© Milevskyi S. Development of threat classifier in socio-cyber-physical systems// Ukrainian Scientific Journal of Information Security, 2023, vol. 29, issue 3, pp. 118-123. ©

**DOI: 10.18372/2225-5036.29.18070**

# РОЗРОБКА КЛАСИФІКАТОРА ЗАГРОЗ У СОЦІОКІБЕРФІЗИЧНИХ СИСТЕМАХ

**Станіслав Мілевський**

*Національний технічний університет "Харківський політехнічний інститут"*

**МІЛЕВСЬКИЙ Станіслав Валерійович,** к.е.н.
*Рік та місце народження:* 1979, Муром, Володимирська область.
*Освіта*: Харківський національний економічний університет, 2001.
*Посада*: доцент кафедри кібербезпеки Національний технічний університет "Харківський політехнічний інститут", Україна.
*Наукові інтереси*: захист інформації у соціокіберфізичних системах.
*Публікації*: більше 60 наукових публікацій, включаючи монографії, підручники, статті та патенти.
*E-mail*: milevskiysv@gmail.com.
*Orcid ID*: 0000-0001-5087-7036.

***Анотація***. *У статті подано новий підхід формування класифікатора загроз у соціокіберфізичних системах, які, як правило, відносяться до комплексованих систем на основі синтезу кіберфізичних систем зі смарт-технологіями та соціальними мережами. Крім цього, такі системи відносяться до об'єктів критичної інфраструктури, що потребує нового підходу формування многоконтурних систем безпеки. Запропонований класифікатор дозволяє сформувати експертний підхід на першому етапі для формування вагових коефіцієнтів впливу загроз (аномалій, відхилення від нормальної роботи, комп'ютерних інцидентів). На другому формуються властивості впливу загроз на платформи соціокіберфізичних систем, а також їх вплив на зовнішній та внутрішній контури системи. А також вплив методів соціальної інженерії, що дозволяє зловмисникам значно підвищити рівень ймовірності реалізації загрози, та формувати декілька каналів реалізації загрози – змішані (цільові) атаки. На основі запропонованого підходу класифікації загроз пропонується методика оцінки потокового стану рівня безпеки (захищеності) соціокіберфізичних систем, а також можливості визначити критичні точки інфраструктури системи, можливість протидії та спосібність механізмів многоконтурних систем безпеки забезпечити захист інфраструктури.*

***Ключові слова***: *соціокіберфізичні системи, інформаційна безпека, кібербезпека, безпека інформації, класифікатор загроз інформації соціокіберфізичних систем, многоконтурна система безпеки інформації.*

**Постановка проблеми**

Сучасний розвиток технологій та обчислювальних можливостей створює еволюційний рух до побудови комплексованих систем на основі об'єднання різних технологій, як інтернет, Інтернет-речей, мобільних технологій з соціальними системами та мережами [1–5]. Такі системи формують соціокіберфізичні системи, які дозволяють отримати емерджентні властивості систем на основі по 'єднання mesh-мереж з бездротовими каналами зв'язку та смарт-технологій. При цьому утворюються гібридні системи, які. Як правило, відносяться до об'єктів критичної інфраструктури, та "притягують" зловмисників. Поява децентралізованих систем та мереж на основі блокчейн технології тільки "отягчають" можливість протистояти змішаним (цільовим) атакам на інфраструктуру соціокіберфізичних систем [6-10]. При цьому соціокіберфізичні системи складаються з декілька платформ^ фізичної, де розташовані датчики сенсори, елементи (механізми) керування, управління, яка, як правило розміщена у хмарі, та соціальна – соціальні мережі та месенджери. Актуальним завданням щодо формування контуру безпеки таких систем є створення класифікатору загроз, який дозволяє формувати об'єктивну оцінку критичності елементів інфраструктури організації (компанії, підприємства, то що), враховувати критичність інформаційних ресурсів (рівень секретності). Такий підхід дозволяє розглядати інформаційні ресурси як товар, та формувати відповідні моделі мінімізації як ризиків зламі, так й фінансових втрат. Крім цього, актуальним питанням є своєчасна оцінка потокового стану рівня безпеки (захищеності) контуру безперервних бізнес-процесів, який забезпечує працездатність компанії (організації, підприємства тощо) в цілому.

