УДК 004.56
DOI: https://doi.org/ 10.17721/3041-2323.2024.355-364

Сергій ТОЛЮПА, д-р техн. наук, проф.
ORCID ID: 0000-0002-1919-9174
e-mail: serhii.toliupa@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Сергій ШТАНЕНКО, канд. техн. наук, доц.
ORCID ID: 0000-0001-9776-4653
e-mail: sh_sergei@ukr.net
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна

Андрій КУЛЬКО, асп.
ORCID ID: 0009-0006-1185-0774
e-mail: kulko452@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

ВИБІР СТРАТЕГІЇ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ТЕОРІЇ ІГОР

В умовах тривалої збройної агресії Росії проти України безпека особи, суспільства та держави суттєво залежить від надійного функціонування об'єктів критичної інфраструктури. Крім фізичних атак на такі об'єкти із застосуванням летальної зброї, Росія разом зі своїми сателітами продовжує намагатися впливати на системи управління об'єктами критичної інфраструктури через кіберпростір і з кіберпростору за допомогою нелетальних засобів – кіберзброї. Ситуація ускладнюється тим, що об'єкти критичної інфраструктури, які функціонують в єдиному інформаційному просторі та підтримують широкий спектр сучасних інформаційних технологій, незважаючи на колосальні зусилля з протидії зовнішньому втручанню з кіберпростору та через нього, залишаються вразливими до нових видів загроз, а тому постає питання оптимального вибору засобів захисту об'єкта, що охороняється.

Ключові слова: ***об'єкт, критична інфраструктура, захист, виживання, мобільний зв'язок, надійність, вразливість.***

Вступ

В умовах тривалої збройної агресії Росії проти України безпека людини, суспільства і держави суттєво залежать від надійного функціонування об'єктів критичної інфраструктури (ОКІ). Крім фізичних впливів на такі об'єкти летальною зброєю російська федерація не полишає спроб разом зі своїми сателітами впливати нелетальними засобами – кіберзброєю – на системи управління об'єктів критичної інфраструктури через кіберпростір та з кіберпростору. З огляду на транскордонність кіберпростору і високий рівень інформатизації об'єктів критичної інфраструктури, систем управління військами та зброєю (Єдиної автоматизованої системи управління) Збройними силами України та її складових тощо, ризики масштабуються не тільки на національний безпековий вимір, а і становлять загрозу для людства на глобальному рівні на досяжну перспективу. Ситуація ускладнюється тим, що об'єкти критичної інфраструктури, які функціонують в єдиному інформаційному просторі й підтримують широкий спектр сучасних інформаційних технологій, всупереч колосальним зусиллям для протидії стороннім втручанням із кіберпростору та через кіберпростір, й надалі залишаються вразливими до загроз нового типу. Виникає питання оптимального вибору засобів захисту для об'єкта, що захищається (Євсєєв та ін., 2024). Незважаючи на значні успіхи у сфері інформаційної безпеки, донині існують труднощі у запобіганні віддаленим атакам на ОКІ. Аналіз мережевих атак показує, що дії захисту найчастіше вживають після того, як уже є зниження продуктивності сервісу. Відбувається це внаслідок складності оцінювання майбутнього масштабу атаки та використання відповідного заходу захисту. Деякі дії (напр., DOS-атаки) характеризуються спонтанним характером, тобто вони можуть починатися і закінчуватися у випадкові моменти часу, що також додає складності виробленню своєчасної реакції на атаку **(**Толюпа та ін., 2021**).** Для виявлення фактів неавторизованого доступу до системи, а також інших типів шкідливої активності, які можуть порушити безпеку інформаційної системи, використовують системи виявлення вторгнень.

Результати

Для підвищення точності передбачення і виявлення атак система виявлення вторгнень повинна збирати різнорідну інформацію про роботу системи, що захищається, а також зберігати й обробляти великий обсяг даних. Використання системи фільтрації за відсутності атаки тягне за собою зниження продуктивності сервера і можливе помилкове спрацьовування фільтра. Досить часто створення ефективної системи захисту стикається з недостатньою обчислювальною потужністю. Отже, постає завдання оптимізації ресурсів, що витрачаються на підтримку працездатності системи захисту від мережевих атак на високому рівні (Даник та ін., 2015).

