КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№2 (6), 2019
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2019.6.154163
УДК 351.82:34+330.47

Гулак Геннадій Миколайович
кандидат технічних наук, доцент,
завідувач лабораторії досліджень кібербезпеки науково-дослідного відділу
ІПММС НАН України, Київ, Україна
ORCID: 0000-0001-9131-9233
h.hulak@ukr.net

Лахно Валерій Анатолійович
доктор технічних наук, професор,
зав. каф. комп'ютерних систем і мереж,
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0000-0001-9695-4543
Valss21@ukr.net

МОДЕЛЬ ПРОЦЕСУ ІНВЕСТУВАННЯ В РОЗВИТОК КІБЕРБЕЗПЕКИ ДЛЯ ПОБУДОВИ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Анотація. Розглянуто актуальну проблему прийняття оптимального рішення щодо фінансування проектів у галузі кібербезпеки в умовах активних дій порушників кібербезпеки. Розроблено модель системи підтримки прийняття рішень для фінансування проектів для створення сприятливих умов розвитку центрів управління кібербезпекою об'єктів критичної інфраструктури. Модель передбачає методи та засоби активної протидії стороні що атакує. На відміну від існуючих підходів, модель заснована на вирішенні білінійної гри диференціальної якості з кількома термінальними поверхнями. У роботі був використаний метод дискретного наближення. Це дало змогу знайти рішення білінейної диференціальної гри якості із залежними рухами. Результати обчислювального експерименту в рамках програмної реалізації системи підтримки прийняття рішень у галузі фінансування проектів кібербезпеки, зокрема, у створенні та розвитку центрів управління кібербезпекою для критично важливих об'єктів інфраструктури описані. Розроблена система підтримки прийняття рішень дозволяє отримувати оптимальні стратегії фінансування із забезпечення кібербезпеки критично важливих об'єктів інфраструктури. У цьому випадку враховується будь яке співвідношення параметрів, що описують процес фінансування, незалежно від того, наскільки фінансово діяв зловмисник (хакери).

Ключові слова: дифереціальна гра якості, кібербезпека, оптимальні стратегії фінансування, система підтримки прийняття рішень.

1. ВСТУП

Найважливішим завданням, що постає перед власниками інформаційних систем (ІС) та службами кіберзахисту, є розв'язок проблеми побудови комплексу методів і засобів захисту від кібератак, який адекватно відповідає внутрішнім і зовнішнім загрозам кібербезпеки та мінімізує ризики значних фінансових і матеріальних втрат [1, 2]. Вирішення цього завдання потребує відповідного інвестування у проекти створення комплексів кібербезпеки [3].

Прийняття рішень щодо фінансування робіт з проектування і створення в ІС комплексів кіберзахисту, а також придбання необхідних програмних та апаратних засобів захисту інформації повинне ґрунтуватись на процедурах, що враховують всю множину суттєвих факторів.

ISSN 2663 - 4023

Складність динамічного стеження за ситуацією, велика множина факторів, що мають бути враховані у галузі кіберзахисту, вимагає розробки та впровадження відповідної автоматизованої системи підтримки прийняття рішень (СППР), яка дозволить в режимі реального часу ефективно обирати рішення щодо раціонального фінансування розвитку системи кібербезпеки ІС та відповідний інструментарій.

Таким чином, постає питання щодо створення для застосування в СППР моделі процесу поточного безперервного фінансування систем кібербезпеки в ІС корпоративних об'єктів інформаційної діяльності.

Зважаючи на викладене, пропонується відповідну модель побудувати виходячі з розв'язку білінійної диференціальної гри якості з двома термінальними поверхнями.

Уявляється доцільним проблему досягнення певного рівня кібербезпеки, аналізувати в контексті протидії двох сторін або гравців: гравець 1 (сторона 1) – служба кіберзахисту, гравець 2 (сторона 2) – порушник системи безпеки (далі – порушник) індивідуального або корпоративного типу.

Відповідно до [3-5] сторона 2 розглядається як певна сукупність потенційних загроз доступності, цілісності і конфіденційності інформаційних ресурсів.

В аналогічних задачах, як відмічене в роботах [6-9], найбільш адекватно описують поведінку систему з двома або більше протиборчими сторонами моделі, що основані на теорії ігор. У випадку відомих стратегій сторін 1 и 2 існує розв'язок задачі раціонального фінансування створення/ розвитку системи кібербезпеки. З точки зору кіберзахисту у порушника безпеки (сторона 2) не вистачить фінансових коштів для подолання системи кіберзахисту ІС (ідеальний варіант). Інший кінцевий результат вказаної задачі відповідає ситуації, в умовах якої внаслідок дефіциту коштів у сторони 1 вона не здатна забезпечити кіберзахист ІС.

