***Козак Б.В.***
*студентка магістратури*
*юридичного факультету*
*Тернопільського національного*
*економічного університету*
*Науковий керівник: к.ю.н., доцентя кафедри*
*кримінального права та процесу ТНЕУ*
*Олійничук Р.П.*

# ОСНОВНІ ПРОБЛЕМИ ТА ПРОГАЛИНИ В ГАЛУЗІ КІБЕРБЕЗПЕКИ УКРАЇНИ

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції. Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави [1].

Слід погодитись із думкою П. Ю. Доброскок та М. В. Бурак які відзначають, що загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як: невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам; недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз; безсистемність заходів кіберзахисту критичної інфраструктури; недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів; недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру; недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки. Науковці акцентують увагу на тому, що національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури. Вони зауважують, що пріоритетами та напрямами забезпечення кібербезпеки України є: розвиток безпечного, стабільного і

надійного кіберпростору; кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом; кіберзахист критичної інфраструктури; розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки [1].

Слушною є думка фахівця у сфері дослідження проблем кібербезпеки в Україні Олексія Янковського (партнер KPMG в Україні, відповідальний за консалтинг в сфері IT і кібербезпеки, віце-президент київського відділення професійної неприбуткової організації ISACA), який у співавторстві з групою експертів, визначив основні прогалини в галузі кібербезпеки України:

– неефективна нормативна база та система управління (аналіз першопричин призводить до цілої низки системних проблем у галузі, ігнорувати які з кожним наступним інцидентом стає дедалі важче);

– низька готовність реагувати на кібератаки (більшість компаній все ще не готові організаційно до нових хвиль кібератак та не мають підготовлених в достатній мірі фахівців у своєму штаті);

– низький рівень залучення професійної спільноти, відсутність трансформаційного підходу (відсутній трансформаційний підхід до управління національною кібербезпекою, що передбачає наявність організації, яка керує впровадженням програми з кібербезпеки, та регулярного контролю за процесом впровадження);

– кіберрозвідка потребує покращення (в Україні все ще недостатньо ефективно працює система кіберрозвідки (Threat Intelligence);

– низька якість аудиту кібербезеки (окрема проблемна ділянка – аудити кібербезпеки. Дозвіл на проведення аудиту мають лише акредитовані державою організації. Міжнародні сертифікати з інформаційної безпеки та IT-аудиту наразі не визнаються, що негативно впливає на якість аудиту);

– роль держави: не регулятор, а фасилітатор.

Фасилітація (від англ. facilitation – допомога, полегшення, сприяння) – це організація процесу колективного розв'язання проблем у групі, який керується фасилітатором (ведучим, керівником). Основна ідея реформи – перейти від моделі, коли держава намагається контролювати кібербезпеку, в тому числі в приватних організаціях, до саморегуляції, яка дозволить бізнесу самостійно визначати і контролювати впровадження стандартів кібербезпеки для відповідних галузей. Очевидно, це має бути не функція контролю (як зараз), а скоріше фасилітації і допомоги у вирішенні проблем кібербезпеки [2].

Отже, внаслідок динамічного розвитку та застосування новітніх технологій, питання захисту суспільства від їхнього використання в злочинних цілях усе більше загострюється. Тому роль держави у розбудові вітчизняної системи кіберзахисту потребує переосмислення та перезавантаження. Потреба у докорінних і термінових змінах також підтверджена численними атаками на об'єкти вітчизняної інфраструктури, та багатьма іншими інцидентами, які протягом останніх років зробили Україну плацдармом кіберзлочинності.

Незважаючи на досить значні наукові здобутки у цьому напрямі, багато аспектів даної проблематики, зокрема роль держави у розбудові власної кібербезпеки залишаються малодослідженими та спірними, особливо у їхньому практичному втіленні.

**Список використаних джерел**

1. Доброскок П. Ю., Бурак М. В. Реалізація стратегії кібербезпеки України. *Актуальні питання протидії кіберзлочинності та торгівлі людьми*: збірник матеріалів Всеукр. наук.-практ. конф. (23 листоп. 2018 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2018. 436 с.
2. Янковський О. Україні потрібна нова кіберстратегія. URL: https://www.pravda.com.ua/columns/2019/09/14/7226291/ (дата звернення: 14.10.2019).

***Козак С.П.***
*студент магістратури*
*юридичного факультету*
*Тернопільського національного*
*економічного університету*
*Науковий керівник: к.ю.н., доцент кафедри*
*конституційного, адміністративного та*
*фінансового права ЮФ ТНЕУ*
*Росоляк О.Б.*

## ОКРЕМІ АСПЕКТИ АДМІНІСТРАТИВНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПОРУШЕННЯ МІГРАЦІЙНОГО ЗАКОНОДАВСТВА УКРАЇНИ

Нещодавно Кабінет міністрів України схвалив Стратегію державної міграційної політики України на період до 2025 року. Основними цілями зазначеного документу є: зниження адміністративних бар'єрів для свободи пересування в Україні; створення необхідних умов для повернення та реінтеграції українських мігрантів в українське суспільство; сприяння легальній міграції в Україну, узгодженій із соціальною політикою та економічним розвитком країни. Крім того, документом передбачено удосконалення прикордонного контролю осіб, адаптованого до змінних міграційних потоків та можливостей інтегрованого управління кордонами; посилення контролю за дотриманням міграційного законодавства всередині країни [4].

Здійснюючи ті чи інші дії в сфері правового регулювання свободи пересування та вибору місця проживання, громадяни України, іноземці й особи без громадянства повинні дотримуватися міграційного законодавства. Ця вимога ґрунтується на положеннях Конституції України. Згідно із статтею 68 кожен зобов'язаний неухильно додержуватися Конституції України і законів України, не посягати на права і свободи, честь і гідність інших людей [1].

У випадку порушення норм міграційного законодавства до винної особи можуть бути застосовані заходи юридичної відповідальності. В даному випадку ми зупинимось на одному із її видів, а саме на адміністративній відповідальності за порушення міграційного законодавства.

Слід відзначити, що Кодекс України про адміністративні правопорушення передбачає конкретні адміністративні проступки в сфері міграції, за які встановлена адміністративна відповідальність.

У Кодексі України про адміністративні правопорушення міститься норма, що встановлює адміністративну відповідальність за правопорушення, пов'язані з дотриманням правил паспортної системи [2].