

Нагорнюк Марія Миколаївна, здобувач вищої освіти НАВС

Науковий керівник – **Резнік Юлія Степанівна**, старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології НАВС, кандидат юридичних наук

АДАПТАЦІЯ НАЦІОНАЛЬНОГО КРИМІНАЛЬНОГО ЗАКОНОДАВСТВА ДО МІЖНАРОДНИХ СТАНДАРТІВ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

У сучасних умовах стрімкого розвитку інформаційних технологій, глобалізації та тотальної цифровізації суспільних відносин кіберзлочинність перетворилася на одну з найбільш серйозних загроз для національної безпеки кожної суверенної держави. Специфіка віртуального простору – його транскордонність, анонімність, висока швидкість передачі даних та відсутність фізичних меж – дозволяє зловмисникам легко дезорганізовувати роботу критичної інфраструктури, залишаючись поза межами юрисдикції держави, яка зазнала атаки. Для України питання забезпечення кібербезпеки набуло стратегічного значення в умовах повномасштабної гібридної агресії. Кібератаки сьогодні є не просто формою комп'ютерного хуліганства чи інструментом економічно вмотивованого криміналу, а виступають повноцінним складником військово-політичного тиску, засобом дезорганізації системи державного управління, знищення конфіденційної інформації та ураження об'єктів критичної інфраструктури (енергетичного сектору, банківської системи, логістики).

Ефективно протидіяти таким викликам виключно в межах внутрішньодержавних правових механізмів неможливо. Кіберпростір за своєю природою є глобальним, що вимагає від нашої держави активного та системного впровадження міжнародних безпекових стандартів у національне правове поле. Ключовим вектором у цьому контексті є адаптація матеріальних і процесуальних норм кримінального права до положень Конвенції про кіберзлочинність (Будапештської конвенції) [1], яка є фундаментальним міжнародно-правовим документом у цій сфері, а також до відповідних Директив Європейського Союзу, що спираються на передовий закордонний досвід правового регулювання інформаційної безпеки.

Питання кримінально-правового забезпечення кібербезпеки та адаптації законодавства до міжнародних стандартів перебувають у центрі уваги багатьох вітчизняних науковців. Різні аспекти цієї проблематики досліджували такі вчені, як В. В. Топчій, О. М. Бодунова, С. Мазепа, П. П. Богуцький, М. В. Гуцалюк та інші. Проте швидкість модернізації цифрових технологій випереджає темпи правотворчості, що зумовлює необхідність постійного теоретичного переосмислення цієї царини. Важливим і першочерговим кроком на шляху адаптації правової системи України до міжнародних стандартів є модернізація матеріального кримінального права, кодифікованого у Кримінальному кодексі (КК) України. На сьогодні кримінально-правова охорона комп'ютерних даних, а також конфіденційності, цілісності та доступності електронних систем забезпечується переважно Розділом XVI Особливої частини КК України [2, с. 131].

Зокрема, базовою у цьому блоці є ст. 361 КК України, яка передбачає кримінальну відповідальність за несанкційоване втручання в роботу інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Конструкція цієї норми неодноразово зазнавала законодавчих змін з метою її синхронізації з міжнародними підходами до визначення протиправного доступу (illegal access) та протиправного втручання (illegal interference), закріплених у ст. 2 та 5 Будапештської конвенції [1]. Водночас стрімка динаміка розвитку сучасних кіберзагроз вимагає від законодавця постійного моніторингу правозастосовчої практики та оперативного вдосконалення диспозицій і санкцій кримінально-правових норм. Особливу увагу в цьому контексті слід приділити ст. 361-1 КК України, яка встановлює відповідальність за створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також ст. 362 КК України, що регламентує відповідальність за несанкційовані дії з інформацією, яка оброблюється в автоматизованих системах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї [2, с. 131].

Аналіз реальної правоохоронної та судової практики свідчить, що диспозиції зазначених статей все ще містять певні термінологічні неузгодженості та прогалини. Правопорушники

постійно модернізують інструменти кібератак, використовують хмарні технології, технології штучного інтелекту для генерації шкідливого коду та децентралізовані криптографічні мережі для приховування слідів злочину й легалізації доходів. За таких умов традиційні формулювання кримінального закону іноді виявляються неефективними або занадто вузькими для охоплення новітніх форм комп'ютерних деліктів.

Як зазначають у своєму глибокому аналітичному дослідженні професор В. В. Топчій та доцент О. М. Бодунова, ефективна протидія комп'ютерній злочинності в умовах сучасних безпекових криз можлива лише за умови чіткого, деталізованого та технологічно нейтрального визначення складу злочину. Науковці справедливо наголошують, що новітні кібератаки дедалі частіше спрямовані не просто на заволодіння майном чи приватними даними громадян, а на масштабну дезорганізацію державного управління та підлив загальної інформаційної безпеки України, що вимагає посилення кримінальної відповідальності за атаки на об'єкти критичної кіберінфраструктури [3, с. 112].

У свою чергу, у наукових матеріалах дослідників Інституту правотворчості та науково-правових експертиз НАН України акцентується увага на методологічних аспектах гармонізації права. Дослідники підкреслюють, що адаптація вітчизняного кримінального законодавства до стандартів Європейського Союзу є ключовим етапом зміцнення правової системи в умовах євроінтеграції. Проте цей процес потребує підходу, вільного від механічного, сліпого копіювання іноземних дефініцій. Натомість він вимагає глибокого практичного впровадження європейських безпекових норм (зокрема Директиви 2013/40/ЄС про атаки на інформаційні системи) в єдиний інформаційно-правовий простір України з урахуванням особливостей національного процесуального права та матеріальної доктрини [4, с. 142].

Поряд із суто практичними та законодавчими аспектами існує вагомий доктринальний пласт проблем. Процес адаптації гальмується через недостатню розробленість фундаментальних теоретичних категорій. Як підкреслює С. Мазепа, ключова наукова проблема в цій сфері полягає у гострій, першочерговій необхідності комплексного теоретичного обґрунтування концептуальних засад правового регулювання кібербезпеки в умовах гібридних загроз та цифрової трансформації державного управління. Існуючі доктринальні підходи у вітчизняному правознавстві не повною мірою враховують транснаціональний та віртуальний характер кіберпростору. Через це значна частина теоретичних досліджень залишається фрагментарною, позбавленою системності та міждисциплінарного підходу, який мав би інтегрувати правові, технічні (ІТ-технології, кібернетика) та соціальні аспекти аналізованої проблеми [5, с. 74].

Для подолання цих недоліків правова наука має запропонувати нову парадигму розуміння об'єкта кіберзлочинів. Об'єктом кримінально-правової охорони сьогодні є не просто «комп'ютерна система» чи «магнітний носій», а стан захищеності інформаційного суверенітету держави та базових прав людини у цифровому вимірі. Крім того, нагальною є потреба адаптації інституту взаємної правової допомоги. Оскільки цифрові докази є вкрай мінливими та можуть бути знищені за лічені секунди, традиційні міжнародні бюрократичні процедури запитів є неефективними. Тут у нагоді стає впровадження стандартів Другого додаткового протоколу до Конвенції про кіберзлочинність, який стосується посиленого співробітництва та розкриття електронних доказів [6].

Реалізація спільних безпекових ініціатив з європейськими інституціями, взаємний обмін оперативною інформацією, технічними даними та практичним досвідом з міжнародними партнерами (зокрема з відповідними підрозділами країн ЄС та агенціями НАТО) дозволяють українським правоохоронним органам та судовому корпусу вчасно виявляти приховані законодавчі прогалини. Це відкриває реальні можливості для оперативної, науково обґрунтованої адаптації норм Особливої частини Кримінального кодексу України до нових способів вчинення високотехнологічних правопорушень.

Підсумовуючи викладене, варто зазначити, що адаптація національного кримінального законодавства до міжнародних стандартів у сфері кібербезпеки є безперервним та динамічним процесом, який не може обмежуватися одноразовим внесенням змін до КК України. Системний підхід вимагає повної термінологічної уніфікації національного законодавства з положеннями Будапештської конвенції та актів *acquis communautaire* ЄС, розробки чітких

кримінально-правових норм, спрямованих на захист критичної інформаційної інфраструктури в умовах війни, а також побудови гнучкого механізму міжнародного співробітництва для швидкого збору та фіксації електронних доказів. Тільки за умови гармонійного поєднання передової світової практики та фундаментальних вітчизняних теоретичних напрацювань Україна зможе створити дієву та сучасну систему кримінально-правової протидії кіберзлочинності, що надійно захистить її національні інтереси у цифровому просторі.

Список використаних джерел

1. Конвенція про кіберзлочинність : Міжнародний документ Ради Європи від 23.11.2001 № ETS-185. Офіційний вісник України. 2006. № 11. Ст. 703. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
2. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
3. Топчій В. В., Бодунова О. М. Проблемні питання забезпечення кібербезпеки в Україні. *Аналітично-порівняльне правознавство*. 2025. № 1. С. 110–115. URL: <https://app-journal.in.ua/wp-content/uploads/2025/02/112.pdf>
4. Адаптація законодавства України до положень права Європейського Союзу : збірник матеріалів науково-практичної конференції (м. Київ, 10 жовтня 2025 р.). Одеса : Видавництво «Юридика», 2025. 480 с.
5. Мазепа С. Інформаційне правопорушення: до питання формалізації правової категорії. *Аналітично-порівняльне правознавство*. 2025. № 4. Вип. 3. С. 72–77.
6. Другий додатковий протокол до Конвенції про кіберзлочинність щодо посиленого співробітництва та розкриття електронних доказів : Міжнародний документ Ради Європи від 12 трав. 2022 р. № CETS-224. URL: <https://rm.coe.int/1680a68840>

Ноготков Артур Андрійович, курсант ВІКНУ імені Тараса Шевченка

Науковий керівник – **Мазур Вікторія Вікторівна**, доцент кафедри цивільного права Навчально-наукового інституту права КНУ імені Тараса Шевченка, кандидат юридичних наук, доцент

ОБОРОННІ ЗАКУПІВЛІ ЯК ІНСТРУМЕНТ АДАПТАЦІЇ ЗАКОНОДАВСТВА УКРАЇНИ ДО СТАНДАРТІВ БЕЗПЕКИ ЄС І НАТО

В умовах повномасштабної збройної агресії Російської Федерації проти України система оборонних закупівель набуває визначального значення для забезпечення обороноздатності держави, безперервного постачання озброєння, військової техніки, матеріальних засобів і послуг для сектору безпеки та оборони. Одночасно євроатлантичний курс України актуалізує необхідність правової адаптації національного законодавства до стандартів Європейського Союзу та НАТО, що охоплює, зокрема, сферу оборонних закупівель як одну з найбільш чутливих і стратегічно важливих.

Порівняльно-правовий аналіз законодавства держав-членів НАТО свідчить, що регулювання оборонних закупівель у більшості країн характеризується поєднанням загальних принципів публічних закупівель із спеціальними безпековими винятками. У державах НАТО існує спільна тенденція до забезпечення прозорості процедур закупівель, однак із збереженням можливості обмеження конкуренції у випадках, коли цього вимагають суттєві інтереси національної безпеки. Такі підходи випливають із положень європейського права, зокрема норм, що дозволяють державам-членам відступати від загальних правил внутрішнього ринку у сфері оборони [1, с. 1].

Європейська модель регулювання оборонних закупівель формувалася поступово. Початково держави-члени ЄС мали широкі можливості для виключення оборонної сфери з дії загальних правил внутрішнього ринку з мотивів національної безпеки. Згодом підхід змінився у бік часткової гармонізації та створення спеціального правового режиму, який поєднує вимоги конкуренції та прозорості з можливістю обмеження доступу до інформації, якщо це обумовлено суттєвими інтересами безпеки.

У європейському праві ключове значення має Директива ЄС щодо оборонних закупівель 2009 року, яка запровадила окремі правила здійснення закупівель у сфері оборони та безпеки,