**УДК 621.391**

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

**Володимир ФЕДОРЧЕНКО,**
*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*

# ПОБУДОВА СИСТЕМ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НА ОСНОВІ КОМПЛЕКСНОГО КРИПТОГРАФІЧНОГО ПІДХОДУ

*Розглядаються принципи побудови крипто-кодових конструкцій на основі алгеброгеометричних (еліптичних) кодів, багатоканальних криптосистем на основі ущербних кодів. Пропонуються гібридні крипто-кодові конструкції на ущербних кодах, алгоритми формування та розшифрування криптограми в гібридних криптосистемах на основі крипто-кодових конструкцій з ущербними кодами. Обґрунтовується ефективність та стійкість запропонованих гібридних конструкцій на основі оцінки енергозатрат і запропонованої методики оцінки стійкості.*

**Ключові слова:** *гібридні криптосистеми, несиметрична криптокодова конструкція, алгеброгеометричні коди, ущербні коди.*

**Постановка проблеми у загальному вигляді.** Швидкий розвиток глобальної комп›ютерної мережі Інтернет, побудованої на відкритих протоколах і моделях взаємодії відкритих систем, стрімкий розвиток інформаційних, комунікаційних, комп'ютерних систем привели до формування нових моделей функціонування державних організацій (у тому числі Державної прикордонної служби України), переходу до систем управління з критичною кібернетичною інфраструктурою (СККІ) [1–8]. Подальша інформатизація державних корпоративних систем (ДКС), розвиток віддаленого доступу до інформаційних активів на основі інтенсивного розвитку інформаційно-обчислювальних мереж державних установ формує на їх основі інформаційно-телекомунікаційні системи (ІТС). Однак негативною стороною є зростання останнім часом кіберзлочинів, використання соціальних мереж в ІТС, модернізація старих і поява нових кібератак, що призводить до загострення проблем захисту інформації та безпеки інформаційних елементів СККІ [9; 10]. У зв'язку з цим, одним з найактуальніших завдань, що стоять перед розробниками і користувачами ІТС, є повномасштабне рішення проблеми інформаційної безпеки (ІБ) – від створення стратегії, політики і стандартів ІБ в ІТС до розробки конкретних технологій, процедур щодо забезпечення ІБ [1]. З цією метою авторами пропонується підхід до формування комплексних криптосистем, що дозволяють будувати багатоканальні системи безпеки на основі крипто-кодових конструкцій з неповноцінними кодами (ККККУК), що забезпечують необхідні показники безпеки, надійності й оперативності.

**Аналіз останніх досліджень і публікацій, в яких започатковано вирішення даної проблеми та на які опираються автори.** У роботі [7] розглядаються питання надання доступу до інформаційних активів ІТС через віддалене підключення, що є одним з найбільш перспективних напрямків розвитку інформаційних систем. Крім переваг, що випливають з мобілізації користувачів ІТС, очевидні також і проблемні

зони – перш за все це безпека даних, які доступні при віддаленому доступі. У роботі [1] систематизовані поняття політики, стандартів, технологій і процедур інформаційної безпеки ІТС, а також запропоновані методи забезпечення ІБ на основі побудови віртуальних приватних мереж (virtual private network) –VPN-мереж. У [4] розглянута концепція інтегрованого захисту мережних ресурсів ІТС на основі трирівневої процесно-сервісної моделі системи управління ІБ. У роботі [9] авторами пропонується синергетичний підхід до моделі оцінки безпеки ІТС, пропонується методологія побудови модифікованої системи електронного документообігу на основі електронного цифрового підпису стандарту X.509. Проведений аналіз засобів захисту в [4] показав, що в сучасних інформаційно-обчислювальних мережах (ІТТ) як і раніше домінують традиції застосування стандартних апаратно-програмних засобів захисту інформації, які практично вичерпали свій потенціал щодо нейтралізації можливих інформаційних загроз.

У цих умовах одним з перспективних напрямків забезпечення безпеки інформаційних потоків (БІП), циркулюючих в ІТС, можна вважати створення системи інтегрованого захисту мережних ресурсів на основі несиметричних крипто-кодових систем (НККС). Їх застосування дозволяє одним механізмом інтегровано забезпечити необхідні рівні показників достовірності, безпеки та оперативності при обробці і передачі конфіденційної інформації по відкритих каналах глобальної мережі Інтернет (ГМІ).

