УДК 519.8

В.М. Горбачук, Г.В. Голоцуков, М.С. Дунаєвський, А.А. Сирку, С.-Б. Сулейманов

ТЕОРЕТИКО-ІГРОВІ ТА ОПТИМІЗАЦІЙНІ МОДЕЛІ І МЕТОДИ ПІДВИЩЕННЯ БЕЗПЕКИ КІБЕРІНФРАСТРУКТУР

Горбачук Василь Михайлович

Інститут кібернетики ім. В.М. Глушкова НАН України,
GorbachukVasyl@netscape.net

Голоцуков Геннадій Володимирович

Інститут кібернетики ім. В.М. Глушкова НАН України,
Golotsukov@nas.gov.ua

Дунаєвський Максим Сергійович

Інститут кібернетики ім. В.М. Глушкова НАН України,
MaxDunaievskyi@gmail.com

Сирку Андрій Анатолійович

Головний центр спеціального контролю Державного космічного агентства України,
saan@ukr.net

Сулейманов Сеїт-Бекір

Інститут кібернетики ім. В.М. Глушкова НАН України,
SBSuleimanov@gmail.com

Критична інфраструктура взаємозалежних сучасних секторів все більше покладається на кіберсистеми та кіберінфраструктури, які характеризуються зростанням ризиків їх кіберкомпонентів, у тому числі кіберфізичних підсистем. Тому кібербезпека є важливою для захисту критичної інфраструктури. Пошук економічно ефективних шляхів підвищення або підвищення безпеки кіберінфраструктури базується на оптимізаційних моделях і методах стабільності, безпеки та надійності кіберінфраструктури. Ці моделі та методи мають різні сфери застосування та різні напрямки, не обов’язково орієнтовані на стійкість кіберінфраструктури. Зростання ролі інформаційно-комунікаційних технологій вплинуло на концепцію безпеки та характер війни. Багато критичних інфраструктур (аеропорти, лікарні, нафтопроводи) стали потенційно вразливими для організованих кібератак. Сьогодні здійснення головної державної функції оборони і безпеки значною мірою залежить від успішного застосування інформаційно-комунікаційних технологій як сучасних конкурентоспроможних (кінцевих і проміжних) продуктів подвійного призначення, які використовують різні особи з різними цілями. Теорію ігор усе більше застосовують для оцінювання стратегічних взаємодій між нападниками й оборонцями у кіберпросторі. Для дослідження безпеки кіберпростору поєднуються підходи теорії ігор і моделювання. У кіберпросторі арсенал зброї будується шляхом знаходження більшої кількості уразливіших місць у захисті цілі. Вразливість — це слабкість у процедурах безпеки системи, проєкті системи чи його реалізації, а також в організації внутрішнього контролю, якими може скористатися джерело загрози. Динамічний характер вразливостей означає, що вони постійно змінюються з часом. Виявлення вразливості оборонцем знижує ефективність кіберзброї нападника, яка користується даною вразливістю, і підвищує захист цілі. Теорія ігор застосовувалася для вирішення багатьох проблем, включаючи розподіл ресурсів, безпеку мережі, кооперацію осіб. У кіберпросторі часто зустрічається гра розміщення, де нападник і оборонець приймають рішення, куди розподіляти свої відповідні ресурси. Ресурсами оборонця можуть бути інфраструктура безпеки (брандмауери), фінанси, підготовка кадрів. Наприклад, адміністратор мережі може шукати таке розміщення ресурсів, яке мінімізує ризики кібератак (нападів) і водночас витрати захисту від кібератак. Нападник має обмежені ресурси і зазнає ризику бути відстеженим і покараним. Проблему розподілу ресурсів у кіберпросторі можна сформулювати як теоретико-ігрову задачу з урахуванням поняття загального знання і проблеми невизначеної спостережуваності.

Ключові слова: рівноваги Штакельберга, змішані стратегії, бюджетні обмеження, мотиваційні обмеження, оборонець, критична інфраструктура.

Вступ

Критична інфраструктура (КрІ) взаємозалежних секторів усе більше покладається на кіберсистеми та кіберінфраструктури (КІ), які характеризуються зростанням ризиків їхніх кіберкомпонентів, зокрема кіберфізичних підсистем. Тому кібербезпека важлива для захисту КрІ. Пошук економічно ефективних шляхів підвищення чи поліпшення безпеки КІ грунтується на оптимізаційних моделях і методах безпеки КІ. Ці моделі та методи мають різні сфери застосування та різне спрямування, не обов'язково орієнтоване на резильєнтність КІ. Зростання ролі інформаційно-комунікаційних технологій (ІКТ) вплинуло на поняття безпеки і природи війни. Багато об'єктів КрІ (аеропорти, лікарні, нафтопроводи) стали потенційно вразливими до організованих кібератак.

Моделі взаємодій між нападниками і оборонцями у кіберпросторі

Сьогодні здійснення головної державної функції оборони і безпеки значною мірою залежить від успішного застосування ІКТ як сучасних конкурентоспроможних (кінцевих і проміжних) продуктів подвійного призначення, які використовують різні особи з різними цілями [1−3]. Теорію ігор усе більше застосовують для оцінювання стратегічних взаємодій між нападниками й оборонцями у кіберпросторі [1, 4−6]. Для дослідження безпеки кіберпростору поєднуються підходи теорії ігор та моделювання.

Хоча ІКТ дозволяють військовим, які приймають рішення, отримувати потрібну інформацію у потрібний час, ІКТ змінюють характер сучасної війни. Кіберпростір став новим простором бою, де зброєю є соціальна інженерія, оновлені віруси, трояни (Trojan horses), хробаки (worms), відмови в обслуговуванні (Denial-of-Service — DoS) через флуд (flooding), розподілені відмови в обслуговуванні (Distributed Denial-of-Service — DDoS) через мережі ботів (botnets) та розширені постійні загрози (Advanced Persistent Threats — APTs) [7, 8]. Кібератаки зазвичай не є безпосередньою причиною летальних наслідків, але можуть спричиняти неналежне використання обладнання, його несправність і руйнування [9, 10].

У кіберпросторі арсенал зброї будується шляхом знаходження більшої кількості вразливих місць у захисті цілі. Вразливість — це слабкість у процедурах безпеки системи, проекті системи чи його реалізації, а також в організації внутрішнього контролю, якими може скористатися джерело загрози [11]. Динамічний характер вразливостей означає, що вони постійно змінюються з часом. Виявлення вразливості оборонцем знижує ефективність кіберзброї нападника, яка користується даною вразливістю, і підвищує захист цілі [10].

Теорія ігор застосовувалася для вирішення багатьох проблем, включаючи розподіл ресурсів, безпеку мережі та кооперацію осіб. У кіберпросторі часто зустрічається гра розміщення [12], у якій нападник і оборонець приймають рішення про те, куди розподіляти свої відповідні ресурси. Ресурсами оборонця можуть бути інфраструктура безпеки (брандмауери), фінанси та підготовка кадрів. Наприклад, адміністратор мережі може шукати таке розміщення ресурсів, при якому мінімізуються ризики кібератак (нападів) і водночас витрати захисту від кібератак [13]. Нападник має обмежені ресурси і зазнає ризику бути відстеженим і покараним.

Проблему розподілу ресурсів у кіберпросторі можна сформулювати як теоретико-ігрову задачу з урахуванням поняття загального знання (common knowledge) і проблеми невизначеної спостережуваності (uncertain observability) [14].

Розробка алгоритмів розміщення ресурсів у сферах фізичної безпеки стала напрямом активних досліджень [4, 6, 15, 16]. Наприклад, ігри розміщення використовувалися, щоб рандомізувати контрольні пункти пропуску в аеропортах, виділяти обмежені ресурси безпеки та будувати резильєнтні мережі [5, 17, 18].

Алгоритми фізичної безпеки все більше адаптуються до кібербезпеки [19], але у кіберпросторі оборонці зіштовхуються зі складнішими і витонченішими атаками: цифрові атаки часто є непомітними для органів чуття людини, але досить динамічними і розподіленими та не обмежуються географічними і політичними кордонами [15].

