© Lakhno V., Malyukov V., Kasatkin D., Bloshova A., Matievsky V. The model of financing of smart city cyber security with procedure of obtaining additional data for the defense // Ukrainian Scientific Journal of Information Security, 2019, vol. 25, issue 1, pp. 38-44.

DOI: 10.18372/2225-5036.25.13667

МОДЕЛЬ ФІНАНСУВАННЯ ЗАСОБІВ КІБЕРБЕЗПЕКИ SMART CITY З ПРОЦЕДУРОЮ ОТРИМАННЯ ДОДАТКОВИХ ДАНИХ СТОРОНОЮ ЗАХИСТУ

Валерій Лахно[1], Володимир Малюков[1], Дмитро Касаткін[1], Андрій Блозва[1], Володимир Матієвський[2]

[1]Національний університет біоресурсів і природокористування України, Україна
[2] Луганський національний університет імені Тараса Шевченка, Україна

ЛАХНО Валерій Анатолійович, д.т.н., професор

Рік та місце народження: 1961 рік, м. Київ, Україна.
Освіта: Луганський машинобудівний інститут (з 2001 року Східноукраїнський Національний університет імені Володимира Даля), 1987 рік.
Посада: завідувач кафедри комп'ютерних систем і мереж НУБіП України.
Наукові інтереси: інформаційна безпека, безпека інформаційно-комунікаційних систем.
Публікації: більше 180 наукових публікацій, серед яких монографії, навчальні посібники, підручники, наукові статті та патенти на винаходи.
E-mail: lva964@nubip.edu.ua.
Orcid ID: 0000-0001-9695-4543.

МАЛЮКОВ Володимир Павлович, д.фіз-мат.н., доцент

Рік та місце народження: 1951рік, м. Київ, Україна.
Освіта: Новосибірський державний університет, Математика, Прикладна математика, 1973 рік..
Посада: професор кафедри комп'ютерних систем і мереж НУБіП України.
Наукові інтереси: математичне моделювання, теорія ігор, прикладні задачі з кібербезпеки.
Публікації: більше 100 наукових публікацій, серед яких монографії, наукові статті.
E-mail: volod.malyukov@gmail.com.
Orcid ID: 0000-0002-7533-1555.

КАСАТКІН Дмитро Юрійович, к.пед.н., доцент, академік Академії наук вищої освіти України

Рік та місце народження: 1975 рік, м. Київ, Україна.
Освіта: Національний аграрний університет, 1997 рік.
Посада: доцент кафедри комп'ютерних систем і мереж НУБіП України.
Наукові інтереси: інформаційно-комунікаційні технології, інформаційна безпека, системи проектування SMART CITY.
Публікації: більше 80 наукових публікацій, серед яких монографії, наукові статті, матеріали та тези доповідей на конференціях, підручники і навчальні посібники.
E-mail: d.kasatkin@nubip.edu.ua.
Orcid ID: 0000-0002-2642-8908.

БЛОЗВА Андрій Ігорович, к.пед.н

Рік та місце народження: 1989 рік, м. Борщів, Тернопільська область, Україна.
Освіта: Національний університет біоресурсів і природокористування України, 2010 рік.
Посада: доцент кафедри комп'ютерних систем і мереж НУБіП України.
Наукові інтереси: інформаційна безпека у комп'ютерних мережах.
Публікації: більше 20 наукових публікацій, серед яких монографії, наукові статті, матеріали та тези доповідей на конференціях, підручник та навчальні посібники.
E-mail: andriy.blozva@nubip.edu.ua.
Orcid ID: 0000-0002-4377-0916.

МАТІЄВСЬКИЙ Володимир Валерійович

Рік та місце народження: 1977 рік, м. Луганськ, Україна.
Освіта: Луганський національний університет імені Тараса Шевченка, 2001.
Посада: асистент кафедри інформаційних технологій та систем ЛНУ імені Тараса Шевченка.
Наукові інтереси: інформаційна безпека, Machine Learning, Data Mining.
Публікації: 10 наукових публікацій, серед яких наукові статті, матеріали та тези доповідей на конференціях.
E-mail: m_vv@outlook.com.
Orcid ID: 0000-0002-1954-8493.

