Браіловський Микола Миколайович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і захисту інформації Київського національного університету імені Тараса Шевченка.
Mykola Brailovskyi, PhD in Engineering Science, Associate Professor, Associate Professor of department of Cybersecurity and Information Protection of the Taras Shevchenko National University of Kyiv.
E-mail: bk1972@ukr.net.
Orcid ID: 0000-0002-3148-1148.

Козюра Валерій Дмитрович, к.т.н., доцент, доцент кафедри ТЗІ центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії СБ України.
Valeriy Kozura, Ph.D., associate professor, associate professor of the Department of Technical and Scientific Research of the Cyber Security Center of the Educational and Scientific Institute of Information Security and Strategic Communications of the National Academy of Security of Ukraine.
E-mail: kozval1948@gmail.com.
Orcid ID: 0000-0002-4769-448X.

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

DOI: 10.18372/2410-7840.25.18224
УДК 336.71:004.056

МОДЕЛІ БЕЗПЕКИ СОЦІОКІБЕРФІЗИЧНИХ СИСТЕМ

Станіслав Мілевський

Об'єктом дослідження є процес побудови многоконтурних систем захисту елементів інфраструктури соціокіберфізичних систем на основі модифікації моделі Лотки-Вольтерию У статті подано формування моделей безпеки соціокіберфізичних системах на основі моделі Лотки-Вольтери, що дозволяє визначити превентивні заходи системи безпеки проти цільових (змішаних) атак з комплексуванням з методами соціальної інженерії та можливістю ознак гібридності та синергізму. Такий підхід дозволяє на основі вихідних даних о соціополітичної (економічної) складової визначити можливість впливу на загальну думку як окремого соціуму, так й окремих вікових груп. Крім цього, визначення ознак гібридності та синергізму кіберзагроз у основних складових соціокіберфізичних систем: соціальних мережах, хмарі та фізичної складової дозволяє визначити основні принципи побудови многоконтурних систем безпеки з урахуванням на кожної платформі системи зовнішнього та внутрішнього контуру безпеки. Для формування многоконтурних систем захисту інформації соціокіберфізичних систем враховуються можливі сценарії реалізації цільових атак та їх направленість. А також можливість впливу на соціопсихологічний стан за рахунок соціальних мереж формальних та неформальних "лідерів" соціума.

***Ключові слова**: соціокіберфізичні системи, модель Лотки-Вольтери, гібридність, синергія, цільові атаки.*

ВСТУП

Розвиток сучасних технологій та бурхливе зростання інформаційних технологій на основі об'єднання смарт-, Інтернет- технологій та речей з мобільними та бездротовими стандартами сформувало поєднання соціальних мереж з кіберфізичними системами. Крім цього, з'єднання штучного інтелекту з дата-центрами та нейронними мережами значно поширює можливості таких змін в рамках диджиталізації та цифровізації суспільства. Окремим питанням у таких системах є необхідність нових концепцій на основі нових та/або модифікованих підходів побудови та /або формування/модифікації систем захисту.

Крім цього, еволюційне зростання обчислювальних можливостей дозволяю формувати моделі загроз на основі повномасштабного квантового комп'ютера, що на основі алгоритмів Гровера та Шора дозволять значно погіршити рівень забезпечення послуг безпеки. У таких умовах використання нестандартних/нових підходів побудови моделей безпеки – багатоконтурних систем, забезпечать нове рішення щодо протидії сучасним загрозам [1-5].

