УДК 004.7 **doi**: https://doi.org/10.20998/3083-6298.2025.01.06

Сергій Погасій[1]

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

РОЗРОБКА МЕТОДОЛОГІЇ ПОБУДОВИ БАГАТОКОНТУРНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ У КІБЕРФІЗИЧНИХ СИСТЕМАХ

Анотація. Актуальність теми. У цій статті представлено методологію побудови багаторівневої системи інформаційної безпеки для кіберфізичних систем (КФС), що відповідає на сучасні виклики, пов'язані з гібридними та постквантовими загрозами. **Мета.** Формування концепції, що базується на п'яти етапах: оцінка ймовірності загрози, превентивне моделювання, теоретико-ігровий аналіз, реалізація постквантових криптографічних механізмів (CCS на основі LDPC) та розробка багатоконтурної архітектури безпеки. **Результати.** Ефективність захисту оцінюється за допомогою показників KPI(eff), KPIeffinv та KPInorm, зокрема в контексті мобільних бездротових технологій (LoRa, Sigfox, LTE-M, NB-CPS). Запропоновано модифікацію протоколу Go-Back-N для підвищення функціональної ефективності бездротових каналів пам'яті. **Висновки.** Запропоновані моделі можуть бути застосовані при розробці безпечних КФС для критичної інфраструктури та промислових систем Інтернету речей.

Ключові слова: кіберфізичні системи, багаторівнева безпека, постквантова криптографія, LDPC-коди, LPWAN

1. Вступ

Релевантність проблеми. У сучасному цифровому суспільстві кіберфізичні системи (КФС) відіграють ключову роль у забезпеченні роботи критичних інфраструктур, промислових об’єктів, медичних закладів, розумних міст та інших складних систем [1-6]. Вони інтегрують обчислювальні ресурси, мережеву інфраструктуру та фізичні компоненти, що взаємодіють у реальному часі. Захист інформаційних ресурсів КФС є стратегічно важливим, оскільки порушення їхньої цілісності чи автентичності може спричинити серйозні економічні та соціальні наслідки.

Загрози для КФС є багатогранними, включаючи традиційні кібератаки (шкідливе ПЗ, несанкціонований доступ, фальсифікація даних) і нові виклики, пов’язані з квантовими обчисленнями, цільовими атаками на мережі та гібридними методами, що використовують соціальну інженерію [7-13]. Особливо вразливими є мобільні бездротові канали, які застосовуються для віддаленого моніторингу, управління та автоматизації в КФС.

За таких умов потрібні інноваційні системи кібербезпеки для надійного захисту даних у КФС. Перспективним є створення багатоконтурних архітектур безпеки, що враховують внутрішні та зовнішні загрози, моделюють поведінку зловмисників і адаптивно формують превентивні заходи. Поєднання з математичними моделями та постквантовою криптографією забезпечує стійкий захист [5,6].

Запропоновано п’ятиетапну методологію захисту КФС [5,6]: оцінка ймовірності кіберзагроз; розробка превентивних моделей на основі рівнянь Лотки-Вольтерри; аналіз ефективності захисту через теоретико-ігрові моделі; створення механізмів забезпечення конфіденційності, цілісності та автентичності; формування стратегій захисту з урахуванням ресурсів зловмисників. Цей підхід гарантує систематичне вирішення завдань безпеки.

Центральним елементом є постквантові криптосистеми на основі кодів (ККК) із LDPC-кодами, які забезпечують високу швидкість криптографічних операцій і низьке енергоспоживання [7-13]. Це критично для мереж LPWAN (LoRa, Sigfox, LTE-M, NB-CPS). LDPC-коди підвищують ефективність безпеки, зберігаючи прийнятні затримки та енергоспоживання.

Для аналізу взаємодії між системою захисту та зловмисником застосовуються теоретико-ігрові моделі, що визначають оптимальні стратегії за обмежених ресурсів [5,6,11]. Модель Лотки-Вольтерри адаптовано до кібербезпеки, враховуючи гібридність і синергізм загроз, а також фінансові й обчислювальні можливості атакуючих [5,6].

Методика оцінки функціональної ефективності КФС враховує ймовірність доставки даних, розмір пакетів, час передачі та стійкість системи [14-17]. Вона базується на ключових показниках ефективності (KPI), обґрунтовуючи економічну доцільність технологій безпеки та забезпечуючи надійність КФС у високоризикових умовах.

Запропонована концепція поєднує математичне моделювання, постквантову криптографію та оцінку ризиків, створюючи основу для гнучкої системи захисту КФС [1-17]. Її актуальність підтверджується зростанням кіберінцидентів, новими загрозами від квантових технологій і вимогами до надійності, енергоефективності та безперебійної роботи КФС у різних сферах.

2. Основна частина

Розвиток складних систем критичної інфраструктури та активізація досліджень динаміки КФС вимагають постійного вдосконалення інструментів моделювання й управління динамічними системами [1-6]. Сучасні наукові підходи зосереджені на розробці методологій для систем із параметрами, що динамічно змінюються,

що значно розширює спектр вирішуваних завдань завдяки аналізу таких систем.

