таких умовах необхідна модифікація сучасних протоколів забезпечення послуг, та/або розробка нових. В умовах постквантового періоду необхідно використовувати криптосистеми, які здатні протистояти алгоритмам Шора та Гровера. Одним з перспективних напрямків є алгоритми на основі крипто-кодових

конструкцій (ККК) Мак-Еліса та Нідеррайтера. Так класична схема Мак-Еліса є претендентом на алгоритм постквантовой криптографії, який проводиться НІСТ США [11].

В роботах [6, 12] пропонується використовувати гібридні крипто-кодові конструкції, які дозволяють зменшити енергоємність при їх практичної реалізації та зберегти рівень стійкості.

Розглянемо формальний опис математичної моделі ГККК Нідеррайтера, яка задається сукупністю таких елементів [6]:

– множина відкритих текстів

$$M = \left\{ M_1, M_{2,} ... M_{q^k} \right\},$$

де $M_i = \left\{ e_0, e_{h_1}, ... e_{h_k}, e_{e-1} \right\}$, $\forall e_e \in GF(q)$; h_e – символи вектору помилки, що дорівнюють нулю, $/h/ = \frac{1}{2} e$, тобто $e_i=0$, $\forall e_i \in h$;

– множина закритих текстів

$$S = \left\{ S_0, S_1, ... S_{q^r} \right\},$$

де $S_i = \left\{ S^*_{X_0}, S^*_{h_1}, ... S^*_{h_j}, S^*_{X_r} \right\}$, $\forall S_{X_r} \in GF(q)$;

– множина прямих відображень (на основі використання відкритого ключа – перевірочної матриці еліптичного коду (*EC*)

$$\varphi = \left\{ \varphi_1, \varphi_2, ..., \varphi_r \right\},$$

де $\varphi_i : M \to S_{r-h_e}$, $i = 1, 2, ..., e$;

– множина обернених відображень (на основі використання закритого (особистого) ключа – матриць маскування)

$$\varphi^{-1} = \left\{ \varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_r^{-1} \right\},$$

де $\varphi_i^{-1} : S_{r-h_e} \to M$, $i = 1, 2, ..., e$;

– множина ключів, які параметризують прямі відображення (відкритий ключ уповноваженого користувача):

$$KU_{a_i} = \left\{ KU_{1_{a_i}}, KU_{2_{a_i}}, ..., KU_{r_{a_i}} \right\} = \left\{ H^{EC_1}_{X_{a_i}}, H^{EC2}_{X_{a_i}}, ..., H^{ECr}_{X_{a_i}} \right\},$$

де $H^{EC_i}_{X_{a_i}}$ – перевірочна $r \times n$ матриця замаскованого під випадковий код алгеброгеометричного блокового (n, k, d) коду з елементами $GF(q), 0$ тобто $\varphi_i : M \xrightarrow{KU_{i_{aj}}} S^*_{r-h_e}$, $i = 1, 2, ..., e$, a_i – набір коефіцієнтів многочлена кривої $a_1 ... a_6$, $\forall a_i \in GF(q)$, однозначно задає конкретний набір точок кривої з простору P^2;

– множина ключів, які параметризують обернені відображення (особистий (закритий) ключ уповноваженого користувача):

$$KR = \left\{ KR_1, KR_2, ..., KR_r \right\} = \left\{ \left\{ X, P, D \right\}_1, \left\{ X, P, D \right\}_2, ..., \left\{ X, P, D \right\}_r \right\},$$

$$\left\{ X, P, D \right\}_i = \left\{ X^i, P^i, D^i \right\},$$

де X^i – маскуюча невироджена випадково рівноймовірно сформована джерелом ключів $k \times k$ матриця з елементами зі $GF(q)$; P^i – перестановочна випадково рівноймовірно сформована джерелом ключів $n \times n$ матриця з елементами з $GF(q)$; D^i – діагональна сформована джерелом ключів матриця з елементами з $GF(q)$, тобто $\varphi_i^{-1} : S^*_{r-h_e} \xrightarrow{KR_i} M$, $i = 1, 2, ..., s$. Складність виконання оберненого відображення ϕ_i^{-1} без знання ключа $K_i^* \in K^*$ пов'язана з розв'язанням теоретико-складної задачі декодування випадкового коду (коду загального положення).

