УДК 004.056:004.738.5:004.932 **doi:** https://doi.org/10.20998/3083-6298.2025.01.05

Станіслав Мілевський[1]

[1] Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна

РОЗРОБКА МЕТОДОЛОГІЇ ПОБУДОВИ СИСТЕМ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ІНТЕРНЕТ-СЕРВІСАХ

Анотація. Актуальність теми. У статті розглядається проблема побудови систем безпеки інформаційних ресурсів в інтернет-сервісах з урахуванням викликів, які породжують соціокіберфізичні системи (SCPS). **Мета.** Запропоновано методологію створення багатоконтурної системи захисту інформації, орієнтованої на мультимедійні ресурси, що використовуються в соціальних інтернет-сервісах. **Результати.** Методологія базується на синтезі сучасних математичних методів, зокрема теорії множин, теорії скінченних полів, криптографії та системного аналізу. Особливу увагу приділено загрозам, що поєднують методи соціальної інженерії з атаками на компоненти SCPS, що є характерним для сучасних умов гібридного протистояння. **Висновок.** Результати дослідження спрямовані на підвищення ефективності захисту мультимедійних ресурсів і протидію цільовим кіберзагрозам.

Ключові слова: соціокіберфізичні системи; соціальні інтернет-сервіси; інформаційна безпека; гібридні криптокодові конструкції; багатоконтурний захист; LDPC-коди; методи соціальної інженерії

1. Вступ

Актуальність. Розвиток світового суспільства тісно пов’язаний з обчислювальними можливостями та еволюційними тенденціями напрямку IT індустрії в умовах глобалізації та суттєвого прискорення формування соціокіберфізичних систем на основі комплексування соціальних інтернет-сервісів (CIC) з кіберфізичними системами (cyber-physical systems, CPS). Соціальні інтернет-сервіси є онлайн-платформи, які надають користувачам можливість створювати, обмінюватися та взаємодіяти з контентом і один з одним, вони сервіси охоплюють широкий спектр застосувань, включаючи соціальні мережі, блоги, форуми, платформи для обміну фото та відео, месенджери та інші. Об’єднання кіберфізичних систем із соціальними аспектами, в тому числі та з CIC, створюють комплексні платформи, які здатні аналізувати, контролювати та управляти різними процесами з урахуванням соціальних факторів, а саме – соціокіберфізичні системи (sociocyberphysical systems, SCPS). За останні десятиліття сформувалися умови «перетворення» CIC на канал (кіберзброю) розповсюдження інформації та комунікації членів (агентів) суспільства. Однак в умовах створення соціокіберфізичних систем формуються нові цільові (змішані) атаки на основі їх комплексування з методами соціальної інженерії, які використовують CIC, що забезпечує підвищення рівня реалізації атак та зламу системи безпеки соціокіберфізичних систем в цілому [1-12]. Досвід збройної агресії російської федерації проти України продемонстрував, що CIC є одним з ефективних інструментів ведення нової форми протистояння – гібридної війни.

Мета роботи полягає у розробці методології побудови систем безпеки мультимедійних ресурсів в інтернет-сервісах як багатоконтурної системи захисту інформації, спрямованої на підвищенні рівня захищеності інформаційних ресурсів.

2. Методи дослідження

Дослідження базується на теоретично обґрунтованих і практично перевірених методах теорії множин (формалізація загроз безпеки інформаційних ресурсів, їх класифікація, визначення вимог і повноти забезпечення безпеки інформаційних ресурсів), теорії скінченних полів Галуа та теорії кодування (використання при розробці гібридних крипто-кодових конструкцій на кодах з нанесенням збитку, LDPC-кодах і обґрунтування їх стійкості), теорії криптографії, теорії ймовірностей та математичної статистики (застосування для дослідження властивостей гібридних крипто-кодових конструкцій на кодах з нанесенням збитку, LDPC-кодах), експертного оцінювання (для визначення вагових коефіцієнтів загроз для формування універсального класифікатора загроз), математичної логіки (для оцінювання енергоємності практичної реалізації гібридних крипто-кодових конструкцій на збиткових, LDPC-кодах, побудові серверної частини програмно-апаратного комплексу), системного аналізу (для ієрархічного подання соціокіберфізичних систем), законах синергетичної взаємодії (для побудови моделі потенційних загроз, дослідження впливу моделі на систему безпеки інформаційних ресурсів).

3. Основна частина

В умовах еволюційного зростання гібридних (комплексованих) систем, які поєднують різні технології актуальним питанням є побудова багатоконтурних систем захисту у відповідності до визначених платформ, а також необхідність розгляду впливу загроз як на зовнішній, так й на внутрішній контури безпеки.

Розроблений удосконалений класифікатор загроз соціокіберфізичних систем з урахуванням гібридності та синергізму цільових (змішаних) атак, комплексування з методами соціальної інженерії та побудови багатоконтурних систем захисту

інформації [13]. Запропонована концепція побудови багатоконтурних систем безпеки в соціальних інтернет-сервісах враховує ознаки синергізму та гібридністю змішаних та цільових атак на кожну з платформ соціокіберфізичних систем (на внутрішній та зовнішній контури):

Загальна оцінка загроз на внутрішній контур за всіма платформами складає:

$$Q_{ISL}^{SCPS} = \bigcup^{1\div 3}\left(Q_{\text{hybrid } C,I,A,Au,Af\ synerg_{1-3\,\text{platform}}}^{SCPS\ ISL}\right) \quad (1)$$

Загальна оцінка загроз для зовнішнього контуру системи за трьома платформами складає:

$$Q_{ESL}^{SCPS} = \bigcup^{1\div 3}\left(Q_{\text{hybrid } C,I,A,Au,Af\ synerg_{1-3\,\text{platform}}}^{SCPS\ ESL}\right) \quad (2)$$