**Мета статті –** розробка ієрархічної структури систем управління з критичною кібернетичною інфраструктурою, розробка гібридних криптосистем на основі модифікованих несиметричних крипто-кодових конструкцій Мак-Еліса на збиткових кодах, розробка методики оцінки стійкості запропонованих гібридних криптосистем на основі ентропійного методу.

**Виклад основного матеріалу дослідження.** Основні принципи побудови криптосистем на збиткових кодах. У роботах [12; 13] розглянуто теоретичні та практичні основи побудови ущербних кодів. Під ущербним текстом розуміється текст, отриманий подальшою деформацією ненадлишкових кодів букв.

Отже, необхідною і достатньою умовою ущербності тексту з втратою сенсу є скорочення довжин кодів символів тексту за межами їх надмірності. Як наслідок, ущербний текст має довжину меншу довжини вихідного тексту і не має сенсу вихідного тексту [12].

Теоретичною основою побудови ущербних текстів є видалення впорядкованості символів вихідного тексту і, як наслідок, зниження надмірності символів мови в ущербному тексті.

При цьому кількість інформації, що виражає цю впорядкованість, дорівнюватиме зменшенню ентропії тексту в порівнянні з максимально можливою величиною ентропії, тобто рівноймовірність появи будь-якої літери після будь-якої попередньої літери. Методи обчислення інформації, запропоновані в роботі [14], дозволяють виявити співвідношення кількості передбачуваною (тобто, що формується за певними правилами) інформації і кількості тієї несподіваної інформації, яку не можна заздалегідь передбачити.

Надмірність тексту розрахуємо за формулою

$$B(M) = B_A L_0 = \left( logN - \frac{H(M)}{L_0} \right) \times L_0,$$

де $M$ – вихідний текст; $B$ – надлишковість мови ( $B = R - r$, $R$ – абсолютна ентропія мови ( $R = logN$, $N$ – потужність абетки, $r$ – ентропія мови на один символ, $r = H(M) / L$, $L$ – довжина повідомлення $M$ у символах мови); $H(M)$ – ентропія (невизначеність) повідомлення; $L_0$ – довжина повідомлення $M$ у символах мови зі змістом; $B_A$ – надмірність мови.

Для отримання ущербного тексту (FTC) і ущербу (DCH) використовується метод "ідеального" стиснення після виконання $m$ циклів механізму заподіяння шкоди $C_m$ [12; 13].

Кількість циклів, необхідних для зменшення довжини початкового тексту $m$, знаходиться в межах відношення:

$$m > \frac{logn - B_A}{log\eta},$$

де $n$ – потужність уявлення символу вихідного тексту; $B_A$ – надмірність мови; $\eta$ – кількість разів зменшення довжини початкового тексту в MV2 на кожному кроці (деякий постійний коефіцієнт).

Кількісною мірою ефективності нанесення шкоди є ступінь руйнування сенсу, що дорівнює різниці ентропій ущербного тексту і вихідного тексту на різних відрізках довжини ущербного тексту:

$$d = H(FTC) - \sum_{i=1}^{s} H(M_i)p_i$$

$$\sum_{i=1}^{s} p_i = 1 \quad s = \left[ \frac{L_0 - L_{FTC}}{L_{FTC}} \right],$$

де $M_i$ – частина вихідного тексту, що відповідає *i*-му відрізку; $p_i$ – її ймовірність, $L_0$ – довжина $M_i$ дорівнює довжині $L_{FTC}$ – ущербного тексту; *s* – кількість відрізків.

Для ергодичного джерела символів вихідного тексту:

$$d_{max} = \log L_{FTC} - H(M_i).$$

Під інформаційним ядром деякого тексту розуміється ущербний текст CFT, отриманий циклічним перетворенням універсального механізму заподіяння шкоди $C_m$.

