УДК 342.9

Котух Є.
д.н. з держ. управління

Сидоренко Я.
аспірант, Університет Единбургу

ОСНОВНІ НАПРЯМИ РОЗВИТКУ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ У КІБЕРПРОСТОРІ: МІЖНАРОДНИЙ ДОСВІД

Сьогоднішній світ все більше залежить від цифрових технологій, що призводить до зростання кіберзлочинності та викликів кібербезпеці [1]. У відповідь на це, країни по всьому світу розробляють та впроваджують нові підходи до правоохоронної діяльності в кіберпросторі [2].

Відповідно до статті 1 закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочином (комп'ютерним злочином) вважається суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Правове регулювання правоохоронної діяльності у кіберпросторі здійснюють норми міжнародного права, Конституція України, закони України, а саме «Про інформацію» від 02.10.1992, «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994, «Про телекомунікації» від 18.11.2003, «Про захист персональних даних» від 01.06.2010, «Про основні засади забезпечення кібербезпеки України» від 05.10.2017, «Про національну безпеку України» від 21.06.2018), укази Президента України, а саме Концепція розвитку сектору безпеки і оборони України від 14.03.2016 № 92/2016, «Про Стратегію кібербезпеки України» від 15.03.2016 №96/2016, «Про затвердження доктрини інформаційної безпеки України» від 25.02.2017 № 47/2017), Постанови Кабінету Міністрів України, а саме «Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373, «Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури» від 23.08.2016 № 563, «Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.2019 № 518) та інші нормативно-правові акти.

Аналіз зазначених законодавчих актів свідчить про наявність достатнього правового підґрунтя у сфері протидії кібернетичним злочинам, водночас практична реалізація спрямована на результативні правоохоронні дії в кіберпросторі вимагають удосконалення. Світовий досвід розвитку правоохоронної діяльності у кіберпросторі в сучасних реаліях та в контексті реформування правової системи в Україні демонструє сталість процесів, що спрямовані збільшення ефективності правоохоронної діяльності в кіберпросторі [3]. Ключові стратегії та тенденції включають:

- співпрацю між країнами та міжнародними організаціями як важливий елемент боротьби з кіберзлочинністю;

- створення спеціалізованих підрозділів та команд для боротьби з кіберзлочинністю на міждержавному рівні;
- використання сучасних технологій, таких як штучний інтелект, машинне навчання та великі дані, для посилення ефективності правоохоронних органів, зокрема в побудові моніторингових систем на рівні об'єктів критичної інформаційної інфраструктури;
- розвиток навчальних програм та підготовки фахівців для роботи в сфері кібербезпеки шляхом посилення рівня науково-педагогічних кадрів в закладах вищої освіти;
- співпраця з приватним сектором для обміну інформацією, ресурсами та експертизою.

Україна зіткнулася з низкою викликів у сфері кібербезпеки, зокрема за умов повномасштабної агресії, зростання кіберзлочинності, кібератак та інформаційної війни [4]. Світовий досвід розвитку правоохоронної діяльності у кіберпросторі демонструє, що ефективна боротьба з кіберзлочинністю вимагає міжнародної співпраці, спеціалізації, технологічного прогресу, освіти та підготовки, а також приватно-публічних партнерств [5,6]. У контексті реформування правової системи в Україні, країна може скористатися цими стратегіями та досвідом, щоб посилити свої зусилля в сфері кібербезпеки та захистити об'єкти критичної інформаційної інфраструктури.

ЛІТЕРАТУРА:

1. INTERPOL. (2021). Cybercrime. URL: https://www.interpol.int/Crime-areas/Cybercrime
2. European Union Agency for Cybersecurity. (2021). Cybersecurity in the European Union. URL: https://www.enisa.europa.eu/topics/cybersecurity-policy-and-strategy/cybersecurity-in-the-european-union
3. National Cyber Security Centre. (2021). Cybercrime. URL: https://www.ncsc.gov.uk/information/cybercrime
4. National Cyber Security Coordination Centre. (2021). Cybersecurity in Ukraine. Електронний ресурс: https://cybersecurity.gov.ua/
5. Ukrainian Centre for Cyber Security. (2021). Cybersecurity in Ukraine. Електронний ресурс: https://uaccc.gov.ua/
6. Cybercrime and Digital Evidence. (2021). Cybercrime and Digital Evidence. Електронний ресурс: https://www.cybercrime-detection.com/