На основі праць [7-13] запропоновано нову методологію захисту інформаційних ресурсів КФС, яка інтегрує моделі багатоконтурних систем безпеки та постквантові криптографічні алгоритми, зокрема крипто-кодові конструкції (ККК) на основі LDPC-кодів (рис 1).

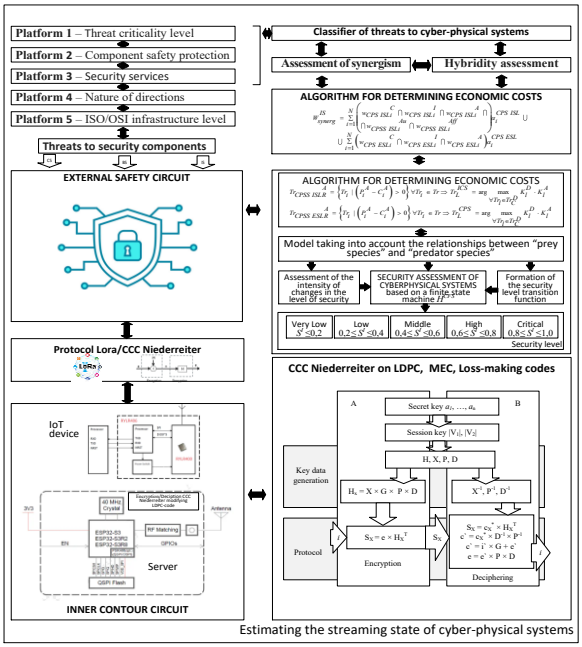

Рис 1. Схематичне зображення потокового стану CPS, що відображає динаміку безпеки [5,6]

Методологія охоплює п'ять етапів [5,6]:

1. Оцінка ймовірності впливу кіберзагроз на КФС.
2. Розробка моделей превентивних заходів із використанням моделі Лотки-Вольтерри.
3. Аналіз ефективності захисту за допомогою теоретико-ігових моделей.
4. Створення комплексних механізмів забезпечення конфіденційності, цілісності, автентичності та доступності інформаційних ресурсів КФС.
5. Визначення стану системи та розробка стратегій побудови багатоконтурних систем захисту. Ці алгоритми вирізняються високою швидкістю обробки даних і придатністю для мобільних технологій Інтернету речей. Структурно-логічна схема методології представлена в джерелах [5,6] та на рис 2.

Перший етап

Для оцінювання ймовірності кіберзагроз у кіберфізичних системах (CPS) застосовується експертний метод із використанням програмного класифікатора загроз, доступного за посиланням https://skl.sspu.sumy.ua/threat [7]. Адаптований класифікатор забезпечує формування експертних оцінок для аналізу безпеки CPS на основі концепції двоконтурної системи захисту.

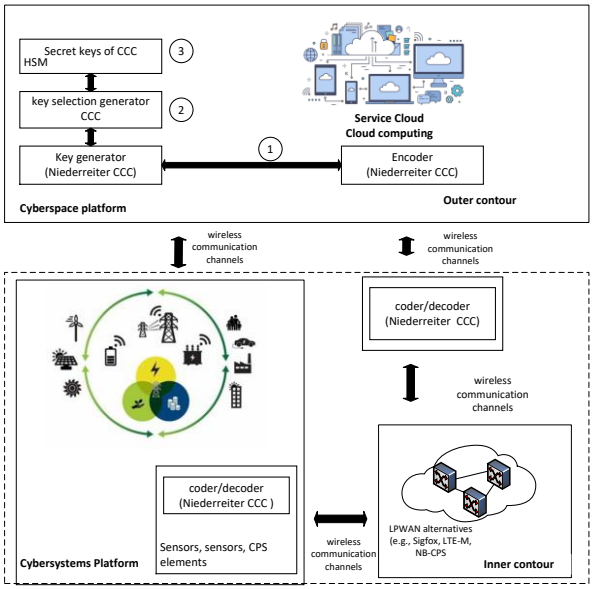

Рис. 2. Структурна схема багатоконтурної системи захисту CPS, що ілюструє взаємодію контурів [5,6]

Поточний стан інформаційної безпеки оцінюється за бінарною шкалою, де значення «1» відповідає максимальному рівню захисту, забезпечуваному системою безпеки, а «0» — повній відсутності захисту інформаційних ресурсів. Ймовірність реалізації загрози визначається через різницю функцій щільності ймовірності випадкової величини (x) Зазначена ймовірність визначається різницею F(B)–F(A), де A – граничний рівень можливостей сторони захисту, B – граничний рівень можливостей реалізації атаки сторони нападу.