Сформулюємо наступну математичну постановку відповідної задачі. Деякою динамічною системою, яка задана системою білінійних диференціальних рівнянь із залежними рухами, керують два гравця. Позначимо множини стратегій 1-го та 2-го гравців як, відповідно, Φ та Ψ, а також оптимальні стратегії 1-го та 2-го гравців рока, як φ_* та ψ_*, відповідно. Також мають бути задані дві термінальних поверхні F_0, G_0.

Ціллю першого гравця є приведення динамічної системи з використанням власних стратегій керування на термінальну поверхню F_0, не зважаючи на обрані стратегії другого гравця. Ціль 2-го гравця полягає у приведенні динамічної системи на основі власних стратегій керування на термінальну поверхню G_0, всупереч можливим діям першого гравця. Рішення полягає в знаходженні множини початкових станів суб'єктів і їх стратегій, які дозволяють їм привести систему на ту, чи іншу поверхню.

В контексті розв'язуваної задачі був поведений аналіз публікацій, в яких для раціонального вибору засобів кібербезпеки для ІС використовуються методи теорії ігор.

Загальний підхід до використання теорії ігор для аналізу взаємодій між учасниками процесу захисту і атаки було викладено в [11, 12], але при цьому не були охоплені всі інтереси сторін, що приймають рішення.

Для розв'язку задачі вибору засобів захисту ІС від зловмисників в роботі [13] запропонована модель, яка заснована на теорії ігор. Робота не отримала розвитку в форматі закінчених рекомендацій і прикладного програмного забезпечення для вирішення аналогічних завдань.

Аналіз теоретико-ігрових методів у задачах забезпечення кібербезпеки також проведено в роботі [14]. При цьому дослідження обмежено лише моделлю для

максимізації сумарної вартості ресурсів для систем захисту інформації без урахування поведінкових стратегій сторін.

Моделі крокових ігор досліджені в [15], при цьому для побудови захисних механізмів від DDoS атак проаналізовані випадки з неповною попередньою інформацію. «Вузьким місцем» згаданого дослідження є необхідність статистичних даних для різних типів засобів кіберзахисту (захисту інформації) для знаходження успішної стратегії гравця 1.

Кінцева безкоаліційна гра з хоча б однією ситуацією рівноваги при змішаних стратегіях сторін розглядалася в роботі [16]. Автори не наводять даних, як знайти ситуацію рівноваги стандартними методами теорії ігор.

Як показав проведений аналіз досліджень в області застосування теорії ігор для визначення стратегій гравців, проблема подальшого розвитку моделей для СППР в завданнях управління процесом фінансування в засоби кіберзахисту ІС залишається актуальною.

Метою подальшого дослідження є розробка моделі для системи підтримки прийняння рішень щодо процесу фінансування в розвиток системи кібербезпеки об'єктів інформаційної діяльності, включаючи сектор національної безпеки і оборони. Розглядаються умови активної протидії з боку 1-го гравця другому. Модель відрізняється від існуючих рішень застосуванням білінійної диференціальної гри якості з декількома термінальними поверхнями.

2. МОДЕЛЬ ФІНАНСУВАННЯ РОЗВИТКУ СИСТЕМИ КІБЕРЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ В РАМКАХ СХЕМИ БІЛІНІЙНОЇ ДИФЕРЕНЦІАЛЬНОЇ ГРИ ЯКОСТІ

Побудуємо математичну модель прийняття рішення стосовно фінансування системи забезпечення кібербезпеки (придбання засобів кіберзахисту) для центру реагування на кіберінциденти ЗГІС ДН ЗВО у сфері національної безпеки і оборони.

В задаче 1 игрок-союзник трактуется для защитника, игрок-противник трактуется для хакера. В задаче 2 игрок-союзник трактуется для хакера, а игрок-противник – для защитника.