– множина збиткових текстів *CFT*,

$$CFT = \{ CFT_1, CFT_2, ..., CFT_{q^k} \};$$

– множина збитків *CHD*,

$$CHD = \{ CHD_1, CHD_2, ..., CHD_{q^k} \};$$

– множина прямого нанесення збитку (на основі використання ключа – K^i_{MV2}, і алгоритму *MV*2)

$$E = \{ E^1_{K_{MV2}}, E^2_{K_{MV2}}, ..., \phi^S_{K_{MV2}} \},\ i = 1, 2, ..., s;$$

– $f(x)_i$ – флаг (збиток, *CHD*), $C(x)_i$ – залишок (збитковий текст, *CFT*); $f(x)=n - |C(x)|$, якщо $|C(x)| > r$, де r – деякий параметр, $r \in_R Z_{q^m}$, $0 \langle r \langle n$;

– множина відображень *MV*2 F_n^r, що задає бієктивне відображення між множиною перестановок $\{S_1, S_2, ..., S_{2^n}\}$ і $\# F_n^r$, $\# F_n^r = \#\{(c, f)\} = 2^n!$;

– множина осмисленого тексту (на основі використання ключа – K^i_{MV2}, і алгоритму *MV*2)

$$E^{-1} = \{ E^1_{K_{MV2}}{}^{-1}, E^2_{K_{MV2}}{}^{-1}, ..., E^S_{K_{MV2}}{}^{-1} \},$$

де $E^{-1}_{K_{MV2}} : \| f(x)_i \| + \| C(x)_i \| \to M$, $i = 1, 2, ..., s$;

$f(x)_i$ – флаг (збиток, *CHD*), $C(x)_i$ – залишок (збитковий текст, *CFT*); $f(x)=n - |C(x)|$, якщо $|C(x)| > r$, де r – деякий параметр, $r \in_R Z_{q^m}$.

Вихідними даними при описі розглянутої несиметричною крипто-кодової системи захисту інформації є:

– недвійковий рівноважний код над *GF(q)*, тобто множина послідовностей довжини n та ваги $w(\varepsilon_i)$;

– алгеброгеометричний блоковий *(n, k, d)* код C над *GF(q)*, тобто така множина кодових слів $C_i \in C$, що виконується рівність $C_i H^T = 0$, де H – перевірочна матриця алгеброгеометричного блокового коду;

– *IV* – вектор ініціалізації, *IV*= |*h*| =½ h_e – елементи скорочення (h_e – символи вектору помилки, рівні нулю, /*h*/=1/2*e*, тобто $e_i = 0,\ \forall e_i \in h$);

– маскуючи матричні відображення, задані множиною матриць $\{X, P, D\}_i$, де X – невироджена $k \times k$ матриця над *GF(q)*; P – перестановочна $n \times n$ матриця над *GF(q)* з одним ненульовим елементом в кожному рядку і в кожному стовпці матриці; D – діагональна $n \times n$ матриця над *GF(q)* з ненульовими елементами на головній діагоналі;

– r – деякий параметр,

$$r \in_R Z_{q^m},\ Z_{q^m} = \left\{0,1,...2^n - 1\right\};$$

– n – деякий параметр

$$n \in_R Z_{q^n},\ Z_{q^n} = \left\{1,...2^n\right\};$$

– множина відображень *MV*2 – F_n^r.

На основі рівноважного кодування формується закритий текст $C_j \in C$ за введеним відкритим текстом $M_i \in M$ і заданим ключем H_X^{ECu}, $u \in \{1,2,...,s\}$. Це здійснюється шляхом формування синдромної (в термінах завадостійкого кодування) послідовності S_{X_j}, що відповідає рівноважній послідовності

$$M_i = e = \{e_0, e_1, ..., e_{n-1}\}:$$

$$S_{X_j} = \phi_u\left(M_i, H_X^{ECu}\right) = M_i \times \left(H_X^{ECu}\right)^T,$$

причому вага Гемінга (кількість ненульових елементів) вектору e не перевищує виправної здатності використовуваного алгебраїчного блокового (n,k,d) коду: $\forall i: 0 \le w(M_i) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Потужність множин *M* та *C* визначається допустимим спектром ваг $w(M_i)$, тобто в загальному випадку (для всіх допустимих значень $w(M_i)$) маємо: $m = \sum_{i=0}^{t} (q-1)^i \times C_n^i$, де C_n^i – біноміальний коефіцієнт, $C_n^i = \frac{n!}{i! \cdot (n-1)!}$.