Рівень безпеки системи обчислюється як частка захищених ресурсів від кібератак:

$$S = F(B) - F(A) = \int_{-\infty}^{B} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt - \int_{-\infty}^{A} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt. \quad (1)$$

Для забезпечення безпеки системи враховуються загрози внутрішнього та зовнішнього контурів з урахуванням їхньої гібридності та синергізму:

$$W^{CPS\ ISL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg} = W^{CPS\ ISLC}_{synerg} \bigcap W^{CPS\ \ ISLI}_{synerg} \bigcap W^{CPS\ \ ISLA}_{synerg} \bigcap W^{CPS\ ISLAu}_{synerg} \bigcap W^{CPS\ \ ISLInv}_{synerg}, \quad (2)$$

$$W^{SCP\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg} = W^{CPS\ ESLC}_{synerg} \bigcap W^{CPS\ \ ESLI}_{synerg} \bigcap W^{CPS\ \ ESLA}_{synerg} \bigcap W^{CPSS\ \ ESLAu}_{synerg} \bigcap W^{CPS\ \ ESLInv}_{synerg}, \quad (3)$$

Для забезпечення безпеки системи враховуються загрози внутрішнього та зовнішнього контурів з урахуванням їхньої гібридності та синергізму:

$\gamma^{CPS}_{ICS\ i} = \left(\beta^{ICS}_i \cup \beta^{CPS}_i\right) \times p_{rj} \times r_{motiv}$, — множини загроз для внутрішнього (ISL) та зовнішнього (ESL) контурів;

$W_{cp}^{CPSS\ ISL}\left(W_{cp}^{CPSS\ ESL}\right)$ — обчислювальні ресурси зловмисника;
$W_{cash}^{CPSS\ ISL}\left(W_{cash}^{CPSS\ ESL}\right)$ — економічні можливості зловмисника [5,6,13].

Класифікація зловмисників формує множини ({H_j}) для ISL та ESL, які визначають ступені впливу на КФС. Ваговий коефіцієнт небезпеки зловмисника розраховується за формулою:

$$\gamma_{ICS}^{CPS} = \frac{1}{N}\sum_{i=1}^{N}\gamma_{ICS\,i}^{CPS}, \qquad (4)$$

Критерії та показники експертної оцінки, наведені в роботах [5,6], дозволяють враховувати, що атака залежить від комплексного критерію, який включає витрати на її проведення та обчислювальні ресурси зловмисника.

Eman 2

Для створення моделей превентивних заходів захисту КФС використовується модель Лотки-Вольтерри «хижак-жертва» .[5,6]

Отримані параметри моделі α=0,39, β=0,32, γ=0,29, φ=0,27, враховують гібридність і синергізм сучасних кіберзагроз, фінансові ресурси, спрямовані на вдосконалення системи безпеки, а також економічні й обчислювальні можливості зловмисників, визначені за виявленими загрозами.

Моделі безпеки КФС розробляються з урахуванням обчислювальних ресурсів і спрямованості цільових кібератак. Чисельність об'єктів, що є потенційними цілями атак із урахуванням їхньої гібридності, описується виразом:

$$\tilde{N}_1 = \sum_{i=1}^{Q}\begin{pmatrix} N_{1_i}^{C}\times A_i^{C} + N_{1_i}^{I}\times A_i^{I} + N_{1_i}^{A}\times A_i^{A} + \\ + N_{1_i}^{Au}\times A_i^{Au} + N_{1_i}^{Aff}\times A_i^{Aff} \end{pmatrix}, \qquad (5)$$

Алгоритм передбачає, що сторони конфлікту оцінюють критичність кіберзагроз, визначаючи економічно доцільні атаки або пріоритетні ресурси для захисту. Коефіцієнт «народжуваності» жертв α взято з роботи [6]. Вплив загроз на захисні механізми β оцінено за виразом із джерел [5,6,7]. Для визначення коефіцієнта обчислювальних можливостей зловмисника γ використано класифікацію зловмисників, наведену в [5,6,7].

У табл. 1 представлено критерії та показники експертної оцінки для визначення вагового коефіцієнта обчислювальних можливостей зловмисника [5,6].

Коефіцієнт ефективності превентивних заходів розраховується як:

$$\gamma^{j} = \frac{1}{K\times B}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\mu_{kg}^{j}\times w_{kg}^{j}\right), \qquad (6)$$

Запропоновані моделі формують метод оцінки безпеки КФС на основі концепції Лотки-Вольтерри «хижак-жертва».

Таблиця 1 – **Критерії та показники експертної оцінки вагового коефіцієнта обчислювальних можливостей зловмисника**

Категорія	Вагові показники оцінки вагового коефіцієнта				
	$\beta_i^{CPS} \in \{\beta_i^{CPS}\}$			prj	rmotiv
	W_{cp}^{CPS}	TCPS	W_{cash}^{CPS}		
критична	1	1	1	1	1
висока	0,75	0,75	0,75	0,75	0,75
середня	0,5	0,5	0,5	0,5	0,5
низька	0,25	0,25	0,25	0,25	0,25
дуже низька	0,001	0,001	0,001	0,001	0,001

Eman 3

Для аналізу ефективності системи безпеки КФС застосовуються моделі взаємодії антагоністичних агентів, описані в роботах [5,6,11]. Ці моделі вирішують дві ключові задачі кібербезпеки: взаємодію системного адміністратора та зловмисника під час захисту інформаційних ресурсів. Розглядаються два сценарії: матриця гри з вартісними оцінками ресурсів і матриця з ймовірностями реалізації загроз. Для різних початкових умов визначено чисті та змішані стратегії, що дозволяє виключити неефективні варіанти захисту.

