УДК 004.056 https://doi.org/10.30837/IYF.PCEIP.2024.150

АНАЛІЗ МОДЕРНІЗАЦІЇ ОСНОВНИХ ЗАГРОЗ В УМОВАХ КІБЕРВІЙНИ

Пічієнко М. Г.
Науковий керівник – проф. Радівілова Т.А.
Харківський національний університет радіоелектроніки, Харків, Україна
e-mail: mariia.pichiienko@nure.ua, +380961690863

The issue of destructive and devastating cyber-attacks by Russia before the invasion of our country demonstrates that cyber-attacks play an important and strategic role in the modern world and warfare, regardless of public awareness. This threat to us is constant and evolving. Cyber-attacks pose significant challenges to our system and infrastructure with paradoxical consequences. Ukraine's security significantly depends on ensuring cyber security. It is not only worth emphasizing attention to this, but also putting in maximum effort. The thesis provides a brief overview of cyber warfare from its beginning to the present, identifies the main current threats and highlights the trends in cyber threats that are relevant to Ukrainian organisations today.

Поняття російсько-українська кібервійни з’явилося значно раніше початку повномасштабного вторгнення Російської Федерації 24 лютого 2022 року. Вважається, що кібервійна відбувається на фоні військового конфлікту між Україною та Російською Федерацією з 2014 року. Цей конфлікт спричинив значну активізацію кібератак і кібероперацій з обох сторін. Російські хакерські групи, а також групи, які зв'язують з російськими інтересами, були звинувачені у проведенні кібератак на українські урядові, військові та критичні інфраструктурні системи. Серед них ураження вірусом BlackEnergy української електроенергетичної системи у 2015 році і поширення вірусу NotPetya у 2017.

Ще до початку військових дій, росіяни почали синхронізувати атаки в кіберпросторі з інформаційними вкиданнями, фейковими новинами та іншими операціями впливу. Наприклад, масова успішна кібератака на більше 70 веб-ресурсів державних органів влади, що відбулася в січні 2022 року, є лише однією з численних інцидентів, які передували повномасштабному вторгненню. [1]

Інформаційні операції та кібератаки в перші дні вторгнення мали на меті локалізувати та паралізувати опір українців. У першу чергу росіяни націлилися

на системи зв’язку, проте більшість атак були відбиті. Суттєвою втратою став злам супутника компанії Viasat, який надавав українцям швидкісний інтернет.

Основні категорії атак під час гібридної війни можна визначити наступним чином:

1. Кібератаки, направлені на порушення доступності сервісів:
- масове ураження державних та комерційних сайтів;
- шкідливе програмне забезпечення Wiper;
- DDoS-атаки;
- атаки на об'єкти критичної інфраструктури та військову інфраструктуру;
2. Кібершпигунство:
- хакерські атаки з метою викрадення конфіденційних даних;
- шкідливе програмне забезпечення для викрадення інформації;
- захоплення облікових записів;
3. Інформаційна війна:
- ферми ботів, що поширюють фейкові новини та пропаганду;
- фейкові акаунти, що видають себе за публічних осіб чи посадовців;
4. Кіберзлочинність з корисливих мотивів:
- шахрайство на військовій тематиці.

З початку повномасштабного вторгнення залежно від виду атаки, їх кількість збільшилася від 3 до 10-12 разів. Експерти стикнулися з чотирма основними видами подій під час кібервійни порівняно з мирним періодом: кібершпигунство, руйнівні атаки на системи критичної інфраструктури, які часто відбувалися разом з військовими операціями, інформаційна війна – розповсюдження фейків, пропаганда, психологічний тиск, та напади кіберзлочинців як зі сторони міжнародних кримінальних угруповань, так і з боку початківців-хакерів. Більшість фізичних атак на цивільну інфраструктуру супроводжувалася атакою у кіберпросторі. [2]

Наразі вже можна спостерігати зміни в кіберпросторі порівняно з початком війни, коли більшість кібератак спланована російською федерацією і мала чітку мету. З третього кварталу 2022 року кіберконфлікт значною мірою пов'язаний з операціями з боку хактивістів, які пов'язані між собою, хоча й не обов'язково спонсоруються. На ці операції припадає 75% інцидентів, зафіксованих з початку конфлікту, і вони включають хвилі DDoS-атак, здійснених групами, які здебільшого були сформовані після початку конфлікту. Деструктивні кібервійськові операції становлять лише 2% від загальної кількості інцидентів і переважно спрямовані проти українських організацій державного сектору.

