ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

DOI: 10.18372/2225-5036.28.16951

МОДЕЛІ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В КІБЕРФІЗІЧНИХ СИСТЕМАХ

Сергій Погасій

Національний технічний університет "Харківський політехнічний інститут", Україна

ПОГАСІЙ Сергій Сергійович, кандидат економічних наук, доцент кафедри кібербезпеки та інформаційних технологій
Рік та місце народження: 1978, Харків, Харківська область, Україна.
Освіта: Харківський національний економічний університет, 1999.
Посада: доцент кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут", Україна
Наукові інтереси: захист інформації у кіберфізичних системах.
Публікації: більше 32 наукових публікацій, включаючи монографії, підручники, статті та патенти.
E-mail: spogasiy1978@gmail.com.
ORCID ID: 0000-0002-4540-3693.

Анотація. *У статті подано новий підхід забезпечення безпеки інформаційних ресурсів в кіберфізичних системах. Сьогодні таки системи, як правило належать до об'єктів критичної інфраструктури. Як правило таки системи формуються внаслідок комплексування різних елементів технологій мобільного зв'язку, класичних комп'ютерних мереж та систем, а також Інтернет-речей та Інтернет-технологій. В роботі пропонується розгляд формування системи безпеки на основі багатоконтурності, що дозволяє розглядати два контури системи безпеки – внутрішній (фізична інфраструктура кіберфізичних систем) та зовнішній (інфраструктура управляючої системи на основі хмарних технологій). За допомогою розробленого класифікатора загроз на об'єкти критичної інфраструктури забезпечується формування класифікатора зловмисників, у якому визначаються його фінансові та обчислювальні можливості, що дозволяє на основі аналізу загроз своєчасно визначати степені можливості зловмисників, а також його наміри та формувати превентивні заходи захисту. Використання запропонованих моделей захисту на основі моделі Лотки-Вольтери дозволяє враховувати тенденції розвитку сучасних технологій, а також вектор направленості кіберзагроз на об'єкти кричної інфраструктури до яких відносяться сучасні кіберфізичні системи. Для забезпечення безпеки передачі інформації відкритими каналами мережі кіберфізичних систем запропоновані методи захисту інформації на основі постквантових алгоритмів – крипто-кодових конструкцій Мак-Еліса на LDPC-кодах, що дозволяє "закрити" канали передачі даних інфраструктури кіберфізичних систем.*

Ключові слова: *кіберфізичні системи, інформаційна безпека, кібербезпека, безпека інформації, моделі безпеки Лотки-Вольтери, класифікатор загроз інформації кіберфізичних систем, система забезпечення захисту інформації.*

Постановка проблеми

Створення великих систем критичної інфраструктури, інтенсифікація досліджень динаміки кіберфізичних систем потребують постійного вдосконалення та оновлення чинного апарату моделювання та управління динамічними системами [1–5]. Останнім часом відбулося зміщення центру тяжкості досліджень у напрямку розробки методології динамічних систем із параметрами, що змінюються. Використання методів аналізу подібних систем дозволяє різко розширити коло розв'язуваних завдань.

Сучасні вимоги практики до дослідження складних кіберфізичних систем призвели до появи нового класу систем, що розвиваються [1–3]. Ці системи характеризуються тимчасовою залежністю їх структури, зміною у процесі розвитку набору вхідних та вихідних параметрів системи, значним рівнем апріорної невизначеності про закономірності функціонування системи. В цей час відсутнє задовільне розв'язання проблем моделювання кіберфізичних систем, що розвиваються, на основі причинно-наслідкової інформації за даними періодично спостерігаються процеси розвитку. Принципові проблеми структурного синтезу моделі зазвичай замінюються припущеннями про закономірності еволюції системи з наступним зведенням завдання до параметричної невизначеності у межах класичної теорії динамічних систем. На початкових стадіях дослідження знаходяться завдання прийняття рішень у кіберфізичних системах (КФС), що розвиваються, коли цільові установки визначаються фахівцем за допомогою розпливчастих інструкцій. Розвиток кіберфізичних систем останніми роками істотно змінило інфраструктури сучасних як інформаційно-кібернетичних систем (ІКС), а й критичних інфраструктур (КІ), і навіть систем Інтернет-речей (ІР). Синтез даних інфраструктур дозволяє значно розширити цифровий спектр послуг, з одного боку, але також підвищує рівень кіберзагроз [6–9]. У

той самий час стрімке зростання обчислювальних технологій дозволяє зловмисникам формувати цільові, гібридні атаки, які дозволяють отримувати синергетичний ефект [6, 8, 9]. У таких умовах невіддільна (частина/ознака) частиною систем безпеки є можливість як своєчасного реагування на інциденти на елементи інфраструктури, а й правильне формування. Важливим завданням є своєчасний і правильний розподіл обмежених безпекових ресурсів в умовах постійної зміни вектора кібератак. Для своєчасної зміни структури захисних ресурсів, оцінки необхідного та поточного положення системи безпеки потрібне використання моделей безпеки. Такий підхід дозволяє суттєво знизити витрати на відновлення інфраструктури мережі, своєчасно вживати превентивних заходів із необхідними витратами на механізми безпеки. Крім цього, створення на основі комплексування загроз на елементи фізичної інфраструктури кіберфізичних систем та елементи системи управління, яка створюється на основі хмарних технологій вимагає створенню багатоконтурної системи безпеки. А поява повномасштабного квантового комп'ютеру вимагає для забезпечення безпеки інформаційних ресурсів, як во внутрішньому, так й зовнішньому контурах системи безпеки використання постквантових алгоритмів щодо надання послуг безпеки та підтримки належного рівня безпеки.

Аналіз останніх досліджень

Аналіз оцінки глобальних тенденцій кіберзагроз показав, що сьогодні немає можливості забезпечити безпеку у повному обсязі. Так, у роботах [3, 4] наводиться аналіз кіберзагроз за 2017–2019 роки. Поданий аналіз свідчить, що вектор кіберзагроз змінюється з тенденціями розвитку цифрових послуг, Інтернет-речей та криптовалют на основі технології блокчейн. У роботі [5] представлено 10 головних трендів у сфері кібербезпеки у 2021 році, що підтверджує тенденції кібератак в умовах пандемії, – в першу чергу на біржі криптовалют, по-друге – на приватні VPN-канали (у зв'язку з віддаленою роботою), та у третю – на основі методів соціальної інженерії – фішингових листів у форматі pdf у рамках корпоративної пошти. У роботі [6] розглянуто методологічні аспекти побудови системи безпеки на основі крипто-кодових конструкцій, їх застосування у різних об'єктах критичної інфраструктури, а також можливості протистояти сучасним загрозам. [8] пропонується використовувати динамічні моделі на основі методів теорії диференціальних ігор і диференціальних перетворень, при цьому забезпечується оцінка поточного стану системи в офлайн режимі. Однак такі методи вимагають значних обчислювальних ресурсів, що суттєво знижує можливість їхньої практичної реалізації. У роботі [9] автори розглядають використання динамічних моделей у різних системах інформаційного простору. Однак у моделях не враховується можливість нарощування обчислювальних можливостей зловмисників, їх об'єднання у групи з метою досягнення цілей атаки. У роботі [10] автори розглядають економічні аспекти, які можуть впливати на побудову не лише моделі безпеки, а й практичної її реалізації у СЗІ транспортної системи. Проте автори не враховують комплексування загроз, їх синергізм та гібридність, що дозволяє з методами соціальної інженерії формувати цільові (комплексовані) загрози.

Виклад основного матеріалу дослідження.

