УДК 004.73

РОЛЬ ДЕРЖАВНОГО РЕГУЛЮВАННЯ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Желновач Ілля Олександрович,
Синжерян Андрій Андрійович,
Гельдт Станіслав Володимирович,
Павленко Станіслав Михайлович
курсанти факультету № 4
Харківського національний університет внутрішніх справ
Заводний Олександр Олександрович
студент факультету № 6
Харківського національний університет внутрішніх справ
Онищенко Юрій Миколайович
заступник декана з навчально-методичної роботи факультету № 4
кандидат наук з державного управління, доцент
http://orcid.org/0000-0002-7755-3071

Згідно з даними компанії «SonicWall Capture Labs» тільки за 2022 рік було виявлено близько 493,33 мільйона атак програм-вимагачів на об'єкти критичної інфраструктури.

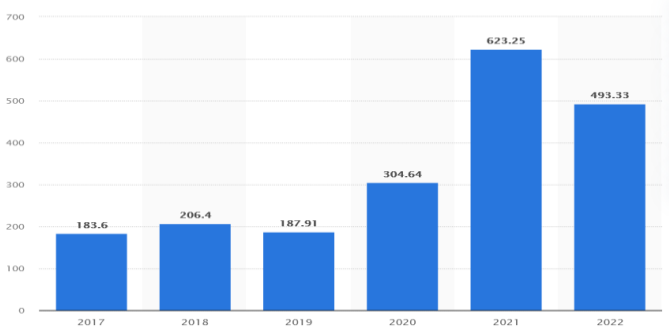

Рис. 1 – Статистика програм-вимагачів за останні 6 років згідно із інфографікою «SonicWall Capture Labs» [1].

Крім того, компанія «IBM» створила глобальний звіт, який включає дані з 17 країн і регіонів і 17 галузей. Середня вартість витоку даних у всьому світі склала 4,35 мільйони доларів США. Виходячи із поданих досліджень,

найпоширенішим типом атак у кіберпросторі став фішинг, за допомогою якого протягом 2022 року було надіслано близько 3,4 мільярда спам-повідомлень [2]. На рисунку 2 наведено графік, в якому витік даних за вартістю стрімко зростає із 2020-го року.

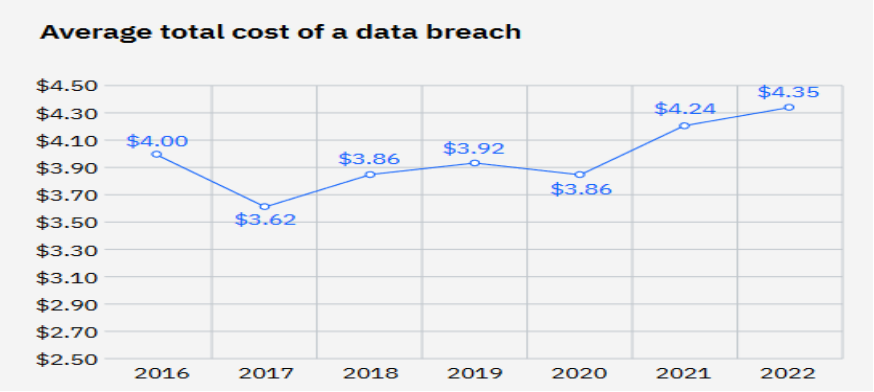

Рис. 2 – Статистика середньої вартості витоку даних по всьому світу [3].

За статистикою, яку наводить Київська школа економіки (“Kyiv School of Economics”, далі – KSE), загальна сума збитків, заподіяних критичній інфраструктурі України внаслідок повномасштабного вторгнення росії, становить 143,8 млрд. доларів США [4]. Окремим важливим аспектом є втрати в галузі цифрової інфраструктури. Як запевняє KSE, загальні прямі втрати телеком-операторів оцінюються у 566 млн. доларів США. У звіті Державного центру кіберзахисту Держспецзв'язку вказано, що атаки, через які відбулися технічні збої, були DNS-Amplification атаками на сервери доменних імен, які забезпечують доступність вебресурсів органів державної влади. Мережева атака була спрямована на порушення сервісів маршрутизації мережевого трафіку, що спричинило тимчасову недоступність резервних маршрутів та відповідних вебресурсів [5].

Отже, метою роботи є дослідження ролі державного регулювання у забезпеченні кібербезпеки об’єктів критичної інфраструктури в Україні, основних причин атак, а також алгоритмів дій державних інституцій для ліквідації наслідків кіберінцидентів.

Розглядаються наступні причини та прояви кібератак на об’єкти критичної інфраструктури в Україні: геополітичний конфлікт України з росією;

шпигунство; екстремізм; хактивізм; кіберзлочинність; військова стратегія.

