Міжнародне право

УДК 004.946.5.056(4-6ЄС+73)

DOI https://doi.org/**10.5281/zenodo.15205134**

Міжнародний досвід протидії кіберзагрозам на прикладі США та ЄС

Петренко Світлана Володимирівна

науковий співробітник науково-організаційного центру Національної академії Служби безпеки України, м.Київ, вул. М.Максимовича, 22, 03022,

https://orcid.org/0000-0003-1219-2401

Прийнято: 20.03.2025| Опубліковано: 31.03.2025

Анотація. *Розвиток новітніх технологій та досягнень з кожним днем набуває все більших обертів, охоплюючи при цьому майже всі сфери людського життя. Саме тому провідні країни світу та міжнародні організації почали активно розвивати сферу захисту і протидії кіберзлочинам та загрозам, що включає в себе розвинену нормативно-правову базу, систему органів, стратегії та практики поведінки під час кіберзагроз чи список превентивних заходів, які покликані попередити їх.*

Дана стаття присвячена аналізу міжнародного досвіду боротьби з кіберзагрозами Сполученими Штатами Америки та Європейським Союзом. У ній проведено детальний аналіз ключових нормативно-правових документів США та ЄС. США є країною-лідером у сфері протидії кіберзагрозам адже одними з перших почали активно працювати над системою безпекових та превентивних заходів у боротьбі з кібезлочинами. У статті зазначено, що Америка першою прийняла Закон щодо протидії комп'терних шахрайств та зловживань. У статті наведене статистичне дослідження щодо розвитку кібербезпеки впродовж декількох наступних років.

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Наукове дослідження звертає увагу також на те, що у сфері протидії кіберзагрозам, США мають розгалужену та багаторівневу систему органів та інституцій, а також ряд домовленостей між державним та приватним секторами. Зазначається, що урядові органи та великі американські технологічні компанії-гіганти співпрацюють між собою у сфері боротьби з кіберзлочинами та розробкою попереджувальних заходів.

У статті також розглянуто основні документи, що регулюють кіберпростір у країнах Європейського Союзу, зокрема зазначено, що першим глобальним законом у сфері протидії кіберзагрозам є Конвенція Ради Європи. Також йде мова про те, що дана Конвенція була адаптована згідно з викликами сьогодення у сфері кіберпростору через прийняття до неї Другого протоколу у 2022 році.

У статті представлено Стратегію кібербезпеки ЄС та наведено п'ять основних принципів її ефективного функціонування, а також проаналізовано діяльність органів та агенцій з протидії кіберзагрозам у Європі.

Міжнародний досвід протидії кібезагрозам показує важливість комплексного підходу, який поєднує в собі всі інструменти та методи боротьби з ними.

Ключові слова: *міжнародне право, кіберзлочинність, кібератаки, кібербезпека, кібервторгнення, кібертероризм.*

International Experience in Countering Cyber Threats: the Cases of the United States and the European Union

Svitlana Petrenko

Researcher, Scientific and Organizational Center National Academy of the Security Service of Ukraine, Kyiv, Mykola Maksymovych Street, 22, 03022, https://orcid.org/0000-0003-1219-2401

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Abstract. *The rapid development of modern technologies is continuously transforming nearly all aspects of human life. In response, leading nations and international organizations have made significant efforts to establish frameworks for protecting against and countering cybercrimes and cyber threats. These efforts include the creation of comprehensive legal structures, the establishment of relevant institutions, the development of strategic policies, and the implementation of preventive measures designed to reduce the risks of such threats.*

This article focuses on analyzing the international experience of combating cyber threats, specifically through the example of the United States and the European Union. It provides a detailed analysis of the key legal documents and regulations of the USA and the EU. The United States is recognized as a leader in the field, being one of the first countries to implement a robust system of security and prevention against cybercrime. Notably, the article highlights the passage of the Computer Fraud and Abuse Act, one of the first laws in the U.S. to address cybercrimes. Additionally, the article includes statistical data on the development of cybersecurity over the years.

The research also underscores the extensive and multi-layered system of government agencies and institutions in the United States dedicated to addressing cyber threats. It emphasizes the collaboration between public authorities and major American technology companies in combating cybercrime and developing preventive measures.

