НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

СТВОРЕННЯ БАГАТОКОНТУРНОЇ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ КІБЕРЗАХИСТУ

КУШНЕРЬОВ О. С.
СОКОЛОВ А. В.
ПІКУЛЬ Р. В.
ДУНАЄВ С. В.

НТУ «ХПІ»

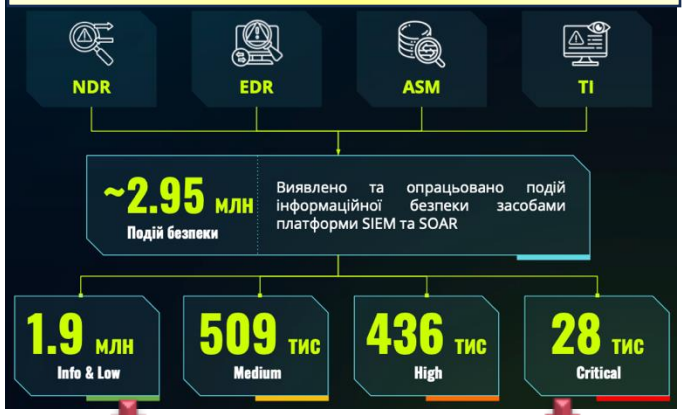
АКТУАЛЬНІСТЬ

МЕТА

КОНКУРЕНТО-СПРОМОЖНІСТЬ

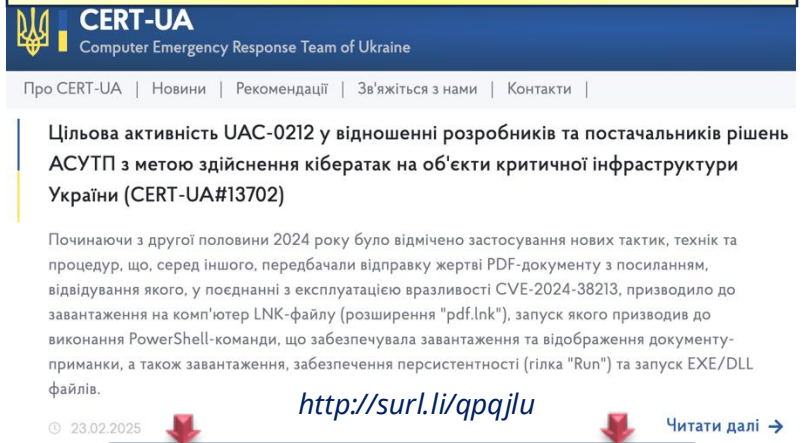
Актуальність теми роботи

ТЕОРІЯ



загрози для національної безпеки і оборони

ПРАКТИКА



наслідки для національної безпеки і оборони

*розробка **багатоконтурної інтелектуальної системи кіберзахисту є необхідним кроком** для підвищення рівня безпеки та адаптивності до сучасних кібератак*

***Мета** –створення багатоконтурної інтелектуальної системи кіберзахисту об'єктів критичної інфраструктури та оцінка її потокового стану захищеності об'єкту.*

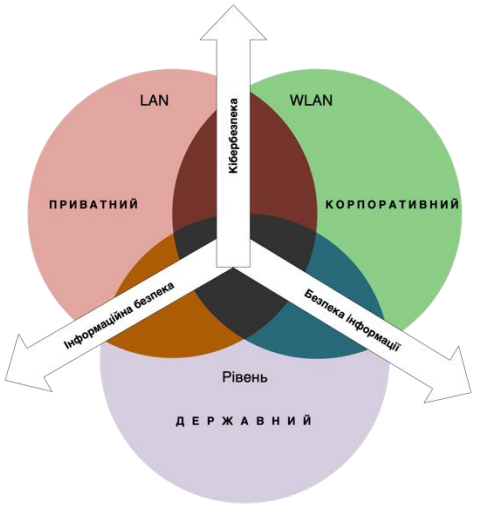
Конкурентоспроможність

4 монографій /з них 1 – за кордоном/	**42 наукові статті** /з них 21 – в журн. категорії А/	**1 патентів України на кор. модель**	**3 авт. свідоцтва на твір**	**27/7 Scopus**	**5/1 Web of Science**	**92/16 Google Scholar**

НТУ «ХПІ»

ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ БАГАТОКОНТУРНИХ СИСТЕМ БЕЗПЕКИ

Теоретичні основи



Багатоконтурність ОКІ

Національна безпека

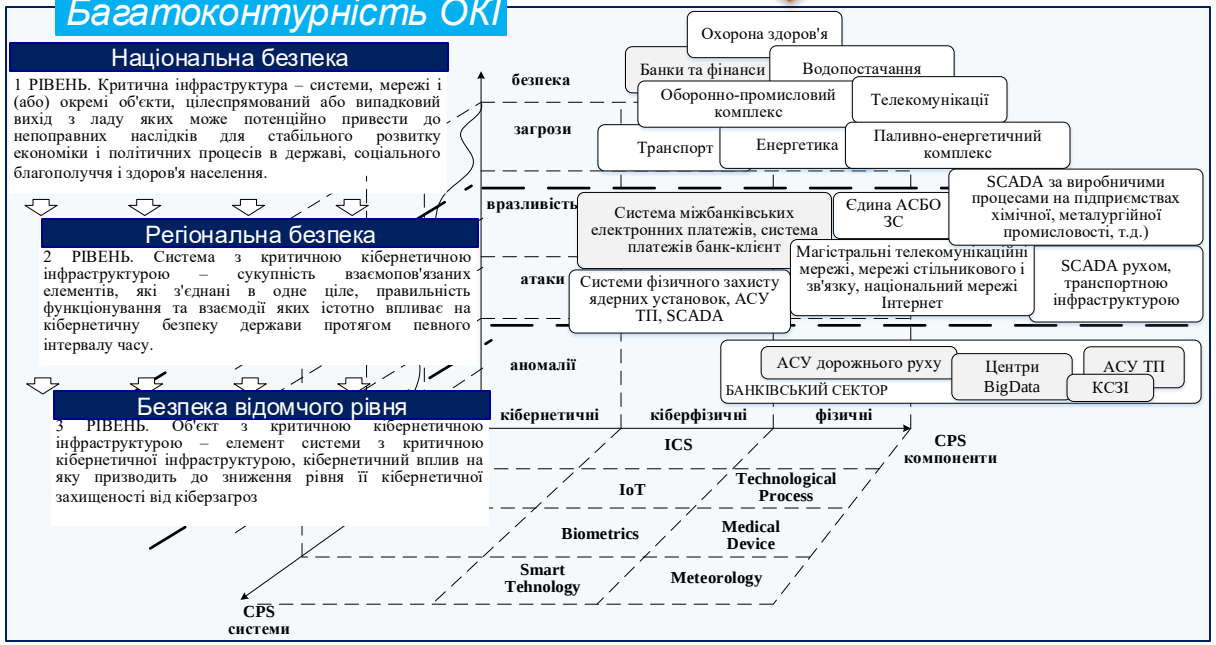
1 РІВЕНЬ. Критична інфраструктура – системи, мережі і (або) окремі об'єкти, цілеспрямований або випадковий вихід з ладу яких може потенційно привести до непоправних наслідків для стабільного розвитку економіки і політичних процесів в державі, соціального благополуччя і здоров'я населення.

Регіональна безпека

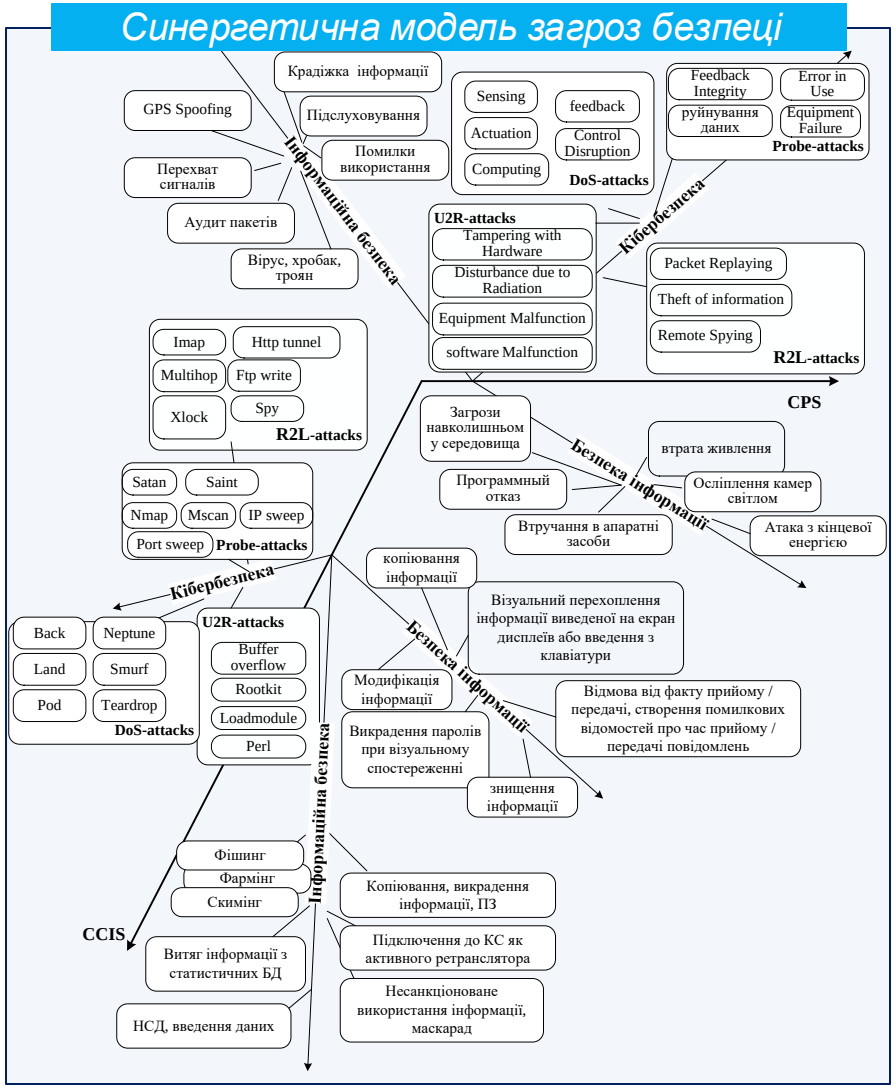
2 РІВЕНЬ. Система з критичною кібернетичною інфраструктурою – сукупність взаємопов'язаних елементів, які з'єднані в одне ціле, правильність функціонування та взаємодії яких істотно впливає на кібернетичну безпеку держави протягом певного інтервалу часу.

