УДК 004.7

О.П. Ігнатенко

ТЕОРЕТИКО-ІГРОВИЙ ПІДХІД ДО ПРОБЛЕМИ БЕЗПЕКИ МЕРЕЖ

В даній роботі здійснено огляд основних напрямків застосування теоретико-ігрового підходу до розв'язання актуальних проблем безпеки. Теорія ігор досліджує взаємодію раціональних агентів за умов конфлікту та невизначеності. Моделі теорії ігор успішно застосовуються для вивчення процесів у економіці, біології, комп'ютерних мережах та інших. Застосування до забезпечення безпеки – відносно новий напрямок, який дозволяє представити проблему захисту у вигляді гри, та застосувати розвинені методи ігрового аналізу. Описано сучасний стан області, виділені основні напрямки загроз та відповідні моделі і методи теорії ігор. Запропоновано класифікацію ігрових підходів у області кібербезпеки та проведено порівняння різних класифікацій. Окремо розглядаються атаки на відмову, які є одним з найбільш небезпечним напрямком розвитку кіберзлочинності. Побудовані ігрові моделі таких атак, та проведений аналіз вразливості стратегій захисту. Виділені майбутні тренди застосування ігрового підходу в області кібербезпеки.

Ключові слова: теорія ігор, мережеві атаки, безпека систем.

Вступ

Сучасні мережі стали невід'ємною частиною повсякденного життя. Комунікації, спілкування, бізнес та держава пронизані невидимими оку зв'язками, які забезпечують швидку, надійну та ефективну роботу механізмів. Водночас, розвиток цієї галузі спричинив також і появу цілої низки негативних явищ, які, в силу проникнення інформаційних мереж в усі області життя, наразі представляють зростаючу загрозу безпеці людей.

До цих явищ відносяться, зокрема, атаки у мережі Інтернет, крадіжка даних, фішинг, спам, вимагання грошей та багато інших. Методи нападу розвинулись настільки, що навіть використовуються для атак на економіку та критичну інфраструктуру цілих держав. Деякі з кіберзагроз ще не з'явились, але очікуються в майбутньому з подальшим розвитком технологій. Наприклад, є думка, що широке впровадження Інтернету речей призведе до появи вірусів, орієнтованих на розумні побутові речі.

Важливо зазначити, що сьогодні у конфлікті нападників і захисників у кіберпросторі присутня суттєва асиметрія. Нападники можуть планувати свої дії, чекати слушного моменту, збирати інформацію та шукати вразливості. Водночас захисники (адміністратори системи) змушені готуватись до нападу з будь-якого напрямку і до атаки будь-якого типу. Захисники мають постійно моніторити активність, реагувати на всі (можливо помилкові) повідомлення системи виявлення та реагувати на дії зловмисників. Навіть після успішного відбиття атаки захисники витрачають ресурси, а за несприятливих умов об'єкт атаки несе збитки та може втратити цінну інформацію. За сучасної архітектури мереж майже ніколи не вдається виявити зловмисників, тим більше притягнути їх до відповідальності, тому нападники майже не ризикують. Безкарність та успішність мережевих атак призвела до появи ринку супутніх послуг. Цей ринок розташований у даркнеті – антиподі Інтернету, де відбувається торгівля краденою інформацією, наркотиками, зброєю, вірусами та послугами з атак сайтів.

Отже, актуальним на сьогодні напрямком є розвиток моделей та методів забезпечення безпеки різноманітних інформаційних систем (які, як правило є складовими мереж: провідних, безпровідних, супутникових тощо).

Існує декілька причин, які обумовлюють проблеми забезпечення безпеки мереж. Як зазначено у [1] "основна причина полягає у тому, що через *складність* та *взаємозв'язаність* сучасних мереж користувачам (і адміністраторам) важко від-

слідковувати та керувати процесами, що відбуваються". По-перше, зазвичай користувачі використовують лише незначну частину ресурсів власних комп'ютерів. Операційна система виконує велику кількість автоматичних процесів, які у забезпечують її взаємодію з користувачем, обладнанням, віддаленими сервісами. Людина має безпосередню справу лише з спрощеним інтерфейсом.

Схожим чином, адміністратори локальних мереж можуть керувати лише локальними налаштуваннями, однак не мають можливості припинити глобальні зв'язки. Включеність усіх пристроїв у глобальну мережу робить їх вразливими і це друга складова проблеми.

Нарешті остання суттєва на нашу думку причина полягає у динамічності процесів захисту та нападу. Динаміка, означає, що з часом характеристики системи захисту і нападу суттєво змінюються. З'являються нові типи атак, виникають нові вразливості у програмному забезпеченні, хакери знаходять нові способи використовувати існуючі особливості систем. З іншого боку фірми створюють нові системи захисту, оновлюють програмне забезпечення, розробляють більш надійні програми. Окрім цієї "повільної" динаміки є також динаміка протікання атаки – дії нападників, протидія адміністраторів, все це відбувається у реальному часі і не може розглядатись статично.

В даній роботі пропонується огляд теоретико-ігрового підходу до аналізу безпеки інформаційних систем. Цей підхід дозволяє розглядати проблеми забезпечення безпеки з точки зору прийняття рішень раціональними агентами за умов конфлікту, невизначеності та використовує апарат аналітичного моделювання теорії ігор.