Загальна оцінка загроз на багатоконтурну систему захисту інформації визначається:

$$Q_{\text{final}}^{SCPS} = Q_{ISL}^{SCPS} \bigcup Q_{ESL}^{SCPS}. \quad (3)$$

Загальний (поточний) рівень захищеності соціокіберфізичних систем на основі бездротових мобільних технологій описується:

–для адитивного згортки:

$$L_{Q_{\text{security}}^{SCPS}} = L_{ISL}\sum_{j=1}^{3}\sum_{i=1}^{12}\left(I_{A_{ij}} \times \beta_{ij}\right) + L_{ESL}\sum_{j=1}^{3}\sum_{i=1}^{12}\left(I_{A_{ij}} \times \beta_{ij}\right). \quad (4)$$

–для мультиплікативної згортки:

$$L_{Q_{\text{security}}^{SCPS}} = 1-\left[1-L_{ISL}\sum_{j=1}^{3}\sum_{i=1}^{12}\left(I_{A_{ij}} \times \beta_{ij}\right)\right]\times\left[1-L_{ESL}\sum_{j=1}^{3}\sum_{i=1}^{12}\left(I_{A_{ij}} \times \beta_{ij}\right)\right]. \quad (5)$$

Таким чином, такий підхід забезпечує об'єктивну оцінку кіберзагроз на соціокіберфізичні системи з урахуванням їхньої гібридності та синергізму, а також можливих інтеграцій та глобалізації технологій та форм власності.

На рис. 1 представлено модель безпеки інформаційних взаємодій у соціокіберфізичних системах.

Такий підхід забезпечує необхідний рівень об'єктивності аналізу можливих кіберфізичних (цільових чи змішаних) загроз з урахуванням можливого комплексування із загрозами на основі методів соціальної інженерії. Крім цього, своєчасно визначити критичні точки в інфраструктурі кожної з платформ та сформувати превентивні заходи захисту.

Для побудови динамічних моделей взаємодії агентів в соціокіберфізичних системах на основі соціальних інтернет-сервісів запропонована модель Лотки-Вольтерри [14]. Для визначення взаємозв'язків між «жертвою» та «хижаком» використовується класифікатор загроз, що забезпечує врахування характеристик та ознак загроз, мінімізацію коштів на підтримку систем захисту інформації з урахуванням безперервності бізнес-процесів.

Розроблена модель безпеки кіберфізичних систем враховує можливу конкуренцію зловмисників по відношенню до «жертви», що дозволяє своєчасно визначити не лише спрямованість загроз, а й обчислювальні ресурси нападаючих, а їх «одночасний» вплив може забезпечити «зниження» ризику реалізації кіберзагроз.

Для забезпечення послуг безпеки у соціокіберфізичних системах пропонується використовувати постквантові алгоритми – крипто-кодові конструкції на основі LDPC-кодів із заподіянням збитку. Однак представлені практичні протоколи розшифрування LDPC-кодів ґрунтуються на м'якому декодуванні, що суттєво впливає на швидкість розкодування та достовірність. Для побудови використається перевірна матриця LDPC-коду. Для використання в крипто-кодових конструкціях McEliece необхідна матриця, яка може бути отримана на основі властивості ортогональності перевірочної і породжувальної матриць. Крипто-кодові конструкції (ССС) реалізовані на модифікованих LDPC-кодах та збиткових кодах. Основні властивості ССС McEliece на LDPC-кодах наведено в табл. 1.

Математична модель гібридної крипто-кодової конструкції McEliece використовує такі вихідні дані:

- множина інформаційних ресурсів $I = \left\{I_1, I_{2,}, ...I_{q^k}\right\}$,

для всіх Ij ∈ GF(q);

- множина криптоперетворень для формування кодового слова на матриці LDPC-коду, що породжує: C=(C1, C2, …, Cs),

де $\phi_i : I \to C_{k-h_j}$, i = 1, 2, ..., s; hj – формує вектори ініціалізації (IV1 – вектор ініціалізації, який визначає кількість та місця «виколювання» символів у кодовому слові, IV2 – вектор ініціалізації, який визначає кількість та місця «до давлення» інформаційних символів у кодовому слові);

– множина криптоперетворень, які дозволяють отримати вихідний інформаційний ресурс:

$$\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, ..., \phi_s^{-1}\}, \quad (6)$$

де $\phi_i^{-1} : C_{k-h_j} \to I$;

– множина відкритих ключів:

$$KU_i = \left\{KU_1, KU_2, ..., KU_S\right\} = \\ = \left\{G_1^{LDPC}, G_2^{LDPC}, ..., G_S^{LDPC}\right\}, \quad (7)$$

де $G_{X_{a_i}}^{LDPC_i}$ – породжувальна матриця LDPC-коду.