Ці моделі створюють основу для таксономії ігор і їхніх моделей. Теоретико-ігові підходи сприяють вирішенню завдань із забезпечення основних аспектів безпеки: конфіденційності, цілісності, доступності та автентичності інформаційних ресурсів.

Eman 4

Для гарантування конфіденційності, цілісності, автентичності та достовірності інформаційних ресурсів КФС пропонується застосування крипто-кодових конструкцій (ККК) Niederreiter, детально описаних у джерелах [5,6,8,10,12].

Генерація відкритого ключа для ККК Niederreiter здійснюється шляхом множення матриці маскування на породжувальну або перевірочну матрицю:

$$H_{X_{a_i}}^{LDPCu} = X^{u}\times H^{LDPCu}\times P^{u}, u\in\{1,2,...,r\}. \qquad (7)$$

У канал зв'язку передається синдромна послідовність:

$$S^{*} = (e_n)\times H_{X_{a_i}}^{LDPC^{T}}. \qquad (8)$$

де (H) — перевірочна матриця; (e) — сеансовий ключ для кожної інформаційної посилки.

Для обробки даних у ССС Niederreiter використовується спеціалізований алгоритм.

На стороні приймача уповноважений користувач, володіючи матрицями маскування, застосовує швидкий алгоритм м'якого декодування для розшифрування повідомлень. Застосування постквантових асиметричних криптосистем забезпечує високий рівень захисту при наданні послуг безпеки. Використання LDPC-кодів сприяє інтеграції з мобільними бездротовими технологіями, що базуються на стандартах IEEE 802.XX.

Eman 5

На п'ятому етапі визначається стан CPS і розробляються стратегії створення багатоконтурних систем захисту. Пропонується поділ CPS на дві підсистеми: безпеки та інфраструктури. Внутрішній контур забезпечує базові послуги та функціональність, тоді як зовнішній контур формує управлінську систему (MS), що поєднує бездротові мережі та хмарні технології.

Такий підхід сприяє інтеграції внутрішнього та зовнішнього контурів, враховуючи їхню оперативність, енергоефективність і рівень безпеки. Він також дозволяє оцінити загрози для кожного контуру, враховуючи обчислювальні ресурси та економічні можливості зловмисників. Структурна схема концепції двоконтурної безпеки CPS представлена в джерелах [5,6].

На основі досліджень розроблено комплексний показник функціональної ефективності CPS, який оцінює продуктивність і надійність системи з урахуванням безпеки, конфіденційності, економічних витрат і якості обслуговування. Для створення моделі цього показника необхідно визначити вплив кожного фактора на загальну ефективність і об'єднати їх у формулу.

Методика оцінювання функціональної ефективності передачі даних на основі комплексного показника враховує емерджентні властивості, синтезуючи показник ефективності інвестицій у безпеку, оцінку сучасних загроз із їхньою гібридністю та синергізмом, а також результати швидкої оцінки стійкості й ефективності програмної або програмно-апаратної реалізації криптографічних алгоритмів.

$$KPI\,(_{eff}) = \frac{R-T}{R} \times B \times P \times KPI_{effin} \times KPI_{norm}, \quad (9)$$

де (P) — ймовірність доставки пакету; (R) — розмір пакету; (T) — час доставки; (B) — стійкість системи безпеки.

Для оцінки ефективності інвестицій у безпеку інформаційних ресурсів у LPWAN застосовується нормалізований багатофакторний підхід, що враховує енергоефективність, енергоспоживання та стійкість системи. Комплексний показник ефективності інвестицій (*KPI(eff)*) обчислюється як зважена сума нормалізованих факторів:

$$KPI_{effinv} = w_1 \frac{P}{P_{\max}} + w_2 \frac{Ef}{Ef_{\max}} + w_3 (1 - \frac{Ed}{Ed_{\max}}) + w_4 \frac{Bi}{Bi_{\max}} + ... + w_m \frac{Bn}{Bn_{\max}}, \quad (10)$$

де Ef – енергоефективність; d – енергоспоживання; Bi – стійкість системи безпеки; wi – вагові коефіцієнти (визначають важливість кожного фактора).