Проведений аналіз загроз [11–17] показав, що кіберфізичні системи перетинаються з об'єктами критичної інфраструктури. При цьому кіберфізичні системи (Cyber-Physical System, CPS) – це системи, що складаються з різних природних об'єктів, штучних підсистем і контролерів, що керують, та дозволяють уявити таку освіту як єдине ціле. У CPS забезпечується тісний зв'язок та координація між обчислювальними та фізичними ресурсами. Комп'ютери здійснюють моніторинг та управління фізичними процесами з використанням такої петлі зворотного зв'язку, де те, що відбувається у фізичних системах, впливає на обчислення і навпаки [11, 13, 14]. Крім цього, умовах появи повномасштабного квантового комп'ютера ставиться під сумнів стійкість практично всіх алгоритмів симетричної та несиметричної криптографії, а бурхливе зростання обчислювальних ресурсів IT та технологій "G" сприяє збільшенню зростання цільових атак на інформаційно-комунікаційні (ICS) та кіберфізичні системи (CPS), які є ядром сучасних інформаційно-критичних кібернетичних систем. Напрямок смарт- технологія та технологій "Розумний дім" використовують як правило механізми безпеки без попереднього комплексного підходу у наданні послуг безпеки. В основному інтегруються механізми комп'ютерних систем та технологій з технологіями бездротових мереж, що не дозволяє формувати системи захисту інформації з необхідним рівнем безпеки. У роботах [18–25] розглянуто основні підходи забезпечення безпеки у кіберфізичних системах та смарт-технологій. Як правило, використовується стандарт KNX (ISO/IEC 14543), який забезпечує послуги безпеки – конфіденційність та цілісність даних. Стандарт KNX IP Secure дозволяє автентифікувати та шифрувати телеграми KNX в IP-мережах. При цьому зазвичай формується тунелювання, що забезпечує конфіденційність інформації. Механізми KNX IP Secure є додатковою захисною оболонкою (оболонкою), яка захищає весь трафік даних KNXnet/IP. Однак KNX IP Secure не така вже й безпечна, є можливість відстежувати мережу, записувати відправлені пакети й легко їх повторювати, тому що з'єднувачі ліній з функцією "Security Proxy" немає. Крім цього, використання при формуванні тунелювання алгоритму AES-128 у постквантовий період не забезпечить необхідний рівень захисту внутрішнього контуру. Проте істотним недоліком такого підходу є відсутність об'єктивної оцінки поточного стану безпеки системи. Як правило такі системи будуються з двох основних підсистем – кіберфізичної, яка безпосередньо виконує функції обслуговування, та керуючої – системи управління, яка розгортається у хмарі. Використання механізмів безпеки другої підсистеми зазвичай не враховується при оцінці поточного стану безпеки. Формально вважається, що хмарні технології забезпечують необхідний рівень безпеки. Головні загрози безпеці у хмарі: розкрадання даних, втрати даних, злом акаунтів, проломи в інтерфейсах та Application Programming Interface (API), DDos-атаки, дії інсайдерів, можливість проникнення хакерів, а також простої з вини провайдера [25].

Запропонований новий підхід автентифікації у CPS та смарт-технологіях також формується на основі симетричного шифрування, що ставить під сумнів його ефективність в умовах постквантового періоду (появи повномасштабного кантового комп'ютера) [26, 27]. Таким чином, виникає необхідність формування підходу забезпечення безпеки CPS на основі комплексування загроз та формування концепції двоконтурної безпеки, яка дозволить забезпечити об'єктивність оцінки не тільки поточного стану інформаційної безпеки таких систем, але й виявити ознаки синергізму та гібридності цільових атак на такі системи. Таким чином в статті на основі досліджень [11–17] пропонується принципово нова концепція побудови системи безпеки інформаційних ресурсів на основі методів і моделей побудови багатоконтурних систем безпеки, а також механізмів забезпечення основних послуг безпеки на основі постквантових алгоритмів – криптокодових конструкцій на LDPC-кодах, які відрізняються швидкістю та використовуються в мобільних Інтернет-технологіях. Вона містить п'ять етапів: 1) визначення ймовірності впливу загроз на кіберфізичні системи, 2) формування моделей превентивних заходів на основі моделі Лотки-Вольтери, 3) оцінювання ефективності на основі моделей теоретико-ігрового підходу, 4) побудова інтегрованих механізмів забезпечення конфіденційності, цілісності, автентичності та вірогідності інформаційних ресурсів кіберфізичних систем, 5) визначення стану та формування стратегій побудови багатоконтурних систем захисту.

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

1) Визначення ймовірності впливу загроз на кіберфізичні системи

Для визначення ймовірності впливу загроз на кіберфізичні системи використовуємо підхід, запропонований у роботі [11], основною відмінністю є експертна оцінка розподілу загроз з урахуванням їхньої гібридності та синергізму на основі синергетичної моделі загроз.

Для формування експертної оцінки використовуємо модифікацію класифікатора загроз, яка запропонована в роботах [11, 13, 14] та представлена на рис. 1. для об'єктивності суджень експертів використовуємо вагові коефіцієнти компетентності експертів (k_k), подані у табл. 1.

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 - α_i, складе: $\left[x_i - \Delta, x_i + \Delta\right]$, де величина x_i розподілена за нормальним законом із центром у та дисперсією σ_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.

Для визначення економічних витрат запобігання атаки скористаємося алгоритмом з урахуванням вартісних показників загроз. Такий підхід дає змогу оцінити економічні витрати на навмисні механізми захисту з урахуванням ранжирування потенційних загроз та важливості інформаційних ресурсів, що підлягають захисту [11, 13, 14, 16]. Обидві сторони нападу визначаються важливість (рейтинг) атак, які економічно доцільно проводити.

1-й крок. Визначення атак, ефект від реалізації яких перевищує витрати на їхнє проведення:

$$Tr_R^A = \left\{Tr_i \,|\, \left(P_i^A - C_i^A\right) > 0\right\} \; \forall Tr_i \in Tr, \quad (4)$$

де Tr_R^A – множина потенційних загроз, реалізація яких ефективна для атакуючого; Tr_i – загроза і-му інформаційному ресурсу; P_i^A – оцінка вартості успішності реалізації атаки на і-й ресурс з боку атакуючого; C_i^A – вартість проведення атаки на і-й ресурс із боку атакуючого.

2-й крок. Визначення напрямку захисту, який забезпечує ефект вищий, ніж витрати на їхнє забезпечення.

$$Tr_C^D = \left\{Tr_j \,|\, \left(P_i^D - C_i^D\right) > 0\right\} \; \forall Tr_j \in Tr, \quad (5)$$

де Tr_C^D – множина загроз, проти яких економічно доцільно вибудовувати захист; P_i^D – оцінка вартості втрати і-го інформаційного ресурсу для сторони захисту; C_i^D – вартість захисту і-го інформаційного ресурсу сторони захисту;

3-й крок. Визначення коефіцієнтів важливості атакуючих. Визначаються як частки виграшу від загальної суми виграшу, яка може бути отримана по-

тенційно під час реалізації всього комплексу загроз для нападників:

$$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^{M}\left(P_i^A - C_i^A\right)}, \forall Tr_i \in Tr_R^A, M = \left|Tr_R^A\right|, \quad (6)$$

де K_i^A – рейтинговий коефіцієнт (важливості) реалізації загрози і-му інформаційному ресурсу; M – потужність безлічі відібраних потенційно ефективних загроз для атакуючої сторони.

4-й крок. Визначення коефіцієнтів важливості захисників. Визначаються як частки виграшу від загальної суми виграшу, яка може бути отримана потенційно під час реалізації всього комплексу захисних заходів:

$$K_j^D = \frac{P_i^D - C_i^D}{\sum_{i=1}^{N}\left(P_i^D - C_i^D\right)}, \forall Tr_j \in Tr_C^D, N = \left|Tr_C^D\right|, \quad (7)$$

де K_j^D – рейтинговий коефіцієнт (важливості) будівництва захисту j-го інформаційного ресурсу.

5-й крок. Відбір критичних загроз на основі оцінки твору коефіцієнтів важливості, атакуючого та нападника виявляється максимальним:

$$Tr_l = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A. \quad (8)$$

Таким чином, використання даного класифікатора, а також запровадження економічних показників вартості здійснення атаки та вартості заходів протидії їй дозволяють отримати інтегральну оцінку безпеки системи.

Для одержання оцінки поточного стану інформаційної безпеки на основі запропонованої концепції двоконтурної системи захисту інформації CPS припустимо, що "1" відповідатиме максимальному рівню безпеки, який забезпечується системою безпеки в цілому, а "0" відповідає відсутності необхідного рівня захисту інформації.

Для визначення ймовірності реалізації загрози при граничних можливостях захисту A та граничних можливостях нападу B використовуватимемо функцію щільності ймовірності випадкової величини x – F(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 визначимо як частку тих ресурсів, захищених від кібератак. Легко бачити, що ця величина може бути визначена таким чином:

$$S = F(B) - F(A) = \int_{-\infty}^{B} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt - \int_{-\infty}^{A} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt. \quad (9)$$

Для оцінки категорії зловмисника та визначення його можливостей (обчислювальні та фінансові ресурси, економічну зацікавленість) скористаємося моделлю зловмисника та методикою визначення категорії зловмисника на CPS запропонованих у [11, 13, 14]. Для забезпечення безпеки всієї системи захисту необхідно враховувати загрози внутрішнього та зовнішнього контурів:

– загрози внутрішнього контуру з урахуванням гібридності та синергізму [11]:

$$W_{\text{hybrid } C,I,A,Au,Af\ synerg}^{CPSS\ ISL} = W_{synerg}^{CPSS\ ISLC} \bigcap W_{synerg}^{CPSS\ \ ISLI} \bigcap \bigcap W_{synerg}^{CPSS\ \ ISLA} \bigcap W_{synerg}^{CPSS\ ISLAu} \bigcap W_{synerg}^{CPSS\ \ ISLInv}, \quad (10)$$

де $W_{synerg}^{CPSS\ ISLC}$ – синергія загроз на послугу конфіденційності, $W_{synerg}^{CPSS\ ISLI}$ – синергія загроз на послугу цілісності, $W_{synerg}^{CPSS\ ISLA}$ – синергія загроз на послугу доступності, $W_{synerg}^{CPSS\ ISLAu}$ – синергія загроз на послугу автентичності, $W_{synerg}^{CPSS\ ISLInv}$ – синергія погроз на послугу причетності.

