Кримінальна відповідальність у цифровому просторі: співпраця між Україною та Польщею щодо протидії кіберзлочинності

Сийплокі Микола Васильович[1], Мудролюбова Наталія Олександрівна[2], Лівак Антон Петрович[3]

Опубліковано	Секція	УДК
24.06.2024	Право	343.97

DOI: https://doi.org/10.5281/zenodo.12512624

Ліцензовано за умовами Creative Commons BY 4.0 International license

Анотація. В сучасних умовах, особливо на період російсько-української війни, авторами досліджуються глобалізаційні загрози у цифровому середовищі. У статті наголошується на необхідності адаптації національної політики інформаційної безпеки до конкретних викликів. Інформаційна безпека є одним з ключових напрямків національної політики, адже вона спрямована на захист інтересів та основоположних прав і свобод громадян в умовах, зокрема, інформаційної війни. Координація дій між силовими структурами, органами влади, місцевого самоврядування та громадянським суспільством має вирішальне значення для протидії реальним і потенційним загрозам, які становлять виклик у сучасному глобалізованому світі.

Аргументовано, що основою забезпечення інформаційної безпеки є створення прогресивної нормативно-правової бази, яка включає нормативно-правові акти, спрямовані на управління цифровою інформацією та захист комунікаційних систем. Реалізація розглянутих у статті напрямів забезпечення інформаційної безпеки вимагає від держави комплексного підходу до, зокрема, протидії дезінформації, розвитку медіаграмотності громадян, захисту персональних даних, забезпечення свободи слова, підтримання комунікації з громадянами.

Автори наголошують на важливості дотримання балансу між захистом інформації та захистом конституційних прав і свобод особи в контексті побудови ефективної системи інформаційного суспільства.

Зазначено, що для досягнення загальної превентивної мети стратегія інформаційної безпеки має включати інноваційні підходи до кібербезпеки, особливо в частині захисту критичної інфраструктури та персональних даних громадян відповідно до міжнародних стандартів, зокрема, використання підходів, отриманих в ході українсько-польського співробітництва..

Обґрунтовано, що протидія сучасним національним та глобальним викликам у сфері інформаційної безпеки залежить від формування національних та міжнародних

[1] Доктор юридичних наук, професор, кафедра кримінального права та правоохоронної діяльності, юридичний факультет, Державний вищий навчальний заклад "Ужгородський національний університет", ORCID: https://orcid.org/0000-0001-6131-9179

[2] Кандидат юридичних наук, Доцент, кафедра теорії та історії держави і права, Навчально-науковий інститут права та політології, Український державний університет імені Михайла Драгоманова, ORCID: https://orcid.org/0000-0002-8594-3053

[3] Кандидат юридичних наук, Голова АО IMG Partners; Адвокат, Адвокатська компанія АО IMG Partners, ORCID: https://orcid.org/0000-0003-1950-1609

стратегій кібербезпеки, а також від залучення країн, які поділяють спільні цілі захисту даних та приватності в цифровому середовищі, наголошуючи на необхідності постійного технічного та технологічного розвитку.

Ключові слова: міжнародне право, аналіз кіберзагроз, боротьба з кіберзлочинністю, інформаційна безпека, цифрове середовище, українсько-польське співробітництво.

Criminal liability in digital space: cooperation between Ukraine and Poland in combating cybercrime

Annotation. In the current context, especially during the Russian-Ukrainian war, the authors study globalisation threats in the digital environment. The article emphasises the need to adapt the national information security policy to specific challenges. Information security is one of the key areas of national policy, as it is aimed at protecting the interests and fundamental rights and freedoms of citizens in the context of, *inter alia*, information warfare. Coordination of actions between law enforcement agencies, government, local self-government and civil society is crucial to counteract real and potential threats that pose a challenge in today's globalised world.

It is argued that the basis for ensuring information security is the creation of a progressive legal framework, which includes regulations aimed at managing digital information and protecting communication systems. Implementation of the areas of information security discussed in the article requires a comprehensive approach from the State to countering disinformation, developing media literacy of citizens, protecting personal data, ensuring freedom of speech, and maintaining communication with citizens.

The authors emphasise the importance of maintaining a balance between information protection and protection of constitutional rights and freedoms of an individual in the context of building an effective information society system.

It is noted that to achieve the overall preventive goal, the information security strategy should include innovative approaches to cybersecurity, especially in terms of protecting critical infrastructure and personal data of citizens in accordance with international standards, in particular, the use of approaches obtained in the course of Ukrainian-Polish cooperation.

It is substantiated that counteracting current national and global challenges in the field of information security depends on the formation of national and international cybersecurity strategies, as well as on the involvement of countries that share common goals of data protection and privacy in the digital environment, emphasising the need for continuous technical and technological development.

Keywords: international law, analysis of cyber threats, combating cybercrime, information security, digital environment, Ukrainian-Polish cooperation.

Вступ

Постановка проблеми. Глобальна цифровізація суспільства, загалом, призвела до підвищення ролі інформаційно-комунікаційних технологій та мережі Інтернет, які дали значний поштовх розвитку практично всіх галузей. Не потрібно порівнювати, для чого використовувались телефони ще 15 років тому, і з якою метою вони використовуються наразі. Те саме можна вказати і про суспільну веб-мережу, яка, на жаль, використовується не тільки заради «добрих цілей».

