КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.20.124141
УДК 004.946.5.056

Лахно Валерій Анатолійович
доктор технічних наук, професор, професор кафедри комп'ютерних систем та мереж
Національний університет біоресурсів і природокористування України, м.Київ, Україна
ORCID ID: 0000-0001-9695-4543
lva964@gmail.com

Малюков Володимир Павлович
доктор фізико-математичних наук., доцент, професор кафедри комп'ютерних систем і мереж
Національний університет біоресурсів і природокористування України,
Україна, м. Київ, вул. Героїв Оборони, 15.
ORCID: 0000-0002-7533-1555
imalyukova82@gmail.com

Малюкова Інна Володимирівна
Провідний аналітик
Рейтингове агентство "Експерт-Рейтинг",
Україна, м. Київ, вул. Героїв Оборони, 15.
imalyukova82@gmail.com
ORCID: 0000-0002-7207-539X
imalyukova82@gmail.com

Оган Аткелди
аспірант кафедри комп'ютерних систем
Казахський національний дослідницький технічний університет імені К. І. Сатпаєва, м.Алмати, Казахстан
ORCID ID: 0000-0002-0968-562X
a.ogaan@satbayev.university

Криворучко Олена Володимирівна
доктор технічних наук, професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0002-7661-9227
kryvoruchko_ev@knute.edu.ua

Десятко Альона Миколаївна
PhD in Computer Sciences, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0003-2860-2188
desyatko@knute.edu.ua

Катерина Володимирівна Степашкіна
Асистент
Державний торговельно-економічний університет
02156, вул. Кіото, 19, м. Київ, Україна
ORCID: 0000-0001-7874-450X
k.stepashkina@knute.edu.ua

МОДЕЛЬ АНАЛІЗУ СТРАТЕГІЙ ПРИ ДИНАМІЧНІЙ ВЗАЄМОДІЇ УЧАСНИКІВ ФІШИНГОВИХ АТАК

Анотація. У роботі запропоновано підхід, що дозволяє здійснювати протидію атакам на криптовалютні біржі та їх клієнтів. Даний підхід формалізований у вигляді синтезу динамічної моделі протистояння фішинговим атакам та моделі персептрона у вигляді найпростішої штучної нейронної мережі. Динаміка протистояння визначається системою

диференціальних рівнянь, що визначає зміну станів жертви фішингових атак та зловмисника, який організовує такі атаки. Це дозволяє знайти оптимальні стратегії протистояння сторін у рамках схеми білінійної диференціальної гри з повною інформацією. Рішення гри дозволяє визначити платіжні матриці, що є елементами навчального набору для штучних нейронних мереж. Синтез таких моделей дасть можливість із достатнім ступенем точності знаходити стратегію протистояння фішингу. Це дозволить мінімізувати втрати жертви фішингових атак та сторони захисту, яка забезпечує безпечну систему спілкування із клієнтами криптовалютної біржі. Запропонований нейро-ігровий підхід дозволяє ефективно здійснювати прогноз процесу протистояння фішингу у контексті витрат для сторін, що використовують різні стратегії.

Ключові слова: інформаційна безпека, фішинг, криптовалюта, ігрова модель, штучна нейронна мережа.

ВСТУП

Фішингова атака – мабуть один із найпростіших і найменш витратних для атакуючої сторони способів отримати інформацію про користувачів. Оскільки атаки фішинга фактично не вимагають високої кваліфікації хакерів і не пов'язані з витратами на проведення, вони користуються великою популярністю, як серед професійних хакерів, так і серед різного роду комп'ютерних шахраїв. Популярність даного способу отримати інформацію про користувача породжує велику кількість тактичних прийомів проведення фішингової атаки. Можна говорити, що на найпростішому рівні зловмисники вдаються до простої розсилки листів, які містять, наприклад, посилання на шкідливий сайт або вкладений файл. За більш витонченої тактики це може бути фішинг, доповнений елементами соціальної інженерії. Так, наприклад, у 2019 році зафіксували подібну фішингову атаку у Венесуелі [1]. Було створено веб-сайт, на якому волонтери зареєструвалися для участі у гуманітарній акції. Для реєстрації необхідно було вказати особисті дані, документ, що підтверджує особу, номер мобільного телефону та ін. Зловмисникам вдалося фактично створити ідентичний сайт. Причому з дуже схожим доменом. В результаті було фактично викрадено особисту інформацію тисяч волонтерів [2].

Фішинг є серйозною загрозою для пересічних користувачів. Наприклад, у міру зростання популярності криптовалют (КВ) і, відповідно, різних криптовалютних бірж (КВБ), багато користувачів почали активно освоювати цей напрямок, сподіваючись швидко заробити. А оскільки часто багато користувачів, не маючи елементарних знань в галузі інформаційної безпеки (ІБ), намагаються отримати швидкий прибуток, то такі власники криптогаманців знаходяться в перших рядах потенційних жертв фішингових атак, оскільки вони швидше за все не помітять або проігнорують ті хитрощі, які використовують зловмисники при крадіжці особистих даних. Так, у 2019 році в пресі було багато повідомлень про використання фішингу для розкрадання коштів одного з криптогаманців на КВБ Binance [3]. КВБ заявило, що зловмисники викрали 7 тис. біткойнів. А це на 2019 рік приблизно 2% всіх біткойнових активів Binance. Щоб викрасти ці засоби, хакери використовували фішинг і вірусні атаки за допомогою яких були отримані важливі дані даних багатьох клієнтів, у тому числі коди двофакторної ідентифікації. Як зазначено в [3] "Хакерам вистачило терпіння дочекатися сприятливого моменту і здійснити добре сплановану операцію через множину рахунків, які, на перший погляд, здавалися абсолютно незалежними".

Постановка проблеми.

Небезпека фішингових атак, що не втрачає актуальності, мотивує дослідників в області ІБ шукати нові методи й технології для протидії фішингу. Зокрема, такі технології можуть бути засновані на застосуванні штучних нейронних мереж (ШНМ), які здатні з високим ступенем ефективності відсіювати листи фішингу або виявляти фішингові сайти. Виникає потреба в визначені підходу формалізованого у вигляді синтезу динамічної моделі протистояння фішинговим атакам та моделі персептрона у вигляді найпростішої штучної нейронної мережі.

Аналіз останніх досліджень і публікацій. Автори робіт [4], [5] розглянули традиційні методи протидії фішингових атак. На думку авторів, ефективним методом протидії можуть стати унікальність дизайну сайту, застосування одноразових паролів, одностороння автентифікація та ін. З цим важко посперечатися, однак зауважимо, що кожен з цих методів призводить до збільшення вартості розробки та підтримки сайту для власника. І навіть така політика не завжди призводить до успіху. Так, наприклад, 2021 року було виявлено підроблений сайт одного з найбільших банків України [6]. Шахраї заманювали клієнтів у нереальні проєкти, пропонуючи високий дохід за схемою, якій притаманні властивості фінансової піраміди із застосуванням методів соціальної інженерії та можливого хакерства.

Аналогічна схема з підробленим сайтом криптовалютної біржі (КВБ) описана в дослідженні [7]. Автори публікації описують ситуацію, коли у 2017 році в Південній Кореї було викрито одну з найвідоміших фальшивих бірж КВБ. Фейкова КВБ мала назву BitKRX. Це було зроблено, щоб назва асоціювалася у клієнтів із найбільшою Південнокорейською фінансовою торговою платформою – Korea Exchange (KRX). У результаті, клієнти, які вважали, що купили біткоїн (BTC), і намагалися отримати доступом до своїх коштів, виявляли, що й гроші просто зникли [8].

У [9], [10] авторами розглядаються як класичні, так і нові методи захисту від фішингових атак. Наприклад, як стверджують дослідники, у ряді випадків досить просто підвищити рівень інформаційної культури клієнтів фінансових установ, щоб уникнути наслідків фішингу. Найпросунутіші технологічні рішення передбачають впровадження шлюзових рішень для боротьби з фішинговими атаками або технологій машинного навчання, наприклад, ШНМ, для розпізнавання фішингових сайтів.