The article also explores the primary legal frameworks governing cyberspace in the European Union, with particular emphasis on the Council of Europe's Convention on Cybercrime, which was the first global legal agreement targeting cyber threats. It also discusses how the Convention was updated in 2022 to address emerging challenges in cyberspace through the adoption of its Second Protocol.

Furthermore, the article presents the EU's Cybersecurity Strategy, outlining five key principles that ensure its effectiveness. It also reviews the roles of various EU agencies and bodies in tackling cyber threats.

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Overall, the international experience in combating cyber threats highlights the importance of a comprehensive, integrated approach that combines various strategies and collaborative efforts to effectively address these global challenges.

Keywords: *international law, cybercrime, cyberattacks, cybersecurity, cyber intrusion, cyberterrorism.*

Постановка проблеми. У сучасному світі поряд з стрімким розвитком новітніх технологій з'являються також і нові види кіберзлочинів та кіберзагроз, котрі постійно еволюціонують та стають дедалі складнішими за своїм складом, а за масштабом– все глобальнішими та інтернаціональними. Злочинці використовують новітні технології, штучний інтелект, щоб обійти існуючі системи захисту чи взагалі знешкодити їх. Через те що технології та методи кіберзагроз весь час вдосконалюються та адаптуються до мінливого середовища, розвиток кібербезпеки є ключовим фактором для забезпечення насамперед безпеки інформації, збереження її конфіденційності, недоторканності, котра стосується окремих осіб, компаній, міжнародних організацій чи навіть держав світу. Розвиток кібербезпеки є тим процесом, який вимагає постійного вдосконалення технологій та стратегій, що матимуть можливість реагувати на нові виклики та загрози. Саме тому запозичення та використання міжнародного досвіду у протидії кіберзагрозам та адаптація існуючої системи кібербезпеки до нових реалій є основними векторами її ефективного розвитку.

У даній статті було проведено аналіз нормативно-правової бази протидії кіберзагрозам США та Європейського Союзу, а також способів і методик реагування на них та встановлення відповідальності за вчинення правопорушень у сфері кібербезпеки. Також було досліджено систему органів, які покликані реагувати та проводити розслідування кібершахрайств.

Аналіз останніх досліджень і публікацій. Тема досвіду протидії кіберзагроз є актуальною та досліджується багатьма вченими та експертами. Її актуальність зумовлена багатьма факторами, зокрема це і значне збільшення числа кіберзлочинів протягом останніх років через зростання кількості

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

користувачів мережі Інтернет, зростаюча загроза національній безпеці країн світу, проблема конфіденційності та захисту даних, стрімкий розвиток технологій, штучного інтелекту та його похідних, складність неправовірних дій та процесів, інтернаціональність злочинів тощо.

Слід звернути увагу, шо велика кількість міжнародних організацій також активно досліджують сферу протидії кібезагрозам, особливу роль у даному процесі відграють Організація Об'єднаних Націй (ООН) та Північноатлантичний Союз (НАТО). ООН випускає ряд документів, звітів, досліджень та різних ініціатив, зокрема сюди можна віднести Резолюції Генеральної Асамблеї, звіти Групи експертів відкритого засідання, рекомендації для урядів у сфері кібербезпеки (прикладом є «Керівні принципи щодо будівництва національної кіберстійкості»), а також організації конференцій, форумів з метою розробки ефективних кіберстратегій державами світу.

Що стосується Північноатлантичного Союзу, то він також активно бере участь у процесі дотримання кіберстійкості та протидії кіберзагрозам та визначає її як частину національної безпеки будь-якої держави-члена. Це проявляється у проведенні навчань, кіберсимуляцій, котрі залучають до співпраці і партнерів по всьому світі не тільки країн-членів, а також у розробці Кіберстратегії НАТО.

Слід звернути увагу на наукові дослідження окремих вчених, котрі присвятили їх саме темі кібербезпеки та загроз, зокрема: Саєнко М.І., Савела Є.А. та Тополянський Ю.Ю., які темою роботи визначили механізми протидії кібершахрайствам та кіберзлочинності на прикладі міжнародної організації ООН [1]. Завгородня Ю.В. досліджувала роль НАТО у боротьбі з кіберконфліктами, а також його реакцію на сучасні виклики та загрози, які виникають за теперішнього світоустрою та виокремила пріоритетні напрямки розвитку його діяльності з метою протидії кіберзагрозам[2]. Тімашов В.О. та Діденко Д.Ш. зосередили увагу на вивченні теми, що стосується досвіду протидії сучасній кібезлочинності у оверлейній мережі «Даркнет» [3]. Білоборова Т.В. провела дослідження щодо міжнародного досвіду протидії кіберзлочинності органами кіберполіції, а саме переваг та позитивних аспектів [4]. Науковці

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Демидов З.Г. та Коломійцев С.О. досліджували стратегії реагування на кіберзагрози та кіберіциденти у своїй роботі [5]. Тєтєвін М.С. зосередив увагу на вивченні досвіду України у галузі міжнародного співробітництва в сфері кібербезпеки [6].

