closed information, as well as means of generation and distribution of keys), means of security signaling and organizational access restriction, etc. In the work, models of the process of interaction of means of cyber-attacks with means of cyber protection were developed to ensure the basic characteristics of the security of resources of information systems in which, due to the amount of residual risk and variation in the mode of operation or unauthorized use of means of storage of information carriers ration and thereby violating its integrity, accessibility and confidentiality, allows to provide a quantitative and qualitative assessment of the state of cyber security. A model of the process of the interaction of protection means is also presented, in which, due to the use of the model of the process of the interaction of means of cyber-attacks with means of cyber protection and the decomposition of the basic security characteristics of information system resources and taking into account the relevant indicators of the basic security characteristics in the process of cyber protection of information system resources, it is possible to increase the accuracy of the dynamic assessment of efficiency dependence from the intensity of the effects of cyberattacks. The proposed cyber protection models make it possible to block cyber-attacks in information systems even before they start to act on the system. In this way, cyber defense can use its resources more effectively, which does not need to respond to every warning, since there can also be false warnings. The considered models make it possible to propose expressions for assessing the residual risk when protecting resources of basic safety characteristics in the form of probabilities of their violation and form the conditions for the transition of the protected resource to the mode of artificial failure.

Keywords: cyber security, information systems, cyber-attacks, security of resources, ensuring cyber security.

Хорошко Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Khoroshko Volodymyr, doctor of technical sciences, professor, professor of the department of security of information technologies of the National Aviation University.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Khokhlachova Yuliia, candidate of technical sciences, associate professor, associate professor of the department of security of information technologies of the National Aviation University.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Погорелов Володимир Володимирович, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Pogorelov Volodymyr, Candidate of Technical Sciences, Associate Professor of the Department of Security of Information Technologies of the National Aviation University.
E-mail: volodymyr.pogorelov@gmail.com.
Orcid ID: 0000-0002-6100-1504.

Аясрах Ахмад Расмі Алі, аспірант кафедри безпеки інформаційних технологій Національного авіаційного університету.

Ayasrah Ahmad, graduate student of the Department of Security of Information Technologies of the National Aviation University.
E-mail: ahmadaesr@gmail.com.
Orcid ID: 0000-0003-4392-1806.

DOI: 10.18372/2410-7840.24.16933
УДК:336.71:004.056

ОЦІНКА РІВНЯ БЕЗПЕКИ В КІБЕРФІЗИЧНИХ СИСТЕМАХ

Сергій Погасій

У статті наведений новий підхід оцінки ризиків та формування превентивних заходів безпеки на основі моделі Лотки-Вольтери. Запропоновані 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" дозволяють забезпечити погляд на можливість формування вектору загроз, а також їх залежність від розвитку цифрових

технологій та нових напрямків цифрових послуг. 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 гибридность сучасних загроз, фінансування на формування та вдосконалення системи захисту, а також дозволяє визначити фінансові та обчислювальні можливості зловмисника по виявленим загрозам. Механізм оцінки також враховує фізичну складову кіберфізичних систем, які формуються, як правило, з двох середовищ – фізичного рівня, та рівня управління. Такий погляд на кіберфізичні системи вимагає створення багатоконтурних систем захисту інформації, а також формування об'єктивності при оцінці загроз як на внутрішній (фізичний рівень) контур системи захисту інформації, так і на зовнішній контур (рівень управління). Пропонований метод оцінки безпеки кіберфізичних систем ґрунтується на базі розробленого класифікатора загроз, дозволяє оцінити поточний рівень безпеки і 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. При імітаційному моделюванні можуть використовуватися фактичні бази оцінки реальних загроз і інцидентів на кіберфізичні системи, що дозволяє провести експертну оцінку їх впливу як на окремі послуги безпеки, так і на складові безпеки (кібербезпека, інформаційну безпеку та безпеку інформації).

Ключові слова: *кіберфізичні системи, інформаційна безпека, кібербезпека, безпека інформації, моделі безпеки Лотки-Вольтери.*

Постановка проблеми

Розвиток кіберфізичних систем (КФС) дозволив суттєво поширити спектр цифрових послуг та забезпечити умови переходу до створення смарт-sity на основі комплексування смарт-технологій з мобільними технологіями бездротових каналів та Інтернет-речей [1-6]. Як правило КФС створюються на основі комплексування двох систем – системи управління (зовнішній рівень) та фізичної інфраструктури системи різноманітних програмно-апаратних та фізичних пристроїв (внутрішній рівень). Однак такий підхід створює можливість зламу не тільки окремих елементів інфраструктури КФС, а також можливість несанкціонованого керування елементами фізичної складової КФС за рахунок зламу та/або перехоплення та заміни управляючих команд систему управління, яка створюється за допомогою хмарних технологій. Аналіз загроз свідчить [3-9] про необхідність не тільки формування об'єктивності оцінки загроз на КФС в цілому, а також формування нових підходів щодо створення двох або багатоконтурних систем безпеки, що потребує моделювання процесів нападу та превентивних заходів безпеки в умовах динамічного зростання кількості інцидентів, появи повномасштабного квантового комп'ютера, а також ознак синергізму та гібридності АРТ-загроз на КФС. 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. Однак поділ безпеки на окремі складові: інформаційну безпеку, кібербезпеку, безпеку інформації в нормативних регуляторах призводить до формування у кожній зі своїх моделей [8, 9]. Такий підхід не дозволяє забезпечити облік гібридності та синергізму загроз, можливості їх комплексування з методами соціальної інженерії та формуванням цільових атак. Одним із напрямків, що забезпечує формування концептуальної основи побудови систем безпеки КФС є модель зрілості безпеки [1, 2]. При цьому під зрілістю безпеки розуміється ступінь впевненості в тому, що стан безпеки відповідає всім потребам організації та вимогам, пов'язаним з безпекою [1]. Зрілість безпеки забезпечує як оцінку поточного рівня безпеки, його необхідність, переваги, а й витрати з його підтримку. Фактори, які необхідно зважити в такому аналізі, включають конкретні загрози галузевої вертикалі організації, нормативні вимоги, унікальні ризики, що існують у середовищі, та профіль загроз організації [1]. Однак побудова системи безпеки пропонується будувати за ієрархічною структурою з подальшим дробленням на сегменти безпеки.