Таким чином розглядається ситуація протидії двох гравців, з яких перший – захисник ІС, другий гравець – порушник кібербезпеки. Перший гравець прагне забезпечити захист власної ІС (наприклад, в ситуаційному центрі [17]), другий – реалізувати кібератаку на ІС. Для реалізації поставлених цілей обом гравцям потрібні певні фінансові ресурси. Ситуація з першим гравцем очевидна, тому що сторона захисту в умовах деструктивних впливів на ІС змушена інвестувати в системи кібербезпеки [3-5]. Інша сторона – порушник, внаслідок тих чи інших мотивів, теж може вдатися до фінансування своєї діяльності. При цьому, фінансовий ресурс другого гравця може бути використаний на придбання спеціального програмно-апаратного забезпечення для реалізації кібератак на ІС, підкуп інсайдера тощо.

Вважаємо, що на заданий період часу $[0,T]$, де $T-$ деяке дійсне позитивне число, перший гравець має фінансовий ресурс в розмірі $h_1(0)$, а другий гравець – $h_2(0)$. Ці параметри визначають прогнозну, в момент часу $t=0$, величину фінансових ресурсів, якими володіють гравці 1 і 2 для досягнення своїх цілей.

У початковий момент часу $t=0$ перший гравець примножує величину $h_1(t)$ на

ISSN 2663 - 4023

коефіцієнт $\mu_1(t)$ – темп зміни/зростання. Далі гравець 1 вибирає величину $\varphi(t) \in [0,1]$, яка визначає частку його ресурсу $\mu_1(t) \cdot h_1(t)$, що виділяється їм на кіберзахист в момент часу t. Аналогічно, в момент часу t гравець 2 примножує величину $h_2(t)$ на коефіцієнт $\mu_2(t)$ зміни. Далі гравець 2 вибирає величину $\psi(t) \in [0,1]$, яка визначає частку ресурсу 2-го гравця $\mu_2(t) \cdot h_2(t)$, що виділяється їм на злом ІС в момент часу t.

Динаміка зміни фінансових ресурсів першого і другого гравця задається наступною системою диференціальних рівнянь:

$$\frac{dh_1}{dt} = -h_1(t) + \mu_1(t) \cdot h_1(t) - \varphi(t) \cdot \mu_1(t) \cdot h_1(t) - \delta_2 \cdot \psi(t) \cdot \mu_2(t) \cdot h_2(t);$$

$$\frac{dh_2}{dt} = -h_2(t) + \mu_2(t) \cdot h_2(t) - \psi(t) \cdot \mu_2(t) \cdot h_2(t) - \delta_1 \cdot \varphi(t) \cdot \mu_1(t) \cdot h_1(t),$$

де δ_1 – ефективність вкладень фінансових ресурсів в засоби кіберзахисту;

δ_2 – ефективність вкладень фінансових ресурсів на реалізацію кібератак;

μ_1 – темп зростання фінансового ресурсу 1-го гравця на кіберзахист ІС;

μ_2 – темп зростання фінансового ресурсу 2-го гравця на реалізацію кібератак на ІС.

За суттю величина δ_1, що показує, яка частина фінансового ресурсу буде потрібна порушнику, щоб успішно атакувати ІС, на захист якої була витрачена одиниця фінансового ресурсу першого гравця. Аналогічно, δ_2 – коефіцієнт, що показує, яка частина фінансового ресурсу буде потрібна захиснику ІС, якщо на кібератаку на ІС була витрачена одиниця фінансового ресурсу другого гравця.

Тоді в деякий момент часу t можливо виникнення одної з трьох ситуацій:

1) $h_1(t) > 0, h_2(t) = 0;$
2) $h_1(t) = 0, h_2(t) > 0;$
3) $h_1(t) > 0, h_2(t) > 0.$

У випадку виконання першої умови, вважаємо, що процедура фінансування системи кібербезпеки завершена. В цьому випадку у порушника не вистачило фінансових коштів для подолання захисту ІС.

В разі виконання другої умови, також стверджуємо, що процедура фінансування системи кібербезпеки завершена, але у цьому випадку у сторони захисту не вистачило фінансових коштів для забезпечення ефективного кіберзахисту.

Якщо має місце третя умова, то фінансування системи кібербезпекі буде продовжено.

Зазначимо, що величини $h_1(T)$, $h_2(T)$ показують результат фінансування систем кібербезпеки на плановому проміжку часу $T^* = [0,T].$

Процес фінансування систем кібербезпекі в дослідженні розглядався в рамках схеми позиційної диференціальної гри з повною інформацією [18]. В цьому випадку процес породжує два завдання: з точки зору першого гравця-союзника і другого гравця-союзника [3, 10]. Внаслідок симетричності обмежимося розглядом завдання з точки зору першого гравця-союзника. Друге завдання вирішується аналогічно.