Виділення невирішених раніше частин загальної проблеми. Кібезагрози та кіберзлочинність не мають кордонів, тому можуть зачепити будь-яку країну світу, незважаючи на присутність чи відсутність нормативно-правового поля регулювання даної сфери. Тема протидії кіберзагрозам у світовій правовій практиці є надзвичайно актуальною, проте містить також і багато невирішених аспектів, зокрема це є те, що досі не створено універсального нормативного-акту та відповідних органів, котрі б регулювали відносини у сфері кіберпростору та загроз, які містяться у ньому, на глобальному рівні. До прикладу, кожна країна може мати своє законодавство у сфері кібербезпеки, проте воно суттєво відрізнятиметься від законодавства інших держав, це може призвести до складнощів у юридичному вирішенні проблеми у сфері кібербезпеки. Велика кількість країн ще й досі не мають точних визначень поняття «кіберзлочинність» у своєму законодавстві, що теж стає проблемою при їхньому вирішенні. Більше того багато з них так і не доєдналися до ратифікації Конвенції Ради Європи, котра має на меті регулювати сферу кібербезпеки на світовому рівні. Саме через це у багатьох країнах немає стандартів щодо юридичних наслідків за вчинення кіберзлочинів.

Складність створення універсального законодавства також полягає у мінливості кіберпростору та надзвичайно швидкому розвитку технологій та досягнень, які значно випереджають його. Деякі країни можуть взагалі не встигати за розвитком новітніх технологій таких як штучний інтелект, Інтернет речей, хмарні технології, розвитком криптовалюти. Дуже часто держава не в змозі здійснювати моніторинг за всіма кіберзлочинами, котрі з'являються у нових формах та видах.

З метою ефективного вирішення даних проблемних аспектів, які виникають у сфері кібербезпеки, країнам слід співпрацювати між собою з метою

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

створення єдиного, уніфікованого законодавства, адаптації його до своєї нормативно-правової бази, покращення власних законів у цій сфері, а також забезпеченні відповідного контролю за його виконанням, розвитком новітніх технологій з обов'язковим дотриманням прав та свобод людини.

Формулювання цілей статті (постановка завдання). Метою наукового дослідження є аналіз досвіду у боротьбі з кібершахрайствами, дослідження правових інструментів та системи органів, котрі покликані регулювати сферу протидії кіберзагрозам в США та ЄС через призму актуальних питань та викликів кіберсвіту у теперішній час.

Завдання статті:

1. Оцінити поточний стан нормативно-правового законодавства США та системи органів у сфері протидії кіберзагрозам.
2. Проаналізувати міжнародний досвід та місце на світовій арені ЄС у сфері протидії кіберзагрозам.
3. Розробити рекомендації щодо покращення законодавства у сфері кібербезпеки з урахуванням розвитку новітніх технологій та досягнень людства.

Виклад основного матеріалу дослідження. Згідно з прогнозом провідної світової дослідницької і консалтингової компанії у сфері інформаційних технологій Gartner у 2025 році світові витрати на кібербезпеку будуть становити 212 млрд дол. США, що є на 15,1 % більше, ніж у попередньому році. Також у дослідженні вказано, що до 2027 року 17% кібератак будуть залучати до своєї діяльності генеративний штучний інтелект. Прогнозується, що світовий ринок кібербезпеки буде зростати з щорічним показником 7,92% до 2029 року [7].

Слід зазначити, що провідні держави світу почали активно працювати у сфері протидії кіберзагрозам ще у XX столітті, а в Україні даний процес почав розвиватися тільки у 2000-их роках та перебуває на початковому етапі свого розвитку у даний період часу.