– загрози зовнішнього контуру з урахуванням гібридності та синергізму [11]:

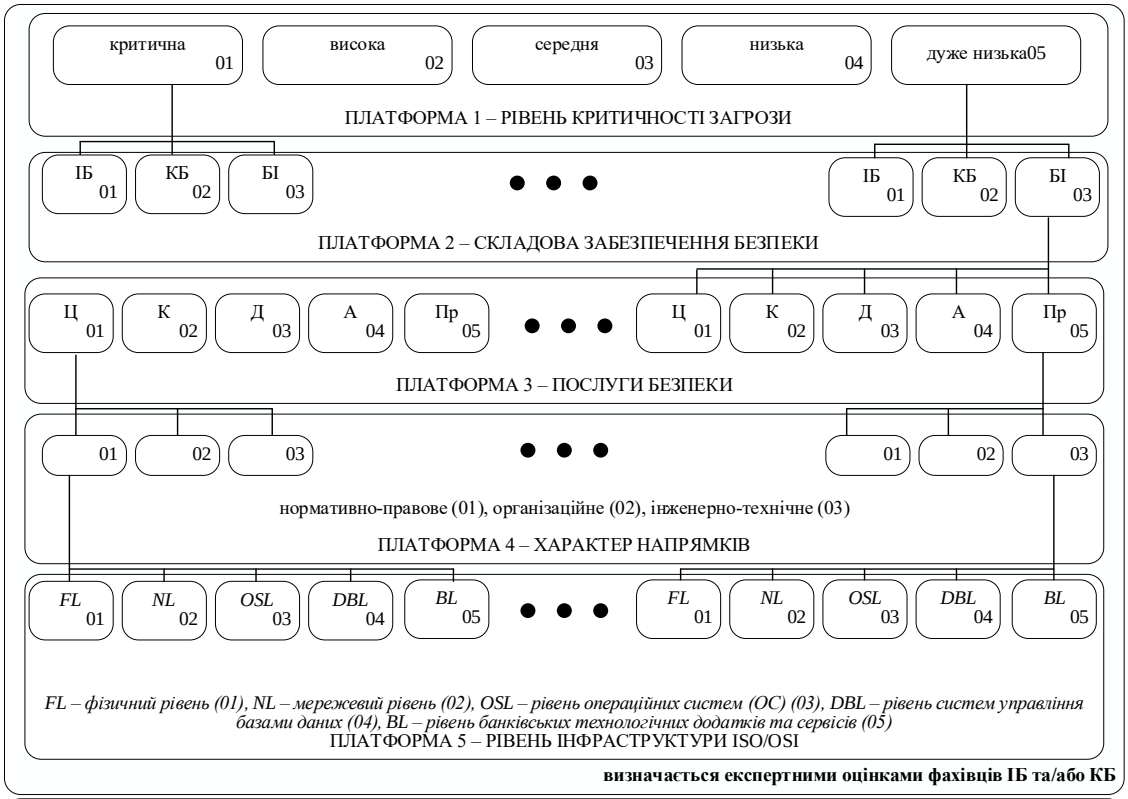
$$W_{\text{hybrid } C,I,A,Au,Af\ synerg}^{SCPS\ ESL} = W_{synerg}^{CPSS\ ESLC} \bigcap W_{synerg}^{CPSS\ \ ESLI} \bigcap \bigcap W_{synerg}^{CPSS\ \ ESLA} \bigcap W_{synerg}^{CPSS\ \ ESLAu} \bigcap W_{synerg}^{CPSS\ \ ESLInv}, \quad (11)$$

де $W_{synerg}^{CPSS\ ESLC}$ – синергія загроз на послугу конфіденційності, $W_{synerg}^{CPSS\ \ ESLI}$ – синергія загроз на послугу цілісності, $W_{synerg}^{CPSS\ \ ESLA}$ – синергія загроз на послугу доступності, $W_{synerg}^{CPSS\ ESLAu}$ – синергія загроз на послугу автентичності, $W_{synerg}^{CPSS\ \ ESLInv}$ – синергія погроз на послугу причетності.

Проведений аналіз [11, 13, 14] показав, що у зовнішньому контурі основними послугами безпеки є цілісність, конфіденційність та доступність, тому послугами автентичності та причетності можна знехтувати. Тоді загрози зовнішнього контуру запишуться у вигляді:

$$W_{\text{hybrid } C,I,A,Au,Af\ synerg}^{CPSS\ ESL} = W_{synerg}^{CPSS\ ESLC} \bigcap W_{synerg}^{CPSS\ \ ESLI} \bigcap \bigcap W_{synerg}^{CPSS\ \ ESLA}. \quad (12)$$

Кожен елемент $I_{A_i} \in \{I_A\}$ інформаційних ресурсів може бути описаний таким вектором: $I_{A_i} = \left(Type_i, A_i^C, A_i^I, A_i^A, A_i^{Au}, A_i^{Inv}, \beta_i\right)$. Type$_i$ – тип інформаційного активу описується безліччю базових значень: 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 таємниця, StR$_i$ – статистичні звіти, PubI$_i$ – загальнодоступна інформація, ContI$_i$ – керуюча інформація, PI$_i$ – персональні дані. $A_i^C, A_i^I, A_i^A, A_i^{Au}, A_i^{Inv}$ – послуги безпеки (A_i^C – конфіденційність, A_i^I – цілісність, A_i^A – доступність, A_i^{Au} – автентичність, A_i^{Inv} – приналежність); β_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). Аналіз класифікації зловмисників дозволяє сформувати множину {H$_j$} CPS ISL, що визначає рівні впливу на CPS внутрішнього контуру, а також множину {Hj} CPS ESL, що визначає рівні впливу на CPS зовнішнього контуру. В роботі [12] наведені результати аналізу, а також запропонована класифікація зловмисників, яка враховує не тільки цілі, а також фінансові та обчислювальні можливості.



визначається експертними оцінками фахівців ІБ та/або КБ

КРОК 1. ФОРМУВАННЯ МЕТРИЧНИХ КОЕФІЦІЄНТІВ ЗАГРОЗ ДЛЯ CPSS ISL І CPSS ESL

$$w_{CPSS\ ESL}{}^{j} = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{CPSS\ ESLik}^{\ j}, \quad w_{CPSS\ ISL}{}^{j} = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{CPSS\ ISLik}^{\ j}$$

КРОК 2. ФОРМУВАННЯ ВАГОВИХ КОЕФІЦІЄНТІВ УМОВ ПРОЯВИ ЗАГРОЗ ДЛЯ CPSS ISL І CPSS ESL

$$\alpha_i^{CPSS\ ISL},\ i \in [0,067;0,133;0,2;0,267;0,333],\ \alpha_i^{CPSS\ ESL},\ i \in [0,067;0,133;0,2;0,267;0,333]$$

КРОК 3 . ВИЗНАЧЕННЯ РЕАЛІЗАЦІЇ КОЖНОЇ ЗАГРОЗИ ДЛЯ CPSS ISL І CPSS ESL

$$w_{CPSS\ ISLi}{}^{j} P_{CPSS\ ISLi}{}^{j} = \frac{1}{K} P_{CPSS\ ISL}{}_{i}^{\ j} \sum_{k=1}^{N} w_{I_{CPSS\ ISL}}{}_{ik}^{\ j}, \quad \text{де } P_{CPSS\ ISL}{}_{i}^{\ j} \in \left\{\alpha_i^{CPSS\ ISL}\right\},$$

$$w_{CPSi}{}^{j} P_{CPSi}{}^{j} = \frac{1}{K} P_{CPSS\ ESLi}{}^{j} \sum_{k=1}^{N} w_{CPSS\ ESLik}^{\ j}, \quad \text{де } P_{CPSS\ ESLi}{}^{j} \in \left\{\alpha_i^{CPSS\ ESL}\right\}$$

КРОК 4 . ВИЗНАЧЕННЯ РЕАЛІЗАЦІЇ КІЛЬКАХ ЗАГРОЗ НА ПОСЛУГУ БЕЗПЕКИ

$$W_{CPSS\ ISLsynerg}^{\ C} = \sum_{i=1}^{M} w_{CPSS\ ISLi}{}^{C} \alpha^{CPSS\ ISLC}_{\ i} \bigcup W_{CPSS\ ESLsynerg}^{\ C} = \sum_{i=1}^{M} w_{CPSi}{}^{C} \alpha^{CPSS\ ESLC}_{\ i}$$

$$W_{CPSS\ ISLsynerg}^{\ I} = \sum_{i=1}^{M} w_{CPSS\ ISLi}{}^{I} \alpha^{CPSS\ ISLC}_{\ i} \bigcup W_{CPSS\ ESLsynerg}^{\ I} = \sum_{i=1}^{M} w_{CPSi}{}^{I} \alpha^{CPSS\ ESLC}_{\ i}$$

$$W_{CPSS\ ISLsynerg}^{\ A} = \sum_{i=1}^{M} w_{CPSS\ ISLi}{}^{A} \alpha^{CPSS\ ISLC}_{\ i} \bigcup W_{CPSS\ ESLsynerg}^{\ A} = \sum_{i=1}^{M} w_{CPSi}{}^{A} \alpha^{CPSS\ ESLC}_{\ i}$$

$$W_{CPSS\ ISLsynerg}^{\ Aff} = \sum_{i=1}^{M} w_{CPSS\ ISL}{}_{i}^{\ Aff} \alpha^{CPSS\ ISL\ Aff}_{\ i}; \quad W_{CPSS\ ISLsynerg}^{\ Inv} = \sum_{i=1}^{M} w_{CPSS\ ISLi}{}^{Inv} \alpha^{CPSS\ IS\ Inv}_{\ i}$$

КРОК 5 . ВИЗНАЧЕННЯ СУМАРНИЙ ЗАГРОЗ НА СКЛАДОВУ БЕЗПЕКИ

$$W_{synerg}^{IS} = \sum_{i=1}^{N}\left(w_{CPSS\ ISLi}{}^{C} \cap w_{CPSS\ ISLi}{}^{I} \cap w_{CPSS\ ISLi}{}^{A} \cap w_{CPSS\ ISLi}{}^{Au} \cap w_{CPSS\ ISLi}{}^{Aff}\right)\alpha_i^{CPSS\ ISL} \cup$$

$$\cup \sum_{i=1}^{N}\left(w_{CPSS\ ESLi}{}^{C} \cap w_{CPSS\ ESLi}{}^{I} \cap w_{CPSS\ ESLi}{}^{A}\right)\alpha_i^{CPSS\ ESL}$$

КРОК 6 . ВИЗНАЧЕННЯ ЕКОНОМІЧНИХ ВИТЯКІВ НА ПОПЕРЕДЖЕННЯ АТАКИ

$$Tr_{CPSS\ ISLR}{}^{A} = \left\{Tr_i \mid \left(P_i^A - C_i^A\right) > 0\right\}\ \forall Tr_i \in Tr \Rightarrow Tr_L^{ICS} = \arg\max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A$$

$$Tr_{CPSS\ ESLR}{}^{A} = \left\{Tr_i \mid \left(P_i^A - C_i^A\right) > 0\right\}\ \forall Tr_i \in Tr \Rightarrow Tr_L^{CPS} = \arg\max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A$$

визначається автоматично на основі математичних виразів

Рис. 1. Класифікатор загроз

Ваговий коефіцієнт "небезпеки" зловмисника визначимо за формулою [12]:

$$\gamma_{ICS}^{CPS} = \frac{1}{N}\sum_{i=1}^{N}\gamma_{ICS\,i}^{CPS}, \quad (13)$$

де $\gamma_{ICS\,i}^{CPS} = \left(\beta_i^{ICS} \cup \beta_i^{CPS}\right) \times p_{rj} \times r_{motiv}$, $\beta_i^{CPSS\ ISL} = W_{cp}^{CPSS\ ISL} \cap W_{cash}^{CPSS\ ISL} \cap T^{CPSS\ ISL}$, $\beta_i^{CPSS\ ESL} = W_{cp}^{CPSS\ ESL} \cap W_{cash}^{CPSS\ ESL} \cap T^{CPSS\ ESL}$ – вагові коефіцієнти можливостей порушника для CPSS ISL та CPSS ESL (відповідно), $W_{cp}^{CPSS\ ISL}\left(W_{cp}^{CPSS\ ESL}\right)$ - обчислювальні ресурси порушника (1 – необмежені ресурси кібертерористів, 0,75 – ресурси держави (спецслужб), 0,5 – ресурси кіберзлочинців, 0,25 – ресурси криміналу, конкурентів, хакерів, 0,001 – ресурси вандалів); TCPSS ISL (TCPSS ESL) – час виконання загрози (1 – загроза реалізується щодня, 0,75 – загроза реалізується протягом тижня, 0,5 – загроза реалізується протягом місяця, 0,25 – загроза реалізується протягом року, 0,001 – необмежений час); $W_{cash}^{CPSS\ ISL}\left(W_{cash}^{CPSS\ ESL}\right)$ – економічні можливості нападаючих (1 – необмежені ресурси кібертерористів, 0,75 – ресурси держави (спецслужб), 0,5 – ресурси кіберзлочинців, 0,25 – ресурси криміналу, конкурентів, хакерів, 0,001 – ресурси вандалів). У табл. 2 наведено вихідні дані критеріїв та показників експертної оцінки його знаходження.

Таблиця 2

Вихідні дані критеріїв та показників експертної оцінки вагового коефіцієнта "небезпеки" порушника

Категорія	Показники оцінки вагового коефіцієнта							
	$\beta_i^{ICS} \in \{\beta_i^{ICS}\}$			$\beta_i^{CPS} \in \{\beta_i^{CPS}\}$			prj	rmotiv
	$W_{cp}^{CPSS\ ISL}$	TCPSS ISL	$W_{cash}^{CPSS\ ISL}$	$W_{cp}^{CPSS\ ESL}$	TCPSS ESL	$W_{cash}^{CPSS\ ESL}$		
критична	1	1	1	1	1	1	1	1
висока	0,75	0,75	0,75	0,75	0,75	0,75	0,75	0,75
середня	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5
низька	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25
дуже низька	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001

Аналіз табл. 2 дозволяє враховувати, що атака визначається комплексним критерієм, який враховує вартість проведення та доступні зловмиснику обчислювальні можливості. Такий підхід забезпечує своєчасне реагування на комп'ютерні інциденти у потрібній залежності від категорії зловмисника та дозволяє забезпечити потрібний рівень безпеки.

2) формування моделей превентивних заходів на основі моделі Лотки-Вольтери

В роботах [14, 18] пропонується метод оцінки безпеки кіберфізичних систем, який ґрунтується на базі розробленого класифікатора загроз, й дозволяє оцінити поточний рівень безпеки, а також в динаміці формувати рекомендації щодо розподілу обмежених ресурсів захисту на основі експертної оцінки відомих загроз. Такий підхід дозволяє проводити динамічне моделювання в оф-лайн режимі, що дозволяє на основі аналізу загроз своєчасно визначити можливості зловмисників і сформувати превентивні заходи захисту.

Запропоновано моделі безпеки кіберфізичних систем: "хижак-жертва" з урахуванням обчислювальних можливостей і спрямованості цільових кібератак, "хижак-жертва" з урахуванням можливої конкуренції зловмисників по відношенню до "жертви", "хижак-жертва" з урахуванням взаємозв'язків між "видами жертв" і "видами хижаків", "хижак-жертва" з урахуванням взаємозв'язків між "видами жертв" і "видами хижаків". На основі запропонованого підходу отримані коефіцієнти моделі Лотки-Вольтери α=0,39, β=0,32, γ=0,29, φ=0,27, які враховують синергізм і гібридність сучасних загроз, фінансування на формування та вдосконалення системи захисту, а також дозволяє визначити фінансові та обчислювальні можливості зловмисника по виявленим загрозам.

Розробка моделей безпеки кіберфізичних систем, що розвиваються, з урахуванням обчислювальних можливостей і спрямованості цільових кібератак.

Чисельність об'єктів, що представляють цілі атак з урахуванням їхньої гібридності, може бути представлена таким чином:

$$\tilde{N}_1 = \sum_{i=1}^{Q}\begin{pmatrix} N_{1_i}^{C} \times A_i^{C} + N_{1_i}^{I} \times A_i^{I} + N_{1_i}^{A} \times A_i^{A} + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix}. \quad (14)$$

При реалізації алгоритму допускається, що сторони конфлікту визначають критичність кіберзагроз, які економічно доцільно проводити та/або яких необхідно захистити інформаційні ресурси(IP) насамперед. Тоді алгоритм визначимо:

1-й крок. Визначення кіберзагроз, ефект від яких перевищує витрати на їх проведення:

$$Tr_R^A = \left\{Tr_i \mid \left(P_i^A - C_i^A\right) > 0\right\} \forall Tr_i \in Tr, \quad (15)$$

де Tr_R^A – множина потенційних загроз, реалізація яких ефективна атакуючого; Tr_i – загроза і-му інформаційному ресурсу; P_i^A – оцінка вартості успішності реалізації атаки на і-й ресурс з боку атакуючого; C_i^A – вартість проведення атаки на і-й ресурс з боку атакуючого.

2-й крок. Визначення напрямку захисту, який забезпечує ефект вищий, ніж витрати на їхнє забезпечення:

$$Tr_C^D = \left\{Tr_j \mid \left(P_i^D - C_i^D\right) > 0\right\} \forall Tr_j \in Tr. \quad (16)$$

3-й крок. Визначення коефіцієнтів важливості нападника. Визначаються як частки виграшу від загальної суми виграшу, яка може бути отримана потенційно під час реалізації всього комплексу загроз для нападників:

$$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^{M}\left(P_i^A - C_i^A\right)}, \forall Tr_i \in Tr_R^A, M = \left|Tr_R^A\right|. \quad (17)$$

4-й крок. Визначення коефіцієнтів важливості захисників. Визначаються як частка виграшу від загальної суми виграшу, яка, можливо, отримана потенційно при реалізації всього комплексу захисних заходів:

$$K_j^D = \frac{P_i^D - C_i^D}{\sum_{i=1}^{N}\left(P_i^D - C_i^D\right)}, \forall Tr_j \in Tr_C^D, N = \left|Tr_C^D\right|. \quad (18)$$

5-й крок. Відбір критичних загроз, для яких на основі оцінки добуток коефіцієнтів важливості атакуючого та захищається виявляється максимальним:

$$Tr_l = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A. \quad (19)$$

Тоді коефіцієнт народжуваності "жертв" пропонується розраховувати, як:

$$\alpha = \frac{\left|\{Tr_l\}\right|}{Q}. \quad (20)$$

Для оцінки впливу сучасних загроз на засоби захисту скористаємося виразом у роботі [15], тоді коефіцієнт β уявімо як:

$$\beta = \sum_{i=1}^{M}\left(w_{CPSi}^{\ C} \cap w_{CPSi}^{\ I} \cap w_{CPSi}^{\ A} \cap w_{CPSi}^{\ Au} \cap w_{CPSi}^{\ Aff}\right)\chi_i^{CPS}. \quad (21)$$

Для визначення коефіцієнта обчислювальних можливостей зловмисника φ, скористаємося класифікацією зловмисників, як представлено у роботі [15], та представимо як:

$$\varphi = \frac{1}{M}\sum_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv}. \quad (22)$$

У табл. 3 наведено вихідні дані критеріїв та показників експертної оцінки його знаходження.

Таблиця 3

Вихідні дані критеріїв та показників експертної оцінки вагового коефіцієнта обчислювальних можливостей зловмисника

Категорія	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

Коефіцієнт можливості превентивних заходів представимо як:

$$\gamma^j = \frac{1}{K \times B}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\mu_{kg}^j \times w_{kg}^j\right). \quad (23)$$

Запропонований підхід моделі безпеки кіберфізичних систем дозволяє, з практичної точки, розглядати кіберпростір як екосистему, враховувати обчислювальні можливості зловмисників та спрямованість цільових кібератак.

Крім цього, кібератаки розглядаються з урахуванням їхнього комплексування з методами соціальної інженерії, що дозволяє формувати зловмисникам цільові атаки. Запропонована модель враховує можливість прояву цільових атак в екосистемі ознак синергізму та гібридності, що суттєво впливає на кількісні показники оцінки поточного стану рівня захищеності.

Таким чином, використовуючи отримані вирази, модель Лотки-Вольтери можна представити в наступному вигляді:

$$\begin{cases} \frac{dN_1}{dt} = \left(\arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A\right) \times \\ \times\left(\sum_{i=1}^{Q}\left(\begin{matrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{matrix}\right)\right) - \\ -\left(\sum_{i=1}^{M}\left(\begin{matrix} w_{CPSi}^{\ C} \cap w_{CPSi}^{\ I} \cap w_{CPSi}^{\ A} \cap \\ \cap w_{CPSi}^{\ Au} \cap w_{CPSi}^{\ Aff} \end{matrix}\right)\chi_i^{CPS}\right) \times \\ \times \tilde{N}_1\left(N_2 \times \left|W_{\text{hybrid } C,I,A,Au,Af\ synerg}\right|\right); \\ \frac{dN_2}{dt} = -\left(\frac{1}{M}\sum_{i=1}^{M}\nu_i \times p_{rj} \times r_{motiv}\right)\tilde{N}_2 + \\ +\left(\frac{1}{KB}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\mu_{kg}^j \times w_{kg}^j\right)\right)\tilde{N}_2\tilde{N}_1. \end{cases} \quad (24)$$

Розробка моделі безпеки кіберфізичних систем на основі моделі "хижак-жертва" з урахуванням можливої конкуренції зловмисників щодо "жертв".

Однією з переваг моделі Лотки-Во»льтери є можливість використовувати "біологічні" аспекти моделі "хижак-жертва" з урахуванням можливої боротьби між самими "хижаками" в умовах зменшення популяції "жертв".

З погляду сучасного розвитку світової спільноти, вже виявляються серед кіберзловмисників/кібергруп окремі прояви конкурентної боротьби. Це, з одного боку, може забезпечити збільшення популяції "жертв", тобто збільшити можливості системи захисту інформації протистояти загрозам та/або своєчасно підготувати превентивні заходи для протидії. З іншого боку, зменшити кількість "хижаків", тобто зменшити різновид загроз, що дозволить своєчасно реагувати на них.

З урахуванням викладених припущень модель "хижак-жертва" представимо як:

$$\begin{cases} \dfrac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum\limits_{i=1}^{Q} \left(\begin{matrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{matrix} \right) \right) - \\ - \left(\sum\limits_{i=1}^{M} \left(\begin{matrix} w_{CPSi}{}^C \cap w_{CPSi}{}^I \cap w_{CPSi}{}^A \cap \\ \cap w_{CPSi}{}^{Au} \cap w_{CPSi}{}^{Aff} \end{matrix} \right) \chi_i^{CPS} \right) \times \\ \times \tilde{N}_1 \left(\tilde{N}_2^1 \cap \tilde{N}_2^2 \cap \ldots \cap \tilde{N}_2^w \right); \\ \dfrac{dN_2}{dt} = - \left(\dfrac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \times \\ \times \left(\tilde{N}_2^1 \cap \tilde{N}_2^2 \cap \ldots \cap \tilde{N}_2^w \right) + \left(\dfrac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \times \\ \times \left(\tilde{N}_2^1 \cap \tilde{N}_2^2 \cap \ldots \cap \tilde{N}_2^w \right) \tilde{N}_1. \end{cases} \quad (25)$$

Запропонована модель безпеки кіберфізичних систем враховує можливу конкуренцію зловмисників щодо "жертви". Це дозволяє своєчасно визначити як спрямованість загроз, а й обчислювальні ресурси нападників, які "одночасне" вплив може забезпечити "зниження" ризику реалізації кіберзагроз.

Розробка моделі безпеки кіберфізичних систем на основі моделі "хижак-жертва" з урахуванням можливості групування зловмисників/кібергруп з метою досягнення цілей кібератаки

Модель Лотки-Вольтери дозволяє враховувати як конкурентність "хижаків", а й їх об'єднання. При цьому, як у будь-якій екосистемі, можуть виявлятися емерджентні властивості "хижаків", що з точки зору безпеки може призвести до значного зменшення стійкості системи захисту контуру бізнес-процесів або до його злому та руйнування безперервності бізнес-процесів. З урахуванням викладених припущень модель "хижак-жертва" представимо як (26).

Запропонована модель безпеки кіберфізичних систем на основі моделі "хижак-жертва" дозволяє враховувати можливості групування зловмисників/кібергруп з метою досягнення цілей кібератаки. Такий підхід дозволяє прогнозувати "найгірші" варіанти розвитку кібератаки, а також формувати відповідні превентивні заходи.

$$\begin{cases} \dfrac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum\limits_{i=1}^{Q} \left(\begin{matrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{matrix} \right) \right) - \\ - \left(\sum\limits_{i=1}^{M} \left(\begin{matrix} w_{CPSi}{}^C \cap w_{CPSi}{}^I \cap w_{CPSi}{}^A \cap \\ \cap w_{CPSi}{}^{Au} \cap w_{CPSi}{}^{Aff} \end{matrix} \right) \chi_i^{CPS} \right) \tilde{N}_1 \left(\sum\limits_{j=1}^{w} \tilde{N}_2^w \right); \\ \dfrac{dN_2}{dt} = - \left(\dfrac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \left(\sum\limits_{j=1}^{w} \tilde{N}_2^w \right) + \\ + \left(\dfrac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \left(\sum\limits_{j=1}^{w} \tilde{N}_2^w \right) \tilde{N}_1. \end{cases} \quad (26)$$

Таким чином, на основі запропонованих моделей пропонується метод оцінки безпеки кіберфізичних систем на основі моделі Лотки-Вольтерри "хижак-жертва", який складається з наступних кроків:

Перший етап. Формуються та/або обчислюються:

- метричні коефіцієнти загроз;
- вагові коефіцієнти прояву загроз;
- визначення реалізації кожної загрози;
- визначення реалізації загроз на послугу безпеки;
- визначення сумарних загроз на складову безпеки;
- визначення економічних витрат на запобігання атаки.

Другий етап. На основі аналізу етапу 1, вибирається модель Лотки-Вольтери, і за формулами (13)-(21) розраховуються відповідні коефіцієнти та складові виразів.

Третій етап. На основі виразів (22)-(26) визначається поточний стан безпеки кіберфізичної системи. Запропонований метод базується на оцінці безпеки кіберфізичних систем з часом. Описовою характеристикою зміни поточного стану безпеки CFS є його інтенсивність l(t) – середня кількість змін, що відбулися із поточним станом безпеки CFS в одиницю часу.

Оцінку інтервалів часу $\Delta t_{[i-q]}$ між змінами, рівня безпеки CFS використовуємо формулу:

$$\Delta t_{[i-q]}(t) = \frac{K}{l(t)}, \quad (27)$$

де K – сумарна кількість змін рівня безпеки; l(t) – інтенсивність змін рівня безпеки; $i, q \in [1; n]$ – порядкові номери змін; $i \geq q$.

Зміни рівнів безпеки опишемо у вигляді кінцевого автомата HCFS, стан якого описує формула:

$$H^{CFS} = \langle S^I, value, \Pi, S_0^I \rangle, \quad (28)$$

де SI – кінцевий стан рівня безпеки CFS; value – значення змін рівня безпеки CFS; П – функція переходів рівня безпеки CFS зі стану k до стану j; S_0^I – початковий стан рівня безпеки CFS.

Функція переходів рівня безпеки CFS П зі стану k до стану j оцінимо за формулою:

$$\Pi = S_0^I \times value \to S^I. \quad (29)$$

3) оцінювання ефективності на основі моделей теоретико-ігрового підходу

В роботі [16] запропоновані моделі основних задач взаємодії антагоністичних агентів систем безпеки. Моделі дозволили отримати рішення двох найбільш поширених задач в області кібербезпеки, а саме, взаємодії системного адміністратора і зловмисника при організації захисту інформаційних ресурсів. Задачі вирішені для двох різних умов – матриця гри містить вартісні оцінки ресурсів і матриця відображає ймовірності реалізації загрози. Визначено чисті і змішані стратегії для різних початкових умов, що дозволяє виключити з розгляду стратегії, що не входять в рішення.

Проведені дослідження напрямків використання теоретико-ігрового моделювання у завданнях забезпечення кібербезпеки дозволили виділити найпоширеніші теоретико-ігрові моделі, що використовуються у сфері безпеки. До них відносяться Стакельберга, ігри Неша та сигнальні ігри. Вибрані моделі ігор не вичерпують всього різноманіття теоретико-ігрових моделей, що застосовуються, а лише є прикладами найбільш поширених застосувань.

У табл. 4 представлені основні компоненти цих ігор. Ці компоненти визначають структуру таксономії ігор та його моделей. Теоретико-ігрові моделі дозволяють формувати множину релевантних завдань для забезпечення основних послуг безпеки: конфіденційності, цілісності, доступності, автентичності.

Таким чином, одна і та сама модель може забезпечувати розв'язання кількох завдань забезпечення безпеки, і навпаки, те саме завдання може бути вирішена з використанням різних моделей. В силу цього на практиці необхідно визначити необхідну підмножину ігрових моделей, що підтримують вирішення безлічі завдань забезпечення безпеки, або виділення їх підмножини.

Таблиця 4

Гравці, типи, дії та корисності для трьох ігор

Гравці P	Типи Θ	Дії A	Корисність U	Тривалість T
Гра Стакельберга між лідером L та послідовником F	Типово однорідний	$L: a_L \in A_L$ $F: a_F \in A_F$	$L: U_L(a_L, a_F)$ $F: U_F(a_L, a_F)$	Однокрокова структура лідер-послідовник
Гра Неша між симетричними гравцями V та W	Типово однорідний	$V: a_V \in A_V$ $W: a_W \in A_W$	$V: U_V(a_V, a_W)$ $W: U_W(a_V, a_W)$	Структура одночасних ходів
Сигнальна гра між відправником S та одержувачем R	S має кілька типів $\theta \in \Theta$	$S: a_S \in A_S$ $R: a_R \in A_R$	S кожного типу $\theta \in \Theta: U_S^{\theta}(a_S, a_R)$ $R: U_R(\theta, a_S, a_R)$	Однокрокова структура відправник-одержувач

4) побудова інтегрованих механізмів забезпечення конфіденційності, цілісності, автентичності та вірогідності інформаційних ресурсів кіберфізичних систем

В умовах стрімкого зростання обчислювальних можливостей мобільних технологій та створення на їх базі бездротових Mesh-, сенсорних-мереж, технологій Інтернет-речей, smart-технологій актуальною проблемою стає забезпечення безпеки інформації. При цьому виникає необхідність розгляду безпеки у двох контурах внутрішньому (безпосередньо всередині інфраструктури мережі) та зовнішньому (хмарних технологіях). У таких умовах необхідно комплексувати загрози як на внутрішній контур безпеки, так і на зовнішній контур. Це дозволяє не лише враховувати гібридність та синергізм сучасних цільових загроз, але й враховувати рівень значущості (ступінь секретності) інформаційних потоків та інформації, що циркулює як у внутрішньому, так і зовнішньому контурі безпеки. Пропонується концепція побудови безпеки на основі двох контурів. Для забезпечення безпеки бездротових мобільних каналів пропонується використовувати крипто-кодові конструкції Мак-Еліса та Нідеррайтера на LDPC-кодах, що дозволяє інтегруватися у технології забезпечення вірогідності стандартів IEEE 802.15.4, IEEE 802.16. Такий підхід дозволяє забезпечити необхідний рівень послуг безпеки (конфіденційності, цілісності автентичності) в умовах повномасштабного квантового комп'ютера. Для забезпечення основних послуг пропонується використовувати крипто-кодові конструкції Мак-Еліса та Нідеррайтера які детально розглянуті у роботах [12–14]. Відкритий ключ формується шляхом перемноження матриць маскування на матриці породжувальну/перевірочну:

- для крипто-кодової конструкції (ССС) Мак-Еліса–

$$G_{X_{a_i}}^{LDPCu} = X^u \times G^{LDPCu} \times P^u, u \in \{1, 2, ..., s\}; \quad (30)$$

- для ССС Нідеррайтера –

$$H_{X_{a_i}}^{LDPCu} = X^u \times H^{LDPCu} \times P^u, u \in \{1, 2, ..., r\}. \quad (31)$$

В канал зв'язку подається:

- для ССС Мак-Еліса – кодове слово:

$$C_j = M_i \times G_{X_{a_i}}^{LDPCu^T} + e, \quad (32)$$

де e – додатковий сеансовий ключ для кожної інформаційної посилки.

- для ССС Нідеррайтера – синдромна послідовність:

$$S^* = (e_n) \times H_{X_{a_i}}^{LDPC^T}. \quad (33)$$

На приймальній стороні уповноважений користувач знає матриці маскування, використовує швидкий алгоритм на основі м'якого декодування.

На рис. 2 представлена структурна схема декодування одержаної послідовності на основі м'якого декодування.

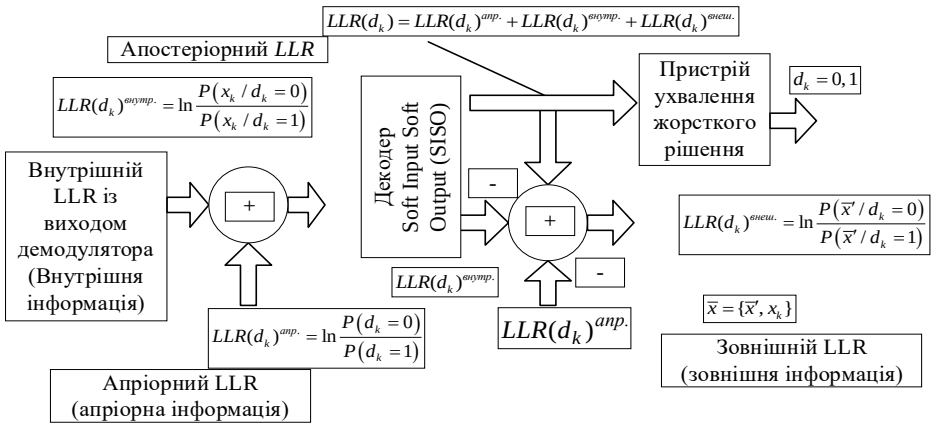


Рис. 2. Схема декодування з урахуванням м'якого рішення

На схемі введені такі позначення: LLR – log-likelihood ratio (логарифм відношення правдоподібності); d*k* – символ кодового слова, dij∈{0, 1}, $x_k=(2d_k\ 1)+pk$, p_k – випадкова величина, що має нормальний розподіл із нульовим середнім значенням.

Аналіз рис. 2 показує, що м'яке рішення є логарифм відношення правдоподібності (апостеріорний LLR). М'яке рішення можна уявити сукупністю апріорної, внутрішньої та зовнішньої інформації. Прийняття жорсткого рішення деякого символу складає основі апостеріорного LLR. Знак логарифму стосовно правдоподібності визначає жорстке рішення, а величина – надійність цього рішення.

Використання постквантових несиметричних криптосистем забезпечить необхідний рівень захищеності при забезпеченні послуг безпеки. Використання кодів LDPC дозволяє без істотних змін використовувати мобільні бездротові технології на основі стандартів IEEE802.11ac, IEEE802.11ax, IEEE-802.16m, IEEE802.15.1, IEEE802.15.4. Система розумний будинок управляє комплексом автономних систем, кожна з яких управляє певними пристроями в будинку, поєднуючи їх загальну кіберфізичну систему. Однак для забезпечення безпеки зовнішнього контуру (системи керування та зберігання інформації) пропонується використовувати розроблений сервер, який фізично розміщується у будинку.

Кожна система відправляє пакет даних на локальний сервер, що дозволяє управляти домом без інтернету, перебуваючи в тій же локальній мережі (бувши підключеним до WI-FI-роутеру). Інформація в мережі кіберфізичної системи передається відкритими бездротовими каналами з шифруванням на основі ССС Мак-Еліса і Нідеррайтера на LDPC-кодах.

Такий підхід забезпечує послуги безпеки, а шляхом використання локального сервера управління забезпечує зниження ймовірності цільових атак на отримання несанкціонованого доступу до системи управління "Розумним будинком". Також підхід забезпечує необхідний рівень безпеки при використанні мобільних програм управління, на основі використання ССС Мак-Еліса і Нідеррайтера на LDPC-кодах. Для забезпечення безпеки бази даних можуть використовуватись ССС Мак-Еліса та Нідеррайтера на ЄС (MEC), що значно ускладнить можливість реалізації кібератак класу R2L (Remote to Local (user) Attack – віддалена атака на локального користувача).

5) визначення стану та формування стратегій побудови багатоконтурних систем захисту

Для забезпечення безпеки соціокіберфізичних систем та систем, заснованих на їхній інфраструктурі, необхідно враховувати не тільки бурхливий розвиток обчислювальних можливостей мобільних технологій (бездротових каналів зв'язку) з їх можливостями забезпечити передачу інформації від 1 Тб/с і вище, зростання можливостей послуг та функціональності хмарних технологій, а також комплексування сучасних загроз на основі синтезу механізмів соціальної інженерії, кіберзагроз (з ознаками гібридності та синергізму), а також можливості спецслужб контролювати значну частину ресурсів хмарних технологій.

Для реалізації такого підходу пропонується розділити CPS на дві підсистеми безпеки та інфраструктури – внутрішній контур, кіберфізична система (CFS), яка забезпечує необхідний набір послуг та функціональності, та зовнішній контур – управлінська система (managerial system, MS) на основі синтезу бездротових мереж та систем хмарних технологій.

Такий підхід забезпечує синтез внутрішнього та зовнішнього контурів, враховує оперативність, енергоємність та відносну безпеку (кожен контур будує безпеку на своїх механізмах та принципах), з одного боку. З іншого боку, дозволяє об'єктивно оцінити загрози кожного з контурів з урахуванням обчислювальних ресурсів та фінансових можливостей зловмисників. На рис. 3 представлено структурну схему концепції двоконтурної безпеки CFS.

Тоді загальний (поточний) рівень захищеності соці-кіберфізичних систем на основі бездротових мобільних технологій описується виразом [11]:

– для адитивного згортки

$$L_{W_{\text{security}}^{CPSS}} = \sum_{W_{\text{hybrid}\,C,I,A,Au,Af\,synerg}^{CPSS\ ISL}} \sum_{i=1}^{8}\left(I_{A_i} \times \beta_i\right) + \\ + \sum_{W_{\text{hybrid}\,C,I,A,synerg}^{CPSS\ ESL}} \sum_{i=1}^{8}\left(I_{A_i} \times \beta_i\right). \quad (34)$$

– для мультиплікативної згортки

$$L_{W_{\text{security}}^{CPSS}} = 1 - \left[1 - \sum_{W_{\text{hybrid}\,C,I,A,Au,Af\,synerg}^{CPSS\ ISL}} \sum_{i=1}^{8} \left(I_{A_i} \times \beta_i \right) \right] \times \times \left[1 - \sum_{W_{\text{hybrid}\,C,I,A,synerg}^{CPSS\ ESL}} \sum_{i=1}^{8} \left(I_{A_i} \times \beta_i \right) \right]. \quad (35)$$

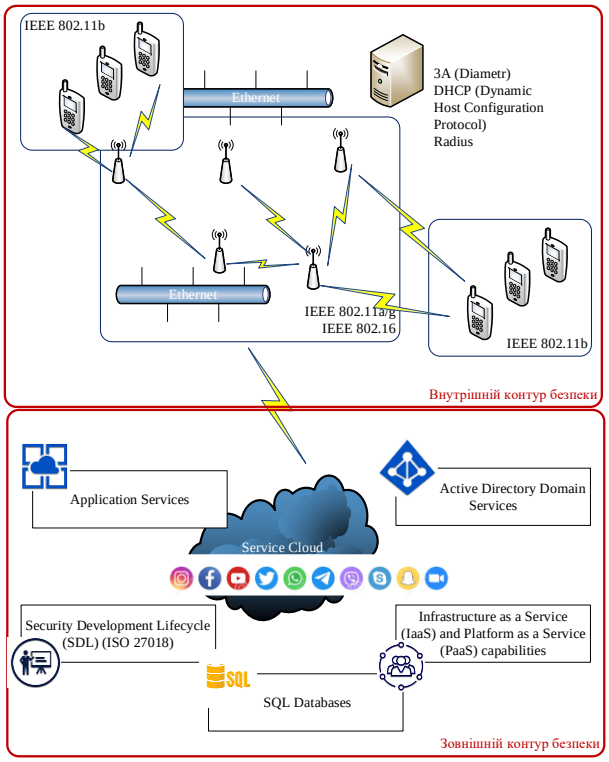


Рис. 2. Структурна схема концепції двоконтурної безпеки кіберфізичних систем

Для визначення поточного стану безпеки внутрішнього контуру використовуємо підхід, запропонований у роботі [9], основною відмінністю є експертна оцінка розподілу загроз з урахуванням їхньої гібридності та синергізму на основі синергетичної моделі загроз. Основні етапи наведені у роботі [11].

У (33), (34) індекс і належить до відповідного типу інформаційного активу, а зовнішнє підсумовування здійснюється за всіма загрозами внутрішнього та зовнішнього контурів.