Проаналізовані моделі побудови систем захисту [6-10] вказують на наявність підходу, що базується на представленні процесу обробки у вигляді абстрактного обчислювального середовища. У цьому середовищі діє множина суб'єктів (користувачів та процесів) з різноманітними об'єктами (ресурси та набори даних). Основна ідея полягає в тому, що побудова системи захисту передбачає створення захисного середовища, яке представляє собою множину обмежень і процедур. Це середовище під управлінням ядра безпеки здатне контролювати доступ суб'єктів до об'єктів, забороняти несанкціонований доступ і здійснювати захист об'єктів від зовнішніх та внутрішніх загроз. Цей підхід ґрунтується на теоретичних моделях безпеки, таких як моделі Хартсона, Белла-Лападули, MMS Лендвера та Мак Ліна, Біба, Кларка – Вілсона та інші, і має статичний характер. Крім цього, визначені моделі враховують тільки розподіл ролей та рівень секретності конфіденційної інформації. Але не дозволяють враховувати побудову складних систем, які можуть складатись з декілька платформ у яких можуть використовуватись різні за природою стандарти та технології. Так в роботі [11] автори пропонують використовувати новий підхід побудови многоконтурних систем безпеки на основі розподілу соціокіберфізичних систем (socio-cyberphysical systems, SCS) на три основі платформи –соціальні мережі, хмарні технології, та фізичні програмно-апаратні (апаратні) застосунки та засоби. Але при цьому не враховується можливість впливу на такі системи з точки зору соціальних мереж та їх використання для зламу систем безпеки. Таким чином, виникає необхідність розгляду моделей побудови многоконтурних систем безпеки з урахування можливостей соціо впливу на інфраструктури соціокіберфізичних систем, а також формування превентивних заходів безпеки.

Метою статті є можливість використання модифікованих моделей Лотки-Вольтери при формуванні многоконтурних систем безпеки соціокіберфізичних систем.

ОСНОВНА ЧАСТИНА

Для оцінки безпеки кіберфізичних систем в умовах впливу сучасних цільових кіберзагроз, які виявляють ознаки гібридності та синергізму, враховується їхнє комплексування з методами соціальної інженерії на елементи інфраструктур. У контексті класичної моделі Лотки-Вольтери використовуються основні підходи, ґрунтовані на наступних парадигмах:

- у відсутності "хижаків" "жертви" експоненційно розмножуються;
- у відсутності "жертв" "хижаки" експоненційно вимирають.

Проте, у багатьох дослідженнях, зокрема [12-18], у ролі "жертв" розглядаються інциденти інформаційної безпеки та зловмисники, тоді як "хижаками" є заходи захисту та елементи системи безпеки.

Такий підхід може виявитися не логічним з точки зору кіберпростору як екосистеми. Математично модель "хижак-жертва" можна описати наступним чином:

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

де N_1 – чисельність жертв, N_2 – чисельність хижаків, α – коефіцієнт народжуваності жертв, β – коефіцієнт впливу хижака на жертву (коефіцієнт хижацтва), φ – коефіцієнт смертності хижака, γ – коефіцієнт впливу жертви на хижака.

Проте, для оцінки безпеки соціокіберфізичних систем введемо дефініції:

"Жертва" – це система або елемент інфраструктури SCS, яка піддається цільовим загрозам з ознаками синергізму та гібридності.

"Хижак" – це цільова загроза чи загроза окремим компонентам безпеки (кібербезпека, інформаційна безпека, безпека інформації (cyber security (CS), information security (IS), security for information (SI))) для системи чи елемента інфраструктури SCS.

"Рівень захищеності інформаційних ресурсів" – це якісний (кількісний) показник здатності системи захисту SCS протистояти синергетичним та гібридним загрозам на складові безпеки: CS, IS, SI.

"Гібридність загроз: CS, IS, SI" – це сукупність кількох загроз на інформаційні ресурси за складовими безпеки: CS, IS, SI, спрямованих на окрему послугу безпеки: конфіденційність, цілісність або автентичність.

"Синергізм загроз CS, IS, SI" – це комбінований вплив кількох загроз на складові безпеки: CS, IS, SI, з послугами безпеки: конфіденційність, цілісність, автентичність. Цей ефект характеризується тим, що їх об'єднана дія істотно перевершує ефект кожної загрози окремо та їх простої суми.