Будемо називати чистою стратегією першого гравця-союзника функцію

$\varphi: T^* \times [0,1] \times [0,1] \to [0,1]$, що ставить у відповідність стану позиції $\left(t,\left(h_1,h_2\right)\right)$ значення $\varphi\left(t,\left(h_1,h_2\right)\right): 0 \le \varphi\left(t,\left(h_1,h_2\right)\right) \le 1.$

Величина $\varphi\left(t,\left(h_1,h_2\right)\right)$ визначає частку фінансового ресурсу гравця захисника ІС, яку він планує витратити на її захист в момент часу t. В рамках схеми позиційної диференціальної гри ніяких припущень щодо інформованості гравця-супротивника не робиться. Це еквівалентно тому, що гравець-противник вибирає своє керуючий вплив на підставі будь-якої інформації.

Після визначення стратегій в задачі 1 необхідно визначити множину «переваги» Z_1 першого гравця. Тобто Z_1 - це множина таких початкових станів $\left(h_1(0),h_2(0)\right)$ фінансових ресурсів захисника і хакера, що мають наступну властивість.

Властивість фінансових ресурсів гравців: для початкових станів існує стратегія першого гравця, яка для будь-яких реалізацій стратегій другого гравця призводить стан системи $\left(h_1(0),h_2(0)\right)$ в таке, при якому буде виконуватися умова 1). При цьому у другого гравця не існує стратегії, яка може привести до виконання умов 2) або 3).

Стратегія $\varphi_*(.,.)$ першого гравця, що задовольняє цій вимозі, називається оптимальною.

Розвязок задачі 1 потребує знаходження множин «переваги» першого гравця і його оптимальних стратегій. Аналогічно ставиться завдання з точки зору другого гравця-союзника.

Розвязок вказаної задачі можна знати за допомогою інструментарію теорії диференціальних ігор якості з повною інформацією [18, 19]. Даний підхід дозволяє знаходити рішення при будь-яких співвідношеннях параметрів гри.

Позначимо R^2_+ – позитивний ортант. Наведемо рішення гри, тобто множини «переваги» і оптимальні стратегії першого гравця.

Варіант 1. $\delta_1 \cdot \delta_2 = 1,\ \mu_2 \ge \mu_1.$ В цьому випадку отримуємо:

$$Z_1 = \left\{\left(h_1(0),h_2(0):\left(h_1(0),h_2(0)\right)\right) \in \operatorname{int} R^2_+,\ \delta_1 \cdot \mu_1 \cdot h_1(0) > \mu_2 \cdot h_2(0)\right\},$$

де Z_1 – множина переваги 1-го гравця;

$\varphi_*\left(h_1,h_2\right) = \left\{1, \text{для } \delta_1 \cdot \mu_1 \cdot h_1(0) > \mu_2 \cdot h_2(0)\right\}, \left(h_1,h_2\right) \in \operatorname{int} R^2_+,$ і не визначена в іншому випадку.

Варіант 2. $\delta_1 \cdot \delta_2 = 1,\ \mu_2 < \mu_1.$ В цьому випадку отримуємо:

$$Z_1 = \left\{\left(h_1(0),h_2(0):\left(h_1(0),h_2(0)\right)\right) \in \operatorname{int} R^2_+,\ \delta_1 \cdot \mu_1 \cdot h_1(0) > \mu_2 \cdot h_2(0)\right\},$$

$$\varphi_*\left(h_1,h_2\right) = \left\{0, \text{для } \mu_2 \cdot h_2 < \delta_1 \cdot \mu_1 \cdot h_1 < \mu_1 \cdot h_2, \left(h_1,h_2\right) \in \operatorname{int} R^2_+\right\};$$

$\varphi_*(h_1,h_2) = \left\{1, \text{для } \delta_1 \cdot \mu_1 \cdot h_1 > \mu_1 \cdot h_2, \left(h_1,h_2\right) \in \operatorname{int} R^2_+\right\}$, і не визначена, в іншому випадку.

Варіант 3. $\delta_1 \cdot \delta_2 \gg 1, \mu_1 \gg \delta_1 \cdot \mu_1 \cdot \delta_2.$

Тут $\varphi_*(.,.), Z_1$ визначаються таким же чином, як і в варіанті 1.

