ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС
Матеріали Міжнародної науково-практичної конференції
2

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

Одеса
2025

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)

За загальною редакцією ***С. В. Ківалова***

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

Відповідальний за випуск ***М. Р. Аракелян***

ISBN 978-617-8430-61-0

СЕКЦІЯ 24. КОГНІТИВНО-ПРАГМАТИЧНІ ДОСЛІДЖЕННЯ ДИСКУРСУ, ТЕОРІЯ ТА ПРАКТИКА ПЕРЕКЛАДУ В АСПЕКТІ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ

думки. Напади на дані медіаорганізацій можуть включати витік конфіденційної інформації, персональних даних користувачів і журналістських джерел.

Важливість ефективної системи захисту полягає в протидії дезінформації та ворожій пропаганді, які можуть маніпулювати свідомістю населення; забезпеченні достовірності та об'єктивності інформації, що формується у ЗМІ; захисті персональних даних та конфіденційної інформації; підвищенні довіри громадськості до національних медіа та гарантуванні свободи слова, але в межах, що не шкодять інтересам держави та суспільства.

Список використаних джерел:

1. Закон України «Про інформацію». Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12

2. Закон України «Про медіа». Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2849-20

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

4. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

5. Кіберзахист медіа в Україні: стан і виклики. *Інститут масової інформації.* URL: https://imi.org.ua

6. General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu

Ключові слова: кібербезпека, безпека даних, захист інформації, система захисту інформації, інформація.

Keywords: cybersecurity, data security, information protection, information protection system, information.

Чепурна Олена Євгенівна

Національний університет «Одеська юридична академія»,

доцент кафедри кібербезпеки, кандидат фізико-математичних наук, доцент

АНАЛІЗ ТЕОРЕТИКО-ІГРОВИХ МЕТОДІВ СУЧАСНОЇ КІБЕРБЕЗПЕКИ

В умовах глобалізації та стрімкого розвитку інформаційних технологій кібербезпека стає критично важливою складовою національної безпеки кожної держави. В особливості це стосується України в контексті військових дій, що тривають на її території, та прагнення до європейської інтеграції. Сучасні методи забезпечення кібербезпеки часто ґрунтуються на застосуванні теоретико-ігрових методів, які дозволяють аналізувати кіберінциденти та моделювати і

прогнозувати виникнення потенційних кіберзагроз, що в свою чергу, є основою розробки оптимальної стратегії захисту.

Одним з основних інструментів для моделювання кіберзагроз є теорія ігор, яка дає змогу оцінювати стратегічні взаємодії між учасниками (наприклад, атакуючими хакерами та оборонцями кіберпростору). Застосування таких моделей дозволяє прогнозувати результати кібероперацій на основі різних стратегій, що обираються кожним учасником. Для розв'язування задач оптимізації безпеки використовуються такі підходи, як гри з нульовою сумою, кооперативні ігри та ігри з неповною інформацією[1].

За даними Урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, в 2024 році було зареєстровано та опрацьовано 4315 кіберінцидентив. Це на 69,8% більше, ніж роком раніше, коли кіберзлочинці атакували український кіберпростір 2541 раз.

Найчастіше зловмисники атакують місцеві органи влади, уряд та урядові організації, сектор безпеки та оборони, енергетичний сектор, комерційні організації, телекомунікації.

За спостереженнями CERT-UA визначається стійка тенденція до зростання кібератак передусім на критично важливу інфраструктуру України. Ворог не полишає спроб дестабілізувати нашу країну і за допомогою кіберзброї. Це свідчить про те, що протистояння в кіберпросторі залишається однією з найгарячіших точок війни[2].

Найпоширенішими типами атак залишаються:

- розповсюдження шкідливого програмного забезпечення
- фішинг
- шкідливе підключення
- компрометація облікових записів або систем

Типи кібератак за секторами :

- Урядові органи та урядові організації: 26% атак
- Місцеві органи влади: 20% атак
- Сектор безпеки та оборони: 13% атак
- Комерційні організації: 9% атак
- Енергетичний сектор: 7% атаки
- Телекомунікації: 6% атака
- Освітні установи:5% атак
- Транспортна галузь:4% атаки
- Фінансовий сектор: 3% атак
- IT-сектор:3% атак
- ЗМІ: 2,5% атак
- Медичні установи: 1,5% атак

Типи атак за методами:

- Розповсюдження шкідливого програмного забезпечення: основний метод атак;

– Фішинг: поширений метод соціальної інженерії;
– Шкідливе підключення: використання вразливостей для несанкціонованого доступу:
– Компрометація облікових записів або систем: захоплення доступу до критичних ресурсів [3].

