УДК 621.391

Сергій ЄВСЕЄВ,
кандидат технічних наук, доцент,
Харківський національний економічний університет
імені Семена Кузнеця, м. Харків

Олександр АНДРОЩУК,
доктор технічних наук, професор,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького, м. Хмельницький

МЕТОД БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ МОДИФІКОВАНИХ КРИПТО-КОДОВИХ СИСТЕМ НІДЕРРАЙТЕРА – МАК-ЕЛІСА

Упровадження OTP-технологій (Technology of One-Time Passwords) дозволить зменшити ризики, з якими стикаються IT-фахівці ІОС при використанні довгострокових паролів. Аналізуються способи формування OTP паролів, основні загрози використання. Розглянуто математичні моделі побудови протоколу багатофакторної аутентифікації на основі гібридних крипто-кодових конструкцій на збиткових кодах (ГККК3К), запропоновані практичні алгоритми їх реалізації.

Ключові слова: *багатофакторна аутентифікація, гібридні крипто-кодові конструкції на збиткових кодах, одноразові паролі.*

Постановка проблеми у загальному вигляді. Розвиток інформаційних службових мереж (ІСМ) тісно пов'язаний із завданням забезпечення безпеки мережі. Розв'язок формується з багатьох складових,

одна з них – безпечна аутентифікація. OTP-технології (Technology of One-Time Passwords) дозволяють зменшити ризики, з якими зустрічаються ІТ фахівці ІСМ при використанні довготривалих паролів, що запам'ятовуються.

Подальший розвиток інформаційно-телекомунікаційних систем (ІТС) на основі інформатизації послуг і використання дистанційного доступу до ресурсів мережі висуває нові вимоги до забезпечення безпеки (цілісності, конфіденційності, доступності й автентичності) під час службової діяльності. Для забезпечення автентичності в ІСМ (ІТС), як правило, використовується електронний цифровий підпис на основі багатофакторної або розширеної аутентифікації. Вона заснована на спільному використанні декількох факторів аутентифікації (знань, засобів або об'єктів зберігання однієї з інформаційних складових легітимної процедури аутентифікації). Такий підхід значно підвищує безпеку використання інформації, щонайменше з боку користувачів, що підключаються до інформаційних систем по захищених і незахищених каналах комунікацій. Серед методів багатофакторної аутентифікації поширення набув метод, заснований на sms аутентифікації. Однак його використання несе істотні ризики для безпеки. Необхідним є використання інших, більш безпечних способів, таких як застосування генераторів одноразових паролів (TOTP – Time-based One-time Password Algorithm) з додатковим криптографічним захистом.

Аналіз останніх досліджень і публікацій, в яких започатковано вирішення даної проблеми та на які опираються автори. Основними механізмами електронної аутентифікації є механізми на основі симетричного й несиметричного шифрування, електронному цифровому підпису (у механізмах технологій PKI (стандарт X.509), сертифікатах Ipsec, PGP, S/MIME), процедури формування MDC і Mac-кодів [1–3]. У роботі [4] розглянуті основні вимоги до архітектури й механізмів безпеки в стільниковій технології четвертого покоління (4G, Long Term Evolution (LTE), основою безпеки яких є механізми захисту в стеці протоколів TCP\IP і Mac-коди. У стандарті [7] запропоновані похідні алгоритму SHA-3 (Keccak) формування Mac-кодів на

основі алгоритмів похідних SHAKE, KMAC, Tuple Hash і Parallel Hash, кожний з яких визначений для 128-і 256-бітної послідовності Маскодів.

Особливе місце серед механізмів електронної аутентифікації (ЕА) займають методи двохфакторної аутентифікації, засновані на різних смарт-картах, Usb ключах, OTP паролях [5, 6, 8-10]. Методи багатофакторної аутентифікації набули широке поширення серед організацій хайтека, фінансового й страхового секторів ринку, великих банківських установ і підприємств держсектора. Тенденції консьюмерізації в ІТС приводять до того, що користувачам потрібно використовувати різні типи обладнань для доступу до ресурсів ІТС – використовується стаціонарний або мобільний комп'ютер, планшет або смартфон [5, 6]. Технологія одноразових паролів (OTP) може допомогти реалізувати строгу двохфакторну аутентифікацію й не зажадає істотних витрат на впровадження й підтримку [5]. Такий пароль практично невразливий для атаки мережевого аналізу пакетів і додатково вимагає від користувача введення Pin коду, що є додатковим чинником аутентифікації [5]. Таким чином, формується двохфакторна аутентифікація користувача в системі на основі володіння чимнебудь (Authentication by Ownership) або на основі знання чого-небудь (Authentication by Knowledge) [5].

