

УДК 343.31

Філей Ю.В.¹, Правда Є.С.²

¹ канд. юрид. наук, проф. НУ «Запорізька політехніка»

² студ. гр. Ю-111 НУ «Запорізька політехніка»

КІБЕРТЕРОРИЗМ ТА КІБЕРШПИГУНСТВО ЯК ЗАГРОЗА СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Швидкий розвиток інформаційних і телекомунікаційних технологій сягає усе нових і нових рівнів, що вказує на їх активне впровадження до всіх сфер життєдіяльності людини. В епоху стрімкого науково-технічного розвитку та втілення у життя суспільства надбань у сфері технологій, серед основних проблем всесвітнього масштабу на одне з перших місць виходить проблема запобігання кібертероризму та кіберзлочинності. З появою всесвітньої мережі Інтернет, кожна країна отримала як безмежний доступ до інформації так і спроби злочинців здійснити кібератаки на більш вразливі системи держав. На сьогоднішній день інформація є однією з найбільших цінностей людства, саме з цієї причини система захисту інформації та забезпечення національної кібербезпеки стають першочерговими аспектами української держави. Підтвердженням цього стала прийнята 15 березня 2016 року Стратегія кібербезпеки України. За умов воєнного стану кібершпигунство та кібератаки набрали стрімкого оберту, що змушує систему національної безпеки України розвиватися та швидко реагувати на небезпечні ситуації.

З початком повномасштабного вторгнення в Україні кібератаки з боку росії стали радше інструментом ведення бойових дій, аніж засобом тиску на окремих людей та їхні приватні дані. Більшість кібератак була спрямована на державний сектор. Загальна їхня кількість зросла в десятки разів. За даними Держспецзв'язку, основні кібератаки з 24 лютого припали на державні та місцеві органи влади, інформаційні ресурси сектору безпеки та оборони. Якщо в лютому до 24 числа на державний сектор здійснили близько 143 тисяч атак, то в наступні

місяці ця цифра стрімко зросла: 42,7 мільйона атак у травні, 32,3 мільйона атак у липні та 28,7 мільйона атак у серпні.

Після численних невдач на полі бою в Україні росіяни посилили кібератаки проти цивільних компаній, таких як постачальники електроенергії та інтернет-провайдери. Ці атаки покликані зламати волю українців і переломити хід війни. Хоча росія для досягнення своїх цілей в Україні більше покладалася на ракетні удари, ніж на кіберзброю, атаки на енергетичні, урядові та транспортні групи показують, що кібератаки залишаються ключовою частиною загальної стратегії Москви, спрямованої на те, щоб зламати волю громадян. Такі атаки стають достатньо складною перешкодою та загрозою національній безпеці України, тож для їх попередження та вирішення повинні бути задіяні найсуворіші методи боротьби.

Одним із можливих підходів до боротьби з кіберзлочинністю у міжнародному аспекті і розвитку співпраці між державами є вироблення і стандартизація нормативно-правової бази. На міжнародному рівні першими документами у цій сфері стали Конвенція про кіберзлочинність, прийнята Радою Європи 23 листопада 2001 р., та Додатковий протокол до Конвенції, направлений на боротьбу з розповсюдженням через комп'ютерні мережі інформації расистського і ксенофобського характеру від 28 січня 2003 р. Прийняття цих актів означувало закладення правового фундаменту у сферу захисту свободи, безпеки і прав людини в мережі Інтернет не тільки на регіональному рівні. Серед шляхів запозичення позитивного досвіду Європейського Союзу в Україні є еволюція вітчизняного законодавства відповідно до європейських стандартів та поширення діяльності європейських міжнародних організацій з боротьби з кіберзлочинністю на українську територію.

Наприклад, Франція одна з перших в Європі вжила заходів до посилення ролі держави в регулюванні кіберпростору. Тому за основу запозичення зарубіжного досвіду слід розглянути методи боротьби з кібершпигунством саме даної країни. Вже сьогодні у Франції діють спеціальні закони, що забороняють публікацію матеріалів, що містять нацистську символіку, яка підтримує ідеї нацизму. Останнім часом в силу повномасштабної війни, спрямованої проти України, це питання актуалізувалося і в наших умовах. У сфері активної боротьби з кіберзлочинністю 14 лютого 2008 р. було прийнято французьку Стратегію по боротьбі з кіберзлочинністю, метою якої є співпраця між постачальниками інформаційно-телекомунікаційних послуг і правоохоронними органами з обміну інформацією і питаннях об'єднання зусиль в боротьбі з кіберзлочинністю.

Аналіз правового регулювання боротьби з кіберзлочинністю у Франції дозволяє виділити наступні шляхи запозичення позитивного досвіду в Україні: 1) встановлення вимоги авторизації авторів веб-сайтів; 2) налагодження співпраці правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз; 3) налагодження двостороннього діалогу з громадянами; 4) встановлення курсу на вільне співробітництво з іншими державами.

Отже, сучасний етап становлення громадянського суспільства визначається входженням України до провідних технологічно розвинутих країн світу, до глобального інформаційного простору. Саме тому, ми маємо на законодавчому рівні визначити способи попередження та боротьби з кібертероризмом, створити відповідні компетентні органи боротьби з кібершпиунством, навчити громадян самостійно оберігатися від кібератак. Запозичуючи досвід зарубіжних країн ми можемо побудувати якісну систему застереження та сповіщення про випадки кібертероризму.