1. What is REvil/Sodinokibi Ransomware.LEPIDE. URL : http://surl.li/njaih
2. Cyberdefense report. Japan's National Cybersecurity and Defense Posture URL : http://surl.li/njaiu.
3. Airbus Cybersecurity. URL : https://www.cyber.airbus.com.

УДК 681.5
DOI: 10.31733/15-03-2024/2/297-300

Світлана ЛУЧИК
професор кафедри
протидії кіберзлочинності,
доктор економічних наук, професор

Олександр МОЙКО
курсант спеціальності «Кібербезпека»
Харківського національного
університету внутрішніх справ

МОДЕЛЮВАННЯ КІБЕРАТАК В КІБЕРПРОСТОРІ

Кібератаки – це зловмисні дії в кіберпросторі, що мають на меті порушити функціонування, конфіденційність, цілісність або доступність інформаційних систем, мереж, ресурсів або даних. Кібератаки можуть мати різні мотиви, цілі, методи та наслідки, а також різний рівень складності, масштабу та впливу. Кібератаки можуть бути спрямовані на окремих осіб, організацій, секторів, країн або регіонів.

Протягом останніх років Україна є однією з найбільш атакованих країн у світі в сфері кібербезпеки. З початку війни Україні вдалося відбити понад 5 тис. російських кібератак. За даними Держспецзв'язку, в Україні у 2023 році кількість кібератак зросла, порівняно з 2022 роком, на 15,9% до 2543 інцидентів. За даними урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, 27,8% кібератак було зафіксовано на уряд та урядові організації, 22,1%– на місцеві органи влади, 14,0% – організації у секторі безпеки та оборони, 10,2% – комерційні організації, 7,4% – енергетичний сектор, 6,5% – телеком, 3,0% – освітні установи. 2,6%– транспортну галузь, по 2% – фінансовий сектор та IT-сектор, 1,2% – ЗМІ, менше 1%– медичні установи (рис. 1).

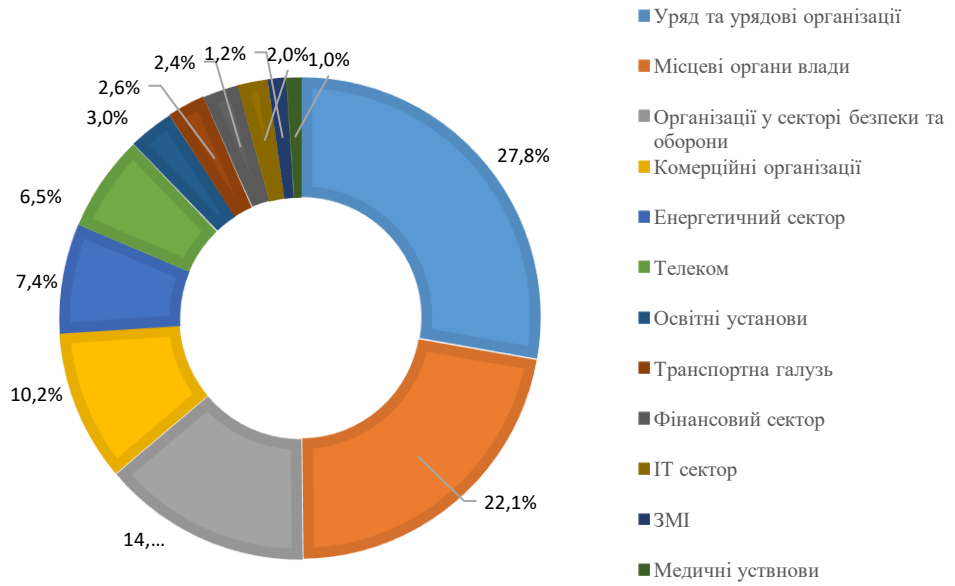

Рис. 1. Кібератаки в Україні, 2023 рік
Джерело: [1]

Лише за другу половину 2023 р. зафіксували та розслідували 1,46 тис кіберінцидентів [1].

З метою запобігти та передбачити нові кібератаки, використовується моделювання кібератак, тобто створення математичних, логічних, або імітаційних моделей, що відображають сценарії, характеристики, параметри та наслідки кібератак.