Вариант 4. $\delta_1 \cdot \delta_2 \gg 1, \mu_1 \le \mu_2 \ll \delta_1 \cdot \mu_1 \cdot \delta_2.$

ISSN 2663 - 4023

В цьому випадку отримуємо:

$$Z_1 = \left\{\left(h_1(0), h_2(0) : \left(h_1(0), h_2(0)\right)\right) \in \operatorname{int} R_+^2,\ \delta_1 \cdot \mu_1 \cdot h_1(0) > \left(\delta_1 \cdot \mu_1 \cdot \delta_2 \cdot \mu_2\right)^{0.5} \cdot h_2(0)\right\},$$

$$\varphi_*\left(h_1, h_2\right) = \left\{1, \text{при } \delta_1 \cdot \mu_1 \cdot h_1 > \left(\delta_1 \cdot \mu_1 \cdot \delta_2 \cdot \mu_2\right)^{0.5} \cdot h_2, \left(h_1, h_2\right) \in \operatorname{int} R_+^2\right\}, \left(h_1, h_2\right) \in \operatorname{int} R_+^2,$$

і не визначена в іншому випадку.

Вариант 5. $\delta_1 \cdot \delta_2 \gg 1, \frac{\mu_1}{\delta_1 \cdot \delta_2} \ll \mu_2 \le \mu_1$

Тут $\varphi_*(.), Z_1$ визначаються таким же чином, як і в варіанті 4.

Варіант 6. $\delta_1 \cdot \delta_2 \gg 1, \mu_2 \ll \frac{\mu_1}{\delta_1 \cdot \delta_2}$.

$$Z_1 = \left\{(h_1(0), h_2(0) : (h_1(0), h_2(0))) \in \operatorname{int} R_+^2,\ \mu_1 \cdot h_1(0) > \delta_2 \cdot \mu_2 \cdot h_2(0)\right\},$$

$$\varphi_*\left(h_1, h_2\right) = \left\{0, \textit{для } \delta_1 \cdot \mu_1 \cdot \delta_2 \cdot h_2 < \delta_1 \cdot \mu_1 \cdot h_1 < \mu_2 \cdot h_2, \left(h_1, h_2\right) \in \operatorname{int} R_+^2\right\};$$

$\varphi_*(h_1, h_2) = \left\{1, \textit{для } \delta_1 \cdot \mu_1 \cdot h_1 > \mu_2 \cdot h_2, \left(h_1, h_2\right) \in \operatorname{int} R_+^2\right\}$, і не визначена, в іншому випадку.

Варіант 7. $\delta_1 \cdot \delta_2 \ll 1, \mu_2 \ge \mu_1$.

Тут $\varphi_*(.,.), Z_1$ визначаються таким же чином, як і в варіанті 1.

Варіант 8. $\delta_1 \cdot \delta_2 \ll 1, \delta_1 \cdot \mu_1 \cdot \delta_2 \le \mu_2 \ll \mu_1$.

В цьому випадку отримуємо:

$$Z_1 = \left\{\left(h_1(0), h_2(0) : \left(h_1(0), h_2(0)\right)\right) \in \operatorname{int} R_+^2,\ \mu_1 \cdot h_1(0) > \delta_2 \cdot \mu_2 \cdot h_2(0)\right\},$$

$$\varphi_*\left(h_1, h_2\right) = \left\{0, \text{при } \delta_1 \cdot \mu_2 \cdot \delta_2 \cdot h_2 < \delta_1 \cdot \mu_1 \cdot h_1 < \mu_1 \cdot h_2, \left(h_1, h_2\right) \in \operatorname{int} R_+^2\right\};$$

$\varphi_*(h_1, h_2) = \left\{1, \textit{для } \delta_1 \cdot \mu_1 \cdot h_1 \ge \mu_1 \cdot h_2, \left(h_1, h_2\right) \in \operatorname{int} R_+^2\right\}$, і не визначена в іншому випадку.

Варіант 9. $\delta_1 \cdot \delta_2 \ll 1, \mu_2 \ll \delta_1 \cdot \mu_2 \cdot \delta_2$.

Тут $\varphi_*(.), Z_1$ визначаються таким же чином, як і в варіанті 8.

Завдання з точки зору другого гравця-союзника вирішується аналогічно.

Множини «переваги» (конуси) з точки зору другого гравця-союзника «примикають» до множин «перевагу» першого гравця-союзника. Ці множини розділяються між собою променями збалансованості.