Безпека відомчого рівня

3 РІВЕНЬ. Об'єкт з критичною кібернетичною інфраструктурою – елемент системи з критичною кібернетичної інфраструктурою, кібернетичний вплив на яку призводить до зниження рівня її кібернетичної захищеності від кіберзагроз

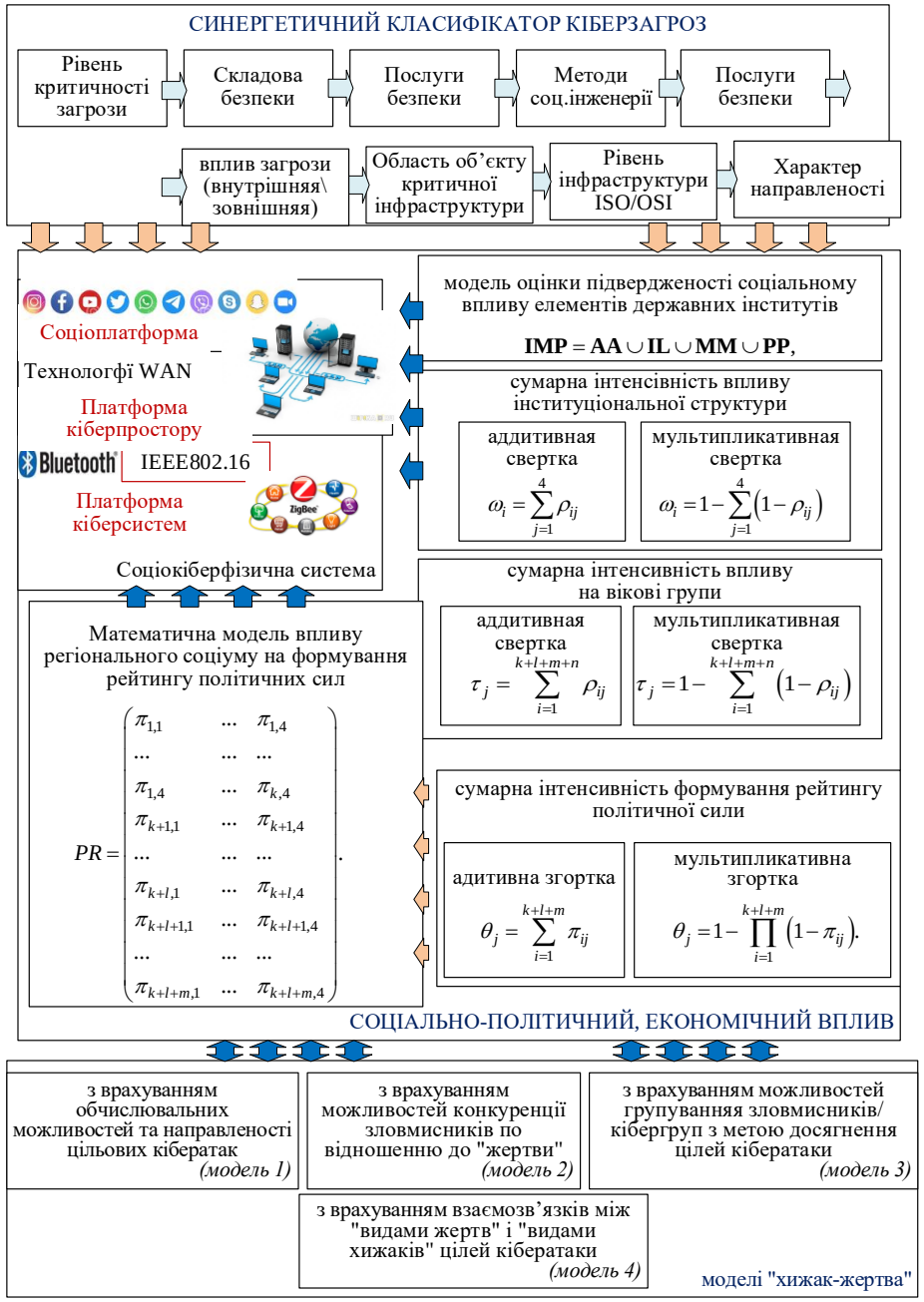


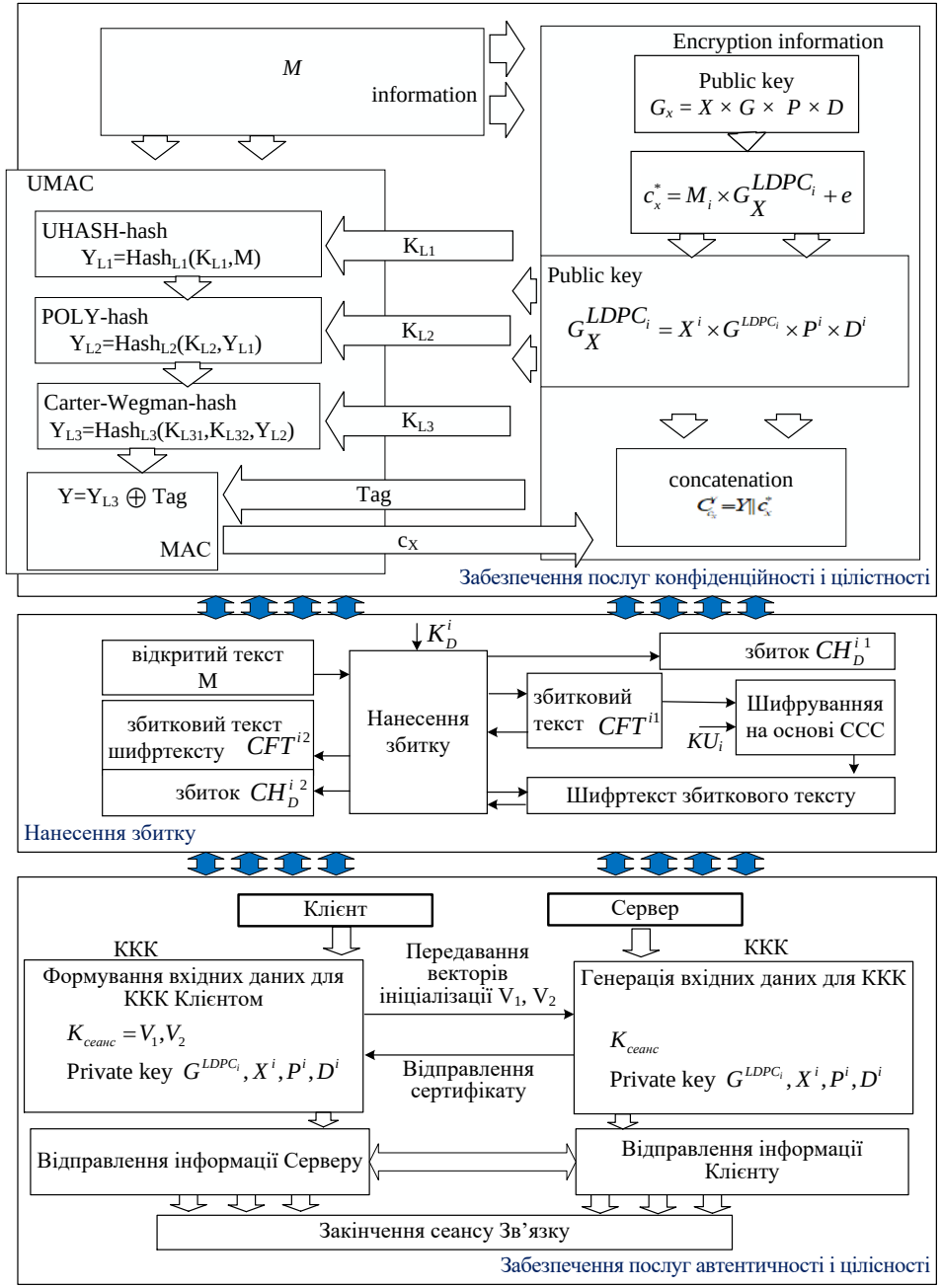
Синергетична модель загроз безпеці



НТУ «ХПІ»

СХЕМА ПОБУДОВИ СИСТЕМИ ОЦІНКИ ПОТОЧНОГО СТАНУ БАГАТОКОНТУРНОЇ СИСТЕМИ ЗАХИСТУ





НТУ «ХПІ»

МАТЕМАТИЧНИЙ ОПИС ФОРМУВАННЯ КОРТЕЖУ ЦІЛЬОВОЇ АТАКИ НА ЕЛЕМЕНТИ ІНФРАСТРУКТУРИ КІБЕРФІЗИЧНИХ СИСТЕМ

$$C^i_{\substack{\text{threat}\\\text{vector}}} = \left\{ L^1_{\substack{\text{criticality}\\\text{of the threat}}}, L^2_{\substack{\text{security}\\\text{component}}}, L^3_{\substack{\text{security}\\\text{service}}}, L^4_{\substack{\text{the nature of}\\\text{the threat's direction}}}, L^5_{\substack{\text{threat impact}\\\text{level}}}, L^6_{\substack{\text{social impact}\\\text{engineering}}}, L^7_{\substack{\text{platform}\\\text{contour}}} \right\},$$

$$L^1_{\substack{\text{criticality}\\\text{of the threat}}} \in \left\{ \begin{array}{l} 01 - \text{критичний}, 02 - \text{високий}, 03 - \text{середній}, \\ 04 - \text{низький}, 05 - \text{занизький} \end{array} \right\};$$

$$L^2_{\substack{\text{security}\\\text{component}}} \in \left\{ \begin{array}{l} 01 - \text{кібербезпека}, 02 - \text{інформаційна безпека}, \\ 03 - \text{безпека інформації} \end{array} \right\};$$

$$L^3_{\substack{\text{security}\\\text{service}}} \in \left\{ \begin{array}{l} 01 - \text{цілісність}, 02 - \text{конфіденційність}, 03 - \text{доступність}, \\ 04 - \text{автентичність}, 05 - \text{приналежність} \end{array} \right\};$$

$$L^4_{\substack{\text{the nature of}\\\text{the threat's direction}}} \in \left\{ \begin{array}{l} 01 - \text{інженерно-технічний}, 02 - \text{організаційний}, \\ 03 - \text{нормативно-правовий} \end{array} \right\};$$

$$L^5_{\substack{\text{threat impact}\\\text{level}}} \in \left\{ \begin{array}{l} 01 - \text{фізичний рівень}, 02 - \text{мережевий рівень}, \\ 03 - \text{рівень ОС}, 04 - \text{рівенб СУБД}, \\ 05 - \text{рівень додатків та сервісів}, 06 - \text{рівень IoT}, \\ 07 - \text{рівень СЗІ} \end{array} \right\};$$

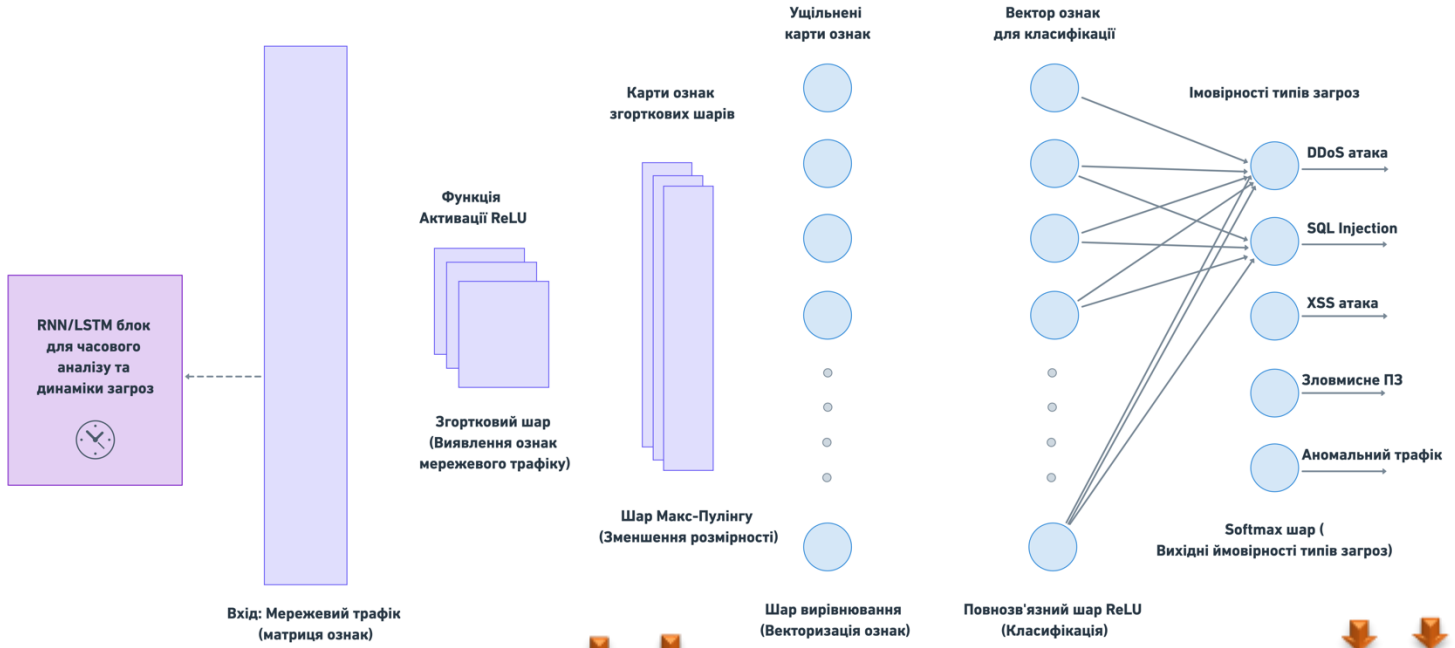
$$L^6_{\substack{\text{social impact}\\\text{engineering}}} \in \left\{ \begin{array}{l} 01 - \text{злам системи}, 02 - \text{компроментація системи}, \\ 03 - \text{компроментація даних}, \\ 04 - \text{находження критичних точок системи}, \\ 05 - \text{збір інформації} \end{array} \right\};$$

$$L^7_{\substack{\text{platform}\\\text{contour}}} \in \left\{ \begin{array}{l} 01 - \text{внутрішній}, 02 - \text{зовнішній}, \\ 03 - \text{внутрішній та зовнішній} \end{array} \right\}.$$

НТУ «ХПІ»

КОНЦЕПЦІЯ НЕЙРОМЕРЕЖ В КОНТУРАХ КІБЕРЗАХИСТУ

Архітектура CNN + RNN/LSTM для зовнішнього контуру



Застосування:

- Виявлення специфічних сигнатур мережевих атак (DDoS, SQL injection, XSS).
- Аналіз у реальному часі потоку пакетів з метою попередження небажаного трафіку.
- Прогнозування розвитку атак (наприклад, багатоступеневі DDoS-атаки).
- Аналіз послідовних логів для виявлення аномальних патернів у часі.
- Виявлення тенденцій у поведінці користувачів та пристроїв (IoT, Smart City), що сигналізують про можливі загрози.