Крім того, в такій моделі не враховуються можливості зловмисників формувати свої мережі, протистояти один одному при реалізації загроз на одну "жертву". Таким чином, виникає необхідність своєчасної оцінки поточного стану рівня безпеки кіберфізичних систем в умовах сучасних загроз, з урахуванням синтезу елементів інфраструктури ІКС з Інтернет-речами в умовах динамічної зміни обставин.

Аналіз останніх досліджень і публікацій

Аналіз оцінки сучасного вектору загроз [3, 4] стверджує про його неуклонний шлях за розвитком найбільш поширених цифрових послуг на основі бездротових каналів зв'язку мобільних технологій, створення комплексування як з Інтернет-речами КФС, так й з смарт-технологіями. Аналіз моделей побудови систем захисту [6-10] показав, що склався підхід, що ґрунтується на представленні процесу її обробки у вигляді абстрактного обчислювального середовища.

У цьому середовищі функціонує множина суб'єктів (користувачів та процесів) одночасно з безліччю об'єктів (ресурси та набори даних). При цьому побудова системи захисту полягає у створенні захисного середовища у вигляді деякої множини обмежень і процедур. Воно має бути здатне під управлінням ядра безпеки заборонити несанкціонований та реалізувати санкціонований доступ суб'єктів до об'єктів та захист останніх від навмисних та випадкових зовнішніх та внутрішніх загроз.

Цей підхід спирається на теоретичні моделі безпеки Хартсона, Белла-Лападули, MMS Лендвера та Мак Ліна, Біба, Кларка-Вілсона та ін. і має статичний характер. Вважається, що перелічені моделі є інструментарієм при розробці безпекових політик, що визначають безліч вимог, які повинні бути виконані в конкретній реалізації системи. Разом з тим, бурхливе зростання кіберфізичних систем Інтернет-речей формує мультисистеми, які, з одного боку, розширюють спектр цифрових послуг, а з іншого – спрощують проведення цільових кібератак.

Другим підходом є використання принципу достатності в рамках запобіжної стратегії захисту, коли на етапі проєктування оцінюються потенційно можливі загрози та реалізуються механізми захисту від них. Однак інфраструктура сучасних ІКС тісно пов'язана з елементами кіберфізичних та Інтернет-речових систем, що значно ускладнює забезпечення безпеки у таких системах та мережах.

Одним з рішень, запропонованих у [7], є використання концепції побудови системи безпеки на основі моделі зрілості безпеки інтернету речей (IIC IoT Security Maturity Model, IoT SMM). Системний підхід до вибору варіантів захисту забезпечується об'єднанням у відповідні домени практик щодо ефекту від їх застосування: управління безпекою та організаційні заходи (Governance); забезпечення безпеки через конструкцію (by design, Enablement); зміцнення безпеки (Hardening) [7]. Модель дозволяє зробити правильний вибір заходів та засобів безпеки, сформувати архітектуру вибору на основі ієрархії практик забезпечення безпеки (security practices). Однак істотним недоліком такої системи може стати зламування верхньорівневих доменів з подальшою ланцюговою реакцією злому всієї системи в цілому, відсутність обліку синергізму і гібридності цільових атак та їх модифікацій.

Перспективним напрямом формування систем безпеки є динамічні моделі, проте часто їх використання практично неможливе через нерозуміння керівництвом їхньої доцільності, значним зростанням економічних та обчислювальних витрат порівняно з класичними (стаціонарними) моделями. Особливий інтерес у цьому напрямі відіграє модель та її модифікації Лотки-Вольтери ("хижак-жертва"), що дозволяє враховувати не лише технічні та економічні аспекти при побудові системи безпеки, а й враховувати можливість "конкуренції" зловмисників, формування мереж для цільових атак. на "жертву".

У роботі [8] наведено математичний апарат використання моделі Лотки-Вольтери у різних галузях – від навколишнього середовища, політології, біології, медицини та фізики. Однак відсутність досліджень їх реалізації не дозволяє використовувати дані моделі у сфері безпеки. У роботах [10, 11] наведено дослідження різних моделей забезпечення кібербезпеки на основі моделі Лотки-Вольтери. Запропонований підхід дозволяє визначити вектори кіберзагроз, проте без урахування їх синергізму та гібридності, комплексування з методами соціальної інженерії, що суттєво знижує їхню практичну цінність. У [12, 13] кіберпростір розглядається як цифрова екосистема, в якій системи можуть адаптуватися та розвиватися, що дозволяє системній інженерії створювати "види", які функціонують та адаптуються у цій екосистемі. Проте автори не зважають на тенденції розвитку обчислювальних ресурсів, можливості

зловмисників, що не дозволяє адекватно використовувати даний підхід у сучасних умовах. У роботі [14] досліджується аналогія "хижак-жертва" для Інтернету та представлені результати про те, як різні рівні диверсифікації видів впливають на стійкість мережі, а також обговорюватиметься зв'язок між диверсифікацією, конкуренцією, антимонопольним законодавством та національною безпекою. У [15, 16] пропонується аналогії між шкідливими програмами та екологічними принципами поведінки "видів" – посередництво, паразитизм, хижацтво та регулювання популяції залежно від щільності. Однак відсутність досліджень сучасних загроз, їх модифікацій та поява нових не забезпечує необхідний рівень вірогідність при оцінці безпеки CFS. У [17] авторами пропонується спрощення моделі Лотки-Вольтери шляхом використання функції модуляції. Функція множиться на обидві сторони моделі Лотки – Вольтера, і модель перетворюється на лінійні рівняння з параметрами, які мають оцінюватися методом дробового інтегрування. У [18] автори пропонують аналіз моделі "хижак-жертва" на основі характеристик, таких, як ефект Аллі, ефект страху, канібалізм та імміграція. Однак у роботах [17–23] не враховуються зміни вектора кіберзагроз, їх гібридність та синергізм, що дозволяє отримувати емерджентний ефект при реалізації цільових атак.

У роботі [20] запропоновано концептуальний підхід використання моделі Лотки-Вольтери в описі взаємозв'язків та основних елементів інфраструктури системи інформаційної безпеки під час реагування на інциденти. Проте автори розглядають лише використання моделі в одній зі складових безпеки, без урахування комплексування загроз із методами соціальної інженерії, ознаками гібридності та синергізму. У роботі [21] пропонується використовувати модель Лотки-Вольтери для оцінки залежності захисту персональних даних від обсягу інформації в системі та довіри до соціальних мереж. Авторами в результаті досліджень доведено, що залежність захисту персональних даних від довіри пропорційна при постійних інших параметрах захисту. Однак при оцінці загроз не розглядаються тенденції їх розвитку та вдосконалення, зв'язок із методами соціальної інженерії, що не дозволяє враховувати можливість синергізму та гібридності загроз.