Універсальний механізм нанесення ущербу $C_m$ може бути описаний [12; 13]:

$$CFT / CH_{FT} = E_1\left(M, KU^{EC}\right),$$

$$CHD / CH_D = E_2\left(M, KU^{EC}\right),$$

$$M = E_{1,2}^{-1}(!\ F'' / CH_{FT}, CHD / CH_D, KU^{EC}),$$

де

$$CF'' / CH_{FT} = CF'' / CH_{FT}^i, ..., !\ F'' / CH_{FT}^m,$$

$$KU^{EC} = j(K_D^i, ..., K_D^m, KU_I^{EC}, ..., KU_m^{EC},$$

$$CHD / CH_D = CHD / CH_D^i, ..., CHD / CH_D^m.$$

Таким чином, у результаті маємо два шифртексти (ущерб ($CH_D$) и ущербний текст (*FTC*), кожен з яких не має сенсу ні в алфавіті початкового тексту, ні в алфавіті шифртексту. Фактично шифртекст вихідного повідомлення (М) представляється у вигляді сукупності двох ущербних шифртекстів, кожен з яких окремо не може відновити вихідний текст.

Для відновлення початкової послідовності немає необхідності знати проміжні ущербні послідовності. Необхідно знати тільки

останню ущербну послідовність (останній ущербний текст після виконання всіх циклів) і всі ущерби з правилами їх нанесення.

Криптографічними ущербними текстами називаються тексти, отримані такими способами [12]:

нанесенням шкоди початковому тексту з подальшим шифруванням ущербного тексту і/або його збитків;

нанесення шкоди шифртексту;

нанесення шкоди шифртексту ущербного тексту і/або шифртексту ущербів.

Основною перевагою в пропонованих способах і протоколах забезпечення послуг безпеки на основі використання ущербних кодів є використання не БСШ, а модифікованих несиметричних кріптокодових систем (МНККС) Мак-Еліса і Нідеррайтера для забезпечення криптостійкості ущербу і/або ущербного тексту.

Відстань єдності для моделі випадкового шифру, для якого існує ймовірність отримати змістовний текст при випадковому і рівноймовірному виборі ключа $K$ і спробі дешифрування шифртекста, при

$$N_S = H(K)\frac{2^{HL}}{|I|^L} = 1:$$

$$L = U_0 = \frac{H(K)}{log|I| - H} = \frac{H(K)}{Blog|I|}, \qquad (1)$$

де $B$ – надлишковість вихідного тексту; $H$ – ентропія на літеру змістовного тексту у вхідному алфавіті $I$, $|I|>2$, $2^{HL}$ – наближене значення числа змістовних текстів.

У роботах [12; 13] під циклічним алгоритмом отримання ущербних текстів розуміють універсальний механізм нанесення ущербу ($C_m$, де $m$ – число циклів), який полягає у випадковій заміні бітового представлення кожного символу вихідного тексту кортежем меншого або рівного числа біт з подальшою їх конкатенацією.

Область визначення перетворення в алгоритмі $MV2$ – множина $\{0, 1\}^n$ – розглядаємо як потужність алфавіту деякого сімейства ви-

хідних текстів, з яким пов'язано деякий розподіл імовірностей літер цього алфавіту, а символи вихідного тексту – значення дискретного випадкового елемента [11].

Нехай X – випадковий дискретний елемент, який бере значення $x_i \in \{0,1\}^n$ з ймовірностями $p_i$ і $T = (c, f) \in F_n^r$ – довільне фіксоване перетворення MV2. Тоді для будь-якого $y \in U_{r\,n-1}$ (деякий двійковий рядок з безлічі рядків змінної довжини) і для будь-якого $1'' \; i'' \; |y|$ виконується:

$$\#\left\{x \in \{0,1\}^n : c(x) = y\right\} = \#\left\{x \in \{0,1\}^n : c(x) = y^{(i)}\right\}.$$

Тоді незалежно від розподілу ймовірностей випадкового елемента X для ентропій випадкових елементів $FTC/FT_{CH}$ (ущербного шифртексту) і *CHD* (ущербу) виконуються рівності:

$$H(FTC / FT_{CH}) \pounds \log(2^n - 2^r),$$

$$H(CHD) \pounds \log(n - r + 1).$$

Таким чином, при рівномірному розподілі входів (прапорів) алгоритму MV2 формується рівномірний розподіл виходу (залишку):

$$P(c_k = 0 \,|\, 0 \pounds k \pounds |FTC / FT_{CH}|) = \frac{1}{2}.$$

Проведений аналіз способів нанесення шкоди показав, що для використання в ІТС найбільш придатним є перший спосіб – нанесення збитку з подальшим криптоперетворенням, що дозволяє знизити потужність алфавіту при формуванні криптограми в МККС Мак-Еліса. Відстань єдності для даного способу (вираз 1) буде трансформовано:

$$U_0 = \frac{\sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right) + H(KU_i^{EC})}{B \log |I|}. \qquad (2)$$