Для розрахунку *KPI(eff)* враховується змінений рівень таємності інформації при використанні ККК на LDPC-кодах, які забезпечують підвищену достовірність завдяки виправленню помилок, оперативність за швидкістю криптоперетворень, порівнянною з симетричною криптографією, і необхідний рівень енергоефективності. Порівняльні дослідження за критеріями оперативності та енергоефективності підтверджують ці властивості. Інтеграція з технологіями на основі ККК і гібридних ККК (ГККК) забезпечує дотримання ключових вимог сучасних бездротових мереж і фундаментально трансформує методологічні підходи до створення систем безпеки.

У табл. 2 наведені результати аналізу показників даних про *KPInorm, KPIeffinv* та *KPI(eff)*.

Таблиця 2 – **Характеристики ефективності бездротових технологій низької потужності широкого радіусу дії**

Технологія	Нормований коефіцієнт ефективності KPI_{norm}	Коефіцієнт ефективності інвестицій KPI_{effinv}	Коефіцієнт ефективності *KPI(eff)*
LoRa	0,21	0,794	0,04218
Sigfox	0,14	0,735	0,00050
LTE-M	0,68	0,378	0,00423
NB-CPS	0,56	0,753	0,00691
EC-GSM-CPS	0,35	0,875	0,36610
LoRa ГККК на LDPC-кодах	0,21	0,919	0,58586
LoRa ККК на LDPC-кодах	0,21	0,981	0,83385

Технології LoRa, що використовують постквантові ККК на основі LDPC-кодів, включаючи асиметричні та гібридні криптосистеми (LoRa ККК і LoRa ГККК), забезпечують достатній рівень ефективності в постквантовий період. Вони дозволяють протидіяти цільовим атакам із ознаками гібридності та синергізму, зокрема комбінованим атакам, що використовують методи соціальної інженерії, а також підвищують достовірність даних і підтримують їхнє застосування в смарт-технологіях із обмеженими вимогами до енергоефективності.

Для підвищення комплексного показника функціональної ефективності *KPI(eff)* КФС пропонується впровадження протоколів управління обміном даними, які забезпечують оперативність передачі, стійкість до перешкод і безпеку. Одним із таких протоколів є Go-Back-N, що реалізує безперервну передачу кадрів зі зворотним зв'язком, сприяючи досягненню необхідного рівня ефективності КФС.

Ефективність управління обміном даними за протоколом Go-Back-N оцінюється за модифікованою формулою, яка враховує повторну передачу вікна пакетів у разі виявлення помилки [14-17]. Модифікація формули методу Go-Back-N передбачає повторну передачу вікна пакетів при виявленні помилки, що може вплинути на ймовірність успішної доставки (P) може незначно знижуватися, якщо помилка часто не виявляється, повторні передачі можуть збільшити час доставки T, споживання енергії збільшується через повторні передачі.

$$KPI\,(_{eff\_GBN}) = \frac{R-T}{R} \times B \times P \times (1-\mathrm{P}_{\mathrm{retry}}) \times KPI_{effin} \times KPI_{norm}, \quad (11)$$

де $\mathrm{P}_{\mathrm{r}\,etry}$ – коефіцієнт, що враховує ймовірність повторної передачі пакетів у разі виявлення помилки. Цей коефіцієнт є критично важливим для “Go-Back-N”, оскільки потрібно враховувати ймовірність того, що помилка може призвести до повторної передачі.

На рис. 3 наведені результати оцінки ефективності інвестицій та загальна ефективність передачі даних для методу “Go-Back-N” з урахуванням особливостей зворотного зв’язку та безперервної передачі кадрів за моделлю передачі даних без пам’яті.

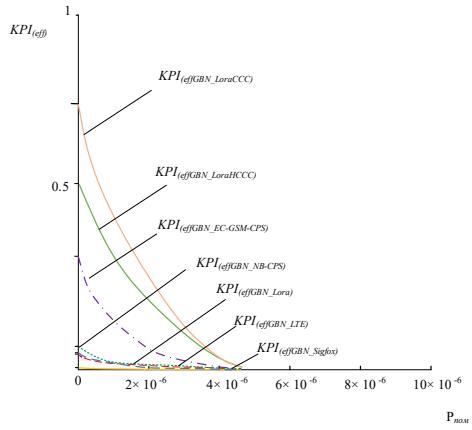

Рис. 3. Оцінка комплексного показника ефективності в каналах без пам’яті

Для розрахунку показника функціональної ефективності *KPI(eff)* за протоколом Go-Back-N у каналах із пам’яттю, враховуючи ймовірність виникнення пакету помилок, внутрішньопакетні помилки, математичне сподівання довжини пакету помилок і середньоквадратичне відхилення, застосовується модифікована формула:

$$KPI\,(_{eff\_GBN\_\mathrm{mem}}) = (\frac{R-T}{R}) \times B \times P \times (1-\Phi(\frac{P_e - E(L)}{\sigma(L)})) \times KPI_{effin} \times KPI_{norm}, \quad (12)$$

де P_e – ймовірність виникнення помилки в пакеті; *E(L)* – математичне сподівання довжини пакету помилок; *σ(L)* – середньоквадратичне відхилення довжини пакету помилок, яка враховує варіативність у кількості пакетів, які можуть бути втрачені через помилки; $\Phi(\frac{P_e - E(L)}{\sigma(L)})$ – кумулятивна функція розподілу нормального розподілу (функція Лапласа), що враховує ймовірність помилки в пакеті (чим ближче значення функції до 1, тим більша ймовірність того, що помилки будуть виявлені та виправлені).