Анотація. *У статті викладена модель вибору стратегій фінансування засобів кібербезпеки Smart City при неповній інформації про фінансові ресурси атакуючої сторони. Запропонована модель, є ядром модуля розробляється системи підтримки прийняття рішень в задачах вибору раціональних варіантів інвестування в захист інформації та кібербезпека Smart City. Модель дозволяє знаходити фінансові рішення за допомогою інструментарію теорії багатокрокових ігор з декількома термінальними поверхнями. Авторами запропонований підхід, який дозволяє менеджменту інформаційної безпеки проводити попередню оцінку стратегій щодо фінансування ефективних систем кіберзахисту Smart City. Модель відрізняє допущення, що сторона захисту не має повної інформації, як про фінансові стратегії атакуючої сторони, так і про станах його фінансових ресурсів, спрямованих на подолання контурів кібербезпеки об'єкта інформатизації. Враховуючі останні дослідження в сфері кіберзахисту можна стверджувати, що тактики та стратегії сторони нападу можуть бути досі різноманітними та відповідно ускладнювати для сторони захисту завдання вибору раціональної стратегії фінансування відповідних засобів кібербезпеки. При цьому сторона захисту має можливість отримання додаткової інформації за рахунок витрати частини своїх фінансових ресурсів. Це дає можливість отримання стороною захисту позитивного для себе результату в разі, коли вона не може його отримати без цієї процедури. Рішення знайдено з використанням математичного апарату нелінійної багатокрокової гри якості з декількома термінальними поверхнями з послідовними ходами. Для перевірки адекватності моделі був реалізований багатоваріантний обчислювальний експеримент. Результати даного експерименту описані в статті. Подальший розвиток цього напряму досліджень полягає у створенні повноцінного програмного продукту, наприклад у вигляді системи підтримки прийняття рішень по вибору раціональної фінансової стратегії стороною захисту при інвестуванні у конкретні проекти кібербезпеки Smart City.*

Ключові слова: *кібербезпека, Smart City, теорія ігор, вибір фінансової стратеги, процедура отримання додаткової інформації, система підтримки прийняття рішень.*

Вступ

Сьогодні практично будь-який проект в області Smart City вимагає вивчення питань, пов'язаних з кібербезпекою і захистом інформації. Подібні об'єкти інформатизації (ОбІ), як правило, мають свою систему захисту інформації (СЗІ) та кібербезпеки (КрБ). Сучасні СЗІ та КрБ для Smart City це багато ешелоновані комплекси. Сучасні методи і засоби захисту інформації та кібербезпеки дозволяють досить надійно захищати інформаційні ресурси різних ОбІ (зокрема, Smart City) від зовнішніх загроз. Однак не завжди при реалізації СЗІ та КрБ до уваги береться такий важливий канал витоку секретних даних, як персонал, що обслуговує подібні комплекси. В [1, 2] було показано, що захист даних від інсайдерів - це проблема перманентна і універсальна, яка не залежить від масштабів Smart City. Різного роду дані, одержувані від інсайдерів, можуть послужити основою для вибору різних стратегій (в тому числі фінансової стратегії) атакуючої сторони. При цьому вважаємо, що дії хакерів (тобто атакуючої сторони) також пов'язані з витратами фінансового ресурсу на злом [3]. Як джерело отримання додаткової інформації про атакуючої стороні можна використовувати закриті дані для отримання, яких потрібен фінансовий ресурс захисника. Наприклад, додаткові відомості про нові технології злому, використовуваних хакерами, або пошук інсайдера в рамках ОбІ.

В [4, 5] показано, що однією з головних проблем при побудові комплексних СЗІ та КрБ, є вибір раціональної стратегії інвестування в подібні системи захисту ОбІ. Сформований в останні роки тренд на інтелектуалізацію підтримки прийняття рішень [6, 7] в області завдань забезпечення кібербезпеки ОбІ, дозволив по-новому поглянути на досі невирішені завдання для подібних систем. Зокрема, актуальною залишається завдання розробки нових моделей на вибір раціональних стратегій фінансування СЗІ та КрБ, зокрема для ситуацій, коли, з'являються нові технології злому, викликають зміна рівня кіберризиків для ОбІ, а, отже, веде до необхідності перегляду стратегій фінансування на захист інформації і кібербезпеки

Мета статті

Розробка моделі для системи підтримки прийняття рішень по вибору раціональних стратегій фінансування систем кіберзахисту об'єкта інформатизації на прикладі Smart City, з урахуванням процедури отримання додаткової інформації про атакуючої стороні, стороною захисту та відповідних витратах фінансового ресурсу на системи кібербезпеки

Огляд літератури

У роботах [8-10] досить докладно були викладені методології створення різних модулів для систем підтримки рішень в області фінансування СЗІ та КрБ для інформаційних систем різного призначення. Загальним недоліком, запропонованих різними авторами підходів є відсутність розглянутих варіан-

тів на вибір стратегій інвестування в СЗІ та КрБ, в ситуаціях, коли сторона захисту не має повної інформації про фінансові ресурси (ФіР) атакуючих. Справді це важлива інформація [11], тому що дозволяє в кінцевому підсумку зрозуміти потенційні можливості зломщиків. Адже фінансовий ресурс, нехай навіть потужного хакерського угрупування і ресурс кібервійськ з боку потенційного супротивника може відрізнятися у рази [3].