**Аналіз останніх досліджень і публікацій**

Аналіз оцінки тенденцій розвитку змішаних загроз (цільових атак) показав, що вектор загроз "клонує" попит цифровізації послуг та еволюційний розвиток як обчислювальної техніки, так і тенденцій розвитку технологій. В першу чергу, це стосується появи соціокіберфізичних систем, ї їх спектром цифрових

послуг, появи повномасштабних квантових комп'ютерів – в другу. В роботах [1-5] автори пропонують використовувати різні підходи побудови класифікації загроз, але не враховані можливості розподілу загроз на складові безпеки: кібербезпеку(КБ), інформаційну безпеку (ІБ),безпеку інформації (БІ), їх влив на послуги безпеки: конфіденційність, цілісність, автентичність, доступність та причасність). В роботі [8] автори пропонують синергетичний підхід побудови моделі загроз, але не враховані можливості впливу методів соціальної інженерії, які спроможні значно посилити реалізацію цільової (змішаної) загрози. В роботі [11] автори пропонують загальний підхід універсалізації побудови класифікаторів, але не враховано необхідність побудови многоконтурних систем захисту інформації в умовах функціонування многоплатформених систем до яких відносяться кіберфізичні системи. Таким чином, проведений аналіз показав, що в умовах еволюційного зростання гібридних (комплексованих) систем, які поєднують різні технології актуальним питанням є побудова многоконтурних систем захисту у відповідності до визначених платформ, а також необхідність розгляду впливу загроз як на зовнішній, так й на внутрішній контури безпеки.

**Мета та постановка завдання**

Метою статті є розробка класифікатора загроз соціокіберфізичних систем з урахуванням гібридності та синергізму цільових (змішаних) атак, комплексування з методами соціальної інженерії та побудови многоконтурних систем захисту інформації.

**Виклад основного матеріалу дослідження**

Для побудови класифікатора загроз соціокіберфізичних систем використаємо підхід, який запропонований у [12]. Введемо наступні позначення:

– інформаційні ресурси визначимо, як сукупність множини $I_{A_i} = \{Type_i, A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}, \beta_i\}$, де $Type_i$ – тип інформаційного активу, $Type_i = \{CI_i, PD_i, CD_i, TS_i, StR_i, PubI_i, ContI_i, PI_i\}$, де $CI_i$ – конфіденційна інформація $PD_i$ – платіжні документи, $CD_i$ – кредитні документи, $TS_i$ – комерційна тайна, $StR_i$ – статистичні звіти, $PubI_i$ – загальнодоступна інформація, $ContI_i$ – інформація управління, $PI_i$ – персональні дані;

– послуги безпеки визначимо як множину $A_i = \{A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}\}$, де $A_i^C$ – конфіденційність, $A_i^I$ – цілісність, $A_i^A$ – доступність, $A_i^{Au}$ – автентичність, $A_i^{Inv}$ – приналежність); $\beta_i$ – метрика співвідношення часу та ступеня секретності інформації для активу (критична – 1,0; висока – 0,75; середня – 0,5; низька – 0,25; дуже низька – 0,01).

Для визначення об'єктивності експертної оцінки та автоматизації розроблений веб-застосунок (https://skl.sspu.sumy.ua/login), який дозволяє формувати експертну оцінку впливу загрози на послугу безпеки.

Наведені вагові коефіцієнти компетентності експертів ($k_k$). Такий підхід дозволяє визначити узгодженість димок експертів з різною мірою знань у галузі кібербезпеки та захисту інформації (табл. 1). Крім того запропонований веб-застосунок, враховує всі складові класифікатору загроз (рис. 1).

Таблиця 1

Ваговий коефіцієнт компетентності експертів

| Кваліфікація експертів | Значення вагового коефіцієнта ($k_k$) |
|---|---|
| міжнародний експерт у галузі ІБ, КБ, Б | 1,0 |
| національний експерт у галузі ІБ, КБ, БІ | 0,95 |
| сертифікований міжнародний спеціаліст у галузі ІБ, КБ, БІ | 0,9 |
| повний доктор наук у галузі ІБ, КБ, БІ | 0,9 |
| голова Служби безпеки | 0,85 |
| доктор філософії в галузі ІБ, КБ, БІ | 0,8 |
| співробітник служби безпеки | 0,7 |
| системний адміністратор | 0,6 |
| інженер служби безпеки | 0,5 |
| аспірант зі спеціальності в галузі ІБ, КБ, БІ | 0,4 |

Сумарна оцінка і-ї загрози визначається за кількістю експертів згідно з виразом:

$$x_i = \frac{\sum_{k=1}^{K} x_k \times k_k}{K}, \quad (1)$$

де $x_k$ – оцінка k-го експерта впливу і-ї загрози; $k_k$ – рівень компетентності експерта; K – кількість експертів.

