УДК 004.056.52

А. В. Скирда

ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ КІБЕРЗБРОЇ ПРОТИ УКРАЇНИ

Вінницький національний технічний університет

Анотація
Розглянуто питання застосування кіберзброї проти України.
Ключові слова: кіберпростір, кібербезпека, кіберзброя.

Abstract
The issue of using cyber weapons against Ukraine is considered.
Keywords: cyberspace, cybersecurity, cyber weapons.

Вступ

Функціонування сучасного суспільства визначається низкою факторів, які, зокрема, пов'язані з розвитком комп'ютерних та інформаційних технологій. З поглибленням цифровізації суспільства з'явилась якісно нова сфера обміну інформацією – кіберпростір. Світовий досвід показує, що захист кіберпростору (кібербезпека), поряд із боротьбою з таким негативним феноменом, як тероризм, став чи не найголовнішою проблемою людства.

Потужним засобом проведення незаконних дій та боротьби в кіберпросторі стала кіберзброя. Провідні країни світу розглядають кіберзброю як фактор [1], потенційно здатний впливати на перебіг воєнних дій і завдавати збитки економіці, порушувати управлінські функції конкретних держав тощо.

Метою роботи є доказ того, що використання кібернетичних засобів ведення війни є цілком реальним, використання кіберзброї проти України несе невиправні, незворотні руйнівні наслідки.

Результати дослідження

Кібербезпека є одним із пріоритетів у системі національної безпеки України. В Стратегії кібербезпеки України [2] зазначено, що кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій, набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

Вказаний стратегічний документ виділяє серед загроз кібербезпеці України гібридну агресію Російської Федерації проти України у кіберпросторі та факт невпинного нарощування державою-агресором арсеналу кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Кібератаки Російської Федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності.

Аналіз законодавчих та нормативно-правових актів України виявив відсутність тлумачення терміну «кіберзброя». Проблематику визначення сутності та поняття кіберзброї фрагментарно пропонували у своїх дослідженнях українські науковці: Д. Дубов, О. Мережко, В. Бабенко, М. Камчатий, Ю. Разметаєва, А. Войцехівський. Серед закордонних вчених цій темі свої роботи присвячували: Дж. Карр (J. Carr), М. Лібіцкі (M. Libicki), Х. Лін (H. Lin), М. Магомедов, Т. Рід (T. Rid), Е. Філіол (E. Filiol), В. Хайнтшель вон Хайнег (W. Heintschel von Heinegg), Г. Шинкарецька, В. Каберник, М. Шмідт (M. Schmitt), Л. Віхул (Liis Vihul), С. Меле (Stefano Mele) [2]. Як і щодо багатьох сучасних термінів, які виникають у процесі розвитку інформаційних технологій, єдиного уніфікованого визначення наведеного поняття не запропоновано. Проте, спираючись на найбільш поширені визначення, можна виокремити його окремі ознаки.

В. Каберник наводить таке розуміння поняття «кіберзброя»: найрізноманітніші технічні та програмні засоби, найчастіше спрямовані на експлуатацію вразливостей у системах передачі та

обробки інформації або програмо-технічних системах. Він також стверджує, що, спираючись на масштабність впливу, до кіберзброї відносять віруси типу Flame, або зомбі-мережі, які використовуються для розсилки спаму й організації розподілених атак, спрямованих на перевантаження інформаційних систем і похідну з неї відмову в обслуговуванні (так звані DOS та DDOS-атаки) [3].

Звертаючись до англомовних ресурсів, можна знайти й інші значення цього поняття. Так, наприклад, у словнику Макмілана надається досить коротке, проте містке визначення терміну «кіберзброя»: шкідливе програмне забезпечення, що використовується однією країною проти іншої для політичних, військових або розвідувальних цілей.

С. Меле (Stefano Mele) наводить таке визначення кіберзброї: пристрій або будь-який набір комп'ютерних інструкцій, що спрямовані на незаконне пошкодження системи, яка функціонує як критична інфраструктура, її інформацію, дані або програми, що містяться в ній, або є відповідними до них, або навіть призначені для сприяння перериванню (повному або частковому) чи зміні у роботі такої системи [3].

П. Паганіні (Pierluigi Paganini) визначає кіберзброю як певний комп'ютерний код, який використовується або призначений для використання з метою загрози або заподіяння фізичної, функціональної або психічної шкоди структурам, системам або живим істотам [3].