Сполучені Штати Америки є тією країною, котра однією з перших почала розробляти нормативно-правову базу, яка регулює кіберпростір та всі негативні

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

явища, які можуть виникати у ньому. Перший кіберзлочин відбувся саме у США у далекому 1969 році і на Конференції Американської Асоціації адвокатів у 1975 році вперше було визначено поняття «кіберзлочин» та описано його властивості [8, с.498]. А вже у 1986 році у США був прийнятий перший документ протидії кіберзлочинам під назвою «Закон про комп'ютерне шахрайство та зловживання» (Computer Fraud and Abuse Act (CFAA)), який встановлює кримінальну відповідальність за злочини, які пов'язані з використанням комп'ютерних систем, а саме несанкціонований доступ до комп'ютерних систем, зловживання доступом, крадіжку конфіденційних даних, пошкодження чи видалення інформації та цивільні санкції за його порушення.

Крім даного закону, Америка має також розвинену правову базу для боротьби з кіберзлочинністю, яка включає низку законів і нормативних актів, зокрема це і «Закон про конфіденційність електронних комунікацій» (прийнятий у 1986 році), який здійснює захист конфіденційності електронних комунікацій та регулює доступ до телефонних дзвінків, електронної пошти з метою обмеження їх неправомірного перехоплення. Також слід звернути увагу на вагомий акт в історії американської боротьби з кіберзлочинністю та тероризмом, а саме «Закон про об'єднання та зміцнення Америки шляхом надання відповідних засобів, необхідних для перехоплення та перешкоджання тероризму» (USA PATRIOT), прийнятий у 2001 році, котрий надає ширші повноваження правоохоронним органам у боротьбі з тероризмом та кіберзлочинністю. Ще одним не менш важливим законом є «Закон про захист кібербезпеки», прийнятий у 2015 році. Даний нормативний акт заохочує співпрацю між державними та недержавними органам щодо обміну інформацією про кіберзагрози, що дозволяє пришвидшувати процес реагування на ті чи інші злочини, а також він вдосконалює інформаційну безпеку країни, враховуючи захист критичної інфраструктури від кіберзагроз.

Загалом у США існує ціла багатогранна система у протидії кіберзлочинності, зокрема сюди входять і спеціалізовані федеральні агентства, законодавчі ініціативи та домовленості між державними та приватними

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

секторами. Одним з таких агентств є Федеральне бюро розслідувань (ФБР), котре займається розслідуваннями у сфері кіберзлочинів, враховуючи фінансові махінації, крадіжки інформації, розслідування самих кіберзлочинів. Слід зазначити, що дане бюро співпрацює з іншими країнами, міжнародними партнерами з допомогою різних програм, зокрема це стосується співпраці з Інтерполом, Європолом.

Ще одним членом системи протидії та боротьби з кіберзлочинністю США є Національний центр кібербезпеки та комунікацій, який є підрозділом Міністерства внутрішньої безпеки США та працює в основному з урядовими установами та приватними компаніями з метою захисту критично важливої інфраструктури від хакерських посягань [9, с.21].

Вагому роль у боротьбі з кіберзлочинами відіграє також Міністерство національної безпеки США, яке здійснює співпрацю з іншими федеральними органами для проведення кримінальних розслідувань, спрямованих і в тому числі на боротьбу з кіберзлочинністю, а також розробляє інструменти та методики боротьби з нею. До його складу входять Секретна служба та Міграційна та митна правоохоронна служба США, котрі в свою чергу містять спеціальні підрозділи, що працюють у сфері боротьби з кіберзагрозами та злочинами. Зокрема у Секретній службі є спеціальні підрозділи з електронних злочинів, котрі розшукують міжнародних кіберзлочинців, які здійснюють злочини пов’язані з банківським сектором, кібервторгненнями чи витоком інформації. А Центр кіберзлочинів при Міграційній правоохоронній службі США надає технічну комп'ютеризовану підтримку з питань розслідувань міжнародних злочинів та проводить навчання навикам комп’ютерного розслідування [10,с.154].

Слід також зазначити, що США активно співпрацює з великими технологічними компаніями такими як Microsoft, Google, Apple у сфері боротьби з кіберзлочинністю, їхнього розслідування та забезпечення захисту конфіденційних даних своїх безпосередніх користувачів. Дані компанії часто співпрацюють з Федеральним бюро розслідувань та Інтерполом з метою

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

виявлення, ідентифікації та заблокування шкідливих акаунтів зловмисників чи підозрюваних у вчиненні кібершахрайств. А якщо це енергетичні, комунікаційні чи фінансові компанії, то між урядом та ними відбувається співпраця щодо захисту критично важливої інфраструктури від кібератак. Технологічні компанії також активно співпрацюють з урядом у сфері боротьби з шкідливим програмним забезпеченням.