У табл. 3 приведені порівняння коефіцієнтів ефективності для технологій LPWAN, зокрема для протоколу “Go-Back-N” у моделях каналів без пам’яті та з пам’яттю.

Таблиця 3– **Порівняння коефіцієнтів ефективності технологій LPWAN для протоколу Go-Back-N у каналах без пам’яті та з пам’яттю**

Технологія	$KPI\,(_{eff})$	$KPI\,(_{eff\_}$	$KPI\,(_{eff\_GBN\_\mathrm{mem}})$
LoRa	0,04218	0,03796	0,04639
Sigfox	0,00503	0,00452	0,00552
LTE-M	0,04234	0,03801	0,04654
NB-CPS	0,06902	0,06212	0,07591
EC-GSM-CPS	0,36609	0,32948	0,40270
LoRa ККК на LDPC-кодах	0,58586	0,52727	0,64444
LoRa ГККК на LDPC-кодах	0,83385	0,75047	0,91723

Аналіз даних із табл. 3 і рис. 3 показує, що використання ККК на LDPC-кодах (LoRa ККК) та гібридних ККК (LoRa ГККК) значно підвищує комплексний показник ефективності завдяки забезпеченню конфіденційності, цілісності й автентичності даних. Однак у разі використання повномасштабного квантового комп’ютера та багатопотокової криптографії показник *KPIeff* знижується на 9% (для LoRa ГККК— до 0,7505, для LoRa ККК — до 0,5273), але необхідний рівень безпеки зберігається.

Результати оцінки ефективності інвестицій і загальної ефективності передачі даних за протоколом Go-Back-N у каналах із пам’яттю, що відображають вплив зворотного зв’язку та безперервної передачі кадрів наведені на рис 4.

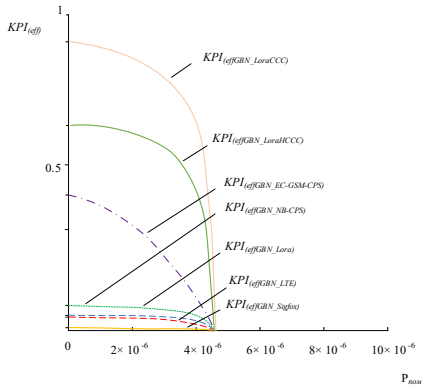

Рис. 4. Оцінка комплексного показника ефективності в каналах з пам’яттю

Модель каналу з пам’яттю забезпечує більш реалістичну оцінку реальних каналів зв’язку, враховуючи можливість пакетування помилок. Дані

з рис. 4 і табл. 3 підтверджують зростання комплексного показника ефективності на 10 % (LoRa ГККК на LDPC-кодах *KPIeff* дорівнює 0,917235,а LoRa ККК на LDPC-кодах *KPIeff* дорівнює 0,644446). При цьому забезпечується необхідний рівень безпеки в постквантовий період, зокрема проти цільових атак із гібридністю та синергізмом, що є критичним для захисту інфраструктури КФС.

Запропонована методика оцінки потокового стану автоматизованих систем передачі даних у бездротових каналах підвищує об’єктивність аналізу цільових атак, враховуючи фінансові, обчислювальні та людські ресурси зловмисників. Вона також ідентифікує критичні точки можливої вразливості інфраструктури та забезпечує механізми протидії кібератакам із визначеними рівнями безпеки.

3. Висновки

Це дослідження представляє комплексну методологію побудови багатоконтурної системи інформаційної безпеки для кіберфізичних систем (КФС), що вирішує сучасні проблеми, пов'язані з гібридними та постквантовими загрозами. Запропонований підхід має стратегічне значення для захисту інфраструктури, що працює в динамічному технологічному ландшафті, що характеризується швидким зростанням технологій бездротового зв'язку та обчислювальної техніки.

Методологія структурована навколо п'яти взаємопов'язаних етапів: оцінка ймовірності реалізації загрози, моделювання превентивних заходів за допомогою рівнянь Лотки-Вольтерра, застосування теоретико-ігрових моделей для оцінки стратегій захисту, реалізація постквантових криптографічних механізмів на основі кодів LDPC та проектування адаптивної багатоконтурної архітектури безпеки КФС. Цей перехід від реактивного до проактивного управління кібербезпекою забезпечує як зменшення загроз у реальному часі, так і системну стійкість.

Перший етап представляє метод оцінки ймовірності реалізації загрози за допомогою функції щільності ймовірності, яка порівнює оборонні та наступальні можливості. Модель враховує як зовнішні, так і внутрішні загрози та включає гібридні та синергетичні характеристики атак, пропонуючи надійну та реалістичну систему оцінки. Ця двоконтурна перспектива дозволяє розрізняти вразливості на системному рівні та вразливості на мережевому рівні.