Наше нове дослідження розвиває ідеї, раніше викладені авторами в роботах [12, 13]. В рамках запропонованої схеми вибору стратегій фінансування в СЗІ та КрБ ОбІ, заснованої на теорії ігор. Відповідно до подібних робіт, що базуються також на теорії [14, 15], розглядаються дві сторони: гравець №1 - захисник інформації (ЗІН); гравець №2 - хакер. Обидва гравці використовують фінансові ресурси для досягнення своїх цілей [13, 16]. Зауважимо, що в рамках аналізу наявних підходів, нам не вдалося виявити докладних викладок, що розглядають ситуацію, коли ЗІН має повну інформацію про ФіР атакуючих. Відповідно до [13, 14, 16], відміну від гри з повною інформацією полягає в тому, що ЗІН точно не відомо початкове фінансовий стан другого гравця (хакера).

З урахуванням вищесказаного, представляється релевантної завдання вдосконалення моделі по вибору раціональних стратегій фінансування СЗІ та КрБ ОбІ з введенням в неї процедури отримання додаткової інформації стороною захисту за рахунок витрати їм частини своїх ресурсів на її отримання.

Моделі та методи

В [13, 17] розглянутій ситуації, коли були знайдені безлічі перевагу першого гравця і знайдені його оптимальні стратегії. Це означало, що якщо стану гравців належать безлічі перевагу першого гравця, то у нього існує стратегія, реалізація якої дозволить йому досягти своєї мети. Таким чином, із заданою вірогідністю гравець 1 (тобто захисник інформації – ЗІН) призводить систему в стан, який відображає позитивний для нього результат. Однак можливі ситуації, коли захисникові потрібно отримати позитивний для нього результат з станів, з яких він при стандартному завданні правил гри не може зробити. Наприклад, він обмежений у часі взаємодії. Тоді за доцільне введення процедури отримання додаткової інформації за рахунок витрати на її отримання частини своїх ресурсів.

Постановка задачі

Нижче буде приведена постановка задачі про фінансування захисника інформації та її зломщика (хакера) з введенням в неї процедури отримання додаткової інформації зін за рахунок витрати їм частини своїх ресурсів на її отримання.

Є два гравці (дві сторони). Один гравець - ЗІН (наприклад, захисник інформаційної системи - ЗІН-Су). Другий гравець - зломщик інформаційної системи (хакер). Перший гравець прагне забезпечити захист своєї ІВ. Другий - провести злом системи з метою порушення її нормального функціонування.

Обом гравцям потрібні фінансові ресурси для реалізації своїх цілей. Будемо вважати, що на заданий період часу $\{0,1,\ldots,T\}$ (Т–натуральне число) у ЗІН виділено $x(0)$ фінансових ресурсів (ФіР). У іншого гравця, відповідно – $y^{\xi}(0)$. Ці ресурси визначають прогнозовану, в момент часу $t=0$, величину ФіР, якими володіють гравці на досягнення своїх цілей. Відбувається взаємодія гравців. Ця взаємодія буде описуватися як білінійная багатокрокова гра з послідовними ходами з неповною інформацією. На відміну від гри з повною інформацією ЗІН точно не відомо початковий стан другого гравця. Однак ЗІН відома функція розподілу початкових станів $F_0(\cdot)$ іншого гравця. Ця функція є рівномірним розподілом у сегменті $[a-r, a+r] \subseteq R_+$. Також відомі початковий стан і параметри першого гравця, що визначають взаємодію і, крім того, в кожен момент часу t йому відомі всі свої статки $x(\tau)$ для $\tau \le t$. Вважається, що перший гравець (ЗіН) може отримувати додаткову інформацію за рахунок витрати частини свого ФіР. Випливає це з результатів введення параметра $k\,(k \in [0,1])$, який визначає частину ресурсу першого гравця. Дана частина ФіР дорівнює $(1-k)\cdot z$ (де z – величина ресурс ЗіН), який йде на отримання інформації про те, що випадкові стани іншого гравця (хакера) рівномірно розподілені у сегменті $\left[c-k^2 d, c+k^2 d\right]$ (де $[c-d, c+d]$ – сегмент, у якому розподілені випадкові стани). Міркування проводяться з позиції першого гравця (тобто ЗіН), тому про інформованість другого гравця (хакера) ніяких припущень не робиться. Кроки гравцями виробляються по черзі. У парні моменти крок робить перший гравець, в непарні - другий.

