DOI https://doi.org/10.36059/978-966-397-557-3-34

КІБЕРБЕЗПЕКА ТА ПРАВА ЛЮДИНИ: УКРАЇНСЬКИЙ ДОСВІД У ПЕРІОД ВІЙНИ

Романова О. М.
доцент кафедри загальнотеоретичних правових і соціально-гуманітарних дисциплін,
Київський університет права Національної академії наук України
м. Київ, Україна

В останнє десятиліття у світі відбувається активний розвиток інформаційних технологій, а разом з тим зростає злочинність у цій сфері. Кіберзлочини є найдинамічнішою групою суспільно небезпечних діянь, адже з кожним роком кіберзлочини стають дедалі масовішими та небезпечнішими.

На сьогодні правове підґрунтя інформаційної безпеки України створюють: Конституція України [1], Кримінальний кодекс України [2], Закони України "Про основні засади забезпечення кібербезпеки України" [3], "Про інформацію" [4], "Про захист інформації в інформаційно-телекомунікаційних системах" [5], "Про національну безпеку України" [6] та інші закони, Доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність [7] та інші міжнародні договори, згоду на обов'язковість яких надала Верховна Рада України.

Законом України «Про основні засади забезпечення кібербезпеки України» закріплено: кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння в кіберпросторі та/ або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [3, ст.1].

У Кримінальному кодексі України ці злочини закріплено в розд. 16 «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» і представлено такими нормами: ст. 361(1,2), ст. 362, ст. 363, ст. 363 (1). Також до цього переліку потрібно зарахувати ст. 176 (порушення авторського права і суміжних прав) і ст. 190 (шахрайство) [2].

На сьогодні, кіберскладник російсько-української війни перебуває у фокусі особливої уваги урядів, військових та спеціальних відомств, міжнародних організацій, експертних груп тощо. Злочини в мережі відбуваються найрізноманітніші: вимагання з погрозою знищення або

блокування баз даних, інформація про теракти, компромат, розкрадання інтелектуальної власності або майна.

Від початку повномасштабного вторгнення Російської Федерації у лютому 2022 року Україна стала об'єктом масштабної кібернетичної агресії. За даними фахівців із кібербезпеки, з початку війни було зафіксовано понад 3 000 кібератак, спрямованих на органи державної влади, енергетичний сектор, засоби масової інформації, телекомунікаційні компанії та інші критично важливі об'єкти інфраструктури [8]. Такі дії становлять загрозу не лише національному суверенітету, але й порушують право громадян на безпечний інформаційний простір.

Серед перших прикладів кібервійни з боку Російської Федерації можна відзначити атаку на системи зв'язку видання «Kyiv Post» та злам супутникової мережі «KA-SAT», що відбулися буквально за годину до початку вторгнення. Ці дії мали на меті порушити інформаційні та комунікаційні канали України [9]. Також було здійснено атаку з використанням шкідливого ПЗ IssacWiper, спрямовану на урядові вебсайти, а окремі кібератаки на пункти прикордонного контролю мали на меті перешкодити евакуації цивільного населення до сусідніх держав, зокрема до Румунії.

Російські хакерські групи неодноразово здійснювали атаки на цифрову інфраструктуру України, що призводило до блокування доступу до фінансових сервісів, енергетичних ресурсів і телекомунікаційних послуг. Від початку війни фіксуються постійні спроби застосування шкідливого програмного забезпечення проти державних та фінансових установ, а також неурядових, благодійних і гуманітарних організацій, діяльність яких була критично важливою для забезпечення населення медикаментами, продовольством і допомогою під час надзвичайних ситуацій.

Окрім цього, активно здійснювались фішингові кампанії, спрямовані на громадян, держслужбовців і військових, а також атаки на операторів зв'язку, що періодично призводили до порушення роботи українських мереж.

Показовим прикладом високотехнологічної кібератаки стало виявлення шкідливого програмного забезпечення CaddyWiper у комп'ютерних системах державних органів і фінансових структур України [10]. Цей вірус належить до класу «wiper», тобто його призначення полягає у знищенні даних на уражених пристроях, що потенційно може паралізувати роботу критичних державних інформаційних ресурсів.

Одним із найвідоміших випадків кібератаки, що мала ознаки інформаційно-психологічної операції, стала провокація із поширенням фальшивого повідомлення, у якому нібито Президент України Володимир Зеленський звернувся до громадян із закликом до капітуляції. Паралельно у мережі Інтернет, зокрема через Telegram-канали, було розповсюджено

діпфейкове відео із зображенням глави держави, яке дублювало цей неправдивий меседж.

Подібні дії свідчать про проведення скоординованої інформаційно-психологічної операції, спрямованої на дестабілізацію внутрішньополітичної ситуації, підрив авторитету державного керівництва та створення панічних настроїв серед населення. Такі методи поєднують елементи кібератак і медіаманіпуляцій, що робить їх особливо небезпечними в умовах воєнного стану та гібридної війни, яку веде Російська Федерація проти України.

Починаючи з кінця березня 2022 року, зафіксовано численні кібератаки проти українських державних структур і критичної інфраструктури. Серед них – фішингові кампанії, спрямовані на працівників органів державної влади, Збройних Сил України та різних організацій. Ці листи містили шкідливі вкладення або посилання, що дозволяли зловмисникам встановлювати бекдор LoadEdge для подальшого встановлення шпигунського програмного забезпечення.