Для аналізу відповіді на втручання (intrusion response) в системах контролю доступу пропонувалася модель некооперативної гри з ненульовою сумою розміщення ресурсів [20] між нападником (зловмисником) і розподіленою системою виявлення втручання, а також розроблявся алгоритм оптимального розподілу дефіцитного ресурсу (scarce resource) — часу системного адміністратора.

Вивчалася гра, в якій нападник намагається завдати шкоди кільком вразливим комп'ютерам шляхом надсилання шкідливих (malicious) пакетів з декількох точок входу в мережу [21]. Оборонець прагне оптимально розподілити наявні ресурси, щоб максимізувати ймовірність виявлення шкідливих пакетів при обмеженнях мережевої затримки (network latency). У згаданій грі було сформульовано задачу на графах з кількома ресурсами різнорідних спроможностей і запропоновано метод математичного програмування для знаходження оптимальних рішень.

При вивченні взаємодії між всюдисущим нападником і командою системних адміністраторів [22] використовувалася теоретико-ігрова модель оптимального розподілу таких ресурсів кібербезпеки, як час адміністратора на виконання різних завдань. Виявилося, що в цій некооперативній статичній грі існує оптимальна стратегія оборонця незалежно від стратегії нападника.

Теорія ігор також використовується для визначення оптимального розподілу загального оборонного бюджету між різними компонентами системи, який мінімізує ймовірність успіху потенційної атаки чи максимізує її очікувану вартість. У грі, в якій оборонець намагається стримувати атаки шляхом максимізації витрат нападника, можна охарактеризувати оптимальні стратегії нападу і захисту [23].

Було запропоновано динамічну гру FlipIt двох гравців у неперервному часі, у якій оборонець і нападник змагаються за контроль над певним ресурсом [24], яким може бути пароль або ціла інфраструктура в залежності від формулювання моделі. Гра FlipIt характеризується ідеєю прихованих ходів або невидимого захоплення [25] і застосовністю до широкого кола реальних проблем безпеки, включаючи стратегії перевизначення пароля (password reset) і хмарного аудиту [26]. Ця гра є корисною у світі, де будь-яка система не гарантує повної безпеки, а припущення розробників системи безпеки мають постійно перевірятися.

Уточнення рівноваг Штакельберга

Подібно до того, як це зроблено у роботах [6, 27] з фізичної безпеки, побудуємо теоретико-ігрову модель безпеки для системи КІ, яка залежить не тільки від нападника (attacker), a й від оборонця (defender) d. Оскільки в реальному світі можуть бути відсутні загальні знання про виграші нападника й оборонця (чимала кількість інформації про нападника й оборонця є конфіденційною чи таємною) і може не задовольнятися припущення визначеної спостережуваності (certain observability), пропонується поєднання підходів моделювання і теорії ігор. Позначимо як $T = \{t_1, t_2, ..., t_n\}$ множину з n цілей (targets), які мають ризик бути атакованими, і позначимо як $S = \{s_1, s_2, ..., s_m\}$ набір (set) з m ресурсів для покриття цілей (обороною). У сфері фізичної безпеки цілями можуть бути польоти і таємні офіцери безпеки польоту (In-Flight Security Officers — IFSOs; air (flight) marshals) на бортах комерційних літаків. У кіберпросторі цілями можуть бути вразливі місця у підключених до Інтернету системах та елементи інфраструктури безпеки (брандмауери, кадри та фінанси).

Змішану стратегію нападника можна представити вектором $\vec{x} = (x_1, x_2, ..., x_n)$, де x_t — ймовірність атаки цілі $t_t \in T$, а змішану стратегію оборонця — вектором $\vec{p} = \vec{p}(S) = (p_1(S), p_2(S), ..., p_n(S))$, де $p_t(S)$ — відособлена ймовірність (marginal probability) оборони цілі $t_t \in T$. Змішані стратегії дозволяють кожному гравцю вибирати розподіл ймовірностей на своїх чистих стратегіях [16, 18]. Комбінацію $(\vec{x}, \vec{p})$ стратегій нападника й оборонця назвемо профілем стратегій.

Позначимо як $r_d(t)$ винагороду (reward) для оборонця, якщо атакована ціль $t_t \in T$ покривається, і позначимо як $c_d(t) < r_d(t)$ вартість (cost) для оборонця, якщо така ціль не покривається. Аналогічно позначимо як $r_a(t)$ винагороду для нападника, якщо атакована ціль $t_t \in T$ не покривається, і позначимо як $c_a(t) < r_a(t)$ вартість для нападника, якщо така ціль покривається. Для профілю $(\vec{x}, \vec{p})$ стратегій очікувані корисності (utilities) оборонця та нападника становитимуть відповідно

$$U_d(\vec{x}, \vec{p}) = \sum_{t=1}^{n} x_t [p_t r_d(t) + (1 - p_t) c_d(t)], \quad (1)$$

$$U_a(\vec{a}, \vec{p}) = \sum_{t=1}^{n} x_t [(1 - p_t) r_a(t) + p_t c_a(t)]. \quad (2)$$

Отже, виграші (1) та (2) залежать лише від атакованих цілей та їх покриття, але не залежать від решти потенційних цілей. Коли обидва гравці вибирають свої стратегії одночасно, рішення гри визначає рівновага Неша (Неш — нобелівський лауреат 1994 р.) [16]. Коли гра складається з послідовного вибору стратегій (оборонець вибирає свою стратегію першим і дотримується її, а нападник реагує на вибір оборонця), класичне рішення гри визначає рівновага Штакельберга взаємодії лідера і послідовника [16, 19].

Ігри Штакельберга спираються на такі припущення: лідер знає як власний виграш, так і виграш послідовника; послідовник знає не лише власний виграш, але й стратегію, якої дотримується лідер. Однак у більшості реальних проблем кібербезпеки ці припущення не завжди задовольняються, бо гравці загалом не можуть точно оцінювати власні виграші та виграші своїх суперників.

Оскільки використання детермінованих значень виграшів для стратегії, якої дотримується лідер, не видається ефективним [14], то виграші (та витрати) можна рандомізувати шляхом стохастичного моделювання: замість статичних значень можна використовувати невизначені значення на заданих проміжках, скажімо, оптимістичні, реалістичні (найімовірніші) та песимістичні значення.

При даній (змішаній) стратегії $\vec{p}$ лідера послідовник максимізує за своєю стратегією $\vec{x}$ функцію очікуваної корисності (2) з обмеженнями

$$\sum_{t=1}^{n} x_t = 1, \quad (3)$$

$$x_t \ge 0, \ \ t = 1, 2, ..., n, \quad (4)$$

які визначають набір допустимих рішень послідовника як розподіл ймовірності на множині T цілей. Тоді очевидно, що оптимальним рішенням послідовника є вибір таких

$$x_k(\vec{p})=1,\quad x_t(\vec{p})=0,\quad t=1,\dots,k-1,k+1,\dots,n, \tag{5}$$

що

$$(1-p_t)\,r_a(t)+p_t c_a(t)\le(1-p_j)\,r_a(k)+p_j\,c_a(k),\quad t=1,2,\dots,n, \tag{6}$$

тобто максимізують за $t\in T$ функцію

$$(1-p_t)\,r_a(t)+p_t c_a(t)=u_a(\vec{p},\ t)\le u_a(\vec{p},\ k(\vec{p})),\quad t=1,2,\dots,n. \tag{7}$$

Тоді задачею лідера є максимізація за $\vec{p}(S)=(p_1(S),\ p_2(S),\dots,\ p_n(S))$ цільової функції (1) лідера — очікуваного виграшу оборонця

$$U_d(\vec{x}(\vec{p}(S)),\ \vec{p}(S))=\sum_{t=1}^{n}x_t(\vec{p}(S))[p_t(S)r_d(t)+(1-p_t(S))c_d(t)] \tag{8}$$

при умовах (3)−(7), а також обмеженнях

$$p_t(S)\in[0,\ 1],\quad t=1,2,\dots,n, \tag{9}$$

$$\sum_{t=1}^{n}p_t(S)\le m. \tag{10}$$

У роботі [28] представлено огляд існуючих теоретико-ігрових підходів до кібербезпеки. Проілюструємо запропонований підхід і задачу (3)−(10) на практичному прикладі гри розподілу ресурсів у нормальній формі зі сфери фізичної безпеки [17, 29].