Нехай $t=2n$ і $x(t), x(t+1)$ – стан першого гравця в моменти часу $t, t+1$. Також $y^{\xi}(t), y^{\xi}(t+1)$ – випадкові стану другого гравця в моменти часу $t, t+1$. Тоді стан гравців у момент часу $t+1, t+2$ визначаються із співвідношень:

$$\begin{aligned} x(t+1) &= k(t)\cdot\alpha\cdot x(t) - u(t)\cdot k(t)\cdot\alpha\cdot x(t); \\ y^{\xi}(t+1) &= y^{\xi}(t) - s_1\cdot u(t)\cdot k(t)\cdot\alpha\cdot x(t); \end{aligned} \quad (1)$$

$$\begin{aligned} y^{\xi}(t+2) &= \beta\cdot y^{\xi}(t+1) - v(t)\cdot\beta\cdot y^{\xi}(t+1); \\ x(t+2) &= x(t+1) - s_2\cdot v(t)\cdot\beta\cdot y^{\xi}(t+1). \end{aligned} \quad (2)$$

Тут $u(t),\ v(t),\ k(t)\colon u(t)\in[0,1],\ v(t)\in[0,1],\ k(t) \in [0,1];\ s_1>0,\ s_2>0$.

В момент часу $t \in \{0,2,4,\ldots,2n\}$ перший гравець (ЗіН) множить величину $x(t)$ на коефіцієнт (темп зміни) росту α. Далі ЗіН обирає величини $u(t)\,(u(t)\in[0,1]), k(t)\,(k(t)\in[0,1])$, які визначають долю ресурсу першого гравця $\alpha\cdot x(t)$, що виокремлює ЗіН на кіберзахист і отримання додаткової інформації у момент часу *t*. Тоді стан гравців у момент часу $t+1$ визначається із співвідношень (1). Тобто другий гравець (хакер) змушений виокремлювати для зламу кібербезпеки ЗіН величину $s_1\cdot u(t)\cdot k(t)\cdot \alpha\cdot x(t)$. В даному виразі прийнято, що s_1 – коефіці-

єнт, який визначає «ефективність» вкладення коштів другого гравця на розробку або на закупівлю інструментів зламу кіберзахисту ЗіН.

У разі якщо виконується умова: $P\left(y^{\xi}(t+1)<0\right) \geq p_0, (0 \leq p_0 \leq 1)$ будемо говорити, що перший гравець (ЗіНС) гарантував собі захист із ймовірністю p_0 і процедура фінансування засобів кіберзахисту завершена. В протилежному випадку процедура фінансування засобів кіберзахисту зі сторони першого гравця продовжиться.

Свій хід здійснює зломщик (хакер). Він діє так само, як і перший гравець (ЗіНС) без використання процедури отримання додаткової інформації. І тоді стани гравців визначаються з співвідношень (2). Якщо виявиться, що після здійснення ходу зломщиком (хакером) буде виконуватися умова: $P\left(x(t+2)>0\right) < p_1, (0 \leq p_1 \leq 1)$, то вважаємо, що зломщик наніс збиток ІС з ймовірністю більше $(1-p_1)$. Тоді процедура фінансування засобів кібербезпеки для даної конфігурації бар'єрів захисту закінчена.

Перший гравець прагне знайти безліч своїх початкових станів (ПС), які мають наступну властивість. Властивість: якщо гра почнеться з ПС, то перший гравець може вибором своїх керуючих впливів $u(0), k(0), ..., u(t), k(t)(t=2n)$ забезпечити захист своєї ІС з ймовірністю більше p_0. При цьому ЗіНС в стані не допустити нанесення збитку хакером з ймовірністю більше $(1-p_1)$. Безліч таких станів будемо називати множиною перевагу першого гравця.