Мірою узгодженості оцінок експертів є дисперсія, яка визначається за виразом:

$$\sigma_x^2 = \frac{1}{K}\sum_{k=1}^{K} k_k \left(x_k - x_i\right)^2. \quad (2)$$

Статистична ймовірність отриманих результатів 1 - $\alpha_i$, складе: $\left[x_i - \Delta, x_i + \Delta\right]$, де величина $x_i$ розподілена за нормальним законом із центром у та дисперсією $\sigma_X^2$. Тоді Δ визначається виразом:

$$\Delta = t\sqrt{\sigma_x^2 / N}, \quad (3)$$

де t – величина за розподілом Стьюдента для K–1 ступенів свободи.

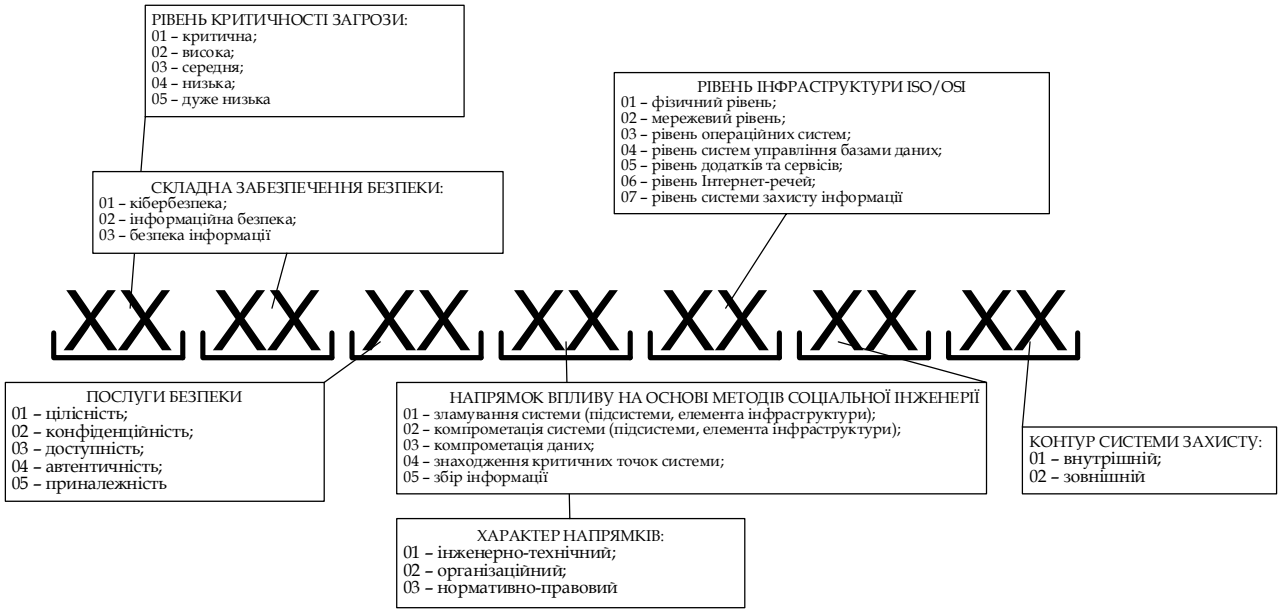


Рис. 1. Класифікатор загроз соціокіберфізичних систем

Класифікатор складається з котеджу який передбачає наступні складові:

– рівень критичності загрози визначається множиною $L_{kr_i} = \left\{L_{kr_1}, L_{kr2}, L_{kr3}, L_{kr4}, L_{kr5}\right\}$, де $L_{kr_1}$ – 01 (критична), $L_{kr2}$ – 02 (висока), $L_{kr3}$ – 03 (середня), $L_{kr4}$ – низька, $L_{kr5}$ – дуже низька;