Інтеграція в ЗОВНІШНІЙ КОНТУР:

- **CNN** обробляє та класифікує вхідний трафік за типом атаки,
- **RNN/LSTM** виконує послідовний (часовий) аналіз для прогнозування та виявлення аномалій у динаміці.

Базове RNN-рівняння:

$$h_t = \sigma(W_{xh}x_t + W_{hh}h_{t-1} + b_h)$$

LSTM-комірка (Long Short-Term Memory):

$$\begin{aligned} h_t &= o_t \odot tanh(C_t)o_t \\ &= \sigma(W_o[h_{t-1}, x_t] + b_o), C_t \\ &= f_t \odot C_{t-1} + i_t \odot \widetilde{C}_t, \widetilde{C}_t \\ &= tanh(W_C[h_{t-1}, x_t] + b_C), f_t \\ &= \left(W_f[h_{t-1}, x_t] + b_f\right), i_t \\ &= \sigma(W_i[h_{t-1}, x_t] + b_i), \end{aligned}$$

Операція згортання (Convolution):

$$z_{i,j}^{(k)} = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} x_{i+m,j+n}^{(in)} w_{m,n}^{(k)} + b^{(k)}$$

Функція активації та пулінг (Pooling):

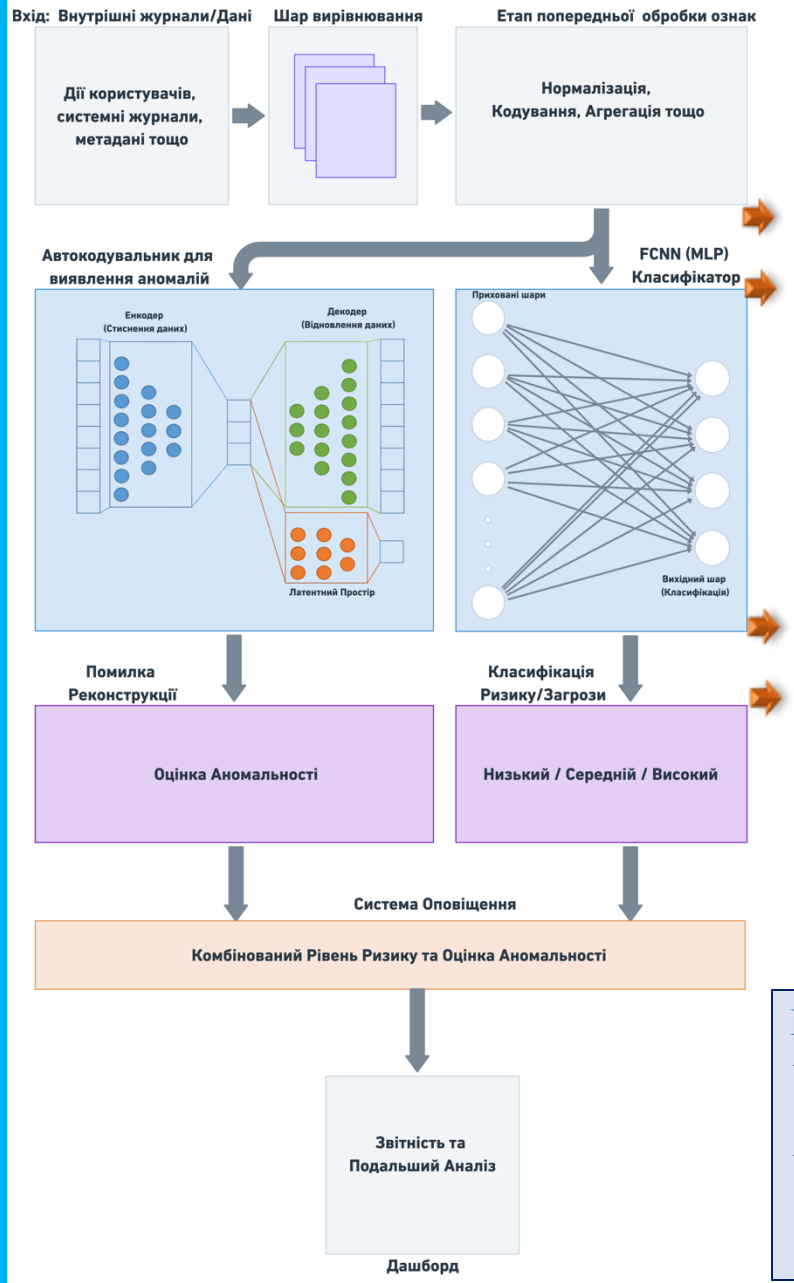
$$a_{i,j}^{(k)} = \sigma\left(z_{i,j}^{(k)}\right), p_{i,j}^{(k)} = pool\left(\{a_{u,v}^{(k)}\}\right)$$

Класифікаційний блок (Fully Connected Layer):

$$\hat{y} = Softmax\left(W_{fc} \cdot Flatten(p) + b_{fc}\right)$$

КОНЦЕПЦІЯ НЕЙРОМЕРЕЖ В КОНТУРАХ КІБЕРЗАХИСТУ

Архітектура FCNN + Autoencoders для внутрішнього контуру



Формалізація MLP:

$$\hat{y} = \sigma\left(W^{(3)}\, h^{(2)} + b^{(3)}\right),$$
$$h^{(2)} = \sigma\left(W^{(2)} h^{(1)} + b^{(2)}\right),$$
$$h^{(1)} = \sigma\left(W^{(1)}\, x + b^{(1)}\right),$$

Функція втрат (Loss Function):

$$\mathcal{L} = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)]$$

Енкодер та декодер:

$$z = \sigma(W_e x + b_e), \hat{x} = \sigma(W_d z + b_d)$$

Функція реконструкції (Reconstruction Loss):

$$\mathcal{L} = \frac{1}{N}\sum_{i=1}^{N}\|x_i - \hat{x}_i\|^2$$

Застосування:

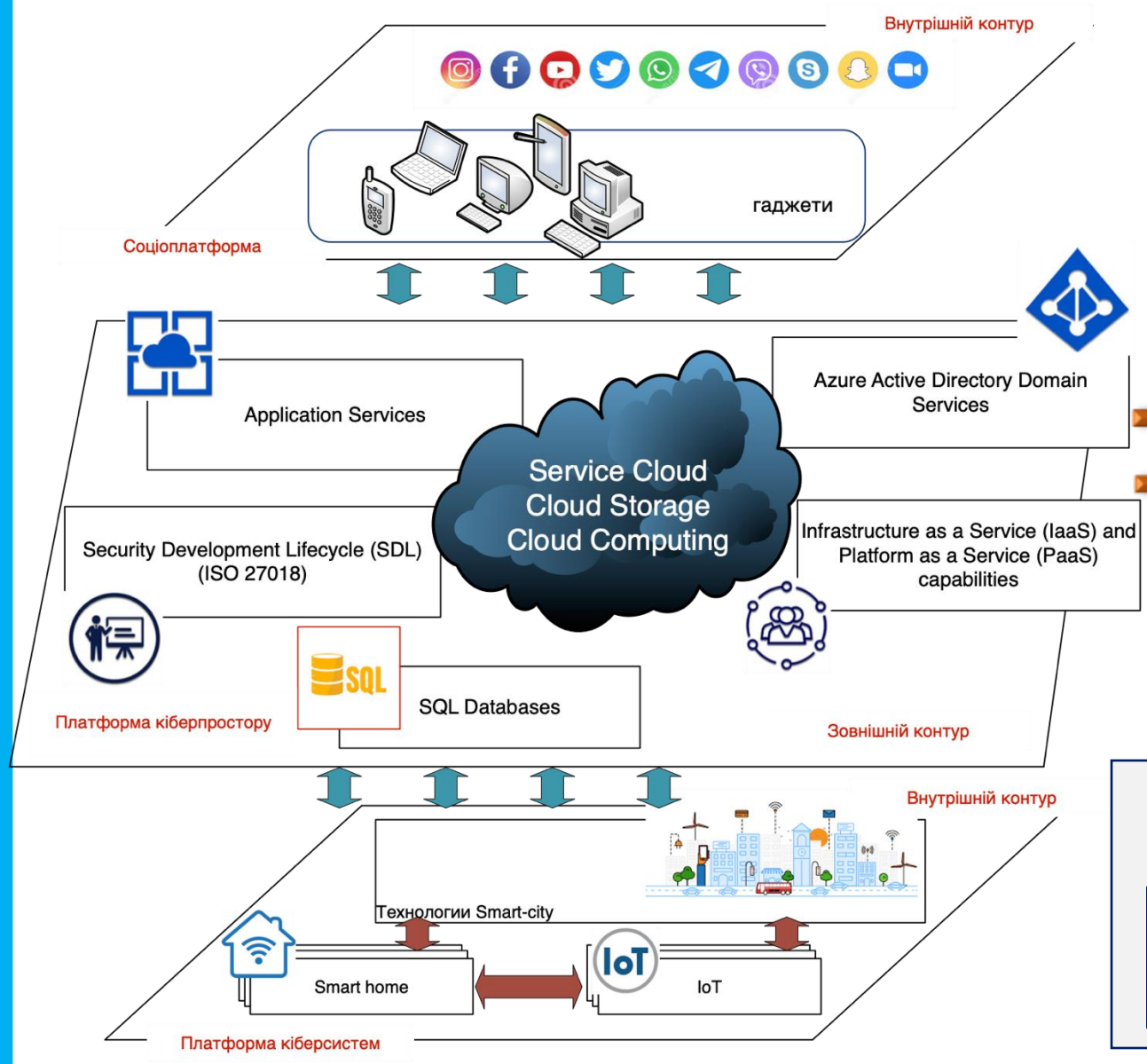
- Визначення рівня критичності (0 – низький, 1 – середній, 2 – високий) внутрішніх інцидентів.
- Пріоритезація подій для оперативної реакції SOC (Security Operation Center).
- Виявлення внутрішніх відхилень від «нормальної» поведінки системи або користувачів.
- Пошук компрометацій даних чи змін у конфігурації, що не відповідають типовим патернам.

Інтеграція у ВНУТРІШНІЙ КОНТУР:

- **FCNN** забезпечує класифікацію та ранжування внутрішніх подій за критичністю.
- **Autoencoder** постійно моніторить системні журнали й виявляє нетипові патерни, що свідчать про можливі латентні загрози.