Оскільки властивістю сильних рівноваг Штакельберга (Strong Stackelberg Equilibrium — SSE) є те, що всі вони дають однаковий виграш лідеру (оборонцю) [30, 31], то виникає питання вибору чи уточнення (refinement) серед них. У багатьох іграх безпеки Штакельберга [32−38], що моделюють реальні проблеми з обмеженнями на розподіл ресурсів безпеки, існує нескінченна кількість рішень SSE, у яких частина наявних ресурсів не використовується продуктивно, бо цю частину можна використовувати довільно, не впливаючи на якість рішення. Крім того, рішення SSE не є робастними відносно відхилень стратегії послідовника (нападника). Тому є сенс застосовувати уточнення SSE для підвищення робастності рішень SSE без погіршення їхньої якості [29].

У 1961 р. президент США наказав залучати офіцерів федеральних правоохоронних органів як офіцерів безпеки на певних авіарейсах високого ризику, що започаткувало у 1962 р. Програму офіцерів миру (Peace Officers Program) Федеральної адміністрації авіації (Federal Aviation Administration — FAA), заснованої у 1958 р. Ця програма зараз відома як Федеральна служба офіцерів безпеки польоту (Federal Air Marshal Service — FAMS) — федеральний правоохоронний орган США під підпорядкуванням Адміністрації безпеки на транспорті (Transportation Security Administration — TSA), заснованої у 2001 р. у відповідь на терористичну атаку 11 вересня 2001 р., Міністерства США внутрішньої безпеки (United States Department of Homeland Security — DHS), заснованого у 2002 р. Через характер своєї роботи IFSOs, або федеральні офіцери безпеки (Federal Air Marshals — FAMs), часто перебувають у відрядженнях і постійно тренуються у влучній стрільбі з вогнепальної зброї. Завдання FAM полягає у тому, щоб розпізнавати злочинні наміри терористів, володіти вогнепальною зброєю та за потреби застосовувати специфічну для літаків тактику заходів самооборони на близькій дистанції для захисту пасажирів на борту літака, не виділяючись при цьому серед інших пасажирів.

У сфері FAMS можуть виникати множинні рівноваги ігор безпеки [17], як показано нижче у таблиці. Нехай $n=4$, причому цілі $t=1,2$ стосуються одного аеропорту, а цілі $t = 3, 4$ — іншого. Кожний аеропорт має лише одного FAM, а тому FAM 1 може працювати тільки на рейсах $t = 1, 2,$ а FAM 2 — тільки на рейсах $t = 3, 4,$ звідки

$$p_1 + p_2 = 1, \quad p_3 + p_4 = 1. \tag{11}$$

Таблиця

t	$r_d(t)$	$c_d(t)$	$r_a(t)$	$c_a(t)$
1	4	3	9	6
2	3	2	7	6
3	6	4	10	8
4	3	2	12	6

Тоді функція виграшу лідера

$$U_d(\vec{x}(\vec{p}), \vec{p}) = x_1[p_1 r_d(1) + (1-p_1)c_d(1)] + x_2[p_2 r_d(2) + (1-p_2)c_d(2)] +$$
$$+ x_3[p_3 r_d(3) + (1-p_3)c_d(3)] + x_4[p_4 r_d(4) + (1-p_4)c_d(4)] =$$
$$= x_1[p_1 r_d(1) + (1-p_1)c_d(1)] + x_2[(1-p_1)r_d(2) + p_1 c_d(2)] +$$
$$+ x_3[p_3 r_d(3) + (1-p_3)c_d(3)] + x_4[(1-p_3)r_d(4) + p_3 c_d(4)] =$$
$$= x_1[4p_1 + 3(1-p_1)] + x_2[3(1-p_1) + 2p_1] +$$
$$+ x_3[6p_3 + 4(1-p_3)] + x_4[3(1-p_3) + 2p_3] =$$
$$= x_1(p_1 + 3) + x_2(3 - p_1) + x_3(2p_3 + 4) + x_4(3 - p_3) =$$
$$= p_1(x_1 - x_2) + 3(x_2 + x_1) + p_3(2x_3 - x_4) + 3x_4 + 4x_3$$

стає сепарабельною за p_1 та p_3.

Якщо $x_1 - x_2 > 0$ (тобто $x_1 = 1,\ x_2 = x_3 = x_4 = 0$), то $p_1 = 1,\ p_2 = 0;$ інакше $p_1 = 1 - p_2$, а p_2 може приймати будь-яке значення на відрізку [0, 1].

Якщо $2x_3 - x_4 > 0$ (тобто $x_3 = 1,\ x_1 = x_2 = x_4 = 0$), то $p_3 = 1,\ p_4 = 0;$ інакше $p_3 = 1 - p_4$, а p_4 може приймати будь-яке значення на відрізку [0, 1].

При $x_1 = 1$ цільова функція лідера дорівнюватиме

$$p_1(x_1 - x_2) + 3(x_2 + x_1) = 1 \times (1 - 0) + 3 \times (0 + 1) = 4,$$

а при $x_3 = 1$ цільова функція лідера дорівнюватиме більшому значенню:

$$p_3(2x_3 - x_4) + 3x_4 + 4x_3 = 1 \times (2 \times 1 - 0) + 3 \times 0 + 4 \times 1 = 6.$$

Отже, лідеру вигідно, щоб послідовник обрав $x_3 = 1,\ x_1 = x_2 = x_4 = 0$ замість $x_1 = 1,\ x_2 = x_3 = x_4 = 0.$ Маючи інформацію про обмеження (11) лідера, послідовник максимізуватиме свою функцію виграшу:

$$U_a(\vec{x}(\vec{p}), \vec{p}) = x_1[(1-p_1)r_a(1) + p_1 c_a(1)] + x_2[(1-p_2)r_a(2) + p_2 c_a(2)] +$$
$$+ x_3[(1-p_3)r_a(3) + p_3 c_a(3)] + x_4[(1-p_4)r_a(4) + p_4 c_a(4)] =$$
$$= x_1[9(1-p_1) + 6p_1] + x_2[7p_1 + 6(1-p_1)] +$$
$$+ x_3[10(1-p_3) + 8p_3] + x_4[12p_3 + 6(1-p_3)] =$$
$$= x_1(9 - 6p_1) + x_2(6 - p_1) + x_3(10 - 2p_3) + x_4(6 + 6p_3) =$$

$$=\begin{cases} 3(3-p_1)\in[6,9], & x_1=1,\ \ x_2=x_3=x_4=0; \\ 7-p_1\in[6,7], & x_2=1,\ \ x_1=x_3=x_4=0; \\ 2(5-p_3)\in[8,10], & x_3=1,\ \ x_1=x_2=x_4=0; \\ 6(1+p_3)\in[6,12], & x_4=1,\ \ x_1=x_2=x_3=0. \end{cases}$$

Послідовник обиратиме $x_3=1$, якщо

$$0 < 2(5-p_3)-3(3-p_1)=10-5p_3-9+3p_1=1+3p_1-5p_3,$$

$$p_3 < 0{,}2(1+3p_1)\in[0{,}2, 0{,}8]$$

при обмеженнях (9) і (11), що узагальнює отримане в роботі [29] рішення

$$\vec{p}= (p_1,\ 1-p_1,\ 0{,}5,\ 0{,}5).$$

Крім того, для $x_3=1$ потрібно виконати нерівності

$$0\le 2(5-p_3)-(7-p_1)=10-2p_3-7+p_1=3-2p_3+p_1, \tag{12}$$

$$0\le 2(5-p_3)-6(1+p_3)=10-2p_3-6-6p_3=4-8p_3,\ \ p_3\le 0{,}5. \tag{13}$$

Очевидно, що нерівність (12) виконується в силу обмежень (9). Нерівність (13) уточнює рішення лідера (оборонця) до

$$\vec{0}\le\vec{p}=(p_1,\ 1-p_1,\ p_3 < \min\{0{,}5; 0{,}2(1+3p_1)\},\ 1-p_3).$$

Зазначимо, що при інтерпретації $-c_d(t)$, $-c_a(t)$ як витрат [14] виникатиме питання мотиваційних обмежень (incentive constraints).