Геополітичний конфлікт України з росією. Після анексії Криму росією в 2014 році та її повномасштабного вторгнення 24 лютого 2022 року відбулось суттєве збільшення кількості кібератак і спроб впливу на критичну інфраструктуру України.

Шпигунство. Ключем для отримання звітів та інформації про критичну інфраструктуру та критично важливих даних держави, зокрема інформації з обмеженим доступом, до якої належать відомості у економічній, військовій та інших сферах, є шпигунство, що може здійснюється різноманітними методами. Серед них виділяють фізичне втручання та використання методів соціальної інженерії. Фізичний метод базується на проникненні до об'єктів критичної інфраструктури, метою якого є збір критично важливої інформації, встановлення шкідливого програмного забезпечення та приладів спостереження й фіксації. У свою чергу соціальна інженерія полягає у введенні в оману працівників об'єктів через онлайн-листування, телефонну комунікацію тощо, за рахунок чого злочинці отримують важливу інформацію.

Екстремізм. Прихильність крайнім поглядам і, особливо, методам, діям, заходам у політиці, що переростають в тероризм, несуть загрозу населенню, особливо під час війни, з метою створення хаосу і завдання значної шкоди суспільству для донесення своїх переконань, що чинить безпосередній вплив на об'єкти критичної інфраструктури.

Хактивізм. Це явище базується, у контексті агресії росії проти України, на діях кіберзлочинців з метою вираження переконань держави-агресора за допомогою комп'ютерних мереж для формування думки населення України про відсутність безпеки їх конфіденційних даних.

Кіберзлочинність. Це кримінально-протиправна діяльність, що спрямована на заволодіння інформацією з баз даних, перехоплення, знищення інформації за допомогою розповсюдження програм-вірусів, фішингових програм, злому програм, інформаційних систем та їх елементів з корисливих, політичних чи особистих мотивів.

Військова стратегія. Два терміни, які були наведені вище, можна об’єднати в один. В цьому випадку чітко видно, що росія використовує кібератаки як складову військової стратегії, спрямовану на ослаблення економіки та дискредитацію чинного політичного режиму України.

Після розглянутих причин та проявів атак на критичну інфраструктуру України слід розглянути порядок дій державних інституцій країни після виявлення інциденту, серед яких можна виокремити: відгуки на інцидент; аналіз та пошук слідів; відновлення критичної інфраструктури; інформування населення; співпраця з міжнародними партнерами; використання результатів дослідження атаки.

Відгуки на інцидент. Після виявлення та ліквідації наслідків атаки розглядається позиція держави та керівників об’єктів критичної інфраструктури на кіберінцидент. Це включає в себе ізоляцію порушника, остаточну зупинку впливу атаки шляхом увімкнення захисних протоколів, що узгоджується з експертами з кібербезпеки.

Аналіз та пошук слідів. Окрім початку кримінального провадження, державні інституції разом із операторами об’єктів критичної інфраструктури працюють над аналізом типу та мети атаки. Неможливо дати гарантію, що після ізоляції та видалення шкідливого програмного забезпечення з інформаційної системи критичної інфраструктури, вірус знову не почне працювати з нуля.

Відновлення критичної інфраструктури. Після вживання первинних заходів реагування на атаку державні інституції мають надати допомогу власникам/керівникам об’єктів критичної інфраструктури щодо відновлення кібербезпеки об’єктів критичної інфраструктури до рівня функціонування у штатному режимі.

Інформування населення. Суспільство повинно знати, що атака була успішно нейтралізована і особисті дані не були втрачені. Прикладом може бути запис відеозвіту від спікера Держспецзв’язку про успішне відбиття кібератаки або ліквідацію її наслідків.

Співпраця з міжнародними партнерами. Однією з головних задач є

співпраця з іншими країнами та міжнародними організаціями для обміну досвідом по вирішенню повторюваних чи нових типів атак, які відбулися чи потенційно можуть статися, що допоможе Україні ефективно боротися з подібними інцидентами.

Використання результатів дослідження атаки. У майбутньому для швидкої та успішної протидії кібератакам усі результати розслідувань інцидентів повинні бути проаналізовані експертами для подальшого набуття практичних навичок та удосконалення існуючих заходів безпеки [6].

Наразі забезпечення кібербезпеки об’єктів критичної інфраструктури державними установами України відіграє вирішальну роль, особливо під час дії правового режиму воєнного стану. Розглянемо декілька напрямків діяльності, які допоможуть знизити ризики.

Встановлення норм і правил. Забезпечення кібербезпеки включає в себе дотримання вимог стандартів безпеки, що містять норми про захист інформації на об’єктах критичної інфраструктури. Закон України «Про основні засади забезпечення кібербезпеки України» визначає, що об’єктами кібербезпеки та кіберзахисту є, зокрема, об’єкти критичної інформаційної інфраструктури [7].