Теоретико-ігровий підхід

Основні визначення. Для кращого розуміння застосування теорії ігор визначимо спочатку основні терміни. *Взаємодія* характеризує процеси практично у будь-якій досить складній системі. Говорячи про теорію ігор ми, насамперед, маємо на увазі системи, що складаються з сутностей здатних приймати рішення. Це можуть бути люди, організації, держави і навіть, комп'ютерні програми. Надалі відносно таких сутностей будемо використовувати термін *гравці*. Рішення має наслідком дію гравця, яка впливає на стан системи.

Майже завжди при цьому виникає питання пов'язаності – дії одних гравців впливають на стан інших, позитивно або негативно. Такі ситуації називають *стратегічною взаємодією* оскільки гравець, який прагне діяти з метою отримання найкращого для себе результату має зважувати на дії інших та враховувати їх інтереси. Стратегічна поведінка, таким чином, має враховувати всі можливі дії гравців, які можуть вплинути на результат гри, та визначати власну дію для кожної ситуації. *Стратегією* гравця називають правило або функцію, яка вичерпно визначає його дії у будь-який момент гри в залежності від доступної йому інформації.

Отже гра присутня за наявності як мінімум двох гравців, які взаємодіють. Для визначення гри у стратегічній формі потрібно визначити три компонента: множини гравців, їх стратегій і виграшів.

Слід відрізняти терміни дія і стратегія. Стратегія є способом прийняття рішень у конкретній грі, і залежить від інформованості, уподобань конкретного гравця, та (можливо) структури гри і стратегій інших учасників. Дія, у свою чергу, є наслідком стратегії та відображає вплив гравця на результат гри.

Класифікація ігор. Ігри можна класифікувати за певними ознаками з метою визначити основні характеристики, які дозволяють віднести ігрову модель до того чи іншого класу.

1. Статичні та динамічні ігри. Статичні ігри можуть розглядатися як динамічні у однокроковій постановці. Основна відмінність полягає у тому, що динамічні ігри розгортаються у часі і гравці отримують інформацію щодо попередніх станів, стратегій та дій інших гравців. На основі цієї інформації можливе налаштування стратегій для покращення виграшу в залежності від протікання гри. Окремим

класом являються стохастичні ігри, у яких гра переходить з одного стану в інший з певною ймовірністю, тому гравці мають будувати свої стратегії на основі *очікуваних виграшів*.

2. Кооперативні і некооперативні ігри. Некооперативна гра означає, що поведінка учасників визначається лише їх власними інтересами, тобто немає зовнішніх сил, які б змушували гравців до виконання певних дій (наприклад, спрямованих на досягнення соціально справедливого рішення). Така постановка є природною для більшості ігор, які ми зустрічаємо у реальних системах. Основною особливістю, яка вирізняє некооперативні ігри поміж інших полягає у індивідуальності дій гравців. Індивідуальна дія – це особисте рішення гравця, яке приймається усвідомлено на базі наявної інформації про гру, інших гравців та їх інтересів. Ще одна ключова відмінність відноситься до виконання рішень групи або коаліції (яка утворюється з метою збільшення виграшу). В кооперативних іграх відхилення від рішення коаліції неможливе або карається штрафом.

3. Ігри з повною та неповною інформованістю. Гра називається грою з повною інформованістю, якщо всі елементи гри відомі всім учасникам. В іншому випадку кажуть про ігри з неповною інформованістю. В грі з повною інформованістю кожен гравець володіє інформацією про множину гравців, їх можливих стратегій і виграшів.

4. Ігри з досконалою та недосконалою інформованістю. В іграх з досконалою інформованістю гравці володіють інформацією про всі попередні дії всіх гравців. Прикладом такої гри є шахи. В іграх з недосконалою інформованістю гравці не мають інформації про (деякі) попередні дії інших, наприклад покер.

Таким чином, гра представляє математичну структуру, що представляє інтерес для дослідження. Головною задачею є *розв'язок гри*. Під розв'язком гри розуміють знаходження результату гри для кожної позиції, виграші гравців та їх стратегії, що призводять до цих виграшів. В залежності від інформованості та постановки гри виграш може бути результатом певного випадкового процесу, в такому разі говорять про *очікуваний виграш*. Вважається, що кожен гравець намагається максимізувати свій виграш, що, як правило, призводить до конфлікту (ситуації в яких інтереси гравців не суперечать можуть розглядатися як задачі оптимізації). Історично перший загальний підхід до розв'язання ігрових задач був запропонований фон Нейманом і отримав назву мінімаксний розв'язок. Пізніше Дж. Нешем було запропоноване узагальнення відоме як рівновага Неша. Основна ідея рівноваги Неша полягає у пошуку ситуації у грі, в якій жодному з гравців невигідно одноосібно змінювати свою стратегію, бо це зменшує його виграш.

Зустрічаються ситуації, коли один з гравців може спостерігати рішення іншого. Для таких ігор рівновага була описана Штакельбергом. Ігри Штакельберга часто використовуються для дослідження атак у мережах, оскільки рішення часто приймаються у відповідь на дії суперника.