Моделювання кібератак – це процес створення математичних, логічних, або імітаційних моделей, що відображають сценарії, характеристики, параметри, результати або наслідки кібератак. Моделювання кібератак може мати різні цілі, такі як аналіз та оцінка ризиків, розробка та тестування стратегій захисту, навчання та підвищення кваліфікації фахівців з кібербезпеки, дослідження та розвиток нових технологій для кібератак та кіберзахисту. Моделювання кібератак може використовувати різні підходи, методи та інструменти, залежно від мети, рівня деталізації, типу моделі, методу аналізу, джерела даних тощо. Розглянемо окремі способи моделювання кібератак.

Атакограф – це графічна модель, що показує послідовність дій, які виконує зловмисник для проведення кібератаки на певну мету. Атакограф складається з вузлів та дуг, де вузли представляють стани системи, а дуги – дії зловмисника. Кожен вузол має атрибути, такі як вразливості, умови, залежності, наслідки тощо. Кожна дуга має атрибути, такі як спосіб, метод, засіб, ймовірність, вартість тощо. Атакографи можуть бути використані для аналізу та оцінки ризиків, вразливостей, наслідків та збитків від кібератак. Розробки та тестування стратегій, методів, засобів та механізмів захисту, виявлення, запобігання, реагування та відновлення від кібератак. Навчання та підвищення кваліфікації фахівців з кібербезпеки, а також підвищення обізнаності та готовності користувачів до кібератак.

Диференційно-ігрова модель описує взаємодію між зловмисником та захисником, які вважаються раціональними гравцями, що максимізують свою користь. Диференційно-ігрова модель складається з таких елементів:

– множина гравців (зловмисник, захисник);

– множина стратегій для кожного гравця (атакувати, не атакувати для зловмисника та захищати, не захищати для захисника);

– множина станів системи (нормальний, атакований, відновлений);

– функція переходів, що визначає ймовірність переходу між станами в залежності від стратегій гравців;

– функція виграшу, що визначає користь кожного гравця в кожному стані.

Диференційно-ігрова модель дозволяє аналізувати та оптимізувати поведінку гравців, визначати рівновагу та динаміку у кіберконфліктах, а також розробляти адаптивні та інтелектуальні механізми кіберзахисту. Вона включає множину гравців, стратегій для кожного з них, стани системи, функцію переходів та функцію виграшу. Цей підхід дозволяє аналізувати та оптимізувати стратегії, визначати рівновагу та динаміку в кіберконфліктах, а також розробляти адаптивні та інтелектуальні механізми кіберзахисту [2, с. 57]

Під імітаційною моделлю розуміють комп'ютерну модель, що відтворює динамічні процеси в реальній системі за допомогою алгоритмів, правил, змінних та випадкових подій. Імітаційна модель дозволяє проводити експерименти з різними параметрами, умовами та сценаріями, а також отримувати статистичні дані про результати. Імітаційні моделі кібератак можуть бути використані для моделювання складних та динамічних сценаріїв кібератак, таких як розповсюдження вірусів, атаки на критичну інфраструктуру, атаки на мережі та протоколи, тестування та перевірка ефективності та надійності систем кіберзахисту, таких як антивіруси, системи виявлення вторгнень, системи резервного копіювання та відновлення.

Шаблон потенційно небезпечної кібератаки визначається як модель, що містить у собі повний набір характеристик та параметрів, характерних цій атаці. Шаблон потенційно небезпечної кібератаки складається з нижче представлених елементів.

Ціль атаки, тобто об'єкт, що піддається атаці, наприклад, система, мережа, ресурс або дані.

Спосіб атаки – тип атаки, такий як вірус, троян, черв'як, шпигунське ПЗ, DDoS, SQL-ін'єкція, фішинг, брутфорс тощо.

Метод атаки – техніка атаки: експлойт, бекдор, ботнет, злам пароля, соціальна інженерія тощо.

Засіб атаки, тобто інструмент атаки, такий як програма, скрипт, команда, посилання, файл тощо.

Наслідки атаки – результат атаки, такий як порушення функціонування, конфіденційності, цілісності або доступності цілі, а також збитки, що завдані цілі або зловмиснику.

