26.12.2012 № 1950/5). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення 09.12.2022).

8. Про затвердження Змін до Інструкції про призначення та проведення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 22 лютого 2019 р. № 563/5. *Офіційний вісник України* від 22.02.2019 р., № 15, ст. 538.

9. Про затвердження Змін до Інструкції про призначення та проведення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 24 лютого 2020 р. № 667/5. *Офіційний вісник України* від 13.03.2020 р., № 20, стаття 777.

10. Про затвердження Інструкції з організації проведення та оформлення експертних проваджень у підрозділах Експертної служби Міністерства внутрішніх справ України : наказ Міністерства внутрішніх справ України від 17.07.2017 р. № 591. *Офіційний вісник України* від 19.09.2017 р., № 73, ст. 2254.

DOI https://doi.org/10.36059/978-966-397-287-9-112

КІБЕРЗЛОЧИННІСТЬ: ВИКЛИКИ СУЧАСНОСТІ

Ломакіна Олена Анатоліївна

кандидатка юридичних наук, доцентка,
доцентка кафедри адміністративного та конституційного права
Національного університету кораблебудування імені адмірала Макарова
м. Миколаїв, Україна

Кравченко Анна Сергіївна

студентка V курсу факультету морського права
Національного університету кораблебудування імені адмірала Макарова
м. Миколаїв, Україна

Повномасштабне вторгнення Російської Федерації (росії) на територію нашої держави змусило активізувати боротьбу українців за власну державність на всіх можливих фронтах. У зв'язку з розвитком світових передових технологій кіберпростір – є одним із найгарячіших «зон» війни.

Забезпечення реалізації державної політики в сфері протидії кіберзлочинності – є одним із завдань Кіберполіції України [1]. Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту

державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України [2].

Серед кіберзлочинів, що активно почали ширитись країною є наступні: скімінг (шимінг), кеш-трапінг, кардінг, фішинг, онлайн-шахрайство, соціальна інженерія. Окрім зазначених є, безпосередньо зумовлені війною, корисливі кіберзлочини, що виявлено Кіберполіцією України останнім часом: псевдо збори, пропозиції з оренди неіснуючого житла, фейкові пасажирські перевезення, продаж неіснуючих товарів, зокрема й військової амуніції, шахрайства під виглядом організації переправлення через державний кордон чоловіків призовного віку, шахрайства під приводом надання інформації щодо безвісно зниклих громадян і тд [3].

Окремим видом шахрайства виступають оголошення щодо надання грошової допомоги від міжнародних організацій. Ці оголошення є популярними в соціальних мережах та в різних месенджерів. Для того щоб охопити більшу аудиторію здійснюються різноманітні телефоні дзвінки з пропозицією «допомоги». Погоджуючись на дану «допомогу», особи передають власні особисті дані, номера карток та надають доступ до власних рахунків. І як наслідок – шахраї володіють і особистими даними, і фінансами ошуканих.

Кібератаки здійснюються не лише на індивідуально, а й масово: за даними СБУ з початку повномасштабного вторгнення росії було виявлено та нейтралізовано понад 120 потужних кібератак на ресурси органів державної влади та військового управління України, а також ІТ-систем об'єктів критичної інфраструктури, операторів зв'язку та ЗМІ [1].

Державна служба спеціального зв'язку та захисту інформації стверджує, що за місяць війни вже сталося майже втричі більше хакерських атак різного виду, ніж за аналогічний період минулого року. Як зазначає голова Держспецзв'язку Юрій Щиголь, атакують передусім державні установи, фінансовий, оборонний сектор, операторів зв'язку, місцеві органи влади, логістичні компанії, медіа [4]. Цинічного характеру набирають численні спроби хакерів зламати ресурси, що збирають інформацію про військові злочини росії в Україні.

Ми бачимо, що виникає необхідність держави побудови правового механізму захисту кіберпростору. В-першу чергу потрібно акцентувати увагу на створені інституту, який допоможе забезпечити безпечність та збереження як персональних, так і держаних даних. Також потрібно звернути увагу на наявні наукові розробки в галузі адміністративного захисту інформаційної сфери та реалізувати вже виробленні прикладні

засади протидії протиправним проявам у сфері кібербезпеки та життєдіяльності держави. Зазначимо, що прикладним аспектом розгляду питання реалізації та забезпечення кібербезпеки є розробка методологічних засад забезпечення безпеки інформаційних відносин у системі адміністративної діяльності держави. Наступним кроком в галузі кібербезпеки потрібно розробити практичні рішення, що дозволять адекватно реагувати на погрози кібербезпеки або передбачати нові погрози та вміти їм протистояти.

Таким чином, можна зробити висновок, що кіберпростір повинен закріпити за собою статус інструмента державної негайної та потужної відповіді на агресію. Кіберзахист нашої держави вимагає правового реформування задля забезпечення протидії можливих атак, затвердження порядку реагування на кіберзлочини та закріплення механізму притягнення до кримінальної відповідальності.

Література:

1. Департамент Кіберполіції України. https://cyberpolice.gov.ua. URL: http://cyberpolice.gov.ua (дата звернення: 25.11.2022).

2. Про основні засади забезпечення кібербезпеки України від 05.10.2017 № 2163-VIII ВР. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Пядишев В. Г. Національна поліція України у боротьбі з корисливими кіберзлочиними, що поширились або виникли під час агресії рф. 2022. URL: http://dspace.oduvs.edu.ua/bitstream/123456789/3279/1/212.pdf.

4. Державна служба спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua (дата звернення: 25.11.2022).

DOI https://doi.org/10.36059/978-966-397-287-9-113

МЕХАНІЗМ МАСОВИХ ЗАВОРУШЕНЬ

Мішустін Владислав Володимирович

аспірант кафедри кримінального процесу та криміналістики
Донецького державного університету внутрішніх справ
м. Кропивницький, Україна

Предметом криміналістики є закономірні зв'язки між елементами механізму злочину, а завданням криміналістики – встановлення цих зв'язків. Механізм злочину розглядається як процес взаємозв'язку та взаємодії суб'єкта злочинної діяльності з предметом посягання, потерпілим, знаряддями й засобами вчинення злочину, часу, місця та