Ще одним напрямком дослідження невизначеності в іграх є Байєсівські ігри. В Байєсівських іграх учасники точно знають тільки свій тип (множину стратегій, функцію виграшу). Щодо типів інших гравців, то кожен знає тільки розподіл на просторі відомих типів гравців, відповідно до якого перед початком гри вибираються учасники. Такі моделі відображають ситуацію атаки мережі, коли тип атаки невідомий, але вибирається з певної відомої множини, захисники мають зважати на це при побудові своїх стратегій.

При розгляді процесів нападу і захисту в мережах слід зафіксувати основні терміни.

Користувачі. Автономні агенти, поведінка яких визначається певними задачами. Ці задачі, як правило, полягають у отриманні певних послуг від мережі (завантаження або пересилка даних, здійснення обчислень та інше).

Мережа. Система, що складається з вузлів, сервісних елементів та ліній передачі даних (ланок). В широкому розумінні мережа включає у себе вузли нападу і захисту, та об'єкти атаки (наприклад, комп'ютери або роутери).

Вузли мережі. Елементи мережі, які можуть мати один або більше сервісних елементів та множину вхідних і вихідних ліній зв'язку.

Сервісні елементи. Елементи мережі, що обслуговують задачі користувачів.

Комунікаційні ресурси. Представляє складне середовище, що включає канали зв'язку, маршрутизатори, протоколи взаємодії користувачів, механізми керування перевантаженнями. До основних задач цієї системи належать: стабільна передача даних користувачів, стабільна і прогнозована робота, рівномірний розподіл ресурсів.

Система виявлення вторгнень. Програмний або апаратний механізм, який відповідальний за виявлення атак. В залежності від рівня абстракції моделі може виявляти атаки без запізнення та надійно (тобто спрацьовує лише за наявності атаки) або ненадійно, в цьому випадку визначаються ймовірності помилкового виявлення атаки та не виявлення.

Захисники. Користувач або адміністратор, які відповідають за безпеку системи та мають можливості впливу на систему виявлення та інші механізми протидії.

Зловмисні користувачі. Відкритість середовища означає, що будь-який користувач може надіслати свої пакети у мережу і мережа вважає їх коректними, доки не було виявлено протилежне. В результаті зловмисники отримують можливість впливу на роботу сервера або елементів мережі.

Атака. Існує велика кількість типів атак. Узагальнено будемо визначати атаку як послідовність кроків нападників і захисників, що утворюють гру.

Важливо сформулювати основні причини успішності застосування теорії ігор в даній області:

- математичний апарат. Сучасні рішення з безпеки використовують евристики, запропоновані спеціалістами з власного досвіду. Теорія ігор дозволяє залучати для прийняття рішень розвинений математичний апарат, який призначений для моделювання ситуацій прийняття рішень агентами за умов конфлікту і невизначеності;

- гарантований результат. Якщо захисний механізм побудований на основі аналітично розв'язаної гри і виконуються припущення (за яких гра була визначена), то стратегія гарантує певний рівень безпеки за будь-яких дій інших учасників;

- розподілене рішення. Централізоване керування має багато недоліків і саме нерідко стає ціллю атаки, тому важливо будувати захисні механізми розподіленим чином, однак це, як правило, складно. Ігрові моделі дозволяють створити систему взаємодії, де кожен гравець максимізує свій виграш і, тим самим, сприяє загальній системі захисту. Інший перспективний напрямок, який може бути корисний у цій області – агентно-орієнтовані системи;

- розробка оптимальних механізмів. Область теорії ігор, що досліджує задачі створення правил гри, за яких гравці ведуть себе потрібним чином. В рамках цього підходу можливе створення протоколів, які заохочують кооперацію між користувачами та дозволяють їм об'єднуватися для відбиття атаки.

Огляд ігрових підходів до проблем безпеки

В даному розділі описані основні огляди і класифікації ігрових підходів. Ми спробуємо описати основні тренди досліджень та їх можливий розвиток а також навести посилання на описові роботи, які демонструють стан розвитку проблематики.

Існують різні підходи до класифікації застосування апарату теорії ігор до розв'язання проблем в області безпеки. Одна з перших робіт, у якій проблема розглядалась системно досліджувала проблему виявлення вторгнення у вигляді гри у розширеній формі [2]. Було описано дві постановки: кооперативну гру системи виявлення в якій сенсори утворюють коаліції для підвищення ймовірності виявлення вторгнення та скінчену некооперативну гру атакуючого та системи захисту. Пізніше автори суттєво доповнили і розширили застосування, фактично очоливши новий напрямок розвитку.

В роботі [1] напрямки досліджень було класифіковано за предметною областю застосування. Були виділені такі області:

- системи виявлення вторгнень;
- прийняття рішень після виявлення атаки (вторгнення);
- моделювання зловмисної діяльності у мережах. Під мережами тут розуміється будь-яка складна мережева система;
- кількісна оцінка ризиків. Зокрема в цій категорії досліджувались інвестиційні ігри;
- алгоритми розподілу ресурсів та побудова стійких протоколів взаємодії;
- приватність, довіра, зручність використання.