Сполучені Штати Америки розробили розгалужену та досить ефективну систему протидії та боротьби з кіберзагрозами і злочинами, про що свідчать потужна нормативно-правова база та органи, котрі здійснюють боротьбу з кібезлочинністю. Загалом слід зазначити, що боротьба з кіберзлочинністю у США ведеться на трьох рівнях: правоохоронному, юстиційному та військовому [11, с.135].

США стали одним з основоположників у сфері протидії та боротьби з кіберзлочинністю у світі, тому країни Європи почали так само активно розробляти відповідне законодавство. Головним документом, котрий регулює дану проблему є Конвенція Ради Європи про кіберзлочинність або Будапештська конвенція, ратифікована у 2004 році. Вона є першим правовим інструментом, що ставить за мету боротьбу з кіберзлочинністю на глобальному рівні. Конвенція передбачає кримінальну відповідальність за різноманітні види кіберзлочинів, зокрема мова йде про проникнення в комп’ютерні системи, поширення шкідливого програмного забезпечення, кібертероризм, порушення авторського права в мережі Інтернет. Країни-підписанти даної Конвенції гармонізували своє законодавство у сфері боротьби з кіберзлочинністю відповідно до неї. Конвенція про кіберзлочинність є важливим етапом у створенні правової бази для боротьби з кіберзлочинністю у Європі.

Слід також зазначити, що у 2022 році було прийнято Другий протокол до Будапештської конвенції під назвою «Про злочини, пов’язані з кібепростором», який має на меті оновити та адаптувати Будапештську конвенцію згідно з теперішніми викликами часу, новими тенденціями та розвитком інновацій та новітніх технологій [12].

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

В ЄС також було прийнято низку нормативно-правових актів з метою протидії та боротьби з кіберзлочинами, а саме: Директива ЄС щодо протидії кібератакам на інформаційні системи, Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет та Стратегія кібербезпеки.

Стратегія кібербезпеки є першим стратегічним документом, який покликаний забезпечувати кібербезпеку на всіх рівнях ЄС, враховуючи і попереджувальні заходи, а також можливу відповідальність за скоєні злочини. У 2020 році Стратегія була оновлена та прийнята до 2030 року. Вона поставила за мету покращити рівень захисту критичної інфраструктури від кібератак, вдосконалити процес захисту даних та сприяти підвищенню розвитку нових технологій у сфері кібербезпеки [13,с.15].

Стратегія виокремлює п’ять головних постулатів щодо гармонізації принципів розвитку кібербезпеки у країнах-членах Європейського Союзу:

1.Значне зменшення кібезлочинності.

2.Досягнення відповідного рівня кіберстійкості.

3.Створення технологічних ресурсів для забезпечення кібербезпеки.

4.Створення заходів політики кібероборони та підвищення зростання у сфері кібербезпеки.

5. Розробка послідовної міжнародної політики ЄС у даній сфері з обов’язковим дотриманням всіх цінностей Співтовариства [14].

У ЄС є кілька органів та агенцій, які забезпечують протидію кіберзагрозам, а саме Агентство ЄС з питань мережевої та інформаційної політики, Агентство з питань європейської політики безпеки та оборони, Центр реагування на кіберінциденти, Європейський центр з боротьби з кіберзлочинністю, Європейська рада з кібербезпеки та інші.

Агентство ЄС з питань мережевої та інформаційної політики є головним органом, котрий підтримує співпрацю між членами Союзу у сфері кібербезпеки. Головна мета його діяльності – це покращення інформаційної та мережевої

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

безпеки в ЄС, сприяючи при цьому розвитку мережевої культури на користь громадян ЄС [15].

Отже, Європейський Союз як і Сполучені Штати Америки також активно працює у зміцненні та розробці превентивних заходів у сфері кібербезпеки, створивши цілу систему для боротьби та протидії з кіберзагрозами, дотримуючись високого рівня співпраці та обміну інформацією між державами-членами, надаючи консультативну міжнародну підтримку. Потужна нормативно-правова база, система органів та агентств, міжнародна співпраця дозволяють зберігати стабільність і безпеку у цифровому середовищі ЄС, а також дотримуватися цінностей, котрі пропагуються у ньому.