Найбільш доцільно величину $w(M_i)$ вибирати відповідно до необхідного значенням рівня безпеки.

Тоді для $w(M_i) = const = w(e)$ маємо:

$$m = (q-1)^{w(e)} \times C_n^{w(e)},$$

а послідовність $M_i = \{e_0, e_1, ..., e_{n-1}\}$ з множини $M = \{M_1, M_2, ..., M_m\}$ формується як результат деякого відображення ψ, реалізованого шляхом надлишкового кодування недвійковими рівноважними кодами ненадлишкових інформаційних послідовностей.

Сформований закритий текст $C_j \in C$ однозначно відповідає вектору $M_i = \{e_0, e_1, ..., e_{n-1}\}$.

Сформуємо вектор ініціалізації *IV*=*EC*–h_j, де h_j – інформаційні символи, що дорівнюють нулю, $|h| = k/2$, тобто $I_i = 0,\ \forall I_i \in h$. Формування укороченого вектору помилки $e_x = e(A) - IV$.

Відкритий ключ формується шляхом множення перевірочної матриці алгеброгеометричного коду на матриці маскування:

$$H_X^{ECu} = X^u \cdot H \cdot P^u \cdot D^u,\ u \in \{1,2,...,s\},$$

де H^{EC} – перевірочна $n \times (n-k)$ матриця алгеброгеометричного блокового (n,k,d) коду з елементами з $GF(q)$.

В алгоритм *MV*2 надходить синдромна послідовність:

$$S^*_{r-h_e} = (e_n - h_e) \times H_X^{ECT}.$$

В *MV*2 синдромна послідовність $S^*_{r-h_e}$ перетворюється на залишок і флаг:

$$E_{K_{MV2}}: S^*_{r-h_e} \to \left\| f(x)_i \right\| + \left\| C(x)_i \right\|.$$

В канал зв'язку поступає $\left\| f(x)_i \right\|$ *та* $\left\| C(x)_i \right\|$, при цьому передача може здійснюватися як за одному, так і по двох незалежних каналах.

На стороні прийому уповноважений користувач, який знає правило нанесення збитку F_n^r, маскування (набір матриць $\{X,P,D\}_u = \{X^u, P^u, D^u\}$) і вектору ініціалізації (кількість і місця нульових символів вектору помилки):

$$E^{-1}_{K_{MV2}}: \left\| f(x)_i \right\| + \left\| C(x)_i \right\| \to S^*_{r-h_e},$$

формує кодову послідовність як одне (будь-яке) з можливих рішень рівняння: $S^*_{r-h_e} = c^*_{X_i} \cdot H^T_{X_j}$, тобто знаходить такий вектор $c^*_{X_i}$, який розкладається на суму: $c^*_{X_i} = c_{X_i} + M_i$, де c_{X_i} – одне (будь-яке) з можливих кодових слів замаскованого коду з перевірочної матрицею $H^T_{X_j}$, тобто $c_{X_i} \times H^T_{X_j} = 0$. Далі уповноважений користувач, використовуючи набір матриць $\{X,P,D\}_u = \{X^u, P^u, D^u\}$, формує вектор:

$$\bar{c}^* = c^*_X \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1},$$

тобто демаскує кодову послідовність $c^*_{X_i}$.

Після підстановки отримаємо рівність:

$$\bar{c}^* = c^*_X \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$

$$= \left(c_{X_i} + M_i\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$

$$= c_{X_i} \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} + M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}.$$

Уповноважений користувач, який сформував вектор, має можливість застосувати швидкий (поліноміальної складності) алгоритм завадостійкого декодування і сформувати таким чином вектор

$$\overline{c}^* = c_X^* \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$$

та вектор

$$M_i^u = M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}.$$

Для відновлення інформаційної рівноважної послідовності M_i достатньо знову помножити вектор M_i^u на матриці маскування D^u та P^u, але в іншому порядку:

$$M_i = M_i^u \cdot P^u \cdot D^u =$$

$$= M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} \cdot P^u \cdot D^u = M_i.$$

Формування шуканого вектору помилки e:

$$M = M_i + IV.$$

Аналіз практичної реалізації алгоритмів шифрування / розшифрування в ГККК Нідеррайтера показує, що при формуванні криптограми (синдрому) після формування вектору помилки алгоритмом рівноважного кодування на основі вектору ініціалізації (формується ПВП і передається закритими каналами або вектор шифрується алгоритмом *MV*2 і передається двома незалежними відкритими каналами) проводиться скорочення – h_e (символи вектору помилки, що дорівнюють нулю), $/h/=1/2e$, тобто $e_i = 0, \forall e_i \in h$. При розшифруванні криптограми (після отримання вектору помилки, перед використанням алгоритму рівноважного кодування) для отримання інформації вводяться "нульові" символи укорочення.