– складова безпеки визначена множиною $S_i^{syb} = \left\{S_1^{syb}, S_2^{syb}, S_3^{syb}\right\}$, де $S_1^{syb}$ – 01 (кібербезпека), $S_2^{syb}$ – 02 (інформаційна безпека), $S_3^{syb}$ – 03 (безпека інформації);

– складова послуг безпеки визначена множиною $S_i^{serv} = \left\{S_1^{serv}, S_2^{serv}, S_3^{serv} S_4^{serv}, S_5^{serv}\right\}$, де $S_1^{serv}$ – 01 ( $A_i^I$ – цілісність), $S_2^{serv}$ – 02 ( $A_i^C$ – конфіденційність), $S_3^{serv}$ – 03 ( $A_i^A$ – доступність); $S_4^{serv}$ – 04 ( $A_i^{Au}$ – автентичність), $S_5^{serv}$ – 05 ( $A_i^{Inv}$ – приналежність);

– складова характеру напрямків формування систем безпеки визначена множиною $S_i^{\text{influence}} = \left\{S_1^{\text{influence}}, S_2^{\text{influence}}, S_3^{\text{influence}}\right\}$, де $S_1^{\text{influence}}$ – 01 (інженерно-технічний), $S_2^{\text{influence}}$ – 02 (організаційний), $S_3^{\text{influence}}$ – 03 (нормативно-правовий);

– складова рівень інфраструктури ISO/OSI визначена множиною $S_i^{ISO} = \left\{S_1^{ISO}, S_2^{ISO}, S_3^{ISO}, S_4^{ISO}, S_5^{ISO}, S_6^{ISO} S_7^{ISO}\right\}$, де $S_1^{ISO}$ – 01 (фізичний рівень), $S_2^{ISO}$ – 02 (мережевий рівень), $S_3^{ISO}$ – 03 (рівень операційних систем); $S_4^{ISO}$ – 04 (рівень додатків та сервісів), $S_5^{ISO}$ – 05 (рівень додатків та сервісів); $S_6^{ISO}$ – 06 (рівень Інтернет-речей), $S_7^{ISO}$ – (рівень системи захисту інформації);

– складова напрямок впливу на основі методів соціальної інженерії визначена множиною $S_i^{\text{sthreats}} = \left\{S_1^{\text{sthreats}}, S_2^{\text{sthreats}}, S_3^{\text{sthreats}} S_4^{\text{sthreats}}, S_5^{\text{sthreats}}\right\}$, де $S_1^{\text{sthreats}}$ – 01 (зламування системи (підсистеми, елемента інфраструктури), $S_2^{\text{sthreats}}$ – 02 (компрометація системи (підсистеми, елемента інфраструктури), $S_3^{\text{sthreats}}$ – 03 (компрометація даних); $S_4^{\text{sthreats}}$ – 04 (знаходження критичних точок системи), $S_5^{\text{sthreats}}$ – 05 (збір інформації);

– складова контуру безпеки визначена множиною $S_i^{\text{safety loop}} = \left\{S_1^{\text{safety loop}}, S_2^{\text{safety loop}}\right\}$, де $S_1^{\text{safety loop}}$ – 01 (внутрішній контур безпеки), $S_2^{\text{ssafety loop}}$ – 02 (зовнішній контур безпеки).

Таким чином, запропонований класифікатор загроз соціокіберфізичних систем визначається як множина: $Q_j^{\text{sthreats}} = \left\{L_{kr_i}, S_i^{syb}, S_i^{serv}, S_i^{\text{influence}}, S_i^{ISO}, S_i^{\text{sthreats}}, S_i^{\text{safety loop}}\right\}$, де $j$ – відповідна загроза, $j \in \forall\overline{1\ldots N}$.

*Формування многоконтурної системи захисту інформації*

Використаємо математичний апарат побудови многоконтурних систем безпеки в [12]. При цьому враховуємо ознаки синергізму та гібридністю змішаних та цільових атак на кожну з платформ соціокіберфізичних систем (на внутрішній та зовнішній контури).