Одним із варіантів розв'язання зазначеної проблеми є мінімізація ресурсів, що витрачаються на підтримку інформаційної безпеки в ті моменти часу, коли активність атакуючої сторони незначна. Із цією метою система виявлення вторгнень має використовувати динамічні методи, що дають змогу оперативно виявляти й запобігати порушенням безпеки, Тобто в системі захисту інформації має бути використана математична модель, що дає змогу в кожен момент часу вибрати необхідний набір засобів захисту, який забезпечує надійний захист і водночас потребує мінімальної кількості ресурсів.

У вітчизняних і зарубіжних роботах останніх років спостерігається тенденція розширення наявних математичних підходів до вибору параметрів системи захисту інформації. Наприклад, різні автори пропонують такі математичні методи для аналізу й оптимізації системи захисту інформації: методи математичної статистики; методи, що ґрунтуються на використанні мереж Петрі; математичний апарат теорії випадкових процесів; методи, що ґрунтуються на застосуванні теорії автоматів; методи на основі теорії нечітких множин; методи, що ґрунтуються на використанні нейронних мереж; методи експертних систем; математичний апарат теорії ігор (Грищук, 2010а).

Будь-яку систему оброблення інформації, що складається з різних апаратних і програмних засобів, можна розглядати як унікальний комплекс зі своїми особливостями. Саме це є поясненням можливості пропуску специфічних для системи, що захищається,

вторгнень тими системами виявлення, які використовують той самий набір параметрів оцінювання. Отже, кращим рішенням буде визначення необхідних параметрів моніторингу в процесі роботи системи. Складність ефективного динамічного формування параметрів спостереження полягає в тому, що розмір області пошуку експоненційно залежить від потужності початкової множини параметрів, які спостерігаються. Для формування багатьох параметрів, що спостерігаються, в системах виявлення вторгнень використовують різні інтелектуальні методи (Толюпа та ін., 2021; Tolupa, Nakonechnyi, & Uspenskyi, 2019). Багато дослідників пропонують застосовувати як математичну основу у побудові й аналізі систем захисту інформації апарат теорії ігор. Теорія ігор є формальним підходом, призначеним для аналізу взаємодії між кількома учасниками процесу, що мають різні інтереси та приймають рішення. У будь-якій системі захисту інформації йдеться про дві сторони: сторону нападу та сторону захисту (систему захисту інформації), що мають протилежні інтереси. Пропонується використовувати математичний апарат теорії ігор для розв'язання завдання вибору засобів захисту від несанкціонованого доступу до інформації в автоматизованій системі. Було виконано математичну постановку завдання у вигляді завдання лінійного програмування з булевими змінними. У математичній постановці введено показник вартості засобів захисту. Обмеження завдання враховують вимоги класів захищенності від несанкціонованого доступу в автоматизованих системах.

У дослідженні (Грищук, 2010б) проведено огляд теоретико-ігрових методів, які використовують у розв'язанні задач інформаційної безпеки. У роботі розглянуто підхід до проєктування систем виявлення вторгнень із використанням математичного апарату матричних ігор для двох гравців. У запропонованій моделі враховано вартість системних ресурсів для організації захисту .

У деяких роботах розглядають можливості використання багатокрокових ігор із неповною інформацією для побудови систем захисту від DoS-атак. Пропонується подати завдання у вигляді гри двох сторін: та, що обороняється (A), і та, що атакує (B). Завданням сторони, що захищається, є мінімізація власних втрат внаслідок дій атакуючої сторони. Завдання сторони B – отри-

мання максимального прибутку. Зазначено, що головною особливістю такої гри є те, як стратегії використовують функції, що описують поведінку сторін у короткостроковій перспективі. Багато функцій пропонується підбирати для кожного завдання індивідуально, з огляду на статистичні дані, зовнішні обмеження та здоровий глузд (Грищук, 2010а).