У зв'язку із зазначеним, зросла потреба для держави та її міжнародних партнерів в забезпеченні скоординованих дій щодо реалізації функцій кібербезпеки з боку держави.

У сучасних умовах усі країни світу застосовують інноваційні стратегії для розв'язання глобальної проблеми захисту цифрової інфраструктури та даних,

усвідомлюючи значні негативні наслідки загрози кібератак, зокрема, вірусів, і нанесення збитків через це.

Аналіз останніх досліджень і публікацій. Питання, пов'язані з підвищенням безпеки у цифровому просторі та попередженню кіберзлочинності, досить широко розглянуто у працях різних науковців. Авторами статті розглянуто праці таких науковців, зокрема: Головко Д.Ю., Довгань Б.В., Кисленко Д.П., Столбовий В.М., Шевчук М.О., Юртаєва К.В. та інші, щоб проаналізувати та виділити конкретні аспекти інформаційної безпеки сьогодення та запропонувати можливі варіанти подальшого розвитку у вказаній сфері.

Метою цієї статті є вивчення правового регулювання інформаційної безпеки в Україні з метою ефективної протидії цифровій злочинності, що передбачає аналіз правових норм і положень, що регулюють захист інформації в цифровому просторі, та оцінку їх ефективності в контексті превентивних заходів протидії кіберзлочинності та іншим формам злочинності у сфері цифрових технологій.

Завданням цієї статті є дослідження співпраці українських та польських методів протидії злочинам у цифровій сфері, та встановлення того, що Україна могла б запозичити та використовувати з того, що на практиці використовує Республіка Польща. Для виконання мети та завдання цієї статті, авторами використовуються такі теоретичні методи емпіричного дослідження як опис, порівняння, аналіз і синтез.

Результати

Інформаційна безпека сьогодні не обмежується лише захистом даних від несанкціонованого доступу [1, с. 45]. Інформаційну безпеку варто вважати правовим явищем, оскільки вона має чітке законодавче підґрунтя та регулюється низкою нормативно-правових актів на національному та міжнародному рівнях [2, с. 295].

Яровенко Г.М. відзначає, що, не дивлячись на зростання впливу інформаційних загроз на різні види та сфери діяльності людини, спостерігається позитивна тенденція щодо використання населенням комп'ютерних та мобільних технологій, додатків, мережі Інтернет для здійснення операцій фінансово-економічного характеру, що може говорити про зростання довіри до них [3, с. 192]. Під кіберзлочинністю можна розуміти будь-яку протиправну діяльність у цифровій сфері, отже, кібербезпека охоплює також кібертероризм, кібершпигунство, дезінформацію та інше. У той же час, кіберзлочини в українському законодавстві охоплені положеннями статей 361 та 361-1 Кримінального кодексу України [4].

Форос Г.В. та Шимко Д.С. визначають, що кіберзлочин – це суспільно небезпечне діяння у кіберпросторі або з його використанням, яке підлягає відповідальності відповідно до національного законодавства, зокрема, Кримінального кодексу України та міжнародних договорів України, а його основною метою є руйнування або незаконне заволодіння інформацією в інформаційних системах [5, с. 42].

До кіберзлочинів варто також віднести злочини, об'єктом яких є не лише комп'ютерні дані інформаційних систем, але й злочини, які вчиняються з використанням кіберпростору, наприклад, торгівля наркотиками через Інтернет, поширення дитячої порнографії, протиправні дії з платіжними картками тощо. [6, с. 126]. Кіберзлочинність завдає сильні економічні збитки як фізичним особам, так і юридичним, до прикладу – масштабна хакерська атака у червні 2017 року "Petya.A" втрутилась і навіть заблокувала на певний час роботу не одного державного і приватного підприємства, зокрема: аеропорту Бориспіль, Укртелекому, ЧАЕС, Укрзалізниці, Кабінету Міністрів України тощо [6, с. 126-127].

Також відомий сценарій із вимаганням грошового забезпечення за повернення викрадених даних. Так, у листопаді 2021 року в Польщі затримали громадянина України, якого підозрювали у зламі американської компанії, що спеціалізується на розробці програмного забезпечення для інфраструктури. Внаслідок кібератаки було

паралізовано роботу щонайменше 200 компаній у США, 800 шведських супермаркетів, 11 шкіл Нової Зеландії і двох IT-компаній Данії. Підозрюють, що за атакою на компанію стояло хакерське угруповання з «REvil», кіберзлочинці якого вимагали 70 мільйонів доларів викупу в криптовалюті для повернення вкраденої ними інформації. Підозрюваному українцю загрожувало до 115 років ув'язнення за повідомленням на веб-сайті Департаменту юстиції США, а його спільника, громадянина Росії, якого ще не вдалося затримати, очікують до 145 років позбавлення волі [7, с. 302].