Загалом підхід має очевидні переваги та практичну орієнтованість. До недоліків слід віднести ad-hoc схему та те, що різні області застосування можуть використовувати одні й ті самі ігрові моделі. Інші огляди [3, 4] будують класифікацію на основі моделей теорії ігор, що використовуються для розв'язання проблем безпеки. Стандартна дихотомія за ознаками, описаними в попередньому розділі дозволяє класифікувати напрямки (таблиця). В роботі [4] наведені посилання на основні роботи за напрямками. Далі наведені основні

Таблиця

Інформованість	Досконала	Недосконала	
	Динамічна постановка	Статична постановка	Динамічна постановка
Повна	Гра виявлення вторгнення у постановці матричної гри двох учасників Штакельберга (що означає наявність лідера який приймає рішення першим, інший гравець будує свою стратегію знаючи цю обставину).	Ігри інвестування у безпеку та розподілу ресурсів у матричній постановці. Гра інформаційного протиборства двох гравців. Оцінка ризиків у мережах для гри двох гравців з нульовою сумою.	Стохастичні ігри. Проблема визначення оптимальної стратегії адміністратора для балансування ризиків в мережі за умов атаки. Обчислення оптимальної протидії. Марковські ігри. Використання Q-навчання у ситуації невідомою перехідної матриці.
Неповна	Виявлення вторгнення в Ad hoc мережі. Формулювання у вигляді сигнальної гри двох гравців. Гра за умов невідомих функцій виграшу гравців. Навчання за різними схемами. Багатокрокові Байєсівські ігри у безпровідних мережах для моделювання атак глушіння.	Інформаційна гра безпеки між експертом та декількома "наївними" агентами за умов обмеженості інформації про ризики інших. Байєсівські ігри двох гравців.	Багатокрокова Байєсівська гра двох гравців у якій кожний гравець намагається покращити своє знання про тип свого суперника.

характеристики досліджень: моделі теорії ігор, що використовуються та проблема безпеки, що вирішується.

В роботі [4] проведена спроба подальшого розвитку класифікації існуючих досліджень, запропонована ідея розділяти дослідження за схемою застосування методів теорії ігор до моделей області безпеки.

В останньому за часом огляді (на момент написання статті) [5] виділені наступні класи ігор у області кібербезпеки:

- стохастичні ігри з нульовою сумою. Запропонований алгоритм пошуку сідлової точки [6];
- Статичні ігри. Як правило, досліджується рівновага Неша і Штакельберга [7];
- Динамічні ігри. Дискретизована модель, пошук точки рівноваги Неша [8];
- Марковські ігри з нульовою сумою [9].

В даній роботі пропонується використовувати для класифікації не окрему категорію а весь процес рішення проблеми (рисунок).

Виділимо основні кроки.

1. Моделювання предметної області. Дослідження будь-якого процесу починається з побудови його моделі. В залежності від вибраної моделі підбирається інструментарій аналізу. Це можуть бути динамічні системи (неперервні, дискретні), що описуються диференціальними рівняннями (з запізненнями, імпульсним керуванням), лінійні стаціонарні системи, мульти-агентні системи тощо.

2. Постановка ігрової задачі. На цьому етапі визначаються всі ігрові характеристики: гравці, стратегії, інформованість, виграші. Ставиться задача ігрового аналізу, яка може полягати у формалізації ігрової моделі, пошуку рівноваги, визначенню найкращих стратегій та розробці оптимальних правил, за яких результат гри буде відповідати заданим критеріям.

3. Розв’язок: стратегії, виграші, алгоритми навчання. Розв’язується задача ігрового аналізу: пошук рівноваги, розв’язання гри (тобто обчислення найкращої поведінки гравців у кожній точці), визначення алгоритмів навчання, які наближаються до точки рівноваги за умов обмеженої інформованості. Пошук алгоритмів навчання особливо важливий з огляду на обмеженість інформованості у реальних системах та розподіленість систем захисту.

4. Побудова моделі взаємодії. На базі отриманих стратегій поведінки гравців та з використанням моделей предметної області будується модель конфлікту з метою визначення важливих характеристик, наприклад обчислення числових параметрів захищеності (вразливості) існуючої системи протидії. На цьому етапі виникає можливість вимірювання параметрів якості системи захисту або вразливості до певного типу атак.

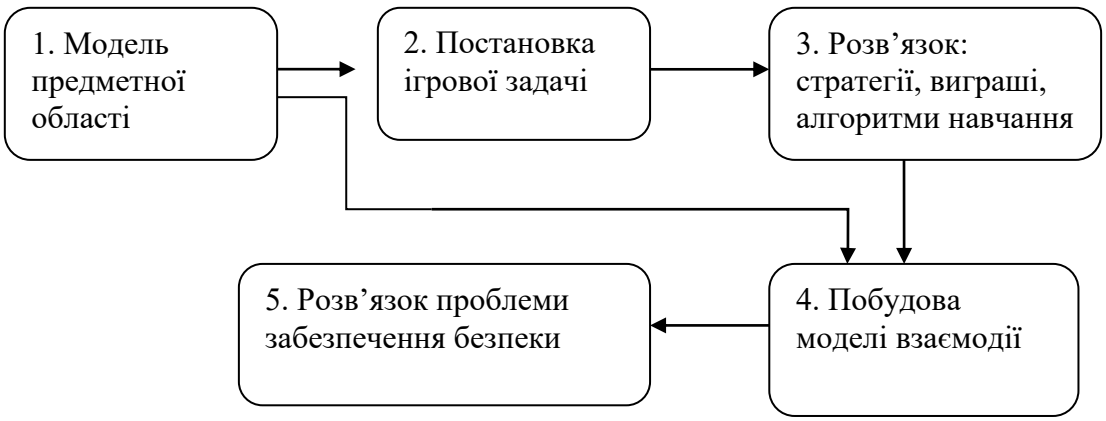

Рисунок. Схема застосування ігрового підходу

5. Розв'язок проблеми забезпечення безпеки. Обчислення характеристик вразливості до тих чи інших атак дає змогу поставити проблему про забезпечення безпеки системи, як задачу теорії ігор: яким параметрам має задовольняти система захисту, щоб гарантувати певний виграш за умов атаки.