У [11], [12], [13], [14], [15], [16] показано, що виявляти фішингові вебсайт можна за допомогою ШНМ. Зрозуміло, це далеко не повний список наукових праць, присвячених дослідженню ефективності та доцільності залучення апарату ШНМ для боротьби з фішинговими сайтами та розсилкою фішингу. Зокрема, у цих роботах показано, що ШНМ можна використовувати для виявлення та запобігання фішингових атак завдяки їхній сильній здатності активного навчання за масивними наборами даних та високою точністю класифікації даних. Однак точки, що повторюються в загальнодоступних наборах даних, а також деякі функції у векторах ознак, ускладнюють навчання ШНМ. Також, ми звернули увагу, що більшість авторів, які пропонують ті чи інші ШНМ, практично не торкаються питання витратності створення такої мережі її навчання та перенавчання при зміні тактики фішингу атакувальною стороною.

Тим часом взаємини зловмисника, тобто фішера та його потенційної жертви, можна описати як взаємодію гравців [17].

Зловмисник (фішер), використовуючи техніку фішингових атак, (часто таргетованих) намагається проникнути в кіберсистеми, наприклад, КВБ для отримання конфіденційної інформації. Це можна зробити, наприклад, через взаємодію зі співробітниками КВБ або її клієнтами. Тобто є дві сторони – атакуючий та жертва.

Апарат теорії ігор можна використати по-різному. У [17], [18] автори пропонують підходи, відповідно до яких теорія ігор дає можливість отримати знання про взаємодію між фішером і жертвою, щоб передбачити наступні дії фішера відповідно до інформації з минулих взаємодій та рекомендувати дії на стороні жертви. Дані роботи описують гру таким чином, щоб можна було передбачити майбутні наміри фішера відповідно до минулих дій обох гравців. Наприклад, автори розглядають такі ітерації стратегій сторін:

1) фішер: використання підробленого вкладення (або посилання); жертва: використання антивірусу;

2) фішер: маскування вмісту електронної пошти; жертва: навчання боротьби з фішингом.

Зрозуміло, це не повний перелік можливих стратегій сторін. Ну, вже з такого простого набору, з погляду затратності, виникають додаткові питання. Наприклад, який антивірус кращий для сторони жертви? Чи достатньо обмежиться базовим набором захисних функцій антивірусу, скажімо, що надається багатьма безплатними антивірусами, чи краще витратитися на більш просунуті платні версії, які надають захист і від фішингу? Або як організувати навчання клієнтів? Скажімо, КВБ випускає розгорнуту інструкцію або організовує онлайн тренінг, залучаючи спеціалістів з ІБ (а вони, швидше за все, вимагатимуть оплату за свої послуги).

Аналогічно можна побудувати й інші пари стратегій дій сторони фішера та жертви чи захисту. Так в [19], [20] автори показують, що для захисту від фішингових атак можна використовувати як вбудовані інструменти в браузерах і на поштових серверах, так і накладені кошти, що надаються сторонніми вендорами. Наскільки ефективними є такі рішення в порівнянні з навчанням користувачів і чи потрібно купувати додаткову систему для боротьби з фішингом, автори не розглядають.

У [21], [22] автори, використовуючи теорію ігор наголошують на розрахунок рівноваги Неша у змішаних стратегіях для гри нападаючий-захисник і представляють раціональну схему отримання переваги, що атакує перед захисником. У розглянутих роботах запропоновано некооперативну модель цільового фішингу з нульовою сумою. Це дозволяє зловмиснику (наприклад, фішеру) вибирати оптимальну стратегію для максимізації виграшу. Однак автори зовсім не торкалися аспекту проблеми вибору, вибору того чи іншого варіанта стратегії захисту та нападу в контексті його впливу на витрати сторін гри.

Власне, все вищесказане і зумовило наш інтерес до цієї теми. Як відомо, синтез різних методів і моделей, використання інструментарію з різних галузей науки, часто призводить до добрих результатів. Це стосується й колаборації апарату теорії ігор та нейронних мереж. Таке поєднання може бути дуже цікавим при вирішенні завдань, пов'язаних із прогнозуванням результату протистояння сторін при оцінці впливу їх витрат на захист та її подолання, зокрема для випадку фішингової атаки на КВБ.

Концептуально взаємодія цих двох фундаментальних розділів математики, яка базується на припущенні, що окремі нейрони, наприклад, в ШНМ, будуть оптимально поводитися при активації їх відповідно до заданої матриці виграшу. Така матриця виграшу може бути сформована, наприклад, при вирішенні звичайної матричної гри або при вирішенні білінійної диференціальної або багатокрокової гри якості з кількома термінальними поверхнями. Таким чином, природно припустити, що теорія ігор може виступати в якості базового організуючого принципу для формування такої ШНМ. Інакше кажучи, теорія ігор дає можливість згенерувати у нашому випадку платіжну матрицю з допомогою рішення білінійної диференціальної гри якості з кількома термінальними поверхнями [23-29]. Це означає, що теорія ігор виступає як керівний

принцип при організації та комунікації нейронів в ШНМ, що застосовується для боротьби з фішингом у контексті витратності різних стратегій жертви або/і сторони захисту, наприклад, адміністратора інформаційної безпеки КВБ.

Також раціональна (оптимальна) стратегія гравця (жертви чи захисника) може використовуватись при виборі оптимальних параметрів навчання (згортки) ШНМ. Наведену в цій статті ігрову модель для захисту КВБ від фішингових атак можна розглядати як етап при побудові ШНМ. Досвід успішних реалізацій ШНМ у завданнях протидії фішишгу дає нам підставу з упевненістю стверджувати, що ШНМ через свої переваги в порівнянні з іншими підходами дозволить ефективно виявляти приховані статистичні та інші залежності фішингових атак, а також отримувати неочевидні та нетривіальні результати. На наш погляд, таке об'єднання двох фундаментальних теорій – ігор та нейромереж дає можливість ефективного розв'язання проблеми боротьби з фішингом за допомогою розробки інтелектуальних інформаційних систем для підтримки прийняття рішень у різних прикладних задачах, боротьби з фішингом КВБ.

Мета та завдання дослідження. Розвиток нейро-ігрового підходу для аналізу оптимальних стратегій при динамічній взаємодії учасників фішингових атак та вибору варіанта, що забезпечує мінімізацію витрат на захист.

Для досягнення мети дослідження необхідно вирішити такі завдання:

1. Розробити на основі моделі для вирішення диференціальної гри якісний підхід з декількома термінальними поверхнями, що дозволяє сформувати платіжні матриці, які є частиною навчального набору для штучних нейронних мереж (ІНП);
2. Провести тестування моделі та початкове навчання найпростішої ШНМ.

МАТЕРІАЛИ ТА МЕТОДИ

Як зазначалося вище, для отримання ефективного результату при боротьбі з фішингом використовується синтез двох підходів – ігрового та нейромереж. Ігровий підхід служить в цьому випадку базою на формування частини навчального набору для ШНМ. Як основна частина навчального набору можуть бути використані дані Alexa, DMOZ для справжніх сайтів та PhishTank, OpenPhish для фішингових [24]. У цій роботі ми розглядаємо переважно ігрову модель, яка описує взаємодію фішера та його потенційної жертви. Така ігрова модель є білінійною диференціальною грою якості з кількома термінальними поверхнями. Наведемо постановку ігрової моделі.

Ситуація, коли під час проведення торгових сесій на КВБ фішер намагається завдати шкоди (насамперед фінансової) учасникам (учаснику) є, на жаль, вже стандартною. Природною реакцією на це є створення інструментів протистояння. Пропонована модель є спробою збільшити арсенал таких інструментів протидії фішингу. При цьому аналізуються витрати з боку жертви (і/або захисту) ті чи інші технічні засоби та методи протидії фішингу. У моделі описується взаємодія учасника торгів (потенційної жертви) та фішера, яка є процедурою безперервною за часом. Зловмисник намагається завдати збитків за допомогою фішингових атак. Надалі називатимемо їх першим і другим гравцями відповідно.