Запропонована концепція двох контурів безпеки забезпечує комплексування та враховує можливості цільових кібератак, їх синергізм, гібридність та можливість комплексування в умовах зростання обчислювальних ресурсів та розширення спектра смарт-технологій.

Висновки Розвиток обчислювальних ресурсів, квантових комп'ютерів та бурхливе зростання використання бездротових та мобільних технологій дозволяє формувати та розвивати смарт-технології, нові формати мереж, що ґрунтуються на їх синтезі з класичними мережами. Однак, у гонитві за надшвидкістю та цифровізацією, розробники не приділяють належної уваги безпеці таких систем.

Формування кіберфізичних систем на основі комплексування та синтезу бездротових технологій та мобільних Інтернет-технологій, з Інтернет-мовами, з одного боку, забезпечують подальший розвиток цифрових послуг. З іншого боку, формують незахищені критичні точки, які використовують кіберзлочинці з метою. Поява повномасштабного квантового комп'ютера лише посилює можливість забезпечити необхідний рівень безпеки. Крім того, використання хмарних технологій потребує переоцінки підходів до формування системи безпеки. У таких умовах запропонований підхід використання двоконтурної системи безпеки є актуальним та своєчасним. Запропонована концепція дозволяє не лише враховувати ознаки синергізму та гібридності сучасних загроз, а й забезпечує об'єктивний підхід до оцінки поточного рівня захищеності у кіберфізичних системах.

Використання для забезпечення безпеки постквантових криптосистем – крипто-кодових конструкцій забезпечує своєчасний перехід на алгоритми постквантового періоду. Такий підхід забезпечує необхідний рівень захищеності послуг безпеки, а використання різних кодів дозволяє з урахуванням вартості (ступеня секретності) інформації забезпечити її безпеку при використанні сучасних стандартів бездротових каналів зв'язку. При цьому вартість безпеки пропонується оцінювати не кількісною оцінкою збитків при її компрометації, а часом її актуальності, що дозволяє варіювати використанням в ССС завадостійких кодів.

Запропоновано моделі безпеки кіберфізичних систем з урахуванням обчислювальних можливостей та спрямованості цільових кібератак, можливу конкуренцію зловмисників щодо "жертви". Моделі також відображають можливості групування з метою досягнення цілей кібератаки, взаємозв'язків між "видами жертв" та "видами хижаків".

На основі запропонованого підходу отримані коефіцієнти моделі Лотки-Вольтері α=0,39, β=0,32, γ=0,29, φ=0,27, які враховують синергізм та гібридність сучасних загроз, фінансування на формування та удосконалення системи захисту, а також дозволяє визначити фінансові та обчислювальні можливості зловмисника щодо виявлених загроз. Розроблено метод оцінки безпеки кіберфізичних систем на основі моделі Лотки-Вольтери "хижак-жертва". Метод ґрунтується на базі запропонованого класифікатора загроз з урахуванням їхньої гібридності та синергізму. Представлено структуру класифікатора, що відображає гібридність та синергізм загроз. Пропонований метод, на відміну від існуючих, дозволяє давати оцінки рівня безпеки кіберфізичних систем і систем безпеки, що розвиваються, тобто виробляти динамічне оцінювання, а не статичне, як пропонувалося в попередніх дослідженнях.

ЛІТЕРАТУРА

[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] Основные результаты глобального исследования тенденций информационной безопасности за 2017 год. URL: https://www.pwc.ru/ru/publications / gsiss-2017.html.

[4] Антифишинг. Годовой отчет о защищенности сотрудников 2020. URL: https://antiphish.ru/tpost/88km7s0a01-otchyot-antifishinga-o-zaschischennosti.

[5] Gartner назвала 10 главных трендов в сфере кибербезопасности в 2021 году. URL: https://www.tadviser.ru /index.php.

[6] 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.

[7] 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. – doi:10.18372/2225-5036.22.10456.

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

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

[10] Петров О. Повышение информационной безопасности автоматизированных систем обработки данных на транспорте/Петров О., Лахно В. // Information Technology in Selected Areas of Management. – Widawnictwa AGH, Krakow 2016. – pp. 65-78.

[11] S. Pohasii and other (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies 3(9 (105)): pp. 6-19.

[12] S. Pohasii and other. Development of a method for assessing forecast of social impact in regional communities. Eastern-European Journal of Enterprise Technologies. 2021. 6/2 (114). pp. 30–47.

[13] 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.

[14] 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.

[15] 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.

[16] S. Pohasii and other. Development and analysis of game the theoretical models of security systems agents interaction. Eastern-European Journal of Enterprise Technologies . 2020. 2/4(104). pp. 15–29.

[17] S. Pohasii and other. Development of a method for assessing the security of cyber-physical systems based on the Lotka–Volterra model. Eastern-European Journal of Enterprise Technologies. 2021. 5/9 (113). pp. 30–47.

[18] KNX Technical Manual 2CKA001473B8668. KNX Technical Manual. Busch-Presence detector KNX / Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 2017. 198 p.

[19] Pohasii, Serhii and Yevseiev, Serhii and Zhuchenko, Oleksandr and Milov, Oleksandr and Lysechko, Volodymyr and Kovalenko, Oleksandr and Volkov, Andrii and Lezik, Aleksandr and Susukailo, Vitalii, Development of crypto-code constructs based on LDPC codes (April 30, 2022). Eastern-European Journal of Enterprise Technologies, 2(116), pp. 44–59. doi: 10.15587 / 1729-4061.2022.254545, Available at SSRN: https: // ssrn.com / abstract = 4100674.

[20] ABB i-bus KNX KNX Security Panel GM/A 8.1 Product Manual // Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 2016. – 648 p.

[21] Jürgen Schilder, Thorsten Reibel – ABB GPG Building Automation Webinar ABB i-bus® KNX Basics and Products. March 3, 2016 / Busch-WatchdogSky KNX. Busch-Jaeger Elektro GmbH, 2016. – 86 p.

[23] Manual for KNX Planning / Siemens Switzerland Ltd, 2017. – 100 p.

[24] Security Technology KNX-Intrusion Alarm System L240 Installation, Commissioning, Operation / Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 2010. – 116 p.

[25] Главные угрозы безопасности в облаке. URL: https://tadviser.com.

[26] Jorge Munilla, Mike Burmester, Raquel Barco. An enhanced symmetric-key based 5G-AKA protocol. Computer Networks. URL: https://doi.org/10.1016 /j.comnet.2021.108373.

[27] Abdulbasit Darem, Asma A. Alhashmi, Jemal H. A. Cybersecurity Threats and Countermeasures of the Smart Home Ecosystem. IJCSNS 22 (3), 303, 2022.

УДК 336.71:004.056

Pohasii S. Models and methods of information protection in cyberphysical systems.

Abstract. *The article presents a new approach to ensuring the security of information resources in cyber-physical systems. Today, such systems, as a rule, belong to objects of critical infrastructure. These systems are formed as a result of the integration of various elements of mobile communication technologies, classic computer networks and systems, as well as Internet of Things and Internet technologies. The work proposes consideration of the formation of the security system based on multi-contours, which allows considering two contours of the security system - internal (physical infrastructure of cyberphysical systems) and external (infrastructure of the control system based on cloud technologies). With the help of the developed classifier of threats to critical infrastructure objects, the formation of a classifier of attackers is ensured, in which its financial and computing capabilities are determined, which allows, based on the analysis of threats, to determine in a timely manner the degree of capabilities of attackers, as well as their intentions, and to form preventive protection measures. The use of the proposed protection models based on the Lotka-Volterra model allows considering the trends in the development of modern technologies, as well as the vector of cyber threats directed at critical infrastructure objects, which include modern cyberphysical systems. To ensure*

the security of information transmission through open channels of the cyber-physical systems network, information protection methods are proposed based on post-quantum algorithms – McEliece crypto-code constructions on LDPC codes, which allows to "close" the data transmission channels of the cyberphysical systems infrastructure.

Keywords: *cyberphysical systems, information security, cyber security, security of information, Lotka-Volterra security models, classifier of cyber-physical systems information threats, information protection system.*

Погасій Сергій Сергійович, кандидат економічних наук, доцент кафедри кібербезпеки та інформаційних технологій Національного технічного університету "Харківський політехнічний інститут".

Pogasii Serhii, candidate of economic sciences, associate professor of the department of cyber security and information technologies of the National Technical University "Kharkiv Polytechnic Institute".

Отримано *28 червня 2022 року,* затверджено редколегією *14 листопада 2022 року*