України. 2024. № 31.1. С. 264–275.

3. Санакоєв Д. Б. Виявлення та розслідування торгівлі людьми підрозділами Національної поліції України : монограф. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2017. 192 с.

4. Шаповалова І. О. Особливості тактики допиту жінок, потерпілих від насильницьких злочинів. *Південноукраїнський правничий часопис*. 2021. № 2. С. 158–162.

Сидорова Е. О.
заступник декана з освітньої
та науково-дослідної діяльності
факультету підготовки фахівців
для органів досудового розслідування
Національної поліції України
Дніпровського державного
університету внутрішніх справ,
доктор юридичних наук, доцент;

Рижкін Д. В.
старший оперуповноважений
в особливо важливих справах
Управління протидії кіберзлочинам
у Дніпропетровській області
Департаменту кіберполіції
Національної поліції України

ПРОТИДІЯ КІБЕРЗЛОЧИНАМ В УМОВАХ ДІЇ ВОЄННОГО СТАНУ В УКРАЇНІ

Питанням виявлення, запобігання, попередження та розкриття кіберзлочинності завжди приділялась значна увага як з боку практиків, так і науковців. Зараз важко собі уявити людину, яка не користується сучасними гаджетами, включаючи проведення електронних платежів. Найпростішими прикладами є плата за проїзд у громадському транспорті, оплата комунальних платежів, здійснення покупок через інтернет-магазини тощо. Усі ці дії відбуваються через використання кіберпростору, тому разом з технічним прогресом отримали й кіберзлочинність, яка створює загрози не тільки окремій людині, а й навіть національній безпеці держави в цілому, зокрема у умовах воєнного стану небезпечними є кібер атаки рф на найважливіші електронні системи, які стосуються національної безпеки України, розповсюдження шкідливого програмного забезпечення представниками росії, заволодіння коштами суб'єктів господарювання з метою подальшого фінансування збройної агресії, коштами громадян під приводом підписання

петиції про присвоєння звання військовим або під приводом отримання коштів від родин безвісти зниклих військових, злочини у сфері критичної інфраструктури.

На теперішній час кількість наукових публікацій, пов'язаних з проблемами протидії кіберзлочинності займає значний об'єм, але з урахуванням військової кіберагресії рф проти України й надалі необхідно досліджувати зазначену проблематику, оскільки кожного дня продовжується атаки з боку росії, зокрема надходять повідомлення про замінування закладів вищої освіти, адміністративних будівель, підприємств тощо, перебої в роботі електронних систем банківської сфери, незаконне заволодіння персональними даними користувачів мобільного зв'язку з метою викрадення коштів громадян. Перерахувати всі можливі способи вчинення кіберзлочинів не вдасться навіть в окремому збірнику тез доповідей конференції, присвяченій проблемам боротьби з кіберзлочинністю.

Ще до початку повномасштабного військового вторгнення рф проти України, Радою національної безпеки і оборони України введено в дію «План реалізації Стратегії кібербезпеки України». Головною метою зазначеного плану є розроблення дієвої системи відповідних індикаторів оцінки стану кібербезпеки, яка охоплюватиме: базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки, індикатори стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом [1].

Ще одним дуже важливим кроком з боку держави, вже після початку війни, було прийняття ряду змін до чинного законодавства. Зокрема, зміни стосувались трьох важливих законів: «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137-IX від 15.03.2022 [2]; «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24.03.2022 [3].

Усі ці зміни направлено на оптимізацію кримінального та кримінального процесуального законодавства щодо удосконалення підстав та процесуальних механізмів притягнення до кримінальної відповідальності кіберзлочинців, але серед фахівців триває жвава дискусія щодо обговорення вказаних змін. Зокрема, Мовчан Р.О. піддає критиці положення про те, що для кваліфікації відповідних посягань за ч. 5 ст. 361 КК не вимагається того, щоб вони скоювались «з використанням умов воєнного стану», а натомість достатньо їхнього вчинення в умовах воєнного стану і спричинення наслідків, передбачених ч. 3 або ч. 4. Автор зазначає, що прямим результатом такого законодавчого кроку стало те, що відтепер, наприклад, банальний, але вчинюваний в умовах воєнного часу несанкціонований перегляд телепередач має отримувати кримінально-правову оцінку з посиланням саме на ч. 5 ст. 361

КК. Також, дослідник аргументує помилковість вилучення існуючого раніше у примітці ст. 361 КК принципово важливого застереження відносно того, що при оцінці «значної шкоди» згаданий майновий еквівалент мав братися до уваги лише тоді, коли така шкода полягала у заподіянні матеріальних збитків, який призвів до суттєвого та нічим невиправданого звуження сфери потенційного застосування ч. 4 ст. 361 КК [4].

На жаль, в цій роботі висвітлити весь масив проблем та надати належну їм оцінку, спираючись на думки вчених та практиків не є можливим. Головною метою було привернути уваги вчених, практичних працівників та інших небайдужих громадян, у тому числі здобувачів вищої освіти до актуальних проблем протидії кіберзлочинам в сучасних умовах. Лише спільною роботою можливо досягнути позитивного результату.

Як підсумок, необхідно зазначити те, що під час військової агресії рф, яка веде гібридну війну, окрім постачання країнами- партнерами воєнної зброї Україні, нам вкрай потрібно технічно бути озброєними у боротьбі з кіберагресією рф. Зокрема, доцільно навчатися та переймати досвід у закордонних фахівців, які працюють у цій сфері. Також, важливим є проведення роботи з приводу інформування громадян про безпеку в кіберпросторі, зокрема важливо підвищити ефективність роботи державних органів у соціальних мережах і месенджерах. Це вкрай необхідно для оперативного поширення достовірної інформації та захисту громадян від дезінформації та шахрайства. Серед основних важливих кроків, як варто впровадити, слід виділити наступні: верифікація профілів державних органів, моніторинг інформації та оперативне реагування на «масові вкиди», надсилання неверифікованих ресурсів до бота «BRAMA» (проєкт започатковано волонтерами та на сьогоднішній день, функціонує за підтримки Департаменту кіберполіції Національної поліції України), створення реєстру офіційних каналів державних органів у соціальних мережах і месенджерах («Кібер Брама» є складовою частиною проєкту «BRAMA»).

***Список використаних джерел**:*

1. Рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»: Указ Президента України від 1 лютого 2022 року № 37/2022.

2. «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації" щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам»: закон України № 2137-IX від 15.03.2022.

3. «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» закон України № 2149-IX від 24.03.2022.

4. Мовчан Р.О. Аналіз законодавчих змін, направлених на підвищення ефективності кримінально-правової протидії кіберзлочинності в умовах дії воєнного стану. URL: https://r.donnu.edu.ua/xmlui/bitstream/handle/123456789/2598/8.pdf?sequence=1&isAllowed=y.