Цікаву думку висловив французький хакер x0rz (відомий своєю участю у висвітленні застосування шкідливого програмного забезпечення Stuxnet в якості кіберзброї, що призвела до пошкодження ядерних центрифуг на іранському заводі в Натанзі). За його словами, «сьогодні все може бути кіберзброєю. Маючи дуже базові навички програмування, ви можете використати документ Word Office в якості кіберзброї, використовучи помилки та незакриті вразливості в існуючому цілком легальному програмному забезпеченні».

Виходячи з наведених визначень та узагальнюючи останні події в сфері кібербезпеки України в 2022 році, можна дійти висновку, що вони пов'язані із масштабним застосуванням кіберзброї проти України (об'єкти критичної інформаційної інфраструктури та державні інформаційні ресурси).

Так, в ніч із 13 на 14 січня 2022 року сталася масштабна «хакерська» атака на низку урядових сайтів України [4]. Було атаковано понад 70 держресурсів, 10 з яких зазнали несанкціонованого втручання. Низка ресурсів, зокрема портал «Дія», були відключені технічними адміністраторами, щоб уникнути ймовірності поширення атаки на ресурси та сервіси. Серед наслідків – назавжди втрачені інформаційні ресурси та примусове відключення окремих сервісів.

12 квітня 2022 року здійснена цільова атака на об'єкт енергетики України [5]. Задум зловмисників передбачав виведення з ладу декількох інфраструктурних елементів об'єкту атаки, а саме:

- високовольтних електричних підстанцій – за допомогою шкідливої програми INDUSTROYER2; причому, кожен виконуваний файл містив статично вказаний набір унікальних параметрів для відповідних підстанцій (дата компіляції файлів: 23.03.2022);
- електронних обчислювальних машин (ЕОМ) під управлінням операційної системи Windows (комп'ютерів користувачів, серверів, а також автоматизованих робочих місць АСУ ТП) – за допомогою шкідливої програми-деструктора CADDYWIPER; при цьому для дешифрування і запуску останнього передбачено використання лоадеру ARGUEPATCH та шелкоду TAILJUMP;
- серверного обладнання під управлінням операційної систем Linux – за допомогою шкідливих скриптів-деструкторів ORCSHRED, SOLOSHRED, AWFULSHRED;
- активного мережевого обладнання.

Централізоване розповсюдження і запуск CADDYWIPER реалізовано за допомогою механізму групових політик (GPO). З метою додавання групової політики, що передбачає завантаження компонентів файлового деструктору з контролеру домену, а також створення запланованого завдання на ЕОМ, використано PowerShell-скрипт POWERGAP. Можливість горизонтального переміщення між сегментами локальної обчислювальної мережі забезпечено шляхом створення ланцюгів SSH-тунелів. Для віддаленого виконання команд використано IMPACKET. Відомо, що організація-жертва зазнала двох хвиль атак. Первинна компрометація відбулася не пізніше лютого 2022 року. Відключення електричних підстанцій та виведення з ладу інфраструктури підприємства було заплановане на вечір п'ятниці, 8 квітня 2022 року.

10 червня 2022 року Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, зафіксоване масове розсилання небезпечних електронних листів із темою "СПИСОК посилань на інтерактивні карти". Розсилання здійснюються, зокрема, серед медійних організацій України (радіостанції, газети, новинні агенції тощо). Встановлено більше 500 електронних адрес отримувачів. Електронні листи містять додаток у вигляді документу "СПИСОК_посилань_на_інтерактивні_карти.docx", відкриття якого може призвести до завантаження

шкідливої програми CrescentImp. Електронні листи надходять здебільшого зі скомпрометованих електронних адрес державних органів.

Найбільш вражаючим фактом використання кіберзброї проти України стала подія, яка мало висвітлюється. Кібератака на службу супутникового інтернету розпочалася 24 лютого 2022 року між 05:00 та 09:00. В ході кібератаки було відключено всі модеми, які зв'язуються із супутником KA-SAT компанії Viasat (в Україні представлена телекомунікаційним провайдером «Датаруп»), та забезпечують доступ до інтернету для клієнтів у Європі, включаючи Україну. За словами фахівців [7, 8], понад два місяці деякі з них, досі не працюють. Кібератака була здійснена із використанням нового шкідливого програмного забезпечення AcidRain, представник компанії Viasat підтвердив його використання [8]. Цей вірус знищує дані з модемів та роутерів і робить їх непрацездатними. Розробників AcidRain не встановлено, але встановлено, що програмний код на 55% збігається з вірусом VPNFilter, розробку якого пов'язують з російськими хакерськими групами Fancy Bear і APT28. AcidRain - це сьомий та потужний вірус-вайпер, використаний в Україні під час війни. Наслідки: фактично знищена система військового супутникового зв’язку ЗСУ. Супутниковий інтернет на території України вдалося відновити тільки завдяки оперативній поставці обладнання супутникового інтернету Starlink компанії Ілона Маска. Також кібератака призвела до «величезних втрат у комунікації»: так було відключено модеми понад 27 тисяч клієнтів у Європі. Виведено з ладу 5800 вітряних турбін німецької енергетичної компанії Enercon. Пошкоджені модеми відновлюються лише в ході «ручного ремонту» в спеціалізованих сервісних центрів компанії Viasat (в Україні відсутні) або заміною на нове обладнання.