КОНЦЕПЦІЯ БАГАТОКОНТУРНОЇ СИСТЕМИ БЕЗПЕКИ

КОНЦЕПЦІЯ БАГАТОКОНТУРНИХ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ КІБЕРЗАХИСТУ



Загрози внутрішнього контуру з урахуванням гібридності та синергії

для трьох платформ

соціальні мережі

$$W^{SS\ ISL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{1platform}} = W^{SS\ ISL}_{synerg_{1platform}\ C} \text{ I } W^{SS\ ISL}_{synerg_{1platform}\ I} \text{ I } W^{SS\ ISL}_{synerg_{1platform}\ A} \text{ I } W^{SS\ ISL}_{synerg_{1platform}\ Au} \text{ I } W^{SS\ ISL}_{synerg_{1platform}\ Inv},$$

кіберпростір

$$W^{CS\ ISL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{2platform}} = W^{CS\ ISL}_{synerg_{2platform}\ C} \text{ I } W^{CS\ ISL}_{synerg_{2platform}\ I} \text{ I } W^{CS\ ISL}_{synerg_{2platform}\ A} \text{ I } W^{CS\ ISL}_{synerg_{2platform}\ Au} \text{ I } W^{CS\ ISL}_{synerg_{2platform}\ Inv},$$

кіберфізичні системи

$$W^{CPS\ ISL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{3platform}} = W^{CPS\ ISL}_{synerg_{3platform}\ C} \text{ I } W^{CPS\ ISL}_{synerg_{3platform}\ I} \text{ I } W^{CPS\ ISL}_{synerg_{3platform}\ A} \text{ I } W^{CPS\ ISL}_{synerg_{3platform}\ Au} \text{ I } W^{CPS\ ISL}_{synerg_{3platform}\ Inv},$$

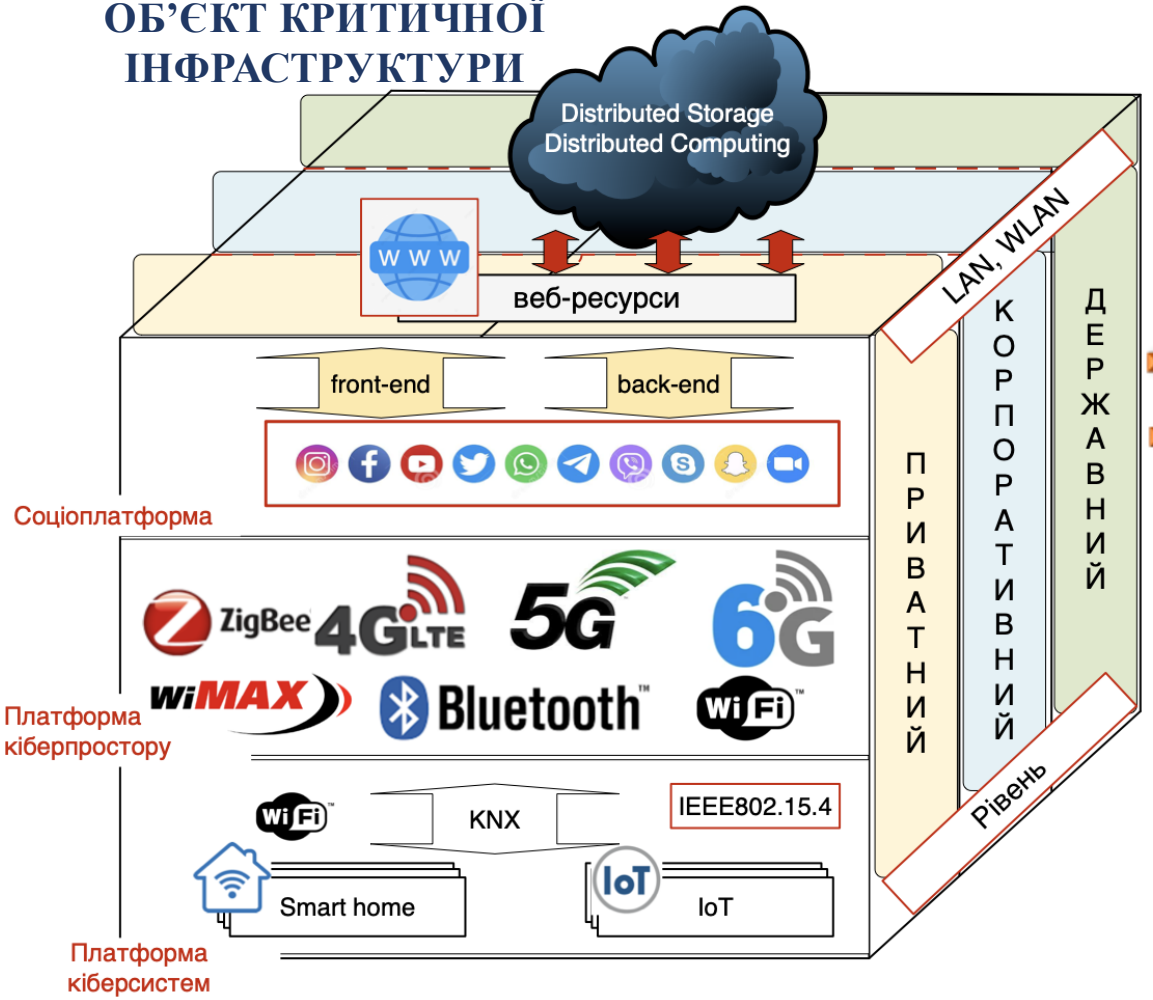
Загальна оцінка загроз внутрішнього контуру

$$W^{CPSS}_{ISL} = W^{SS\ ISL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{1platform}} \text{ U } UW^{CS\ ISL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{2platform}} \text{ U } W^{CPS\ ISL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{3platform}}$$

НТУ «ХПІ»

КОНЦЕПЦІЯ БАГАТОКОНТУРНИХ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ КІБЕРЗАХИСТУ

ОБ'ЄКТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ



Загрози зовнішнього контуру з урахуванням гібридності та синергії
для трьох платформ

соціальні мережі

$$Q^{SCS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg\ 1\text{platform}} = \left(Q^{SCS\ ESL}_{synerg_{1\text{platform}}}\ {}^{C}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right) \mathrm{I}$$

$$\mathrm{I}\left(Q^{SS\ ESL}_{synerg_{1\text{platform}}}\ \mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right)^{I} \mathrm{I}\left(Q^{SCS\ ESL}_{synerg_{1\text{platform}}}\ \mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right)^{I} \mathrm{I}$$

$$\mathrm{I}\left(Q^{SCS\ ESL}_{synerg_{1\text{platform}}}\ {}^{A}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right) \mathrm{I}\left(Q^{SCS\ ESL}_{synerg_{1\text{platform}}}\ {}^{Au}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right) \mathrm{I}$$

$$\mathrm{I}\left(Q^{SCS\ ESL}_{synerg_{1\text{platform}\,\partial}}\ {}^{Inv}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right),$$

кіберпростір

$$Q^{SCS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{2\text{platform}}} = \left(Q^{SCS\ ESL}_{synerg_{2\text{platform}}}\ {}^{C}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right) \mathrm{I}$$

$$\mathrm{I}\left(Q^{SCS\ ESL}_{synerg_{2\text{platform}}}\ {}^{I}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right) \mathrm{I}\left(Q^{SCS\ ESL}_{synerg_{2\text{platform}}}\ {}^{A}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right) \mathrm{I}$$

$$\mathrm{I}\left(Q^{SCS\ ESL}_{synerg_{2\text{platform}}}\ {}^{Au}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right) \mathrm{I}\left(Q^{SCS\ ESL}_{synerg_{2\text{platform}}}\ {}^{Inv}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right),$$

кіберфізичні системи

$$Q^{SCS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{3\text{platform}}} = \left(Q^{SCS\ ESL}_{synerg_{3\text{platform}}}\ {}^{C}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right) \mathrm{I}$$

$$\mathrm{I}\left(Q^{SCS\ ESL}_{synerg_{3\text{platform}}}\ {}^{I}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right) \mathrm{I}\left(Q^{SCS\ ESL}_{synerg_{3\text{platform}}}\ {}^{A}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right) \mathrm{I}$$

$$\mathrm{I}\left(Q^{SCS\ ESL}_{synerg_{3\text{platform}}}\ {}^{Au}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right) \mathrm{I}\left(Q^{SCS\ ESL}_{synerg_{3\text{platform}}}\ {}^{Inv}\mathrm{U}\sum_{i=1}^{5} S_i^{s\text{threats}} \times \alpha_i\right),$$

Загальна оцінка загроз внутрішнього контуру

$$W^{CPSS}_{ESL} = W^{SS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{1\text{platform}}}\ \mathrm{U}$$

$$\mathrm{U}W^{CS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{2\text{platform}}}\ \mathrm{U}W^{CPS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{3\text{platform}}}$$

Загальна оцінка загроз багатоконтурній системі безпеки

$$Q^{CPSS}_{\text{final}} = Q^{CPSS}_{ISL}\ \mathrm{U}\,Q^{CPSS}_{ESL}\ .$$

ОЦІНКА ЗАХИЩЕНОСТІ РІВНЯ БЕЗПЕКИ

МЕТОДИКА ОЦІНКИ ПОТОКОВОГО СТАНУ РІВНЯ БЕЗПЕКИ ОБ'ЄКТА КРИТИЧНОНОЇ ІНФРОСТРУКТУРИ

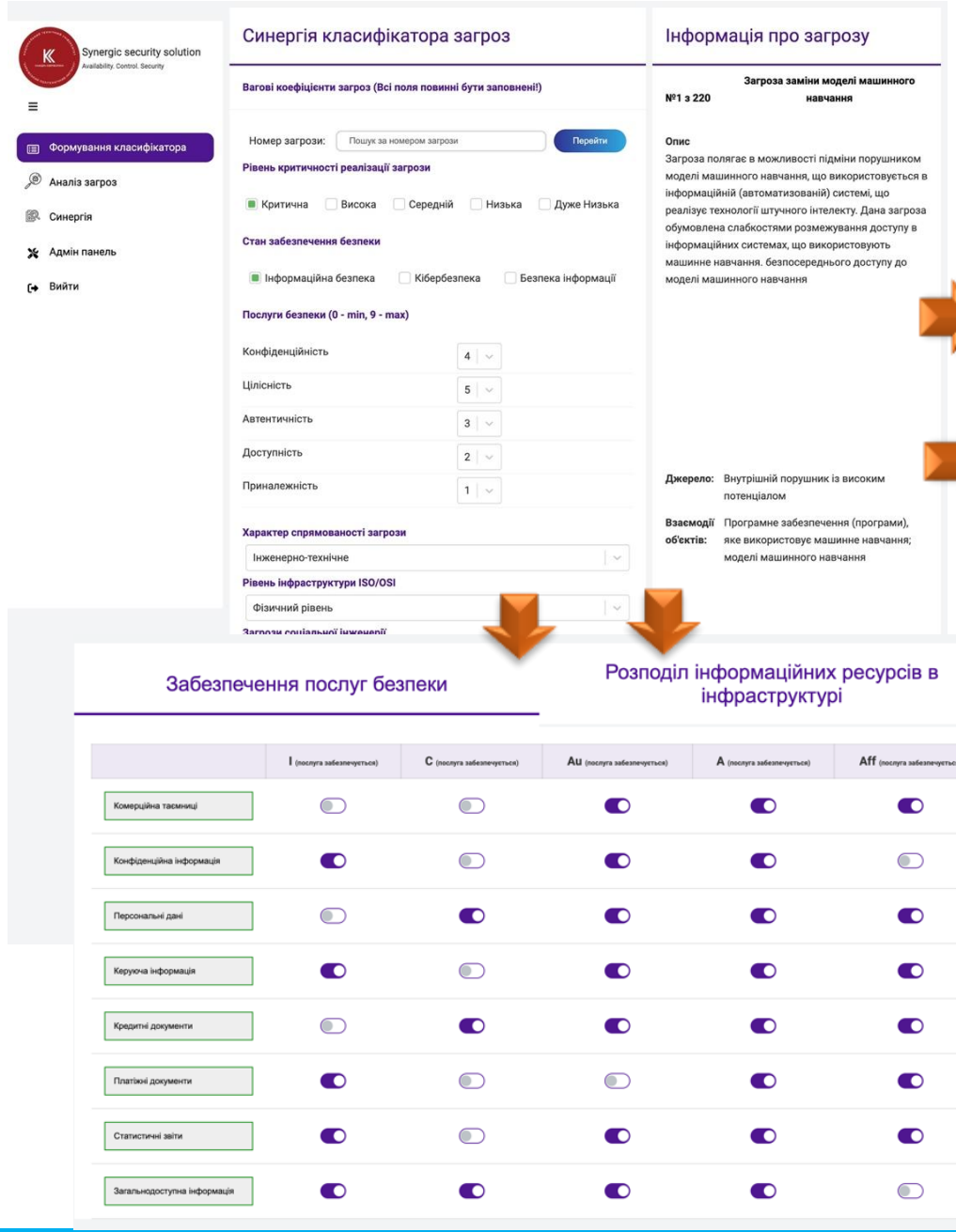
Запропонована багатоконтурна інтелектуальна система кіберзахисту об'єкту охорони забезпечує не тільки об'єктивні оцінку потокового стану захищеності, оцінку можливості систем безпеки протидіяти цільовим атакам, а також забезпечує багатоконтурність захисту інформації на різних платформах, що забезпечує підвищення рівня безпеки об'єкта охорони у цілому.

