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).