Взаємодія відбувається в такий спосіб. Перший гравець має M технологічні стратегії для протидії атакам другого гравця. Це, наприклад, часткове ігнорування помилкової інформації, її уникнення, ігнорування листів, SMS та інших. Для заподіяння шкоди першому гравцю другий гравець має N технологічні стратегії, це, наприклад, соціальна інженерія, використання кейлогерів, стилерів паролів електронної пошти та

інших. Застосування другим гравцем його технологічних стратегій призводить до фінансових збитків.

Зауважимо, що, наприклад, вбудовані засоби інформаційної безпеки поштових сервісів та браузерів надають лише базовий рівень захисту від фішингу. Кваліфіковані зловмисники здатні обійти такі засоби, оскільки мають можливості протестувати відповідні механізми ще до початку атак. Накладені кошти реалізують складніші алгоритми. І хоча ці алгоритми також можуть бути вивчені кіберзлочинцями, проте це суттєво підвищити вартість атак. Тобто збільшить для другого гравця необхідність мати у своєму розпорядженні відповідні ФР. І дійсно, фішеру доведеться придбати відповідні рішення для перевірки та тестування. Не всі фішери готові піти на такий крок.

Відповідно, більші кошти утворюють "вікно безпеки", що забезпечує ефективний захист. Позначимо через φ_i – величину фінансових збитків, які другий гравець завдає першому гравцю застосуванням своєї i – їй технологічної стратегії; через перший φ_j – величину фінансового доходу, який гравець отримає при застосуванні ним його j – їй технологічної стратегії; через γ_{ij}^1 – відношення φ_i / φ_j, а через γ_{ij}^2 – відношення φ_j / φ_i.

Якщо $\varphi_i = 0$ при деякому i або $\varphi_j = 0$ при деякому j, то їх виключаємо із розгляду. У момент часу t $(t \in [0,\infty))$ перший гравець у рамках операцій на КВБ, маючи фінансовий ресурс (далі ФР) $h_1(t)$, перетворює його до величини $\lambda_1 \cdot h_1(t)$ (λ_1 - темп зростання його ФР). Потім за допомогою вибору своєї стратегії $u(t): 0 \le u(t) \le 1$, він визначає величину своїх інвестицій у технологічні аспекти забезпечення інформаційної безпеки торгових сесій на КВБ - $u(t) \cdot \lambda_1 \cdot h_1(t)$. Вважається, що задана структура інвестування своїх технологічних стратегій. Ця структура задається набором: $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_M : 0 \le \alpha_i \le 1, \sum_{i=1}^{M} \alpha_i = 1$ (M – число технологічних стратегій першого гравця, тобто величину інвестиції можна записати так: $u(t) \cdot \lambda_1 \cdot h_1(t) = \alpha_1 \cdot u(t) \cdot \lambda_1 \cdot h_1(t) + ... + \alpha_M \cdot u(t) \cdot \lambda_1 \cdot h_1(t).$

Величина $\alpha_j \cdot u(t) \cdot g_1 \cdot h_1(t), j = 1,...,M$ компенсує $\sum_{i=1}^{N} s_{ij}^1 \cdot \alpha_j \cdot u(t) \cdot \lambda_1 \cdot h_1(t)$ втрат від дій другого гравця. Це визначає зменшення величини його ФР на цю величину.

Отже, загальна компенсація втрат фішера (другого гравця) від інвестицій першого гравця у захисні механізми від фішингу дорівнює: $\sum_{j=1}^{M} \sum_{i=1}^{N} s_{ij}^1 \cdot \alpha_j \cdot u(t) \cdot \lambda_1 \cdot h_1(t).$ Позначимо через ψ_1 коефіцієнт $\sum_{j=1}^{M} \sum_{i=1}^{N} s_{ij}^1 \cdot \alpha_j$.

У момент часу t $(t \in [0,\infty))$ фішер (другий гравець) має $h_2(t)$ ФР, які він має намір витратити на організацію атак фішингу. Другий гравець, маючи на момент часу t $(t \in [0,\infty))$, $h_2(t)$ ФР, перетворює їх до величини $\lambda_2 \cdot h_2(t)$ ресурсів (тут λ_2 – темп зростання ФР першого гравця). Потім він за допомогою вибору своєї стратегії $v(t): 0 \le v(t) \le 1$, визначає величину $v(t) \cdot \lambda_2 \cdot h_2(t)$. Вважаємо, що задана структура інвестування ним своїх технологічних стратегій, яка задається набором:

ISSN 2663 - 4023

$\beta_1, \beta_2, \beta_3.\beta_4, ...\beta_N : 0 \le \beta_i \le 1, \sum_{i=1}^{N} \beta_i = 1$ (N – кількість технологічних стратегій фішера (другого гравця)). Або можна записати так: $v(t) \cdot \lambda_2 \cdot h_2(t) = \beta_1 \cdot v(t) \cdot \lambda_2 \cdot h_2(t) + ... + \beta_N \cdot v(t) \cdot \lambda_2 \cdot h_2(t)$.

Величина $\beta_i \cdot v(t) \cdot \lambda_2 \cdot h_2(t), i = 1,..., N$ нівелює $\sum_{j=1}^{M} s_{ij}^2 \cdot \beta_i \cdot v(t) \cdot \lambda_2 \cdot h_2(t)$ прибутків від дій першого гравця. Наприклад, якщо той вибрав правильну стратегію боротьби з фішингом і, відповідно, проінвестував вдалі технологічні рішення, що ефективно реалізують захист від фішингу. Це визначає те, що ФР першого гравця зменшиться на цю величину. Тобто загальне нівелювання ФР першого гравця від інвестицій другого гравця дорівнює: $\sum_{j=1}^{N} \sum_{i=1}^{M} s_{ij}^2 \cdot \beta_i \cdot v(t) \cdot \lambda_2 \cdot h_2(t)$. Позначимо через ψ_2 коефіцієнт $\sum_{j=1}^{N} \sum_{i=1}^{M} s_{ij}^2 \cdot \beta_i$. Тоді ФР гравців у момент часу t $(t \in [0, \infty))$ будуть задовольняти наступну систему диференціальних рівнянь:

$$dh_1(t)/dt = -h_1(t) + \lambda_1 \cdot h_1(t) - u(t) \cdot \lambda_1 \cdot h_1(t) - \psi_2 \cdot v(t) \cdot \lambda_2 \cdot h_2(t); \quad (1)$$

$$dh_2(t)/dt = -h_2(t) + \lambda_2 \cdot h_2(t) - v(t) \cdot \lambda_2 \cdot h_2(t) - \psi_1 \cdot u(t) \cdot \lambda_1 \cdot h_1(t); \quad (2)$$

Умовами закінчення взаємодії гравців у момент t $(t \in [0, \infty))$ буде виконання умов (3) або (4):

$$h_1(t) \succ 0, h_2(t) = 0; \quad (3)$$

$$h_1(t) = 0, h_2(r) \succ 0; \quad (4)$$

$$h_1(t) = 0, h_2(t) = 0; \quad (5)$$

Якщо виявиться, що виконується умова (3), то говоритимемо, що у взаємодії гравців у момент часу t $(t \in [0, \infty))$ перший гравець досяг бажаного результату і процедура взаємодії закінчена. Для першого гравця його витрати (інвестиції) на проведення заходів захисту від фішингової атаки виявилися успішними, а обрані стратегії принесуть йому виграш.

Якщо виявиться, що виконується умова (4), то говоритимемо, що у взаємодії гравців у момент часу t $(t \in [0, \infty))$ другий гравець досяг бажаного результату і процедура взаємодії закінчена. Для другого гравця його витрати (інвестиції) на проведення атаки фішингу виявилися успішними, а обрані стратегії принесуть йому виграш.