Розроблений фреймворк оцінки кіберзахищеності об'єктів критичної інфраструктури демонструє високий рівень адаптації до сучасних викликів у сфері кібербезпеки.

На практиці на основі синергетичної моделі загроз безпеці **розроблено веб-застосунок (*https://skl.khpi.edu.ua/*), який дозволяє в автоматизованому режимі одержувати результати експертного оцінювання впливу загрози на послугу безпеки**

Реалізація багатоконтурної інтелектуальної системи кіберзахисту забезпечує можливість автоматизованого моніторингу та оцінки стану кіберзахищеності в режимі реального часу, що сприяє зменшенню часу реакції на інциденти.

ЕТАПИ МЕТОДИКИ ОЦІНКИ ПОТОЧНОГО СТАНУ ЗАХИЩЕНОСТІ



1 крок. Формування експертних оцінок загроз, їх вплив на послуги безпеки, можливість ознак синергізму та гібридності, а також комплексування методів соціальної інженерії. Визначення впливу загрози на рівень інфраструктури (моделі ISO/OSI). При цьому формується матриця вагових коефіцієнтів:

$$S^*_{\text{sthreats}} = \left\| S_{\text{sthreats}\,ij} \right\|,$$

де i – послуги безпеки, j – загроза, $j \in \overline{\forall 1\text{K}\ N}$.

2 крок. Формування матриці відповідності між інформаційними ресурсами та послугами безпеки:

$$S^*_{\text{inf}} = \left\| S_{\text{inf}\,il} \right\|,$$

де l – інформаційний ресурс, $l \in \overline{\forall 1\text{K}\ L}$.

Під час заповнення матриці враховується необхідність надання відповідної послуги безпеки (1 – послуга, 0 – послуга не потрібна).

ЕТАПИ МЕТОДИКИ ОЦІНКИ ПОТОЧНОГО СТАНУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ КІБЕРФІЗИЧНИХ СИСТЕМ

Розподіл інформаційних ресурсів в елементах інфраструктури

	Фізичний рівень	Мережевий рівень	Рівень операційних систем	Рівень систем управління базами даних	Рівень додатків і сервісів	Рівень Інтернету речей	Рівень системи захисту інформації	Інтегральний показник за інформаційними ресурсами
Комерційна таємниці	0.1052	0.1052	0.6707	0.6707	0.0042	0.0042	0.0042	**0.2235**
Конфіденційна інформація	0.0998	0.0998	0.6585	0.6585	0	0	0	**0.2167**
Персональні дані	0.25	0.25	1	1	0.1161	0.1161	0.1161	**0.4069**
Керуюча інформація	0.2495	0.2495	0.9987	0.9987	0.1157	0.1157	0.1157	**0.4062**
Кредитні документи	0.25	0.25	1	1	0.1161	0.1161	0.1161	**0.4069**
Платіжні документи	0.1011	0.1011	0.6616	0.6616	0.0011	0.0011	0.0011	**0.2184**
Статистичні звіти	0.2495	0.2495	0.9987	0.9987	0.1157	0.1157	0.1157	**0.4062**
Загальнодоступна інформація	0.2447	0.2447	0.9878	0.9878	0.112	0.112	0.112	**0.4001**
Інтегральний показник за елементами інфраструктури	**0.1937**	**0.1937**	**0.872**	**0.872**	**0.0726**	**0.0726**	**0.0726**	

Інтегральний показник: **0.3356**

3 крок. Формування залежності між інформаційними ресурсами та рівнями інфраструктури (моделі ISO/OSI), де циркулює та/або зберігається інформація:

$$S^{*}_{\text{ISO}} = \left\| S_{ISO_{kl}} \right\|,$$

де k – наявність та тип зв'язку, елемент інфраструктури (рівень) де зберігається інформація, l – інформаційний ресурс, $l \in \forall 1\text{K}\ L$.

ЕТАПИ МЕТОДИКИ ОЦІНКИ ПОТОЧНОГО СТАНУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ КІБЕРФІЗИЧНИХ СИСТЕМ

Забезпечення послуг безпеки для інформаційних ресурсів

	Комерційна таємниці	Конфіденційна інформація	Персональні дані	Керуюча інформація	Кредитні документи	Платіжні документи	Статистичні звіти	Загальнодоступна інформація	Інтегральний показник за послугами безпеки
Цілісність	0.2664	0.2585	0.4796	0.4788	0.4796	0.2605	0.4788	0.4717	**0.3967**
Конфіденційність	0.0048	0	0.1327	0.1322	0.1327	0.0012	0.1322	0.1279	**0.083**
Доступність	0.6588	0.6461	1	0.9986	1	0.6494	0.9986	0.9873	**0.8674**
Автентичність	0.528	0.5169	0.8265	0.8253	0.8265	0.5197	0.8253	0.8155	**0.7105**
Приналежність	0.3972	0.3877	0.6531	0.6521	0.6531	0.3901	0.6521	0.6436	**0.5536**
Інтегральний показник за інформаційними ресурсами	**0.371**	**0.3618**	**0.6184**	**0.6174**	**0.6184**	**0.3642**	**0.6174**	**0.6092**	

Інтегральний показник: **0.5222**

Забезпечення послуг безпеки в елементах інфраструктури

	Фізичний рівень	Мережевий рівень	Рівень операційних систем	Рівень систем управління базами даних	Рівень додатків і сервісів	Рівень Інтернету речей	Рівень системи захисту інформації	Інтегральний показник за послугами безпеки
Цілісність	0.1691	0.1691	0.5702	0.5702	0.0974	0.0974	0.0974	**0.253**
Конфіденційність	0.043	0.043	0.2837	0.2837	0	0	0	**0.0933**
Доступність	0.3582	0.3582	1	1	0.2436	0.2436	0.2436	**0.4924**
Автентичність	0.2951	0.2951	0.8567	0.8567	0.1948	0.1948	0.1948	**0.4126**
Приналежність	0.2321	0.2321	0.7135	0.7135	0.1461	0.1461	0.1461	**0.3328**
Інтегральний показник за елементами інфраструктури	**0.2195**	**0.2195**	**0.6848**	**0.6848**	**0.1364**	**0.1364**	**0.1364**	

Інтегральний показник: **0.3168**

4 крок. Формування залежності загроз та інформаційних ресурсів (оцінка критичності інфраструктури):

$$S^*_{\text{inf}/\text{sthreats}} = \left\| S_{\text{inf}\ lj} \right\|,$$

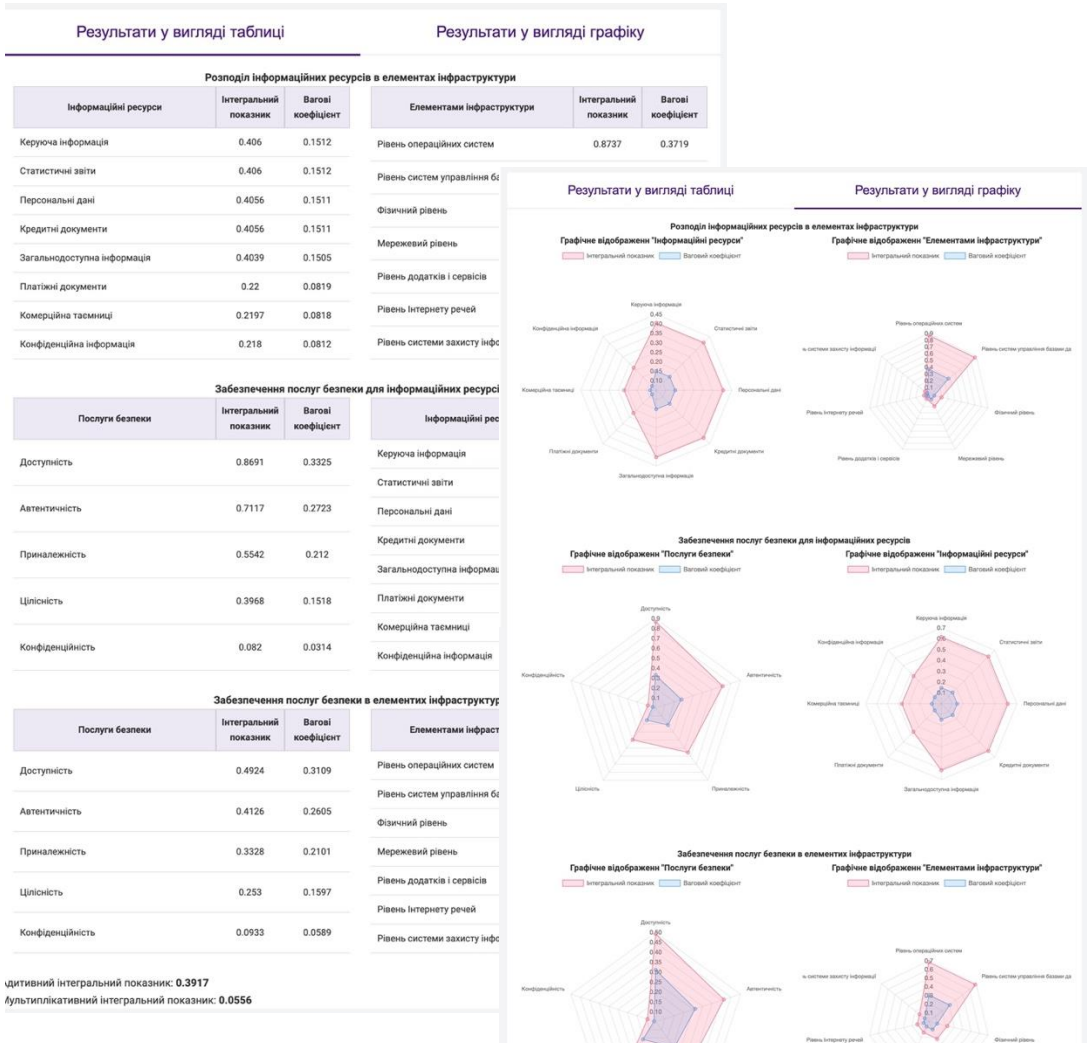
що дозволяє визначити критичність несанкціонованого доступу до того чи іншого інформаційного ресурсу.

5 крок. Формування залежності загроз та елементів інфраструктури (рівень моделі ISO/OSI):

$$S^*_{\text{sthreats}/ISO} = \left\| S_{\text{sthreats}/ISO_{kj}} \right\|,$$

що дозволяє визначити критичні точки в інфраструктурі та заздалегідь визначити превентивні заходи безпеки.

ЕТАПИ МЕТОДИКИ ОЦІНКИ ПОТОЧНОГО СТАНУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ КІБЕРФІЗИЧНИХ СИСТЕМ



6 крок. Формування оцінки захищеності соціокіберфізичної системи на основі аналізу 2 та 3 кроків (знаходження зв'язку між інформаційними ресурсами, елементами інфраструктури (критичними точками несанкціонованого доступу/витоку інформації) та послугами безпеки).