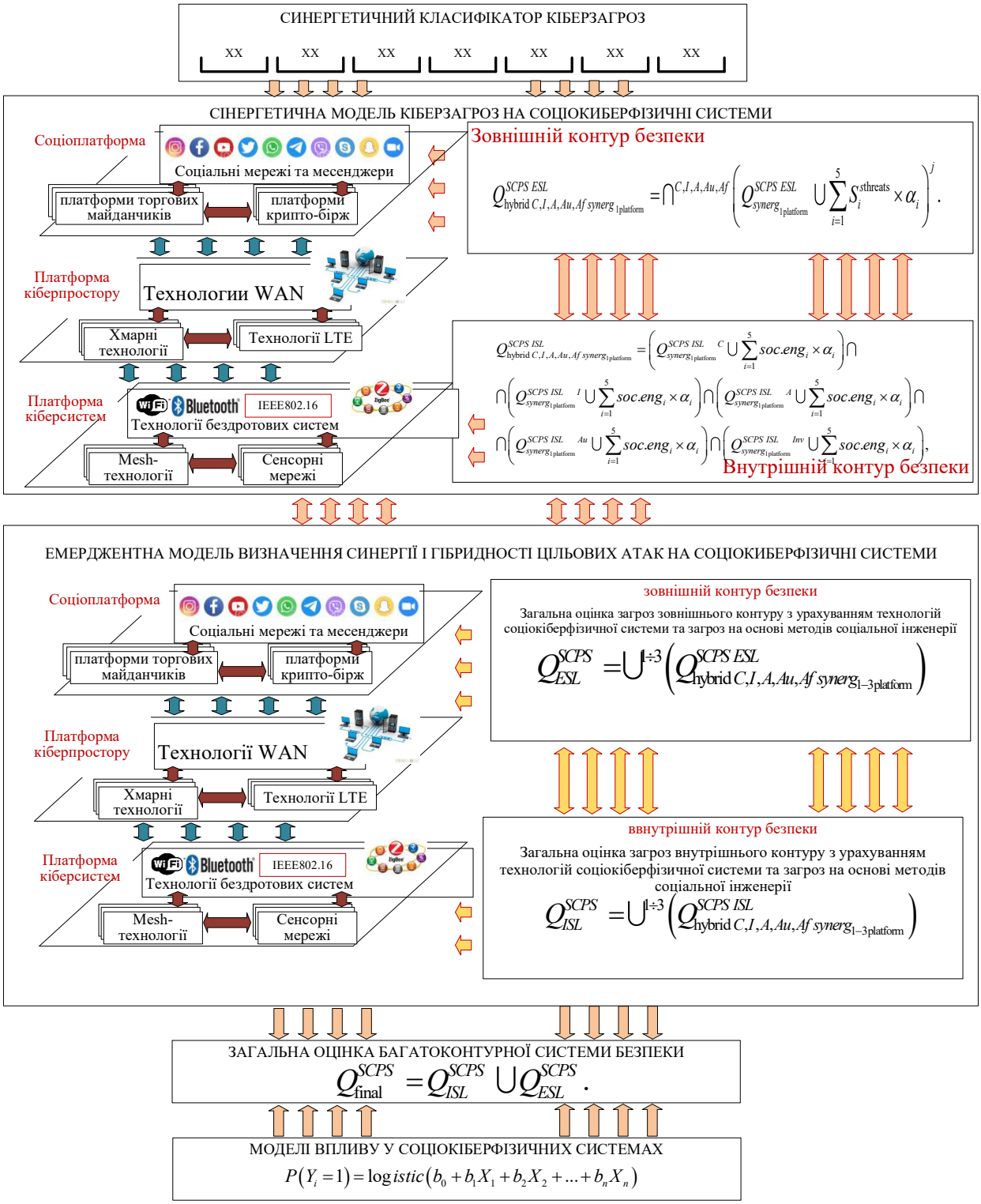

Рис. 1. Модель безпеки інформаційних взаємодій у соціокіберфізичних системах

Таблиця 1 – **Основні властивості CCC McEliece на LDPC-кодах**

Властивість	Скорочені LDPC-коди	Подовжені LDPC-коди
Довжина відкритого тексту	$l_I = l_z^c + l_z^f$	$l_I = 1/2k \times m + l_z^c + l_z^f$
Довжина кодограми (в бітах)	$l_S = \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m;$	$l_S = \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m.$
Довжина відкритого ключа (в бітах)	$l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m,$	$l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m.$

Властивість	Скорочені LDPC-коди	Подовжені LDPC-коди
Довжина закритого ключа (в бітах)	$l_{K_+} = 1/2k\left\lceil \log_2\left(2\sqrt{q}+q+1\right)\right\rceil + \left\lvert F_u^v \right\rvert,$	$l_{K_+} = (1/2k - 1/2k)\left\lceil \log_2\left(2\sqrt{q}+q+1\right)\right\rceil + \left\lvert F_u^v \right\rvert.$
Складність формування кодограми для систематичного кодування	$O_K = (r+1)\times\left(2\sqrt{q}+q+1-1/2k\right) + +O\left(\frac{1-K_C^u}{K_f}\times L\right);$	$O_K = (r+1)\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right) + +O\left(\frac{1-K_C^u}{K_f}\times L\right);$
Складність формування кодограми для несистематичного кодування	$O_K = O_K = (k+1)\times(k+1)\times \times\left(2\sqrt{q}+q+1-1/2k\right) + +O\left(\frac{1-K_C^u}{K_f}\times L\right);$	$O_K = (k+1)\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right) + +O\left(\frac{1-K_C^u}{K_f}\times L\right).$
Складність розкодування кодограми	$O_{SK} = 2\times\left(2\sqrt{q}+q+1-1/2k\right)^2 + 1/2k^2 + +4t^2 + \left(t^2+t-2\right)^2/4 + O\left(\frac{\alpha - z\times\log k}{\left\lvert K_z^c \times L\right\rvert}\right);$	$O_{SK} = 2\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)^2 + +k^2 + 4t^2 + \left(t^2+t-2\right)^2/4 + O\left(\frac{\alpha - z\times\log k}{\left\lvert K_z^c \times L\right\rvert}\right).$
Складність процесу декодування	$O_{K+} = N_{покр}\times\left(2\sqrt{q}+q+1-1/2k\right)\times r + +N_{F\ або}\left(N_K\right),$	$O_{K+} = N_{покр}\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)\times \times r + N_F$ або $\left(N_K\right).$

Для формування ключа використовуємо:

$$G_{X_{a_i}}^{LDPCu} = X^u \times G^{LDPCu} \times P^u, \quad u \in \{1,2,...,s\}; \tag{8}$$

– множина особистих (закритих) ключів користувачів:

$$KR = \{KR_1, KR_2, ..., KR_r\} = = \left\{X^i, P^i, D^i\right\}, \tag{9}$$

де матриці маскування: Xi – невироджена k×k-матриця; Pi – перестановна n×n-матриця; Di – діагональна n×n-матриця.