Оптимізація критичних інфраструктур

Для ідентифікації (наближених) оптимальних рішень застосовується арсенал оптимізаційних моделей і методів [39]. Такими моделями є: лінійне, нелінійне, змішане цілочисельне, стохастичне, напіввизначене, багатокритеріальне програмування; дворівневе, трирівневе і багаторівневе прийняття рішень; теорія ігор; марківські процеси прийняття рішень. Серед таких методів виділяють точні (метод динамічного програмування, метод гілок і границь, алгоритм Дійкстри (Dijkstra), метод генерації стовпців для великих моделей лінійного програмування) та неточні (алгоритми апроксимації, евристичні алгоритми, метаевристичні алгоритми (генетичний алгоритм, метод рою частинок (particle swarm) тощо).

У багатьох дослідженнях реальних проблем з великими даними точні методи не розробляються, створюючи певну прогалину в науковій методології алгоритмів. Іноді використовуються не оптимізаційні моделі, а оптимізаційні методи, наприклад генетичні алгоритми для розв’язання задачі планування системи розподілу електроенергії [40].

Теорія ігор користується математичними моделями для охоплення стратегічних взаємодій між принаймні двома раціональними особами, які приймають рішення. Такими рішеннями часто є рівноваги Неша, одностороннє (некооперативне) відхилення від яких знижує виграш ініціатора відхилення (скажімо, зловмисника). Наприклад, при моделюванні взаємозв’язків між захистом і відновленням інфраструктури можна запропонувати досконалі рівноваги Неша підігор для стратегій захисника і нападника [41]. Ціллю захисника може бути мінімізація збитків, спричинених нападником [42], або інша [43–45].

Поширеною оптимізаційною моделлю є змішане цілочисельне програмування (Mixed Integer Programming — MIP) з лінійними обмеженнями, де частина змінних є цілими числами. Наприклад, розміщуючи довірчі вузли (trust nodes) на інтелектуальній решітці чи гратці (grid network) для мінімізації витрат маршрутизації зв'язку, захисник може розв'язувати задачу MIP для упаковки множини (set packing) [46]. Для побудови евристичного підходу до розв'язання цієї задачі можна застосовувати алгоритм Дійкстри пошуку маршруту мінімальної вартості між двома вузлами. Задачу віртуального розміщення для глибокої перевірки мережевих пакетів (deep packet inspection) можна формулювати як задачу MIP пошуку багатотоварного потоку мінімальної вартості [47], для розв'язання якої також можна застосовувати алгоритм Дійкстри як частину жадібного алгоритму розміщення (greedy placement algorithm) з порівнянням знайдених рішень на різних мережах. Для кібербезпеки промислової системи управління пропонується комбінаторна модель MIP [48], для якої встановлюються рівні заходів безпеки, мінімізується загальний ризик внаслідок кібератак при бюджетному рюкзачному (knapsack) обмеженні та пропонується поліноміальний алгоритм апроксимації з гарантованими межами наближення.

Широко розповсюдженими є моделі лінійного та нелінійного програмування (Nonlinear Programming — NLP), які, на відміну від моделі MIP, використовують лише неперервні змінні. Модель NLP застосовується для мінімізації нелінійної функції витрат на безпечне охолодження суперкомп'ютера при нелінійних бюджетних обмеженнях [49]. Модель NLP також застосовується для мінімізації суми залишкових ризиків (residual risks) після впровадження заходів безпеки (security controls) КрІ у страховій галузі [50].

Моделі змішаного цілочисельного нелінійного програмування (Mixed Integer Nonlinear Programming — MINLP) поєднують властивості MIP та NLP, використовуючи цілочисельні та неперервні змінні разом з принаймні одним нелінійним обмеженням чи нелінійною цільовою функцією [51, 52]. Для моделювання водної мережі пропонується задача мінімізації зважених витрат дефіциту води і перевезення води вантажівками [51], яка лінеаризується і розв'язується як MIP.

Коли математична оптимізаційна задача має принаймні дві цільові функції, зазвичай не існує єдиного допустимого розв'язку, який одночасно максимізує всі цільові функції. Тоді використовується поняття Парето-оптимальних рішень з багатокритеріальної оптимізації (Multi-Objective Optimization — MOO) чи багатокритеріального програмування: рішення є Парето-оптимальним, якщо покращення значення одного з критеріїв веде до погіршення значення іншого критерію. Моделі MOO пропонуються для мінімізації впливу кібератак на системи контролю руху автострад (freeway traffic control) [53] і моделювання реакції на кібервтручання (cyber intrusions) у промислові системи управління [54], де підцілями є функціональність системи, якість стану системи та рівень безпеки системи. Для пошуку наближених розв'язків цих моделей пропонується генетичний алгоритм.

Оптимізаційну задачу можна моделювати за допомогою принаймні двох вбудованих підзадач, кожній з яких відповідає певна особа, що приймає рішення. Зазвичай кожна така особа прагне оптимізувати власну цільову функцію, враховуючи рішення інших осіб. Дворівневій (bi-level) задачі оптимізації відповідає випадок двох вбудованих підзадач, трирівневій — випадок трьох вбудованих підзадач. Дворівнева оптимізація використовується для моделювання структури гри захисника і нападника [55−59]. Наприклад, дворівнева оптимізація використовується для моделювання задачі оптимізації перехоплень (interdiction optimization problem) в електромережах, вразливих до кібератак [56]. У підзадачі нижнього рівня нападник намагається атакувати енергомережу, позаяк у підзадачі верхнього рівня захисник максимізує число відбитих атак (disrupted attacks) при своїх обмежених ресурсах. Для розв'язання такої задачі пропонується евристична декомпозиція. Дворівнева оптимізація також використовується для проекту перехоплення, у якому особи, які приймають рішення, розгортають заходи, спрямовані на максимальні затримки множинних ворожих атак, коли тривалості затримки є невизначеними [59].

Оскільки в реальних задачах не завжди всі параметри відомі напевне, пропонуються моделі стохастичної оптимізації [60], зокрема модель вибору портфеля засобів контролю безпеки з урахуванням середнього та найменшого значень міри ефективності [61, 62].

Для моделювання задачі безпеки пропонується трирівнева оптимізація [63], при якій на другому рівні рішення приймає нападник, а на першому і третьому рівнях — захисник, причому на третьому рівні — з урахуванням дій нападника. У рішенні першого рівня захисник виділяє профілактичні ресурси на захист ліній електропередачі в енергомережі; у рішенні другого рівня зловмисник намагається максимізувати навантаження енергосистеми шляхом від'єднання ліній електропередачі; у рішенні третього рівня захисник реагує на збої (disruptions), спричинені зловмисником, шляхом мінімізації навантаження (load shed) з використанням лінійного програмування.

Марковський процес прийняття рішень (Markov Decision Process — MDP) є засобом оптимізації, корисним для моделювання системи, що змінюється стохастично відповідно до рішень, які приймаються послідовно і мають стохастичні наслідки [64]. MDP використовується для моделювання в інтелектуальній мережі взаємодій між провайдерами і нападниками, які максимізують спад ринкової ціни [65]. MDP також використовується для моделювання ітеративної гри між оборонцем, який намагається захищати інфраструктуру фірми, та нападником, який намагається скомпрометувати цю інфраструктуру [66].