На другому етапі превентивні дії моделюються за допомогою модифікованої системи Лотки-Вольтерра, яка традиційно використовується для представлення динаміки «хижак-жертва». Ця модель дозволяє відображати економічні та обчислювальні ресурси, доступні як зловмисникам, так і захисникам. Ключові коефіцієнти (α, β, γ, φ) відображають агресивність, стійкість та масштабованість як загроз, так і захисних механізмів, забезпечуючи основу для моделювання для розробки раціональної пріоритезації захисту.

На третьому етапі використовується теорія ігор для аналізу взаємодії між зловмисниками та системними адміністраторами, що дозволяє визначити оптимальні (чисті або змішані) стратегії в умовах невизначеності та обмежених ресурсів. Цей підхід особливо корисний для моделювання прийняття рішень у реальному часі та дозволяє усунути нежиттєздатні сценарії захисту в складних умовах конфлікту.

На четвертому етапі дослідження зосереджується на розробці криптографічних механізмів, що забезпечують конфіденційність, цілісність, автентичність та достовірність переданих даних. У дослідженні обґрунтовується використання CCC Niederreiter, побудованого на LDPC-кодах, які демонструють високу ефективність, відмовостійкість та низькі обчислювальні витрати. Ці криптосистеми сумісні з мобільними та бездротовими пристроями з обмеженими ресурсами та забезпечують стійкість до атак квантових обчислень.

На п'ятому та заключному етапі пропонується двоконтурна архітектурна модель для CPS, яка розділяє систему на операційну (внутрішню) та управлінську (зовнішню) підсистеми. Внутрішній контур керує наданням послуг та керуванням у режимі реального часу, тоді як зовнішній контур інтегрує бездротові та хмарні технології для віддаленого адміністрування та зв'язку. Цей поділ забезпечує багаторівневу безпеку та дозволяє диференційовані стратегії оцінки ризиків та їх зменшення для кожної підсистеми.

Окрім архітектурної основи, у статті представлено новий метод оцінки функціональної ефективності CPS в умовах конкуренції. Запропонована метрика KPI(eff) агрегує такі параметри, як ймовірність доставки даних, розмір пакета, час доставки, надійність безпеки та енергоефективність. Було продемонстровано, що інтеграція криптографічних механізмів на основі LDPC у бездротові технології LoRa значно покращує ці показники ефективності порівняно з іншими альтернативами LPWAN (наприклад, Sigfox, LTE-M, NB-CPS).

Крім того, у дослідженні оцінюється вплив модифікації протоколу Go-Back-N для бездротових каналів з пам'яттю та без неї. Було показано, що врахування ймовірностей повторної передачі та коефіцієнтів помилок пакетів покращує надійність та використання пропускної здатності в шумному середовищі, тим самим підвищуючи стабільність зв'язку.

Основний науковий внесок цієї роботи полягає у формалізації багаторівневої стратегії безпеки для CPS з використанням математичних моделей поведінки загроз, передових криптографічних методів та інструментів оцінки ефективності в режимі реального часу. Цей підхід забезпечує основу для адаптивних систем безпеки, які не тільки захищають від зовнішніх вторгнень, але й динамічно реагують на загрози, що розвиваються, та самокоригують свої операції.

Результати цього дослідження застосовні до проектування безпечних CPS у різних галузях, включаючи інтелектуальні мережі, промислову автоматизацію, електронну охорону здоров'я, інтелектуальні транспортні системи, військові технології та розумні міста. Вони також відкривають нові шляхи для майбутніх досліджень адаптивних самоорганізуючих механізмів кібербезпеки, гібридних криптографічних систем та стійкості до збройних атак на основі штучного інтелекту та квантових обчислень.

