DOI https://doi.org/10.30525/978-9934-26-419-1-21

ON THE NEED TO IMPROVE LEGAL REGULATION OF COUNTERING CYBERCRIME IN UKRAINE

ДО ПИТАННЯ ПРО НЕОБХІДНІСТЬ УДОСКОНАЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Kotsman I. I.
Postgraduate student of the Department of Public Management and Administration, Vinnytsia State Pedagogical University named after Mykhailo Kotsiubynskyi, Chief Lawyer at PJSC «Volochyska Kura»

Коцман І. І.
аспірант кафедри публічного управління та адміністрування, Вінницький державний педагогічний університет імені Михайла Коцюбинського, головний юрист в ПАТ «Волочиська Кура»

Сучасний розвиток суспільства, широке впровадження інформаційних та цифрових технологій спричинив зростання кіберзлочинності, що становить серйозну загрозу для національної безпеки, економіки та прав громадян. В Україні, з огляду на активну цифровізацію та загострення гібридних загроз, особливо в умовах воєнного стану, проблема ефективного правового регулювання протидії кіберзлочинності набуває особливої актуальності. Чинне законодавство потребує вдосконалення з урахуванням нагальних викликів, міжнародних стандартів, сучасних методів кіберзахисту та новітніх форм злочинної діяльності у кіберпросторі.

Ефективне державне регулювання будь-якої сфери суспільного життя базується на функціонуванні організаційно-правової системи, яка забезпечує порядок і стабільність. Основу такої системи становить правове регулювання, що є ключовим інструментом державного впливу на різні об’єкти управління. За допомогою правового регулювання держава встановлює чіткі правила поведінки, координує діяльність учасників правовідносин і забезпечує дотримання законності.

Правове регулювання протидії кіберзлочинності в Україні можна визначити як систему правових норм, принципів і механізмів, спрямованих на запобігання, своєчасне виявлення, ефективне розслідування та припинення кримінальних правопорушень, що вчиняються у кіберпросторі, а також на притягнення винних осіб до відповідальності.

Серед елементів системи правового регулювання протидії кіберзлочинності в Україні необхідно визначити такі складові, як:

1) Національне законодавство, яке визначає склад кіберзлочинів, повноваження правоохоронних органів та санкції за вчинення правопорушень у сфері кібербезпеки, засади здійснення внутрішньої і зовнішньої політики у сфері кібербезпеки, функціонування та захисту електронних комунікацій, захисту державних інформаційних ресурсів та інформації;

2) Міжнародні правові акти, що регулюють співпрацю держав у сфері боротьби з кіберзлочинністю (наприклад, Будапештська конвенція про кіберзлочинність [1]). Міжнародна співпраця у боротьбі з кібертероризмом здійснюється під егідою ООН, Ради Європи, Інтерполу, Європолу та інших організацій. ООН відіграє ключову роль у координації цих зусиль, залучаючи Генеральну Асамблею, Раду Безпеки та багатосторонні партнерства. Більшість міжнародних структур розробляють нормативну базу та створюють спеціалізовані органи для ефективної взаємодії у сфері протидії кіберзлочинності. В межах ООН ухвалено низку резолюцій, спрямованих на запобігання кібертероризму та зміцнення міжнародної безпеки;

3) Процесуальні та процедурні механізми, які забезпечують оперативне розслідування та переслідування кіберзлочинців, реалізацію державної політики у даній сфері, удосконалення протоколів та технологій захисту державних інформаційних ресурсів та об’єктів критичної інфраструктури. Такі механізми охоплюють комплекс заходів, спрямованих на вдосконалення законодавчої бази, оперативну взаємодію між правоохоронними органами, кіберпідрозділами та міжнародними партнерами, а також підвищення кваліфікації спеціалістів у сфері цифрової безпеки. Процедурні механізми повинні передбачати створення ефективної системи реагування на кіберзагрози, що передбачає розробку сучасних протоколів розслідування, впровадження інноваційних технологій для збору та аналізу доказів, а також посилення механізмів контролю за кіберпростором. Крім того, особливу увагу слід приділяти вдосконаленню засобів захисту державних інформаційних ресурсів та об’єктів критичної інфраструктури, розробці стандартів кібербезпеки, що відповідатимуть міжнародним вимогам, і створенню умов для швидкого реагування на нові виклики в сфері кіберзлочинності;

4) Заходи з кібербезпеки, що застосовуються державними та приватними структурами для запобігання злочинам у цифровому середовищі. Вказані заходи охоплюють комплекс технологічних, організаційних та правових інструментів. Державні органи впроваджують політику кіберзахисту шляхом створення спеціалізованих кіберпідрозділів, здійснення моніторингу загроз та швидкого реагування на кібератаки. Приватний сектор, у свою чергу, активно впроваджує сучасні технології захисту, зокрема багаторівневу

аутентифікацію, системи виявлення та запобігання вторгненням (IDS/IPS), шифрування даних, резервне копіювання та аналіз загроз за допомогою штучного інтелекту. Ефективна взаємодія державних і приватних структур у сфері кібербезпеки дозволяє створювати надійну систему захисту цифрового середовища, запобігати фінансовим, інформаційним та інфраструктурним ризикам, а також оперативно нейтралізувати загрози у разі їх виникнення.