Ризики атаки, або ймовірність та вартість атаки, а також можливі протидії або санкції.

Шаблони потенційно небезпечних кібератак можуть бути використані для різних цілей, таких як:

створення баз знань про кібератаки, що міститимуть інформацію про їх характеристики, параметри, сигнатури та індикатори;

розробка та налаштування систем кібермоніторингу та кіберрозвідки, що дозволяють виявляти, блокувати та аналізувати кібератаки в реальному часі;

підтримка прийняття рішень з кібербезпеки, що допомагають оцінювати ризики, вибирати стратегії, методи, засоби та механізми захисту, а також планувати реагування та відновлення від кібератак.

Алгоритми символьного моделювання та алгебраїчного зіставлення дозволяють ефективно знаходити вразливість за її алгебраїчним шаблоном на рівні бінарного коду [3]. Алгебраїчний підхід до формалізації вразливостей, зокрема використання абстракцій, дає змогу знаходити прояви невідомих вразливостей, що можуть стати мішенню для шкідливих дій зловмисників. Метод алгебраїчного фазингу (fuzzing), за допомогою якого за попереднім аналізом коду можна виявити критичні вхідні дані, що зламують програму, є одним із методів пошуку так званих «вразливостей нульового дня». Для виявлення зловмисників у мережі або хмарному середовищі алгебраїчний підхід використовується також у комбінації з методами машинного навчання [4]. Модель класифікації, яка попередньо виявляє підозру на поведінку зловмисника на рівні нейронної мережі, може активувати алгебраїчні алгоритми для точного виявлення атаки.

Таким чином, моделювання кібератак дозволяє аналізувати, оцінювати, прогнозувати, запобігати, виявляти, реагувати та відновлюватися від зловмисних дій, а також розробляти ефективні та надійні системи кіберзахисту. Атакографи є найбільш простим і доступним способом моделювання кібератак. Вони можуть бути використані для аналізу і оцінки ризиків, розробки стратегій захисту, навчання фахівців з кібербезпеки та підвищення обізнаності користувачів. Диференційно-ігрові моделі є більш точними і потужними, ніж атакографи, але вони більш складні у використанні. Вони можуть бути використані для аналізу складних кібератак, визначення рівноваги та динаміки в кіберконфліктах, а також розробки адаптивних механізмів кіберзахисту. Імітаційні моделі є найбільш складними і потужними. Вони можуть бути використані для моделювання складних сценаріїв кібератак, перевірки ефективності систем кіберзахисту, а також отримання статистичних даних про результати. Оптимальний спосіб моделювання кібератак залежить від конкретних цілей і завдань, які необхідно вирішити. Якщо потрібне просте і доступне рішення для загального аналізу і оцінки кібератак використовуватимуть атакограф. Для точного аналізу складних кібератак, використовують диференційно-ігрові моделі. Якщо потрібне рішення для моделювання складних і динамічних сценаріїв кібератак використовуються найпотужніші – імітаційні моделі. Ефективність алгебраїчного методу полягає в подоланні проблеми помилкових виявлень (false positive) та покритті більш широкого класу вразливостей.

Вибір способу моделювання кібератак залежить від конкретної задачі, цілі, контексту та ресурсів, що доступні для моделювання. Немає одного універсального способу моделювання кібератак, що підходить для всіх випадків. Однак, комбінування різних способів моделювання кібератак може підвищити якість, повноту та корисність моделей для різних зацікавлених сторін.

У лютому 2024 року компанія Market Research Intellect представила Звіт про дослідження ринку інструментів моделювання кібератак 2023-2031. Ключовими гравцями, що працюють на ринку інструментів моделювання кібератак, сьогодні є Sophos, Cymulate, AttackIQ, BitDam, Core Security, Cronus Cyber Technologies, Elasticito, XM Cyber, Guardicore, Pcysys, Picus Security, SafeBreach, Scythe, foreseeti, Threatcare, Verodin, IronSDN , CyCognito. Розмір ринку інструментів моделювання кібератак класифікується за типом (локальний, хмарний) і додатком (підприємство, уряд) і географічними регіонами (Північна Америка, Європа, Азіатсько-Тихоокеанський регіон, Південна Америка, Близький Схід і Африка) [5].