Діагональна матриця LDPC-коду дорівнює одиничній матриці і може не використовуватися;

– множина збиткових текстів (C(x)i) – $CFT = \{CFT_1, CFT_2, ..., CFT_{q^k}\}$;

– множина збитків (f(x)i - прапор), $CHD = \{CHD_1, CHD_2, ..., CHD_{q^k}\}$;

– множина формування збиткового тексту та шкоди (на основі ключа алгоритму MV2) – $E = \{E_{K_{MV2}}^1, E_{K_{MV2}}^2, ..., \phi_{K_{MV2}}^S\}$, f(x)=n –|C(x)|, якщо |C(x)|> r, де r – певний параметр, $r \in_R Z_{q^m}$, $0\langle r\langle n$;

– множина відображення MV2 $\rightarrow F_n^r$, що задає об'єктивне відображення між безліччю перестановок $\{S_1, S_2, ..., S_{2^n}\}$ і безліччю $\#F_n^r$, $\#F_n^r = \#\{(c,f)\} = 2^n!$;

– множина відображення неповноцінного тексту в інформаційний ресурс (на основі ключа – Ki MV2, і алгоритму MV2) – $E^{-1} = \{E_{K_{MV2}}^{1\ -1}, E_{K_{MV2}}^{2\ -1}, ..., E_{K_{MV2}}^{S\ -1}\}$, де $E_{K_{MV2}}^{-1}: \left\|f(x)_i\right\| + \left\|C(x)_i\right\| \rightarrow I.$

Відправник формує кодове слово: $C_j = M_i \times G_{X_{a_i}}^{LDPCu^T} + e,$ де є додатковий сеансовий ключ кожної інформаційної посилки.

До алгоритму MV2 надходить кодове слово $C_j = M_i \times G_{X_{a_i}}^{LDPCu^T} + e$ і перетворюється в алгоритмі MV2 у збитковий текст (залишок) та збиток (прапор):

$$E_{K_{MV2}}: \mathrm{C}^* \rightarrow \left\|f(x)_i\right\| + \left\|C(x)_i\right\|. \tag{10}$$

У канал зв'язку надходить ‖ f(x)i ‖ і ‖ C(x)i ‖ при цьому передача може проводитись як по одному, так і по двох незалежних каналах.

На стороні прийому одержувач використовує правило завдання шкоди F_n^r, маскування, кількість та місця нульових інформаційних символів може

розкодувати кодове слово та отримати інформаційне повідомлення:

$$E_{K_{MV2}}^{-1}:\left\|f(x)_i\right\|+\left\|C(x)_i\right\|\to C_j^{*},\quad I_i=\phi_u^{-1}\left(C_j^{*},\{X,P,D\}_u\right). \tag{11}$$

При використанні подовженого модифікованого LDPC-коду одержувач додає

$$C=C_j^{*}\times\left(P^u\right)^{-1}=\left(I_i\times\left(G_X^{LDPCu}\right)^T+e\right)\times\left(P^u\right)^{-1}=\left(I_i\times\left(X^u\times G^{LDPC}\times P^u\right)^T+e\right)\times$$
$$\times\left(P^u\right)^{-1}=I_i\times\left(X^u\right)^T\times\left(G^{LDPC}\right)^T\times\left(P^u\right)^T\times\left(P^u\right)^{-1}+e\times\left(P^u\right)^{-1}= \tag{12}$$
$$=I_i\times\left(X^u\right)^T\times\left(G^{LDPC}\right)^T+e\times\left(P^u\right)^{-1},$$

нульові інформаційні символи (по вектору ініціалізації V1), а також і «отримує» інформаційні символи (по вектору ініціалізації V2 $CHD=\{CHD_1,CHD_2,...,CHD_{q^k}\}$,

а потім розкодує отриманий вектор за алгоритмом Берлекемпа-Месі:

$$C=I_i\times\left(X^u\right)^T\times\left(G^{LDPC}\right)^T+e\times\left(D^u\right)^{-1}\times\left(P^u\right)^{-1}. \tag{13}$$

Отримуємо інформаційний ресурс:

$$\left(I_i\cdot\left(X^u\right)^T\right)\times\left(X^u\right)^{-1}=I_i. \tag{14}$$

Представлений математичний апарат дозволяє оцінити основні параметри крипто-кодових конструкцій на LDPC-кодах із заподіянням збитку та на модифікованих кодах На рис. 2 та 3 наведено порівняння кількості операцій, необхідних для шифрування та розшифрування повідомлення основі крипто-кодових конструкцій на модифікованих LDPC–кодах та крипто-кодових конструкцій на основі модифікованих еліптичних кодах.