Промені збалансованості мають наступну властивість: якщо пара $\left(h_1(0), h_2(0)\right)$ належить променю, то у гравців існують стратегії, які дають можливість перебувати на промені збалансованості для всіх наступних моментів часу. Це може дозволити при заданих $\left(h_1(0), h_2(0)\right)$ знайти співвідношення на параметри взаємодії, при яких пара $\left(h_1(t), h_2(t)\right)$ буде перебувати на промені збалансованості.

3. РЕЗУЛЬТАТИ ОБЧИСЛЮВАЛЬНОГО ЕКСПЕРИМЕНТУ

Обчислювальний експеримент був проведений в середовищі Mathcad 15.

Ціль експерименту – визначити множини стратегій гравців Φ і Ψ. Розглянуті

випадки, коли стратегії гравців виводять їх на відповідні термінальні поверхні F_0, G_0. В ході експерименту знайдені множини початкових станів об'єктів і їх стратегій, які дозволяють об'єктам привести систему на ту, чи іншу термінальну поверхню.

Результати експерімента демонструють ефективність запропонованого підходу, підчас тестування моделі підтверджена коректність отриманих результатів.

Подальшу апробацію запронованого підходу доцільно продовжити з урахуванням результатів реальних інвестиційних проектів в сфері кібербезпеки України [19, 20].

В [19, 20] підтверджена прийнятна точність роботи програмного модуля СППР в співвідношенні з результатами обчислювальних експериментів в Mathcad 15. Розбіжність в середньому становило 3-7%.

Зауважимо, що запропонована модель описує процес прогнозування результатів інвестування в засоби кібербезпекі для ІС. Виявленим недоліком моделі, є той факт, що отримані дані прогнозної оцінки при виборі стратегій інвестування в засоби кібербезпекі, певні похибки порівняно з фактичними даними.

За результатами обчислювальних експериментів та на основі даних практичної апробації [19, 20], встановлено, що запропонована модель в рамках схеми билинейной диференціальної гри якості для системи підтримки прийняття рішень в ході керування фінансуванням в кібербезпекі ІС, дозволяє адекватно описувати залежні рухи за допомогою білінійних функцій. Це дає ефективний інструментарій для учасників інвестиційного процесу в засоби кібербезпекі. У порівнянні з наявними моделями, запропоноване рішення покращує показники ефективності і прогнозованості для інвестора в середньому на 11-15% [15, 16, 21, 22].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] M. Fey, B. Kenyon, K. Reardon, B. Rogers and C. Ross, *Security Battleground: An Executive Manual, IntelPRESS*. 2013, p. 240.

[2] C. Zimmerman, *Ten Strategies of a World-Class. Cybersecurity Operations Center*. MITRE Corporate Communications and Public Affairs, 2014, p. 334.

[3] M. Manshaei, Q. Zhu and T. Alpcan, "Game theory meets network security and privacy", *ACM Computing Surveys*, vol. 48, pp. 51-61, 2015.

[4] N. Ben–Asher, C. Gonzalez, "Effects of cyber security knowledge on attack detection", *Computers in Human Behavior*, vol. 48, pp. 51–61, 2015.

[5] K. Goztepe, "Designing Fuzzy Rule Based Expert System for Cyber Security", *International Journal of Information Security Science*, vol. 1, no. 1, pp. 13-19, 2012.

[6] J. Grossklags, "Secure or insure?: a game-theoretic analysis of information security games", in *17th international conference on World Wide Web*, Beijing, China, 2008, pp. 209-218.

[7] H. Cavusoglu, B. Mishra, S. Raghunathan, "A model for evaluating IT security investments", *Communications of the ACM*, vol. 47, no. 7, pp. 87–92, 2004,

[8] A. Fielder, E. Panaousis, P. Malacaria et al, "Decision support approaches for cyber security investment", *Decision Support Systems*, vol. 86, pp. 13–23, 2016.

[9] P. Meland, I. Tondel, B. Solhaug, "Mitigating risk with cyberinsurance", *IEEE Security & Privacy*, no. 13(6), pp. 38–43, 2015.

[10] V. Malyukov, "A differential game of quality for two groups of objects", *Journal of Applied Mathematics and Mechanics*, vol. 55, no.5, pp. 596 – 606, 1991.

[11] A. Lavrent'ev, V. Zjazin, "O primenenii metodov teorii igr dlja reshenija zadach komp'juternoj bezopasnosti", *Bezopasnost' informacionnyh tehnologij*, no. 3, pp. 19 – 24, 2013.