Зворотним боком використання OTP паролів є можливість "перехоплення" зловмисником тексту (sms повідомлення) з однієї частиною токена. Атакуючі можуть скомпрометувати двохфакторну аутентифікацію на основі методів соціальної інженерії (переадресація повідомлень через провайдера за допомогою IMSI уловлювача (International Mobile Subscriber Identity – міжнародний ідентифікатор мобільного абонента), використовуючи недоліки протоколів зв'язку [11, 12].

Отже, виникає протиріччя між використанням OTP паролів у протоколах двохфакторної аутентифікації й забезпеченням безпеки при передачі окремих її факторів.

Мета статті – розробка вдосконаленого методу строгої двохфакторної аутентифікації з OTP паролем на основі гібридних

крипто-кодових конструкцій на збиткових кодах, що дозволяє подальше використання 2 FA на основі sms.

Виклад основного матеріалу дослідження. Для досягнення мети розглянемо такі задачі:

опис математичних моделей гібридних крипто-кодових конструкцій на збиткових кодах на основі модифікованих несиметричних крипто-кодових систем (МНККС) Мак-Еліса й Нідеррайтера на еліптичних кодах;

розробка практичного алгоритму шифрування й розшифрування даних у гібридних крипто-кодових конструкціях на збиткових кодах (ГККККЗК) Нідеррайтера – Мак-Еліса.

Математична модель МНККС Мак-Еліса на основі укорочення (скорочення інформаційних символів) формально задається сукупністю таких елементів [22]:

множина відкритих текстів

$$M = \{ M_1, M_2, ..., M_{q^k} \},$$

де $M_i = \{ I_0, I_{h_1}, .. I_{h_j}, I_{k\text{-}1} \}$, $\forall I_j \in GF(q), h_j$– інформаційні символи, рівні нулю, $|h| = \frac{1}{2}k$, тобто $I_i = 0$, $\forall I_i \in h$;

множина закритих текстів (кодограм)

$$C = \{ C_1, C_2, ..., C_{q^k} \},$$

де $C_i = (A^*_{X_0}, A^*_{h_1}, ..., A^*_{h_j}, A^*_{X_{n-1}})$, $\forall A^*_{X_j} \in GF(q)$;

множина прямих відображень (на основі використання відкритого ключа – матриці, що породжує)

$$\varphi = \{ \varphi_1, \varphi_2, ..., \varphi_{q^k} \},$$

де $\varphi_i : M \to C_{k-h_j}$, $i = 1,2,...,s$;

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

$$\varphi^{-1} = \{ \varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_s^{-1} \},$$

де $\varphi_i^{-1} : C_{k-h_j} \to M$, $i = 1,2,...,s$;

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 завдання збитків (на основі використання ключа $-K_{MV2}^i$, і алгоритму *MV2*) – $E = \{E_{K_{MV2}}^1, E_{K_{MV2}}^2, ..., \varphi_{K_{MV2}}^S\}$, $i = 1,2,...,s$; $f(x)_i$ – прапор (збиток, *CHD*), $C(x)_i$ – остача (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 $MV2\,F_n^r$ задається біактивним відображенням між множиною перестановок $\{S_1, S_2, ..., S_{2^n}\}$ і множиною $\#F_n^r$, $\#F_n^r = \#\{(c, f)\} = 2^n!$;

множина осмисленого тексту (на основі використання ключа – K_{MV2}^i, і алгоритму *MV2*) –

$$E^{-1} = \{E_{K_{MV2}}^{1\ -1}, E_{K_{MV2}}^{2\ -1}, ..., E_{K_{MV2}}^{S\ -1}\},$$

де $E_{K_{MV2}}^{-1} : \|f(x)_i\| + \|C(x)_i\| \to M$, $i = 1,2,...,s$; $f(x)_i$ – прапор (збиток, CHD), $C(x)_i$ – остача (збитковий текст, CFT); $f(x)=n-|C(x)|$, якщо $|C(x)|>r$, де r – деякий параметр $r \in_R Z_{q^m}$;

множина ключів, параметризуючих прямі відображення (відкритий ключ уповноваженого користувача)

$$K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, ..., K_{s_{a_i}}\} = \{G_X^{EC_1}{}_{a_i}, G_X^{EC_2}{}_{a_i}, ..., G_X^{ECs}{}_{a_i}\},$$