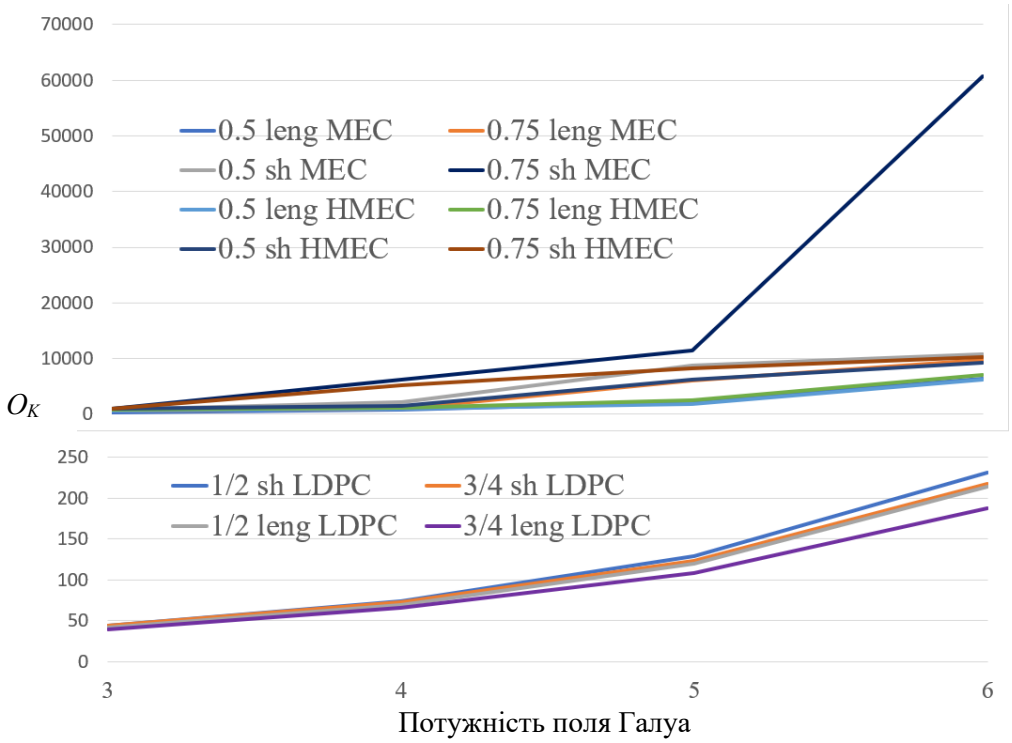

Рис. 2. Складність формування кодограми в залежності від потужності поля Галуа

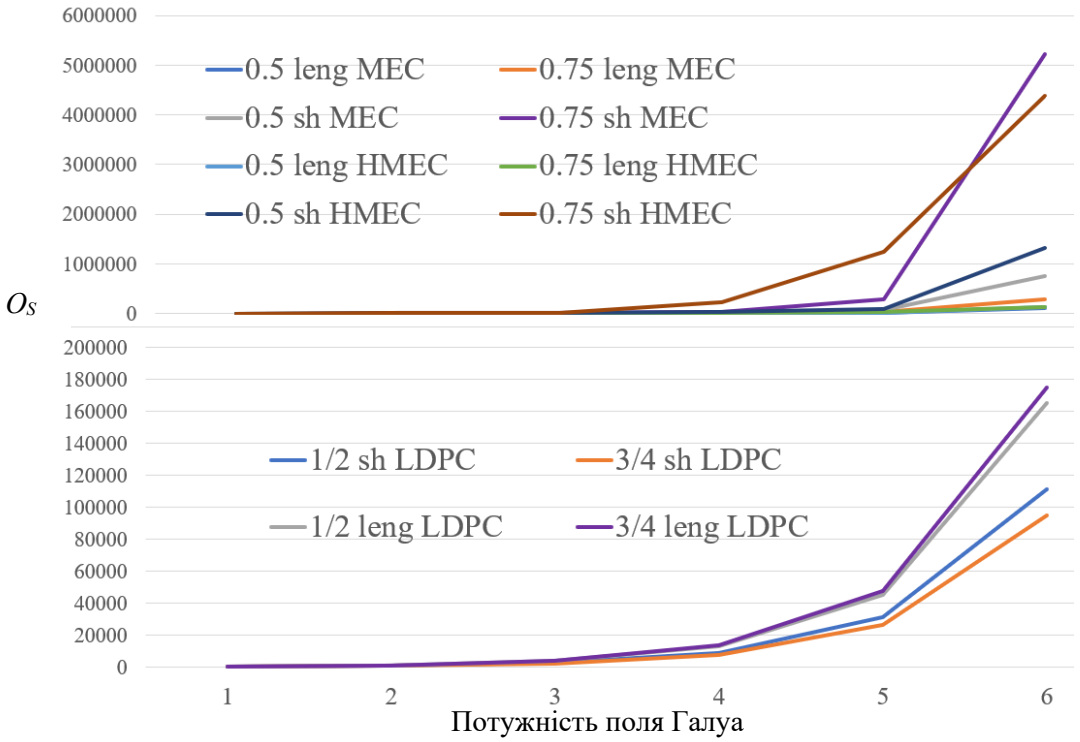

Рис.3. Складність розкодування в залежності від потужності поля Галуа

Розроблена математична модель дозволяє використовувати ССС McEliece для забезпечення послуг конфіденційності цілісності та автентичності та практично реалізувати запропонований метод. Основною відмінністю від відомих моделей є збереження рівня пропускних можливостей бездротового каналу інтегровано забезпечити необхідний рівень захищеності (криптостійкості) каналу (криптостійкість на основі постквантових алгоритмів на рівні 1025–1035 групових операцій), достовірності ($P_{пом}$ не нижче 10-9–10-12).