Отже, виникає необхідність розгляду цього підходу (використання моделі "хижак-жертва") з урахуванням сучасного розвитку обчислювальних ресурсів, фінансових можливостей як зловмисників, і захисників. Необхідно також враховувати зміни вектора цільових атак з урахуванням їхньої гібридності та синергізму за всіма складовими безпеки.

Основні матеріали дослідження

Для оцінки безпеки кіберфізичних систем в умовах впливу сучасних цільових кіберзагроз з ознаками гібридності та синергізму враховується їхнє комплексування з методами соціальної інженерії на елементи інфраструктур. При цьому в класичній моделі Лотки-Вольтери використовуються основні підходи на основі наступних парадигм:

– за відсутності "хижаків" "жертви" експоненційно розмножуються;

– за відсутності "жертв" "хижаки" експоненційно вимирають.

При цьому, як правило, у роботах [12-22] у рамках "жертви" розглядаються інциденти ІБ/зловмисники, а як "хижака" – заходи захисту/елементи системи захисту. Це нелогічно з погляду екосистеми, під якою розуміється кіберпростір. Математично модель "хижак-жертва" можна описати як [22]:

$$\begin{cases} \frac{dN_1}{dt} = \alpha N_1 - \beta N_1 N_2; \\ \frac{dN_2}{dt} = -\varphi N_2 + \gamma N_2 N_1, \end{cases} \quad (1)$$

де N1 – чисельність жертв, N2 – чисельність хижаків, α – коефіцієнт народжуваності жертв, β – коефіцієнт впливу хижака на жертву (коефіцієнт хижацтва), φ – коефіцієнт смертності хижака, γ – коефіцієнт впливу жертви на хижака.

Однак для оцінки безпеки кіберфізичних систем пропонується використовувати такі поняття:

– "жертва" – система або елемент системи/інфраструктури інформаційно-комунікаційної системи/кіберфізичної системи, яка піддається цільовим загрозам з ознаками синергізму та гібридності;

– "хижак" – цільова загроза або загроза на окремі складові безпеки (кібербезпеки (КБ), інформаційної безпеки (ІБ), безпеки інформації (БІ)) на систему або елемент системи/інфраструктури інформаційно-комунікаційної системи/кіберфізичної системи або системи Інтернет-речей.

Для визначення взаємозв'язків між "жертвою" та "хижаком" використовується класифікатор заг-

роз та етапи експертної оцінки, запропоновані в роботі [22]. Такий підхід дозволяє враховувати характеристики та ознаки сучасних загроз, мінімізацію коштів на підтримку систем захисту інформації (ЗЗІ) з урахуванням безперервності бізнес-процесів.

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

Для використання моделі "хижак-жертва" для моделювання динаміки функціонування та оцінки кіберфізичних систем необхідно не лише дати предметну інтерпретацію базової моделі в термінах та поняттях системи безпеки, але й виконати параметризацію моделі. Інакше кажучи, необхідно визначити значення коефіцієнтів, які входять у рівняння моделі, і навіть задати початкові значення досліджуваних змінних.

Параметризацію моделі почнемо з першого її рівняння.

Оцінку чисельності елементів захисту контуру безпеки безперервності бізнес-процесів виконаємо, виходячи з таких припущень:

1. Загрози спрямовані на відповідні послуги безпеки, які у класифікаторі загроз представлені 3-ю платформою [22].

2. Для кожної з послуг безпеки в контурі захисту є засоби, які забезпечують ці послуги. Розподіл цих засобів по діапазону послуг, що розглядається, описується вектором де, наприклад, – ваговий коефіцієнт, який забезпечує послугу конфіденційності, – ваговий коефіцієнт, який забезпечує послугу цілісності; – ваговий коефіцієнт, що забезпечує послугу доступності управління; – ваговий коефіцієнт, що забезпечує послугу автентичності; – ваговий коефіцієнт, що забезпечує послугу власності. При цьому виконується рівність де j – послуги безпеки, і – загроза елементам інфраструктури КФС.

3. Загроза вважається гібридною, якщо вона спрямована одночасно на всі безпекові послуги.
Чисельність об'єктів, що представляють цілі атак з урахуванням їхньої гібридності, може бути представлена таким чином:

$$\tilde{N}_1 = \sum_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix}, \quad (2)$$

де індекси змінних відповідають основним послугам безпеки: C – конфіденційність; I – цілісність; A – доступність; Au – автентичність, Aff – причетність (приналежність); – кількість об'єктів, які забезпечують послугу безпеки, як конфіденційність; для інших служб безпеки – аналогічно; Q – загальна кількість відомих кіберзагроз. Припускаємо, що коефіцієнт впровадження нових елементів СЗІ відповідає рівню захищеності елементів, що забезпечують послуги безпеки КФС. Рівень безпеки, згідно [22, 23] оцінюється у відносних одиницях: 1 – відповідає максимальному рівню безпеки, що забезпечується системою безпеки; 0 – система безпеки не забезпечує захист інформаційних ресурсів.

Припускатимемо, що вартість проведення атак та вартість заходів щодо захисту від них мають нормальний розподіл.

У цьому випадку ймовірність реалізації загрози при максимальних можливостях захисту A та нападу B визначатиметься різницею щільності ймовірності F(B)–F(A), де A – граничні можливості захисту, B – граничні можливості реалізації атаки сторони нападу. За цих припущень величина S=F(B)–F(A) визначає частку незахищених цілей, на які можуть бути спрямовані кібератаки. Тоді рівень безпеки визначиться як частка інформаційних ресурсів, захищених від кібератак. Ця величина може бути обчислена як:

$$S = 1 - F(B) - F(A) = \\ = \int_{-\infty}^{B} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)} dt - \int_{-\infty}^{A} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)} dt, \quad (3)$$

де S – рівень безпеки системи, F(B) та F(A) – частки ресурсів сторін кіберконфлікту, t – змінна інтегрування, що визначає рівень доступних ресурсів "хижака" та "жертви", μ та σ – величини, що визначають математичне очікування та дисперсію статистичного розподілу ресурсів, що мають у сторін.