Необхідність удосконалення національної системи протидії кіберзлочинності зумовлена кількома ключовими факторами. По-перше, сучасне суспільство дедалі більше покладається на інформаційно-комунікаційні технології, що інтегровані у всі сфери життя — від державного управління та економіки до приватного сектору і повсякденного життя громадян. Це робить інформаційний простір вразливим до різноманітних загроз, таких як кібератаки, шахрайство чи викрадення даних.

По-друге, у контексті триваючої війни, яку Україна змушена вести, кіберпростір стає одним із ключових напрямів протистояння. Постійні кібератаки, спрямовані на державні інституції (як це сталося 19 грудня 2024 року, коли відбулася масштабна зовнішня кібератака, внаслідок якої призупинили роботу Єдині та Державні реєстри, які перебувають у компетенції Міністерства юстиції України [2]), критичну інфраструктуру та бізнес (зокрема, 12 грудня 2023 року у результаті хакерської атаки на ядро мережі «Київстару» було знищено тисячі віртуальних серверів і ПК [3]), підкреслюють необхідність формування ефективної системи кіберзахисту, яка здатна реагувати на такі загрози.

По-третє, національне законодавство, попри певні позитивні зрушення, все ще має низку прогалин і правових колізій, які заважають ефективній боротьбі з кіберзлочинністю. Недостатня адаптація до міжнародних стандартів та відсутність чітких механізмів взаємодії між державними органами, приватним сектором та громадськістю є додатковими викликами, які потребують вирішення.

Розвиток сучасних технологій та активне впровадження AI-асистентів у всіх сфери життя ставить нові виклики щодо захисту кіберпростору і вимагає вироблення єдиного підходу до регулювання цього питання. У сучасному цифровому середовищі, де традиційні засоби кіберзахисту не справляються зі складними загрозами, впровадження стратегій, заснованих на ШІ, стало новою віхою у зміцненні кібербезпеки.

Висновки. Оптимізація правових механізмів дозволить підвищити ефективність боротьби з кіберзлочинністю, забезпечити належний рівень захисту інформаційної безпеки та сприятиме інтеграції України в європейську систему кібербезпеки. Таким чином, з огляду на зростання загроз у кіберпросторі, удосконалення правового регулювання протидії

кіберзлочинності в Україні є нагальною потребою. В тому числі важливим є закріплення на законодавчому рівні основних понять, принципів і механізмів, що спрямовані на протидію кіберзлочинності в Україні.

В умовах воєнного стану кіберпростір став важливим фронтом протистояння, а кібератаки на державні інституції, критичну інфраструктуру та фінансовий сектор підтверджують необхідність створення ефективної системи захисту. Це потребує адаптації національного законодавства до міжнародних стандартів, посилення механізмів співпраці між державними органами та приватним сектором, а також удосконалення технічних і організаційних заходів безпеки. Крім того, динамічний розвиток штучного інтелекту відкриває нові можливості у сфері кіберзахисту, однак водночас породжує нові виклики, пов'язані з регулюванням та етичними аспектами його використання. Тому формування єдиної державної стратегії протидії кіберзлочинності має включати сучасні технологічні рішення, міжнародний досвід та комплексну систему правового регулювання, що дозволить підвищити рівень безпеки в цифровому середовищі України.

Література:

1. Convention on Cybercrime. Budapest, 23.11.2001. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

2. Кібератака на реєстри: у МВС тимчасово призупинили надання окремих послуг. *УНІАН: офіційний вебсайт інформаційного агенства.* Допис від 20 грудня 2024 року. URL: https://www.unian.ua/economics/transport/kiberataka-na-reyestri-u-mvs-timchasovo-prizupinili-nadannya-okremih-poslug-12859068.html

3. Тарасовський Ю. Хакери перебували в системі «Київстару» з травня 2023 року. СБУ розкрила деталі кібератаки. Forbes.ua: *офіційний вебсайт журналу.* Допис від 4 січня 2024 року. URL: https://forbes.ua/news/khakeri-perebuvali-v-sistemi-kiivstar-z-travnya-2023-roku-sbu-04012024-18307.