Таким чином, враховуючі модифікації, які запропоновані авторами в [19] моделі Лотки-Вольтери, та використовуючи вихідні дані в [20] сформуємо моделі безпеки SCS. При формуванні моделі безпеки також визначимо підхід їх класифікації на основі [11] та формування коефіцієнтів [19, 20]:

- коефіцієнт народжуваності "жертв" пропонується розраховувати, як:

$$\alpha = \frac{\left|\left\{\arg\max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A.\right\}\right|}{Q},$$

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

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

де K_j^D – рейтинговий коефіцієнт (важливості) побудови захисту j-го інформаційного ресурсу. При цьому під ресурсом може бути одна з складових соціума – інтенсивності впливу тієї чи іншої інституційної структури (формальний чи неформальний лідер, політична партія, засоби масової інформації) [20]. 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 для сторони захисту; 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; Q – загальна кількість відомих кіберзагроз;

- коефіцієнт впливу цільових атак на SCS β представим як:

$$\beta = \sum_{i=1}^{M}\left(w_{SCSi}{}^{C} \cap w_{SCSi}{}^{I} \cap w_{SCSi}{}^{A} \cap w_{SCSi}{}^{Au} \cap w_{SCSi}{}^{Aff}\right)\chi_i^{SCS},$$

де M – кількість погроз, обраних експертом з множини $\{i\}_i^M$, яка є підмножиною всієї множини загроз класифікатора, тобто $M \le Q$. $w_{SCSi}{}^{C}, w_{SCSi}{}^{I}$, $w_{SCSi}{}^{A}, w_{SCSi}{}^{Au}, w_{SCSi}{}^{Aff}$ – експертні вагові коефіцієнти послуг безпеки: конфіденційності, цілісності, доступності, автентичності та причетності; χ_i^{SCS} – ваговий коефіцієнт послуг безпеки: конфіденційності, цілісності, доступності, автентичності та справжності прояву атаки і-ї загрози.

Для визначення коефіцієнта обчислювальних можливостей зловмисника φ, скористаємося класифікацією зловмисників, як представлено у роботі [16], та представимо як:

$$\varphi = \frac{1}{M}\sum_{i=1}^{M} v_i \times p_{rj} \times r_{motiv},$$

де $v_i^{SCS} = W_{cp}^{SCS} \cap W_{cash}^{SCS} \cap T \cup \omega_i$, – вагові коефіцієнти можливості зловмисника; p_{rj} – ймовірність реалізації хоча б однієї загрози і-му активу; j – загроза, $\forall i \in Q$, Q – кількість угроз, і – інформаційний ресурс (актив), $\forall i \in M$, M – кількість активів; r_{motiv} – ймовірність мотивації зловмисника до реалізації загрози; W_{cp}^{CCS} – обчислювальні ресурси зловмисника (використовуємо з роботи [21]); ω_i – розрахунок сумарної інтенсивності впливу тієї чи іншої інституційної структури (формальний чи неформальний лідер, політична партія, засоби масової інформації) можна подати у вигляді згортки по рядку (за всіма віковими категоріями) (використовуємо з роботи [20]).

Таким чином, запропоновані коефіцієнти дозволяють поєднувати необхідні дані щодо формування моделей Лотки-Вольтери для SCS.

Для формування коефіцієнту превентивних заходів використовуємо [19]:

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

де μ_{kg}^l – ваговий коефіцієнт g-ї метрики l-ї послуги безпеки для k-го експерта.

Нормування вагових коефіцієнтів: $\sum_{k=1}^{K}\sum_{g=1}^{B}\mu_{kg}^{l}=1$,

w_{kg}^{l} – значення оцінки g-ї характеристики механізму СЗІ k-м експертом для l-ї послуги безпеки у разі, коли ступінь захищеності системи та деструктивні дії зловмисників є незалежними.

При цьому B = {cryptographic resistance, стійкість ТСЗІ (C_r), обсяг ключових даних (Key data amount, S_c), складність виконання прямого та зворотного криптографічного перетворення (шифрування/розшифрування) (encryption/decryption of data, OE)}. Таким чином, маємо таку множину характеристик технічних засобів СЗІ: $\mu^{l}=\left|\left\{C_r^{l},S_c^{l},O_E^{l}\right\}\right|$, що відповідає рівню стійкості криптографічних засобів СЗІ.

Для опису множини характеристик використовуємо індекс g: μ_g, де $(\{g\}_1^B)$.