Якщо виявиться, що виконується умова (5), то говоритимемо, що у взаємодії гравців у момент часу t $(t \in [0, \infty))$ обидва гравці не досягли бажаного результату і процедура взаємодії закінчена.

Якщо не виконуються ні умова (3), ні умова (4), ні умова (5), то процедура взаємодії гравців продовжується далі для моментів часу $\tau : \tau \succ t$.

Позначимо $T^* = [0, \infty)$ множина зміни тимчасової змінної.

Перший гравець на підставі наявної інформації може визначати величину обсягу ФР, які йому необхідно виділити на протидію другому гравцю (фішеру). Розмір витрачається ФР впливає і те, наскільки ефективним буде захист від фішингу. Витрати на створення ефективного фільтра для блокування фішингових сайтів і фішингових листів обійдеться КВБ в рази дорожче, ніж просто пояснення клієнтам небезпеки

ISSN 2663 - 4023

відкриття підозрілих пишемо і т.п. Другий гравець обирає свою стратегію $v(.)$ на основі будь-якої інформації.

Перший гравець прагне знайти множину початкових ФР $h_1(0)$ та початкових станів $h_2(0)$ першого і другого гравців, які мають наступну властивість, описану нами в роботі [25].

Якщо, гра почнеться з них, то перший гравець може вибором своєї стратегії $u_*(.,.,.)$ забезпечити в один із моментів часу виконання умови (3). При цьому стратегія, обрана першим гравцем, сприяє недопущенню фішером (другим гравцем) виконання умов (4), (5) у попередні моменти часу.

Множина таких станів – це множина переваг першого гравця Q_1. Відповідно, стратегії $u_*(.,.,.)$ першого гравця, які мають зазначені властивості, його оптимальні стратегії.

Мета першого гравця – знаходження множини переваги та оптимальних стратегій, застосовуючи які він отримає виконання умови (3).

Сформульована ігрова модель відповідає за класифікацією теорії прийняття розв'язання задачі прийняття рішень із повною інформацією. Крім того, така модель є білінійною диференціальною грою якості з кількома термінальними поверхнями. Знаходження множини переваги першого гравця та його оптимальних стратегій залежить від багатьох параметрів.

Для того, щоб сформувати відповідну частину навчального набору для ШНМ, знайдемо рішення поставленого завдання за допомогою інструментарію теорії диференціальних ігор якості [25]. Ця частина навчального набору формується в результаті вирішення завдання з погляду першого гравця. Тобто знаходиться множина «переваг» Q_1 та оптимальні стратегії $u_*(.,.,.)$ за всіх співвідношеннях параметрів гри. Вирішення завдання з погляду другого гравця аналогічне.

РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Розв'язання задачі залежить від співвідношення параметрів взаємодії. Різні випадки співвідношення параметрів було розглянуто у роботі [25]. Тому обмежимося їх коротким перерахуванням, приведеним у таблиці 1.

Таблиця 1

Випадки співвідношення параметрів гри та залежності для визначення області переваги гравця 1 та його оптимальної фінансової стратегії протистояння фішинговим атакам

Варіанти	Множина "переваг" W_1 та оптимальна стратегія знаходяться за формулами:
Основні варіанти	
1. $\psi_1 \cdot \psi_2 = 1, \lambda_2 \geq \lambda_1$	$Q_1 = \left\{ \begin{array}{l} (h_1(0), h_2(0)) : (h_1, h_2) \in \operatorname{int} R_+^2, \\ \lambda_2 h_2(0) < \psi_1 . \lambda_1 \cdot h_1(0) \end{array} \right\}$

ISSN 2663 - 4023

	$u_*(h_1(0),h_2(0))=\left\{\begin{matrix}1,(h_1(0),h_2(0)):(h_1,h_2)\in \text{int } R_+^2,\\ \lambda_2 h_2(0)<\psi_1\,.\,\lambda_1\cdot h_1(0)\end{matrix}\right\}$ і невизначена в іншому випадку
2. $\psi_1\cdot\psi_2=1,\lambda_2\prec\lambda_1$	$Q_1=\left\{\begin{matrix}(h_1(0),h_2(0)):(h_1,h_2)\in \text{int } R_+^2,\\ \lambda_2 h_2(0)<\psi_1\,.\,\lambda_1\cdot h_1(0)\end{matrix}\right\}$ $u_*(h_1(0),h_2(0))=\left\{\begin{matrix}0,(h_1(0),h_2(0)):(h_1,h_2)\in \text{int } R_+^2,\\ \lambda_2 h_2(0)<\psi_1\,.\,\lambda_1\cdot h_1(0)<\psi_1 h_2(0)\end{matrix}\right\}$ $u_*(h_1(0),h_2(0))=\left\{\begin{matrix}1,(h_1(0),h_2(0)):(h_1,h_2)\in \text{int } R_+^2,\\ \lambda_2 h_2(0)<\psi_1\,.\,\lambda_1\cdot h_1(0)\end{matrix}\right\}$ і невизначена в іншому випадку
3. $\psi_1\cdot\psi_2<1,$ $\psi_1\cdot\lambda_1\cdot\psi_2\le\lambda_2<\lambda_1;$	$Q_1=\left\{\begin{matrix}(h_1(0),h_2(0)):(h_1,h_2)\in \text{int } R_+^2,\\ \psi_2\cdot\lambda_2\cdot h_2(0)<\lambda_1\cdot h_1(0)\end{matrix}\right\}$ $u_*(h_1(0),h_2(0))=\left\{\begin{matrix}0,(h_1(0),h_2(0)):(h_1,h_2)\in \text{int } R_+^2,\\ \psi_1\cdot\lambda_2\cdot\psi_2\cdot h_2(0)<\psi_1\cdot\lambda_1\cdot h_1(0)<\\ <\lambda_1\cdot h_2(0)\end{matrix}\right\}$ $u_*(h_1(0),h_2(0))=\left\{\begin{matrix}1,(h_1(0),h_2(0)):(h_1,h_2)\in \text{int } R_+^2,\\ \psi_1\cdot\lambda_1\cdot h_1(0)\ge\lambda_1\cdot h_2(0)\end{matrix}\right\}$ і невизначена в іншому випадку
4. $\psi_1\cdot\psi_2>1,$ $\lambda_1\le\lambda_2<\psi_1\,.\,\lambda_1\cdot\psi_2$	$Q_1=\left\{\begin{matrix}(h_1(0),h_2(0)):(h_1,h_2)\in \text{int } R_+^2,\\ (\psi_1\cdot\lambda_1\cdot\psi_2\cdot\lambda_2)^{0.5}h_2(0)<\psi_1\,.\,\lambda_1\cdot h_1(0)\end{matrix}\right\}$ $u_*(h_1(0),h_2(0))=\left\{\begin{matrix}1,(h_1(0),h_2(0)):(h_1,h_2)\in \text{int } R_+^2,\\ (\psi_1\cdot\lambda_1\cdot\psi_2\cdot\lambda_2)^{0.5}h_2(0)<\psi_1\,.\,\lambda_1\cdot h_1(0)\end{matrix}\right\}$ і невизначена в іншому випадку
5. $\psi_1\cdot\psi_2>1,$ $\lambda_2<\lambda_1/(\lambda_1\cdot\psi_2);$	$Q_1=\left\{(h_1(0),h_2(0)):(h_1,h_2)\in \text{int } R_+^2,\psi_2\cdot\lambda_2\cdot h_2(0)<\lambda_1\cdot h_1(0)\right\}$ $u_*(h_1(0),h_2(0))=\left\{\begin{matrix}0,(h_1(0),h_2(0)):(h_1,h_2)\in \text{int } R_+^2,\\ \psi_1\cdot\lambda_1\cdot\psi_2\cdot h_2(0)<\psi_1\cdot\lambda_1\cdot h_1(0)<\\ <\psi_2\cdot h_2(0)\end{matrix}\right\}$

	$u_*(h_1(0),h_2(0))=\begin{Bmatrix}1,(h_1(0),h_2(0)):(h_1,h_2)\in \text{int}\, R_+^2,\\ \psi_1\cdot\lambda_1\cdot h_1(0)>\lambda_2\cdot h_2(0)\end{Bmatrix}$ і невизначена в іншому випадку
Допоміжні варіанти	
6. $\psi_1\cdot\psi_2>1,$ $\lambda_2>\psi_1.\lambda_1\cdot\psi_2$	Аналогічно варіанту 1.
7. $\psi_1\cdot\psi_2>1,$ $\lambda_1/(\psi_1\cdot\psi_2)<\lambda_2<\lambda_1$	Аналогічно варіанту 4.
8. $\psi_1\cdot\psi_2<1,$ $\lambda_2\geq\lambda_1;$	Аналогічно варіанту 1.
9. $\psi_1\cdot\psi_2<1,$ $\lambda_2<\psi_1.\lambda_1\cdot\psi_2$	Аналогічно варіанту 3.