Напіввизначене програмування (Semidefinite Program — SDP) використовується для поліпшення зв'язку в інтелектуальній мережі шляхом збільшення її надлишковості (adding redundancy) та стабілізування стану системи [67]. У задачі SDP мінімізується лінійна цільова функція [68] при обмеженні з афінною комбінацією симетричних позитивно напіввизначених матриць. Оскільки це обмеження є опуклим, але не є лінійним, то SDP узагальнює LP . Крім того, задачі SDP можна розв'язувати за поліноміальний час, як і задачі LP [69].

При оптимізації (змішаному цілочисельному програмуванні, дворівневому програмуванні, багатокритеріальній оптимізації, евристичній оптимізації тощо) використовується моделювання для генерування сценаріїв [70−72], верифікації параметрів задачі чи валідації результатів [42, 44, 54, 67, 73−78]. Моделювання частіше використовується у теорії ігор [42, 44, 70, 74, 75, 79, 80].

Для вивчення вразливостей мережі часто використовується методологія графа чи дерева атак [81−84], яку можна застосувати до вивчення безпеки КІ [85]. Наприклад, для вибору заходів посилення безпеки, які мінімізують залишкові збитки при бюджетних обмеженнях, застосовується задача MOO на дереві атак [81], яку можна конкретизувати для підвищення безпеки КІ [86, 87]. Для визначення оптимального рішення перехоплення на графі атаки пропонується дворівнева модель MIP [82], де мінімізуються втрати, спричинені проривами системи безпеки, не обов'язково системи безпеки КІ. Для зниження ймовірності успішних атак противника аналізується стохастична атака на загальні складні мережі [83]. Для забезпечення підтримки рішень мережевих адміністраторів розробляється метод мінімізації зв'язності графа атаки [84] — жадібний алгоритм пошуку наближеного оптимального розв'язку.

Висновок

Нормальне функціонування суспільства й економіки залежить від ефективної роботи різноманітних секторів КрІ — від державних установ та енергетики до охорони здоров'я і зв'язку. КрІ значною мірою залежить від таких КІ, як мережі ІКТ. КІ складається з таких кіберфізичних підсистем, як апаратне і програмне забезпечення, що дозволяє зберігати, обробляти і передавати інформацію, необхідну для роботи всіх секторів КрІ. КрІ є вразливою до природних катаклізмів, фізичних інцидентів та антропогенних організованих дій. Сучасною основою безпеки КрІ є КІ, яка може моделюватися та оптимізуватися.

V. Gorbachuk, G. Golotsukov, M. Dunaievskyi, A. Syrku, S.-B. Suleimanov

GAME THEORY AND OPTIMIZATION MODELS AND METHODS TO INCREASE SECURITY OF CYBERINFRASTRUCTURES

Vasyl Gorbachuk

V.M. Glushkov Institute of Cybernetics of NAS of Ukraine,
GorbachukVasyl@netscape.net

Gennadii Golotsukov

V.M. Glushkov Institute of Cybernetics of NAS of Ukraine,
Golotsukov@nas.gov.ua

Maksym Dunaievskyi

V.M. Glushkov Institute of Cybernetics of NAS of Ukraine,
MaxDunaievskyi@gmail.com

Andrii Syrku

Main Center of Special Monitoring of the Ukrainian National Spase Facilities Control and Test Center of the State Space Agency of Ukraine,
saan@ukr.net

Seit-Bekir Suleimanov

V.M. Glushkov Institute of Cybernetics of NAS of Ukraine,
SBSuleimanov@gmail.com

Critical infrastructure of interdependent modern sectors is increasingly relying on cyber systems and cyber infrastructures, which are characterized by growing risks of their cyber components, including cyberphysical subsystems. Therefore, cybersecurity is important for the protection of critical infrastructure. The search for cost-effective ways to increase or improve the security of cyber infrastructure is based on optimization models and methods of cyber infrastructure stability, safety, and reliability. These models and methods have different fields of application and different directions, not necessarily focused on the cyber infrastructure resilience. The growing role of information and communication technologies has influenced the concept of security and the nature of war. Many critical infrastructures (airports, hospitals, oil pipelines) have become potentially vulnerable to organized cyber attacks. Today, the implementation of the major state function of defense and security largely depends on the successful use of information and communication technologies as modern competitive (final and intermediate) dual-use products used by different people for different purposes. Game theory is increasingly used to assess strategic interactions between attackers and defenders in cyberspace. Game research and modeling combinations are combined to study the security of cyberspace. In cyberspace, the arsenal of weapons is built by finding more vulnerabilities in the defense of the target. Vulnerability is a weakness in the security procedures of the system, the design of the system or its implementation, as well as in the organization of internal control, which may be used by the source of the threat. The dynamic nature of vulnerabilities means that they are constantly changing over time. Detecting a vulnerability by a defender reduces the effectiveness of the attacker's cyber weapon, which exploits the vulnerability, and increases the target protection. Game theory has been applied to many issues, including resource allocation, network security, and human cooperation. In cyberspace, there is often a placement game where the attacker and the defender decide where to allocate their respective resources. Defender's resources can be security infrastructure (firewalls), finance, training. For example, a network administrator might look for a resource allocation that minimizes the risk of (cyber) attacks and at the same time protects against cyberattacks. The attacker has limited resources and is at risk of being tracked down and punished. The problem of resource allocation in cyberspace can be formulated as a game-theoretic problem, taking into account the concept of common knowledge and the problem of uncertain observability.

Keywords: Stackelberg equilibria, mixed strategies, budget constraints, incentive constraints, defender, critical infrastructure.

REFERENCES

1. Chikrii A. Conflict-controlled processes. Dordrecht, Netherlands : Springer Science & Business Media, 1997. 404 p. https://doi.org/10.1007/978-94-017-1135-7.
2. Савчук М.М. Захист інформаційних технологій та кібербезпека. *Вісник НАН України.* 2019. № 11. С. 23–28. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/162506/06-Savchuk.pdf?sequence=1.