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

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

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

де – множина потенційних загроз, реалізація яких ефективна атакуючого; – загроза і-му інформаційному ресурсу; – оцінка вартості успішності реалізації

атаки на і-й ресурс з боку атакуючого; – вартість проведення атаки на і-й ресурс з боку атакуючого.

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

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

3 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:

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

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

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

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

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

Тоді коефіцієнт народжуваності "жертв" пропонується розраховувати, як:

$$\alpha = \frac{\left| \{ Tr_l \} \right|}{Q}. \quad (9)$$

Для оцінки впливу сучасних загроз на засоби захисту скористаємося виразом у роботі [23], тоді коефіцієнт β уявімо як:

$$\beta = \sum_{i=1}^{M} \left(w_{CPSi}{}^{C} \cap w_{CPSi}{}^{I} \cap w_{CPSi}{}^{A} \cap w_{CPSi}{}^{Au} \cap w_{CPSi}{}^{Aff} \right) \chi_i^{CPS}. \quad (10)$$

Для визначення коефіцієнта обчислювальних можливостей зловмисника φ, скористаємося класифікацією зловмисників, як представлено у роботі [23], та представимо як:

$$\varphi = \frac{1}{M} \sum_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv}. \quad (11)$$

У табл. 1 наведено вихідні дані критеріїв та показників експертної оцінки його знаходження.

Таблиця 1

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

Категорія	показники оцінки вагового коефіцієнта				
	$\beta_i^{CPS} \in \left\{ \beta_i^{CPS} \right\}$			prj	rmotiv
	W_{op}^{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:

$$\gamma^j = \frac{1}{K \times B} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right). \quad (12)$$

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:

$$\begin{cases} \frac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum\limits_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix} \right) - \\ - \left(\sum\limits_{i=1}^{M} \begin{pmatrix} w_{CPSi}{}^C \cap w_{CPSi}{}^I \cap w_{CPSi}{}^A \cap \\ \cap w_{CPSi}{}^{Au} \cap w_{CPSi}{}^{Aff} \end{pmatrix} \chi_i^{CPS} \right) \times \\ \times \tilde{N}_1 \left(N_2 \times \left| W_{\text{hybrid } C,I,A,Au,Af \text{ synerg}} \right| \right); \\ \frac{dN_2}{dt} = - \left(\frac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \tilde{N}_2 + \\ + \left(\frac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \tilde{N}_2 \tilde{N}_1. \end{cases} \quad (13)$$

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

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

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

$$\begin{cases} \frac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum\limits_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix} \right) - \\ - \left(\sum\limits_{i=1}^{M} \begin{pmatrix} w_{CPSi}{}^C \cap w_{CPSi}{}^I \cap w_{CPSi}{}^A \cap \\ \cap w_{CPSi}{}^{Au} \cap w_{CPSi}{}^{Aff} \end{pmatrix} \chi_i^{CPS} \right) \times \\ \times \tilde{N}_1 \left(\tilde{N}_2^1 \cap \tilde{N}_2^2 \cap \ldots \cap \tilde{N}_2^w \right); \\ \frac{dN_2}{dt} = - \left(\frac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \times \\ \times \left(\tilde{N}_2^1 \cap \tilde{N}_2^2 \cap \ldots \cap \tilde{N}_2^w \right) + \left(\frac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \times \\ \times \left(\tilde{N}_2^1 \cap \tilde{N}_2^2 \cap \ldots \cap \tilde{N}_2^w \right) \tilde{N}_1, \end{cases} \quad (14)$$

де кількість "хижаків" належить множині $\overline{\left\{ \tilde{N}_2^j \right\}}, j \in 1, \ldots w.$

Таким чином, 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.

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.

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 конкретність "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.

Запропонована модель безпеки кіберфізичних систем на основі моделі "хижак-жертва" дозволяє враховувати можливості групування зловмисників/кібергруп з метою досягнення цілей кібератаки.

$$\begin{cases} \frac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum\limits_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix} \right) - \\ - \left(\sum\limits_{i=1}^{M} \begin{pmatrix} w_{CPSi}{}^C \cap w_{CPSi}{}^I \cap w_{CPSi}{}^A \cap \\ \cap w_{CPSi}{}^{Au} \cap w_{CPSi}{}^{Aff} \end{pmatrix} \chi_i^{CPS} \right) \tilde{N}_1 \left(\sum\limits_{j=1}^{w} \tilde{N}_2^w \right); \\ \frac{dN_2}{dt} = - \left(\frac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \left(\sum\limits_{j=1}^{w} \tilde{N}_2^w \right) + \\ + \left(\frac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \left(\sum\limits_{j=1}^{w} \tilde{N}_2^w \right) \tilde{N}_1, \end{cases} \quad (15)$$

Такий підхід дозволяє прогнозувати "найгірші" варіанти розвитку кібератаки, а також формувати відповідні превентивні заходи.

Розробка моделі безпеки кіберфізичних систем на основі моделі "хижак-жертва" з урахуванням взаємозв'язків між "видами жертв" та "видами хижаків"

У роботі [21] авторами розглядається m-мірний випадок, у якому враховуються взаємодії у "середовищі" "хижаків", і навіть взаємодії у "середовищі" "жертв". Така модель цікава насамперед з погляду взаємодії "жертв", під якими розуміються засоби/механізми ЗЗІ. При цьому враховується одним із принципів формування СЗІ – принцип достатності. У пропонованій моделі:

$$\tilde{N}_i = N_i \cdot f(N), \qquad (16)$$

де $f(N) = r + \|A\| \times N$, N_1, …, N_m – розміри популяцій m-різних видів "хижаків" і "жертв", які взаємодіють в одному середовищі, N – вектор, складений із цих невідомих. Параметри у векторі r відповідають за успіх (імовірність) "народжуваності" (появі нових кіберзагроз, або засобів захисту відповідно від видів) (r_i>0) або "смертності" (r_i<0). Матриця $\|A\|$ описує взаємовідносини між "хижаками" чи "жертвами" різних видів, у своїй [21]: a_{ij} – описує вплив виду j з вигляду i, a_{ji} – вплив виду і з вигляду j. Якщо ж a_{ij}>0, a_{ji}<0, то вигляд і буде хижаком, а вид j – жертвою йому. Значення aii – описують вплив виду самого себе. З урахуванням викладених припущень модель "хижак-жертва" представимо як:

$$\begin{cases} \frac{dN_1}{dt} = \left(\arg \max_{\forall Tr_j \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum_{i=1}^{Q} \left(\begin{array}{l} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{array} \right) \right) - \\ - \left(\sum_{i=1}^{M} \left(\begin{array}{l} w_{CPSi}{}^C \cap w_{CPSi}{}^I \cap w_{CPSi}{}^A \cap \\ \cap w_{CPSi}{}^{Au} \cap w_{CPSi}{}^{Aff} \end{array} \right) \chi_i^{CPS} \right) \times \\ \times \tilde{N}_1 \left(\sum_{j=1}^{w} \tilde{N}_2^w \right) - \varepsilon \tilde{N}_2^2; \\ \frac{dN_2}{dt} = -\left(\frac{1}{M} \sum_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \left(\sum_{j=1}^{w} \tilde{N}_2^w \right) + \\ + \left(\frac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \left(\sum_{j=1}^{w} \tilde{N}_2^w \right) \tilde{N}_1 - \xi \tilde{N}_2^2. \end{cases} \qquad (17)$$

Розробка методу оцінки безпеки кіберфізичних систем на основі моделі Лотки-Вольтери "хижак-жертва"

Однією з особливостей кіберфізичних систем є відсутність СЗІ в елементах інфраструктури, передача сигналів від датчиків/сенсорів по відкритих каналах та забезпечення управління та адміністрування на основі хмарних технологій. Це суттєво знижує можливості формування контуру безпеки та призводить до збільшення критичних точок для реалізації кібератак. У таких умовах оцінку безпеки необхідно проводити в офлайн режимі, що дозволяє враховувати динаміку як кіберзагроз, з одного боку, так і можливість засобів захисту, протистояти їм.

На рис. 1 наведена структурна схема запропонованого методу оцінки.

На першому етапі. 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.

На другому етапі. На основі аналізу етапу 1, вибирається модель Лотки-Вольтери, і за формулами (2)-(17) розраховуються відповідні коефіцієнти та складові виразів.

На третьому етапі на основі виразів (18)-(20) визначається поточний стан безпеки кіберфізичної системи.

Практичне використання запропонованого методу.

Розглянемо можливість формування об'єктивної оцінки потокового стану у кіберфізичної системі на основі запропонованих моделей та можливість модифікації (удосконалення) системи захисту інформації КФС на прикладі "Розумний будинок". Такі КФС потребують формування двох системи захисту – фізичний рівень КФС (внутрішній контур захисту),рівень управління КФС на основі хмарних технологій (зовнішній рівень). На рис. 2 наведена можливість використання запропонованих моделей для оцінки ймовірнісних загроз на фізичний та рівень управління КФС.

Проведений Аналіз показує, що для отримання об'єктивності потокового стану загроз на КФС

необхідно використовувати всі моделі Лотки-Вольтери.

Таким чином узагальнений показник формується шляхом перетину отриманих результатів кожної з моделей (13)–(17):

$$W_{\text{general}}^{CPS} = W_1^{CPS} \cap W_{21}^{CPS} \cap W_3^{CPS} \cap W_4^{CPS} \cap W_5^{CPS},$$

де W_{general}^{CPS} – узагальнений показник загроз, $W_1^{CPS}, W_{21}^{CPS}, W_3^{CPS}, W_4^{CPS}, W_5^{CPS}$ – відповідні моделі Лотки-Вольтери.

Рис. 1. Структурна схема запропонованого методу оцінки

Для оцінки кожної моделі необхідно враховувати наступне:

1. Описовою характеристикою зміни поточного стану безпеки КФС є його інтенсивність *l(t)* – середня кількість змін, що відбулися із поточним станом безпеки КФС в одиницю часу. Оцінку інтервалів $\Delta t_{[i-q]}$ між змінами, рівня безпеки КФС використовуємо формулу:

$$\Delta t_{[i-q]}(t) = \frac{K}{l(t)}, \qquad (18)$$

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

2. Функція переходів рівня безпеки КФС зі стану *k* в стан *j* оцінимо за формулою:

$$\Pi = S_0^I \times value \to S^I. \qquad (19)$$

3. Зміни рівнів безпеки визначається у вигляді кінцевого автомата H^{CPS}, стан якого описує формула:

$$H^{CPS} = \langle S^I, value, \Pi, S_0^I \rangle, \qquad (20)$$

де S^I - кінцевий стан рівня безпеки КФС;
value – значення змін рівня безпеки КФС;
П – функція переходів рівня безпеки КФС зі стану *k* до стану *j*;
S_0^I – початковий стан рівня безпеки КФС.

4. Формування метричних коефіцієнтів загроз, що обчислюються як:

$$w_j^{CPS} = \frac{1}{K} \sum_{i=1}^{Q} \sum_{k=1}^{K} w_{ijk}^{CPS}, \qquad (21)$$

де $w^{C}_{CPSi}, w^{I}_{CPSi}, w^{A}_{CPSi}, w^{Au}_{CPSi}, w^{Aff}_{CPSi}$ – експертні вагові коефіцієнти послуг безпеки: конфіденційності, цілісності, доступності, автентичності та причетності, як було зазначено раніше.

Пропонується для формування вагових коефіцієнтів впливу кіберзагрози на послуги безпеки експертам у роботі [23] використовувати значення $w^{CPS}_{j} \in \{0;\ 0{,}1;\ 0{,}25;\ 0{,}33;\ 0{,}5;\ 0{,}66;\ 0{,}75;\ 0{,}9;\ 1\}$.

5. Розподіл технічних засобів СЗІ визначається як:

$$\lambda^{CPS\ CIF}_{j} = N^{j}_{1} \times w^{CPS\ CIF}_{j}, \qquad (22)$$

де j – послуга безпеки, N^{j}_{1} – чисельність об'єктів "жертви" (технічних засобів СЗІ). Обмеженням у моделюванні є припущення, що технічні засоби СЗІ не можуть забезпечувати декілька послуг безпеки.

6. Для визначення вартісних показників атак використовуємо таблицю розміру можливих втрат методики оцінки ризиків FAIR (Factor Analysis of Information Risk) [24, 25]. Витрати зловмисників на проведення атак оцінюватимемо, виходячи з припущення, що вони становлять не більше 10% від розміру можливих втрат жертви (табл. 2).