Серед поточних трендів кіберзагроз можна виділити наступні.

1. Кількість кіберінцидентів продовжує збільшуватись.
2. Цивільний і правоохоронний сектори, Сили безпеки і оборони України залишаються основними цілями атаки з метою викрадення конфіденційних даних.
3. При виявленні більшості атак з'ясовується, що первинний доступ до систем був отриманний зловмисниками заздалегідь (рік та більше).
4. Тенденція до повторних атак тих об’єктів, що вже були уражені.
5. Атаки через ланцюжок постачання і застосування легітимного ПЗ для зловмисних дій у хакнутій системі.

Російсько-українська кібервійна відображає загальний тренд в сучасних конфліктах, де кіберпростір стає важливим полем боротьби між державами та некерованими суб'єктами. Кібератаки можуть мати серйозні наслідки для економіки, інфраструктури та безпеки країн, тому відповідна кібербезпека стає важливим елементом національної безпеки кожної країни

Список використаних джерел

1. Lessons from Russia’s cyber-war in Ukraine / The Economist, 2022. URL: https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine (дата звернення: 24.02.2022).
2. Про кібербезпеку в Україні. Як бізнес зараз вирішує питання кіберзахисту? // KPMG в Україні. URL: https://kpmg.com/ua/uk/home/media/press-releases/2023/08/pro-kiberbezpeku-v-ukrayini.html (дата звернення: 24.02.2022).
3. Російські кібероперації. Аналітика за перше півріччя 2023 року: звіт Державної служби спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=60201 (дата звернення: 24.02.2022).
4. 2022-2023 : A year of Cyber Conflict in Ukraine: Summary of extensive analysis from the Thales Cyber Threat Intelligence Team. URL: https://bo-cyberthreat.thalesgroup.com/sites/default/files/2023-03/A%20year%20of%20Cyber%20Conflit%20in%20Ukraine_CTI-2023.pdf (дата звернення: 24.02.2022).

004.056.5:004.722 https://doi.org/10.30837/IYF.PCEIP.2024.153

ЗАХИСТ ДАНИХ ЗА ДОПОМОГОЮ БЛОКЧЕЙНУ ТА ШТУЧНОГО ІНТЕЛЕКТУ

Просолов В.В.
д.т.н. проф. Халімов Г.З.
Харківський національний університет радіоелектроніки, Харків, Україна
e-mail: vladyslav.prosolov@nure.ua

In this article, we will analyze SecNet, an architecture that can provide secure data storage, computation, and sharing in a large-scale Internet environment, aiming for a more secure cyberspace with true big data and thus advanced AI with a large number of data sources, through the integration of three key components: blockchain-based data sharing with a guarantee of ownership; a secure computing platform based on artificial intelligence; a trusted value exchange mechanism for purchasing a security service.

У доповіді розглядається можливість захистити дані шляхом поєднання блокчейну та штучного інтелекту, а також дослідити архітектуру захищеної мережі, щоб значно підвищити безпеку обміну даними та всієї мережі [1].

Щоб використовувати штучний інтелект (ШІ) і блокчейн для вирішення проблеми зловживання даними, а також розширити можливості штучного інтелекту за допомогою блокчейну для довіреного керування даними в недовіреному середовищі, пропонуємо SecNet, яка є новою мережевою парадигмою, зосередженою на безпечному зберіганню даних, обмін та обчислення замість спілкування.