3. Lande D.V., Novikov O.M., Stopochkina I.V. Reference functions of cyber incidents displaying in the media space. *Theoretical and Applied Cybersecurity*. 2021. **3**, N 1. P. 64–74. https://doi.org/10.20535/tacs.2664-29132021.1.251315.
4. Roy S., Ellis C., Shiva S., Dasgupta D., Shandilya V., Wu Q. A survey of game theory as applied to network security. *43-rd Hawaii International Conference on System Sciences (January 5−10, 2010, Honolulu, HI).* IEEE, 2010. URL: doi: 10.1109/HICSS.2010.35. https://doi.org/10.1109/HICSS.2010.35.
5. Kiekintveld C., Lisý V., Píbil R. Game-theoretic foundations for the strategic use of honeypots in network security. *Cyber Warfare. Advances in Information Security.* S. Jajodia, P. Shakarian, V. Subrahmanian, V. Swarup, C. Wang (eds.). Cham, Switzerland : Springer, 2015. **56**. P. 81–101. https://doi.org/10.1007/978-3-319-14039-1_5.
6. Tambe M. Security and game theory: algorithms, deployed systems, lessons learned. Cambridge University Press, 2011. 336 p. https://doi.org/10.1017/CBO9780511973031.
7. Bernier M., LeBlanc S., Morton B. Metrics framework of cyber operations on command and control. *Proceedings of the 11th European Conference on Information Warfare and Security (July 5–6, 2012, Laval, France).* E. Filiol, R. Erra (eds.) Laval, France : The Institute Ecole Superieure en Informatique Electronique et Automatique, 2012. P. 53–62. ISBN 978-1-908272-56-0.
8. Aslanoglu R., Tekir S. Recent cyberwar spectrum and its analysis. *Ibid*. 2012. P. 45–52. http://hdl.handle.net/11147/5130.
9. Ziolkowski K. Computer network operations and the law of armed conflict. *Military Law and Law of War Review*. 2010. **49** (2). P. 47–94. http://www.ismllw.org/REVIEW/2010%20ART%20Ziolkowski.php.
10. Czosseck C., Podins K. A vulnerability-based model of cyber weapons and its implications for cyber conflict. *International Journal of Cyber Warfare and Terrorism*. 2012. **2** (1). P. 14–26. http://doi.org/10.4018/ijcwt.2012010102.
11. Stoneburner G., Goguen A., Feringa A. Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology. NIST Special Publication: 800-30. Gaithersburg, MD: Computer Security Division; Information Technology Laboratory; NIST, 2002. 55 p. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf.
12. Bier V.M., Cox L.A., Azaiez M.N. Why both game theory and reliability theory are important in defending infrastructure against intelligent attacks. Game Theoretic Risk Analysis of Security Threats. *The International Series of Operations Research and Management Science.* V.M. Bier, M.N. Azaiez (eds.). New York, NY : Springer, 2009. **28**. P. 1–11. https://doi.org/10.1007/978-0-387-87767-9_1.
13. Acquaviva J.R., Mahon M., Einfalt B., LaPorta T. Optimal cyber-defense strategies for advanced persistent threats: a game theoretical analysis. *36-th Symposium on Reliable Distributed Systems (September 25–29, 2017, Hong Kong, China).* IEEE, 2017. URL: doi:10.1109/SRDS.2017.29. https://doi.org/10.1109/SRDS.2017.29.
14. Sokri A. Optimal resource allocation in cyber-security: a game theoretic approach. *Procedia Computer Science*. 2018. **134**. P. 283–288. https://doi.org/10.1016/j.procs.2018.07.172.
15. Moisan F., Gonzalez C. Security under uncertainty: adaptive attackers are more challenging to human defenders than random attackers. *Frontiers in Psychology*. 2017. **8**:982. URL: doi: 10.3389/fpsyg.2017.00982. https://doi.org/10.3389/fpsyg.2017.00982.
16. Coniglio S. Algorithms for finding leader-follower equilibrium with multiple followers. PhD Thesis. Milan : Politecnico di Milano, 2014. 116 p. https://www.politesi.polimi.it/bitstream/10589/92066/1/Algorithms%20for%20Finding%20Leader-Follower%20Equilibrium%20with%20Multiple%20Followers.pdf.
17. Jain M., Tsai J., Pita J., Kiekintveld C., Rathi S., Tambe M., Ordonez F. Software assistants for randomized patrol planning for the LAX airport police and the Federal Air Marshals Service. *Interfaces*. 2010. **40** (4). P. 267–290. https://doi.org/10.1287/inte.1100.0505.
18. Kiekintveld C., Jain M., Tsai J., Pita J., Ordonez F., Tambe M. Computing optimal randomized resource allocations for massive security games. *8-th International Joint Conference on Autonomous Agents and Multi-Agent Systems (May 10–15, 2009, Budapest, Hungary).* Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems, 2009. P. 689–696. https://dl.acm.org/doi/pdf/10.5555/1558013.1558108.
19. Sinha A., Nguyen T.H., Kar D., Brown M., Tambe M., Jiang A.X. From physical security to cybersecurity. *Journal of Cybersecurity.* 2015. **1** (1). P. 19–35. https://doi.org/10.1093/cybsec/tyv007.
20. Bloem M., Alpcan T., Basar T. Intrusion response as a resource allocation problem. *45-th Conference on Decision and Control. (December 13–15, 2006, San Diego, CA)*. IEEE, 2007. URL: doi: 10.1109/CDC.2006.376981. https://doi.org/10.1109/CDC.2006.376981.
21. Vanek O., Yin Z., Jain M., Boransky B., Tambe M., Pechoucek M. Game-theoretic resource allocation for malicious packet detection in computer networks. *11-th International Joint Conference on Autonomous Agents and Multi-Agent Systems* (June, 4–8, 2012, Valencia, Spain. W. van der Hoek, L. Padgham, V. Conitzer, M. Winikoff (eds.). Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems, 2012.) **2**. P. 905–912. https://www.ifaamas.org/Proceedings/aamas2012/papers/4E_3.pdf.
22. Fielder A., Panaousis E., Malacaria P., Hankin C., Smeraldi F. Game theory meets information security management. ICT Systems Security and Privacy Protection (June 2–4, 2014, Marrakech, Morocco). SEC 2014. *IFIP Advances in Information and Communication Technology.* N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, T. Sans (eds.). Berlin, Heidelberg : Springer, 2014. **428**. P. 15–29. https://doi.org/10.1007/978-3-642-55415-5_2.

23. Azaiez N., Bier V.M. Optimal resource allocation for security in reliability systems. *European Journal of Operational Research*. 2007. **181** (2). P. 773–786. https://doi.org/10.1016/j.ejor.2006.03.057.
24. Van Dijk M., Juels A., Oprea A., Rivest R.L. FLIPIT: the game of stealthy takeover. *Journal of Cryptology*. 2013. **26** (4). P. 655–713. https://doi.org/10.1007/s00145-012-9134-5.
25. Rasouli M., Miehling E., Teneketzis D. A supervisory control approach to dynamic cyber-security. Decision and Game Theory for Security. *5-th International Conference GameSec (November 6–7, 2014, Los Angeles, CA). Lecture Notes in Computer Science*. R. Poovendran, W. Saad (eds.). Cham, Switzerland : Springer, 2014. **8840**. P. 99–117. https://doi.org/10.1007/978-3-319-12601-2_6.
26. Bowers K.D., van Dijk M., Griffin R., Juels A., Oprea A., Rivest R.L., Triandopoulos N. Defending against the unknown enemy: applying FLIPIT to system security. Decision and Game Theory for Security. *3-rd International Conference GameSec (November 5–6, Budapest, Hungary). Lecture Notes in Computer Science.* J. Grossklags, J. Walrand (eds.). Heidelberg : Springer, 2012. **7638**. P. 248–263. https://doi.org/10.1007/978-3-642-34266-0_15.
27. Paruchuri P., Pearce J., Marecki J., Tambe M., Ordonez F., Kraus S. Playing games for security: an efficient exact algorithm for solving Bayesian Stackelberg games. *7-th International Joint Conference on Autonomous Agents and Multi-Agent Systems (May 12–16, 2008, Estoril, Portugal).* L. Padgham, D.C. Parkes, J.P. Müller, S. Parsons (eds.). Richland, SC : International Foundation for Autonomous Agents and Multiagent Systems, 2008. **2**. P. 895–902. https://ifaamas.org/Proceedings/aamas08/proceedings/pdf/paper/AAMAS08_0057.pdf.
28. Do C.T., Tran N.H., Hong C., Kamhoua C.A., Kwiat K.A., Blasch E., Ren S., Pissinou N., Iyengar S.S. Game theory for cyber security and privacy. *ACM Computing Surveys.* 2017. **50** (2). P. 1–37. https://doi.org/10.1145/3057268.
29. An B., Tambe M., Ordonez F., Shieh E., Kiekintveld C. Refinement of strong Stackelberg equilibria in security games. *Proceedings of the 25-th Conference on Artificial Intelligence (August 7–11, 2011, San Francisco, CA).* W. Burgard, D. Roth (eds.). Association for the Advancement of Artificial Intelligence Press, 2011. P. 587–593. https://ojs.aaai.org/index.php/AAAI/article/view/7864.
30. Leitmann G. On generalized Stackelberg strategies. *Optimization Theory and Applications.* 1978. **26** (4). P. 637–643. https://doi.org/10.1007/BF00933155.
31. Breton M., Alg A., Haurie A. Sequential Stackelberg equilibria in two-person games. *Optimization Theory and Applications.* 1988. **59** (1). P. 71–97. https://doi.org/10.1007/BF00939867.
32. Горбачук В.М. Синтетическое равновесие Курно–Штакельберга–Нэша. *Теорія оптимальних рішень.* 2003. № 2. С. 68–74. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/84857/10-Gorbachuk.pdf?sequence=1.
33. Горбачук В.М., Ненахова С.Г. Пошук прийнятних рівнів інфляції і бюджетного дефіциту через рівноваги Штакельберга. Системний аналіз та інформаційні технології. Київ : ІПСА НТУУ «КПІ», 2005. С. 112. https://www.researchgate.net/publication/361291997_Finding_acceptable_levels_of_inflation_and_budget_deficits_through_Stackelberg_equilibria.
34. Gorbachuk V.M. Generalized Cournot–Stackelberg–Nash equilibrium. *Cybernetics and Systems Analysis.* 2006. **42**, N 1. P. 25–33. https://doi.org/10.1007/s10559-006-0033-3.
35. Горбачук В.М. Равновесия Курно–Нэша и Курно–Штакельберга–Нэша для дробных целевых функций. *Теорія оптимальних рішень*. 2007. № 6. С. 117–124. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/85002/14-Gorbachuk.pdf?sequence=1.
36. Горбачук В.М., Гаркуша Н.І. Рівновага Курно–Неша за умов асиметричної невизначеності як узагальнена рівновага Курно–Штакельберга–Неша. PDMU-2007 (21–23 травня 2007 р., Чернівці, Україна). Київ : КНУ ім. Т. Шевченка, 2007. С. 94. https://www.researchgate.net/publication/361292640_Cournot_-_Nash_equilibrium_under_conditions_of_asymmetric_uncertainty_as_a_generalized_Cournot_-_Stackelberg_-_Nash_equilibrium.
37. Gorbachuk V.M. An asymmetric Cournot–Nash equilibrium under uncertainty as a generalized Cournot–Stackelberg–Nash equilibrium. *Cybernetics and Systems Analysis*. 2007. **43**, N 4. P. 471–477. https://doi.org/10.1007/s10559-007-0073-3.
38. Горбачук В.М., Гаркуша Н.І. Рівноваги Курно–Неша за асиметричної невизначеності та узагальнені рівноваги Курно–Штакельберга–Неша. *Вісник Київського університету. Серія: фізико-математичні науки.* 2007. № 1. С. 143–148. https://bphm.knu.ua/index.php/bphm/issue/view/11/2007_1.
39. Enayaty-Ahangar F., Albert L.A., DuBois E. A survey of optimization models and methods for cyberinfrastructure security. *IISE Transactions*. 2020. URL: doi:10.1080/24725854.2020.1781306.
40. Kapourchali M.H., Sepehry M., Aravinthan V. Fault detector and switch placement in cyber-enabled power distribution network. *IEEE Transactions on Smart Grid*. 2016. **9** (2). P. 980–992. https://doi.org/10.1109/TSG.2016.2573261.
41. Chen J., Touati C., Zhu Q. A dynamic game approach to strategic design of secure and resilient infrastructure network. *IEEE Transactions on Information Forensics and Security*. 2020. **15**. P. 462–474. https://doi.org/10.1109/TIFS.2019.2924130.
42. Panfili M., Giuseppi A., Fiaschetti A., Al-Jibreen H.B., Pietrabissa A., Delli Priscoli F. A game theoretical approach to cyber-security of critical infrastructures based on multi-agent reinforcement learning. *26-th Mediterranean Conference on Control and Automation (June 19–22, 2018, Zadar, Croatia)*. IEEE, 2018. P. 460–465. https://doi.org/10.1109/MED.2018.8442695.