Для зниження енергетичних витрат та практичної реалізації крипто-кодових конструкцій без зниження рівня криптостійкості пропонується використовувати модифіковані (укорочені та/або подовжені) LDPC-коди. Також наведені результати досліджень залежності програмної реалізації від потужності поля, як видно з таблиці, використання модифікованих крипто-кодових конструкцій забезпечує зниження енергетичних витрат на програмну реалізацію практично в 5 разів, що дозволяє забезпечити їх практичну цінність (табл. 2). В табл. 3 наведено результати оцінки статистичної безпеки

Таблиця 2 – **Залежність програмної реалізації від потужності поля**

Криптосистеми	2^5	2^6	2^7	2^8	2^9	2^{10}
ССС McEliece на LDPC-кодах	10018042	18048068	32847145	47489784	63215578	82467897
ССС McEliece на скорочених LDPC-кодах	10007947	17787431	28595014	44079433	61974253	79554764
ССС McEliece на подовжених LDPC-кодах	11156138	18561228	33210708	48297112	65171690	84051337

Таблиця 3 – **Результати дослідження статистичної безпеки (NIST STS 822)**

Криптосистеми	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей	Кількість тестів, в яких тестування пройшли менше 96% послідовностей
ССС McEliece	149 (78,83%)	189 (100%)	0 (0%)

Криптосистеми	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей	Кількість тестів, в яких тестування пройшли менше 96% послідовностей
CCC McEliece на укорочених LDPC-кодах	151 (79,89%)	189 (100%)	0 (0%)
CCC McEliece на подовжених LDPC-кодах	152 (80,42%)	189 (100%)	0 (0%)
HCCC McEliece на подовжених LDPC-кодах	153 (80,95%)	189 (100%)	0 (0%)
HCCC McEliece на укорочених LDPC-кодах	155 (82 %)	189 (100%)	0 (0%)

Результати наведені в табл. 3, підтверджують можливість їх використання в СІС, а також доцільність використання запропонованих гібридних криптосистем в СІС.

На рис. 4 наведено структурну схему методології формування багатоконтурної системи захисту інформаційних ресурсів у соціальних інтернет-сервісах. Основною відмінністю від відомих підходів є можливість синтезу як експертного, так і системного аналізу не тільки цільових загроз на соціокіберфізичні системи, а й можливість об'єктивної оцінки поточного стану захищеності інформації [15].

Такий підхід дозволяє своєчасно реагувати на можливі зміни (модифікації) цільових загроз, а також враховувати їхню синергію та гібридність, можливість комплексування з методами соціальної інженерії. Пропоновані практичні рішення щодо забезпечення послуг безпеки на основі постквантових алгоритмів дозволяють забезпечити необхідний рівень стійкості конфіденційної інформації з різними рівнями їх секретності.

За результатами оцінювання для кожної групи показників формується інтегральний показник поточного рівня безпеки для відповідності матриці між послугами безпеки та інформаційними ресурсами. Для цього визначається абсолютне та відносне значення інтегрального показника:

$$IS_{\inf\_abs} = \frac{\sum S_{\inf_{il}}}{i \times l}, \qquad IS_{\inf\_rel} = \frac{IS_{\inf\_abs} - S_{\inf_{il}\min}}{S_{\inf_{il}\max} - S_{\inf_{il}\min}}, \tag{15}$$

де $IS_{\inf\_abs}$ – абсолютний інтегральний показник поточного рівня захищеності інформації для матриці відповідності послуг безпеки та інформаційних ресурсів; $IS_{\inf\_rel}$ – відносний інтегральний показник поточного рівня захищеності інформації для матриці відповідності послуг безпеки та інформаційних ресурсів; $S_{\inf_{il}}$ – елементи загальної матриці відповідності послуг безпеки та інформаційних ресурсів; i – кількість послуг безпеки; l – кількість інформаційних ресурсів; $S_{\inf_{il}\min}$ – мінімальний елемент матриці відповідності послуг безпеки та інформаційних ресурсів; $S_{\inf_{il}\max}$ – мінімальний елемент матриці відповідності послуг безпеки та інформаційним ресурсам.

Загальний інтегральний показник поточного рівня захищеності інформації в аналізованій системі безпеки формується за допомогою адитивної згортки окремих абсолютних інтегральних показників та мультиплікативної згортки окремих відносних інтегральних показників.

Адитивний інтегральний показник поточного рівня безпеки інформації в системі безпеки розраховується за формулою:

$$IS_{add} = IS_{\inf\_abs} + IS_{ISO\_abs} + IS_{serv\_abs}. \tag{16}$$

Мультиплікативний інтегральний показник поточного рівня захисту в системі безпеки розраховується за формулою:

$$IS_{mult} = IS_{\inf\_rel} \times IS_{ISO\_rel} \times IS_{serv\_rel}. \tag{17}$$

Таким чином, можна визначити загальну інтегральну оцінку захищеності системи: чим ближче значення відносного показника до 1, тим вище вплив відповідних факторів на захищеність інформації в системі безпеки. Розрахунок в програмному комплексі проводиться автоматично, результат наведено на рис. 5.