Безліч перевагу ЗіНСу з урахуванням процедури отримання додаткової інформації відрізняються від множин переваги першого гравця без цієї процедури наступним обставинам. За рахунок того, що перший гравець, отримуючи додатковий інформацію під час здійснення свого ходу (і витрачаючи частину свого ФіР), може забезпечити собі досягнення позитивного результату з станів, в яких він не міг цього зробити при відсутності цієї процедури. Велика кількість параметрів, різних випадків в розглянутій задачі «змушують» в рамках статті обмежитися розглядом процедури отримання додаткової інформація під час здійснення першим гравцем на першому кроці. Розгляд випадків реалізації процедури отримання додаткової інформації на наступних кроках абсолютно аналогічно. Відзначимо, що розгляд процедури отримання інформації на першому кроці впливає на весь процес взаємодії на всіх етапах.

Надалі будемо вважати, що $p_1 = p_0$.

Безліч переваг першого гравця на кроці T для випадку з використанням процедури додаткової інформації будемо позначати через $V^{T}_{1,k(1)}(p_0, p_0)$.

$T=1$. При $p_0: 0 \leq p_0 \leq 0{,}5$ будет $V^{1}_{1,k(1)}(p_0, p_0) = \varnothing$.

– При $p_0: 0{,}5 < p_0 < 1$:

Якщо $a < 2 \cdot p_0 \cdot r - r$, то

$$V^{1}_{1,k(1)}(p_0, p_0) = \left\{x(0): 2\sqrt{a(2 \cdot p_0 \cdot r - r)} \leq s_1 \cdot \alpha \cdot x(0) < a + 2 \cdot p_0 \cdot r - r\right\},$$

Оптимальною стратегією ЗіНС буде пара функцій $\left[u(.,.,.), k(.,.,.)\right]$:

$$\left(\bar{k}(1)\right)_2 < k^*(x(0), F(.)) < \left(k(1)\right)_1,$$

$$\left(\bar{k}(1)\right)_{1,2} = \frac{s_1 \cdot \alpha \cdot x(0) \pm \sqrt{\left(s_1 \cdot \alpha \cdot x(0)\right)^2 - 4 \cdot a(2 \cdot p_0 \cdot r - r)}}{2 \cdot (2 \cdot p_0 \cdot r - r)}; \quad (3)$$

– $u^*(x(0), F(.)) = 1$; при

$$x(0): 2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)} \leq s_1 \cdot \alpha \cdot x(0); \quad (4)$$

– $u^*(x(0), F(.)) = 0$; ; при

$$x(0): s_1 \cdot \alpha \cdot x(0) < 2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)}. \quad (5)$$

При $a \geq 2 \cdot p_0 \cdot r - r$ буде $V^{1}_{1,k(1)}(p_0, p_0) = \varnothing$.

Безлічі перевагу першого гравця (ЗіНС) з урахуванням процедури додаткової інформації будуть записуватися наступним чином для $T = 2 \cdot k + 1 \leq 2 \cdot k_0 + 1$:

– при $k_0 \geq 1$, $s_1 \cdot \alpha \cdot s_2 < \left(\frac{\beta}{\alpha}\right)^{k_0 - 1}$, $s_1 \cdot \alpha \cdot s_2 \geq \left(\frac{\beta}{\alpha}\right)^{k_0}$;

– при $\alpha > \beta$, $s_1 \cdot \beta \cdot s_2 \geq \frac{2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)}}{a + 2 \cdot p_0 \cdot r - r}$;

$$V^{2k+1}_{1,k(1)}(p_0, p_0) = \left\{x(0): 2 \cdot \left(\frac{\beta}{\alpha}\right)^{k} \sqrt{a(2 \cdot p_0 \cdot r - r)} \leq s_1 \cdot \alpha \cdot x(0) < 2 \cdot \left(\frac{\beta}{\alpha}\right)^{k-1} \sqrt{a(2 \cdot p_0 \cdot r - r)}\right\}, \quad (6)$$
$$(k = 1, ..., k_0).$$

Оптимальною стратегією першого гравця буде пара функцій $\left[u^*(.,.,.), k^*(.,.,.)\right]$:

$$\left(\bar{k}(1)\right)_2 < k^*(x(0), F_0(.)) < \min\left(1, \left(\bar{k}(1)\right)_1\right); \quad (7)$$

$$\left(\bar{k}(1)\right)_{1,2} = \frac{s_1 \cdot \alpha \cdot x(0) \cdot \left(\frac{\alpha}{\beta}\right)^{k} \pm \sqrt{\left(s_1 \cdot \alpha \cdot x(0)\right) \cdot \left(\left(\frac{\alpha}{\beta}\right)^{k}\right)^2 - 4 \cdot a(2 \cdot p_0 \cdot r - r)}}{2(2 \cdot p_0 \cdot r - r)}.$$

Для перевірки працездатності та адекватності запропонованої моделі, були виконані імітаційні експерименти. Цілями імітаційного моделювання були: 1) визначення безлічі стратегій гравців (ЗіНСу) і атакуючої сторони; 2) оцінка адекватності математичної моделі.