Відповідно, правове регулювання у цій сфері має включати законодавство, спрямоване на запобігання таким загрозам, виявлення порушень та покарання винних. Ефективне правове регулювання інформаційної безпеки потребує наявності чітких і конкретних нормативно-правових актів, які визначають права та обов'язки суб'єктів у цій сфері, процедури виявлення та реагування на інциденти, а також механізми міжнародного співробітництва у цій сфері [1, с. 45-46]

Варто звернути увагу, що ст. 361 КК України криміналізує не доступ до комп'ютерної інформації, а несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних, комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, адже саме це втручання має деструктивний характер, оскільки полягає у зміні режиму роботи вказаних вище систем і мереж [8, с. 410]

Що ж стосується кримінальної відповідальності за українським законодавством, то, відомо, що це є видом юридичної відповідальності, тому варто почати із визначення складу вказаних вище злочинів. У науковій літературі та на практиці нерідко ототожнюють поняття «суб'єкт злочину» і «особа злочинця», коли мова йде про суб'єкта злочину як один з чотирьох елементів складу злочину [9, с. 81].

Варто зазначити, що суб'єкт злочину характеризується *сукупністю* обов'язкових ознак, та деколи факультативних, визначених складом конкретної кримінально-правової норми (загальний та спеціальний суб'єкт). Таким чином, під суб'єктом розуміється не конкретна людина, особа, а юридична *умовність*, що є сукупністю ознак, які визначають правовий, віковий і психічний статус особи, відповідальної за вчинення злочину [9, с. 81].

Суб'єктом злочину за загальним правилом є фізична осудна особа, якій на момент вчинення злочину виповнилося 16 років [9, с. 81]. Відповідно до положення ст. 361 КК України, суб'єкт вказаного злочину є загальним, а вина характеризується умислом (прямим – до дій, прямим чи непрямим – до наслідків діяння) [10], тоді як за ст. 361-1 КК України вина характеризується лише прямим умислом [11]. Відносно віку притягнення до кримінальної відповідальності за несанкціонований доступ до ЕОМ зарубіжні законодавці також не досягли єдності, що пов'язано з різними підходами у встановленні віку кримінальної відповідальності, що, наприклад, у Польщі становить 15 років [12, с. 106].

Об'єктом посягання можна визначити електронно-обчислювальні машини, комп'ютери, автоматизовані системи, комп'ютерні мережі, мережі електрозв'язку, їх нормальну роботу [10, 11]. А об'єктивна сторона прямо вказана у диспозиції відповідних статей.

Юртаєва К.В. у своїх працях цілком погоджується і вважає слушною пропозицію Мовчана Р.О. кваліфікувати кібератаки Російської Федерації як одну з форм диверсії у зв'язку із наступним: згадані у ч. 4 ст. 361 КК України «потенційні наслідки» у вигляді «тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків» фактично повністю охоплюються положенням статті 113 КК України (диверсія). Додатково, Мовчан Р.О. пропонує кваліфікувати кібератаки та диверсію за сукупністю, тобто відповідно ч. 1-3 ст. 361 КК України та ч. 1 ст. 113 КК України (за умови, коли правовий режим воєнного стану не

запроваджений) або ч. 5 ст. 361 КК України та ч. 2 ст. 113 КК України (в умовах вчинення злочину під час воєнного стану) [8 , с. 411]

Однак, лише розуміння різновидів кіберзлочинів не є достатнім для ефективної боротьби, тому Чекмарьова І.М. поділилась стратегіями протидії онлайн шахрайству [13, с. 643]:

●захист інформації – використання надійного шифрування для захисту конфіденційної інформації та регулярне поновлення системи безпеки;

●медіаосвіта – організація навчання для персоналу і не тільки з метою вчасного розпізнавання та запобігання кіберзлочинам;

●моніторинг мережі – постійний контроль мережі на наявність шкідливого програмного забезпечення та надзвичайних активностей;

●співпраця з іншими організаціями – встановлення партнерських зв'язків з іншими агентствами, включаючи військові підрозділи;

●розробка кризового плану – створення плану реагування на кібератаки та інші загрози.

Літвінова Ю.О. та Мельник М.І. вважають, що посилення санкцій та додаткова криміналізація окремих діянь можуть частково стримати потенційних злочинців від вчинення нових кримінальних правопорушень, тому запровадження відповідальності за злочини, вчинені під час воєнного стану, є важливим [14, с. 55]

Так, 16.01.2024 Верховна Рада України прийняла в першому читанні за основу законопроєкт «Про внесення змін до Кримінального кодексу України щодо встановлення кримінальної відповідальності за несанкціоноване втручання, збут або розповсюдження інформації, що оброблюється в публічних електронних реєстрах та посилення кримінальної відповідальності під час дії воєнного стану за кримінальні правопорушення у сфері використання інформаційно-комунікаційних систем» (№10242), який наразі очікує на друге читання [15].