Так само вирішується завдання 2 з погляду другого гравця (фішера). Тоді при формуванні частини навчальної вибірки для ШНМ, яка міститиме результати реалізації множини результатів гри, можна буде уявити позитивний ортант у площині $(h_1(0),h_2(0))$ у вигляді трьох множин (конусів з вершиною у точці $(0,0)$. Одна множина (конус), що примикає до осі $0H_1$, є множиною кращим для першого гравця (жертви атаки фішинга). Друга множина (конус) є множиною кращою для другого гравця (фішера). Третя множина (конус) є безліччю множиною нейтральною, з погляду обох гравців. Фактично це множина характеризує властивість збалансованості для гравців, зайнятих протистоянням, зумовленим атаками фішингу. При певних співвідношеннях параметрів протистояння гравців множини збалансованості є промінь збалансованості. Тобто у гравців, для станів, що належать цій множині, існують стратегії, що дозволяють гравцям, як завгодно, довго продовжувати процес протистояння. Це означає, що будуть виконуватись умови $(h_1(0),h_2(0))\in R_+^2$ для будь-якого моменту часу *t*.

Зазначимо, що промені, які є межами конусів, задаються за допомогою коефіцієнтів, що є комбінацією параметрів, які задають динаміку, що описує процес протистояння гравців. Отже, якщо задані початкові величини $(h_1(0),\varphi(0))$ ФР сторін протистояння, можна, наприклад, варіювати цими параметрами. Зокрема, вимагати, щоб параметри, що задають динаміку зміни ФР, були такими, щоб точка $(h_1(0),h_2(0))$ знаходилася в області збалансованості, або, на промені збалансованості, якщо конус, що розділяє дві множини переваги, є променем. Якщо ж, зафіксовані деякі параметри, що визначають динаміку зміни ФР, можна зажадати, щоб значення $(h_1(0),h_2(0))$ і частина нефіксованих параметрів були такі, щоб крапка $(h_1(0),h_2(0))$ потрапила до області збалансованості. Це, своєю чергою, може впливати як на процес протистояння, так і на рекомендації при виборі стратегій гравцями, насамперед це стосується потенційних жертв фішингу, а також сторони захисту. Якщо ж не можна нічого змінити, то наведене вище рішення гри в задачі 1, або рішення гри в задачі 2, вкаже на можливий результат проведення процедури протистояння, в рамках припущень, при яких розглядалися завдання 1 і 2.

Таким чином, рішення розглянутої гри, яка дозволила знайти стратегії двох гравців – потенційної жертви фішингу та фішера, дає можливість сформувати платіжну матрицю, яка є частиною навчальної вибірки для ШНМ. Дана платіжна матриця по

горизонталі має кінцевий набір груп параметрів потенційної жертви фішингу, а вертикалі стоїть кінцевий набір груп параметрів фішера. Кожен гравець може вибрати групу параметрів. Ці групи параметрів (жертви фішингу) служать описи конкретної гри (потенційної ситуації фішингу). Оскільки гра вирішена при всіх співвідношеннях параметрів гри, то на перетині горизонтальної та вертикальної лінії платіжної матриці можна буде поставити одне зі значень (+1, 0, -1). Вирішуючи цю матричну гру і знайшовши значення гри у змішаних стратегіях та оптимальні змішані стратегії, отримаємо, що ситуація з фішингом на КВБ буде або позитивна (при позитивному значенні гри) або негативна (при негативному значенні гри), або нейтральна (при нульовому значенні гри).

Це дає підстави вибору відповідного навчального набору груп параметрів гравців у платіжну матрицю.

Отримані результати гри, як було зазначено вище, можуть використовуватися для формування частини навчальної вибірки ШНМ. І на даному етапі метою навчання ШНМ є визначення її вагових коефіцієнтів.

Запропонована у роботі модель була реалізована у вигляді програмного модуля для аналізу стратегії сторони захисту для протистояння атакам фішингу для КВБ та/або їх клієнтів. Обчислювальний експеримент проведено з використанням пакета MathCad. Обчислювальний експеримент дозволив візуалізувати результати гри між жертвою фішингової атаки та зловмисником (фішером, що реалізує різні тактики фішингових атак). Мета проаналізувати витрати сторін у ході гри та, відповідно, зібрати дані для частини загального масиву навчальної вибірки для ШНМ, яка є частиною більшого проєкту із застосування ШНМ для розпізнавання фішингових адрес та послань, наприклад, адресованих клієнтам КВБ. Результат гри, реалізованої в ході обчислювального експерименту, показаний на рисунку 1.

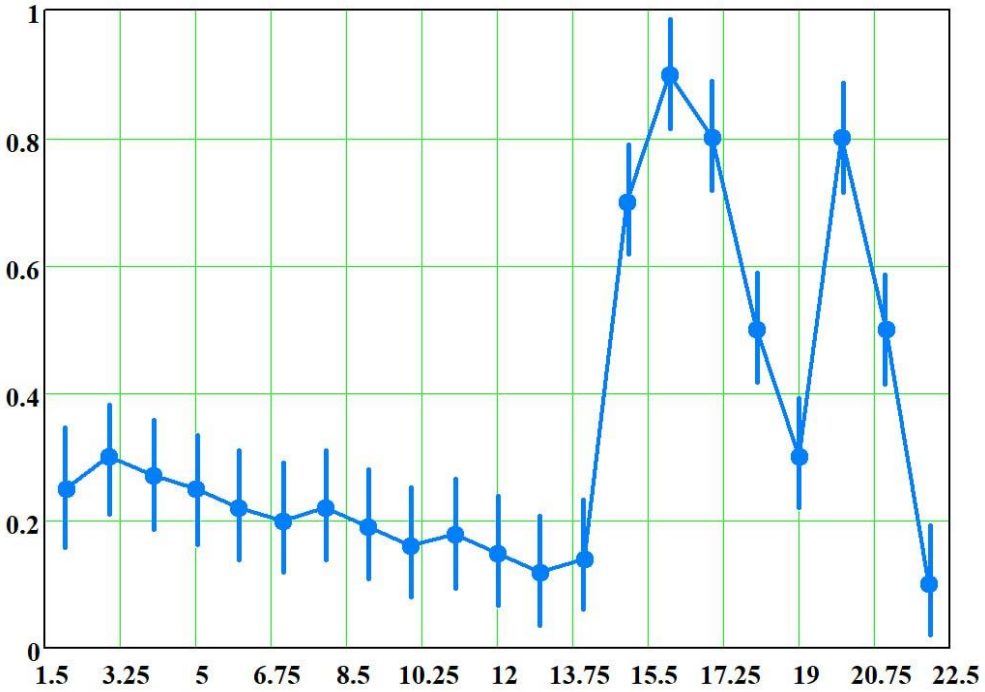

Рис. 1. Результати обчислювального експерименту

ISSN 2663 - 4023

Траєкторія руху гравця другого гравця (зловмисника)

Обчислювальні експерименти, що ґрунтуються на знаходженні рішення білінійної диференціальної гри якості, розглянутої в роботі, дають можливість формувати платіжні матриці, які є необхідними компонентами для функціонування ШНМ. Зазначимо, що для вирішення матричних ігор може використовуватися стандартний пакет лінійного програмування шляхом зведення матричної гри до задачі лінійного програмування. Нижче наведено приклади найпростіших матричних ігор, що генеруються білінійною диференціальною грою якості для ШНМ, див таблицю 2.

