УДК 004.492:341.31
DOI: 10.31733/15-03-2024/2/337-338

Андрій ЗВАГОЛЬСКИЙ
аспірант кафедри адміністративного права, процесу та адміністративної діяльності Дніпропетровського державного університету внутрішніх справ

ДЕЯКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ

У зв'язку з дією воєнного стану в країні, питання забезпечення кібербезпеки набуває надзвичайної актуальності та потребує першочергової уваги. Адже в умовах військового конфлікту різко зростають ризики масштабних кібератак з боку держави-агресора, спрямованих на дестабілізацію ситуації, поширення паніки, дезінформації та порушення роботи критичної інфраструктури. Як показує світовий досвід, кіберпростір стає одним з ключових напрямків протистояння у сучасних війнах.

Відповідно до Закону України «Про основні засади кібербезпеки України» кібербезпека – це захист життєво важливих інтересів особистості і громадянина, суспільства і держави при використанні кіберпростору, який забезпечує сталий розвиток інформаційного суспільства та цифрового комунікаційного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних та потенційних загроз до національної безпеки України в кіберпросторі [1].

Для України питання забезпечення кібербезпеки є особливо гострим, адже наша держава вперше опинилася в умовах повномасштабної війни з агресором, який володіє потужними кібервійськами та регулярно застосовує їх для атак на об'єкти критичної інфраструктури. Тому Україна має негайно вжити рішучих заходів як на державному рівні, так і на рівні приватних компаній та окремих громадян, для мінімізації уразливості та посилення стійкості кіберпростору до зовнішніх загроз.

Для забезпечення кібербезпеки в умовах воєнного стану необхідно вжити негайних та комплексних заходів як на державному рівні, так і на рівні приватних компаній та окремих громадян.

Першочерговим завданням є посилення захисту об'єктів критичної інфраструктури, таких як енергосистеми, транспорт, банки, телекомунікації. Адже їх працездатність є запорукою стабільності в країні. Необхідно максимально убезпечити ці об'єкти від зовнішніх кібератак, які можуть паралізувати їх роботу. Ключовим тут є як фізичний захист серверів та обладнання, так і використання надійного спеціалізованого програмного забезпечення для кіберзахисту.

Таку необхідність в захисті підтверджують, наприклад, слова дослідників Горінова П.В. та Драпушко Р.Г. У своїй роботі «Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану» вони зазначають: «Під час війни Інтернет стає потужною зброєю, яка значно посилюється технологіями штучного інтелекту. Кіберзброя включає в себе широкий спектр технічних і програмних засобів, які часто спрямовані на використання вразливостей у системах передачі даних. Варто нагадати, що країни Північноатлантичного альянсу відносять кібератаки до основних сучасних гібридних загроз, а кіберпростір – це оперативна зона бойових дій на рівні з сушею, морем і повітрям. Так, сьогодні фахівці фіксують зростання кількості кіберінцидентів і кібератак на державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури України» [2].

Важливо також забезпечити захищеність інформаційних систем та ресурсів державних органів, насамперед силових відомств, розвідувальних служб, органів державної влади. Адже вони містять конфіденційні дані, витік яких може зашкодити національній безпеці. Необхідно запобігти несанкціонованому доступу до таких даних, а також посилити рівень шифрування та захисту каналів зв'язку.

Окремо слід звернути увагу на протидію кібершпигунству та деструктивній діяльності противника в кіберпросторі. Адже в умовах війни агресор значно активізує такі зусилля задля дестабілізації ситуації, поширення паніки та дезінформації. Необхідно

виявляти і блокувати бот-мережі та фейкові акаунти, які використовуються з такою метою. Також вкрай важливо оперативно реагувати на кібератаки проти органів державної влади та ЗМІ, не дозволяючи зловмисникам досягти своїх цілей.

Зокрема, уваги потребує захист персональних даних громадян від витоків та кібератак. Адже в умовах хаосу зростають ризики незаконного збору та використання особистої інформації для шахрайських, пропагандистських чи інших цілей. Держава має убезпечити бази персональних даних, а громадян просвітити щодо цифрової гігієни та захисту приватності.

Окремого значення набуває посилення боротьби з кіберзлочинністю, що завжди активізується в умовах хаосу. Необхідно жорстко протидіяти різноманітним проявам шахрайства в мережі, крадіжкам грошей із банківських рахунків, поширенню шкідливого програмного забезпечення тощо. Адже такі дії підривають довіру громадян до цифрових технологій. Пов'язаність вчинення кіберзлочину з комп'ютерною технікою та інформаційними технологіями дає змогу розглядати як кіберзлочини як усі види злочинів, що можуть бути вчинені з її використанням, так і лише ту групу злочинів, що безпосередньо визначена у КК України саме як кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку [3].

Для ефективного забезпечення кібербезпеки вкрай важливу роль відіграє співпраця держави, ІТ-компаній та небайдужих громадян. Залучення фахівців ІТ-сфери допоможе посилити кіберзахист на технологічному рівні. А інформування та освіта населення щодо цифрової безпеки зменшать ризики уразливості перед кіберзагрозами. Тільки об'єднавши зусилля, можна забезпечити надійний захист кіберпростору України.

Також дуже важливо налагодити конструктивну співпрацю на міжнародному рівні, зокрема з країнами НАТО та ЄС. Адже глобальні виклики вимагають глобальної координації та об'єднання зусиль у сфері кібербезпеки. Спільними силами можна досягти значно більшого результату у протидії кіберзагрозам, ніж поодинці.

Отже, забезпечення надійної кібербезпеки в умовах воєнного стану потребує комплексу заходів як на державному рівні, так і на рівні бізнесу та суспільства. Лише об'єднавши зусилля та убезпечивши ключову інфраструктуру, дані та системи, можна гарантувати цифровий суверенітет та безпеку України від зовнішніх і внутрішніх загроз кіберпростору.

1. Про основні засади кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19.

2. Горінова П.В. та Драпушко Р.Г. Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану. *Юридичний науковий електронний журнал*. № 1/2023. URL : http://lsej.org.ua/1_2023/63.pdf.

3. Харитоненко І. О. Правові засади забезпечення кібербезпеки україни в умовах цифрового комунікативного середовища. *Часопис Київського університету права*, 2023, 2: 61 – 64. URL : https://chasprava.com.ua/index.php/journal/article/view/858.

УДК 004.492:341.31:351.74
DOI: 10.31733/15-03-2024/2/338-341

Олександр КАРПАНЕЦЬ
ад'юнкт відділу організації
освітньо-наукової підготовки
Харківського національного
університету внутрішніх справ

СУЧАСНИЙ СТАН ТА ПРІОРИТЕТИ ВДОСКОНАЛЕННЯ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ ОРГАНІВ МВС УКРАЇНИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ПРОТИДІЇ ЗБРОЙНІЙ АГРЕСІЇ

У сучасних умовах протидії збройній агресії, спрямованої проти України, питання забезпечення кібербезпеки для нашої держави відіграє ключове значення. На сьогоднішній день в Україні ухвалено цілу низку нормативно-правових актів, які спрямовані на