Атаки відмови в обслуговуванні

На сьогодні існує велика кількість загроз безпеки сучасних мереж. Це спам, фішинг, крадіжка даних, несанкціоноване вторгнення, віруси та атаки. Одним з найбільш небезпечних видів є так звані атаки типу "відмова в обслуговуванні" (Denial of Service Attack – DoS) [10]. Ціллю DoS атаки є сервіс, що надається користувачам. Якщо пакети, що перешкоджають роботі системи надходять з різних джерел, таку атаку називають розподіленою. Існує велика кількість DoS атак [10, 11]. Кожна з них використовує певну слабкість програмного забезпечення, реалізації протоколів і навіть принципів побудови Інтернету. Принципово можна виділити два основних типи атак. Перший тип використовує слабкості і помилки програмного забезпечення, служб або протоколів які використовуються об'єктом атаки для надання сервісів користувачам. Використання спеціально сформованих шкідливих пакетів дозволяє ускладнити або заблокувати роботу системи. Другий спосіб полягає у використанні великих об'ємів беззмістовного трафіку для завантаження ресурсів, необхідних для обробки запитів звичайних користувачів. І якщо у першому випадку можна захиститися знешкоджуючи слабкості шляхом оновлення програм, то попередити атаку другого типу вже не так просто. При цьому потужність і складність атак постійно зростає. Так загальним явищем стала ситуація, коли трафік атаки надсилається з багатьох джерел (такі атаки отримали назву розподілені атаки на відмову). Останні тенденції показують на появу нових типів атак – прихованих атак. В цьому випадку підконтрольні атакуючому комп'ютери отримують доступ до цільового сервісу на цілком законних підставах (наприклад, відвідують веб сайт компанії) і завантажують канал ресурсоємними операціями (атака погіршення якості) або в певний момент «вибухають» беззмістовним трафіком, що ставить перед системами захисту нові нетривіальні задачі виявлення і протидії.

На відміну від загальних проблем безпеки, застосування ігрового підходу до моделювання атак на відмову є рідкістю. Зокрема, один з останніх оглядів області [11] не згадує про такі роботи, хоча вони трапляються. В огляді [5] наведено докладний опис застосування ігрових підходів до моделювання проблем безпеки, зокрема і атак типу відмова в обслуговуванні. Основними напрямками застосування є:

- визначення основних стратегій поведінки нападника та формування стратегій протидії (запуск фільтрації пакетів, обмеження пропускної здатності, яка виділяється користувачам тощо);
- побудова функцій виграшу захисників, яка включає якість послуг, що надаються користувачам. Така функція виграшу має враховувати погіршення якості обслуговування, затримки, втрачені пакети (внаслідок помилкової реакції на атаку). Після побудови функцій виграшу можливе застосування відомих методів ігрового аналізу;
- застосування методу fictitious play (уявної гри) дозволяє запустити алгоритм навчання гравців за умов невідомих функцій виграшу.

В роботах [12–15] авторами було розроблено підхід до моделювання атак на основі теорії конфліктно-керованих систем (підрозділ загальної теорії ігор, що досліджує диференціальні ігри). Нагадаємо постановку задачі. Розглянемо мережу, що складається з M робочих вузлів. Кожен вузол містить принаймні один сервісний елемент, при цьому сумарний ресурс всіх сервісних елементів обмежений. Позначимо множину індексів вузлів мережі $I = \{1,...,M\}$, множину індексів сервісних елементів $K = \{1,...,L\}$. Максимальний ресурс вузла з індексом $k \in K$ позначимо $p_i \in R^M_{++}$, а максимальну долю,

яку може отримати сервісний елемент з індексом $k \in K$ позначимо $q_k \in R_{++}^L$. Нехай матриця C описує структуру відповідності вузлів та сервісних елементів, $C = \{c_{ik}\}_{k \in K, i \in I}$, де елемент c_{ik} дорівнює 1 якщо елемент k належить *i*-тому вузлу і 0 в іншому випадку. Будемо вважати, що у кожного вузла має бути як мінімум один сервісний елемент, та кожний сервісний елемент не може належати більш як одному вузлу.