Таблиця 2

Приклади матричних ігор, що генеруються білінійною диференціальною грою якості для навчання ШНМ

Номер прикладу	Матриця, що використовується для навчання ШНМ	Пояснення
1	$\begin{pmatrix} 100000 \\ 010000 \\ 001000 \\ 000100 \\ 000010 \\ 000001 \end{pmatrix}$	Значення гри дорівнює 1/6. Оптимальні змішані стратегії – вибір кожної чистої стратегії гравцями з ймовірністю 1/6. Ситуація із фішингом позитивна.
2	$\begin{pmatrix} -100000 \\ 0-10000 \\ 00-1000 \\ 000-100 \\ 0000-10 \\ 00000-1 \end{pmatrix}$	Значення гри дорівнює -1/6. Оптимальні змішані стратегії – вибір кожної чистої стратегії гравцями з ймовірністю 1/6. Ситуація із фішингом негативна.

Навчання ШНМ проводилося за допомогою аналізу локальних наслідків ігор, описаних вище (відповідно, варіанти 1-9, представлені в таблиці 1). В ШНМ у вигляді персептрона (використовувалося середовище MATLAB – пакет прикладних програм Neural Network Toolbox) автоматично подавалася велика кількість (близько 250) зіграних локальних ігор та їх результатів.

В результаті навчання ШНМ було отримано відповідні значення коефіцієнтів зв'язків, а також визначено дисперсію результатів навчання ШНМ. Дисперсія представлена малюнку 2. Таким чином, ми можемо прийняти стандартне відхилення точності моделі на тестовому наборі оцінкою дисперсії прогнозів отриманих результатів результатів ігор, зроблених з допомогою нашої моделі.

Обмеження. Персептрон, розглянутий у роботі, є найпростішою ШНМ. Це відповідає закону еволюції – йти від простого до складного. Надалі, коли статистика матеріалів стане достатньою, буде зроблено перехід, який дозволить створити складнішу ШНМ. На цьому ж етапі дослідження можна було обмежитися найпростішою ШНМ, оскільки пріоритетом було прогнозування протистояння сторін при фішингових загрозах і визначення впливу витрат сторін на захист як жертви фішингу, і її подолання зловмисником.

ISSN 2663 - 4023

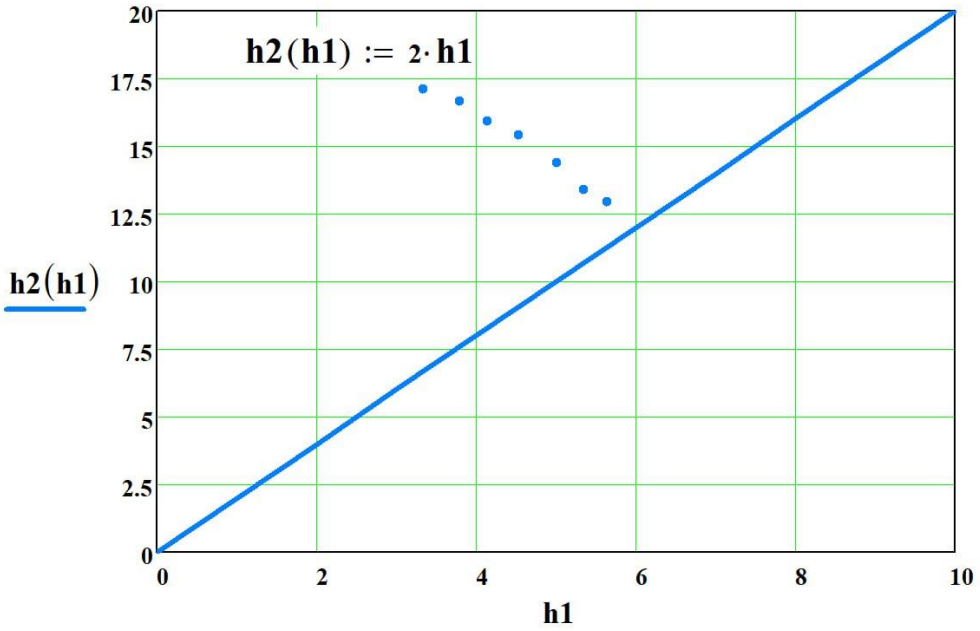

Рис. 2. Дисперсія результатів навчання ШНМ

Рисунок 1 демонструє ситуацію, в якій перший гравець (жертва атаки фішинга), використовуючи неоптимальну поведінку другого гравця (фішера) у початковий момент часу, домагається того, що "приводить" стан системи на "свою" термінальну поверхню. Ця термінальна поверхня характеризує втрату фішером ФР, оскільки витрати на проведення атаки фішинга не дали результату.

Якщо траєкторія гравців збігатиметься з променем збалансованості, то це буде відповідати ситуації рівноваги у протистоянні гравців. В цьому випадку (що, втім, малоймовірно) гравці, застосовуючи свої оптимальні стратегії, "рухаються" по цьому променю. Це "задовольняє" одночасно і "жертву" та/або бік захисту та фішера. Відповідно витрати жертви (і/або сторони захисту) на нівелювання фішингу мінімальні. Наприклад, це може бути висока пильність потенційної жертви, а також ігнорування підозрілих посилань та повідомлень на пошту, SMS та ін. Витрати фішера також мінімальні. Оскільки він, не вдаючись до витратних стратегій фішингу, може просто реалізовувати розсилку фішингу в розрахунку на везіння і випадковість. Складні, і, відповідно, витратні стратегії фішером не застосовуються.

Якщо траєкторія руху перебуватиме під променем збалансованості, це проілюструє ситуацію, коли перший гравець (жертва і/або сторона захисту, наприклад, КВБ) має перевагу у співвідношенні параметрів. Тобто в цьому випадку вони перебувають у багатьох перевагах першого гравця. У цьому випадку перший гравець, застосовуючи свою оптимальну стратегію, досягне своєї мети, а саме приведення стану системи на "свою" термінальну поверхню.

Як показує графік рисунка 2 дисперсія, характеризує розкид результатів експерименту показує, що, починаючи зі значення (кількості кроків, рівну кількості стратегій платіжної матриці) 2 і значення 14 значення дисперсії є "прийнятним", тобто розкид значень невеликий. Крім того, зі значення 21 він також стає "прийнятним". При значеннях від 14 до 21 з'являється зона турбулентності. Це дає підстави визначити величину вибірки (числа стратегій у платіжній матриці), яка дозволить за допомогою,

навченої ШНМ, зробити досить точний прогноз за результатом боротьби з фішингом, а саме, в цьому випадку достатньо обмежитися числом кроків 14.

ВИСНОВКИ

Запропоновано підхід, що дозволяє здійснювати протидію атакам на криптовалютні біржі та їх клієнтів. Даний підхід формалізований у вигляді синтезу динамічної моделі протистояння фішинговим атакам та моделі персептрона у вигляді найпростішої штучної нейронної мережі. Динаміка протистояння задавалася системою диференціальних рівнянь, яка описувала зміну станів жертви фішингових атак та зловмисника, який організує такі атаки. Було знайдено оптимальні стратегії протистояння сторін у межах схеми білінійної диференціальної гри з повною інформацією. Рішення гри дозволило визначити платіжні матриці, що є елементами навчального набору для штучних нейронних мереж. Колаборація таких моделей дозволила з достатньою мірою точності знаходити стратегії протистояння фішингу. Це мінімізувало втрати жертви фішингових атак та сторони захисту, яка забезпечує безпечну систему спілкування з клієнтами криптовалютної біржі.

