УДК 351.746:004.056.55(100)
DOI https://doi.org/10.32782/1813-3401.2024.4.39

І. І. Коцман
аспірант кафедри публічного управління та адміністрування
Вінницького державного педагогічного університету імені Михайла Коцюбинського,
головний юрист в ПАТ «Волочиська Кура»
ORCID ID: 0009-0009-1791-1592

ЗАРУБІЖНИЙ ДОСВІД ДЕРЖАВНОГО РЕГУЛЮВАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

У статті досліджено зарубіжний досвід державного регулювання протидії кіберзлочинності в країнах Європи та США. Автором проаналізовано державне регулювання, правове забезпечення, організаційну структуру та міжнародне співробітництво у сфері боротьби з кіберзлочинністю. У статті розкривають успішні моделі боротьби з кіберзлочинністю та акцентовано увагу на можливості їх застосування в Україні.

У статті проаналізовано досвід США, зокрема акт Computer Fraud and Abuse Act (CFAA), що передбачає кримінальну відповідальність за несанкціонований доступ до комп'ютерних систем, охарактеризовано ключові органи в цій сфері, зокрема, Федеральне бюро розслідувань (FBI) та Національне агентство з безпеки (NSA), які здійснюють ефективну боротьбу з кіберзлочинністю через Національну стратегію кібербезпеки. У статті акцентовано увагу, що вкрай важливим є публічно-приватне партнерство для обміну інформацією та розробки стандартів безпеки в цій сфері.

Було проаналізовано досвід ЄС у боротьбі із кіберзлочинністю та переваги державного регулювання у цьому напрямку. Так, зазначено, що в країнах ЄС де ключовими документами у сфері регулювання боротьби із кіберзлочинністю є Будапештська конвенція Ради Європи та Директива NIS 2, що встановлює стандарти кібербезпеки для країн-членів. В Україні, хоча Будапештська конвенція була ратифікована, її положення ще не повністю імплементовані в національне законодавство. Окремо проаналізовано досвід Німеччини, Франції та Польщі, де створені ефективні національні системи кібербезпеки, що дозволяють швидко реагувати на кіберзагрози завдяки багаторівневій організації. Зокрема, зазначено, що в Німеччині діє Федеральне управління з інформаційної безпеки (BSI), а у Франції – Національне агентство з кібербезпеки (ANSSI).

У статті запропоновано вдосконалення української системи кібербезпеки шляхом адаптації кращих міжнародних практик, зокрема створення спеціалізованих підрозділів, розвитку співпраці між державними та приватними органами, а також посилення міжнародного співробітництва. Акцентовано увагу на необхідність оновлення українського законодавства, створення нових інституційних механізмів та активної участі приватного сектору у забезпеченні кібербезпеки для ефективної боротьби з кіберзлочинністю в Україні.

Ключові слова: *публічне управління, кібербезпека, кіберзлочинність, державне регулювання, публічно-приватне партнерство, зарубіжний досвід регулювання боротьби із кіберзлочинністю.*

Постановка проблеми. Актуальність дослідження зарубіжного досвіду державного регулювання протидії кіберзлочинності обумовлена глобальним характером кіберзагроз, які не знають державних кордонів і впливають на всі сфери суспільного життя. Сучасний світ, що все більше залежить від інформаційно-комунікаційних технологій, стикається з новими викликами у сфері безпеки, серед яких кіберзлочинність посідає одне з ключових місць. У цьому контексті вивчення та адаптація найкращих практик інших країн може допомогти удосконалити національні механізми реагування на кіберзагрози, зокрема, шляхом впровадження ефективних законодавчих, організаційних та технічних рішень.

Кожна країна має свої особливості державного

регулювання протидії кіберзлочинності, вивчення якого може бути корисним з точки зору можливості впровадження в Україні. Крім того, врахування досвіду розвинутих країн у створенні та функціонуванні спеціалізованих правоохоронних структур, діяльність яких спрямована на боротьбу із кіберзлочинністю, формуванні державно-приватного партнерства та розробці міжнародно-правових механізмів співпраці є важливим етапом у зміцненні національної кібербезпеки. Аналіз міжнародного досвіду дозволяє не лише виявити успішні моделі протидії кіберзлочинності, а й уникнути помилок, які допускалися іншими країнами, враховуючи специфіку правової, економічної та технічної інфраструктури України. У підсумку це сприяє підвищенню ефективності боротьби з кіберзлочинністю на національному та глобальному рівнях.

