УДК 343.3/7
DOI: 10.31733/15-03-2024/1/530-531

Сергій БАБАНІН
доцент кафедри кримінального права
та кримінології Дніпропетровського
державного університету
внутрішніх справ, кандидат
юридичних наук, доцент

КІБЕРНЕТИЧНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Захист кібернетичної безпеки як складової національної безпеки України в умовах воєнного стану спирається на відповідну нормативно-правову базу.

Законом України «Про національну безпеку України» від 21 червня 2018 р. інформаційну безпеку та кібербезпеку віднесено до складових частин національної безпеки: державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України тощо (ч. 4 ст. 3) [1].

Законом України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 р. до об'єктів кібербезпеки віднесені, зокрема, держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність (п. 3 ч. 1 ст. 4) [2].

Крім того, Указом Президента України від 26 серпня 2021 р. № 447/2021 затверджена Стратегія кібербезпеки України, яка визначає, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України [3]. Планом реалізації цієї Стратегії передбачено, зокрема, завершити імплементацію в законодавство України положень Конвенції про кіберзлочинність (далі – Конвенція) (п. 15) [4].

Станом на сьогодні більшість положень Конвенції [5] в частині імплементації матеріального кримінального права до кримінального законодавства України є виконаною.

Водночас і Конвенція, і КК України [6] у чинній редакції не враховують особливості суспільної небезпечності комп'ютерних кримінальних правопорушень, які вчиняються в умовах збройного конфлікту чи воєнного стану.

При цьому у нормативно-правових актах має місце неузгоджене використання різної за змістом термінології. Так, вже згадуваний План реалізації Стратегії кібербезпеки України [4] вживає терміни «кібершпигунство» та «кібертероризм» (пп. 9, 14), зміст яких розкривається Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. [2].

Згідно з п. 13, 14 ч. 1 ст. 1 цього Закону кібертероризмом визнається терористична діяльність, що здійснюється у кіберпросторі або з його використанням, а кібершпигунством – шпигунство, що здійснюється у кіберпросторі або з його використанням [2].

У судовій практиці як кібершпигунство фактично кваліфікуються дії особи, пов'язані з несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України).

Так, дії ОСОБА_5 були кваліфіковані за ч. 1 ст. 361 КК за наступних обставин. ОСОБА_5, перебуваючи за місцем свого проживання, діючи умисно, з корисливих мотивів, усвідомлюючи суспільно-небезпечний характер своїх дій та передбачаючи їх суспільно-небезпечні наслідки і бажаючи їх настання, використовуючи свій персональний комп'ютер та обладнання для доступу до мережі Інтернет: Wi-Fi роутер «TP-Link TL-WR840 N», який наданий у користування Інтернет-провайдером, – через мережу Інтернет придбав від невстановленого досудовим розслідуванням користувача мережі Інтернет шкідливе програмне забезпечення «Suprime Miner», «BetaBoot», «Arkei», «RAT» та «LookiBot», яке в подальшому використав для викрадення персональних даних третіх осіб та, в порушення вимог абз. 6 ч. 1 ст. 2, ч. 1, 2 ст. 11, ст. 21 Закону України «Про інформацію», здобув у такий спосіб логіни, паролі, електронні адреси та файли «кукі» [7].

Отже, Конвенція та КК України не містять термінів «кібершпигунство» та «кібертероризм».

Разом з тим, кримінальна відповідальність за терористичну діяльність (ст. ст. 258–258-6 КК) та шпигунство (ст. ст. 111, 114 КК) передбачена кримінальним законодавством України. Однак склади цих кримінальних правопорушень не враховують особливості їх вчинення з використанням електронно-обчислювальної техніки та ступеня суспільної небезпечності таких діянь.

Крім зазначених складів кримінальних правопорушень, електронно-обчислювальна техніка використовується і при вчиненні суспільно небезпечних діянь з ознаками диверсії. Однак ст. 113 КК України не враховує такий спосіб як обов'язкову ознаку.

В умовах збройного конфлікту чи воєнного стану терористичні, шпигунські та диверсійні дії з використанням електронно-обчислювальної техніки набувають принципово вищого ступеня суспільної небезпечності порівняно з мирним часом, оскільки, у випадку з Україною, є частиною так званої гібридної війни, розпочатої російською федерацією. З початку повномасштабного вторгнення відбулись десятки хакерських атак, об'єктом яких були державні і недержавні установи, підприємства та організації України.

Прикладами таких хакерських атак є втручання у діяльність органів державної влади України (атаки на офіційні сайти цих органів, на їхні внутрішні інформаційно-комунікаційні системи), атаки на енергетичний сектор, зокрема на структурні підрозділи компанії «ДТЕК», Запорізької АЕС, атаки на ресурси операторів мобільного зв'язку, зокрема компанії «Київстар», тощо.

У зв'язку з зазначеним вбачається доцільною криміналізація таких діянь, а тому пропонуємо зміни та доповнення до кримінального законодавства України.

Частину 1 ст. 113 КК України викласти у такій редакції: «Вчинення з метою ослаблення держави вибухів, підпалів, несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж або інших дій…».

Частину 1 ст. 258 КК України викласти у такій редакції: «Терористичний акт, тобто застосування зброї, вчинення вибуху, підпалу, несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж чи інших дій…».

Частину 4 ст. 361 КК України викласти у такій редакції: «Дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку інформації, що становить державну таємницю…».

1. Про національну безпеку України : Закон України від 21 червня 2018 р. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text.

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 р. № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text.

4. Про План реалізації Стратегії кібербезпеки України : рішення Ради національної безпеки і оборони України від 30.12.2021. URL : https://zakon.rada.gov.ua/laws/show/n0087525-21#Text.

5. Конвенція про кіберзлочинність від 23.11.2001. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text.

6. Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

7. Кримінальна справа № 696/1095/19. Архів Смілянського міськрайонного суду Черкаської області.