де $G_X^{ECi}{}_{a_i}$ – $n \times k$ матриця, що породжує, замаскованого під випадковий код алгебро-геометричного (n, k, d) блокового коду з елементами $GF(q)$, тобто $\varphi_i : M \xrightarrow{K_{ia_i}} C_{k-h_j}$; $i = 1,2,...,s$; a_i – набір коефіцієнтів багаточлена кривої $a_1 ... a_6$, $\forall\ a_i \in GF(q)$ конкретний однозначно заданий набір крапок кривої з простору P2;

множина ключів, параметризуючих зворотні відображення (особистий (закритий) ключ уповноваженого користувача)

$$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X, P, D\}_1, \{X, P, D\}_2, ..., \{X, P, D\}_s\},$$

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

де X^i – маскує невироджені випадково рівноймовірно сформовані джерелом ключів $k \times k$ матрицю з елементами з $GF(q)$; P^i – перестановочна випадково рівно ймовірно сформована джерелом ключів $n \times n$ матриця з елементами з $GF(q)$; D^i – діагональна сформована джерелом ключів $n \times n$ матриця з елементами з $GF(q)$, тобто $\varphi_i^{-1} : C \xrightarrow{K_i^*} M, i = 1,2,...,s,$ складність виконання зворотного відображення φ_i^{-1} без знання ключа $K_i^* \in K^*$ сполучене з розв'язком теоретико-складної задачі декодування випадкового коду (коду загального положення);

множина ключів перетворення збиткових кодів

$$K_{MV2}^i \in K_{MV2}.$$

Вихідними даними при описі розглянутої несиметричної криптокодової системи захисту інформації є:

алгеброгеометричний блоковий (n, k, d) код C_{k-h_j} над $GF(q)$, тобто множина кодових слів $C_i \in C_{k-h_j}$, таких, що виконується рівність $C_i H^T = 0,$ де H – перевірочна матриця алгебро-геометричного блокового коду;

a_i – набір коефіцієнтів багаточлена кривій $a_1 \ldots a_6$, $\forall a_i \in GF(q)$ конкретний однозначно заданий набір крапок кривої із простору P2 для формування матриці, що породжує;

h_j – інформаційні символи, рівні нулю, $|h|=1/2k$, тобто $I_i=0$, "$I_i \in h$;

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

r – деякий параметр $r \in_R Z_{q^m}, Z_{q^m} = \{0,1,...2^n - 1\}$, n – деякий параметр

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

множина відображень $MV2\,F_n^r$.

У МНККС Мак-Еліса модифікований (укорочений) алгебро-геометричний *(n, k, d)* код C_{k-h_j} зі швидким алгоритмом розкодування маскується під випадковий *(n, k, d)* код $C_{k-h_j}{}^*$ за допомогою множення матриці, що породжує, GEC C_{k-h_j} коду на матриці, що X^u маскують, що P^u зберігаються D^u, в секреті, що й забезпечує формування відкритого ключа вповноваженого користувача:

$$G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u,\ u \in \{1,2,...,s\},$$

де G^{EC} – $n \times k$ матриця, що породжує, алгебро-геометричний (n, k, d) блоковий код з елементами $GF(q)$, з побудованою на основі використання обраних користувачем коефіцієнтів багаточлена кривої $a_1 \ldots a_6$, (a_i(GF(q), що однозначно задають конкретний набір крапок кривій із простору $P2$.

Формування закритого тексту $C_j \in C_{k-h_j}$ по введеному відкритому тексту $M_i \in M$ й заданому відкритому ключу $G_X^{ECu}{}_{a_i}$, $u \in \{1,2,...,s\}$ здійснюється шляхом формування кодового слова замаскованого коду з додаванням до нього випадково сформованого вектора $e = (e_0, e_1, ..., e_{n-1})$:

$$C_j = \varphi_u\left(M_i, G_X^u\right) = M_i \cdot \left(G_X^u\right)^T + e,$$

причому вага Хеммінга (число ненульових елементів) вектора e не перевищує здатності, що виправляє, використовуваного алгебраїчного блокового коду:

$$0 \le w(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

$\lfloor x \rfloor$ – ціла частина речовинного числа x.