Запропонований нейро-ігровий підхід дозволяє ефективно здійснювати прогноз процесу протистояння фішингу у контексті витрат для сторін, які використовують різні стратегії.

Наведено результати обчислювального експерименту, в ході якого враховані різні співвідношення параметрів, що описують процес протистояння фішинговим атакам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Rao, R. S., Pais, A. R. (2018). Detection of phishing websites using an efficient feature-based machine learning framework. *Neural Computing and Applications*, *31*(8), 3851–3873. https://doi.org/10.1007/s00521-017-3305-0

2 Gupta, B. B., Arachchilage, N. A. G., Psannis, K. E. (2017). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z

3 Хакери викрали з найбільшої біржі криптовалют понад 40 мільйонів доларів. https://www.epravda.com.ua/rus/news/2019/05/8/647630/

4 Луговець, Д. В., Петренко, А. Б. (2021, December). СТРУКТУРА ВИЯВЛЕННЯ ФІШИНГОВИХ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ. In *The 6th International scientific and practical conference "International scientific innovations in human life"(December 15-17, 2021) Cognum Publishing House, Manchester, United Kingdom. 2021. 998 p.* (p. 201).

5 Opirskyy, I., Vynar, A. (2020). АНАЛІЗ ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ ДЛЯ ФІШИНГОВИХ АТАК. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *1*(9), 59-68.

6 Виявлено фальшивий сайт "ПриватБанку": українців просять бути обережнішими. https://www.unian.ua/economics/finance/viyavleno-falshiviy-sayt-privatbanku-ukrajinciv-prosyat-buti-oberezhnishimi-foto-novini-ukrajina-11489212.html.

7 Fake Cryptocurrency Exchanges. https://www.gemini.com/cryptopedia/cryptocurrency-exchange-fake-website.

8 Sharma, A., Srivastava, A., & Dhingra, D. (2021). Cryptocurrency. У *Industry 4.0 Technologies for Business Excellence* (с. 205–219). CRC Press. https://doi.org/10.1201/9781003140474-12.

9 Laptiev, S. (2022). УДОСКОНАЛЕНИЙ МЕТОД ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ВІД АТАК ЗА ДОПОМОГОЮ АЛГОРИТМІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *4*(16), 45-62.

10 Довганик, С. С. ЗАХИСТ ВІД ФІШИНГОВИХ АТАК ЗА ДОПОМОГОЮ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ. In *Importance of Soft Skills for Life and Scientific Success: Proceedings of the 1st International Scientific and Practical Internet Conference, March 1-2, 2022. FOP Marenichenko VV, Dnipro, Ukraine, 163 p.* (p. 122).

11 Anutthamaa, M. et al. (2011). A framework for predicting phishing websites using neural networks. arXiv preprint arXiv:1109.1074.

12 Mohammad, R. M., Thabtah, F., McCluskey, L. (2014). Predicting phishing websites based on self-structuring neural network. *Neural Computing and Applications, 25*, 443-458.

13 Feng, F. et al. (2018). The application of a novel neural network in the detection of phishing websites. *Journal of Ambient Intelligence and Humanized Computing*, 1-15.

14 Wei, W. et al. (2020). Accurate and fast URL phishing detector: a convolutional neural network approach. *Computer Networks, 178*, 107275.

15 Bahnsen, A. C. et al. (2017, April). Classifying phishing URLs using recurrent neural networks. In *2017 APWG symposium on electronic crime research (eCrime)* (pp. 1-8). IEEE.

16 Ali, W., Ahmed, A. A. (2019). Hybrid intelligent phishing website prediction using deep neural networks with genetic algorithm-based feature selection and weighting. *IET Information Security, 13(6)*, 659-669.

17 Tchakounte, F. et al. (2021). A game theoretical model for anticipating email spear-phishing strategies. *EAI Endorsed Transactions on Scalable Information Systems, 8(30)*.

18 Figueroa, N., L'Huillier, G., Weber, R. (2017). Adversarial classification using signaling games with an application to phishing detection. *Data mining and knowledge discovery, 31*, 92-133.

19 Sharma, P. et al. (2022). Anti-phishing techniquesa review of Cyber Defense Mechanisms. *IJARCCE, 11(7)*, 153-160.

20 Jansen, J., van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies, 123*, 40-55.

21 Bebeshko, B. (2022). ANALYSIS OF DIGITAL CRYPTOCURRENCY MARKET FORECASTING METHODS AND MODELS. *Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique»*, *2*(18), 163–174. https://doi.org/10.28925/2663-4023.2022.18.163174

22 Khan, H., Alam, M., Al-Kuwari, S., Faheem, Y. (2021). OFFENSIVE AI: UNIFICATION OF EMAIL GENERATION THROUGH GPT-2 MODEL WITH A GAME-THEORETIC APPROACH FOR SPEAR-PHISHING ATTACKS. У *Competitive Advantage in the Digital Economy (CADE 2021)*. Institution of Engineering and Technology. https://doi.org/10.1049/icp.2021.2422

23 Lakhno, V. et al. Development of a model for decision support systems to control the process of investing in information technologies, (2020) *Eastern-European Journal of Enterprise Technologies, 1 (3)*, pp. 74-81.

24 Eint Sandi, A., Chaw Thet, Z., Hayato, Ya. (2019). A Survey of URL-based Phishing Detection. *Department of Computer Science and Communication Engineering, Graduate School of Fundamental Science and Engineering, Waseda University*.

25 Malyukov, V. P. (1989). A constructive method of solving a differential game of quality with two terminal surfaces. *Computational Mathematics and Mathematical Physics*, *29*(2), 1-6.

26 Romaniuk, O., Skladannyi, P., Shevchenko, S. (2022). COMPARATIVE ANALYSIS OF SOLUTIONS TO PROVIDE CONTROL AND MANAGEMENT OF PRIVILEGED ACCESS IN THE IT ENVIRONMENT. *Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique»*, *4(16)*, 98–112. https://doi.org/10.28925/2663-4023.2022.16.98112

27 Bebeshko, B., Malyukov, V., Lakhno, M., Skladannyi, P., Sokolov, V., Shevchenko, S., Zhumadilova, M. (2022) Application of game theory, fuzzy logic and neural networks for assessing risks and forecasting rates of digital currency *Journal of Theoretical and Applied Information Technology, 100(24).* http://www.jatit.org/volumes/Vol100No24/15Vol100No24.pdf

28 Kipchuk, F., et al. (2021). Assessing Approaches of IT Infrastructure Audit. In *8th International Conference on Problems of Infocommunications, Science and Technology* (pp. 213–217). https://doi.org/10.1109/picst54195.2021.9772181

29 Brzhevska, Z., Kyrychok R., Anosov A., Skladannyi P., Vorokhob, M. (2021) *Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact*. Cybersecurity Providing in Information and Telecommunication Systems II 2021, *3188*(2), 257-264.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023

Valery Lakhno
Doctor of Technical Sciences, Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0001-9695-4543
lva964@gmail.com

Volodymyr Malyukov
Doctor of Physical and Matematical Sciences, Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0002-7533-1555
imalyukova82@gmail.com

Inna Malyukova
Lead Analyst
Rating agency "Expert-rating",
ORCID: 0000-0002-7207-539X
imalyukova82@gmail.com

Ogan Atkeldi
PhD student of Department of Computer Systems
Kazakh National Research Technical University named after K. I. Satpaev, Almaty, Kazakhstan
ORCID ID: 0000-0002-0968-562X
a.ogaan@satbayev.university

Olena Kryvoruchko
Doctor of Engineering Sciences, Professor, Head of Department of Software Engineering and Cyber Security
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0002-7661-9227
kryvoruchko_ev@knute.edu.ua

Alona Desiatko
PhD in Computer Sciences, Associate Professor of Department of Software Engineering and Cyber Security
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0003-2860-2188
desyatko@knute.edu.ua

Kateryna Stepashkina
Assistant of Department of Software Engineering and Cyber Security
State University of Trade and Economics, Kyiv, Ukraine
ORCID:0000-0001-7874-450X
k.stepashkina@knute.edu.ua

A MODEL OF STRATEGY ANALYSIS DURING THE DYNAMIC INTERACTION OF PHISHING ATTACK PARTICIPANTS

Abstract. The paper proposes an approach that allows countering attacks on cryptocurrency exchanges and their clients. This approach is formalized in the form of a synthesis of a dynamic model of resistance to phishing attacks and a perceptron model in the form of the simplest artificial neural network. The dynamics of the confrontation are determined by a system of differential equations that determines the change in the states of the victim of phishing attacks and the attacker who organizes such attacks. This allows to find optimal strategies for opposing parties within the scheme of a bilinear differential game with complete information. The solution of the game allows you to determine payment matrices, which are elements of the training set for artificial neural networks. The synthesis of such models will make it possible to find a strategy to resist phishing with a sufficient degree of accuracy. This will minimize the losses of the victim of phishing attacks and of the protection side, which provides a secure system of communication with clients of the cryptocurrency exchange. The proposed neuro-game approach makes it possible to effectively forecast the process of countering phishing in the context of costs for parties using different strategies.