Вказаним законопроєктом запропоновані такі зміни до чинного КК України [16]:

1. Встановлення кримінальної відповідальності за:
   - неправомірне втручання в роботу електронних реєстрів (внесення змін до ст. 361 КК України);
   - незаконне заволодіння та поширення інформації з обмеженим доступом з електронних реєстрів (внесення змін до ст. 361-2 КК України);
   - блокування та перешкоджання роботі інформаційно-комунікаційних систем і електронних реєстрів (внесення змін до ст. 363, 363-1 КК України);
   - зловживання повноваженнями публічного реєстратора з корисливою метою (внесення змін до ст. 365-2 КК України);
2. Посилення покарання за:
   - злочини у цифровій сфері, вчинені під час дії воєнного стану (внесення змін до ст. 361-1, 361-2, 362 КК України);
   - втручання в роботу електронних реєстрів і поширення конфіденційної інформації з них, вчинені службовими особами (внесення змін до ст. 361, 361-2 КК України);
3. Приведення законодавства про кримінальну відповідальність у відповідність до Закону України «Про публічні електронні реєстри»;
4. Забезпечення ефективнішого кримінально-правового захисту електронних реєстрів та інших об'єктів критичної інформаційної інфраструктури;
5. Гармонізація національного законодавства з нормами міжнародного права у сфері цифрової безпеки;
6. Посилення протидії кіберзлочинності та загрозам національній безпеці в інформаційній сфері.

Таким чином, визнаючи проблему кібератак, українські законодавці вносять відповідні зміни та доповнення до кримінального та адміністративного законодавства із урахуванням міжнародного право, що у процесі сприяє удосконаленню основ та процедур притягнення осіб до відповідальності [5, с. 42].

Крім того, комплексним стратегічним планом реформування правоохоронних органів як частини сектору безпеки і оборони України на 2023-2027 роки передбачено необхідність посилити спроможність державних органів, зокрема, прокуратури, у напрямку боротьби з внутрішніми та зовнішніми загрозами у цифровій сфері [17, с. 180-181].

Важливим компонентом стає впровадження систем моніторингу та реагування в режимі реального часу, що дозволяє оперативним чином виявляти та зреагувати на потенційно небезпечні події [6, с. 127].

У зв'язку із цим, Гунько І. пропонує запровадити наступні методи тестування програмного забезпечення, що також може вплинути на процеси у сфері цифрової безпеки [18, с. 31-32]:

- Використання штучного інтелекту та машинного навчання, що, зокрема, матимуть змогу прогнозувати дефекти у програмах;
- Автоматизація тестування, що пов'язане з практиками DevOps;
- Інтеграція технології блокчейн;
- Етичні міркування при тестуванні, зокрема, щодо конфіденційності даних користувачів;
- Віртуалізація даних, автоматизація інфраструктури й контейнеризація можуть допомогти розв'язати проблеми із середовищем тестування;
- Автоматизація обслуговування сценаріїв, вибір інструментів та комплексного покриття тестів.

Столбовий В.М. та Кисленко Д.П. виділяють наступні підходи забезпечення стійкості держави до кіберзагроз [17, с. 181]:

- моніторинг засобів кібератак (систематичний аналіз нових технологій, методів та загроз, що виникають у сфері кібербезпеки);
- аутсорсинг функцій (залучення фахівців із кібербезпеки для виконання необхідних завдань або послуг – аудиту безпеки, розробки захисних стратегій та впровадження технологій);
- державні програми посилення кіберстійкості (стратегічні програми, фінансування досліджень, створення та впровадження стандартів безпеки);
- розширення міжнародного співробітництва (обмін інформацією, фахівцями та досвідом, спільні навчальні програми, спільна діяльність);
- технічне забезпечення (передові технології та захисні засоби, системи виявлення інцидентів, захист мережі, шифрування даних, багатофакторна аутентифікація).

Дикий А.П. і Барановська Т.В. погоджуються з твердженням Грицишена Д.О. про те, що «реалізація правоохоронної функції держави має відбуватися як з позиції реалізації внутрішньої політики, так і зовнішньої, зокрема в частині взаємодії із міжнародними правоохоронними організаціями» [19, с. 274]. Калініна М.Р. відзначає наступні пріоритети міжнародної політики ЄС у кіберпросторі [20, с. 436-437]:

- свобода та відкритість: стратегія визначає принципи реалізації основних прав людини та громадянина у кіберпросторі;
- застосування законодавства ЄС у кіберпросторі;
- розвиток потенціалу кібербезпеки через співпрацю (міжнародні партнери та організації, приватні компанії, громадянське суспільство).

Так, у 2019 році в рамках постійно діючої операції «MISMED», за участі України, Польщі та Франції та підтримки Європолу та Євроюсту, було викрито злочинну групу та заарештовано 9 осіб, які займались міжнародними переміщеннями замінника героїну,

вартістю 100 тис. доларів США. В 2020 році в рамках цієї ж операції було здійснено 165 арештів осіб, які займалися реалізацією підроблених медикаментів, викрадених протиракових і допінгових препаратів [19, с. 280]. Правову основу для протидії кіберпосяганням у Європейському Союзі безпосередньо визначає Будапештська Конвенція Ради Європи з кіберзлочинності, учасниками якої є не тільки країни Європи, а й інші (США, Аргентина, Австралія, Чилі, Японія та інші) [21, с. 100].