Для кожного формованого закритого тексту $C_j \in C_{k-h_j}$ відповідний вектор $e = (e_0, e_1, ..., e_{n-1})$ виступає як одноразовий сеансовий ключ,

тобто для конкретного E_j вектор e формується випадково, рівноймовірно й незалежно від інших закритих текстів.

На алгоритм *MV2* надходить

$$C_j^* = C_j - C_{k-h_j},\ E_{K_{MV2}} : C_j^* \to \left\| f(x)_i \right\| + \left\| C(x)_i \right\|.$$

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

На прийомній стороні вповноважений користувач, що знає правила завдання збитків F_n^r, маскування, кількість і місця нульових інформаційних символів може скористатися швидким алгоритмом розкодування алгебро-геометричного коду (поліноміальної складності) для відновлення відкритого тексту:

$$E_{K_{MV2}}^{-1} : \left\| f(x)_i \right\| + \left\| C(x)_i \right\| \to C_j^*,\ M_i = \varphi_u^{-1}\left(C_j^*, \{X,P,D\}_u^{\lambda}\right).$$

Для відновлення відкритого тексту вповноважений користувач додає нульові інформаційні символи $C_j^* = C_j + C_{k-h_j}$, з відновленого закритого тексту C_j знімає дію секретних перестановочної й діагональної матриць P^u і D^u:

$$C = C_j^* \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \left(M_i \cdot \left(G_X^u\right)^T + e\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$

$$= \left(M_i \cdot \left(X^u \cdot G \cdot P^u \cdot D^u\right)^T + e\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$

$$= M_i \cdot \left(X^u\right)^T \cdot (G)^T \cdot \left(P^u\right)^T \cdot \left(D^u\right)^T \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$

$$= M_i \cdot \left(X^u\right)^T \cdot (G)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1},$$

розкодує отриманий вектор по алгоритму Берлекемпа-Мессі [11]:
$C = M_i \cdot \left(X^u\right)^T \cdot \left(G^{EC}\right)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$,

тобто позбувається від другого доданка й від співмножника $(G)^{ECT}$ в першому доданку в правій частині рівності, після чого знімається дія матриці маскування X^u. Для цього отриманий результат розкодування

$M_i \cdot \left(X^u\right)^T$ слід помножити на $\left(X^u\right)^{-1} : \left(M_i \cdot \left(X^u\right)^T\right) \cdot \left(X^u\right)^{-1} = M_i$. Отриманий розв'язок – суть відкритий текст M_i.

Алгоритм формування кодограми в ГККК Мак-Еліса на збиткових кодах задамо послідовністю певних кроків:

Крок 1. Зафіксуємо кінцеве поле *GF(q)*. Зафіксуємо еліптичну криву $y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xz+a_6z^3$ і набір її крапок $EC(GF(q)):(P_1, P_2, \ldots, P_N)$ над *GF(q)*. Зафіксуємо підмножину крапок $h(GF(q)): (P_{x1}, P_{x2}, \ldots, P_{xx})$, $h \subseteq EC(GF(q))$, $|h|=x$ і зберігаємо його в секреті.

Крок 2. Сформуємо вектор ініціалізації $IV=EC-h_j$, h_j – інформаційні символи рівні нулю, $|h|=\frac{1}{2}k$, тобто $I_i=0$, $\forall I_i \in h$.

Крок 3. По введеному інформаційному вектору *I* сформуємо кодове слово с. Якщо *(n, k, d)* код над *GF(q)* заданий своєю матрицею, що породжує, тоз=I(G.

Крок 4. Сформуємо випадковий вектор помилки *e* такий, що $w(e) \le t$, $t = \lfloor (d-1)/2 \rfloor$. Додамо сформований вектор до кодового слова, одержимо кодове слово: $з^*=з+е$.

Крок 5. Сформуємо кодограму, шляхом видалення (укорочення) символів вектора ініціалізації: $с_X{}^*=з^*-IV$.

Крок 6. Формуємо збитковий текст (остача) і прапор (збиток)

$$C_j^* = C_j - C_{k-h_j},\ E_{K_{MV2}} : C_j^* \to \left\| f(x)_i \right\| + \left\| C(x)_i \right\|.$$

Алгоритм розкодування кодограм у ГКККЗК Мак-Еліса задамо послідовністю визначених кроків.

Крок 1. Одержання осмисленого тексту кодограми на основі алгоритму *MV2*:

$$E_{K_{MV2}}^{-1} : \left\| f(x)_i \right\| + \left\| C(x)_i \right\| \to C_j{}^*.$$

Крок 2. Уведення кодограми, що підлягає розкодуванню. Уведення закритого ключа, що породжує й/або перевірочної матриці еліптичного коду.