[12] A. Bykov, N. Altuhov and A. Sosenko, "Zadacha vybora sredstv zashhity informacii v avtomatizirovannyh sistemah na osnove modeli antagonisticheskoj igry", *Inzhenernyj vestnik*, no. 4, pp. 525–542, 2014.

[13] G. Basalova, A. Sychugov, "Primenenie metodov teorii igr dlja optimizacii vybora sredstv zashhity informacii", *Izvestija Tul'skogo gosudarstvennogo universiteta, Tehnicheskie nauki*, no. 11(1), pp. 122–

128, 2016.
[14] A. Fielder, E. Panaousis, P. Malacaria et al, "Game theory meets information security management", in *IFIP International Information Security Conference*, Marrakech, Morroco, 2014, pp. 15–29.
[15] R. Zarkumova, "Primenenie metodov teorii igr pri vybore sredstva jeffektivnoj zashhity", *Sbornik nauchnyh trudov Novosibirskogo gosudarstvennogo tehnicheskogo universiteta*, no. 4, pp. 41–46, 2009.
[16] X. Gao, W. Zhong and S. Mei, "A game-theoretic analysis of information sharing and security investment for complementary firms", *Journal of the Operational Research Society*, vol. 65, no. 11, pp. 1682–1691, 2014.
[17] V. Lakhno, "Model' intellektual'noj sistemy upravlenija gorodskimi avtobusnymi perevozkami", *Radioelektronika, informatika, upravlinnja*, no. 2, pp. 119–127, 2016.
[18] V. Malyukov, "Discrete-approximation method for solving a bilinear differential game", *Cybernetics and Systems Analysis*, vol. 29, no. 6, pp. 879 – 888, 1993.
[19] V. Lakhno, V. Malyukov, N. Gerasymchuk et al, "Development of the decision making support system to control a procedure of financial investment", *Eastern-European Journal of Enterprise Technologies*, vol. 6, no. 3, pp. 24–41, 2017.
[20] V. Lakhno, "Development of a support system for managing the cyber security", *Radio Electronics, Computer Science, Control*, no. 2, pp. 109–116, 2017.
[21] F. Smeraldi and P. Malacaria, "How to spend it: optimal investment for cyber security", in *1st International Workshop on Agents and CyberSecurity*, Paris, France, 2014, p. 8.
[22] D. Tosh, M. Molloy and S. Sengupta, "Cyber-investment and cyber-information exchange decision modeling", in *High Performance Computing and Communications IEEE 7th International Symposium on Cyberspace Safety and Security (CSS)*, New York, 2015, pp. 1219-1224.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (6), 2019
ISSN 2663 - 4023

Hennadii Hulak
PhD Technical sciences,
Head of Laboratory Research CyberSecurity Department
Institute of Mathematical Machines and Systems Problems,
National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0001-9131-9233
h.hulak@ukr.net

Valeriy Lakhno
Dr. Sc., Professor,
Head of Department of computer systems and network
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0001-9695-4543
Valss21@ukr.net

MODEL OF THE INVESTMENT PROCESS IN CYBER SECURITY DEVELOPMENT FOR BUILDING A DECISION SUPPORT SYSTEM

Abstract. The topical problem of making the optimal decision on financing pro-jects in the field of cybersecurity in the conditions of active actions of cybersecu-rity violators is considered. A model has been developed for a decision support system for financing projects for the creation and development of cybersecurity management centers for critical infrastructure facilities. The model assumes meth-ods and means of actively countering the attacking side. In contrast to existing approaches, the model is based on solving a bilinear differential quality game with several terminal surfaces. A discrete approximation method was used in the solution. This made it possible to find a solution to the bilinear differential quality game with dependent movements. The results of a computational experiment within the framework of the software implementation of a decision support sys-tem in the field of financing projects in the field of cybersecurity, in particular, in the creation and development of cybersecurity management centers for critical in-frastructure facilities are described. The developed decision support system al-lows obtaining optimal financing strategies by the side of cybersecurity protec-tion. In this case, any ratio of parameters describing the financing process is con-sidered, no matter how financially the attacker (hackers) acted.

Keywords: differential quality game, cyber security, optimal financing strategies, decision support system.