Стратегія інформаційної безпеки України передбачає, зокрема, активне залучення до міжнародного співробітництва в сфері кібербезпеки та обміну досвідом з іншими країнами, оскільки наша країна прагне підтримувати спільні стандарти та процедури для захисту інформації, відповідати їм, а також взаємно надавати допомогу у рамках міжнародного співробітництва. Міжнародне співробітництво у сфері кіберзахисту відіграє ключову роль у зміцненні національної та глобальної інформаційної безпеки [2, с. 296].

Задля створення організаційних передумов для проведення спільних розслідувань кіберзлочинів у 2013 році в ЄС у складі Європолу було створено Європейський центр по боротьбі з кіберзлочинністю (European Cybercrime Centre), основними завданнями якого передбачено: забезпечення обміну інформацією між підрозділами правоохоронних органів ЄС та третіми країнами; боротьба з розповсюдженням у мережі Інтернет дитячої порнографії; підготовка кваліфікованих кадрів у сфері боротьби з кіберзлочинністю; розробка методики виявлення і припинення злочинів у сфері інформаційних технологій тощо. Своєрідною "підслідністю" ЕСЗ є кіберзлочини, які: скоєні міжнародними злочинними угрупованнями з метою отримання значних прибутків, або у результаті діяльності яких було завдано значної шкоди; завдають значної шкоди потерпілим, зокрема, кібернасильство, сексуальна експлуатація дітей онлайн, розповсюдження порнографії тощо; завдають шкоди критичній інфраструктурі країн-членів ЄС [21, с. 101].

Так, окремої уваги заслуговує досвід Польщі у протидії кіберпосяганням, який свідчить про важливість стратегії, нормативних актів, впровадження їх в життя, ведення підготовки фахівців у сфері кібербезпеки, а також контролю окремих установ, підприємств і громадян, міжнародної співпраці, а також безперервного розвитку в цій сфері [21, с. 100]. Особливістю Стратегії Польщі у цифровому просторі є те, що в ній закріплено необхідність розглянути можливість правового регулювання так званих програм «bug bounty», завдяки яким люди можуть вносити корективи до роботи певної програми, виправляючи помилки та отримуючи винагороду [22, с. 164]

Польща бере активну участь у реалізації політики ООН, НАТО та ЄС, а також на оперативному рівні співпрацює з Чехією, Словаччиною, Угорщиною та Австрією у межах Центральноєвропейської платформи кібербезпеки [21, с. 102]. Досвід Польщі цікавий для України тим, що там створено Урядовий центр безпеки (RCB) задля створення ефективної та всебічної системи антикризового управління: надвідомча структура, спрямована на оптимізацію та стандартизацію сприйняття загроз окремими урядовими відомствами з метою підвищення їх здатності вирішувати складні ситуації [21, с. 102].

Цікавим для врахування Україною є приклад функціонування Національного науково-дослідного інституту Польщі (NASK), яким керує Міністерство цифрових справ Польщі і основна функція якого – забезпечення інформаційної безпеки у Інтернеті, оскільки NASK – це польський національний реєстратор імен в домені.pl; NASK керує центром стратегічного аналізу щодо кібербезпеки; команда швидкого реагування CERT Polska також діє в структурі NASK; у цій установі створена платформа для державного та приватного партнерства [21, с. 103].

Крім того, NASK здійснює науково-дослідну діяльність у галузі безпеки, надійності та ефективності мереж ІКТ, зокрема CyberSecIdent, Cyberpark ENIGMA – тобто проєкти, присвячені питанням кібербезпек та запроваджені в цій установі [21, с. 103].

Більше того, Академія NASK проводить унікальні тренінги для компаній та установ з акцентом на безпеку ІКТ, а також провадить програму ЄС Безпечний Інтернет, що сприяє безпечному використанню технологій та мережі Інтернет серед молоді [Петров, с. 103]. Таким чином, вказана вище установа є не тільки адміністративним органом щодо регулювання доменних імен, реагування на інциденти у цифровому просторі тощо, а й платформою для широкомасштабних наукових та освітніх проектів [21, с. 103].

Цілком погоджується із думкою Петрова С.Г. про те, що вказаний досвід є релевантним для України, бо передбачає поєднання наукових підходів, освітніх програм і практичної реалізації заходів протидії посяганням на цифрову безпеку та кіберзлочинам, а також піднімає обізнаність населення, зокрема, не дуже активних користувачів мережі Інтернет. Головко Д.Ю. в рамках освітнього курсу було досліджено, на кого найбільше були спрямовані атаки у цифровому просторі у 2022 та 2023 роках [23, с. 29] (Таблиця 1).

Таблиця 1.

Найбільші жертви кібератак у 2022-2023 роках

№	Жертва кібератаки	Наслідки
1.	Твіттер (X)	Викрадено особисту інформацію про 5,4 млн. користувачів
2.	Червоний Хрест	Викрадено особисту інформацію про 515 тис. людей, зокрема, дані про локацію
3.	Міністерство національної оборони Португалії	Викрадено конфіденційні документ НАТО
4.	Веб-сторінки аеропортів	Зламано 23 веб-сайти аеропортів у США, Японії, Естонії та Литви

Нижче наводимо світову статистику кіберзлочинів за останні роки.