Результати трьох обчислювальних експериментів представлені на рис. 1-3.

Рішення отримані для всіх випадків співвідношення, розглянутих в роботі, параметрів гри. Використавши результати гри, були знайдені оптимальні варіанти фінансових стратегій захисника об'єкта інформатизації.

Максимальне відхилення результатів обчислювального імітаційного експерименту від практичних даних становило 9-12%.

Береться тривимірний позитивний ортант в тривимірному просторі – $(t, x(0), a)$. Вісь часу t «йде знизу-уверх, від нуля». Прийнято, що параметр t буде визначати число кроків гравців.

У цій тривимірній ортанті розглядається сукупність поверхонь, що виходять з точки (0,0,0). Поверхні перпендикулярні площині $(0, x(0), a)$.

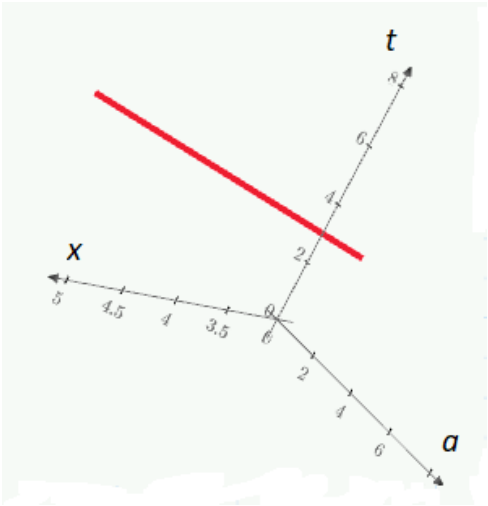

Рис. 1. Результати обчислювального експерименту №1

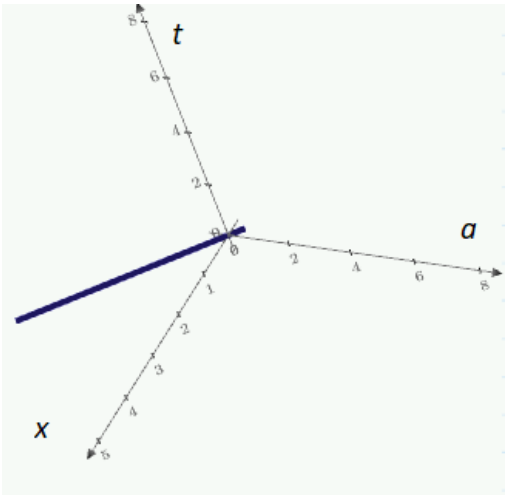

Рис. 2. Результати обчислювального експерименту № 2

Таким чином, обчислювальними експериментами була підтверджена адекватність уточненої моделі. Також підтверджена здатність моделі забезпечити результативну підтримку прийняття рішень в сфері фінансування засобів кібербезпеки різних Обі. Робота продовжила ряд публікацій авторів [8, 12, 13], в яких були викладені теоретичні та методологічні основи проектування СППР. Дана робота розвиває ці дослідження в рамках доповнення існуючих СППР [13, 15] математичними моделями, які базуються на білініній багатокрокової грі якості з декількома термінальними поверхнями [15, 18]. Уточнення в моделі усувають недоліки варіантів рішень, викладених в [8, 13, 19, 20]. Так як в [8, 13] не були враховані всі початкові умови вибору фінансових стратегій для інвестування в кіберзахист Обі.

Висновки

Запропоновано уточнену модель фінансування системи кібербезпеки для різних об'єктів інформатизації, наприклад Smart City. Запропонований варіант уточненої моделі, відрізняє допущення, що сторона захисту не має повної інформації, як про фінансові стратегії атакуючої сторони, так і про станах його фінансових ресурсів, спрямованих на подолання рубежів захисту об'єкта кібератаки. При цьому сторона захисту має можливість отримання додаткової інформації за рахунок витрати частини своїх фінансових ресурсів. Останнє дає можливість отримання стороною захисту позитивного для себе результату в разі, коли вона не може його отримати без цієї процедури.