Крім того, кібератаки були спрямовані на оператора зв'язку "Укртелеком" та сайти, створені на платформі WordPress, унаслідок чого виникли масштабні перебої в роботі телекомунікаційних мереж, а також тимчасове обмеження доступу до фінансових і державних сервісів.

Окремої уваги заслуговує використання викрадача інформації MarsStealer, за допомогою якого зловмисники отримали доступ до облікових даних українських громадян і працівників організацій. Подібним чином хакери здійснювали витяг конфіденційних даних із систем державних установ, медіаструктур і фінансових організацій, а також отримували банківську та платіжну інформацію громадян через троянські програми та шахрайські опитування в соціальних мережах.

Окремі кібератаки мали на меті завдати шкоди цивільному населенню. Так, фіксувалися спроби порушення роботи українських електростанцій із потенційним ризиком припинення постачання електроенергії мільйонам громадян. Іншим прикладом є кібератака на "Укрпошту", яка тимчасово зупинила роботу під час випуску поштових марок, присвячених війні, що свідчить про прагнення агресора підірвати моральний дух населення.

У цілому, воєнні дії супроводжувалися масштабною хвилею кібератак, спрямованих на урядові ресурси, телекомунікаційні послуги та об'єкти критичної інфраструктури, що підкреслює системний характер гібридної агресії Російської Федерації проти України. [8, с. 2].

Однією з найулюбленіших тактик інтернет-зловмисників є фішинг. Хакери надсилають шкідливі гіперпосилання або вкладення. Їх відкриття запускає програму, що надає доступ до даних. За допомогою фішингу російські спецслужби намагаються зібрати про українців усю можливу інформацію, в їхньому фокусі – персональні дані.

Для захисту своїх особистих прав, інтересів та даних варто дотримуватися правил безпечного використання мережі Інтернет, це: створення надійних паролів, захист інформації та періодична їх зміна; поінформованість про розповсюджені прийоми, які використовують злочинці для того, щоб розпізнавати їх; захист пристроїв, встановлення антивірусних програм; використання захищених мереж; перевірка своїх облікових записів; використання інструментів конфіденційності та безпеки Google чи інших браузерів.

Попри обмежені ресурси та можливості у сфері кібероборони, Україна активно зміцнює свою кіберстійкість, зокрема завдяки міжнародній підтримці та залученню фахівців з усього світу. З перших днів повномасштабного вторгнення уряд ініціював створення ІТ-армії України – спільноти волонтерів і кіберфахівців, яка координується під егідою Міністерства цифрової трансформації України.

У відповідь на масштабні кібератаки з боку Російської Федерації українська ІТ-спільнота здійснювала контркібероперації, спрямовані на російські державні та військові структури. Зокрема, ІТ-армія України проводила DDoS-атаки (які перевантажують сервери, створюючи надмірний трафік) та атаки типу “wiper”, що призводять до знищення або пошкодження даних. Серед основних цілей цих операцій були урядові установи Російської Федерації, медіаорганізації, фінансові структури, об’єкти оборонної промисловості, енергетичні мережі та транспортна інфраструктура, зокрема залізниці.

У межах глобальної протидії російській кіберагресії до ініціативи долучилися й незалежні хакерські угруповання та волонтери з різних країн світу. У результаті спільних дій було зламано та оприлюднено російські урядові й фінансові дані, включно з електронним листуванням, інформацією про банківську діяльність, енергетичне виробництво, пропагандистські кампанії, а також даними про військовослужбовців та співробітників Федеральної служби безпеки (ФСБ) [2].

Такі дії засвідчили формування нової форми цифрової солідарності, коли кіберфахівці, державні інституції та волонтери об’єдналися задля захисту інформаційного суверенітету України та протидії російській кіберагресії на глобальному рівні. [8, с.3].

Отже, в епоху стрімкого й активного розвитку інформаційних технологій вони стають невід'ємною частиною нашого повсякденного життя, робочих процесів і діяльності державних органів та бізнесу, а тому особливу увагу слід приділяти власній кібербезпеці. З упевненістю можна сказати, що кіберзлочини – це одна з основних проблем XXI ст., вирішення якої потребує сучасних методів, активних, рішучих заходів і своєчасного нормативного реагування. Це один з важливих пріоритетів нашої країну та світу.

Література

1. Конституція України (Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141) URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

2. Кримінальний Кодекс України (Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131) URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

3. Закон України Про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

4. Закон України Про інформацію (Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650) URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

5. Закон України Про захист інформації в інформаційно-комунікаційних системах URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

6. Закон України Про національну безпеку України (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241) URL: https://zakon.rada.gov.ua/laws/show/2469-19 7. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р URL: https://zakon.rada.gov.ua/laws/show/994_575

8. Державна служба спеціального зв'язку та захисту інформації України. Звіт про кіберактивність РФ проти України, 2023.

9. Microsoft Threat Intelligence. Special Report: Ukraine – Cyber Operations in Hybrid War, 2022.

10. CERT-UA. Alert (No. 4385) – Detection of CaddyWiper Malware in Ukraine, 2022.

11. Війна Росії проти України: хронологія кібератак URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf