SECTION 8.
INSTITUTE OF LAW ENFORCEMENT, JUDICIAL SYSTEM AND NOTARY

Габорець Ольга Андріївна
доктор філософії,
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки
Донецький державний університет внутрішніх справ, Україна

КІБЕРБЕЗПЕКА: ВАЖЛИВА СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВІЙНИ

В епоху сучасних технологій, коли інформаційний простір став неот'ємною складовою нашого повсякденного життя, поняття "національна безпека" придбуло новий вимір. На сьогоднішній день важливість безпеки в цифровому середовищі стає все більш істотною для держав, оскільки атаки в кіберпросторі можуть суттєво підірвати економіку, політичну стабільність та загрожувати життям індивідів. Україна, яка переживає виклик війни, стає свідком того, як кібербезпека стає важливою складовою національної безпеки в контексті військового конфлікту.

Саме в умовах війни актуальність кібербезпеки в Україні набуває особливого зваження, оскільки кібератаки можуть бути однією зі збройних сил, які ворог використовує для завдання шкоди національним інтересам. В цьому контексті важливо розглянути роль та стратегії України у забезпеченні кібербезпеки під час війни, а також докласти зусиль для захисту інформаційного простору країни від кіберагресій та кіберзагроз.

Дослідження проблеми кібербезпеки, зокрема захисту прав людини в інформаційному середовищі, було вивчено українськими вченими, такими як Д. Березовський, А. Бежевець, А. Глушко, О. Мережко, С. Онищенко, Ю. Яковенко та інші. Головною метою цієї статті є аналіз ключових змін у сфері кібербезпеки під час військового конфлікту в Україні та надання рекомендацій щодо поліпшення безпеки національного кіберпростору.

Кіберправо, як важлива частина інформаційного права, представляє собою один із найбільш перспективних напрямків розвитку українського законодавства. У вітчизняній системі нормативно-правового регулювання кібербезпеки важливе значення мають не лише Конституція України та Стратегія кібербезпеки України, але і: Закон України (далі – ЗУ) «Про інформацію» від 2 жовтня 1992 року № 2657-XII, ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР, ЗУ «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, ЗУ «Про захист персональних даних» від 1 червня 2010 року № 2297-VI, Постанова Кабінету Міністрів «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29 березня 2006 року № 373, Постанова Кабінету міністрів України «Про затвердження загальних вимог до кіберзахисту об’єктів критичної інфраструктури» від 19 червня 2019 року № 518 та ряд інших.

Окрім означених вище документів, про кібербезпеку міститься, зокрема, в ЗУ «Про національну безпеку України» в пп. 21 п. 1 ст. 1 цього закону визначено, що Стратегія кібербезпеки України – це документ довгострокового планування, який визначає загрози

кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [1]. Як відомо, основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. При цьому, контроль за законністю заходів із забезпечення кібербезпеки України відповідно до статті 15 ЗУ «Про основні засади забезпечення кібербезпеки України» в сфері дотримання законодавства здійснюється Верховною Радою України. А контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони та інших державних органів здійснюється Президентом України та Кабінетом Міністрів України в порядку, визначеному Конституцією і законами України [2]. 19 року № 518 та ряд інших.

Окрім означених вище документів, про кібербезпеку міститься, зокрема, в ЗУ «Про національну безпеку України» в пп. 21 п. 1 ст. 1 цього закону визначено, що Стратегія кібербезпеки України – це документ довгострокового планування, який визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [1]. Як відомо, основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. При цьому, контроль за законністю заходів із забезпечення кібербезпеки України відповідно до статті 15 ЗУ «Про основні засади забезпечення кібербезпеки України» в сфері дотримання законодавства здійснюється Верховною Радою України. А контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони та інших державних органів здійснюється Президентом України та Кабінетом Міністрів України в порядку, визначеному Конституцією і законами України [2].

Сучасні реалії вимагають створення та постійного розширення вітчизняних кібервійськ з двома головними метами. По-перше, це захист критично важливої інформаційної інфраструктури від можливих кібератак. По-друге, це реалізація превентивних наступальних кібероперацій, включаючи DDoS-атаки на корпоративні, новинні та державні сайти противника, відключення критично важливих об'єктів інфраструктури, компрометацію баз даних телекомунікаційних, роздрібних та урядових організацій, та інші заходи.

Вже з початку війни було створено добровольчу ІТ-армію України, яка об'єднала близько 175 тисяч учасників із різних країн світу. У цьому об'єднанні взяли участь білі хакери, хактивісти і представники технологічних компаній, включаючи такі великі гравці, як SpaceX. Також в цю діяльність включилася міжнародна мережа активістів і хакерів, відома як Anonymous Collective.