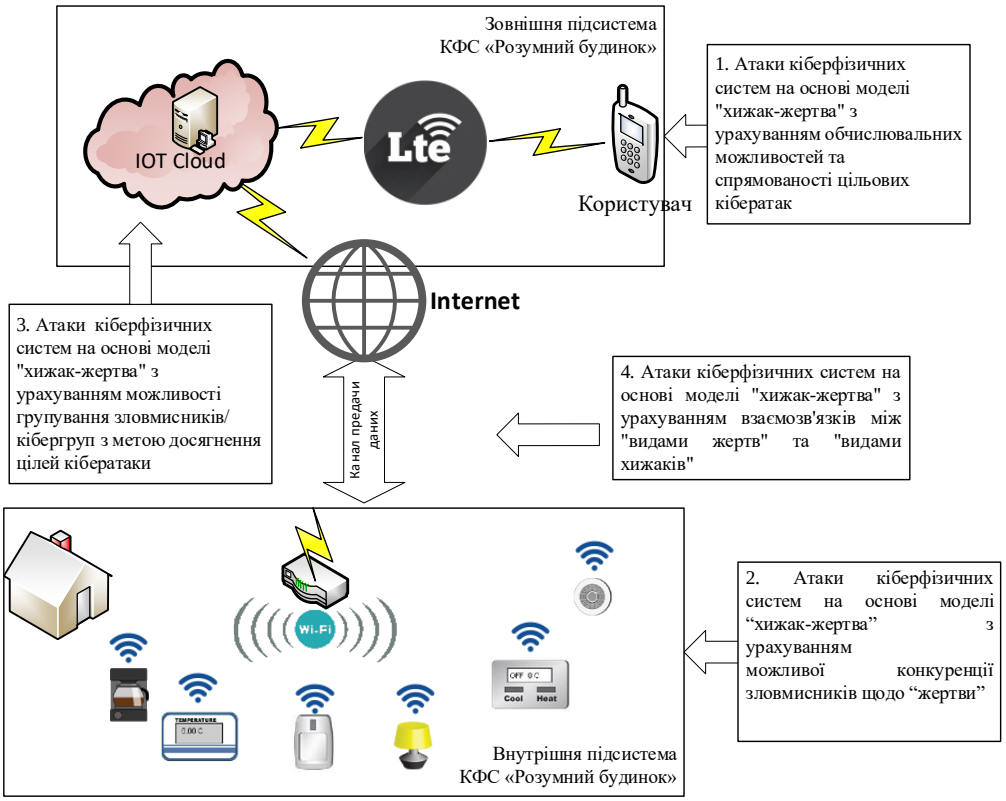

Рис. 2. Структурна схема загроз на основі моделей Лотки-Вольтери

На рис.3. наведена структурна схема формування двоконтурної системи захисту КФС "Розумний будинок".

Модифікована КФС "Розумний будинок" управляє комплексом автономних систем, кожна з яких управляє певними пристроями в будинку, з'єднуючи їх у загальну систему, що дозволяє зручно керувати кожною окремо, застосовувати різні протоколи автоматизації, а також має можливість повністю автономної роботи.

На рис. 3 у модифікованій КФС "Розумний будинок" наведено два контури обробки та передачі інформації.

Внутрішній контур містить дві основні підсистеми:

- підсистема вимірювання збирає інформацію з усіх датчиків про фізичний стан будинку;
- підсистема управління подає захищенні команди на сам пристрій, яким керує система- локальний сервер.

Таблиця 2

Розмір можливих втрат (PLM) (дол.)

№	втрати	нижня межа	верхня межа
1	критичні (SV)	10 000 000	–
2	високі (H)	1 000 000	9 999 999
3	значні (Sg)	100 000	999 999
4	середні (M)	10 000	99 999
5	малі (L)	1 000	9 999
6	гранично малі (VL)	0	999

Кожна підсистема вимірювання є пристрій, який може працювати повністю автономна, незалежно від загальної системи розумний будинок, керуючи певною його частиною з можливістю прямого захищеного керування через смартфон або комп'ютер. Кожна підсистема вимірювання відправляє пакет даних на локальний сервер, що дозволяє управляти домом без інтернету, перебуваючи в тій же локальній мережі (будучи підключеним до WI-FI-роутеру). Для забезпечення захисту бездротових каналів пропонується використовувати постквантові алгоритми на основі несиметричних криптосистем, які будуються на основі крипто-кодових конструкцій Мак-Еліса та Нідеррайтера.

Використання крипто-кодових конструкцій забезпечує основні послуги безпеки: конфіденційність, цілісність та автентичність. Крім цього, крипто-кодові конструкції інтегровано забезпечують необхідний рівень стійкості (також в умовах появи повномасштабного квантового комп'ютера), оперативність (швидкість шифрування порівнянна зі швидкістю криптоперетворень у сучасних блокових шифрах) та достовірність (за рахунок використання завадостійких кодів при побудові несиметричних криптосистем). З урахування рівня (степені) секретності в запропонованих крипто-кодових конструкціях можливе використання різноманітних кодів: еліптичних кодів, модифікованих еліптичних кодів, LDPC та збиткових кодів. Використання двох симетричних систем дозволяє підвищити рівень системи захисту як min у 2 рази.

Інформація в мережі внутрішнього контуру КФС "Розумний будинок" передається відкритими бездротовими каналами з шифруванням на основі крипто-кодовій конструкції (ККК) Нідеррайтера на завадостійких кодах.

При управлінні модифікованою КФС "Розумний будинок" з зовнішнього середовища (Internet) в систему додається зовнішній контур взаємодії з іншими системами. В цьому випадку інформація, що була отримана з датчиків та оброблена в локальному сервері (який фізично знаходиться в будинку), передається за інтернет з'єднанням, до кінцевого споживача застосовуючи алгоритми шифрування на основі ККК Мак-Еліса на LDPC-кодах.

Таким чином, при реалізації цієї концепції, відпадає необхідність у використанні Хмарних обчислень, що у свою чергу нівелює атаки кіберфізичних систем на основі моделі "хижак-жертва" з урахуванням можливості групування зловмисників з метою досягнення цілей кібератаки, та зменшує потенціал атак кіберфізичних систем на основі моделі "хижак-жертва" з урахуванням взаємозв'язків між "видами жертв" та "видами хижаків" за рахунок впровадження алгоритмів шифруванням на основі ККК Мак-Еліса на LDPC-кодах. Також зменшується можливість проникнення до внутрішнього контуру модифікованою КФС «Розумний будинок» використовуючи атаки кіберфізичних систем на основі моделі "хижак-жертва" з урахуванням можливої конкуренції зловмисників щодо "жертви".