У відсотковому вимірі кібератак на організації за континентами у 2021 році виглядає наступним чином [24] (Рисунок 1):

- Азія (26%)
- Європа (24%)
- Північна Америка (23%)
- Близький Схід та Африка (14%)
- Латинська Америка (13%).

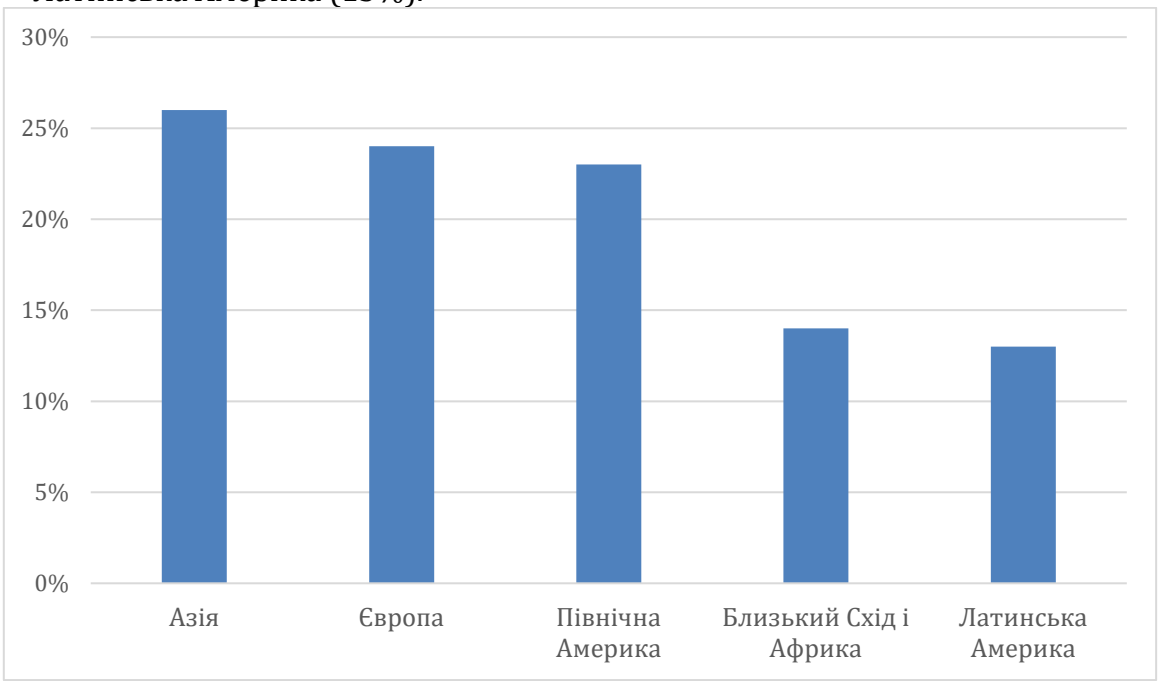

Рисунок 1. Регіони, у яких організації були жертвами кіберзлочинців

Таким чином, відповідно до інформації з відкритих джерел, у 2021 році найбільше кібератак у світі зазнали саме азійські організації. Далі, на противагу вказаному вище, наводимо статистичні дані згідно з Національним індексом кібербезпеки (NCSI) [24]. NCSI вимірює здатність країни запобігати кіберзагрозам та управляти кіберінцидентами. Станом на грудень 2023 року, 5 країн з найвищими показниками NCSI (Рисунок 2):

- Польща (90,83)
- Естонія (85,83)
- Україна (80,83)
- Латвія (79,17)
- Велика Британія (75,00)

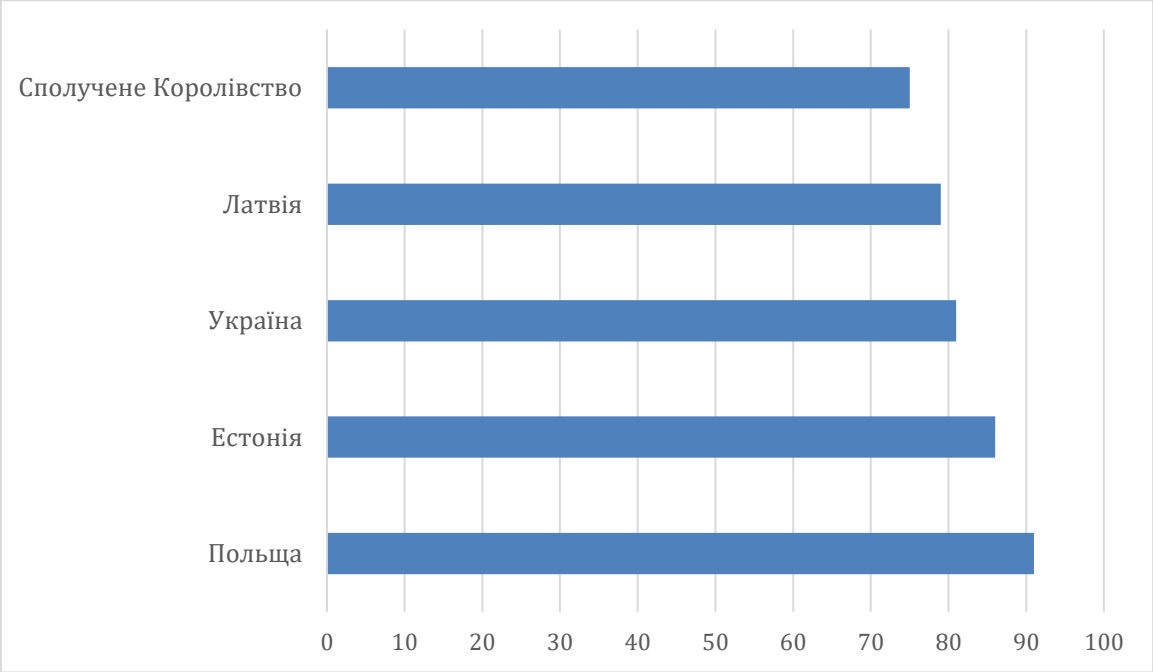

Рисунок 2. Країни з найсильнішою кібербезпекою

Таким чином, варто вважати, що Польща має найсильнішу кібербезпеку.

Науковцями також пропонується вважати стратегічними такі напрямами протидії кримінальним правопорушенням у контексті євроінтеграційних процесів [25, с. 108-109]:

- визначення спільного інструментарію співпраці;
- узгодження правових засад протидії злочинності;
- співпраця у сфері протидії кримінальним правопорушенням з урахуванням суб'єктного складу діяльності;
- кадрове забезпечення системи охорони та захисту державного кордону.

Висновки

Ефективна протидія злочинності у цифровому просторі потребує інтеграції технологічних та стратегічних підходів, а також глобальної співпраці для створення безпечного та захищеного цифрового простору.

Актуальним для України є досвід Польщі у формуванні RCB – надвідомчої структури, покликаної оптимізувати та стандартизувати сприйняття загроз державними органами задля підвищення їхньої здатності реагувати на складні ситуації, у тому числі у сфері захисту критичної інфраструктури, до якої належить і кіберсистема.

На особливу увагу для українського сьогодення заслуговує приклад NASK Польщі, яка поєднує наукові дослідження, освітні програми та практичну реалізацію заходів з протидії кібератакам.

Список використаних джерел

1. Шевчук М.О. Особливості правового забезпечення інформаційної безпеки з урахуванням сучасних загроз національній безпеці. *Правовий часопис Донбасу*. 2024. № 1 (86). С. 45-50. URL: https://ljd.dnuvs.ukr.education/index.php/ljd/article/view/28
2. Олійник А.А. Сутність інформаційної безпеки як правового явища у національному та міжнародному просторі. *Актуальні проблеми вітчизняної юриспруденції*. 2023. № 6. С. 293-299. URL: http://apnl.dnu.in.ua/6_2023/47.pdf
3. Яровенко Г.М. Вплив рівня економічного розвитку країни на залежність використання персональних засобів інформаційної безпеки та наслідків кіберзлочинів. *Вісник СумДУ. Серія «Економіка»*. 2020. № 1. С. 188-198. URL: https://www.researchgate.net/profile/Hanna-Yarovenko/publication/351165643_INFLUENCE_OF_THE_COUNTRY_ECONOMIC_DEVELOPMENT_ON_THE_DEPENDENCE_OF_THE_USE_OF_PERSONAL_INFORMATION_SECURITY_AND_THE_CONSEQUENCES_OF_CYBERCRIME/links/614d71c1519a1a381f7d46ec/INFLUENCE-OF-THE-COUNTRY-ECONOMIC-DEVELOPMENT-ON-THE-DEPENDENCE-OF-THE-USE-OF-PERSONAL-INFORMATION-SECURITY-AND-THE-CONSEQUENCES-OF-CYBERCRIME.pdf
4. Кримінальний кодекс України у редакції від 19.05.2024. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
5. Форос Г., Шимко Д. Організаційно-правові питання забезпечення кібербезпеки та протидії кіберзлочинності співробітниками Національної поліції України. *Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф.*, м. Одеса, 17.11.2023. Одеса: ОДУВС. 2023. С. 41-43. URL: https://dspace.oduvs.edu.ua/items/df8d57ea-8c47-46f5-9fce-e22d057d45ea
6. Тінін Д.Г. Сучасні тенденції злочинності в даркнеті: можливі шляхи попередження в умовах сьогодення. *Collection of Scientific Papers «SCIENTIA»,* (01.12.2023); Берлін. 2023. С. 126–128. URL: https://previous.scientia.report/index.php/archive/article/view/1400
7. Гуцалюк М.В, Клименко О.А. Забезпечення кібербезпеки та протидія кіберзлочинності як необхідна умова розвитку цифрових трансформацій сучасного суспільства. *Права людини в епоху цифрових трансформацій: Матеріали XII Міжнародної науково-практичної конференції.* Київ: Національний авіаційний університет. 2022. С. 301-303. URL: https://dspace.nau.edu.ua/handle/NAU/57937
8. Юртаєва К. В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. *Юридичний науковий електронний журнал*. 2022. № 12. С. 409-414. URL: http://lsej.org.ua/12_2022/96.pdf
9. Логвинський Г.В. Суб'єкт посягання на захисника чи представника особи. *Науковий юридичний журнал "Правові Новели"*. 2021. № 2(13). С. 81-86. URL: http://www.legalnovels.in.ua/journal/13-2_2021/13-2_2021.pdf#page=81
10. Науково-практичний коментар до статті 361 Кримінального кодексу України від 01.01.2009. URL: https://ips.ligazakon.net/document/KK004880
11. Науково-практичний коментар до статті 361-1 Кримінального кодексу України від 01.01.2009. URL: https://ips.ligazakon.net/document/KK004881

12. Дрижакова Д.Ю. Зарубіжний досвід кримінальної відповідальності за несанкціановане втручання в роботу інформаційних (автоматизованих), електронних, комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Міжнародна наукова конференція, 7-8 лютого 2024 р. Рига, Латвія. С. 104-108. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/download/436/11707/24506-1
13. Чекмарьова І.М. Шахрайство в Інтернеті як один із видів шахрайства. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. С. 639-643. URL: http://journal-app.uzhnu.edu.ua/article/view/303719/295753
14. Літвінова Ю.О., Мельник М.І., Татарин І.І. Шляхи вирішення проблеми кіберзлочинності в Україні. *Процесуальне та криміналістичне забезпечення досудового розслідування: тези доповідей учасників науково-практичного семінару* (01.12.2023). Львів: Львівський державний університет внутрішніх справ. С. 53-58. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/6777/1/01_12_2023.pdf#page=53
15. Проект Закону про внесення змін до Кримінального кодексу України щодо встановлення кримінальної відповідальності за несанкціоноване втручання, збут або розповсюдження інформації, що оброблюється в публічних електронних реєстрах та посилення кримінальної відповідальності під час дії воєнного стану за кримінальні правопорушення у сфері використання інформаційно-комунікаційних систем № 10242 від 09.11.2023. Офіційний веб-сайт Верховної Ради України. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43139
16. Мироненко В. Армія кібервоїнів: міжнародно-правовий досвід у сфері боротьби з кіберзлочинністю. 28.02.2024. URL: https://mind.ua/openmind/20270195-armiya-kibervoyiniv-mizhnarodno-pravovij-dosvid-u-sferi-borotbi-z-kiberzlochinnistyu
17. Столбовий В.М., Кисленко Д.П. Заходи з підвищення кібербезпеки на державному та корпоративному рівнях в умовах діджеталізації суспільства. *Наукові записки Львівського університету бізнесу та права. Серія економічна, серія юридична*. 2023. № 37. URL: https://nzlubp.org.ua/index.php/journal/article/view/802/729
18. Гунько І. Тестування програмного забезпечення у 2023 році: нові тенденції та проблеми. *Вісник Київського інституту бізнесу та технологій*. 2023. № 1-2 (49). С. 25-36. URL: https://herald.kibit.edu.ua/index.php/visnyk/article/view/1489/134
19. Дикий А.П., Барановська Т.В. Міжнародна співпраця в сфері запобігання та протидії економічній злочинності. *Журнал «Наукові інновації та передові технології». Серія «Міжнародна економіка».* 2022. № 5(7). С. 272-285. URL: http://perspectives.pp.ua/index.php/nauka/article/download/3644/3664
20. Калініна М.Р. Зарубіжний досвід боротьби із кіберзлочинністю. *Реформування правової системи в контексті євроінтеграційних процесів: матеріали VI Міжнародної науково-практичної конференції* (м. Суми, 19–20 травня 2022 року). Суми: Сумський державний університет. С. 436-439. URL: https://law.sumdu.edu.ua/wp-content/uploads/2022/06/Збірник_2022.pdf#page=436
21. Петров С.Г. Організаційні і правові основи вирішення проблем протидії кіберпосяганням у Європейському Союзі. *Інформація і право*. 2020. № 1(32). С. 99-105. URL: http://il.ippi.org.ua/article/view/200386
22. Довгань Б.В., Міхайліна Т.В. Регулювання відносин у цифровому просторі: порівняльно-правовий аналіз міжнародного та національного досвіду. *Вісник студентського наукового товариства Донецького національного університету*

імені Василя Стуса. 2020. № 2(12). С. 161-166. URL: https://jvestnik-sss.donnu.edu.ua/article/view/9257
23. Головко Д.Ю. Безпека в цифровому просторі. Біла Церква: БІНПО ДЗВО «УМО» НАПН України. 2024. URL: https://lib.iitta.gov.ua/739432/1/ЕНК%20Безпека%20в%20ЦП.pdf
24. Остання статистика кіберзлочинності за 2024 рік (оновлено у червні 2024 року). URL: https://aag-it.com/the-latest-cyber-crime-statistics/
25. Орловська Н.А., Степанова Ю.П. Концептуальні питання євроінтеграції у сфері протидії транскордонним кримінальним правопорушенням. *Південноукраїнський правничий часопис. Протидія злочинності: проблеми практики та науково-методичне забезпечення*. 2022. № 4, частина 2. С. 104-109. URL: http://www.sulj.oduvs.od.ua/archive/2022/4/part_2/16.pdf