Висновки. Враховуючи значну цифровізацію та автоматизацію суспільних і виробничих процесів, можна зробити висновок, що проблема протидії кіберзлочинам та розвитку кібербезпеки набуває все більшої актуальності та важливості. Держави та міжнародні організації щодня постають перед новими викликами, які виникають та стосуються передусім захисту їхньої національної безпеки через призму кібербезпеки. Як бачимо, США та країни ЄС створили ефективну систему протидії та захисту своєї безпеки у інформаційному просторі, проте це не завжди відбувається успішно, бо сучасна нормативно-правова база все ж таки відстає від розвитку новітніх технологій. Незважаючи на всі досягнення та розробки урядів, міжнародних організацій у сфері протидії кіберзагрозам, кількість та складність кібератак, кіберзлочинів тільки зростає з кожним роком, адже вони вимагають постійного оновлення, розробки та адаптації все нових і нових механізмів та методик протидії та захисту. Дана протидія повинна стати пріоритетом у розвитку правової політики кожної держави світу та міжнародної організації з метою подолання цієї проблеми.

Список використаних джерел

1. Саєнко М.І., Савела Є.А. та Тополянський Ю.Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. Науковий вісник

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Ужгородського Національного Університету, серія ПРАВО. Ужгород, 2021. Вип. 64. С. 386-391.

2. Завгородня Ю.В. Роль НАТО у боротьбі з кіберконфліктами: політико-правовий аспект. Регіональні студії. Ужгород, 2022. Вип. 30. С. 62-65.

3. Тімашов В. О., Діденко Д. Ш. Міжнародний досвід протидії сучасній кібезлочинності в мережі «Даркнет». Південноукраїнський правничий часопис. Одеса, 2021. Вип.1. С. 167-172.

4. Білоборова Т.В. Міжнародний досвід протидії кібезлочинності органами кіберполіції. Право і суспільство. Київ, 2020. Вип.3. С. 121-126.

5. Демидов З.Г., Коломійцев С.О. Стратегія реагування на кіберзагрози та кіберінциденти. Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VIII Міжнародної науково- практичної конференції (м. Дніпро, 15 бер. 2024 р.); у 2-х част. Дніпро. 2024.С. 331-333.

6. Тєтєвін М.С. Досвід України в галузі міжнародного співробітництва в галузі кібербезпеки. Науковий вісник Ужгородського національного університету, серія ПРАВО. Ужгород, 2024.Вип. 82: частина 3. С.263-266.

7. Gartner Forecasts Global Information Security Spending to Grow 15% in 2025. URL:{ https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025} (дата звернення: 07.03.2025).

8. Голін І.В. Боротьба з кіберзлочинами: досвід окремих зарубіжних країн. ДВНЗ Ужгородський національний університет, Аналітично-порівняльне правознавство. Ужгород, 2025.Вип.1.С. 497-501.

9. Аніщук В.В., Зицик С.Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. Науковий вісник Ужгородського національного університету, Серія: Право. Ужгород, 2024. Вип.83. С. 19-23.

10. Колосов О.О. Особливості протидії кіберзлочинам у Сполучених Штатах Америки. Ірпінський юридичний часопис: науковий журнал. Ірпінь, 2023. Вип.1(10). С. 151-160.

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

11. Буяджи С.А. Особливості правового регулювання боротьби з кіберзлочинністю у США. Lex portus,2017.Вип.2. С. 130-141.

12. Карвацька С., Іванюк Р. Будапештська конвенція про кіберзлочинність як основний міжнародно – правовий стандарт щодо кіберзлочинності. URL: {https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist/} (дата звернення: 10.03.2025).

13. Марущак А.І. Європейський досвід з питань боротьби з правопорушеннями в інформаційній сфері. Український науковий журнал інформаційної безпеки. Київ, 2019. Вип.1. С. 13-17.

14. Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń. Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu ekonomiczno-społecznego i Komitetu regionów. URL: {https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52013JC0001} (дата звернення: 17.03.2025).

15. Our vision: A Trusted and Cyber Secure Europe. European Union Agency for Cybersecurity. URL: {https://www.enisa.europa.eu/about-enisa/what-we-do} (дата звернення: 19.03.2025).

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license