Таким чином, модель безпеки соціокіберфізичних систем на основі моделі "хижак-жертва" з урахуванням обчислювальних можливостей та спрямованості цільових кібератак (модель 1) визначимо:

$$A_1^{SCS}=\begin{cases}\dfrac{dN_1}{dt}=\left(\arg\max\limits_{\forall Tr_l\in Tr_C^D}K_l^D\times K_l^A\right)\times\\ \times\left(\sum\limits_{i=1}^{Q}\left(\begin{matrix}N_{1_i}^C\times A_i^C+N_{1_i}^I\times A_i^I+N_{1_i}^A\times A_i^A+\\+N_{1_i}^{Au}\times A_i^{Au}+N_{1_i}^{Aff}\times A_i^{Aff}\end{matrix}\right)\right)-\\ -\left(\sum\limits_{i=1}^{M}\left(w_{SCSi}{}^{C}\cap w_{SCSi}{}^{I}\cap w_{SCSi}{}^{A}\cap w_{SCSi}{}^{Au}\cap w_{SCSi}{}^{Aff}\right)\chi_i^{SCS}\right)\tilde{N}_1\times\\ \times\left(N_2\times\left|W_{\text{hybrid }C,I,A,Au,Af\,synerg}\right|\right);\\ \dfrac{dN_2}{dt}=-\left(\dfrac{1}{M}\sum\limits_{i=1}^{M}v_i\times p_{rj}\times r_{motiv}\right)\widetilde{N_2}+\\ +\left(\dfrac{1}{KB}\sum\limits_{k=1}^{K}\sum\limits_{g=1}^{B}\left(\mu_{kg}^{l}\times w_{kg}^{l}\right)\right)\widetilde{N_2N_1}\end{cases},$$

де:

- $\tilde{N}_1=\sum\limits_{i=1}^{Q}\left(\begin{matrix}N_{1_i}^C\times A_i^C+N_{1_i}^I\times A_i^I+N_{1_i}^A\times A_i^A+\\+N_{1_i}^{Au}\times A_i^{Au}+N_{1_i}^{Aff}\times A_i^{Aff}\end{matrix}\right)$ – чисельність об'єктів, що представляють цілі атак з урахуванням їхньої гібридності;

- $N_2=N_2\times\left|W_{\text{hybrid }C,I,A,Au,Af\,synerg}\right|$ – рівняння зміни чисельності сучасних загроз на SCS з урахуванням можливості їх ознак синергізму та гібридності, де $\left|W_{\text{hybrid }C,I,A,Au,Af\,synerg}\right|$ – потужність множини гібридних загроз (тобто їх кількість), а $W_{\text{hybrid }C,I,A,Au,Af\,synerg}=W_{synerg}^{C}\cap W_{synerg}^{I}\cap W_{synerg}^{A}\cap W_{synerg}^{Au}\cap W_{synerg}^{Aff}$, де множина гібридних загроз, які відповідно до прийнятого припущення, визначається як безліч загроз одночасно для всіх служб безпеки. Обчислення окремих складових наведено у роботі [21].

Використання моделі дозволяє оцінити обчислювальні можливості та сформувати класифікацію зловмисників.

Такий підхід формує точку незворотності при якому визначається "неможливість" проведення цільовий атаки.

Наступна модель дозволяє враховувати "зацікавленості" злочинців та/або кібергруп у проведені цільової атаки, їх мотивацію та конкуренцію.

Модель безпеки соціокіберфізичних систем на основі моделі "хижак-жертва" з урахуванням можливої конкуренції зловмисників по відношенню до "жертви" (модель 2) визначимо:

$$A_2^{SCS}=\begin{cases}\dfrac{dN_1}{dt}=\left(\arg\max\limits_{\forall Tr_l\in Tr_C^D}K_l^D\times K_l^A\right)\times\\ \times\left(\sum\limits_{i=1}^{Q}\left(\begin{matrix}N_{1_i}^C\times A_i^C+N_{1_i}^I\times A_i^I+N_{1_i}^A\times A_i^A+\\+N_{1_i}^{Au}\times A_i^{Au}+N_{1_i}^{Aff}\times A_i^{Aff}\end{matrix}\right)\right)-\\ -\left(\sum\limits_{i=1}^{M}\left(w_{SCSi}{}^{C}\cap w_{SCSi}{}^{I}\cap w_{SCSi}{}^{A}\cap w_{SCSi}{}^{Au}\cap w_{SCSi}{}^{Aff}\right)\chi_i^{SCS}\right)\times\\ \times\tilde{N}_1\left(N_2^1\cap N_2^2\cap\ldots\cap N_2^w\right);\\ \dfrac{dN_2}{dt}=-\left(\dfrac{1}{M}\sum\limits_{i=1}^{M}v_i\times p_{rj}\times r_{motiv}\right)\times\widetilde{\left(N_2^1\cap N_2^2\cap\ldots\cap N_2^w\right)}+\\ +\left(\dfrac{1}{KB}\sum\limits_{k=1}^{K}\sum\limits_{g=1}^{B}\left(\mu_{kg}^{l}\times w_{kg}^{l}\right)\right)\times\widetilde{\left(N_2^1\cap N_2^2\cap\ldots\cap N_2^w\right)N_1},\end{cases}$$

де кількість "хижаків" належить множині $\left\{\overline{N_2^j}\right\}$, $j\in 1,\ldots Q$.

Таким чином запропонована модифікація моделі Лотки-Вольтери дозволяє формувати вектор "зацікавленості" цільових (змішаних) атак з урахуванням еволюційного розвитку технологій.

Модель безпеки соціокіберфізичних систем на основі моделі "хижак-жертва" з урахуванням можливості групування зловмисників/кібергруп з метою досягнення цілей кібератаки визначимо (модель 3):

$$A_3^{SCS} = \begin{cases} \dfrac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum\limits_{i=1}^{Q} \left(\begin{matrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{matrix} \right) \right) - \\ - \left(\sum\limits_{i=1}^{M} \left(w_{SCSi}^{\ C} \cap w_{SCSi}^{\ I} \cap w_{SCSi}^{\ A} \cap w_{SCSi}^{\ Au} \cap w_{SCSi}^{\ Aff} \right) \times \right. \\ \left. \times \chi_i^{SCS} \right) \times \\ \times \tilde{N}_1 \left(\sum\limits_{j=1}^{w} N_2^w \right); \\ \dfrac{dN_2}{dt} = -\left(\dfrac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \left(\overline{\sum\limits_{j=1}^{w} N_2^w} \right) + \\ + \left(\dfrac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^l \times w_{kg}^l \right) \right) \times \left(\overline{\sum\limits_{j=1}^{w} N_2^w} \right) \overline{\tilde{N}_1}, \end{cases}.$$

Модель дозволяє враховувати політичні та/або економічні та/або соціальні складові мотивації реалізації загроз. Це пов'язано з загальною тенденцію розвитку мирового суспільства, етнічними та культурними цінностями, а також формуванню кіберугрупувань які підконтрольні державі та виконують замовлення за рахунок фінансування та підтримки держави в цілому. прикладом такої моделі може бути військова частина №61398 НВАК (Відділ APT1) Китаю, яка реалізує електронний шпіонаж.

Модель безпеки соціокіберфізичних систем на основі моделі "хижак-жертва" з урахуванням взаємозв'язків між "видами жертв" та "видами хижаків" (модель 4) визначимо:

$$A_4^{SCS} = \begin{cases} \dfrac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum\limits_{i=1}^{Q} \left(\begin{matrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{matrix} \right) \right) - \\ - \left(\sum\limits_{i=1}^{M} \left(w_{SCSi}^{\ C} \cap w_{SCSi}^{\ I} \cap w_{SCSi}^{\ A} \cap w_{SCSi}^{\ Au} \cap w_{SCSi}^{\ Aff} \right) \times \right. \\ \left. \times \chi_i^{SCS} \right) \times \\ \times \tilde{N}_1 \left(\sum\limits_{j=1}^{w} N_2^w \right) - \varepsilon N_1^{\ 2}; \\ \dfrac{dN_2}{dt} = -\left(\dfrac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \left(\overline{\sum\limits_{j=1}^{w} N_2^w} \right) + \\ + \left(\dfrac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^l \times w_{kg}^l \right) \right) \times \left(\overline{\sum\limits_{j=1}^{w} N_2^w} \right) \overline{\tilde{N}_1 - \xi N_2^{\ 2}}, \end{cases}$$

де коефіцієнти $\varepsilon, \zeta > 0$, і описують завдання шкоди "жертви" і "хижака" він відповідно.