7 крок. Формування оцінки можливостей чинної системи захисту інформації протистояти загрозам:

$$S^{*}_{\text{sthreats/protection system}} = \left\| S_{\text{sthreats/protection system}_{qj}} \right\|,$$

де q – наявність механізму протидії загрозі.

8 крок. Формування оцінки регуляторів та законодавчих актів.

9 крок. Формування оцінки поточного стану системи безпеки. При цьому враховуються результати кроків 7–9.

МЕТОДИКА ОЦІНКИ ПОТОКОВОГО СТАНУ ЗАСОБІВ ЗАХИСТУ

Етап. 1. Формування кортежів кіберзагроз на основі експертної оцінки. Формування матриці метрик кіберзагроз:

$$S^*_{\text{sthreats}} = \left\| S_{\text{sthreats}_{ij}} \right\|,$$ де i – послуги безпеки j – кіберзагрози

Етап. 2. Формування матриці взаємозв'язків інформаційних ресурсів та необхідних послуг безпеки:

$$S^*_{\text{inf}} = \left\| S_{\text{inf}_{il}} \right\|,$$ де l – і нформаційний ресурс

Етап. 3. Формування матриці взаємозв'язків інформаційних ресурсів та елементів інфраструктури:

$$S^*_{\text{ISO}} = \left\| S_{ISO_{kl}} \right\|,$$ де k – наявність та тип звя'зку

Етап. 4. Формування матриці взаємозв'язків інформаційних ресурсів та кіберзагроз:

$$S^*_{\text{inf/sthreats}} = \left\| S_{\text{inf}_{ij}} \right\|,$$

Етап. 5. Формування матриці взаємозв'язків кіберзагроз та елементів інфраструктури:

$$S^*_{\text{sthreats}/ISO} = \left\| S_{\text{sthreats}/ISO_{kj}} \right\|,$$

Етап. 6. Формування оцінки захищеності кіберфізичної системи на основі аналізу етапів 2 та 3. Оцінка взаємозв'язків інформаційних ресурсів, заходи їхньої конфіденційності, необхідності надання послуг безпеки та елементів інфраструктури

Етап. 7. Оцінка наявності спеціального механізму реалізації послуги безпеки та кіберзагрози:

$$S^*_{\text{sthreats/protection system}} = \left\| \Psi^{SCPS}_{\text{safety mechanism}} \right\| \cap \left\| Q_j \right\|.$$

Етап. 8. Оцінка виконання вимог міжнародних регуляторів та законодавчих актів щодо забезпечення необхідного рівня захищеності інформаційних ресурсів

Етап. 9. Оцінка потокового стану рівня захищеності елементів інфраструктури та інформаційних ресурсів:

$$IS_{serv\_abs} = \frac{\sum S_{serv_{il}}}{i \times l},$$

Окремо визначимо етап 7, який дозволяє оцінити можливості спеціальних механізмів забезпечення послуг безпеки автоматизованих систем передачі даних, та соціокіберфізичних систем. Для цього визначимо наступні складові запропонованого алгоритму

1 крок. Оцінка можливих APT-атак на елементи інфраструктури визначимо як

$$S^*_{\text{malefactors/ ISO}} = \left\| S_{ISO\ pl} \right\|,$$ де p – тип зловмисника.

КАТЕГОРІЇ КОРИСТУВАЧІВ СОЦІОКІБЕРФІЗИЧНИХ СИСТЕМ

МЕТОДИКА ОЦІНКИ ПОТОКОВОГО СТАНУ ЗАСОБІВ ЗАХИСТУ

2 крок. Оцінка можливостей зловмисників (фінансові, обчислювальні, людські). Ваговий коефіцієнт «небезпеки» зловмисника визначимо за формулою:

$$p^{SCPS}_{\text{malefactors}} = \frac{1}{N}\sum_{i=1}^{N}\beta^{SCPS}_{p\ i},$$

3 крок. Оцінка ймовірності реалізації APT-атак з урахуванням коефіцієнта «небезпеки» зловмисника визначимо як:

$\|Q_j\| = p^{SCPS}_{\text{malefactors}_j} \times P^{j}_{\alpha}$, де j – загроза, α – ймовірність появи кіберзагрози,

4 крок. Оцінка наявності спеціальних механізмів забезпечення послуг безпеки визначається відповідно

$$\Psi^{SCPS}_{\text{safety mechanism}} = \|F_{ij}\| \times \Psi_i,$$

5 крок. Оцінка превентивних заходів протидії APT-атак визначається:

$$S^{*}_{\text{sthreats/protection system}} = \|\Psi^{SCPS}_{\text{safety mechanism}}\| \text{ I } \|Q_j\|.$$

Вагові коефіцієнти Ψ_i наявності спеціальних механізмів забезпечення послуг безпеки та достовірності системи передачі даних

тип механізму	спеціальні механізми, які забезпечують:															
	виявлення					сигналізацію					блокування					
	рівень стійкості					рівень стійкості					рівень стійкості					
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
IDS	+	+	+	+	+	+	+	+	+	+	–	–	–	–	–	
IPS	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
SIEM	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	

тип механізму (біт)	механізми, які забезпечують послугу:																				
	конфіденційність					цілісність					автентичність					достовірність					
	рівень стійкості					рівень стійкості					рівень стійкості					рівень стійкості					
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
Симетричні блокові шифри (БСШ)																					
БСШ з ключем 128	+	–	–	–	–	+	–	–	–	–	+	–	–	–	–	–	–	–	–	–	
MAC+БСШ з ключем 256	+	+	–	–	–	+	+	–	–	–	+	+	–	–	–	–	–	–	–	–	
БСШ з ключем 256	+	+	+	–	–	+	+	+	–	–	+	+	+	–	–	–	–	–	–	–	
MAC+БСШ з ключем 256	+	+	+	+	–	+	+	+	+	–	+	+	+	+	–	–	–	–	–	–	
БСШ з ключем 256	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–	–	–	–	–	–	
Симетричні поточні шифри (ПСШ)																					
рівномірний рух регістрів	+	+	+	–	–	+	+	+	–	–	+	+	+	–	–	+	+	+	–	–	
нерівномірний рух регістрів	+	+	+	+	–	+	+	+	+	–	+	+	+	+	–	+	+	+	+	–	
несиметричні алгоритми																					
Цифровий підпис (ЦП)	+	+	+	–	–	+	+	+	–	–	+	+	+	–	–	–	–	–	–	–	
на ЕС	+	+	+	+	–	+	+	+	+	–	+	+	+	+	–	–	–	–	–	–	
постквантові алгоритми																					
ЦП	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–	–	–	–	–	
НССС на МЕС	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ССС на МЕС (ЕС)	+	+	+	+	–	+	+	+	+	–	+	+	+	+	+	+	+	+	+	+	
ССС на LDPC	+	+	+	–	–	+	+	+	–	–	+	+	+	–	–	+	+	+	+	+	

ОЦІНКА ПОТОКОВОГО СТАНУ КІБЕРЗАГРОЗ

Оцінка групового показника (OV_{IU_i}) обчислюється з оцінок, що входять до нього часткових показників (OV_{IU_ij}): $OV_{IU_i} = \frac{\sum_j IU_{ij}}{j}$

Оцінка ступеня виконання вимог за напрямом R_{BBi} «поточний рівень ІБ організації» здійснюється за виразом:

$$R_{BBI_1} = \min\left(OV_{БІТП}, OV_{БПТП}, OV_{ooIP}, OV_{ozIP}\right),$$

Оцінка ступеня виконання вимог за напрямом «менеджмент ІБ організації» визначається виразом: $R_{BBI_2} = k_{R_{BBI_2}} \frac{\sum_{j=1}^{m} IU_{1j}}{j}$

Оцінка ступеня виконання вимог за напрямом «рівень усвідомлення ІБ організації» визначається виразом: $R_{BBI_3} = k_{R_{BBI\,3}} \frac{\sum_{j=1}^{m} IU_{2j}}{j}$

Оцінка ступеня виконання вимог, що регламентують обробку БІР визначається виразом: $OV_{ooIP} = k_{ooIP} \frac{\sum_{j=1}^{m} IU_{3j}}{j}$

Оцінка ступеня виконання вимог, що регламентують банківський інформаційний технологічний процес визначається виразом: $R_{OV_{БІТП}} = k_{OV_{БІТП}} \frac{\sum_{j=1}^{m} IU_{4j}}{j}$

Оцінка ступеня виконання вимог, що регламентують банківський платіжний технологічний процес визначається виразом: $OV_{БПТП} = k_{БПТП} \frac{\sum_{j=1}^{m} IU_{5j}}{j}$

Оцінка ступеня захисту БІР з використанням криптографічних ЗЗІ визначається виразом: $OV_{ozIP} = k_{ozIP} \frac{\sum_{j=1}^{m} IU_{6j}}{j}$

j – номер приватного показника, $j = \overline{1, \ldots, m}$.
де $k_{R_{BBI_2}}, k_{R_{BBI_3}}, k_{ooIP}, k_{OV_{БІТП}}, k_{БПТП}, k_{ozIP}$ – коригуючі коефіцієнти

Правила визначення коригувальних коефіцієнтів

коригувальний коефіцієнт	Кількість часткових показників, оцінки яких дорівнюють нулю (Повністю не виконуються)		
$k_{R_{BBI_2}}$	0	1 – 15	більш 15
$k_{R_{BBI_3}}$	0	1 –20	більш 20
k_{ooIP}	0	1 –25	більш 25
$k_{OV_{БІТП}}$	0	1 – 30	більш 30
$k_{БПТП}$	0	1 – 10	більш 10
k_{ozIP}	0	1 – 15	більш 15
Значення коригуючого коефіцієнта	1	0,85	0,7

Узагальнений показник рівня захищеності багатоконтурної інтелектуальної системи кіберзахисту дозволяє оцінити рівень відповідності технічних засобів захисту інформації вимогам регуляторів та визначається:

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i$$

СТЕГАНОГРАФІЧНИЙ МЕТОД З КОДОВИМ УПРАВЛІННЯМ ВБУДОВУВАННЯМ ДЛЯ БАГАТОРІВНЕВИХ КОДОВИХ СЛІВ

Вхідні параметри методу:
μ — розмір блоку,
λ— кількість біт ДІ на один блок,
T_i — застосовуване кодове слово.

$$T_1^+ = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix}, \quad W_1^+ = \begin{bmatrix} 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix};$$

$$T_2^+ = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}, \quad W_2^+ = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix};$$

$$T_3^+ = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}, \quad W_3^+ = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix};$$

$$T_4^+ = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad W_4^+ = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Набір кодових слів порядку $N = 4$, що забезпечують стійкість до атак проти вбудованого повідомлення

Вбудовування ДІ

Крок 1. Розбити стандартним чином $m \times n$ - матрицю контейнера P на $\mu \times \mu$-блоки. Нехай B — довільний блок, що використовується для вбудовування ДІ.

Крок 2. Визначити J — загальна кількість кодових слів;

$$\lambda = \log_2 J$$

— кількість біт ДІ, що вбудовуються в кожний черговий блок контейнера.

Крок 3. Сформувати $m|\mu \times n|\mu$- матрицю ДІ $\bar{D}$, кожний елемент d_{ij} якої визначається λ бітами ДІ, що вбудовуються у відповідний блок B.

Крок 4. Провести кодування $\bar{D}$ шляхом подання кожного d_{ij} за допомогою кодових слів $\{T_i^+\}$ та їх інверсій $\{T_i^-\}$. Результат — $m \times n$ - матриця D.

Крок 5. Вбудувати ДІ в контейнер відповідно до формули: $M = P + D$
де M — матриця стеганоповідомлення.

Декодування ДІ

Крок 1. Побудувати $m \times n$ - матрицю:

$$W = \overline{M} - P$$

де $\overline{M}$ — матриця можливо збуреного стеганоповідомлення.