References

1. Holovka A. (2016). Information threats in a globalized world: economics, politics, society (experience of Ukraine). Baltic Journal of Economic Studies, 2 (3), 42 – 47. doi: https://doi.org/10.30525/2256-0742/2016-2-3-42-47.
2. DeBenedictis K. (2021). Russian “Hybrid Warfare” and the Annexation of Crimea. Bloomsbury Publishing. doi: https://doi. org/10.5040/9780755640027.
3. Yevseiev S., Katsalap V., Mikhieiev Y., Savchuk V., Pribyliev Y., Milov O., Pohasii S., Opirskyy I., Lukova-Chuiko N., Korol O. (2022). Development of a method for determining the indicators of manipulation based on morphological synthesis. Eastern-European Journal of Enterprise Technologies, №3 (9 (117)), Pp. 22–35. https://doi.org/10.15587/1729-4061.2022.258675.
4. Pohasii S., Yevseiev S., Milov O. and others (2020). Development and analysis of game-theoretical models of security systems agents interaction. Eastern-European Journal of Enterprise Technologies, № 4 (104). Pp. 15-29.
5. Pohasii S., Yevseiev S., Ryabukha Y. and others (2021). Development of a method for assessing forecast of social impact in regional communities. Eastern-European Journal of Enterprise Technologies, № 6/2 (114). Pp. 30-43.
6. Ekshmidt V. (2015). Verbal Manipulation: Persuasion and Suggestion. Movni i kontseptualni kartyny svitu, №1, Pp. 275–281. URL: http://nbuv.gov.ua/UJRN/Mikks_2015_1_31.
7. Kolmogorova A. V., Kalinin A. A., Malikova A. V. (2018). Linguistic principles and computational linguistics methods for the purposes of sentiment analysis of cyrillic texts. Current Issues in Philology and Pedagogical Linguistics, №1 (29), Pp. 139 – 148. doi: https://doi.org/10.29025/2079-6021-2018-1(29)-139-148.
8. Lytvyn V., Vysotska V., Uhryn D., Hrendus M., Naum O. (2018). Analysis of statistical methods for stable combinations determination of keywords identification. Eastern-European Journal of Enterprise Technologies, №2 (92), Pp. 23–37. doi: https:// doi.org/10.15587/1729-4061.2018.126009.
9. Molodetska-Hrynchuk K. (2017). Outreaches content tracing technique for social networking services. Radio Electronics, Computer Science, Control, №2 (41), Pp. 117-126. doi: https://doi.org/10.15588/1607-3274-2017-2-13.
10. Savchuk V. S., Hryshchuk R. V., Hryshchuk O. M., Musienko A. P. (2018). Intelligent system for evaluating destructive nature of text content of social networks based on fuzzy logic. Science-based technologies, №38 (2). doi: https://doi.org/10.18372/2310- 5461.38.12838.
11. Palchuk V. (2017). Methods of Content-Monitoring and Content-Analysis of Information Flows: Modern Features. Academic Papers of The Vernadsky National Library of Ukraine, №48, Pp. 506–526. doi: https://doi.org/10.15407/np.48.506.
12. Snitsarenko P., Nakonechnyi V., Mikhieiev Y., Hrytsiuk V. (2019). The approach to automated internet monitoring system creation. IEEE International Conference on Advanced Trends in Information Theory (ATIT). doi: https://doi.org/10.1109/ atit49449.2019.9030446.
13. Kuznetsov O. O., Oliinykov R. V., Horbenko Yu. I., Pushkariov A. I., Dyrda O. V., Horbenko I. D. (2014). Justification of requirements, design, and analysis of promising symmetric cryptographic transformations based on block ciphers. Bulletin of the National University "Lviv Polytechnic". Computer Systems and Networks. № 806, c. 124 – 141.
14. Sobchuk V. V., Laptev O. A., Pohasii S. S., Barabash A. O., Salanda I. P. (2021). Mathematical model for protecting an information network based on hierarchical hypernetworks. Scientific discussion. Praha, Czech Republic, Vol 1. No 61. Pp. 31 – 36.
15. GOST 34.601-90. Information technology. Set of standards for automated systems. Automated systems. Stages of development. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=53626.
16. Ian F Akyildiz, Tommaso Melodia, and Kaushik R Chowdury (2007). Wireless multimedia sensor networks: A survey. IEEE Wireless Communications, №14(6), Pp.32–39.

Received (Надійшла) 30.05.2025
Accepted for publication (Прийнята до друку) 21.05.2025

Відомості про авторів/ About the Authors

Погасій Сергій Сергійович – доктор технічних наук, доцент, професор кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Serhii Pohasii – Doctor of Technical Sciences, Docent, Professor of Cybersecurity Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: spogasiy1978@gmail.com; ORCID Author ID: https://orcid.org/0000-0002-4540-3693;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57217487471.

DEVELOPMENT OF A METHODOLOGY FOR BUILDING A MULTI-CIRCUIT INFORMATION RESOURCE PROTECTION SYSTEM IN CYBER-PHYSICAL SYSTEMS

Serhii Pohasii

Abstract. Relevance of the topic. This paper presents a methodology for constructing a multi-layered information security system for cyber-physical systems (CPS), addressing modern challenges related to hybrid and post-quantum threats. **The purpose.** Concept formation based on five stages: threat probability assessment, preventive modeling, game-theoretical analysis, implementation of post-quantum cryptographic mechanisms (LDPC-based CCS), and multi-contour security architecture development. **Results.** The effectiveness of protection is evaluated using KPI(eff), KPIeffinv, and KPInorm indicators, particularly in the context of mobile wireless technologies (LoRa, Sigfox, LTE-M, NB-CPS). A modification of the Go-Back-N protocol is proposed to enhance functional efficiency in wireless memory channels. **Conclusions.** The proposed models can be applied in the development of secure CPS for critical infrastructure and industrial IoT systems.

Keywords: cyber-physical systems, multi-layered security, post-quantum cryptography, LDPC codes, LPWAN