43. Rao N.S., Poole S.W., Ma C.Y., He F., Zhuang J., Yau D.K. Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models. *Risk Analysis*. 2016. **36** (4). P. 694–710. https://doi.org/10.1111/risa.12362.
44. Bedi H.S., Roy S., Shiva S. Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows. *IEEE Symposium on Computational Intelligence in Cyber Security (April 11–15, 2011, Paris, France)*. IEEE, 2011. P. 129–136. https://doi.org/10.1109/CICYBS.2011.5949407.
45. Miao F., Zhu Q., Pajic M., Pappas G.J. A hybrid stochastic game for secure control of cyber-physical systems. *Automatica*. 2018. **93**. P. 55–63. https://doi.org/10.1016/j.automatica.2018.03.012.
46. Zhang Y., Sun W., Wang L. Location and communication routing optimization of trust nodes in smart grid network infrastructure. *Power and Energy Society General Meeting (July 22–26, 2012, San Diego, CA)*. IEEE, 2012. P. 1–8. https://doi.org/10.1109/PESGM.2012.6345688.
47. Bouet M., Leguay J., Combe T., Conan V. Cost-based placement of vDPI functions in NFV infrastructures. *International Journal of Network Management*. 2015. **25** (6). P. 490–506. https://doi.org/10.1002/nem.1920.
48. Milošević J., Tanaka T., Sandberg H., Johansson K.H. Exploiting submodularity in security measure allocation for industrial control systems. *Proceedings of the 1-st ACM Workshop on the Internet of Safe Things (November 7, 2017, Delft, Netherlands)*. M.R. Eskicioğlu (ed.). ACM, 2017. P. 64–69. https://doi.org/10.1145/3137003.3137011.
49. Patterson I., Nutaro J., Allgood G., Kuruganti T., Fugate D. Optimizing investments in cyber-security for critical infrastructure. *Proceedings of the 8-th Annual Cyber Security and Information Intelligence Research Workshop (January 8–10, 2013, Oak Ridge, TN)*. F. Sheldon, A. Giani, A. Krings, R.K. Abercrombie (eds.). Article 20. ACM, 2013. P. 1–4. https://doi.org/10.1145/2459976.2459999.
50. Young D., Lopez Jr.J., Rice M., Ramsey B., McTasney R. A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*. 2016. **14**. P. 43–57. https://doi.org/10.1016/j.ijcip.2016.04.001.
51. Turner J.P., Qiao J., Lawley M., Richard J.-P., Abraham D.M. Mitigating shortage and distribution costs in damaged water networks. *Socio-Economic Planning Sciences*. 2012. **46** (4). P. 315–326. https://doi.org/10.1016/j.seps.2012.02.001.
52. Wang C., Hou Y. Reliability-based updating strategies of cyber infrastructures. *Power and Energy Society General Meeting (July 26–30, 2015, Denver, CO)*. IEEE, 2015. P. 1–5. https://doi.org/10.1109/PESGM.2015.7286403.
53. Reilly J., Martin S., Payer M., Bayen A.M. Creating complex congestion patterns via multi-objective optimal freeway traffic control with application to cyber-security. *Transportation Research Part B: Methodological*. 2016. **91**. P. 366–382. https://doi.org/10.1016/j.trb.2016.05.017.
54. Li X., Zhou C., Tian Y.-C., Qin Y. A dynamic decision making approach for intrusion response in industrial control systems. *IEEE Transactions on Industrial Informatics*. 2019. **15** (5). P. 2544–2554. https://doi.org/10.1109/TII.2018.2866445.
55. Khanna K., Panigrahi B.K., Joshi A. Bi-level modelling of false data injection attacks on security constrained optimal power flow. *IET Generation, Transmission and Distribution*. 2017. **11** (14). P. 3586–3593. https://doi.org/10.1049/iet-gtd.2017.0226.
56. Salmeron J., Wood K., Baldick R. Analysis of electric grid security under terrorist threat. *IEEE Transactions on Power Systems*. 2004. **19** (2). P. 905–912. https://doi.org/10.1109/TPWRS.2004.825888.
57. Zeraati M., Aref Z., Latify M.A. Vulnerability analysis of power systems under physical deliberate attacks considering geographic-cyber interdependence of the power system and communication network. *IEEE Systems Journal*. 2018. **12** (4). P. 3181–3190. https://doi.org/10.1109/JSYST.2017.2761844.
58. Kushal T.R.B., Lai K., Illindala M.S. Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system. *IEEE Transactions on Smart Grid*. 2018. **10** (5). P. 4741–4750. https://doi.org/10.1109/TSG.2018.2867809.
59. Zheng K., Albert L.A. Interdiction models for delaying adversarial attacks against critical information technology infrastructure. *Naval Research Logistics*. 2019. **66** (5). P. 411–429. https://doi.org/10.1002/nav.21859.
60. Heyman D.P., Sobel M.J. Stochastic models in operations research. Volume II. Stochastic optimization. Mineola : Dover Publications, 2003. 576 p. ISBN 978-0486432601.
61. Zheng K., Albert L., Luedtke J., Towle E. A budgeted maximum multiple coverage model for cybersecurity planning and management. *IISE Transactions*. 2019. **51** (3). P. 1–37. https://doi.org/10.1080/24725854.2019.1584832.
62. Zheng K., Albert L.A. A robust approach for mitigating risks in cyber supply chains. *Risk Analysis*. 2019. **39** (9). P. 2076–2092. https://doi.org/10.1111/risa.13269.
63. Yuan W., Zhao L., Zeng B. Optimal power grid protection through a defender-attacker-defender model. *Reliability Engineering & System Safety*. 2014. **121** (C). P. 83–89. https://doi.org/10.1016/j.ress.2013.08.003.
64. Puterman M.L. Markov decision processes: discrete stochastic dynamic programming. Hoboken, NJ: John Wiley & Sons, 2014. 684 p. ISBN 978-1-118-62587-3.
65. Ma C.Y.T., Yau D.K.Y., Rao N.S.V. Scalable solutions of Markov games for smart-grid infrastructure protection. *IEEE Transactions on Smart Grid*. 2013. **4** (1). P. 47–55. https://doi.org/10.1109/TSG.2012.2223243.