Розбити W стандартним чином на $\mu \times \mu$ - блоки Δ_r, $r = 1, 2, \ldots, mn$.

Крок 2. Для кожної T_i^+ і кожної Δ_r розрахувати

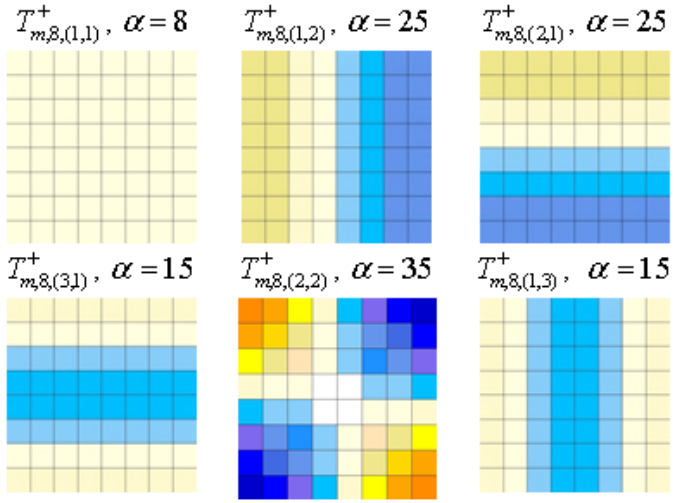
$$\sigma_j = \sum_{l=0}^{\mu-1} \sum_{k=0}^{\mu-1} \Delta_r(l,k) T_i^+(l,k) \quad j = 0,1,\ldots, J/2-1$$

Крок 3. Для кожного Δ_r визначити: $\sigma_{\bar{j}} = \max_j \sigma_j$

при цьому $T_{\bar{j}}^?$ - декодоване кодове слово, знак знайденого максимуму відповідає знаку, з яким $T_{\bar{j}}^?$ було вбудовано (прямий або інверсний вигляд).

СТЕГАНОГРАФІЧНИЙ МЕТОД З КОДОВИМ УПРАВЛІННЯМ ВБУДОВУВАННЯМ ДІ НА ОСНОВІ БАГАТОРІВНЕВИХ КОДОВИХ СЛІВ

Вхідні параметри методу:
μ — розмір блоку,
α — амплітуда впливу,
Ti — застосовуване кодове слово.



Розшифровка кольорів

	1		2		3		4
	5		6		7		8
	−1		−2		−3		−4
	−5		−6		−7		−8

Кодові слова з високою селективністю для μ=16

Вбудовування ДІ

Крок 1. Розбити стандартним чином $m \times n$ - матрицю контейнера P на $\mu \times \mu$ - блоки, що не перетинаються. Нехай B — довільний блок, що використовується для вбудовування ДІ.

Крок 2. Задати цільову трансформанту ДКП (k,l), і значення амплітуди впливу α. Побудувати вектор Z і матрицю $A_{1\mu^2}$, де матриця A_1 розраховується для ДКП відповідно до Твердження 2, V — вектор-рядок, що представляє шукане кодове слово, Z — вектор-рядок, що складається з усіх нулів і значення α на позиції $N \cdot n + m$, що відповідає (n, m) трансформанті ДКП при їх представленні за допомогою двовимірного ДКП.

Крок 3. Розв'язати систему рівнянь $V \cdot A_1 = Z$. Результат — вектор V.

Крок 4. Округлити елементи V до найближчого цілого, записати у вигляді m-кової $\mu \times \mu$ - матриці. Результат — кодові слова $T^{+}_{m,\mu,(k,l)}$, $T^{-}_{m,\mu,(k,l)}$

Крок 5. Вбудувати у блок B черговий біт ДІ p

$$\text{Якщо}: p = 0$$
$$\text{то}: M = B + T^{+}_{m,\mu,(k,l)},$$
$$\text{інакше}: M = B + T^{-}_{m,\mu,(k,l)}.$$

Вилучення ДІ

$$W = \overline{M} - P$$

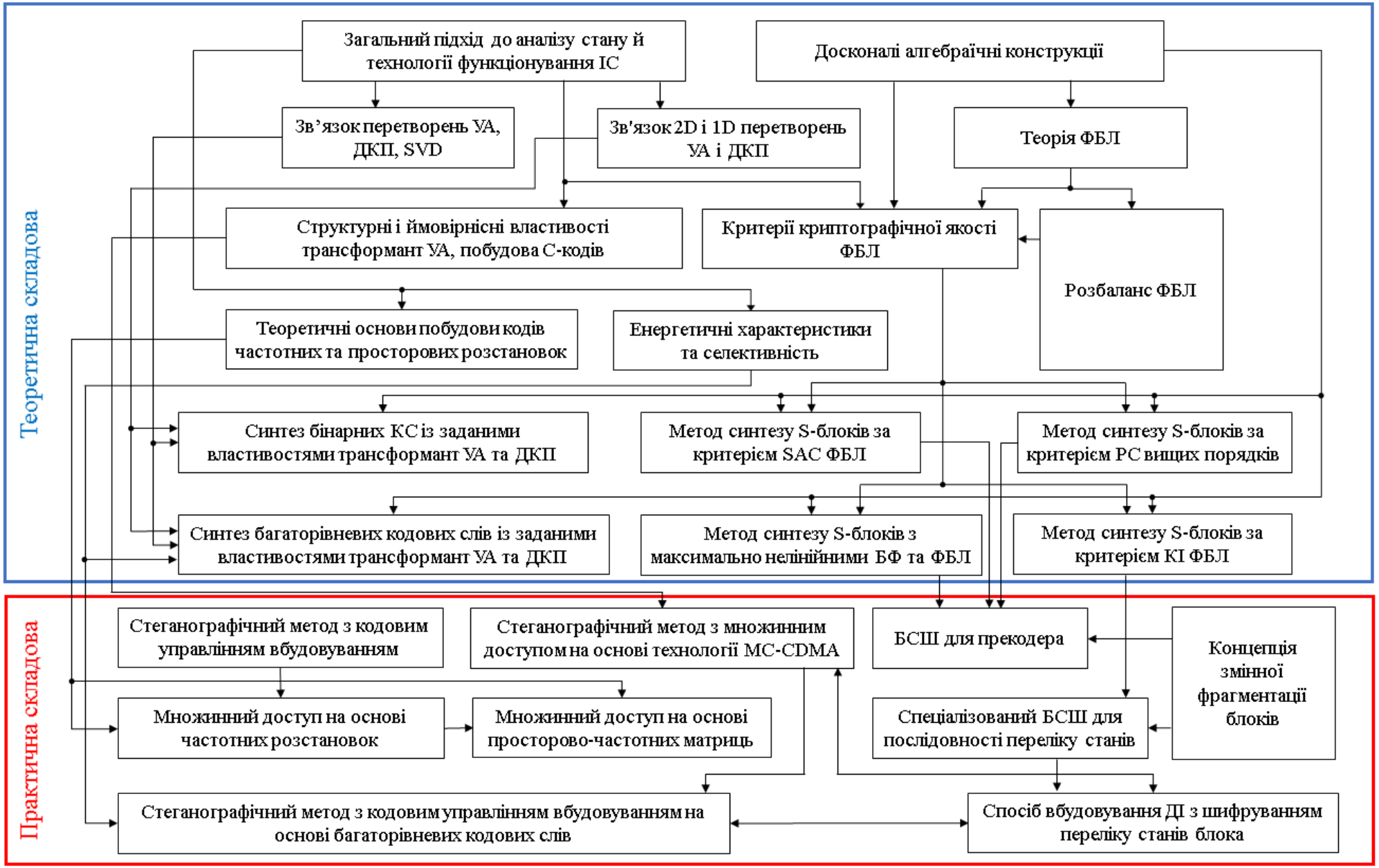
Крок 1. Побудувати $m \times n$- матрицю: де $\overline{M}$ — матриця можливо збуреного стеганоповідомлення.

Розбити W стандартним чином на $\mu \times \mu$ - блоки Δ_r, $r = 0, 1, \ldots, mn-1$.

Крок 2. Для кожного Δ_r вилучити відповідний біт $\bar{p}$ ДІ

$$\overline{p} = sign\left(\sum_{i,j=0}^{\mu-1} \Delta_r(i,j) T^{+}_{m,\mu,(k,l)}(i,j)\right)$$

СТРУКТУРНА СХЕМА РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ ОБ'ЄДНАННЯ КРИПТОГРАФІЧНОЇ ТА СТЕГАНОГРАФІЧНОЇ СКЛАДОВОЇ У КРИПТО-СТЕГАНОГРАФІЧНУ СИСТЕМУ



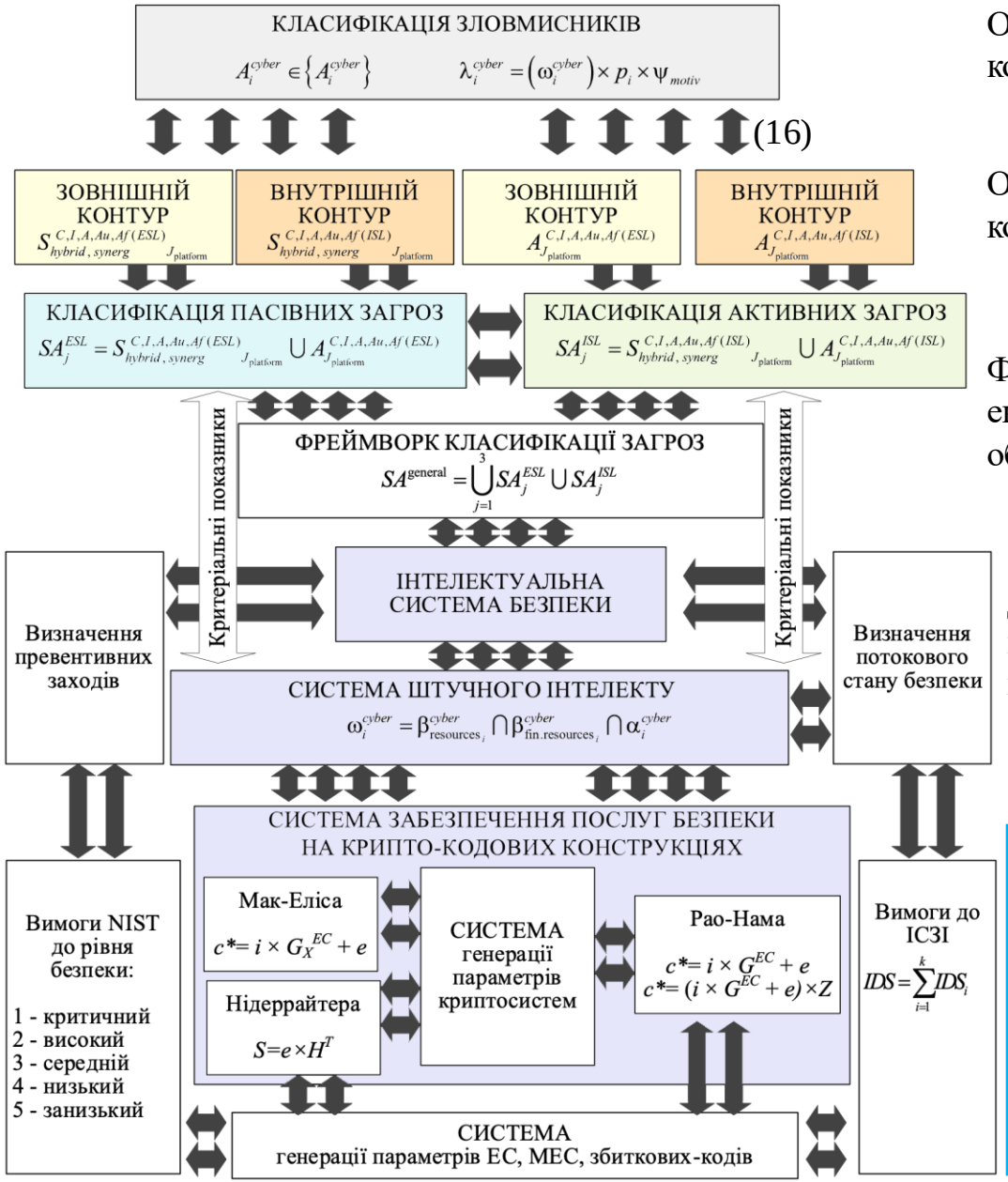
СТРУКТУРНА СХЕМА РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ ОБ'ЄДНАННЯ КРИПТОГРАФІЧНОЇ ТА СТЕГАНОГРАФІЧНОЇ СКЛАДОВОЇ У КРИПТО-СТЕГАНОГРАФІЧНУ СИСТЕМУ

Вперше створено теоретичні основи кодового управління, що включають встановлений взаємозв'язок між трансформантами перетворення Уолша-Адамара, дискретного косинусного перетворення та сингулярного розкладання матриці, достатні умови забезпечення надійності сприйняття та нечутливості стеганоповідомлення до збурень, а також теоретичний базис для синтезу ефективних кодових слів. Розроблено та практично апробовано стеганографічний метод з кодовим управлінням, який перевищує сучасні аналоги за ефективністю, забезпечує надійне приховування додаткової інформації та стабільну роботу в режимі реального часу на ресурсообмежених платформах.