Запропоновані моделі практично дозволяють враховувати сучасні фінансові, обчислювальні можливості зловмисників. Крім цього, запропонований підхід враховує можливість не тільки впливу на "жертву" за рахунок комплексування цільових (змішаних) атак з методами соціальної інженерії, а також враховувати соціально-політико-економічний стан соціуму, в якому знаходиться "жертва".

Для формування многоконтурних систем захисту SCS на рис 1 наведена структурно-логічна схема.

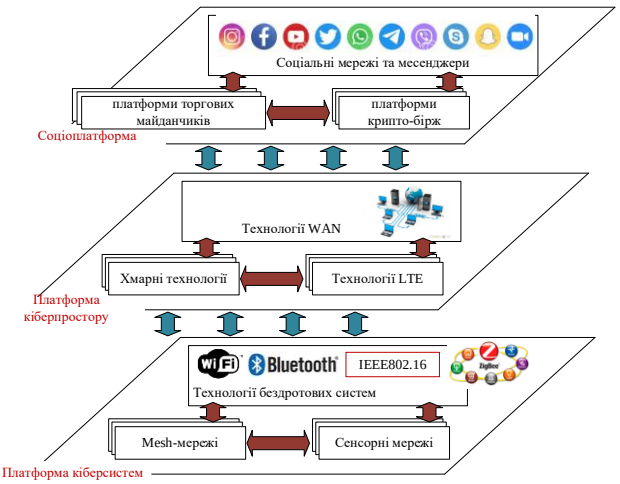

Рис. 1. Структурно-логічна схема соціокіберфізичної системи

Проведений аналіз [1-5, 11, 19-21] показав, що для побудови многоконтурних систем безпеки необхідно враховувати окремо можливості загроз як на внутрішній, так й на зовнішній контури, можливість їх комплексування з методами соціальної інженерії. Таким чином, з урахуванням платформ пропонується об'єднання моделей безпеки на основі Лотки-Вольтери.

Для побудови моделі безпеки платформи кіберсистем необхідно враховувати:

- внутрішній контур: $Q_{ISL_1}^{SCS} = A_1^{SCS} \cup A_3^{SCS} \cap A_2^{SCS} \cap A_4^{SCS}$,
- зовнішній контур: $Q_{ESL_1}^{SCS} = A_1^{SCS} \cup A_3^{SCS} \cap A_2^{SCS} \cap A_4^{SCS}$.

Для побудови моделі безпеки платформи кіберпростору необхідно враховувати:

- внутрішній контур: $Q_{ISL_2}^{SCS} = A_1^{SCS} \cup A_2^{SCS} \cup A_3^{SCS}$;

- зовнішній контур: $Q_{ESL_2}^{SCS} = A_1^{SCS} \cup A_2^{SCS} \cup A_3^{SCS} \cap A_4^{SCS}$.

Для побудови моделі безпеки платформи соці мереж необхідно враховувати:

- внутрішній контур: $Q_{ISL_3}^{SCS} = A_1^{SCS} \cup A_2^{SCS} \cup A_3^{SCS}$;

- зовнішній контур: $Q_{ESL_3}^{SCS} = A_1^{SCS} \cup A_2^{SCS} \cup A_3^{SCS} \cap A_4^{SCS}$.

Таким чином, з урахуванням запропонованого підходу загальна модель многоконтурної системи безпеки SCS складається:

$$Q_{загальн}^{SCS} = \left(Q_{ISL_1}^{SCS} \cup Q_{ESL_1}^{SCS}\right) \cup \left(Q_{ISL_2}^{SCS} \cup Q_{ESL_2}^{SCS}\right) \cup \left(Q_{ISL_3}^{SCS} \cup Q_{ESL_3}^{SCS}\right).$$

Отже, сформовані основні вимоги щодо побудови многоконтурних систем захисту соціокіберфізичних систем.