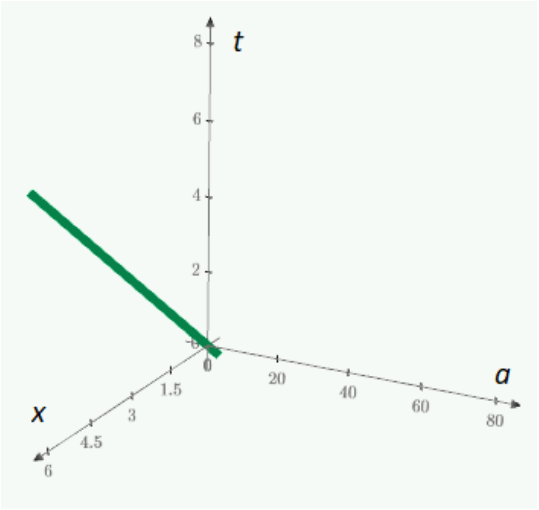

Рис. 3. Результати обчислювального експерименту № 3

Рішення базується на методі динамічного програмування. Це дозволяє, на відміну від існуючих підходів, більш ефективно знаходити рішення. Для пошуку рішення також використовувався математичний апарат нелінійної багатокрокової гри якості з декількома термінальними поверхнями з послідовними ходами.

У статті розглянуті варіанти ситуацій, в яких, інформаційне наповнення вимагає витрат ресурсів гравців з боку захисту об'єкта інформатизації.

Також наведені результати імітаційного експерименту. Розглянуто варіанти оптимального поведінки боку кіберзахисту об'єкта інформатизації. Імітаційні експерименти підтвердили адекватність моделі. Відхилення результатів імітаційного експерименту від практичних даних не перевищує 9-12%.

Література

[1]. C. Posey, T. Roberts, P. Lowry, B. Bennett, J. Courtney, *Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors*, 2013.

[2]. C. Posey, T. Roberts, P. Lowry, R. Hightower, "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders", *Information & management*, *51*(5), pp. 551-567, 2014.

[3]. R. Taylor, E. Fritsch, J. Liederbach, *Digital crime and digital terrorism*. Prentice Hall Press, 2014.

[4]. L. Gordon, M. Loeb, L. Zhou, "Investing in cybersecurity: Insights from the Gordon-Loeb model", *Journal of Information Security*, *7*(02), pp. 49, 2016.

[5]. B. Kelly, "Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cybersecurity reform", *BUL Rev.*, *92*, pp. 1663, 2012.

[6]. 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.

[7]. A. Fielder, E. Panaousis, P. Malacaria, "Decision support approaches for cyber security investment", *Decision Support Systems*, Vol. 86, pp. 13-23, 2016.

[8]. V. Lakhno, "Development of a support system for managing the cyber security", *Radio Electronics, Computer Science, Control,* No. 2, pp. 109-116, 2017.

[9]. 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.

[10]. L. Gordon, M. Loeb, W. Lucyshyn, L. Zhou, "The impact of information sharing on cybersecurity underinvestment: a real options perspective", *Journal of Accounting and Public Policy*, *34*(5), pp. 509-519, 2015.

[11]. A. Fielder, S. Konig, E. Panaousis, S. Schauer, S. Rass, S, *Uncertainty in Cyber Security Investments*, 2017. arXiv preprint arXiv:1712.05893.

[12]. B. Akhmetov, V. Lakhno, Y. Boiko, A. Mishchenko, "Designing a decision support system for the weakly formalized problems in the provision of cybersecurity", *Eastern-European Journal of Eenterprise Technologies*, (1 (2)), pp. 4-15, 2017.

[13]. V. Lakhno, V. Malyukov N. Gerasymchuk, "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. 24-1, 2017.

[14]. M. Manshaei, Q. Zhu, T. Alpcan, "Game theory meets network security and privacy", *ACM Computing Surveys*, Vol. 45, No. 3, pp. 1-39, 2013.

[15]. V. Malyukov, "Discrete-approximation method for solving a bilinear differential game", *Cybernetics and Systems Analysis*, Vol. 29, No. 6, pp. 879-888, 1993.

[16]. A. Fielder, E. Panaousis, P. Malacaria, "Game theory meets information security management", *IFIP International Information Security Conference, Marrakech, Morroco, 2–4 June 2014: proceedings, Berlin, Springer,* pp. 15-29, 2014.

[17]. X. Gao, W. Zhong, 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.

[18]. R. Isaacs, "Differential games: a mathematical theory with applications to warfare and pursuit, control and optimization", *Courier Corporation*, 1999.