– загрози внутрішнього контуру з урахуванням гібридності та синергізму загроз для 1 платформи – соціальні мережі:

$$Q^{SCS\ ISL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{1\text{platform}}} = \left(Q^{SCS\ ISL\ \ C}_{synerg_{1\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap$$
$$\cap\left(Q^{SCS\ ISL\ \ I}_{synerg_{1\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ISL\ \ A}_{synerg_{1\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \quad (4)$$
$$\cap\left(Q^{SCS\ ISL\ \ Au}_{synerg_{1\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ISL\ \ Inv}_{synerg_{1\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right),$$

де $Q^{SCS\ ISL\ \ i}_{synerg_{1\text{platform}}}$ – синергія загроз на відповідну послугу безпеки; $a_i$ – ваговий коефіцієнт можливості реалізації загрози на основі методів соціальної інженерії, $i \in \{0{,}25; 0{,}5; 0{,}75; 1{,}0\}$, де 0,25 – ймовірність використання загрози на основі методів соціальної інженерії 1 раз на рік (низький рівень); 0,5 – ймовірність використання загрози на основі методів соціальної інженерії 1 раз на місяць (середній рівень); 0,5 – ймовірність використання загрози на основі методів соціальної інженерії 1 разів на тиждень (високий рівень), 1,0 – ймовірність використання загрози на основі методів соціальної інженерії 1 раз на день (критичний рівень).

– загрози внутрішнього контуру з урахуванням гібридності та синергізму загроз для 2 платформи – кіберпростір:

$$Q^{SCS\ ISL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{2\text{platform}}} = \left(W^{SCS\ ISL\ \ C}_{synerg_{2\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap$$
$$\cap\left(Q^{SCS\ ISL\ \ I}_{synerg_{2\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ISL\ \ A}_{synerg_{2\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \quad (5)$$
$$\cap\left(Q^{SCS\ ISL\ \ Au}_{synerg_{2\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ISL\ \ Inv}_{synerg_{2\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right);$$

– загрози внутрішнього контуру з урахуванням гібридності та синергізму загроз для 3 платформи – кіберфізичні системи:

$$Q^{SCS\ ISL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{3\text{platform}}} = \left(Q^{SCS\ ISL\ \ C}_{synerg_{3\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap$$
$$\cap\left(Q^{SCS\ ISL\ \ I}_{synerg_{3\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ISL\ \ A}_{synerg_{3\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \quad (6)$$
$$\cap\left(Q^{SCS\ ISL\ \ Au}_{synerg_{3\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ISL\ \ Inv}_{synerg_{3\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right).$$

Загальна оцінка загроз на внутрішній контур за всіма платформами складає:

$$Q^{SCS}_{ISL} = W^{SCS\ ISL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{1\text{platform}}} \cup Q^{SCS\ ISL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{2\text{platform}}} \cup$$
$$\cup Q^{SCS\ ISL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{3\text{platform}}}. \quad (7)$$

Загрози на зовнішній контур по кожній з платформ визначаються:

– загрози зовнішнього контуру з урахуванням гібридності та синергізму для 1 платформи – соціальні мережі:

$$Q^{SCS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg\ 1\text{platform}} = \left(Q^{SCS\ ESL\ \ C}_{synerg_{1\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap$$
$$\cap\left(Q^{SS\ ESL}_{synerg_{1\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right)^{I} \cap \left(Q^{SCS\ ESL}_{synerg_{1\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right)^{I} \cap$$
$$\cap\left(Q^{SCS\ ESL\ \ A}_{synerg_{1\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL\ \ Au}_{synerg_{1\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \quad (8)$$
$$\cap\left(Q^{SCS\ ESL\ \ Inv}_{synerg_{1\text{platform}}\ i} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right);$$

– загрози зовнішнього контуру з урахуванням гібридності та синергізму для 2 платформи –кіберпростір:

$$Q^{SCS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{2\text{platform}}} = \left(Q^{SCS\ ESL\ \ C}_{synerg_{2\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap$$
$$\cap\left(Q^{SCS\ ESL\ \ I}_{synerg_{2\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL\ \ A}_{synerg_{2\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \quad (9)$$
$$\cap\left(Q^{SCS\ ESL\ \ Au}_{synerg_{2\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL\ \ Inv}_{synerg_{2\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right);$$