Ця ситуація представляла парадокс, оскільки досі жодному уряду в світі не вдавалося набрати настільки чисельну та глобальну групу незалежних іноземних суб'єктів, які б добровільно приєдналися до такого великого волонтерського об'єднання в кіберпросторі.

Крім цього, з метою поліпшення системи кібербезпеки в Україні було прийнято рішення внести законодавчі зміни до статей 361 та 361-1 Кримінального кодексу України [3], спрямовані на легалізацію процедури "Bug Bounty". Це офіційне визнання програми, яка надає можливість залучити зовнішніх фахівців для пошуку помилок та вразливостей у державних програмах, урядових веб-сайтах та інших інформаційних ресурсах.

По додатковій інформації від Державного спеціального зв'язку, в найближчий період планується створити посади "офіцерів із кіберзахисту" в органах державної влади та на об'єктах критичної інформаційної інфраструктури. Ці офіцери будуть підпорядковуватися

службам захисту інформації [4], і це крок спрямований на подальше зміцнення кібербезпеки в Україні.

Важливо також відзначити, що діяльність Кіберполіції в Україні суттєво змінилася через російське вторгнення. Кіберполіцейським довелося взяти на себе більше функціональних обов'язків та завдань. Крім того, в сфері програмування та розробки розумних ІТ-рішень Кіберполіція спільно з волонтерами та міжнародними партнерами здійснила значний успіх, зокрема:

- телеграм-бот під назвою "Народний месник", який є офіційним чат-ботом України для повідомлення про ворожі дії на території держави. Цей бот був спеціально створений для реагування Національної поліції та Збройних сил України на повідомлення громадян про виявлені ворожі мітки, рух техніки чи живих сил ворога, виявлення не розірваних боєприпасів, мародерів та диверсантів [5];

- телеграм-канал "StopRussiaChannel | MRIYA" [6] та телеграм чат-бот "StopRussia | MRIYA". Вони є складовими частинами екосистеми "MRIYA" і були спеціально розроблені для перевірки та блокування диверсійних ресурсів, які поширюють фейки та пропаганду. Окрім цього, на цих платформах можна знайти інструкції щодо боротьби з ворогом на інформаційному фронті та надсилати скарги на небезпечний, частково фейковий чи проросійський контент у соціальних мережах та месенджерах;

- онлайн-ресурс "DefenseUa" [7], який надає ворожим військовим-загарбникам детальну інструкцію щодо того, як відмовитися від участі у кривавій війні проти України та/або як вступити до лав Збройних сил України;

- інші офіційні сервіси, веб-ресурси, сайти, інструменти та ІТ-механізми, призначені, зокрема, для збору інформації про осіб, які підтримують російське вторгнення, надання можливості громадянам із території Російської Федерації голосувати щодо припинення війни, розпізнавання облич російських загарбників та багато інших завдань.

Отже, Національна система кібербезпеки України ще не досягла повноцінного розвитку, але російським кіберзагарбникам не вдається досягти своєї стратегічної мети та завдати значної шкоди критичній інфраструктурі нашої країни. Справжня правда полягає в тому, що Росія недооцінила Україну не лише у військовому плані, але й у кіберпросторі. Створення кіберсил України є наступним важливим кроком у забезпеченні кібербезпеки країни, навіть не зважаючи на те, що вже з початку війни фахівці з інформаційних технологій з усієї України активно долучилися до кіберполіції і внесли значний внесок у створення функціонуючої кіберармії.

Важливо відзначити, що виконання рекомендацій, включених у цьому дослідженні, щодо розширення кіберпотужностей, безперечно, піднесе Національний індекс кібербезпеки (NCSI) України до лідируючих позицій у світі.

Список використаних джерел:

1. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Кримінальний кодекс України: Закон України від 05 квітня 2001 року № 2341-III. URL : https://zakon.rada.gov.ua/laws/show/2341-14#top.
4. The Village Україна. В Україні узаконять процедуру Bug Bounty та створять посаду офіцера з кібербезпеки. URL : https://www.the-village.com.ua/village/city/city-news/321781-v-ukrayini-uzakonyatprotseduru-bug-bounty-i-stvoryat-posadu-ofitsera-z-kiberbezpeki?from=readmore
5. «Народний месник». Офіційний чат-бот України для повідомлення про ворожі дії на території нашої держави. URL : https://t.me/ukraine_avanger_bot
6. “StopRussiaChannel | MRIYA”. Офіційний телеграм-канал України для перевірки і блокування ресурсів, які поширюють фейки та пропаганду. URL: https://web.archive.org/web/20220601090556/https://t.me/stoprussiachannel
7. DefenseUa. URL : https://www.defenseua.com