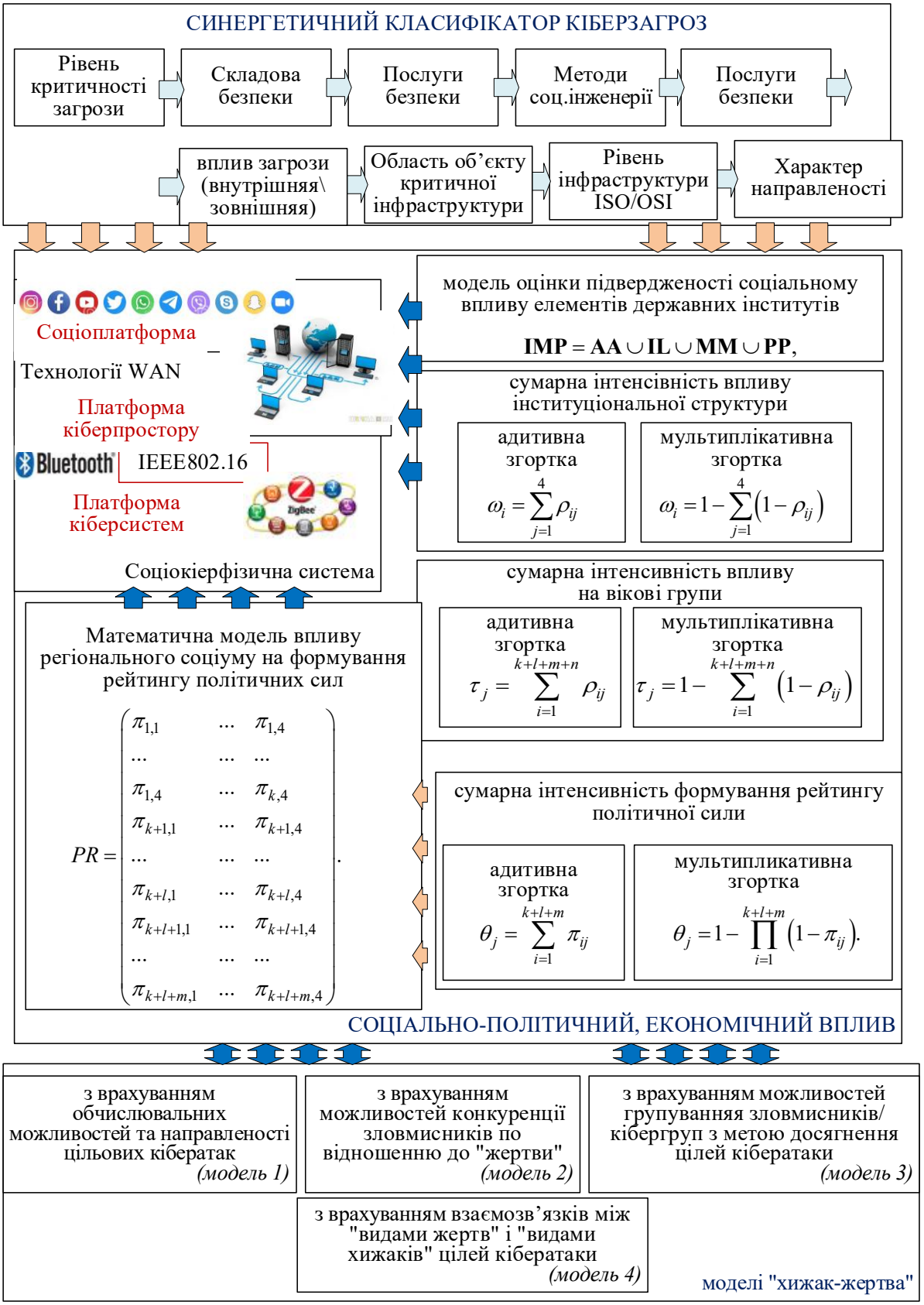

Рис. 4. Структурна схема побудови системи оцінки поточного стану багатоконтурної системи захисту

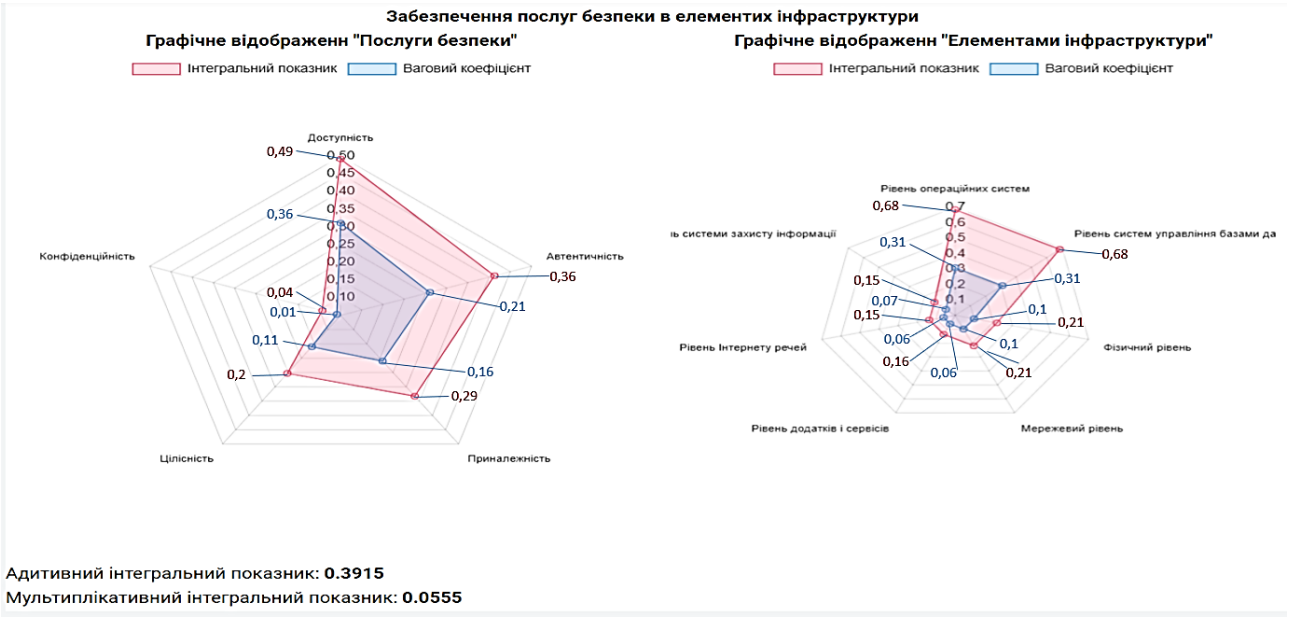

Рис. 5. Інтегральні показники захищеності інформаційних ресурсів в програмному комплексі – графічна інтерпретація

4. Висновки

Проведений аналіз загроз на соціокіберфізичні системи (об'єкти критичної інфраструктури)дозволяє сформувати методологію побудови багатоконтурних систем захисту інформації Одним з основних елементів таких систем пропонується використовувати постквантові алгоритми – крипто-кодові конструкції на різних завадових кодах з можливістю завдання шкоди. Пропоновані крипто-кодові конструкції McEliece на LDPC-кодах забезпечують оперативність та стійкість, забезпечують необхідний рівень основних послуг безпеки.