REFERENCES

[1] M. Fey, B. Kenyon, K. Reardon, B. Rogers and C. Ross, *Security Battleground: An Executive Manual, IntelPRESS*. 2013, p. 240.
[2] C. Zimmerman, *Ten Strategies of a World-Class. Cybersecurity Operations Center*. MITRE Corporate Communications and Public Affairs, 2014, p. 334.
[3] M. Manshaei, Q. Zhu and T. Alpcan, "Game theory meets network security and privacy", *ACM Computing Surveys*, vol. 48, pp. 51-61, 2015.
[4] N. Ben–Asher, C. Gonzalez, "Effects of cyber security knowledge on attack detection", *Computers in Human Behavior*, vol. 48, pp. 51–61, 2015.
[5] K. Goztepe, "Designing Fuzzy Rule Based Expert System for Cyber Security", *International Journal of Information Security Science*, vol. 1, no. 1, pp. 13-19, 2012.
[6] J. Grossklags, "Secure or insure?: a game-theoretic analysis of information security games", in *17th international conference on World Wide Web*, Beijing, China, 2008, pp. 209-218.
[7] H. Cavusoglu, B. Mishra, S. Raghunathan, "A model for evaluating IT security investments", *Communications of the ACM*, vol. 47, no. 7, pp. 87–92, 2004,
[8] A. Fielder, E. Panaousis, P. Malacaria et al, "Decision support approaches for cyber security investment", *Decision Support Systems*, vol. 86, pp. 13–23, 2016.
[9] P. Meland, I. Tondel, B. Solhaug, "Mitigating risk with cyberinsurance", *IEEE Security & Privacy*, no. 13(6), pp. 38–43, 2015.

[10] V. Malyukov, "A differential game of quality for two groups of objects", *Journal of Applied Mathematics and Mechanics*, vol. 55, no.5, pp. 596 – 606, 1991.
[11] A. Lavrent'ev, V. Zjazin, "O primenenii metodov teorii igr dlja reshenija zadach komp'juternoj bezopasnosti", *Bezopasnost' informacionnyh tehnologij*, no. 3, pp. 19 – 24, 2013.
[12] A. Bykov, N. Altuhov and A. Sosenko, "Zadacha vybora sredstv zashhity informacii v avtomatizirovannyh sistemah na osnove modeli antagonisticheskoj igry", *Inzhenernyj vestnik*, no. 4, pp. 525–542, 2014.
[13] G. Basalova, A. Sychugov, "Primenenie metodov teorii igr dlja optimizacii vybora sredstv zashhity informacii", *Izvestija Tul'skogo gosudarstvennogo universiteta, Tehnicheskie nauki*, no. 11(1), pp. 122–128, 2016.
[14] A. Fielder, E. Panaousis, P. Malacaria et al, "Game theory meets information security management", in *IFIP International Information Security Conference*, Marrakech, Morroco, 2014, pp. 15–29.
[15] R. Zarkumova, "Primenenie metodov teorii igr pri vybore sredstva jeffektivnoj zashhity", *Sbornik nauchnyh trudov Novosibirskogo gosudarstvennogo tehnicheskogo universiteta*, no. 4, pp. 41–46, 2009.
[16] X. Gao, W. Zhong and S. Mei, "A game-theoretic analysis of information sharing and security investment for complementary firms", *Journal of the Operational Research Society*, vol. 65, no. 11, pp. 1682–1691, 2014.
[17] V. Lakhno, "Model' intellektual'noj sistemy upravlenija gorodskimi avtobusnymi perevozkami", *Radioelektronika, informatika, upravlinnja*, no. 2, pp. 119–127, 2016.
[18] V. Malyukov, "Discrete-approximation method for solving a bilinear differential game", *Cybernetics and Systems Analysis*, vol. 29, no. 6, pp. 879 – 888, 1993.
[19] V. Lakhno, V. Malyukov, N. Gerasymchuk et al, "Development of the decision making support system to control a procedure of financial investment", *Eastern-European Journal of Enterprise Technologies*, vol. 6, no. 3, pp. 24–41, 2017.
[20] V. Lakhno, "Development of a support system for managing the cyber security", *Radio Electronics, Computer Science, Control*, no. 2, pp. 109–116, 2017.
[21] F. Smeraldi and P. Malacaria, "How to spend it: optimal investment for cyber security", in *1st International Workshop on Agents and CyberSecurity*, Paris, France, 2014, p. 8.
[22] D. Tosh, M. Molloy and S. Sengupta, "Cyber-investment and cyber-information exchange decision modeling", in *High Performance Computing and Communications IEEE 7th International Symposium on Cyberspace Safety and Security (CSS)*, New York, 2015, pp. 1219-1224.