– загрози зовнішнього контуру з урахуванням гібридності та синергізму для 3 платформи – кіберфізичні системи:

$$Q^{SCS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{3\text{platform}}} = \left(Q^{SCS\ ESL\ \ C}_{synerg_{3\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap$$
$$\cap\left(Q^{SCS\ ESL\ \ I}_{synerg_{3\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL\ \ A}_{synerg_{3\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \quad (10)$$
$$\cap\left(Q^{SCS\ ESL\ \ Au}_{synerg_{3\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL\ \ Inv}_{synerg_{3\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right).$$

Загальна оцінка загроз на зовнішній контур за всіма платформами складає:

$$Q^{SCS}_{ESL} = Q^{SCS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{1\text{platform}}} \cup$$
$$\cup Q^{SCS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{2\text{platform}}} \cup Q^{SCS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg_{3\text{platform}}}. \quad (11)$$

Загальна оцінка загроз на многоконтурну систему захисту інформації визначається:

$$Q^{CPSS}_{\text{final}} = Q^{CPSS}_{ISL} \cup Q^{CPSS}_{ESL}. \quad (12)$$

На основі запропонованого підходу щодо оцінки потокового стану захищеності елементів системи (інфраструктури) пропонується наступна методика оцінки захищеності соціокіберфізичних систем:

1 етап. Формування експертних оцінок загроз, їх вплив на послуги безпеки, можливість ознак синергізму та гібридності, а також комплексування з методами 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, $j$ – відповідна загроза, $j \in \forall\overline{1\ldots N}$.

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

$S^*_{\text{inf}} = \left\| S_{\text{inf}_{il}} \right\|$, де $i$ – послуги безпеки, $l$ – інформаційний ресурс, $l \in \forall\overline{1\ldots L}$. При заповнені матриці враховується необхідність надання відповідної послуги безпеки (1 – послуга потрібна, 0 – послуга не потрібна).

3 етап. 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 і тип зв'язку, елемент інфраструктури (рівень) де зберігається інформація, $l$ – інформаційний ресурс, $l \in \forall\overline{1\ldots L}$.

4 етап. Формування залежності загроз та інформаційних ресурсів (оцінка критичності інфраструктури): $S^*_{\text{inf/sthreats}} = \left\| S_{\text{inf}_{lj}} \right\|$, де $l$ – інформаційний ресурс, $l \in \forall\overline{1\ldots L}$, $j$ – відповідна загроза, $j \in \forall\overline{1\ldots N}$. Етап дозволяє визначити критичність несанкціонованого доступу до того чи іншого інформаційного ресурсу

5 етап. Формування залежності загроз та елементів інфраструктури (рівень моделі ISO/OSI): $S^*_{\text{sthreats}/ISO} = \left\| S_{\text{sthreats}/ISO_{kj}} \right\|$, де $k$ – наявність і тип зв'язку, елемент інфраструктури (рівень) де зберігається інформація, $j$ – відповідна загроза, $j \in \forall\overline{1\ldots N}$. Етап дозволяє визначити критичні точки у інфраструктурі та заздалегідь визначити превентивні заходи безпеки.

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

7 етап. Формування оцінки можливостей діючої системи захисту інформації протистояти загрозам: $S^*_{\text{sthreats/protection system}} = \left\| S_{\text{sthreats/protection system}_{qj}} \right\|$, де $q$ – наявність механізму протидії загрозі, $j$ – відповідна загроза, $j \in \forall\overline{1\ldots N}$.

8 етап. Формування оцінки регуляторів та законодавчих актів.

9 етап. Формування оцінки потокового стану системи безпеки. При цьому враховуються результати етапів 7-9.

Таким чином запропонована методика дозволяє враховувати запропоновані критерії класифікатора загроз соціокіберфізичних систем, потоковий стан системи захисту та виконання керівництвом (в першу чергу) вимог міжнародних регуляторів, та законодавчих актів держави.

**Висновки**. Запропонований класифікатор загроз соціокіберфізичних систем дозволяє враховувати ознаки синергізму та гібридності цільових (змішаних) атак, можливість їх комплексування з методами соціальної інженерії. Такий підхід дозволяє формувати вимоги та будувати многоконтурні системи захисту інформації з урахуванням платформеності (структурі) соціокіберфізичних систем.