Запропонована структурна схема методології побудови багатоконтурних систем захисту забезпечує можливість отримання об'єктивної оцінки поточного стану захищеності в соціокіберфізичних системах. Пропонований програмний комплекс оцінки дозволяє отримати інтегрований показник безпеки, виявити критичні точки вразливості та «можливість» зловмисника отримати доступ до конфіденційної інформації. А запропоновані механізми та протоколи на основі постквантових алгоритмів забезпечать необхідний рівень стійкості та оперативності у період появи повномасштабного квантового комп'ютера.

REFERENCES

1. Zargar S.T., Anuar N.B., Khan M.K. A Survey on Social Engineering Attacks, Detection and Countermeasures in the Modern Era. // Computers & Security. – 2023. – Vol. 130. – Article 103129. https://doi.org/10.1016/j.cose.2023.103129.
2. Conti M., Dehghantanha A., Fratantonio Y. Cyber Threat Intelligence: Challenges and Opportunities in a Fast-Changing Landscape. // Future Generation Computer Systems. – 2022. – Vol. 135. – Pp. 346–357.
3. Singh M., Shukla, S. Multi-Layered Information Security Framework for Social Media Platforms. // Journal of Information Security and Applications. – 2022. – Vol. 65. – Article 103064.
4. Wang Y., Chen C. A Lightweight LDPC-Based Cryptographic Construction for Multimedia Security. // IEEE Access. – 2023. – Vol. 11. – Pp. 512–525.
5. Khan R., Alazab M. Hybrid Cryptographic Schemes for Secure Data Transmission in Cyber-Physical Systems. // Journal of Network and Computer Applications. – 2022. – Vol. 200. – Article 103321.
6. Mahmood A., Malik, H. Modern Threats to Information Security in Social Networks: Analysis and Detection Techniques. // Computers & Security. – 2021. – Vol. 108. – Article 102344.

7. Zhang Y., & Lin X. Recent Advances in Secure Multimedia Systems Based on Coding Theory. // IEEE Transactions on Multimedia. – 2021. – Vol. 23. – Pp. 4012–4025.
8. Beshaj L. Applications of Finite Fields in Cryptography and Coding Theory. // Mathematics. – 2021. – Vol. 9(12). – Article 1376.
9. Kaur J., Arora A. A Survey on Cryptographic Algorithms and Their Role in Securing Social Media. // Journal of Cybersecurity and Privacy. – 2022. – Vol. 2(1). – Pp. 91–112.
10. Radanliev P., et al. Cyber-Physical Systems Threat Modelling for Critical Infrastructures. // Journal of Cybersecurity. – 2021. – Vol. 7(1). – Pp. 1–16.
11. European Union Agency for Cybersecurity (ENISA). Threat Landscape for Social Engineering Attacks 2023. – ENISA Report. – 2023. – 48 p. https://www.enisa.europa.eu.
12. U.S. Department of Homeland Security. Securing the Future: Strategic Approach to Cyber-Physical System Security. – DHS White Paper. – 2022. – 34 p.
13. Milevskyi S., Yevseiev S., Hryshchuk R. and others. Modeling of security systems for critical infrastructure facilities: monograph. Kharkiv: Pc Technology Center. – 2022, 196 p. DOI: 10.15587/978-617-7319-57-2
14. Milevskyi S., Yevseiev S., Pohasii S., Milov O., Melenti Y., Grod I., Berestov D., Fedorenko R., Kurchenko O. Development of a method for assessing the security of cyber-physical systems based on the Lotka-Volterra model. // Eastern-European Journal of Enterprise Technologies. - 2021. - № 5/9 (113). - Pp. 30–47. DOI: 10.15587/1729-4061.2021.241638.
15. Milevskyi S., Yevseiev S., Ryabukha Y., Milov O., Pohasii S., Ivanchenko Y., Ivanchenko I., Melenti Y., Opirskyy I., Pasko I. Development of a method for assessing forecast of social impact in regional communities. // Eastern-European Journal of Enterprise Technologies. - 2021. - № 6/2 (114). - Pp. 30-43. DOI: 10.15587/1729-4061.2021.249313.

Received (Надійшла) 29.04.2025
Accepted for publication (Прийнята до друку) 20.05.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Мілевський Станіслав Валерійович – доктор технічних наук, доцент, професор кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Stanislav Milevskyi – Doctor of Technical Sciences, Docent, Professor of Cybersecurity Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: milevskiysv@gmail.com; ORCID Author ID: https://orcid.org/0000-0001-5087-7036;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57211218421.

DEVELOPMENT OF THE METHODOLOGY FOR BUILDING SECURITY SYSTEMS OF INFORMATION RESOURCES IN INTERNET SERVICES

Stanislav Milevskyi

Abstract. Relevance of the topic. The article addresses the issue of developing security systems for information resources in internet services in the context of sociocyberphysical systems (SCPS). **The purpose.** A methodology for constructing a multi-layered information protection system is proposed, focusing on multimedia content used within social internet services. **Results.** The approach integrates advanced mathematical methods, including set theory, finite field theory, cryptography, and systems analysis. Special attention is given to hybrid threats that combine social engineering with attacks on SCPS components, which are typical of modern hybrid warfare. **Conclusions.** The results aim to enhance the protection of multimedia resources and improve resistance to targeted cyber threats.

Keywords: sociocyberphysical systems; social internet services; information security; hybrid crypto-code constructions; multi-layered protection; LDPC codes; social engineering methods