УДК 343.9(043.2)

Продан Т.В., к.ю.н., доцент,
Чернівецький національний університет імені Ю. Федьковича,
м. Чернівці, Україна

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

З розвитком новітніх технологій розвиваються й нові злочинні можливості, а саме серйозний виклик для держави становить боротьба із негативними проявами кіберзлочинності. Що ми розуміємо під кіберзлочинністю? Кіберзлочинність – це кримінально-протиправна діяльність, що спрямована на заволодіння інформацією з баз даних, перехоплення інформації, знищення інформації за допомогою розповсюдження програм-вірусів, фішингових програм, злому з корисливих, політичних чи особистих мотивів.

Існування кіберзлочинності становить досить серйозну проблему в умовах глобального процвітання інноваційно-технологічних ресурсів. Це впливає абсолютно на всіх, як на окремих фізичних та юридичних осіб, так і на об'єкти критичної інфраструктури й державні органи. Окрім, відповідної прямої шкоди, кіберзлочинність є величезною перешкодою для цифрової довіри, значною мірою підриваючи переваги кіберпростору.

Україна останніми роками дедалі більше відчуває на собі масштаби кібернетичних атак та їх негативні наслідки. Так, кількість кримінальних правопорушень у сфері інформаційних технологій постійно зростає. Зокрема, з огляду статистичних даних Генеральної прокуратури України випливає, що станом на 1 грудня 2022 року обліковано у звітному періоді 3415 кримінальних правопорушень у сфері інформаційних технологій, що на 105 кримінальних правопорушень більше порівняно з 2021 роком та на 917 – більше порівняно з 2020 роком (станом на цей же період) [1]. Це свідчить в цілому про суттєве зростання, а саме – на 3,1% порівняно з 2021 роком та – на 26,8% порівняно з 2020 роком, кількості зареєстрованих кримінальних правопорушень.

Варто зазначити, що поширенню кіберзлочинності сприяють такі чинники: гіперпопит на різні види інформаційних послуг у розвинутих країнах світу; процеси глобалізації світової економіки; розвиток сучасних інформаційних технологій, особливо інтернет-ресурсів, що забезпечують майже неконтрольований процес формування спокус [2, с. 161].

Враховуючи вищезазначене, питання боротьби з кіберзлочинністю є особливо актуальним, оскільки необхідно вживати відповідних заходів щодо зменшення проявів кібератак у мережі Інтернет.

Одним з напрямків боротьби з цим негативним явищем є прийняття на законодавчому рівні нормативно-правових актів, які регулюють відносини

у цій сфері. Зокрема, нормативно-правову базу у даній сфері складають: Конституція України, Кримінальний кодекс України, закони України: «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про основи національної безпеки», Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Також з метою недопущення зростання рівня кіберзлочинності Верховною радою України прийнято Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах воєнного стану», який набув чинності 24 березня 2022 року. Метою даного закону є забезпечення надійності та безпеки використання цифрових послуг, впровадження дієвих кримінально-правових механізмів протидії кіберзлочинності, оптимізація національної системи кібербезпеки щодо протидії кіберзагрозам. Відповідне посилення санкцій та додаткова криміналізація окремих діянь, на нашу думку, здатні частково стримати потенційних злочинців від вчинення нових кримінальних правопорушень [3].

Варто зазначити, що Україна бере активну участь на міжнародному рівні у протидії кіберзлочинності. А саме, бере участь у: проєктах ЄС та НАТО з метою посилення спроможності України у сфері кібербезпеки; проведенні спільних навчань суб'єктів сектору безпеки та оборони в рамках заходів колективної оборони; у спільних проєктах Ради Європи та ЄС щодо підвищення обізнаності та навчання співробітників правоохоронних органів у сфері кібербезпеки; проведенні спільних навчань суб'єктів сектору безпеки та оборони в рамках заходів колективної оборони.

Протидія кіберзлочинності є основне завдання кіберполіції. Так, саме кіберполіція повинна завчасно інформувати населення про нові схеми кіберзлочинів та впроваджувати різні програмні засоби, щоб уберегти громадян від кібератак.

З вище викладеного випливає, що кіберзлочинність в Україні розвивається досить швидко, але й кіберполіція не стоїть на місці та з кожним днем демонструє високі показники викриття кримінально-протиправної діяльності. Протидія кіберзлочинності здійснюється не лише на спеціальному рівні, але й на індивідуальному, а тому громадянам необхідно особисто підвищувати свій рівень цифрової грамотності та приділяти увагу кібербезпеці. Одним із способів є постійне використання антивірусного програмного забезпечення та його оновлення тощо.

Таким чином, Україні потрібен подальший розвиток кібербезпеки, адже злочинці завжди йдуть щонайменше на крок попереду механізмів, які мають відповідні державні органи щодо протидії даному виду

злочинності. А тому, лише завдяки належному рівню кібербезпеки можливе нормальне функціонування мереж та систем, які з кожним днем все більше інтегруються в життя нашого суспільства.

Література

1. Генеральна прокуратура України. URL: https://www.gp.gov.ua/ (дата звернення: 28.01.2023)

2. Таволжанський О.В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія Право*. 2018. № 6 (18). С. 154-163.

3. Боротьба з кіберзлочинністю в умовах воєнного стану. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення: 27.01.2023)

УДК 343.14(043.2)

Рябоконь Ю.В., здобувач вищої освіти
першого (бакалаврського) рівня,
Національний авіаційний університет, м. Київ, Україна
Науковий керівник: Тарасюк С.М., доктор філософії

ОСОБЛИВІ ВИПАДКИ ВИЗНАННЯ НСРД НЕДОПУСТИМИМИ

Питання допустимості доказів закріплені ч. 1 ст. 87 КПК України, що виражає їх придатність у використанні та розгляду в кримінальному провадженні. Критерії допустимості злочинів виражається в належному процесуальному оформлені проведення негласних слідчих (розшукових) дій та спеціальному суб'єкті, який має право проводити дані процесуальні дії. Аналізуючи практику ЄСПЛ, вирішення питання щодо допустимості доказів не є в їхній компетенції. Тобто, не є завданням суду вирішувати чи є даний доказ допустимим, та яким шляхом його було отримано (Справа ЄСПЛ Биков проти Росії). Враховуючи дані особливості, досить часто проведення негласних (розшукових) дії визнаються недопустимими доказами у ході кримінального провадження.

Правова позиція касаційної інстанції неодноразово формулювала висновки щодо випадків недопустимості доказів у результаті проведення НС(Р)Д. Так, ВСУ висловив думку, щодо обов'язковості застосування ст. 290 КПК України, яка стосується своєчасному відкриттю матеріалів іншій стороні. Якщо сторона обвинувачення не змогла вжити усіх необхідних засобів та недодержалась своєчасних таймлайнів щодо відкриттю матеріалів згідно ст. 290 КПК України, то в такому випадку наявне порушення розсекречення доказів. Виходячи із вищесказаного, суд