Така система базується на непоправному спотворенні шкоди і забезпеченні стійкості за рахунок використання в подальшому шифрування на основі МККС. Це призводить до неможливості дізнатися шифртекст ущербного тексту.

Таким чином, застосування основних принципів побудови МККС Мак-Еліса і систем багатоканальної криптографії на ущербних кодах дозволяє розробити гібридні криптосистеми на основі модифікованих несиметричних крипто-кодових систем Мак-Еліса і систем багатоканальної криптографії на ущербних кодах. Відмінною особливістю від "класичного" підходу формування гібридної криптосистеми є використання несиметричних крипто-кодових конструкцій (належать до секретних моделей доказової стійкості) з швидкими криптоперетвореннями (швидкість перетворень порівнянна з криптоперетвореннями в БСШ) як основний механізм забезпечення стійкості (безпеки) інформації з подальшим використанням алгоритму MV2 (системи на ущербних кодах) для зниження енергетичних витрат (потужності алфавіту МНККС Мак-Еліса) подальшою передачею по одному або декількох каналах.

**Висновки.** Використання алгоритму MV2 систем на ущербних кодах збільшує криптостійкість запропонованої гібридної системи і дозволяє "знизити" потужність алфавіту (розмірність поля GF (26-28) для побудови МККС Мак-Еліса) без зниження рівня криптостійкості системи в цілому.

Даний підхід дозволяє будувати гібридні криптосистеми, основною відмінністю яких є новий підхід до їх формування – для шифрування використовуються несиметричні криптосистеми на основі МНККС, а для посилення стійкості – багатоканальні системи на ущербних кодах. Для оцінки їх стійкості можна використовувати методику на основі ентропійного методу оцінки, що дозволяє оцінити сумарну стійкість гібридної криптосистеми.

Передача конфіденційних даних і ключових послідовностей стандартних алгоритмів шифрування в ІТС на основі запропонованої гібридної криптосистеми дозволяє використовувати відкриті канали різних систем. Для користувачів ІТС забезпечуються необхідні показники безпеки, достовірності й оперативності всього циклу обробки інформації.

Побудова програмної складової є предметом для проведення **подальших досліджень.**

**Список використаної літератури**

1. Усков А. В. Технологии обеспечения информационной безопасности корпоративных образовательных сетей / А. В. Усков, А. Д. Иванников, В. Л. Усков // Educational Technology & Society, 2008. № 11(1). – С. 472–479.

2. Груздева Л. М. Повышение производительности корпоративной сети в условиях воздействия угроз информационной безопасности / Л. М. Груздева, М. Ю. Монахов // Известия высших учебных заведений. Приборостроение. – Санкт-Петербург. – 2012. – Т. 55. – № 8. – С. 53–56.

3. Аникин И. В. Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях / И. В. Аникин, Л. Ю. Емалетдинова, А. П. Кирпичников // Вестник технологического университета. – 2015. – Т. 18. – № 6. – С. 195–197.

4. Надеждин Е. Н. Проблемные вопросы управления рисками информационной безопасности в сфере образования // Научный поиск. Специальный выпуск : материалы V научной конференции "Шуйская сессия студентов, аспирантов, молодых учёных". – 2012. – №2.6. – С. 50–56.