Під час аналізу питань захисту від різних загроз безпеці доцільно розглядати дії двох сторін: сторони захисту (інформаційної системи) та сторони порушника. Як порушника можна розглядати всю сукупність загроз безпеки: дії окремих осіб, які мають різні цілі, великомасштабні сплановані атаки, а також випадкові впливи на систему. Подібні моделі, коли існують дві або більше протиборчих сторін, типові для теорії ігор. Якщо відомі варіанти дій (стратегії) кожної зі сторін, а також виграш (або програш) від кожного з варіантів дій, то є можливість сформулювати математичну модель ситуації у вигляді моделі безкоаліційної антагоністичної гри (напр., матричної). На основі сформульованого завдання можна отримати оптимальні стратегії сторони нападу та сторони захисту, що вимагають мінімуму ресурсів (Грищук, 2010а).

Розглянемо взаємодію системи виявлення вторгнень і атакуючого як безкоаліційну кінцеву гру. Нехай сторона захисту A та порушник B мають кінцеву кількість стратегій n_B і n_A, що відповідає реальності, оскільки сторона захисту завжди має обмеження за кількістю можливих варіантів реагування, а сторона нападу – за кількістю варіантів організації атаки. Наприклад, для захисту пропонується використовувати стратегії ("ігнорувати підозрілу активність", "підсилити моніторинг"); а для сторони нападу можна розглядати безліч стратегій ("завершити атаку", "продовжити без паузи", "зробити паузу в атаці"). Набір стратегій гравців $s = (s_A, s_B)$, де $s_A \in S_A, s_B \in S_B$ – набір ситуацій. Функції ω_A і ω_B виграшів гравців визначені на безлічі ситуацій:

$$S = S_A \times S_B. \quad (1)$$

Рішенням безкоаліційної гри є ситуації рівноваги, але не обов'язково у чистих стратегіях. Як відомо, кожна кінцева антагоністична гра має хоча б одну ситуацію рівноваги у змішаних стратегіях. У процесі аналізу систем захисту інформації змішані стратегії має сенс розглядати за припущення, що робота системи триває знач-

ний час, тобто ітерації атаки і захисту повторюються багаторазово. Причому стратегії використовуються сторонами з деякою недетермінованою закономірністю і витрати / доходи накопичуються із часом. Змішаною стратегією гравців *A* і *B* називатимемо повний набір імовірностей застосування їхніх чистих стратегій:

$$P_A = \{p_{A_1}, p_{A_2}, \dots, p_{A_n}\}; P_B = \{p_{B_1}, p_{B_2}, \dots, p_{B_n}\}. \quad (2)$$

У безкоаліційній грі кожен гравець використовує свої чисті стратегії незалежно від іншого учасника процесу, тому у змішаній ситуації $p = (P_A, P_B\}$ ймовірність $p(s)$ появи ситуації $s = (s_A, s_B)$ дорівнює добутку ймовірностей використання обома гравцями своїх чистих стратегій, тобто

$$p(s) = p(s_A, s_B). \quad (3)$$

Знайдемо середній виграш (програш) гравців. Математичне очікування виграшу гравця *A* у змішаній грі $p = (P_A, P_B\}$визначається так:

$$W_A(p) = w_A(P_A, P_B) = \sum_{s \in S} w_A(s)p(s) = \sum_{s_1 \in S_A} \sum_{s_2 \in S_B} w_A(s_1, s_2)p_A(s_A)(p_B(s_B)),$$

де S_A, S_B – кількість можливих ситуацій гравців *A* і *B* відповідно; w_A – функція виграшу (а насправді – програшу або витрат) системи захисту інформації, якщо система захисту інформації обрала стратегію s_1, а порушник – стратегію s_2.

Виграш гравця (порушника системи захисту інформації) у загальному випадку визначають аналогічно.