Розроблення протоколу TLS з використанням постквантових алгоритмів на основі крипто-кодових конструкцій

В поточній версії протоколу доступні такі алгоритми [13]:

– для обміну ключами і перевірки їх справжності використовують комбінації алгоритмів: RSA (асиметричний шифр), Diffie-Hellman (безпечний обмін ключами), DSA (алгоритм цифрового підпису) і алгоритми технології Fortezza;

– для симетричного шифрування: RC2, RC4, IDEA, DES, Triple DES або AES;

– для геш-функцій: MD5 або SHA.

Однак проведений аналіз [14, 15] сучасних загроз показав, що вони набувають ознак гібридності та синергізму. Крім цього поява повномасштабного квантового комп'ютера суттєво зменшує стійкість алгоритмів, які використовуються. Крипто-кодові конструкції Мак-Еліса та Нідеррайтера дозволяють забезпечити необхідний рівень стійкості, оперативності та достовірності. Це підтверджується проведеними попередніми дослідженнями [6, 9, 12].

На рис. 1 запропонована схема використання крипто-кодових конструкцій в протоколі TLS.

Пропонується використовувати ККК Мак-Еліса для забезпечення безпеки передачі сертифікатів (їх обміну між користувачем і сервером), а для забезпечення безпеки передачі повідомлень і запитів – використовувати крипто-кодові конструкції Нідеррайтера. Такий підхід забезпечить необхідний рівень безпеки і достовірності в умовах сучасних кіберзагроз та бурхливого зростання обчислювальних ресурсів.

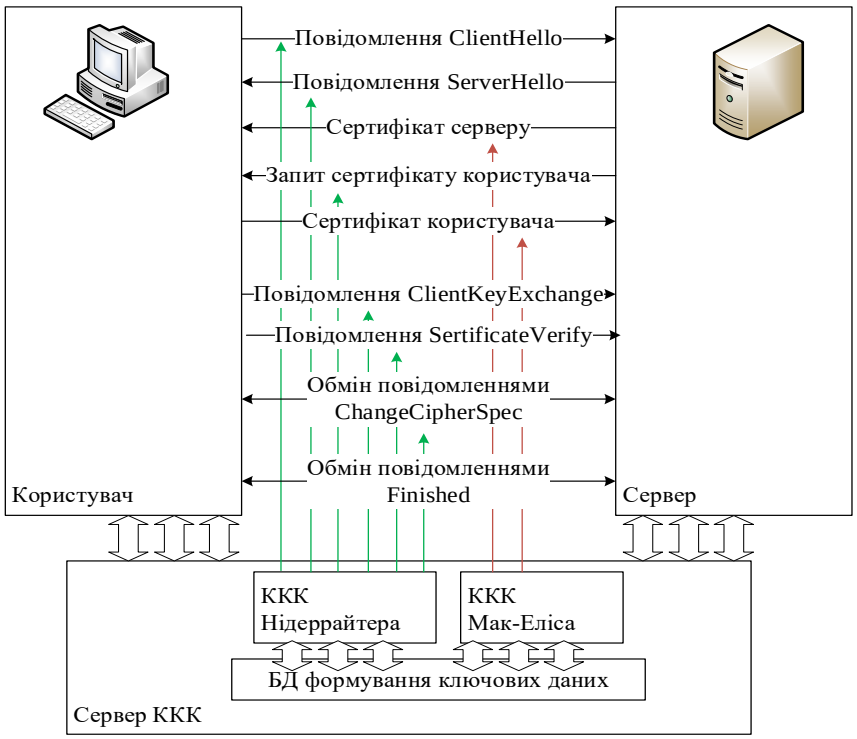

Рис. 1. Структурна схема протоколу TLS з використанням крипто-кодових конструкцій

На рис. 2 та в табл. 1 наведені результати досліджень часових витрат на забезпечення необхідного рівня безпеки в протоколі TLS.