66. Barreto C., Cardenas A.A., Bensoussan A. Optimal security investments in a prevention and detection game. *Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp (April 4–5, 2017, Hanover, MD).* ACM, 2017. P. 24–34. https://doi.org/10.1145/3055305.3055314.
67. Rana M.M., Li L., Su S.W. Microgrid protection and control through reliable smart grid communication systems. *14-th International Conference on Control, Automation, Robotics and Vision (November 13–15, 2016, Phuket, Thailand*). IEEE, 2016. P. 1–6. https://doi.org/10.1109/ICARCV.2016.7838766.
68. Vandenberghe L., Boyd S. Semidefinite programming. *SIAM Review*. 1996. **38** (1). P. 49–95. https://doi.org/10.1137/1038003.
69. Хачиян Л.Г. Полиномиальный алгоритм в линейном программировании. *Доклады АН СССР*. 1979. **244** (5). С. 1093–1096. http://www.mathnet.ru/links/aa0a1616aac4375c8a61c02b885269e8/dan42319.pdf.
70. Darwish I., Igbe O., Saadawi T. Vulnerability assessment and experimentation of smart grid DNP3. *Journal of Cyber Security and Mobility*. 2016. **5** (1). P. 23–54. https://doi.org/10.13052/jcsm2245-1439.513.
71. Canzani E., Pickl S. Cyber epidemics: modeling attackerdefender dynamics in critical infrastructure systems. *Advances in Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing*. D. Nicholson (ed.). Cham, Switzerland: Springer, 2016. **501**. P. 377–389. https://doi.org/10.1007/978-3-319-41932-9_31.
72. Genge B., Haller P. A hierarchical control plane for softwaredefined networks-based industrial control systems. *2016 IFIP Networking Conference (IFIP Networking) and Workshops (May 17–19, 2016, Vienna, Austria).* IEEE, 2016. P. 73–81. https://doi.org/10.1109/IFIPNetworking.2016.7497208.
73. Zhang Y., Wang L., Sun W. Trust system design optimization in smart grid network infrastructure. *IEEE Transactions on Smart Grid.* 2013. **4** (1). P. 184–195. https://doi.org/10.1109/TSG.2012.2224390.
74. Cano J., Pollini A., Falciani L., Turhan U. Modeling current and emerging threats in the airport domain through adversarial risk analysis. *Journal of Risk Research*. 2016. **19** (7). P. 894–912. https://doi.org/10.1080/13669877.2015.1057201.
75. Ravishankar M., Rao D.V., Kumar C.R.S. A game theoretic software test-bed for cyber security analysis of critical infrastructure. *Defence Science Journal.* 2018. **68** (1). 54–63. https://doi.org/10.14429/dsj.68.11402.
76. Puzis R., Klippel M.D., Elovici Y., Dolev S. Optimization of NIDS placement for protection of intercommunicating critical infrastructures. *Intelligence and Security Informatics (December 3–5, 2008, Esbjerg, Denmark). Lecture Notes in Computer Science.* D. Ortiz-Arroyo, H.L. Larsen, D.D. Zeng, D. Hicks, G. Wagner (eds.). Heidelberg, Germany: Springer. 2008. **5376**. P. 191–203. https://doi.org/10.1007/978-3-540-89900-6_20.
77. Zhang Y., Sun W., Wang L. Location and communication routing optimization of trust nodes in smart grid network infrastructure. *Power and Energy Society General Meeting (July 22–26, 2012, San Diego, CA).* IEEE, 2012. P. 1–8. https://doi.org/10.1109/PESGM.2012.6345688.
78. Eldosouky A., Saad W., Kamhoua C., Kwiat K. Contract-theoretic resource allocation for critical infrastructure protection. *2015 IEEE Global Communications Conference (December 5–10, 2015, San Diego, CA).* IEEE, 2015. P. 1–6. https://doi.org/10.1109/GLOCOM.2015.7417071.
79. Ravishankar M., Rao D.V., Kumar C. A game theoretic approach to modelling jamming attacks in delay tolerant networks. *Defence Science Journal*. 2017. **67** (3). P. 282–290. https://doi.org/10.14429/dsj.67.10051.
80. Wei L., Sarwat A., Saad W., Biswas S. Stochastic games for power grid protection against coordinated cyber-physical attacks. *IEEE Transactions on Smart Grid.* 2018. **9** (2). P. 684–694. https://doi.org/10.1109/TSG.2016.2561266.
81. Dewri R., Poolsappasit N., Ray I., Whitley D. Optimal security hardening using multi-objective optimization on attack tree models of networks. *14-th ACM Conference on Computer and Communications Security (October 28–31, 2007, Alexandria, VA).* P. Ning, S. De Capitani di Vimercati, P.F. Syverson (eds.). ACM, 2007. P. 204–213. https://doi.org/10.1145/1315245.1315272.
82. Nandi A.K., Medal H.R., Vadlamani S. Interdicting attack graphs to protect organizations from cyber attacks: a bi-level defender–attacker model. *Computers & Operations Research.* 2016. **75**. P. 118–131. https://doi.org/10.1016/j.cor.2016.05.005.
83. Almohri H.M., Watson L.T., Yao D., Ou X. Security optimization of dynamic networks with probabilistic graph modeling and linear programming. *IEEE Transactions on Dependable and Secure Computing.* 2016. **13** (4). P. 474–487. https://doi.org/10.1109/TDSC.2015.2411264.
84. Sawilla R., Skillicorn D. Partial cuts in attack graphs for cost effective network defence. *2012 IEEE Conference on Technologies for Homeland Security (November 13–15, 2012, Waltham, MA).* IEEE, 2012. P. 291–297. https://doi.org/10.1109/THS.2012.6459864.
85. Korzhyk D., Conitzer V., Parr R. Complexity of computing optimal Stackelberg strategies in security resource allocation games. *24-th AAAI Conference on Artificial Intelligence (July 11–15, 2010, Atlanta, GA).* M. Fox, D. Poole (eds.). AAAI Press, 2010. P. 805–810. https://www.aaai.org/ocs/index.php/AAAI/AAAI10/paper/view/1870/2093.

86. Горбачук В.М., Дунаєвський М.С., Морозов О.О. Рівноважні інвестиції у кібербезпеку мережі ланцюгів постачання. *Вісник Київського університету. Серія: фізико-математичні науки.* 2017. № 2. С. 47–52. http://nbuv.gov.ua/UJRN/VKNU_fiz_mat_2017_2_10.
87. Горбачук В.М., Дунаєвський М.С., Сирку А.А., Сулейманов С.-Б. Економіка кібербезпеки. *Інформаційні технології та взаємодії*. Київ : КНУ ім. Т. Шевченка, 2017. С. 207–208. https://www.researchgate.net/publication/361292763_Cybersecurity_economics.

Отримано 26.05.2022