Також запропонована методика оцінки потокового стану системи безпеки соціокіберфізичних систем дозволяє визначити фінансову складову інформаційних ресурсів при несанкціонованому доступі/втрати, критичні точки інфраструктури та можливості механізмів системи захисту інформації. Крім того оцінка виконання вимог міжнародних регуляторів та законодавчих актів дозволяє отримати об'єктивну оцінки захищеності безперервних бізнес процесів.

**Список літератури**

[1]. IoT Security Maturity Model: Description and Intended Use. URL: http://www.iiconsortium.org/ pdf/ SMM_Description_and_Intended_Use_2018-04-09.pdf.

[2]. IoT Security Maturity Model: Practitioner's Guide. URL: IoT Security Maturity Model: Practitioner's Guide.

[3]. Edited by Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph/S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. Kharkiv: PC TECHNOLOGY CENTER, 2021. 188 p.

[4]. Hryshchuk R. The synergetic approach for providing bank information security: the problem formulation // R. Hryshchuk , S. Yevseiev/Безпека інформації. 2016. № 22 (1). С. 64-74.

[5]. Грищук Р.В. Основи кібернетичної безпеки: Монографія/Р.В. Грищук, Ю.Г. Даник; за заг. ред. Ю.Г. Данника. Житомир: ЖНАЕУ, 2016. 636 с.

[6]. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. Kharkiv: PC TECHNOLOGY CENTER, 2022. 196 p.

[7]. Serhii Yevseiev, Oleksandr Milov, Ivan Opirskyy, Olha Dunaievska, Oleksandr Huk, Volodymyr Pogorelov, Kyrylo Bondarenko, Nataliia Zviertseva, Yevgen Melenti, Bogdan Tomashevsky. Development of concepts for the cyber security metrics classification. Eastern-European Journal of Enterprise Technologies. 4/4 (118). 2022. pp. 6-18.

[8]. S. Pohasii and other. Development of conception for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies. 2021. 3/9 (111). pp. 63-83.

[9]. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. Kharkiv: PC TECHNOLOGY CENTER, 2023. 168 p.

[10]. O. Shmatko, S. Balakireva, A. Vlasov, N. Zagorodna, O. Korol, O. Milov, O. Petrov, S. Pohasii, Kh. Rzayev, V. Khvostenko. Development of methodological foundations for a classifier of threats to cyberphysical systems design. Eastern-European Journal of Enterprise Technologies. 3/9 (105), 2020, pp. 6-19

[11]. Serhii Yevseiev, Pierre Murr, Stanislav Milevskyi, Olha Korol, Marharyta Melnyk. Development of a Sociocyberphysical Systems Cyber Threats Classifier. 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT).

**УДК 336.71:004.056**

***Milevskyi S. Development of threat classifier in socio-cyber-physical systems***

***Abstract***. *The article presents a new approach to forming a classifier of threats in socio-cyber-physical systems, which, as a rule, refer to complex systems based on the synthesis of cyber-physical systems with smart technologies and social networks. In addition, such systems belong to objects of critical infrastructure, which requires a new approach to the formation of multi-contour security systems. The proposed classifier allows for the formation of an expert approach at the first stage for the formation of weighting factors for the impact of threats (anomalies, deviations from normal operation, computer incidents). On the second stage, the properties of the influence of threats on the platforms of socio-cyber-physical systems, as well as their influence on the external and internal contours of the system, are formed. And also, the influence of social engineering methods, which allows criminals to significantly increase the level of threat implementation probability, and to form several channels of threat implementation – mixed (targeted) attacks. Based on the proposed threat classification approach, a technique for assessing the actual state of the security (protection) level of socio-cyber-physical systems is proposed, as well as the ability to determine the critical points of the system infrastructure, the possibility of countermeasures, and the ability of the mechanisms of multi-loop security systems to ensure infrastructure protection.*

***Keywords****: socio-cyber-physical systems, information security, cyber security, security of information, information threat classifier of socio-cyber-physical systems, multi-contour information security system.*

**Мілевський Станіслав Валерійович**, кандидат економічних наук, доцент кафедри кібербезпеки Національний технічний університет "Харківський політехнічний інститут", Україна.

**Stanislav Milevsky**, Ph.D., Associate Professor, Department of Cybersecurity, National Technical University "Kharkiv Polytechnic Institute," Ukraine.

Отримано *23 вересня 2023 року*, затверджено редколегією *30 жовтня 2023 року*