Аналіз наукових досліджень. У сучасному цифровому світі кіберзлочинність стала однією з найсерйозніших загроз національній безпеці, економіці та приватному життю громадян. У зв'язку з цим питання ефективного державного регулювання у сфері протидії кіберзлочинності набуває особливої актуальності. Вказана проблема є предметом дослідження багатьох науковців, серед яких Біленький В. П. [1], Самойленко О. А. [2], Сосін О .В. [3], Теплицький Б. Б. [4], Яцишин М. Ю. [5] та багато інших. Проте, більшість досліджень зроблено з точки зору правової науки, питання державного регулювання протидії кіберзлочинності приділяється недостатньо уваги, що обумовлює необхідність ґрунтовних досліджень у цій сфері. Вивчення зарубіжного досвіду дозволяє виявити ефективні підходи, законодавчі моделі та організаційні механізми, які можуть бути адаптовані в національне законодавство для підвищення рівня кібербезпеки в Україні.

Метою статті є вивчення зарубіжного досвіду державного регулювання протидії кіберзлочинності в країнах Європи та у США та можливість імплементації цього досвіду у національне законодавство.

Виклад основного матеріалу. У більшості країн світу державне регулювання протидії кіберзлочинності ґрунтується на комплексному підході, який включає правові, технічні та організаційні заходи. Основними елементами такого підходу є: удосконалення законодавства у сфері кібербезпеки; створення системи національних органів кібербезпеки; розвиток публічно-приватного партнерства; міжнародне співробітництво у сфері кібербезпеки.

Сполучені Штати Америки є одним із лідерів у сфері боротьби з кіберзлочинністю. У країні діє низка законів, зокрема Computer Fraud and Abuse Act (CFAA), які передбачають кримінальну відповідальність за несанкціонований доступ до комп'ютерних систем [6]. Основним органом у сфері протидії кіберзлочинам є Федеральне бюро розслідувань (FBI), яке має спеціальні підрозділи кібербезпеки. Окрім того, в США активно функціонує Національне агентство з безпеки (NSA) та Департамент внутрішньої безпеки (DHS), що координують політику у сфері кіберзахисту. Діяльність цих правоохоронних органів координується відповідно до Національної стратегії кібербезпеки, яка визначає пріоритети державної політики в цій сфері, зокрема запобігання, виявлення та реагування на кіберзагрози.

Важливою особливістю американської моделі є розвинене публічно-приватне партнерство. Держава активно взаємодіє з представниками бізнесу, зокрема у галузі критичної інфраструктури та інформаційних технологій, з метою обміну даними про кіберінциденти, розробки спільних стандартів безпеки та впровадження превентивних механізмів. США також відіграють провідну роль у міжнародному співробітництві з питань кібербезпеки, укладають двосторонні угоди щодо обміну інформацією про кіберзлочинність, що сприяє підвищенню ефективності глобального реагування на кіберзагрози.

Дослідники підкреслюють, що в США функціонує цілісна система органів, які здійснюють боротьбу із кіберзлочинністю: 1) кібернетичне командування США (USCYBERCOM) – підрозділ збройних сил США, який проводить операції кібервійни, управління та захист військових комп'ютерних мереж; 2) Комп'ютерна команда екстреної готовності США (US-CERT) – частина Національного відділу кіберзахисту Міністерства внутрішньої безпеки, що надає інформацію про безпеку та працює над усуненням вразливостей у системах безпеки; 3) відділ комп'ютерної злочинності та інтелектуальної власності (CCIPS) – підрозділ Міністерства юстиції США, який розслідує комп'ютерні злочини та порушення прав інтелектуальної власності, спеціалізуючись на захопленні цифрових доказів [7, с. 212].