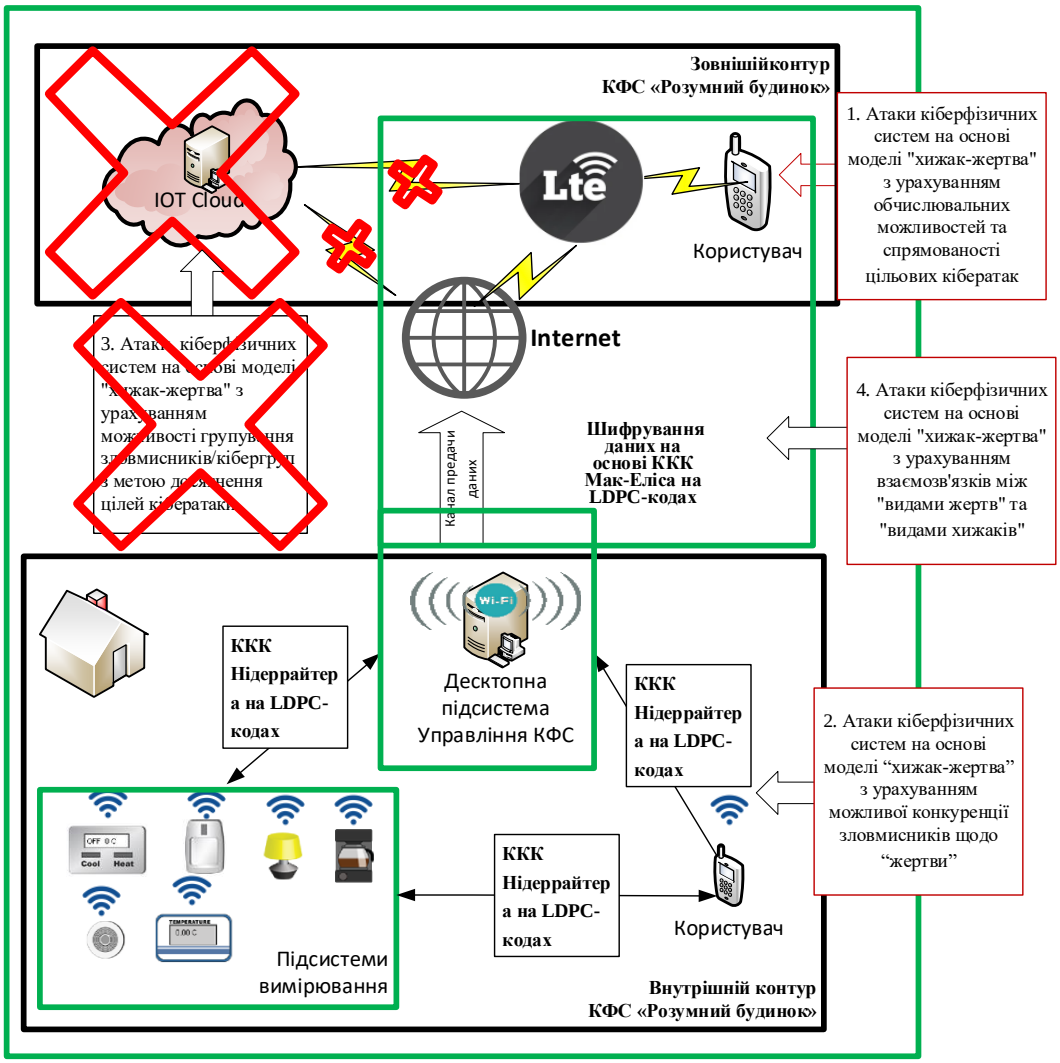

Рис. 3. Структурна схема побудови двоконтурної системи захисту у КФС "Розумний будинок"

ВИСНОВКИ

1. Розроблено моделі безпеки кіберфізичних систем з урахуванням обчислювальних можливостей та спрямованості цільових кібератак, можливої конкуренції зловмисників стосовно "жертви". Моделі також показують можливості групування з метою досягнення цілей кібератаки, взаємозв'язків між "видами жертв" та "видами хижаків". На основі пропонованого підходу отримані коефіцієнти моделі Лотки-Вольтери α=0,39, β=0,32, γ=0,29, φ=0,27, які враховують синергізм та гібридність сучасних загроз, фінансування на формування та вдосконалення системи захисту, а також дозволяє визначити фінансові та обчислювальні можливості зловмисника щодо виявлених загроз.

2. Модифікація моделі "хижак-жертва" дозволяє як групувати "види жертв", а й "види хижаків", що впливає як формування колективного захисту, а й отримувати синергетичний ефект кіберзагроз з метою досягнення цілей кібератаки з урахуванням взаємозв'язків між "видами жертв" та "видами хижаків".

3. Розроблено метод оцінки безпеки кіберфізичних систем на основі моделі Лотки-Вольтери "хижак-жертва". Метод ґрунтується на базі запропонованого класифікатора загроз з урахуванням їх гібридності та синергізму. Пропонований метод дозволяє давати оцінки рівня безпеки кіберфізичних систем і систем безпеки, що розвиваються, тобто виробляти

динамічне оцінювання, а не статичне, як пропонувалося в попередніх дослідженнях.

4. Запропонований підхід формування многоконтурних систем захисту інформації КФС дозволяє сформувати об'єктивну оцінку загроз та своєчасно визначити необхідні превентивні заходи протидії APT-загрозам. Формування двох контурів безпеки забезпечує необхідний рівень захищеності та забезпечення основних послуг безпеки на основі постквантових несиметричних криптосистем – ККК Мак-Еліса та Нідеррайтера.

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] 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.

[6] 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.

[7] Модель зрелости безопасности интернета вещей: толчок к развитию безопасных систем. URL: https://ics-cert.kaspersky.ru/reports/ 2019/08/14/the-internet-of-things-security-maturity-model-a-nudge-for-iot-cybersecurity/.

[8] Д.И. Трубецков, Феномен математической модели Лотки-Вольтерры и сходных с ней. URL: https://andjournal.sgu.ru/ru/articles/fenomen-matematicheskoy-modeli-lotki-volterry-i-shodnyh-s-ney.