Як можна знайти виграші гравців у цьому випадку? Система виявлення вторгнень S у кожний момент часу дає безліч параметрів M_S за допомогою сенсорів. Кожну атаку можна подати у вигляді послідовності ітерацій. Після кожного кроку система виявлення вторгнень намагається "передбачити" наступні кроки порушника. Кожен крок порушника породжує певний вид активності, який можна знайти за допомогою датчиків системи. Якщо блок аналізу розпізнає активність як підозрілу, безліч базових параметрів, що спостерігаються, M_S, має бути розширено. Нехай безліч додаткових параметрів спостереження буде $M_{S_{\text{дод}}} = \{x_1, x_2, x_3, \dots, x_n\}$, а вартість додаткових ресурсів, що витрачаються на їх спостереження протягом часу $t - C_A(t)$. Припустимо, що витрати на спостереження прямо пропорційні часу

спостереження. Якщо моніторинг розширеної множини параметрів проводять протягом часу t_m, то вартість додаткових витрат на спостереження буде визначатись як

$$C_A(t) = \sum_{i=1}^{n} c_i\, t_m, \qquad (4)$$

де n – кількість додаткових параметрів спостереження; c_i – витрати на моніторинг i-го параметра.

У разі прийняття рішення – ігнорувати можливу атаку – система захисту інформації не несе витрат на додатковий моніторинг.

Оцінимо витрати порушника системи захисту інформації. У разі прийняття рішення про припинення атаки порушник не несе додаткових витрат, а у разі прийняття рішення про продовження атаки витрати атакуючої сторони залежать від кількості k генерованих запитів до системи, що захищається: $C_B = gk$, де g – вартість генерації одного запиту.

У разі успішної атаки система захисту інформації зазнає збитків c_A^*, а порушник отримує виграш c_B^*. Витрати системи захисту за реалізації кожної з можливих стратегій складаються з витрат на організацію захисту $C_A(t) = \sum_{i=1}^{n} c_i\, t_m$ та збитків від можливих порушень безпеки c_A^*. Аналогічно виграш порушника складається з виграшу від порушення роботи системи захисту інформації c_B^* і через витрати на проведення атак C_B.

Для аналізованої системи виявлення вторгнень передбачено, що зі збільшенням додаткових параметрів спостереження зростає ймовірність визначення атаки. Однак визначення точної залежності успішного виявлення атаки від кількості та набору параметрів моніторингу, а також від часу спостереження вимагає експериментального дослідження для кожного типу систем захисту інформації.

Варто відмітити деякі особливості використання цієї методики щодо систем захисту інформації. Передусім, виграші гравців у змішаній грі визначено однаковим математичним очікуванням їх виграшів. По-друге, модель може використовувати ті чи інші дані як вхідні параметри. Зауважимо, що можливості отримання різних даних можуть бути завданнями різного ступеня складності. Далі, відомо, що у виявленні мережевих вторгнень дуже велику роль відіграє багато параметрів оцінювання. Тому у виявленні ано-

малій однією з головних завдач є вибір оптимальної множини параметрів оцінювання, що неможливо виконати методами теорії ігор. Тому доцільно застосовувати різні математичні методи під час побудови систем захисту, зокрема і систем виявлення вторгнень.

Дискусія і висновки

У цілому, математичний апарат теорії ігор дозволяє аналізувати задачі з антагоністичною природою, що повторюється, і це типово для задач захисту інформації. Пропоновані методи дають можливість вибрати на початковому етапі стратегії дій у процесі роботи системи виявлення вторгнень і знизити обчислювальні витрати на оброблення даних у системі захисту інформації.

Список використаних джерел

Даник, Ю., Вдовенко, С., Шестаков, В., Писарчук, О., Грищук, Р., Куликівський, М., & Ходаківський, В. (2015). *Основи захисту інформації.* ЖВІ ДУТ. https://miljournals.knu.ua/index.php/zbirnuk/article/download/704/665

Грищук, Р. (2010а). *Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень.* РУТА. http://library.kpi.kharkov.ua/uk/inftechnologies_gryshyuk

Грищук, Р. (2010б). Диференціально-ігрова модель системи захисту інформації. *Інформаційна безпека*, 2(4), 23–29. СНУ ім. В. Даля. https://jrnl.nau.edu.ua/index.php/ZI/article/download/1987/1978

Євсєєв, С., Заковоротний, О., Мілов, О., Кучук, Г., Галуза, О., Коваль, М., Войтко, О., & Грищук, Р. (2024). *Методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури*. Новий Світ-2000. http://www.kdpu-nt.gov.ua/uk/content/metodologiya-syntezu-modeley-intelektualnyh-system-upravlinnya-ta-bezpeky-obyektiv