Проаналізувавши досвід США у сфері державного регулювання протидії кіберзлочинності, можна зробити висновок про можливість запозичення досвіду щодо декількох рівнів

боротьби із кіберзлочинністю. В Україні боротьбою із кіберзлочинністю переважно займається Департамент кіберполіції Національної поліції України. Як показує досвід кібератак на бази даних державних органів та банківську систему України з боку країни-агресора, ресурсів Департаменту кіберполіції недостатньо. У США ж, на відміну від України, існують три рівні боротьби з кіберзлочинністю: військовий, правоохоронний та юстиційний, причому кожен має свої специфічні повноваження. Це забезпечує значно вищу ефективність у боротьбі з кіберзлочинністю.

У країнах Європейського Союзу кібербезпека є пріоритетним напрямом безпекової політики. Рамковим документом у сфері протидії кіберзлочинності є Будапештська конвенція Ради Європи [8], яка визначає основні кримінально-правові та процесуальні норми для боротьби з кіберзлочинами. Україна, із певними застереженнями, ратифікувала Будапештську Конвенцію у 2006 році [9]. Наразі вказана конвенція залишається єдиним міжнародним юридично обов'язковим документом у сфері кібербезпеки. Вона спрямована на створення єдиної кримінальної політики для протидії кіберзлочинності шляхом гармонізації національного законодавства та активізації міжнародного співробітництва. Однак на сьогодні далеко не всі положення Конвенції впроваджені в українське законодавство, що ускладнює її практичну реалізацію. Для повного дотримання її вимог необхідне внесення значних змін, зокрема до Кримінального процесуального кодексу України, з метою удосконалення механізмів розслідування кіберзлочинів і підвищення ефективності міжнародної взаємодії у цій сфері. Будапештською Конвенцією передбачено перелік заходів, що мають здійснюватися на національному рівні в матеріальному кримінальному праві (ч.1 розділ 2), кримінальному процесуальному («процедурному») праві (ч. 2 розділ 2), передбачено також систему міжнародного співробітництва (розділ 3), окремо виділено питання юрисдикційного характеру (ч. 3 розділ 2) [8].

Варто підкреслити, що у Європейському Союзі протидія посяганням на електронні інформаційні ресурси регулюється низкою актів, зокрема Директивою ЄС щодо боротьби з кібератаками (2013 р.) та Директивою Єврокомісії щодо протидії шахрайству й інтернет-злочинам у фінансовій сфері (2017 р.). Позитивно слід відмітити, що у країнах ЄС значну увагу приділяють ранньому виявленню та оперативному реагуванню на кіберінциденти, що є запорукою швидкого розслідування злочинів, вчинених у кіберпросторі, а також мінімізації негативних наслідків для критичної інфраструктури, державних органів, бізнесу та громадян.

У жовтні 2024 року набула чинності директива з кібербезпеки Network and Information Security 2 (далі – NIS 2), яка установила єдині для країн ЄС стандарти у сфері кібербезпеки [10]. Директива NIS 2 зобов'язує компанії документувати стратегії кібербезпеки, впроваджувати механізми управління ризиками та повідомляти державні органи про серйозні кіберінциденти. За недотримання вимог передбачено штрафи – до 20 мільйонів євро або до 4% від загального річного обороту компанії (залежно від того, яка сума є більшою). Окрім того, керівники компаній можуть нести особисту фінансову відповідальність за недотримання положень директиви, що посилює принципи підзвітності у сфері цифрової безпеки.

Хоча Україна не є членом ЄС, і ця директива не є обов'язковою для виконання, вона слугує цінним орієнтиром для впровадження кращих практик у сфері кібербезпеки. Частина її положень була адаптована й інтегрована в українське законодавство на добровільних засадах, проте значна частина рекомендацій досі залишається поза увагою, що створює прогалини у забезпеченні ефективної кібербезпеки. Впровадження таких стандартів могло б підвищити рівень захисту критичної інфраструктури та сприяти посиленню міжнародного співробітництва у цій сфері.

Стратегія кібербезпеки ЄС передбачає виявлення, блокування та розслідування кібератак незалежно від джерела їх походження, а також захист цивільної інфраструктури. Європейська агенція з мережевої та інформаційної безпеки (ENISA) координує заходи з кіберзахисту, а CERT-EU виявляє атаки через мережу сенсорів. У разі фіксації злочинних дій інформація надходить до Європейського центру з розслідування кіберзлочинів, який може залучити Європейську оборонну агенцію чи Службу зовнішніх дій для організації відповідних заходів.

У багатьох країнах ЄС, зокрема в Німеччині, Франції, Польщі, створено національні центри кібербезпеки, що займаються моніторингом інцидентів, реагуванням на кіберзагрози та координацією між різними суб'єктами державної та недержавної сфери.

Варто підкреслити, що хоча у країнах ЄС державне регулювання кіберзлочинності здійсню-

ється на основі загальноєвропейських стратегічних документів, проте кожна окрема держава реалізує власну національну політику у цій сфері. Так, у Німеччині ключову роль у забезпеченні кібербезпеки відіграє Федеральне управління з інформаційної безпеки (BSI), яке функціонує під егідою Федерального міністерства внутрішніх справ [11]. Позитивно слід відмітити, що у Німеччині на законодавчому рівні запроваджені обов'язкові вимоги до операторів критичної інфраструктури щодо повідомлення про кіберінциденти та впровадження захисних заходів.

У Франції координацію заходів кібербезпеки здійснює Національне агентство з кібербезпеки (ANSSI) [12], підпорядковане прем'єр-міністру. Національне агентство з кібербезпеки у Франції виконує як превентивні, так і реагувальні функції, зокрема розробку нормативних документів, контроль за кіберзахистом державних органів і стратегічних підприємств. Франція, як і інші країни ЄС, також розвиває структури реагування на інциденти, а її законодавство передбачає суворі санкції за несанкціоноване втручання в інформаційні системи, що визначено у кримінальному кодексі Франції.

Цікавим є досвід Польщі, в якій заходи з протидії кіберзлочинності координуються Урядовим центром безпеки (RCB) та Агентством внутрішньої безпеки (ABW). Польське законодавство активно імплементує положення директив ЄС, зокрема згадану вище NIS 2, через національні правові акти, серед яких Закон про національну систему кібербезпеки [13]. Вартує уваги дослідження національної системи реагування на кіберінциденти у Польщі – Computer Security Incident Response Team (CSIRT), яка має чітку структуру. Так, система CSIRT складається з трьох основних підрозділів, кожен з яких відповідає за кіберзахист у відповідному секторі. Державний сектор (CSIRT GOV) відповідає за обробку інцидентів у державному секторі, включаючи органи публічної адміністрації, державні підприємства та інші інституції, що мають критичне значення для функціонування держави. Координація діяльності цього сектора покладається на Державне управління цифровізації. Військовий сектор (CSIRT MON) діє в межах Міністерства національної оборони Польщі та забезпечує кіберзахист військової інфраструктури, а також координацію в межах національної оборонної системи. Цей підрозділ тісно пов'язаний з військовою розвідкою та іншими структурами, що займаються інформаційною безпекою у збройних силах. Фінансовий сектор (CSIRT NBP) функціонує при Національному банку Польщі та несе відповідальність за кібербезпеку фінансового сектору, включаючи банківські системи, електронні платіжні інфраструктури та обіг фінансової інформації [14]. Можна зробити висновок, що поділ національної системи реагування на кіберінциденти у Польщі на три окремих сектори дозволяє забезпечити швидке реагування на інциденти у специфічних сферах, враховуючи їх функціональні особливості та потенційні ризики.

Висновки. Зарубіжний досвід таких країн, як США, Німеччина, Польща, Франція свідчить про важливість системного, стратегічного підходу до державного регулювання у сфері протидії кіберзлочинності. Боротьба з кіберзлочинністю вимагає тісної міжнародної співпраці, оскільки злочини у кіберпросторі не визнають державних кордонів. Дослідження світових практик у цій сфері дозволяє зробити висновки, що Україна має всі передумови для вдосконалення власної системи кібербезпеки шляхом оновлення законодавства, створення ефективних інституційних механізмів, розвитку співпраці з міжнародними партнерами та залучення приватного сектору до реалізації державної політики у сфері кіберзахисту. Так, досвід США, зокрема активна взаємодія між державою та бізнесом, показує важливість розвитку публічно-приватного партнерства. В Україні варто посилити співпрацю між державними органами, критично важливими підприємствами та іншими приватними структурами для забезпечення кіберзахисту. Створення спеціалізованих органів та підрозділів, як у Польщі, має значний потенціал для оперативного реагування на кіберінциденти в окремих секторах економіки. Для України важливо запровадити подібну модель, що дозволить швидше реагувати на загрози та знизити ризики кібератак на критичну інфраструктуру, що є вкрай важливим, особливо в умовах воєнного стану.