Крок 3. Кодограма – суть кодове слово з помилками еліптичного коду. Вага вектора помилок $w(e) \le t$. Розкодовуємо кодограму – знаходимо вектор помилок.

Крок 4. Формуємо шуканий інформаційний вектор.

Алгоритм формування криптограми в МККС Нідеррайтера представимо у вигляді послідовності таких кроків:

Крок 1. Уведення інформації, що підлягає кодуванню. Уведення відкритого ключа H_X^{EC}.

Крок 2. Формування вектора помилок *e*, вага якого не перевищує *t*, що виправляє здатність еліптичного коду на основі алгоритму недвійкового рівноважного кодування [13, 14].

Крок 3. Формування вкороченого вектора помилки:

ex=e(A)–IV.

Крок 4. Формування кодограми

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

Крок 5. Формування збиткового тексту (остачі) і прапора (збитку)

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

Алгоритм розкодування кодограми в МККС Нідеррайтера представимо у вигляді послідовності кроків.

Крок 1. Одержання осмисленого тексту кодограми на основі алгоритму *MV2*:

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

Крок 2. Уведення кодограми SX, що підлягає декодуванню. Уведення закритого ключа – матриці X, P, D.

Крок 3. Знаходження одного з можливих розв'язків рівняння:

$S^*_{r-h_e} = \bar{c}^* \times \left(H_X^{EC} \right)^T$.

Крок 4. Зняття дії діагональної й перестановочної матриць:

$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$.

Крок 5. Розкодування вектора $\bar{c}^*$. Формування вектора *ex'*.

Крок 6. Перетворення вектора *ex'*:

ex=ex'×P×D.

Крок 7. Формування шуканого вектора помилки *e*:

e=ex+IV.

Крок 8. Перетворення вектора *e* на основі використання недвійкового рівноважного коду в інформаційну послідовність.

Розроблена схема багатофакторної аутентифікації на основі ГККЗК Нідеррайтера – Мак-Еліса дозволяє усунути істотний недолік 2FA на основі OTP повідомлень – забезпечення конфіденційності при передачі OTP пароля по каналах мобільного зв›язку. Проведені дослідження підтверджують, що застосування запропонованих процедур забезпечує швидкодія криптоперетворень порівнянних із БСШ, доказову криптостійкість на основі теоретико-складної задачі – декодування випадкового коду (забезпечується 1030–1035 групових операцій), і вірогідність на основі використання вкороченого алгебро-геометричного коду (забезпечується $P_{пом}10^{-9}$–10^{-12}).

Висновки. Запропонований у роботі вдосконалений метод строгої двохфакторної аутентифікації з OTP паролями на основі крипто-кодових конструкцій МНКК Мак-Еліса й Нідеррайтера, що дозволяє усунути основний недолік протоколу 2FA – передачу окремих токенів аутентифікатора по відкритих каналах мобільного зв'язку. Із цією метою запропоновані крипто-кодові системи на збиткових кодах, що дозволяють забезпечити необхідні показники безпеки на основі використання шифрування несиметричної крипто-кодової системи Нідеррайтера/Мак-Еліса, швидкість криптоперетворень на рівні блокових криптоалгоритмів і забезпечення передачі даних із прямим виправленням помилок. Даний підхід можна реалізувати у сучасних мобільних й десктопдодатках, використовуючи протоколи Інтернету й/або мобільних мереж.

Для зменшення потужності алфавіту – поля Галуа до *GF* (24–26) – у подальших дослідженнях пропонується використовувати системи на збиткових кодах, що дозволяють одночасно формувати багатоканальні криптосистеми.

Список використаної літератури

1. Шнайдер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Электронный ресурс]. – Режим доступа : https://www.labirint.ru/books/345501/

2. Digital Identity Guidelines [Електронний ресурс]. – Режим доступу : – https://doi.org/10.6028/NIST.SP.800-63b

3. The Cyber security Framework [Електронний ресурс]. – Режим доступу : http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf

4. Guide to LTE Security // [Електронний ресурс]. – Режим доступу : csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf

5. Шапиро Л. Аутентификация и одноразовые пароли. Теоретические основы. Часть 1 [Электронный ресурс]. – Режим доступа : https://elibrary.ru/item.asp?id=20464464