Обсяг публікації не дозволяє привести інші факти застосування кіберзброї. Але їх чимало. Кіберінциденти, пов’язані із наслідками кібератак проти державних інформаційні ресурси та об’єктів критичної інформаційної інфраструктури, взагалі не припиняються. Так оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку оприлюднив звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти у першому кварталі 2022 року [9].

Згідно цього звіту за перші три місяці року система зареєструвала 14 млн. підозрілих подій інформаційної безпеки. З них 78 тис. опрацьовано як критичні. За результатами було зареєстровано 40 кіберінцидентів. 65% підозрілих подій виявлені у міністерствах та організаціях, 35% припало на обласні державні адміністрації.

Висновки

Сьогодні людство остаточно увійшло в нову еру, яку вже з упевненістю можна назвати цифровою. Відповідно до сучасного стану розвитку технологій з’являються і нові засоби ведення війни. Серед інших можна виділити також такі, що застосовуються у кіберпросторі. Засобами в даному аспекті є нові види озброєнь, що спираються на використання інформаційних технологій. Такі засоби за своєю природою значно відрізняються від загальноприйнятого розуміння терміну «зброя», проте, незважаючи на це, наслідки їх застосування можна порівняти з найбільш руйнівними з тих, що були раніше, та відомих загальному колу осіб видів озброєнь. Сьогодні народ України відчуває на собі не тільки удари ракет та артилерії, а й не менш руйнівну дію кіберзброї.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стенограма 19-го засідання 69-ої сесії Першого комітету Генеральної Асамблеї ООН від 28.10.2014 року, присвяченому терміновому вирішенню зростаючої перспективи кібервійни. Офіційний сайт ООН. URL: https://www.un.org/press/en/2014/gadis3512.doc.htm

2. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021.

3. М. Камчатний. Заборонені засоби ведення кібервійни. // Підприємництво, господарство і право. 2017. № 9/2017. С. 211-217.

4. Офіційне повідомлення Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 15.01.2022 рокую URL: https://cip.gov.ua/ua/news/derzhspeczv-yazku-z-yasuvala-yak-khakeri-zlamali-saiti-derzhustanov-sho-stalosya

5. Офіційне повідомлення Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA від 12.04.2022 року. URL: https://cert.gov.ua/article/39518

6. Офіційне повідомлення Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA від 12.04.2022 року. URL: https://cert.gov.ua/article/160530

7. Стаття «На початку війни хакери зламали європейську систему супутникового інтернету, наслідки помітні досі» від 27.03.2022 року. URL: https://zn.ua/ukr/TECHNOLOGIES/na-pochatku-vijni-khakeri-zlamali-jevropejsku-sistemu-suputnikovoho-internetu-naslidki-pomitni-dosi.html

8. Стаття «У день вторгнення хакери вивели з ладу супутник, який роздає інтернет у Європі та Україні» від 04.04.2022 року. URL: https://forbes-ua.translate.goog/ru/innovations/u-den-vtorgnennya-khakeri-viveli-z-ladu-suputnik-shcho-rozdae-internet-u-evropi-ta-ukraini-teper-v-atatsi-znayshli-rosiyskiy-slid-04042022-5275?_x_tr_sl=ru&_x_tr_tl=uk&_x_tr_hl=uk&_x_tr_pto=sc
9. Офіційне повідомлення Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 27.05.2022 року. URL: https://cip.gov.ua/ua/news/14-mln-pidozrilikh-podii-informaciinoyi-bezpeki-za-tri-misyaci-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz

Скирда Антон Вячеславович – студент групи УБ-21м факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: skirdaanton1@gmail.com

Науковий керівник: **Шиян Анатолій Антонович** – доцент, доцент кафедри менеджменту та базпеки інформаційних систем, кандидат фізико-математичних наук.

Skyrda Anton Vyacheslavovich - faculty of management and information security, Vinnytsia National Technical University, Vinnytsia.

Scientific adviser: **Shyian Anatolii** - associate professor, associate professor of management and security of information systems, candidate of physical and mathematical sciences