Взаємодія. Об'єднання зусиль усіх уповноважених державних інституцій, зокрема правоохоронних органів, та приватного сектору в питанні забезпечення кібербезпеки об’єктів критичної інфраструктури збільшить ефективність спільного реагування на кіберінциденти та усунення наслідків від кібератак.

Фінансування. Якщо держава нехтуватиме фінансовою підтримкою заходів із підвищення кібербезпеки критичної інфраструктури, зокрема, розробки та впровадження нових технологій для забезпечення захисту інформації з обмеженим доступом, головними ризиками стануть втрати у галузі критично важливих даних об’єктів критичної інфраструктури.

Отже, фінансування цієї сфери на належному рівні є константою для стійкого фундаменту національної безпеки, особливо в умовах воєнного стану, під час якого головний партнер України, Сполучені Штати Америки, спрямовують на допомогу Україні близько 19% від власного бюджету оборони

у 2023 році [8].

Своєчасне реагування на надзвичайні ситуації. Враховуючи усі вищевказані аспекти, під час будь-якого інциденту своєчасне реагування становитиме виключну роль для мінімізації збитків і відновлення режиму нормального функціонування.

Отже, в останні десятиліття, а особливо з 2014 року, забезпечення кібербезпеки України знаходиться в умовах систематичних потужних кібератак з боку рф.

Держава-терорист здійснює акти агресії, зокрема кібератаки, на українські об’єкти критичної інфраструктури не тільки для створення панічних настроїв серед населення нашої держави, а й для фізичного знищення як найтехнологічніших галузей економіки, так і різноманітних систем життєзабезпечення, зокрема системи енергетики, транспорту тощо.

У відповідь на російську військову агресію виникає потреба зосередитися на швидкому виявленні інцидентів, аналізі, пошуку та документуванні слідів злочинних дій та відновленні об’єктів критичної інфраструктури – поверненні до штатного режиму функціонування.

Важливим та необхідним напрямком діяльності суб’єктів забезпечення кібербезпеки країни є інформування населення (через офіційні джерела інформації) про стан ліквідації наслідків від різних кіберінцидентів, що дозволить знизити рівень паніки серед суспільства та зменшити вірогідність спроб зловмисників розхитувати ситуацію в країні шляхом маніпуляцій з інформацією (розповсюдження неправдивих відомостей, дезінформації).

Нарешті, варто підсумувати, що без належного фінансування та інвестицій навіть найдосконаліше законодавство не зможе забезпечити повноцінний захист від кіберзагроз.

Пріоритетним питанням є налагодження ефективної співпраці суб’єктів забезпечення кібербезпеки об’єктів критичної інфраструктури, зокрема, правоохоронних органів, з представниками приватного сектору та міжнародними партнерами.

СПИСОК ЛІТЕРАТУРИ

1. Annual number of ransomware attempts worldwide from 2017 to 2022. URL: https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/ (дата звернення: 20.02.2024).
2. What’s New in the 2022 Cost of a Data Breach Report. URL: https://securityintelligence.com/posts/whats-new-2022-cost-of-a-data-breach-report/ (дата звернення: 20.02.2024).
3. Cost of a Data Breach Report 2022. URL: https://www.ibm.com/downloads/cas/3R8N1DZJ (дата звернення: 20.02.2024).
4. Загальна сума збитків, заподіяних інфраструктурі України внаслідок повномасштабного вторгнення росії, становить 143,8 млрд доларів. URL: https://www.ukrinform.ua/rubric-economy/3686173-rosia-zavdala-zbitkiv-infrastrukturi-ukraini-na-144-milardi-kse.html (дата звернення: 20.02.2024).
5. Сайти державних органів 6 липня зазнали мережевої атаки – Держспецзв’язку. URL: https://www.radiosvoboda.org/a/news-ataka-merezha-saity/31346083.html (дата звернення: 20.02.2024).
6. The Role of Government in Regulating Data Privacy and Cyber Security. URL: https://amlegals.com/the-role-of-government-in-regulating-data-privacy-and-cyber-security/# (дата звернення: 20.02.2024).
7. Закон України від 05.10.2017 № 2163-VIII «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.02.2024).
8. Сенат США схвалив бюджет на 2023 рік: Україні та союзникам виділять майже $45 млрд. URL: https://fakty.com.ua/ru/svit/20221222-senat-ssha-shvalyv-byudzhet-na-2023-rik-ukrayini-ta-soyuznykam-vydilyat-majzhe-45-mlrd/ (дата звернення: 20.02.2024).