5. Кондратова Е. Г. Социальные сети как канал утечки корпоративной информации / Е. Т. Кондратова // Безопасность информационных технологий. "Проблемы информационной безопасности в системе высшей школы" [Электронный ресурс]. – Режим доступа : https://elibrary.ru/item.asp?id=21003147&

6. Литвинов В. А. Информационная безопасность высшего учебного заведения в рамках современной глобализации / В. А. Литвинов // [Электронный ресурс]. –Режим доступа : conference.osu.ru/assets/files/conf_reports/conf13/132.doc

7. Вахонин С. Удаленный доступ и утечка данных / С. Вахонин // [Электронный ресурс]. – Режим доступа : http://www.itsec.ru/articles2/Inf_security/udalennyy-dostup-i-utechka-dannyh/

8. Замараева О. А. Разработка политики информационной безопасности для экономического вуза: определение информации, подлежащей защите, и построение модели злоумышленника / О. А. Замараева [Электронный ресурс]. – Режим доступа : https://www.science-education.ru/ru/article/view?id=13106

9. Евсеев С. П. Моделирование процессов управления в информационной экономике. Раздел: Методология построения модифицированной системы электронного документооборота в университете на основе элек-

тронной цифровой подписи стандарта X.509 / С. П. Евсеев. – Бердянск : Издатель Ткачук А.В., 2017. – 420 с.

10. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Грищук. – Житомир : Рута, 2010. – 280 с.

11. Блейхут Р. Теория и практика кодов, контролирующих ошибки [Текст] Р. Блейхут; пер. с англ. – М. : Мир, 1986. – 576 с.

12. Мищенко В. А. Ущербные тексты и многоканальная криптография / В. А. Мищенко. – Минск : Энциклопедикс. 2007. – 292 с.

13. Мищенко В. А., Виланский Ю. В., Лепин В. В. Криптографический алгоритм MV 2 / В. А. Мищенко, Ю. В. Виланский, В. В. Лепин. – Минск , 2006. 177 с.

14. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон. – М. ИЛ., 1963. – С. 333–369.

*Евсеев С., Федорченко В., Андрощук А.* **Построение систем безопасности информационно-телекоммуникационных систем на основе комплексного криптографического подхода**

Рассматриваются принципы построения крипто-кодовых конструкций на основе алгеброгеометрических (эллиптических) кодов, многоканальных криптосистем на основе ущербных кодов. Предлагаются гибридные крипто-кодовые конструкции на ущербных кодах, алгоритмы формирования и расшифрования криптограммы в гибридных криптосистемах на основе крипто-кодовых систем Мак-Элиса с ущербными кодами. Обосновывается эффективность и стойкость предложенных гибридных конструкций на основе оценки энергозатрат и предложенной методики оценки стойкости.

**Ключевые слова:** *гибридные криптосистемы, несимметричная крипто-кодовая конструкция, алгеброгеометрические коды, ущербные коды.*

*Yevseiev S., Fedorchenko V., Androshchuk O.* **Analysis Approaches for Forecasting Activities Department Border Guard checkpoint**

The application of the basic principles of constructing the MacAlice ICAC and the systems of multichannel cryptography on degraded codes allows us to develop hybrid cryptosystems based on the modified Mac-Alice modified asymmetric crypto-code systems and multichannel cryptography

systems on degenerate codes. A distinctive feature of the "classic" approach to the formation of a hybrid cryptosystem is the use of asymmetric crypto-code structures (refer to secret models of evidentiary stability) with fast cryptographic transformations (the rate of transformation is comparable to crypto transformations in BSS) as the main mechanism for ensuring the stability (security) of information with subsequent use algorithm MV2 (systems with defective codes) to reduce energy costs (capacity of the alphabet MNKKK Mak-Alisa) for further transmission by one or dec some channels

Conclusions Thus, the use of the MV2 algorithm on degraded codes increases the cryptostability of the proposed hybrid system, and allows to "lower" the power of the alphabet (the dimension of the GF field ($2^6$-$2^8$) for the construction of the MacAlice MKKS) without reducing the cryptostability of the system as a whole.

This approach allows to build hybrid cryptosystems, the main difference of which is a new approach to their formation - for encryption used asymmetric cryptosystems on the basis of MNKSK, and to strengthen the stability – multichannel systems on degraded codes. To assess their stability, one can use a method based on the entropy estimation method, which allows us to estimate the overall stability of the hybrid cryptosystem.

The transmission of confidential data and key sequences of standard encryption algorithms in the ITS based on the proposed hybrid cryptosystem allows the use of open channels of different systems. IT users are provided with the necessary security, reliability and efficiency indicators throughout the information processing.

**Keywords:** *hybrid cryptosystems, asymmetric crypto-code design, algebra-geometric codes, degraded codes.*