SecNet гарантує право власності на дані за допомогою технологій блокчейну та безпечної обчислювальної платформи на основі ШІ, а також механізму стимулювання на основі блокчейну, пропонуючи парадигму та стимули для об’єднання даних і більш потужний ШІ для досягнення кращої безпеки мережі. Крім того, ми обговорюємо типовий сценарій використання SecNet у системі медичного обслуговування та надаємо альтернативні способи використання функції зберігання SecNet. Також, ми оцінюємо його покращення щодо вразливості мережі під час протидії DDoS-атакам і аналізуємо винахідницький аспект щодо заохочення користувачів до спільного використання правил безпеки для більш безпечної мережі.

Дані дуже важливі для їх власника, і різні типи даних можна створювати, змінюючи необроблені дані відповідно до різних вимог і сценаріїв. Наприклад, інформацію про здоров’я користувача, яка зберігається в PDC, можна витягти та реорганізувати, щоб стати структурованими медичними даними, що дуже зручно для покупців із лікарень, науково-дослідних інститутів і розробників програм [2].

Усі дані об’єкта в кіберпросторі зберігаються в PDC, тому їх безпека має велике значення для власника, оскільки дані фактично є цифровим клоном

об’єкта в реальному світі. Для захисту даних SecNet впроваджує компонент ASC в OSS у кожному PDC.

AI є однією з основних можливостей, інтегрованих у PDC. Для різних штучних інтелектів було винайдено різні методи машинного навчання, наприклад, зіставлення шаблонів, комп’ютерний зір і самостійне керування. Наразі досліджуються різні методи ШІ для обробки різних типів даних. Ці специфічні для даних функції штучного інтелекту можна розглядати як великий набір «острівців рішень»: наукові кола та індустрія створили численні ізольовані програмні компоненти та механізми, які мають справу з різними частинами інтелекту окремо. PDC працює як операційна платформа штучного інтелекту, об’єднуючи окремі компоненти штучного інтелекту в узгоджену інтелектуальну систему ширшого характеру. Різні функції штучного інтелекту взаємодіють одна з одною в PDC і діють як інтелектуальна система.

Для захищених обчислень на самому початковому етапі ASC може інтегрувати модуль Generative Adversarial Network (GAN) для генерації більш потужних правил безпеки, що розвиваються, і ввімкнення безпечного та інтелектуального OSS для PDC.

Модуль GAN ASC може вивчати поточні правила безпеки PDC, а потім генерувати зловмисні, але «схожі на законні» запити на доступ до деяких особистих даних, щоб заплутати OSS PDC, щоб змусити OSS втратити здатність класифікувати запит на доступ є незаконним чи ні. Після тривалого раунду генерації та класифікації за допомогою модуля GAN OSS PDC стане набагато розумнішим і потужнішим, а фальшиві запити доступу до даних матимуть мало шансів конкурувати з таким безпечним і інтелектуальним OSS цього PDC.

SecNet забезпечить величезну кількість додатків завдяки вбудованому штучному інтелекту та блокчейну. Одним із типових випадків розгортання та застосування SecNet є довірчий обмін медичними даними між недовіреними різними сторонами для підтримки інтелектуальної та безпечної екосистеми керування медичними даними, яка є ключем до глобальної системи охорони здоров’я.

У майбутній роботі ми дослідимо, як використовувати блокчейн для авторизації доступу до запитів на дані, а також розробимо безпечні та детальні смарт-контракти для обміну даними та обчислювальної служби на основі ШІ в SecNet. Крім того, ми змоделюємо SecNet і проаналізуємо його продуктивність за допомогою масштабних експериментів на основі передових платформ.

Список використаних джерел

1. H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu and J. Xing, "Hyperconnected network: A decentralized trusted computing and networking paradigm", IEEE Netw., vol. 32, pp. 112-117, Jan./Feb. 2018.

2. Y.-A. de Montjoye, E. Shmueli, S. S. Wang and A. S. Pentland, "openPDS: Protecting the privacy of metadata through SafeAnswers", PLoS ONE, vol. 9, no. 7, 2014.