4. Про альтернативне вирішення спорів (АВС). *Український центр медіації (UCM)*. URL: https://ukrmediation.com.ua/ua/korysna-informatsiia/pro-alternatyvne-vyrishennia-sporiv
5. Альтернативні способи вирішення спорів: теоретичні та практичні аспекти Ю. О. Фідря 2024. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/320323/310906

Жеруль Анастасія Сергіївна
здобувач вищої освіти навчально-наукового інституту права та психології НАВС
Науковий керівник:
Щерба Вікторія Миколаївна
кандидат юридичних наук, доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології НАВС

ЦИФРОВІ ЗЛОЧИНИ ПІД ЧАС ВІЙНИ: ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ КІБЕРЗЛОЧИНІВ

Повномасштабна збройна агресія Російської Федерації проти України суттєво трансформувала природу кіберзагроз та способи вчинення цифрових злочинів. Кіберпростір став повноцінним театром бойових дій, що істотно ускладнює кваліфікацію кіберзлочинів та висуває нові вимоги до кримінально-правової оцінки таких посягань.

Одним із ключових елементів кваліфікації цифрових злочинів є встановлення характеру несанкціонованого доступу. Відповідно до положень Конвенції про кіберзлочинність кожна сторона вживатиме таких законодавчих та інших заходів, які можуть бути необхідними для встановлення як кримінальних правопорушень умисного доступу до всієї комп’ютерної системи або її частини без права на те [3,ст.4].

Національне законодавство України повністю кореспондує цим стандартам. Так, ст. 361 Кримінального кодексу України (далі КК України) визначає, що кримінальним правопорушенням є несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж [1].

Стаття 362 КК України прямо зазначає, що кримінально караним є несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї. А ст. 363 КК України встановлює відповідальність за порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється [1].

У контексті війни важливим є також розуміння того, як міжнародні принципи втручання в дані застосовуються в Україні. У Конвенції наголошено на необхідності криміналізувати умисне пошкодження, видалення, погіршення, зміну або придушення комп'ютерних даних без права на те [3, ст. 4], що чітко узгоджується з положеннями вищезазначених статей КК України.

Разом із тим, у реаліях війни кваліфікація кіберзлочинів повинна враховувати зміну цілей та масштабів кібератак. За даними Центру реагування на комп'ютерні надзвичайні події України (CERT-UA), у 2022 році кількість кібератак проти України зросла більш як у три рази, а їхня мета змінилася з викрадення інформації на деструктивний вплив на об'єкти критичної інфраструктури.

Також значна частина атак мала характер цілеспрямованих операцій, спрямованих на порушення безперервності роботи державних сервісів. Таким чином, цифрові посягання дедалі частіше перетворюються з класичних злочинів проти інформаційної безпеки на складові воєнних операцій.

Питання кіберзахисту розкривається у Законі України «Про основні засади забезпечення кібербезпеки України» [2], де прямо сказано: «Кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на захист від кіберзагроз, забезпечення кібербезпеки, стійкості, цілісності, доступності та конфіденційності інформаційних ресурсів у кіберпросторі, а також здатності інфраструктури до їх обробки» [2, ст.1]

Цей же закон визначає, що об'єкти критичної інфраструктури є першочерговими для захисту, адже вони забезпечують стале функціонування життєво важливих для суспільства систем [2, ст.1]. Саме ці об'єкти найчастіше стають мішенню кібератак у період війни.

Особливого значення набуває і питання причинно-наслідкового зв'язку між військовими діями та кібератаками. У спеціальному звіті Microsoft Threat Intelligence підкреслюється. За день до військового вторгнення оператори, пов'язані з ГРУ, російською військовою розвідкою, здійснили руйнівні атаки на сотні українських урядових систем, IT, енергетичних та фінансових організаціях. Відтоді активність, яку ми спостерігали, включала спроби знищити, порушити роботу або проникнути в мережі урядових установ та широкий спектр організацій критичної інфраструктури, на які російські військові сили в деяких випадках націлювалися, здійснювали наземні атаки та ракетні удари [4, с.1].

Кваліфікація таких посягань більше не може ґрунтуватися лише на технічній фіксації несанкціонованого доступу чи пошкодження даних – вона повинна охоплювати міжнародні стандарти, норми КК України та воєнно-політичний контекст, у якому ці злочини вчиняються.

Масштаб кібератак, їхня спрямованість на критичну інфраструктуру та синхронізація з військовими операціями свідчать про їхню системність та стратегічний характер. Це вимагає подальшого вдосконалення правового регулювання, посилення спроможностей держави у сфері кіберзахисту та розширення міжнародної співпраці.

Список використаних джерел

1. Кримінальний кодекс України: Закон України від 05.04.2001 р. №2341-III. URL: https://zakon.rada.gov.ua/go/2341-14
2. «Про основні засади забезпечення кібербезпеки України» Закон України від 05.10.2017 р. №2163-VIII. URL: https://zakon.rada.gov.ua/go/2163-19
3. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.201 р. ратифікована 07.09.2005 р. №994_575.
URL: https://zakon.rada.gov.ua/go/994_575
4. Microsoft Threat Intelligence. Special Report on Russian Cyber Operations against Ukraine від 2022 р. URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/1212211-ms-ukrainespecialreport-fy23-link-update.pdf

Загородній Євгеній Олегович
аспірант кафедри кримінальної юстиції навчально-наукового інституту права та психології Національної академії внутрішніх справ, адвокат
Науковий керівник
Степанова Ганна Миколаївна
професор кафедри кримінальної юстиції навчально наукового інституту права та психології НАВС,
кандидат юридичних наук, доцент

ВИКОНАННЯ КЕРІВНИКОМ ПРОКУРАТУРИ ПОВНОВАЖЕНЬ СЛІДЧОГО СУДДІ: МЕЖІ ДОПУСТИМОСТІ ТА ГАРАНТІЇ СПРАВЕДЛИВОГО СУДОВОГО КОНТРОЛЮ

Реформування кримінального процесуального законодавства України, пов’язане з запровадженням 24 лютого 2022 р. воєнного стану, викликало питання допустимості тимчасового поєднання процесуальних функцій прокурора та слідчого судді в одній особі прокурора. Безумовно, запроваджені законодавцем випадки, які дозволяють прокурору здійснювати окремі повноваження слідчого судді, мають на меті забезпечити оперативність досудового розслідування та безперервність кримінального провадження. Водночас така практика неминуче ставить під сумнів дотримання фундаментальних гарантій незалежності, неупередженості та ефективного судового контролю, що є ключовими елементами права на справедливий суд, гарантованого ст. 6 Конвенції про захист прав людини і основоположних свобод та національними процесуальними нормами.

Наразі у правозастосуванні виникла проблема у визначенні підстав та меж участі прокурора як тимчасового виконавця повноважень слідчого судді та у встановленні таких процесуальних запобіжників, які б мінімізували ризики концентрації владних повноважень в руках сторони обвинувачення. У цьому контексті особливого значення набуває аналіз співвідношення публічного