Аналіз рис. 2 показав. що для обміну даними в протоколі TLS забезпечує необхідний рівень оперативності, при цьому забезпечуючи і необхідний рівень безпеки.

Використання пропонованої модифікації протоколу забезпечить його використання в умовах повномасштабного квантового комп'ютера.

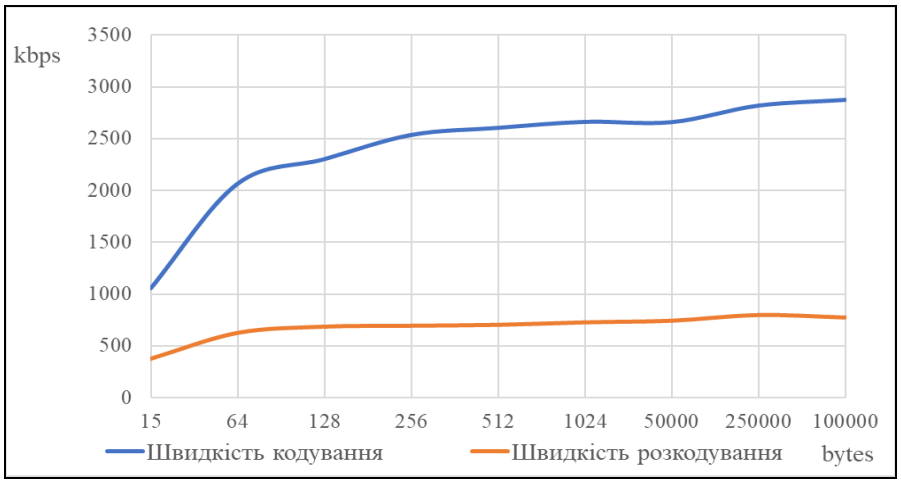

Рис. 2. Оцінка витрат часу на виконання шифрування / розшифрування ККК

Таблиця 1 – **Оцінка витрат часу на виконання шифрування / розшифрування крипто-кодових конструкцій**

Кількість інформації, байт	Швидкість кодування, кбайт/с	Швидкість разкодування, кбайт/с
15	1052	373
64	2063	624
128	2301	684
256	2535	693
512	2604	702
1024	2662	726
50000	2659	742
250000	2819	797
100000	2874	773

Розробка комплексного показника якості обслуговування на основі крипто-кодових конструкцій

Для оцінки комплексного показника ефективності були розроблені опорні таблиці, що дозволяють виділити діапазони зміни необхідних параметрів і визначити їх в умовних балах. Цей простий метод дозволяє отримати досить адекватні результати оцінки, і крім того, об'єднати їх з результатами точних розрахунків за окремими конкретними параметрами. В опорних табл. 2–9 наведені параметри систем передачі даних, які враховуються в інтегральному показнику функціональної ефективності *IP*-мережі [16].

Таким чином, на основі моделі багатофакторного аналізу можливо описати абсолютно різні параметри, які в інший спосіб аналітично об'єднати практично неможливо.

Таблиця 2 – **Вартість розгортання мережі**

Бали	Опис параметру
1	Дуже висока вартість
2	Висока вартість
3	Середня вартість
4	Низька вартість
5	Дуже низька вартість

Таблиця 3 – **Швидкість передачі даних**

Бали	Опис параметру
1	Мала (10Мб/с)
2	Середня (100 Мб/с)
3	Висока (1Гб/с)
4	Дуже висока (10Гб/с)
5	Надзвичайно висока (40 Гб/с)

Таблиця 4 – **Ймовірність доставки пакету**

Бали	Опис параметру
1	Мала (> 0)
2	Середня (0.95)
3	Висока (0.97546)
4	Дуже висока (0.999999)

Таблиця 9 – **Рівень безпеки**

Бали	Опис параметру
1	критичний
2	Малий
3	середній
4	високий

Таблиця 6 – **Затримка пакету**

Бали	Опис параметру
1	Велика
2	Середня
3	Мала

Таблиця 7 – **Продуктивність мережі**

Бали	Опис параметру
1	Мала
2	Середня
3	Висока

Таблиця 5 – **Час доставки пакету**

Бали	Опис параметру
1	Дуже великий (1875 с)
2	Великий
3	Середній
4	Малий (0.006 с)
5	Дуже малий (0.0003 с)

Таблиця 8 – **Рівень загроз**

Бали	Опис параметру
1	Критичний
2	високий
3	середній
4	малий
5	дуже малий

Для порівняння існуючих технологій передачі даних було відібрано наступні: пакетна комутація за стандартами глобальних обчислювальних мереж (ГОМ): *Gigabit, 10 Gb, 40 Gb Ethernet*. Порівняльні характеристики зазначених технологій показані в табл. 10, 11.