6. Шапиро Л. Аутентификация и одноразовые пароли. Часть 2. Внедрение OTP для аутентификации в AD [Электронный ресурс]. – Режим доступа : https://elibrary.ru/item.asp?id=20464277

7. SHA-3 Derived Functions: cSHAKE, KMAC, Tuple Hash and Parallel Hash [Електронний ресурс]. – Режим доступу : https://csrc.nist.gov/publications/.../800-185/sp800_185_draft.pdf

8. Евсеев С. П. Алгоритм мониторингу метода двухфакторной аутентификации на основе системы Passwindow / С. П. Евсеев, В. Г. Абдуллаев // Восточно-европейский журнал передовых технологий. – Харьков. – 2015. – Вып. 2/2(74). – С. 9–15.

9. Евсеев С. П. Усовершенствование метода двухфакторной аутентификации на основе использования модифицированных крипто-кодовых схем / С. П. Евсеев, В. Г. Абдуллаев, Ж. Ф. Агазаде, В. С. Аббасова // Системи обробки інформації. – 2016. – № 9(146). – С. 132-145.

10. Евсеев С. П. Разработка метода многофакторной аутентификации на основе модифицированных крипто-кодовых систем Нидеррайтера – Мак-Элиса / С. П. Евсеев, Г. П. Коц, Е. В. Лекарев // Восточно-европейский журнал передовых технологий. – Харьков. – 2016. 6/4(84). – С. 11–23.

11. David Meyer. Time is running out for this popular online security technique [Електронний ресурс]. – Режим доступу : – http://fortune.com/2016/07/26/nist-sms-two-factor/

12. Robert Hackett. You're implementing this basic security feature all wrong [Електронний ресурс]. – Режим доступу : http://fortune.com/2016/06/27/two-factor-authentication-sms-text/

Евсеев С., Андрощук А. **Метод многофакторной аутентификации на основе модифицированных крипто-кодовых систем Нидеррайтера – Мак-Элиса**

Внедрение ОТР-технологий (Technology of One-Time Passwords) позволит уменьшить риски, с которыми сталкиваются IT-специалисты ИОС при использовании долговременных запоминаемых паролей. Анализируются способы формирования ОТР-паролей, основные угрозы использования. Рассмотрены математические модели построения протокола многофакторной аутентификации на основе гибридных крипто-кодовых конструкций на ущербных кодах (ГККККУК), предлагаются практические алгоритмы их реализации.

Ключевые слова: многофакторная аутентификация, гибридные крипто-кодовые конструкции на ущербных кодах, одноразовые пароли.

Yevseiev S., Androshchuk O. **Manufacturing Authentication Method Based on Modified Crypto-Codes Systems Niderraiter – Make-Elis**

The proposed mathematical models and practical encryption / decryption algorithms for cryptogram / codograms in hybrid crypto-code designs based on modified coder-coded Niderraiter and Mac-Alice systems on loss codes differ from the known shortening of error vector characters (vector of initialization), and provide the necessary cryopresistance when transmitting data through open channels of mobile communication.

A multi-factor authentication scheme based on hybrid crypto-code designs on the loss-making Niderraiter-Mac-Alice codes allows eliminating a significant 2FA defect based on Sms-Messages - ensuring privacy when transmitting Otp-Password via mobile communication channels. The conducted researches in the work confirm that the application of the proposed procedures ensures the speed of cryptographic transformations comparable with known approaches, the proof of cryopreservation on the basis of a complex theoretical problem - the decoding of a random code (about a thousand group operations are provided) and the probability of using a shortened algebraic geometric code.

An improved method of strict two-factor authentication with Otr-Passwords is proposed on the basis of crypto-code designs of modified asymmetric Mc-Alice and Niderraiter crypto-code systems, which allows eliminating the main shortcoming of the 2FA protocol - the transmission of individual token tokens by open channels of mobile communication . To

this end, crypto-code systems are proposed at the loss-making codes that provide the necessary security measures based on encryption of the asymmetric Niderraiter / Mac-Alice crypto-coding system, the speed of crypto transformations at the level of block crypto algorithms, and the provision of data transmission with direct error correction. This approach can be implemented in modern mobile and desktop applications using Internet protocols and / or mobile networks.

In order to further reduce the power of the alphabet - the Galois fields - in further research, it is proposed to use systems on the loss codes that allow simultaneously to form multichannel cryptosystems.

Keywords: *multi-factor authentication, hybrid crypto-code designs on unprofitable codes, one-time passwords.*