Толюпа, С., Лукова-Чуйко, Н., Толюпа, С., Наконечний, В., & Браіловський, М. (2021). *Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз*. Формат. https://science.lpnu.ua/sites/default/files/journal-paper/2022/mar/27268/stattya3stolyupanlukova-chuykoyashestak.pdf

Tolupa, S., Nakonechnyi, V., & Uspenskyi, O. (2019). Signature and statistical analyzers in the cyber attack detection system. *Information Technology and Security. Ukrainian Research Papers Collection,* 7(1), 69–79. DOI: 10.20535/2411-1031.2019.7.1.184326

References

Danik, Y., Vdovenko, S., Shestakov, V., Pisarchuk, O., Gryshchuk, R., Kulikivskyi, M., & Khodakivskyi, V. (2015). *Fundamentals of information protection.* ZVI DUT [in Ukrainian]. https://miljournals.knu.ua/index.php/zbirnuk/article/download/704/665

Gryshchuk, R. (2010). *Differential-game model of the information security system.* Information Security, 2(4), 23–29. Luhansk: Volodymyr Dahl East Ukrainian National University [in Ukrainian]. https://jrnl.nau.edu.ua/index.php/ZI/article/download/1987/1978

Gryshchuk, R. (2010). *Theoretical foundations of modeling information attack processes using the theories of differential games and differential transformations.* RUTA [in Ukrainian]. http://library.kpi.kharkov.ua/uk/inftechnologies_gryshyuk

Evsjeev, S., Zakovorotnyi, O., Milov, O., Kuchuk, G., Galuza, O., Koval, M., Voytko, O., & Gryshchuk, R. (2024). *Methodology for synthesizing models of intelligent management and security systems for critical infrastructure objects.* New World-2000 [in Ukrainian]. http://www.kdpu-nt.gov.ua/uk/content/metodologiya-syntezu-modeley-intelektualnyh-system-upravlinnya-ta-bezpeky-obyektiv

Tolupa, S., Lukova-Chuyko, N., Tolupa, S., Nakonechnyi, V., & Brailovskyi, M. (2021). *Intrusion detection systems and functional resilience of distributed information systems to cyber threats.* Format [in Ukrainian]. https://science.lpnu.ua/sites/default/files/-journal-paper/2022/mar/27268/stattya3stolyupanlukova-chuykoyashestak.pdf

Tolupa, S., Nakonechnyi, V., & Uspenskyi, O. (2019). Signature and statistical analyzers in the cyber attack detection system. *Information Technology and Security. Ukrainian Research Papers Collection,* 7(1), 69–79. DOI: 10.20535/2411-1031.2019.7.1.184326

Отримано редакцією журналу / Received: 17.09.24
Прорецензовано / Revised: 27.09.24
Схвалено до друку / Accepted: 01.10.24

Serhii TOLIUPA, DSc (Engin.), Prof.
ORCID ID: 0000-0002-1919-9174
e-mail: serhii.toliupa@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Serhii SHTANENKO, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0001-9776-4653
e-mail: sh_sergei@ukr.net
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine

Andrii KULKO, PhD Student
ORCID ID: 0009-0006-1185-0774
e-mail: kulko452@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

CHOOSING A STRATEGY FOR PROTECTION OF CRITICAL INFRASTRUCTURE OBJECTS BASED ON GAME THEORY

In the context of the ongoing armed aggression of the Russian Federation against Ukraine, the security of individuals, society and the state

significantly depends on the reliable functioning of critical infrastructure facilities (CIF). In addition to physical attacks on such facilities with lethal weapons, the Russian Federation, together with its satellites, continues to try to influence the control systems of critical infrastructure facilities through cyberspace and from cyberspace with non-lethal means - cyber weapons. The situation is complicated by the fact that critical infrastructure facilities operating in a single information space and supporting a wide range of modern information technologies, despite enormous efforts to counteract outside interference from and through cyberspace, remain vulnerable to new types of threats, and therefore the issue of optimal choice of means of protection for the protected object arises.

Keywords: ***object, critical infrastructure, protection, survivability, mobile communication, reliability, vulnerability.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.