Таблиця 10 – **Порівняльна характеристика протоколу Ethernet**

Технологія ГОМ	Вартість	Швидкість передачі даних, Мбіт/с	Довжина пакету, біт	Ймовірність правильної доставки пакету, $P_{пр.п}$	Час доставки пакету, $t_д$, с
Gigabit Ethernet	висока	1000	1518	0.99999	0.006
10 GbE	висока	10 000	1518	0.99999	0.006
40GbE	висока	40 000	1518	0.99999	0.006

Таблиця 11 – **Узагальнена ефективність мереж передачі даних**

Технологія з використанням *TLS*	Умовні бали									
	група								узагальнений індекс ефективності	Відносна ефективність,%
	1	2	3	4	5	6	7	8		
Gigabit Ethernet	3	3	3	1	2	1	1	1	54	10,6
10 Gb Ethernet	2	4	3	2	2	1	1	1	96	18,8
40 Gb Ethernet	1	5	3	3	2	1	2	2	360	70,6
Всього:									510	100
Технологія з використанням модифікованого *TLS*										
Gigabit Ethernet	3	3	4	5	3	3	4	4	25920	40,9
10 Gb Ethernet	2	4	4	5	3	3	4	4	23040	36,4
40 Gb Ethernet	1	5	4	5	3	3	4	4	14400	22,7
Всього:									63360	100

Використовуючи дані з табл. 2–10, отримуємо таблицю узагальненої ефективності мереж передачі даних, де відібрані показники вже подано в умовних балах в діапазоні від 1 до 5. Крім цього враховуються показники не тільки надійності, а також і безпеки в умовах цільових атак з ознаками синергізму та гібридності, що дозволяє отримати комплексний показник якості обслуговування. В табл. 11 група: 1 – вартість розгортання мережі; 2 – швидкість передачі даних; 3 – ймовірність доставки пакету; 4 – час доставки пакету; 5 – затримка пакету; 6 – продуктивність мережі; 7 – рівень загроз; 8 – рівень безпеки.

Отримані результати використання відповідних технологій кіберпростору з використанням протоколу TLS, та з використанням запропонованих моделей та методів його модифікації у табл. 11 свідчать, що використання запропонованих рішень не тільки збільшує показник рівня безпеки, а також дозволяє забезпечити можливість передачі даних з прямим виправленням помилок за рахунок використання методів завадостійкого кодування в крипто-кодової конструкції Нідеррайтера, що дозволяє підвищити рівень якості обслуговування до максимальних значень безпеки та надійності при використанні технології *Gigabit Ethernet*, та *10 Gb Ethernet*.

Таким чином, приведені результати свідчать про необхідність використання нових, або модифікованих/інтегрованих механізмів забезпечення не-

обхідних рівнів надійності та безпеки інформації в інформаційних системах та кіберпросторі.

Висновки

1. 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 *MEC* (*EC*) забезпечує швидкодію на рівні швидкості криптоперетворень симетричних криптоалгоритмів, доказову криптостійкість на основі теоретико-сложностної задачі декодування випадкового коду (забезпечується 10^{30} – 10^{35} групових операцій), і достовірність на основі використання укороченого алгеброгеометричного коду (забезпечується $P_{пом}$=10^{-9}–10^{-12}). Для подальшого зменшення потужності алфавіту (поля Галуа до *GF* (2^4–2^6) пропонується використовувати системи на збиткових кодах, що дозволяють одночасно формувати багатоканальні криптосистеми.

2. Удосконалений метод оцінки якості обслуговування інформаційних систем на основі багатокритеріальної оцінки, що дозволило, на відміну від існуючих виділити діапазони зміни параметрів критеріїв надійності та безпеки визначити їх в умовних балах. Запропонований модифікований протокол TLS на ККК Нідеррайтера дозволяє збільшити відносну ефективність в мережі на основі *Gigabit Ethernet* з 10,6% до 40,9%, а на основі 10 *Gb Ethernet* з 18,8% до 36,4%, що свідчить про ефективність запропонованого підходу.