Keywords: information security, phishing, cryptocurrency, game model, artificial neural network.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Rao, R. S., Pais, A. R. (2018). Detection of phishing websites using an efficient feature-based machine learning framework. *Neural Computing and Applications*, *31*(8), 3851–3873. https://doi.org/10.1007/s00521-017-3305-0

2 Gupta, B. B., Arachchilage, N. A. G., Psannis, K. E. (2017). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z

3 Khakery vykraly z naibilshoi birzhi kryptovaliut ponad 40 milioniv dolariv. https://www.epravda.com.ua/rus/news/2019/05/8/647630/

4 Luhovets, D. V., Petrenko, A. B. (2021, December). STRUKTURA VYIaVLENNIa FIShYNHOVYKh ATAK SOTsIALNOI INZhENERII. In The 6th International scientific and practical conference "International scientific innovations in human life"(December 15-17, 2021) Cognum Publishing House, Manchester, United Kingdom. 2021. 998 p. (p. 201).

5 Opirskyy, I., Vynar, A. (2020). ANALIZ VYKORYSTANNIa KhMARNYKh SERVISIV DLIa FIShYNHOVYKh ATAK. Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika», 1(9), 59-68.

6 Vyiavleno falshyvyi sait "PryvatBanku": ukraintsiv prosiat buty oberezhnishymy. https://www.unian.ua/economics/finance/viyavleno-falshiviy-sayt-privatbanku-ukrajinciv-prosyat-buti-oberezhnishimi-foto-novini-ukrajina-11489212.html.

7 Fake Cryptocurrency Exchanges. https://www.gemini.com/cryptopedia/cryptocurrency-exchange-fake-website.

8 Sharma, A., Srivastava, A., & Dhingra, D. (2021). Cryptocurrency. У *Industry 4.0 Technologies for Business Excellence* (с. 205–219). CRC Press. https://doi.org/10.1201/9781003140474-12.

9 Laptiev, S. (2022). UDOSKONALENYI METOD ZAKhYSTU PERSONALNYKh DANYKh VID ATAK ZA DOPOMOHOIu ALHORYTMIV SOTsIALNOI INZhENERII. Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika», 4(16), 45-62.

10 Dovhanyk, S. S. ZAKhYST VID FIShYNHOVYKh ATAK ZA DOPOMOHOIu ELEKTRONNOHO TsYFROVOHO PIDPYSU. In Importance of Soft Skills for Life and Scientific Success: Proceedings of the 1st International Scientific and Practical Internet Conference, March 1-2, 2022. FOP Marenichenko VV, Dnipro, Ukraine, 163 p. (p. 122).

11 Anutthamaa, M. et al. (2011). A framework for predicting phishing websites using neural networks. arXiv preprint arXiv:1109.1074.

12 Mohammad, R. M., Thabtah, F., McCluskey, L. (2014). Predicting phishing websites based on self-structuring neural network. *Neural Computing and Applications*, *25*, 443-458.

13 Feng, F. et al. (2018). The application of a novel neural network in the detection of phishing websites. *Journal of Ambient Intelligence and Humanized Computing*, 1-15.

14 Wei, W. et al. (2020). Accurate and fast URL phishing detector: a convolutional neural network approach. *Computer Networks*, *178*, 107275.

15 Bahnsen, A. C. et al. (2017, April). Classifying phishing URLs using recurrent neural networks. In *2017 APWG symposium on electronic crime research (eCrime)* (pp. 1-8). IEEE.

16 Ali, W., Ahmed, A. A. (2019). Hybrid intelligent phishing website prediction using deep neural networks with genetic algorithm-based feature selection and weighting. *IET Information Security*, *13(6)*, 659-669.

17 Tchakounte, F. et al. (2021). A game theoretical model for anticipating email spear-phishing strategies. *EAI Endorsed Transactions on Scalable Information Systems*, *8(30)*.

18 Figueroa, N., L'Huillier, G., Weber, R. (2017). Adversarial classification using signaling games with an application to phishing detection. *Data mining and knowledge discovery*, *31*, 92-133.

19 Sharma, P. et al. (2022). Anti-phishing techniquesa review of Cyber Defense Mechanisms. *IJARCCE*, *11(7)*, 153-160.

20 Jansen, J., van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40-55.

21 Bebeshko, B. (2022). ANALYSIS OF DIGITAL CRYPTOCURRENCY MARKET FORECASTING METHODS AND MODELS. *Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique»*, *2*(18), 163–174. https://doi.org/10.28925/2663-4023.2022.18.163174

22 Khan, H., Alam, M., Al-Kuwari, S., Faheem, Y. (2021). OFFENSIVE AI: UNIFICATION OF EMAIL GENERATION THROUGH GPT-2 MODEL WITH A GAME-THEORETIC APPROACH FOR SPEAR-PHISHING ATTACKS. У *Competitive Advantage in the Digital Economy (CADE 2021)*. Institution of Engineering and Technology. https://doi.org/10.1049/icp.2021.2422

23 Lakhno, V. et al. Development of a model for decision support systems to control the process of investing in information technologies, (2020) *Eastern-European Journal of Enterprise Technologies, 1 (3)*, pp. 74-81.

24 Eint Sandi, A., Chaw Thet, Z., Hayato, Ya. (2019). A Survey of URL-based Phishing Detection. *Department of Computer Science and Communication Engineering, Graduate School of Fundamental Science and Engineering, Waseda University*.

25 Malyukov, V. P. (1989). A constructive method of solving a differential game of quality with two terminal surfaces. *Computational Mathematics and Mathematical Physics*, *29*(2), 1-6.

26 Romaniuk, O., Skladannyi, P., Shevchenko, S. (2022). COMPARATIVE ANALYSIS OF SOLUTIONS TO PROVIDE CONTROL AND MANAGEMENT OF PRIVILEGED ACCESS IN THE IT ENVIRONMENT. *Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique», 4(16),* 98–112. https://doi.org/10.28925/2663-4023.2022.16.98112

27 Bebeshko, B., Malyukov, V., Lakhno, M., Skladannyi, P., Sokolov, V., Shevchenko, S., Zhumadilova, M. (2022) Application of game theory, fuzzy logic and neural networks for assessing risks and forecasting rates of digital currency *Journal of Theoretical and Applied Information Technology, 100(24).* http://www.jatit.org/volumes/Vol100No24/15Vol100No24.pdf

28 Kipchuk, F., et al. (2021). Assessing Approaches of IT Infrastructure Audit. In *8th International Conference on Problems of Infocommunications, Science and Technology* (pp. 213–217). https://doi.org/10.1109/picst54195.2021.9772181

29 Brzhevska, Z., Kyrychok R., Anosov A., Skladannyi P., Vorokhob, M. (2021) *Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact.* Cybersecurity Providing in Information and Telecommunication Systems II 2021, *3188*(2), 257-264.