Список використаної літератури:

1. Білєнький В. П. Відповідальність за кіберзлочини за кримінальним правом США, Великої Британії та України (порівняльно-правове дослідження): автореф. дис. … канд. юрид. наук : 12.00.08. Київ, 2016. 20 с.
2. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.

3. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України : автореф. дис. ... д-ра політ. наук : 23.00.02. Одеса, 2005. 36 с.
4. Теплицький Б. Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електроннообчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. ... канд. юрид. наук: 12.00.09. Київ, 2021. 268 с.
5. Яцишин М. Ю. Міжнародно-правове співробітництво у сфері боротьби з кіберзлочинністю : дис. ... канд. юрид. наук : 12.00.11: Міжнародне право; Нац. авіац. ун-т. Київ, 2019. URL: https://scc.knu.ua/upload/iblock/5c8/dis_Yatsyshyn_M_Y.pdf
6. United States Congress. Computer Fraud and Abuse Act of 1986, 18 U.S. Code § 1030. Fraud and related activity in connection with computers. Enacted: 1986. URL: https://www.law.cornell.edu/uscode/text/18/1030
7. Орлов О. В., Онищенко Ю.М. Узагальнення міжнародного досвіду ство– рення державної системи попередження та запобігання злочинам у мережі інтернет *Теорія та практика державного управління*. 2014. Вип. 2. С. 212-219.
8. Convention on Cybercrime. Budapest, 23.11.2001. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
9. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року N 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text
10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union.* 2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
11. Federal Office for Information Security (BSI). Operators of critical infrastructure and requirements for reporting cyber incidents. URL: https://www.bsi.bund.de
12. French National Agency for Cybersecurity (ANSSI). About the French Cybersecurity Agency (ANSSI). URL: https://cyber.gouv.fr/en/about-french-cybersecurity-agency-anssi
13. Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. Dziennik Ustaw. 2018. Nr 1560. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560
14. CSIRT Poland. National Computer Security Incident Response Team (CSIRT) Structure. URL: https://csirt.gov.pl

Kotsman I. I. FOREIGN EXPERIENCE IN STATE REGULATION OF COUNTERING CYBERCRIME

The article explores foreign experience in state regulation of countering cybercrime in European countries and the United States. The author analyzes state regulation, legal support, organizational structure, and international cooperation in the fight against cybercrime.

The experience of the United States is examined, with a focus on the Computer Fraud and Abuse Act (CFAA), which criminalizes unauthorized access to computer systems. Key agencies in this field, such as the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA), are characterized, along with their effective role in combating cybercrime through the National Cybersecurity Strategy. The importance of public-private partnerships for information sharing and developing security standards is emphasized.

The article highlights that public-private partnerships for information exchange and the development of security standards in this area are extremely important. The article further analyzes the European Union's experience in combating cybercrime and the advantages of state regulation in this direction. It notes that key documents in EU countries regarding the regulation of cybercrime are the Council of Europe's Budapest Convention and the NIS 2 Directive, which establishes cybersecurity standards for member states. Although Ukraine has ratified the Budapest Convention, its provisions have not yet been fully implemented into national legislation.

The experiences of Germany, France, and Poland are analyzed, where robust national cybersecurity systems enable rapid responses to cyber threats through multi-level organizational structures. Notably, in Germany, the Federal Office for Information Security (BSI) and in France, the National Cybersecurity Agency (ANSSI) play pivotal roles.

To enhance Ukraine's cybersecurity system, the author suggests adapting best international practices, including the establishment of specialized units, fostering cooperation between public and private sectors, and strengthening international collaboration. The need for updates to Ukrainian legislation, the creation of new institutional mechanisms, and the active involvement of the private sector in cybersecurity are underscored to ensure effective counteraction against cybercrime.

Key words: *public governance, cybersecurity, cybercrime, state regulation, public-private partnership, foreign experience in regulating the fight against cybercrime.*