СПИСОК ЛІТЕРАТУРИ

1. Яновский Г. Г. Качество обслуживания в сетях IP / Г.Г. Яновский // Вестник связи. – 2008. – №1. – С. 1 – 16.
2. ISO 9000:2005. Системы менеджмента качества. Основные положения и словарь [Електронний ресурс]. URL: https://www.iso.org/obp/ui#iso:std:iso:9000:ed-3:v1:ru.
3. Рекомендация МСЭ Е.800. [Електронний ресурс]. URL: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809. Дата звернення: 20.05.2021.
4. Рекомендация МСЭ X.134// [Електронний ресурс]. URL: www.itu.int/rec/T-REC-X.134. Дата звернення: 20.05.2021.
5. Рекомендация МСЭ-Т Е.802 Принципы и методики определения и применения параметров QoS [Електронний ресурс]. URL: https://www.itu.int/rec/T-REC-E.802-200702-I/es. Дата звернення: 20.05.2021.
6. Edited by Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
7. Yevseiev and other. Development of conception for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies. 2021. 3/9 (111). P. 63–83.
8. O. Shmatko and other. Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies ISSN 1729-3774 3/9 (105) 2020. p. 6–19.
9. Tsyhanenko. Development of digital signature algorithm based on the Niederriter crypto-code system / O. Tsyhanenko // Information Processing Systems, 2020. – Issue 3 (162) – С. 86 –94.
10. Р. В. Грищук, та Ю. Г. Даник. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016.
11. Round 3 Submissions - Post-Quantum Cryptography.URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions
12. Development of Niederreiter hybrid crypto-code structure on flawed codes / S. Yevseiev, O. Tsyhanenko, A. Gavrilova, V. Guzhva, O. Milov, V. Moskalenko, I. Opirskyy, O. Roma, B. Tomashevsky, O. Shmatko // Eastern-European Journal of Enterprise Technologies, 2019. – № 1/9 (97). – p. 27–38
13. Описание протоколов SSL/TLS. URL: www.cryptopro.ru/sites/default/files/docs/TLS_description.pdf
14. Р. В. Грищук, та Ю. Г. Даник, "Синергія інформаційних та кібернетичних дій", Труди університету. НУОУ, № 6 (127), с. 132–143. 2014.
15. Р. В. Грищук, "Синтез систем інформаційної безпеки за заданими властивостями", Вісник національного університету "Львівська політехніка". Серія : Автоматика, вимірювання та керування : зб. наук. пр., ЛП, № 74, с. 271 –276, 2012.
16. С. П. Євсеєв, С. Е. Остапов, Х. Н. Рзаєв, та В. І. Ніколаєнко, "Оцінка обміну даними в глобальних обчислювальних мережах на основі комплексного показника якості обслуговування мережі", Науковий журнал Радіоелектроніка, інформатика, управління, № 1(40), с. 115 – 128, 2017.

Received (Надійшла) 28.06.2021
Accepted for publication (Прийнята до друку) 25.08.2021

Development of a comprehensive service quality indicator based on postquantum algorithms

Serhii Yevseiev, Vladyslav Khvostenko, Kyrylo Bondarenko

Abstract. The development of modern technologies allows expanding digital services significantly. SSL and TLS integrity protocols are commonly used to provide services in the Internet. However, the rapid development of computing technologies allows attackers not only to modify cyber threats, but also to develop new-targeted threats. In addition, the advent of a full-scale quantum computer, according to US NIST experts, will break symmetric and asymmetric cryptosystems based on Grover's and Shor's algorithms in polynomial time. The paper proposes a modification of the TLS protocol based on the use, as an algorithm that ensures the stability of the TLS protocol, the use of post-quantum algorithms based on crypto-code constructions of McEliece and Niederreiter on elliptical codes. To study the properties of the proposed approach, the method of multicriteria analysis is used, which allows to form a comprehensive indicator of service quality. The presented studies confirm that the use of post-quantum algorithms as a stability algorithm in the TLS protocol provides a 30% increase in efficiency when used in a network based on Gigabit Ethernet, and 2 times when using 10 Gb Ethernet.

Keywords: post-quantum period, integrity protocol, Niederreiter crypto-code constructions, elliptical codes.