Припустимо, що в мережі присутні N користувачів, проіндексованих множиною $J = \{1,..., N\}$. Поставимо кожному з них у відповідність функцію $x_j(t)$, $j \in J$, $t \geq 0$, яка описує його швидкість його передачі даних у мережу (наприклад, завантаження файлу на віддалений сервер) в момент часу *t*. Природно обмежити вектор можливих швидкостей

$$x(t) = (x_1(t),..., x_N(t))$$

областю $X \subset R_+^n$. Кожен користувач зацікавлений в отриманні найкращого рівня обслуговування, і намагається діяти відповідно. Пакети користувачів опрацьовуються послідовно, переміщуючись з вузла на вузол, при цьому за кожним користувачем закріплений маршрут руху пакетів, який описується індексами сервісних елементів

$$m_j = \{k_1,..., k_{n_j}\},\ k_p \in K,\ p \in \{1,..., n_j\}.$$

Припустимо, що зафіксовано вектор $x(t) = (x_1(t),..., x_N(t))$, тоді сервісний елемент $k \in K$ отримує навантаження

$$y_k(t) = \sum_{j \in s(k)} x_j(t),$$

де $s(k) = \{j \in J : k \in m_j\}$. Введемо функції швидкості обслуговування $u_k(t)$, $k \in K$. Функція $u_k(t) = (u_1(t),..., u_L(t))$ – це керування мережі. Нехай

$$P = diag\{p_1,..., p_M\},\ Q = diag\{q_1,..., q_L\},$$

діагональні матриці, тоді множина керування дорівнює:

$$U = \{u \in R_+^L \mid P^{-1} C Q^{-1} \bar{u} \leq \bar{1}\},$$

де нерівність розуміється порядково, а $\bar{1} = (1,...,1)^T$. Множина $U \subset R_+^L$ є опуклою і містить початок координат. Матриця маршрутизації $R = \{r_{ij}\}$, $i, j \in K$ визначається наступним чином: елемент r_{ij} дорівнює 1, якщо вихід *i*-го сервісного елемента є входом *j*-го сервісного елемента і 0 в іншому разі. При цьому будемо вважати, що в системі відсутні цикли і будь-який пакет полишає мережу менш як за $L-1$ кроків, іншими словами $R^L = 0$. Матриця

$$A = \{a_{kj}\},\ k \in K,\ j \in J$$

визначається структурою вхідного потоку, при цьому a_{kj} дорівнює 1, якщо користувач з індексом j надсилає свої дані на вхід сервісного елемента з індексом k і 0 в іншому разі. Визначимо динамічну систему

$$\dot{\bar{y}}(t) = A\bar{x} - B\bar{u}, \qquad (1)$$

де матриця $B = [I - R^T]$, $\bar{y} \in R_+^L$. Динамічна система (1) описує процес взаємодії користувачів та мережі. Можливі дві задачі: моделювання системи керування мережею за умов роботи звичайних користувачів та робота системи захисту за умов атаки. В останньому випадку виділяється група зловмисних користувачів, які атакують мережу.

В роботах [14, 15] проведено узагальнення та здійснене моделювання атак поглинаючого типу для такого типу систем.

Пізніше, в роботах [16, 17] виконано застосування апарату теорії еволюційних ігор до проблеми (1).

Була побудована модель та знайдені умови існування рівноваги в змішаних стратегіях для моделі взаємодії багатьох типів AIMD-з'єднань. Виявляється, що тип рівноваги сильно залежить від параметрів, що характеризують протоколи і поведінку користувачів. В роботі [15] представлено умови, що пов'язують ці параметри.

Проблеми і перспективи подальших досліджень

Описані роботи показують, що застосування ігрового підходу до розв'язання проблем безпеки (що включає моделювання, постановку проблеми і її рішення) все ще сильно залежить від вибраної схеми ігрової взаємодії користувачів, яка, як правило, є спрощенням реального світу.

Наприклад, якщо розглядаються ігри між одним нападником і системою захисту, то використовують ігри двох учасників. Якщо ситуація розгортається у часі, використовують динамічну постановку. Важливою є також припущення про інформованість учасників, в залежності від чого використовуються ігри з досконалою або недосконалою та повною або неповною інформованістю.

Основні недоліки сучасних підходів. Обмеженість даного підходу зрозуміла:

1. По-перше, оскільки найбільш дослідженими є ігри двох учасників, то при розгляді проблем безпеки намагаються звести задачу до цього типу.

2. По-друге, матричні (статичні) ігри, які використовують через їх простоту, малореалістичні. Майже всі реальні процеси змінюються у часі і вимагають відповідного моделювання.

3. При моделюванні стратегій, як правило, фіксується певна скінченна кількість станів у яких може знаходитись гра. Відповідна скінчена гра може бути розв'язана, але на практиці кількість таких станів нескінченна, що потребує додаткових досліджень.

Майбутні напрямки досліджень. Виділимо найбільш перспективні можливі напрямки досліджень, у яких буде розвиватись теоретико-ігровий підхід у області кібербезпеки.

1. Соціальні мережі. Останнім часом соціальні мережі такі як Фейсбук і Твіттер стали найпоширенішим засобом комунікації. Внаслідок цього соцмережі накопичили гігантські обсяги приватних даних, які можуть бути об'єктом атаки. Іншою ціллю можуть бути фірми, які перенесли свою діяльність у Фейсбук. Вже спостерігаються скоординовані атаки з негативними відгуками та зниженням рейтингу. В роботі [18] описані існуючі на сьогодні атаки і загрози в таких мережах.