ВИСНОВКИ

Запропоновані модифікації моделі Лотки-Вольтери які дозволяють формувати моделі загроз з урахуванням співвідношення "жертва–хижак", розвитку та напряму еволюції сучасних технологій. Запропонований підхід дозволяє формувати моделі безпеки соціокіберфізичних систем з урахуванням не тільки ознак гібридності та синергії цільових загроз, їх комплексування з методами соціальної інженерії, а також враховувати мотивацію та "можливості" реалізації APT-атак на елементи інфраструктури SCS.

Запропонований підхід формування многоконтурної моделі безпеки соціокіберфізичних систем враховує складну логічну структуру та фізичну побудову SCS, взаємозв'язок основних технологій та платформ. Такий підхід забезпечує не тільки підвищення рівня об'єктивності оцінки загроз, можливостей комп'ютерних інцидентів (відхилень від нормальної роботи та/або аномалій), а також вплив соціо-політичної та економічної складової соціума, який використовує SCS.

Крім цього, забезпечується врахування можливого впливу на елементи многоконтурної системи захисту інформації SCS за рахунок "використання" соціальних мереж, проведення спеціальних операцій на основі методів соціальної інженерії з метою компрометації довіри та іміджу відповідної соціокіберфізичної системи, зламу інфраструктури безперервності бізнес-процесів.

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

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

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

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

[7] 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.

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

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

[10] 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.

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

[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] 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.
[16] Fink, Glenn A., Haack, Jereme N., McKinnon, Archibald D., and Fulp, Errin W. Defense on the Move: Ant-Based Cyber Defense. United States, 2014. Web. doi:10.1109/MSP.2014.21.
[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), pp. 6412-6416. 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, 1783 p. URL: https://doi.org/ 10. 3390/math9151783.
[19] 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.
[20] Serhii Yevseiev 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.
[21] O. Shmatko and other. Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies ISSN 1729-3774 3/9 (105) 2020. pp. 6-19.

SOCIOCYBERPHYSICAL SYSTEMS' SECURITY MODELS

The object of the study is the process of building multi-contour systems for the protection infrastructure elements of socio-cyber-physical systems based on a modification of the Lotka-Volterra model. The article presents the formation of security models for socio-cyber-physical systems based on the Lotka-Volterra model, which allows determining preventive measures of the security system against targeted (mixed) attacks with integration with social engineering methods and the possibility of hybridity and synergism signs. This approach allows, based on the initial data on the socio-political (economic) component, to determine the possibility of influencing the general opinion of both a separate society and certain age groups. In addition, the identification of signs of hybridity and synergism of cyber threats in the main components of socio-cyber-physical systems: social networks, the cloud and the physical component allows to determine the basic principles of building multi-contour security systems, considering the external and internal security contour systems on each platform. For the formation of multi-contour information protection systems of socio-cyber-physical systems, possible scenarios of the implementation of targeted attacks and their directionality are considered. And also, the possibility of influencing the socio-psychological state through social networks of formal and informal "leaders" of society.

Keywords: socio-cyberphysical systems, Lotka-Volterra model, hybridity, synergy, targeted attacks.

Мілевський Станіслав Валерійович, кандидат економічних наук, доцент кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут", Україна.
Stanislav Milevsky, Ph.D., Associate Professor, Department of Cybersecurity, National Technical University "Kharkiv Polytechnic Institute," Ukraine.
E-mail: milevskiysv@gmail.com.
Orcid ID: 0000-0001-5087-7036.

DOI: 10.18372/2410-7840.25.18225
УДК 004.056.5

ВИКЛИКИ ТА СТРАТЕГІЇ ЗБЕРІГАННЯ ВЕЛИКИХ ОБСЯГІВ ДАНИХ У СУЧАСНОМУ СВІТІ

Олег Дейнека, Олег Гарасимчук

У сучасному світі, зберігання великих обсягів даних стає надзвичайно актуальною проблемою. Споживачі та організації постійно генерують великі обсяги інформації, і ця тенденція зростає. Щоб забезпечити ефективне