[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] Кононович І. Динаміка кількості інцидентів інформаційної безпеки. Informatics and Mathematical Methods in Simulation. Vol. 4 (2014), № 1, pp. 35–43.

[11] І.В. Кононович, Д.А. Маєвський, Р.С. Подобний. Моделі забезпечення кібербезпеки із запізнюванням реагування на інциденти. Informatics and Mathematical Methods in Simulation.Vol. 5 (2015), № 4, pp. 339–346.

[12] Lippert, K.J.; Cloutier, R. Cyberspace: A Digital Ecosystem. // Systems 2021, 9, 48. URL: https://doi.org/10.3390/systems9030048.

[13] Mazurczyk,W.; Drobniak, S.; Moore, S. Towards a Systematic View on Cybersecurity Ecology. URL: https://arxiv.org/ftp/arxiv/papers/1505/1505.04207.pdf.

[14] Gorman, S.P.; Kulkarni, R.G.; Schintler, L.A.; Stough, R.R. A Predator Prey Approach to the Network Structure of Cyberspace. URL: https://www.researchgate.net/publication/255679706_A_predator_prey_approach_to_the_network_structure_of_cyberspace.

[15] Fink, Glenn A., Haack, Jereme N., McKinnon, Archibald D., and Fulp, Errin W. Defense on the Move: Ant-Based Cyber Defense. United States: N. p., 2014. Web. doi:10.1109/MSP.2014.21.

[16] Crandall J R, Ladau J, Ensafi R, Shebaro B, Forrest S, The Ecology of Malware, Proceedings of the New security paradigms Workshop (NSPW '08), pp. 99–106, Lake Tahoe, CA, USA.

[17] Lifeng Wu and Yinao Wang. Estimation the parameters of Lotka-Volterra model based on grey direct modelling method and its application. Expert Syst. Appl. 38, 6 (2011), 6412-6416. DOI=10.1016/j.eswa.2010.09.013. URL: http:// dx.doi.org/10.1016/j.eswa.2010.09.013.

[18] Diz-Pita, É.; Otero-Espinar, M.V. Predator–Prey Models: A Review of Some Recent Advances. Mathematics 2021, 9, 1783. URL: https:// doi.org/10.3390/math9151783.

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

[20] В.А. Минаев Математическая модель "хищник–жертва" в системе информационной безопасности. URL: http://runsec.ru/art51/.

[21] Я догоняю, ты убегаешь. Что такое модель Лотки-Вольтерры и как она помогает биологам. URL: https://nplus1.ru/material/2019/12/04/lotka-volterra-model.

[22] 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). P. 30–47.

[23] 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.

[24] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.
[25] An Introduction to Factor Analysis of Information Risk (FAIR) URL: http: // riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf.

ASSESSMENT OF THE LEVEL OF SECURITY IN CYBERPHYSICAL SYSTEMS

The article presents a new approach to risk assessment and the formation of preventive security measures based on the Lotka-Volterra model. Proposed models of security of cyber-physical systems: "predator-prey" taking into account computing capabilities and targeting of targeted cyber-attacks, " predator-prey" taking into account the possible competition of attackers in relation to the "prey", "predator-prey" taking into account the relationships between "species" by "preys" and "predator species", "predator-prey" taking into account the interrelationships between "prey species" and "predator species" allow to provide a view of the possibility of forming a vector of threats, as well as their dependence on the development of digital technologies and new directions of digital services . Based on the proposed approach, the coefficients of the Lotka-Volterra model α=0.39, β=0.32, γ=0.29, φ=0.27 were obtained, which take into account the synergy and hybridity of modern threats, funding for the formation and improvement of the defense system, and also allows you to determine the financial and computing capabilities of the attacker based on the identified threats. The evaluation mechanism also takes into account the physical component of cyber-physical systems, which are formed, as a rule, from two environments - the physical level and the management level. This view of cyber-physical systems requires the design of multi-circuit information protection systems, as well as the formation of objectivity in the assessment of threats to both the internal (physical level) loop of the information protection system and the external loop (management level). The proposed method of assessing the security of cyber-physical systems is based on the basis of the developed threat classifier, allows to assess the current level of security and dynamically form recommendations for the distribution of limited protection resources based on an expert assessment of known threats. This approach allows for dynamic modeling in off-line mode, which allows timely identification of the capabilities of attackers and the formation of preventive protection measures based on threat analysis. Simulation can use actual bases of assessment of real threats and incidents on cyber-physical systems, which allows for an expert assessment of their impact on both individual security services and security components (cyber security, information security, and security of information).
Keywords: cyber-physical systems, information security, cyber security, security of information, Lotka-Voltarra security models.

Сергій Погасій, кандидат економічних наук, доцент кафедри кібербезпеки та інформаційних технолгій Національного технічного університету "Харківський політехнічний інститут".
Serhii Pogasii, Candidate of Economic Sciences, Associate Professor of the Department of Cyber Security and Information Technologies of the National Technical University "Kharkiv Polytechnic Institute".
E-mail: spogasiy1978@gmail.com.
Orcid ID: 0000-0002-4540-3693.

DOI: 10.18372/2410-7840.24.16934
УДК 57.087.1:004.932.7

ВИДІЛЕННЯ ОБЛИЧЧЯ ЛЮДИНИ У ВІДЕОПОТОЦІ ДЛЯ КОНТРОЛЮ ЗА ДОТРИМАННЯМ СПІВРОБІТНИКАМИ СТАНУ БЕЗПЕКИ В ПРОЦЕСІ РОБОТИ ТА НАВЧАННЯ

Олена Висоцька, Анатолій Давиденко, Владислав Христевич

Дослідження присвячене задачі виділення обличчя людини в відеопотоці, розглянуто області застосування функції виділення обличчя. Проаналізовані вимоги до механізмів вирішення даної задачі у випадку використання їх для моніторингу, в режимі онлайн, присутності людини на робочому місці, перед комп'ютером. Вказані принципи, за якими здійснюється виділення об'єктів (обличчя людини) в відеопотоці. В якості механізму вирішення зазначеної задачі запропоновано використовувати технологію MobileSSD, яка є комбінацією згорткових нейронних мереж MobileNetV2 та SSD. Проаналізовано принцип дій обраних нейронних мереж та