2. Хмарні обчислення. Хмарні обчислення (Cloud computing) це нова парадигма, яка дозволяє отримувати доступ до програмних, обчислювальних та інформаційних ресурсів у вигляді мережевих сервісів. З розвитком та ускладненням хмарних сервісів виникає проблема побудови ефективних алгоритмів забезпечення їх безперешкодної роботи. Користувачі, таким чином, отримують доступ на основі принципу pay-as-you-use до найбільш сучасної інфраструктури не витрачаючи коштів на її створення та підтримку. Провайдери в свою чергу максимізують використання своїх потужностей та можуть балансувати навантаження через мережі для досягнення рівномірної загрузки.

Таким чином, ключовим елементом роботи хмарної системи є ефективні алгоритми надання сервісів користувачам. Сучасна хмарна система існує у середовищі постійних змін. Змінюються технології, протоколи та програмне забезпечення. Змінюються користувачі, їх пріоритети, задачі і поведінка. Всі ці зміни є непередбачуваними.

Тому теорія ігор, яка вже має історію успішного застосування до розв'язання задач маршрутизації, планування, керування потоками даних і перевантаженнями, є головним напрямком аналітичного моделювання хмарних систем.

3. Інтернет речей. Інтернет речей об'єднує в одну мережу всі розумні прилади, що уже в недалекому майбутньому будуть забезпечувати людське життя. За оцінками понад два мільярди нових приладів буде під'єднано до глобальної мережі у наступні 10 років. Проникнення розумних речей у наше життя стає тотальним і тому і загрози, які при цьому виникають також є тотальними. Вже фіксуються появи вірусів, що здатні брати під свій контроль кавоварки, тостери та інші прилади. Застосу-

вання теорії ігор та основні загрози з цього напрямку описані в [19]

4. Блокчейн. Технологія блокчейн, на основі якої будуються криптовалюти і декі нові сервіси. Одною з ключових проблем є забезпечення ефективного та безпечного “майнинга” (тобто обчислення підтвердження нових операцій або одиниць валюти). Теорія ігор моделює процес майнингу як взаємодію автономних агентів, що конкурують за ресурси. Враховуючи сучасну вартість криптовалюти біткоін атака на механізми обчислення може бути надзвичайно прибутковою. Атаки відмови в обслуговуванні, спрямовані на процес майнингу описані в роботі [20], а, власне, теоретико-ігровий аналіз і стратегії майнингу проаналізовані, наприклад, в роботі [21].

Підсумовуючи описане, можна сказати, що застосування теоретико-ігрового підходу до проблем безпеки, хоча і продовжується два десятиліття, все ще є новим підходом з багатьма нерозв’язаними проблемами. Складність ігор з багатьма учасниками за умов конфлікту і невизначеності стимулює дослідників до створення нових моделей і методів, які допоможуть створити новий, безпечний і ефективний кіберпростір.

1. Alpcan T., Başar T. Network security: A decision and game-theoretic approach. Cambridge University Press, 2010.
2. Alpcan T., Başar T. A game theoretic approach to decision and analysis in network intrusion detection. Decision and Control, 2003. Proceedings. 42nd IEEE Conference on. Vol. 3. IEEE, 2003.
3. Roy, Sankardas, et al. A survey of game theory as applied to network security. System Sciences (HICSS), 2010 43rd Hawaii International Conference on. IEEE, 2010.
4. Liang, Xiannuan, and Yang Xiao. Game theory for network security. IEEE Communications Surveys & Tutorials 15.1. 2013. P. 472–486.
5. Do, Cuong T., et al. Game Theory for Cyber Security and Privacy. ACM Computing Surveys (CSUR) 50.2. 2017. 30 p.
6. Zhu Q., Basar T. Robust and resilient control design for cyber-physical systems with an application to power systems. In Proceedings of IEEE Conference on Decision and Control and European Control Conference. 2011. P. 4066–4071.
7. Fei He, Jun Zhuang, and United States. Game-theoretic analysis of attack and defense in cyber-physical network infrastructures. In Proceedings of the Industrial and Systems Engineering Research Conference. 2012.
8. Abhishek Gupta, Cedric Langbort, and Tamer Basar. Optimal control in the presence of an intelligent jammer with limited actions. In Proceeding of the 49th IEEE Conference on Decision and Control (CDC). 2010. P. 1096–1101.
9. Андон П.І., Ігнатенко О.П. Протидія атакам на відмову в мережі інтернет: концепція підходу. *Проблеми програмування.* 2008. № 2-3. С. 564–574.
10. Андон П.І., Ігнатенко О.П. Атаки на відмову в мережі Інтернет: опис проблеми та підходів щодо її вирішення. Київ. (Препр./Ін-т програмних систем НАН України. 2008 – 50 с.).
11. Zargar, Saman Taghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." IEEE communications surveys & tutorials 15.4. 2013. P. 2046–2069.
12. Andon F.I., and Ignatenko O.P. Modeling conflict processes on the internet. *Cybernetics and Systems Analysis.* 49.4. 2013. P. 616–623.
13. Ігнатенко О.П. Одна динамічна конфліктно керована модель взаємодії користувачів у відкритих інформаційних середовищах. *Проблеми програмування.* 2012. № 4. С. 50–63.
14. Ignatenko O.P. Game theoretic modeling of AIMD network equilibrium. *Проблеми програмування.* 2016. № 1. С. 115–127.
15. Ігнатенко О.П. Моделі керування потоками даних мережі інтернет за умов нестабільної поведінки. *Проблеми програмування.* 2011. № 3. С. 38–51.
16. Ігнатенко О.П., Молчанов О.А. Еволюційні ігри в TCP мережах з політиками обмеження швидкості. *Проблеми програмування.* 2016. № 4. С. 33–47.
17. Ignatenko O. and Synetskyi O. Evolutionary Game of N Competing AIMD Connections.