[19]. B. Akhmetov, V. Lakhno, "System of decision support in weakly-formalized problems of transport cybersecurity ensuring", *Journal of Theoretical and Applied Information Technology,* Vol. 96, No. 8, pp. 2184-2196, 2018.

[20]. V. Lakhno, "Developing of the cyber security system based on clustering and formation of control deviation signs", *Journal of Theoretical & Applied Information Technology*, Vol. 95, No. 21, pp. 5778-5786, 2017.

УДК 004.056

Лахно В., Малюков В., Касаткин Д., Блозва А., Матиевский В. Модель финансирования средств киберзащиты Smart City с процедурой получе-ния дополнительных данных стороной защиты

Аннотация. *В статье изложены новые подходы к синтезу модели выбора рациональных стратегий финансирования средств кибербезопасности Smart City в ситуации, когда защита столкнулась с неполнотой данных о финансовых ресурсах атакующей стороны. Авторами предлагается модель, которая является ядром проектируемой системы поддержки принятия решений в задачах выбора рациональных вариантов инвестирования в защиту информации и кибербезопасности Smart City. Изложенная модель позволяет находить финансовые решения с помощью инструментария теории многошаговых игр с несколькими терминальными поверхностями. Изложенный подход позволяет менеджменту информационной безопасности проводить предварительную оценку потенциально возможных стратегий по финансированию эффективных систем киберзащиты Smart City. Модель отличает допущение, что сторона защиты не имеет полной информации, как о финансовые стратегии атакующей стороны, так и о состояниях его финансовых ресурсов, направленных на преодоление рубежей кибербезопасности Smart City. Учитывая последние исследования в сфере киберзащиты, можно утверждать, что тактики и стратегии стороны нападения могут быть еще разнообразными и, соответственно, усложнять для стороны защиты задачу выбора рациональной стратегии финансирования соответствующих средств кибербезопасности. При этом сторона защиты имеет возможность получения дополнительной информации за счет расходования части своих финансовых ресурсов. Это дает возможность получения стороной защиты положительного для себя результата в случае, когда она не может его получить без этой процедуры. Решение найдено с использованием математического аппарата нелинейной многошаговой игры качества с несколькими терминальными поверхностями с последовательными ходами. Для проверки адекватности модели был реализован многовариантный вычислительный эксперимент. Результаты данного эксперимента описаны в статье. Дальнейшее развитие этого направления исследований заключается в создании полноценного программного продукта, например, в виде системы поддержки принятия решений по выбору рациональной финансовой стратегии стороной защиты при инвестировании в конкретные проекты кибербезопасности Smart City.*

Ключевые слова: *кибербезопасность, Smart City, теория игр, выбор финансовой стратегии, процедура получения дополнительной информации, система поддержки принятия решений.*

Lakhno V., Malyukov V., Kasatkin D., Bloshova A., Matievsky V. The model of financing of smart city cyber security with procedure of obtaining additional data for the defense

Abstract. *The article outlines the model for choosing cyber security financing strategies for Smart City with no complete information about the financial resources of the attacking party. The proposed model is the core of the*

decision-making support system development module in the task of selecting rational investment options in the protection of information and cyber security of Smart City. The model allows to find financial solutions with the help of the tools of the theory of multistage game with several terminal surfaces. The authors propose an approach that allows information security management to pre-evaluate strategies for financing Smart City cybersecurity systems. The model distinguished by the assumption, that the defense party does not have complete information about both the financial strategies of the attacking party and the state of its financial resources aimed at overcoming the cybersecurity boundaries of the object of informatization. Considering recent cybersecurity studies, it can be argued that the tactics and strategies of the attacking party can still be diverse and, accordingly, make it difficult for the defense the task of choosing a rational strategy for financing the appropriate cyber security tools. In this case, the defense can obtain additional information at the expense of the cost of part of its financial resources. This enables a defense party to secure a positive result for themselves in case it cannot obtain it without this procedure. The solution was found using a mathematical apparatus of a nonlinear multi-stage game with several terminal surfaces with successive turns. To test the adequacy of the model, a multivariate computing experiment was conducted. The results of this experiment are described in the article. Further development of the research aim to create a complete software product, for example, a decision support system for selecting a rational financial strategy by the defense, when investing in specific Smart City cybersecurity projects.

Keywords: *cybersecurity, Smart City, game theory, financial strategy choice, obtaining additional information procedure, decision support system.*

Отримано 12 *квітня 2019 року*, затверджено редколегією *26 квітня 2019 року*