Вперше створено теоретичні засади синтезу багаторівневих кодових слів із селективним впливом на частотні складові контейнера, що дозволило розробити новий стеганографічний метод, який за рівнем стійкості до атак проти вбудованого повідомлення перевищує як відомі аналоги, так і стеганографічний метод з кодовим управлінням на основі бінарних кодових слів.

Вперше запропоновано науково-обґрунтовану методологію розробки крипто-стеганографічної системи, яка забезпечує високу ефективність як криптографічної, так і стеганографічної складової, зокрема на ресурсообмежених платформах, на відміну від існуючих сучасних аналогів.

СТРУКТУРНА СХЕМА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ



Оцінку загальної загрози реалізації загроз внутрішнього контуру визначимо:

$$SA_j^{ESL} = S_{hybrid,\,synerg}^{C,I,A,Au,Af(ESL)}{}_{J_{\text{platform}}} \cup A_{J_{\text{platform}}}^{C,I,A,Au,Af(ESL)},$$

Оцінку загальної загрози реалізації загроз зовнішнього контуру визначимо:

$$SA_j^{ISL} = S_{hybrid,\,synerg}^{C,I,A,Au,Af(ISL)}{}_{J_{\text{platform}}} \cup A_{J_{\text{platform}}}^{C,I,A,Au,Af(ISL)}.$$

Фреймворк класифікації загроз забезпечує узагальнення експертних оцінок загроз з урахуванням їх комплексування та об'єднання:

$$SA^{\text{general}} = \bigcup_{j=1}^{3} SA_j^{ESL} \cup SA_j^{ISL},$$

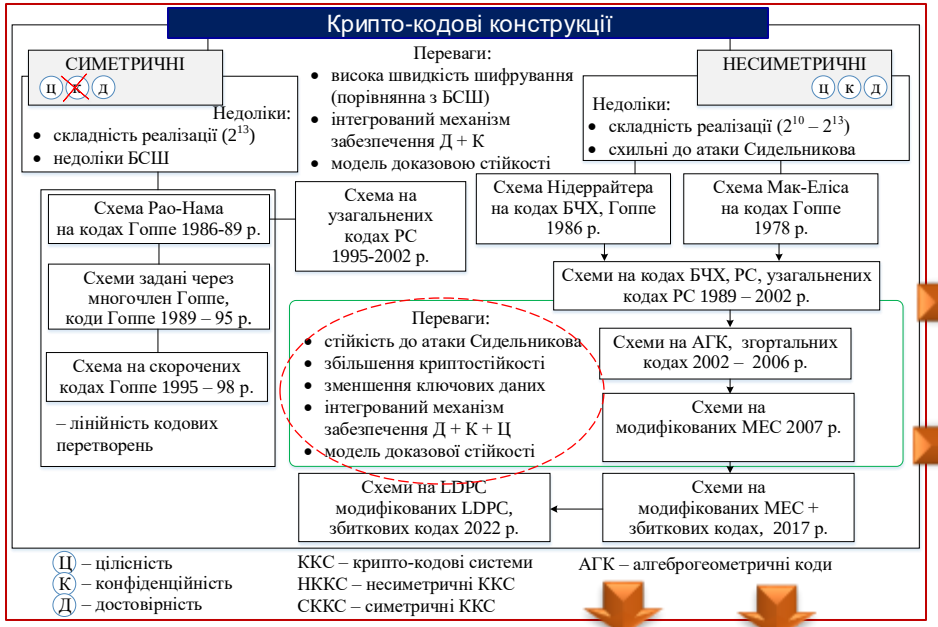
Для врахування рівня захисту, можливостей зловмисника, та ймовірності реалізації визначимо показник «можливостей» порушника:

$$\omega_i^{cyber} = \beta_{\text{resources}_i}^{cyber} \cap \beta_{\text{fin.resources}_i}^{cyber} \cap \alpha_i^{cyber},$$

Такий підхід забезпечує для кожної платформи інфраструктури мережі побудову як зовнішнього контуру захисту, так й внутрішнього, що забезпечує підвищення рівня об'єктивності оцінки загроз, їх комплексування з методами соціальної інженерії, та активними діями терористів.

НТУ «ХПІ»

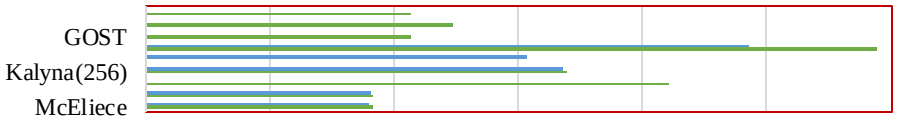
МЕХАНІЗМИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ПОСЛУГ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ



Властивість	Укорочені *MEC*	Подовжені *MEC*
(n, k, d) параметри коду, який побудований через відображення виду $\varphi: X \to P^{k-1}$	$n = 2\sqrt{q} + q + 1 - x$, $k \geq \alpha - x$, $d \geq n - \alpha$, $\alpha = 3 \times degF$, $k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3 \times degF$
n, k, d) параметри коду, який побудований через відображення виду $\varphi: X \to P^{r-1}$	$n = 2\sqrt{q} + q + 1 - x$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$, $k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$

Властивість	Укорочені *MEC*	Подовжені *MEC*
розмірність секретного ключа	$l_{K+} = x \times \lceil \log_2(2\sqrt{q} + q + 1) \rceil$	$l_{K+} = (x - x_1) \times \log_2(2\sqrt{q} + q + 1)$
розмірність інформаційного вектора	$l_I = (\alpha - x) \times m$	$l_I = (\alpha - x + x_1) \times m$
розмірність криптограми	$l_S = (2\sqrt{q} + q + 1 - x) \times m$	$l_S = (2\sqrt{q} + q + 1 - x + x_1) \times m$
відносна швидкість передачі	$R = (\alpha - x) / (2\sqrt{q} + q + 1 - x)$	$R = (\alpha - x + x_1) / (2\sqrt{q} + q + 1 - x + x_1)$

Властивість	Укорочені *LDPC*-коди	Подовжені *LDPC*-коди
(N, k) параметри коду	$N = 2\sqrt{q} + q + 1 - x$, $k < N$	$N = 2\sqrt{q} + q + 1 - x + x_1$, $k < N$
Довжина відкритого тексту	$l_I = l_z^e + l_z^f$	$l_I = 1/2k \times m + l_z^e + l_z^f$
Довжина кодограми (в бітах)	$l_S = (2\sqrt{q} + q + 1 - 1/2k) \times m$;	$l_S = (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times m$.
Довжина відкритого ключа (в бітах)	$l_K = 1/2k \times (2\sqrt{q} + q + 1 - 1/2k$	$l_K = 1/2k \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times m$.
Довжина закритого ключа (в бітах)	$l_{K+} = 1/2k \lceil \log_2(2\sqrt{q} + q + 1) \rceil$	$l_{K+} = (1/2k - 1/2k) \lceil \log_2(2\sqrt{q} + q + 1)$
Складність формування кодограми для систематичного кодування	$O_K = (r+1) \times (2\sqrt{q} + q + 1 - 1/2k) + O\left(\frac{1 - K_C^u}{K_f} \times L\right)$;	$O_K = (r+1) \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) + O\left(\frac{1 - K_C^u}{K_f} \times L\right)$;
Складність формування кодограми для несистематичного кодування	$O_K = O_K = (k+1) \times (k+1) \times (2\sqrt{q} + q + 1 - 1/2k) + O\left(\frac{1 - K_C^u}{K_f} \times L\right)$;	$O_K = (k+1) \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) + O\left(\frac{1 - K_C^u}{K_f} \times L\right)$.
Складність разкодування кодограми	$O_{SK} = 2 \times (2\sqrt{q} + q + 1 - 1/2k)^2 + 1/2k^2 + 4t^2 + (t^2 + t - 2)^2 / 4 + O\left(\frac{\alpha - z \times \log k}{\lvert K_z^c \times L \rvert}\right)$;	$O_{SK} = 2 \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k)^2 + k^2 + 4t^2 + (t^2 + t - 2)^2 / 4 + O\left(\frac{\alpha - z \times \log k}{\lvert K_z^c \times L \rvert}\right)$.
Складність процесу декодування	$O_{K+} = N_{покр} \times (2\sqrt{q} + q + 1 - 1/2k) \times r + N_{F\,або}(N_K)$,	$O_{K+} = N_{покр} \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times r + N_F$ або (N_K).



	McEliece	Niederreiter	Kalyna(128)	Kalyna(256)	Kalyna(512)	AES	GOST	BelT	Kuznyechik
256 bit	357.534	361.239		673.174	614.239	971.725			
128 bit	365.551	366.614	842.061	678.096		1177.95	427.362	495.39	425.908

Оцінка швидкодії криптоперетворень

ВИСНОВКИ

Запропоновано методологію синтезу моделей інтелектуальних систем управління та безпеки об’єктів критичної інфраструктури, що спрямована на підвищення рівня захищеності інформаційних ресурсів та модернізацію існуючих систем захисту інформації.

Розроблено підхід до побудови багатоконтурних систем захисту, що враховує фізичні складові інфраструктури та формує зовнішній і внутрішній контури безпеки.

Удосконалено метод оцінювання рівня безпеки інформаційних ресурсів на основі комплексного показника ефективності інвестицій, що дозволяє оптимізувати витрати на управління та безпеку. Синтезовано методи забезпечення конфіденційності, цілісності та автентичності державних інформаційних ресурсів на гібридних крипто-кодових конструкціях зі збитковими кодами, що підвищує стійкість до атак.

Удосконалено класифікатор загроз для інтелектуальних систем управління та безпеки об’єктів критичної інфраструктури, що забезпечує більш точну ідентифікацію та класифікацію небезпек.

Запропонована методологія синтезу моделей інтелектуальних систем управління та безпеки об’єктів критичної інфраструктури, яка забезпечує об’єктивну оцінку будь-якої інфраструктури об’єктів критичної інфраструктури (будь-якої галузі), підтверджуючи її універсальність.

ВИСНОВКИ

Розроблено методологію синтезу моделей інтелектуальних систем управління та безпеки об’єктів критичної інфраструктури, яка базується на концепції побудови синергетичної моделі загроз.

Встановлено залежність рівня захищеності контуру бізнес-процесів системи безпеки від часу перемикання з захисту одного вектору безпеки до іншого, демонструючи кількісну оцінку впливу цього параметра на ефективність захисту.

Запропоновано ефективний з позицій витрачених коштів на управління та безпеку підхід до модернізації чинних та створення перспективних інтелектуальних систем управління та безпеки об’єктів критичної інфраструктури держави на основі розробленої методології.

Запропоновано застосування гібридних крипто-кодових конструкцій зі збитковими кодами для забезпечення конфіденційності, цілісності та автентичності державних інформаційних ресурсів в інтелектуальних системах управління та безпеки об’єктів критичної інфраструктури.