Information and Communication Technologies in Education, Research, and Industrial Applications, Springer International Publishing. 2014. P. 325–342.
18. Carbunar, Bogdan, et al. "A survey of privacy vulnerabilities and defenses in geosocial networks." IEEE Communications Magazine 51.11. 2013. P. 114–119.
19. Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava. "Security in internet of things: Challenges, solutions and future directions." System Sciences (HICSS), 2016 49th Hawaii International Conference on. IEEE. 2016.
20. Johnson, Benjamin, et al. "Game-theoretic analysis of DDoS attacks against Bitcoin mining pools." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014.
21. Lewenberg, Yoad, et al. "Bitcoin mining pools: A cooperative game theoretic analysis." Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems. International Foundation for Autonomous Agents and Multiagent Systems, 2015.

Reference

1. Alpcan T., Başar T. Network security: A decision and game-theoretic approach. Cambridge University Press. 2010.
2. Alpcan T., Başar T. A game theoretic approach to decision and analysis in network intrusion detection. Decision and Control, 2003. Proceedings. 42nd IEEE Conference on. Vol. 3. IEEE, 2003.
3. Roy, Sankardas, et al. A survey of game theory as applied to network security. System Sciences (HICSS), 2010 43rd Hawaii International Conference on. IEEE, 2010.
4. Liang, Xiannuan, and Yang Xiao. Game theory for network security. IEEE Communications Surveys & Tutorials 15.1 (2013): 472-486.
5. Do, Cuong T., et al. Game Theory for Cyber Security and Privacy. ACM Computing Surveys (CSUR) 50.2 (2017): 30.
6. Zhu Q., Basar T. Robust and resilient control design for cyber-physical systems with an application to power systems. In Proceedings of IEEE Conference on Decision and Control and European Control Conference. 2011. P. 4066–4071.
7. Fei He, Jun Zhuang, and United States. Game-theoretic analysis of attack and defense in cyber-physical network infrastructures. In Proceedings of the Industrial and Systems Engineering Research Conference. 2012.
8. Abhishek Gupta, Cedric Langbort, and Tamer Basar. Optimal control in the presence of an intelligent jammer with limited actions. In Proceeding of the 49th IEEE Conference on Decision and Control (CDC). 2010. P. 1096–1101.
9. Andon P.I., Ignatenko O.P. Mitigation of denial of service attacks in Internet: agent concept. Problems of Programming. 2008. N 2-3. P. 564–574.
10. Andon P.I., Ignatenko O.P. Denial of service attacks on the Internet: survey of problems and solutions. Kyiv. Institute of Software Systems. 2008. 50 p.
11. Zargar, Saman Taghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." IEEE communications surveys & tutorials 15.4. 2013. P. 2046–2069.
12. Andon F.I., and Ignatenko O.P. "Modeling conflict processes on the internet." Cybernetics and Systems Analysis 49.4. 2013. P. 616–623.
13. Ignatenko O.P. About one dynamic model of conflict-control user interaction in open information environments. Problems of Programming. 2012. N 4. P. 50–63.
14. Ignatenko O.P. Game theoretic modeling of AIMD network equilibrium. Problems of Programming. 2016. N 1. P. 115–127.
15. Ignatenko O.P. Control models of data flows in Internet under instability. Problems of Programming. 2011. N 3. P. 38–51.
16. Ignatenko O.P., and Molchanov O.A. Evolutionary games in TCP networks with speed restriction policies. Problems of Programming. 2016. N 4. P. 33–47.
17. Ignatenko O. and Synetskyi O. Evolutionary Game of N Competing AIMD Connections. Information and Communication Technologies in Education, Research, and Industrial Applications, Springer International Publishing. 2014. P. 325–342.
18. Carbunar, Bogdan, et al. "A survey of privacy vulnerabilities and defenses in geosocial networks." IEEE Communications Magazine 51.11. 2013. P. 114–119.

19. Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava. "Security in internet of things: Challenges, solutions and future directions." System Sciences (HICSS), 2016 49th Hawaii International Conference on. IEEE, 2016.
20. Johnson, Benjamin, et al. "Game-theoretic analysis of DDoS attacks against Bitcoin mining pools." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014.
21. Lewenberg, Yoad, et al. "Bitcoin mining pools: A cooperative game theoretic analysis." Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems. International Foundation for Autonomous Agents and Multiagent Systems, 2015.

Одержано 03.08.2017

Про автора:

Ігнатенко Олексій Петрович,
кандидат фізико-математичних наук,
старший науковий співробітник,
Кількість наукових публікацій в українських виданнях – понад 25.
Кількість наукових публікацій в зарубіжних виданнях – 8.
http://orcid.org/0000-0001-8692-2062.

Місце роботи автора:

Інститут програмних систем
НАН України,
03187, Київ-187,
проспект Академіка Глушкова, 40.
Тел.: 526 6025.
E-mail: o.ignatenko@gmail.com