За результатами звіту ринок інструментів моделювання кібератак, який характеризується швидким і значним зростанням протягом останніх років, продовжить

значне зростання з 2023 по 2031 роки. Прогнозується, що до 2029 року розмір ринку інструментів для моделювання кібератак досягне кількох мільйонів доларів США порівняно з 2022 роком за неочікуваного CAGR (сумарна річна швидкість зростання) протягом 2022-2029 років. Отже, ринок інструментів моделювання кібератак готовий до надзвичайного розвитку.

1. Жарикова А. Кількість кібератак у 2023 році зросла на 16% – Держспецзв'язку. *Економічна правда,* 2024. URL : https://www.epravda.com.ua/news/2024/01/31/709355/ (дата звернення: 26.02.2024).

2. Грищук О.М., Грищук Р.В., Охрімчук В. В. Верифікація узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної кібератаки. Телекомунікаційні та інформаційні технології. 2020. №1(66). С. 53-67. DOI: https://doi.org/10.31673/2412-4338.2020.015367

3. Letychevskyi O. Two-Level Algebraic Method for Detection of Vulnerabilities in Binary Code. In: Proc. of 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (18-21 September, 2019, Metz, France). DOI: https://doi.org/10.1109/IDAACS.2019.8924255

4. Letychevskyi O., Polhul T. Detection of Fraudulent Behavior Using the Combined Algebraic and Machine Learning Approach. In: Proc. of IEEE International Conference on Big Data (9-12 December, 2019, Los Angeles, USA). DOI: https://doi.org/10.1109/BigData47090.2019.9006546

5. Розмір ринку та прогноз глобальних інструментів моделювання кібератак. Market Research Intellect. URL : https://www.marketresearchintellect.com/product/global-cyber-attack-simulation-tools-market-size-and-forecast/?utm_source=Artrocker&utm_medium=019/ (дата звернення: 28.02.2024).

УДК 004.048/383.8:314.114
DOI: 10.31733/15-03-2024/2/300-301

Артур МАРГУЛОВ
професор кафедри міжнародних
відносин та соціально-гуманітарних
дисциплін Дніпропетровського
державного університету
внутрішніх справ,
доктор історичних наук, професор

ШТУЧНИЙ ІНТЕЛЕКТ ТА ДЕМОГРАФІЧНА СИТУАЦІЯ В УКРАЇНІ

Системна депопуляція населення України за часів незалежності з 2022 року набула катастрофічних масштабів. Перебуваючи у форматі повномасштабного військового вторгнення російської федерації, деформацій зазнали усі сфери життя як державницьких інституцій так і суспільного сприйняття населенням ментальних орієнтацій. Моделювання можливих форматів повоєнного розвитку є стратегічно необхідним до системи національної безпеки.

Дуже гостро війна позначилась на демографічних показниках. За підрахунками Інституту демографії та соціальних досліджень імені М.В. Птухи Національної академії наук України, які оприлюднила її директор, Елла Лібанова, на 2033 рік Україна показники чисельності населення України може коливатись від 26 до 35 млн. осіб у кордонах 1991 року.[1] Серед негативних показників є: швидке скорочення населення де коефіцієнт народжуваності неприродно низький а смертності нетипово високий, зростання чисельності людей із інвалідністю, масова вимушена міграція українців за кордон, демографічне старіння населення.

Фактори стабілізації демографічних показників, навіть у повоєнний період, є нестабільними. Припустити швидке повернення усіх українських біженців за кордону або «бєбібум» у повоєнній країні у нас немає підстав. Виникають ще додаткові питання із реінтеграцією деокупованих територій. Демографічний чинник усе більше стає найактуальнішим у концепції національної безпеки. Для стабілізації демографічних показників держава та українське суспільство стоїть перед непростим вибором – вирішувати це питання за рахунок мігрантів. Для українського суспільства, яке лише не так давно стало на шлях реального державного націотворення це є небезпечний виклик. У такому мультикультурному та глобалізованому середовище запрацює процес етнічної