Однією з ключових задач є оптимізація стратегій захисту від кібератак, де сторони (ті що здійснюють кібератаку і ті, що обороняються) виступають як гравці. Задача полягає в виборі оптимальної стратегії для мінімізації втрат при атаках або запобіганні атакам. Це класичний приклад гри з нульовою сумою, де виграш однієї сторони є рівним програшу іншої. Проте при більш складних атаках, зокрема в умовах використання шкідливого програмного забезпечення, можливе застосування кооперативних ігор, де кілька учасників можуть співпрацювати для оптимізації своїх ресурсів для захисту.

Ще один з напрямків використання теорії ігор це координація дій між різними державними та приватними структурами: Кібербезпека вимагає скоординованих зусиль між урядовими органами, приватними компаніями та міжнародними партнерами. В цьому випадку важливими є кооперативні ігри, де учасники можуть обмінюватися інформацією та ресурсами для зменшення ризику кібератак. Теорія ігор дозволяє оцінити вигоди від співпраці і забезпечити максимальну ефективність у випадках обміну даними та координації відповідних заходів.

Інформаційна війна та кібервійни: у рамках кібервійни часто спостерігаються гри з неповною інформацією, де кожна зі сторін має обмежене розуміння можливих ходів суперника. Теоретико-ігрові моделі дозволяють аналізувати, як учасники можуть змінювати свої стратегії в реальному часі залежно від отриманих даних. Це дозволяє приймати тактичні рішення, які оптимізують ефективність контрзаходів і мінімізують можливі втрати.

З розвитком нових технологій з'являються нові загрози, які вимагають застосування нових ігрових моделей для захисту мереж і пристроїв. Наприклад, у хмарних обчисленнях та IoT пристроях кібербезпека забезпечується за допомогою розподілених ігор, де кожен елемент мережі або пристрій може бути незалежним гравцем, що взаємодіє з іншими для захисту або атаки. Такі моделі дозволяють врахувати ризики, пов'язані з масштабними кібератаками, і оптимізувати стратегії захисту на рівні окремих вузлів.

Ігрові моделі для кібербезпеки дозволяють розробляти стратегії для різних типів кіберзагроз, оцінювати ймовірні наслідки різних варіантів атак та захисту, а також визначати оптимальні стратегії реагування в реальному часі. Наприклад, ігри з нульовою сумою використовуються для простих атак, де є чітка перемога однієї сторони, тоді як кооперативні ігри допомагають у створенні безпечних взаємодій між державними органами та приватними компаніями[4].

Теоретико-ігрові методи мають великий потенціал для розвитку та вдосконалення сучасних підходів до забезпечення кібербезпеки, особливо в

умовах гібридних загроз і кіберконфліктів. Вони дозволяють не лише прогнозувати можливі сценарії атак, але й оптимізувати стратегії реагування на них, що є особливо важливим для України на етапі європейської інтеграції. Адаптація цих методів до національної системи кібербезпеки допоможе не лише ефективно протистояти поточним загрозам, але й забезпечити стійкість до майбутніх кібератак, сприяючи зміцненню національної безпеки в цілому.

Список використаних джерел:

1. Patterson W., Winston-Proctor C. E. Game Theory. Behavioral Cybersecurity. First edition. Boca Raton : CRC Press, 2021., 2020. P. 69–79. URL: https://doi.org/10.1201/9781003052029-9

2. CERT-UA минулого року опрацювала 4315 кіберінцидентів. *Державна служба спеціального зв'язку та захисту інформації України.* URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv

3. Кучма О., Котух Є. Критична інфраструктура та кіберзагрози: досягнення стратегічних цілей державного аудиту щодо кіберзахисту критичної інфраструктури. *Наукові перспективи (Naukovì perspektivi).* 2023. № 10(40). URL: https://doi.org/10.52058/2708-7530-2023-10(40)-161-

4. Metcalf L., Casey W. Game theory. *Cybersecurity and Applied Mathematics*. 2016. P. 95–112. URL: https://doi.org/10.1016/b978-0-12-804452-0.00006-3

Ключові слова: кібербезпека, теорія ігор, оптимізація стратегій захисту кіберпростору.
Keywords: cybersecurity, game theory, optimization of cyberspace protection strategies.

Соколов Артем Вікторович
Національний університет «Одеська юридична академія»,
професор кафедри кібербезпеки, доктор технічних наук, професор

Баландіна Наталія Миколаївна
Національний університет «Одеська юридична академія»,
старший викладач кафедри кібербезпеки

Зігінова Юлія Костянтинівна
Національний університет «Одеська політехніка»,
студентка магістратури

КОНЦЕПТУАЛЬНА ІДЕЯ ЗБІЛЬШЕННЯ БЛОКУ ДЛЯ МЕТОДУ З КОДОВИМ УПРАВЛІННЯМ ТА СЛІПИМ ДЕКОДУВАННЯМ

Наразі серед стеганографічних методів захисту інформації особливо актуальними є методи, що володіють високою обчислювальною ефективністю при збереженні таких характеристик, як стійкість до атак проти вбудованого пові-