УДК 341.3
DOI https://doi.org/10.24144/2307-3322.2024.82.3.41

# ДОСВІД УКРАЇНИ В ГАЛУЗІ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА В ГАЛУЗІ КІБЕРБЕЗПЕКИ

**Тєтєвін М.С.,**
*аспірант Київського університету права*
*Національної академії наук України*
*ORCID: https://orcid.org/0000-0002-5161-1480*
*e-mail: mykyta.tietievin.off@gmail.com*

**Тєтєвін М.С. Досвід України в галузі міжнародного співробітництва в галузі кібербезпеки.** У сучасному цифровому світі кібербезпека стала однією з найбільш актуальних проблем, оскільки зростання кількості підключених пристроїв призвело до збільшення кіберзагроз, які становлять серйозний ризик для національної та міжнародної безпеки. У цьому контексті співпраця між країнами стає надзвичайно важливою для захисту суверенітету та забезпечення кібербезпеки на глобальному рівні. Україна, яка має багатий досвід у протистоянні з кіберзагрозами, активно приймає участь у міжнародних ініціативах та співпраці в цій галузі. Стаття присвячена розгляду міжнародного співробітництва в галузі кібербезпеки та ролі України у цьому процесі. Дослідження розкриває значення ефективної нормативно-правової бази, зокрема програми Bug Bounty та механізму виявлення вразливостей. Україна активно співпрацює з міжнародними партнерами, що сприяє обміну досвідом та зміцненню кібербезпеки. Ключове значення має також міжнародне співробітництво з організаціями, які визнають безпеку однією з основних цілей, такими як НАТО та Європейський Союз. Зазначається, що Україна, будучи активним учасником міжнародних ініціатив та маючи великий досвід у галузі кібербезпеки, продовжує грати важливу роль у зміцненні світової кібербезпеки та сприяє створенню безпечнішого кіберпростору для всіх країн.

У процесі забезпечення кібербезпеки, Україна розвиває і впроваджує нові програми та стратегії, такі як Bug Bounty, що сприяють виявленню та усуненню вразливостей у інформаційних системах. Крім того, важливим кроком є прийняття Порядку пошуку та виявлення вразливостей, який надає можливість власникам бізнесу та державних установ оголосити про дозвіл на пошук слабкостей у своїх системах. Ці ініціативи дозволяють Україні активно брати участь у міжнародних процесах з кібербезпеки та сприяють підвищенню загальної безпеки в Інтернеті.

**Ключові слова.** Вразливості інформаційних систем, Bug Bounty, Міжнародні ініціативи, Кіберзагрози, Міжнародні організації, Цифрова безпека, Інформаційна технологія.

**Tietievin. M.S. Experience of Ukraine in the field of international cooperation in the field of Cyber Security.** In today's digital world, cybersecurity has become one of the most pressing issues, as the growing number of connected devices has led to an increase in cyber threats that pose a serious risk to national and international security. In this context, cooperation between countries becomes extremely important to protect sovereignty and ensure cybersecurity at the global level. Ukraine, which has extensive experience in countering cyber threats, is actively involved in international initiatives and cooperation in this area. The article is devoted to the analysis of international cooperation in the field of cybersecurity and Ukraine's role in this process. The study reveals the importance of an effective regulatory framework, in particular the Bug Bounty program and the vulnerability detection mechanism. Ukraine actively cooperates with international partners, which facilitates the exchange of experience and strengthening of cybersecurity. International cooperation with organizations that recognize security as one of their main goals, such as NATO and the European Union, is also of key importance. It is noted that Ukraine, being an active participant in international initiatives and having extensive experience in the field of cybersecurity, continues to play an important role in strengthening global cybersecurity and contributes to the creation of a safer cyberspace for all countries.

In the process of ensuring cybersecurity, Ukraine is developing and implementing new programs and strategies, such as Bug Bounty, to help identify and eliminate vulnerabilities in information systems. In addition, an important step is the adoption of the Vulnerability Search and Identification Procedure, which allows business owners and government agencies to request permission to search for weaknesses in their systems. These initiatives allow Ukraine to actively participate in international cybersecurity processes and contribute to improving overall Internet security.

**Key words.** Information systems vulnerabilities, Bug Bounty, International initiatives, Cyber threats, International organizations, Digital security, Information technology.

**Постановка проблеми**. У сучасному цифровому світі, де інформація стала найціннішим активом, питання кібербезпеки набули надзвичайної актуальності та важливості для всіх країн. Швидкий розвиток технологій і зростання кількості підключених до мережі пристроїв призвели до збільшення кількості кіберзагроз, які становлять серйозний ризик для національної та міжнародної безпеки. У цьому контексті, співпраця між країнами в галузі кібербезпеки стає необхідною складовою для захисту суверенітету кожної держави та гарантує забезпечення кібербезпеки на глобальному рівні.

Міжнародна співпраця в галузі кібербезпеки є надзвичайно важливою, оскільки інтернет не має фізичних кордонів, і кіберзагрози можуть легко перетнути державні межі. Україна, яка сама стала об'єктом серйозних кібератак та має багатий досвід у сфері кібербезпеки, активно приймає участь у міжнародних ініціативах з обміну інформацією та співпраці в цьому важливому сегменті сучасної безпеки.

Стаття присвячена розгляду міжнародного співробітництва в галузі кібербезпеки та ролі України у цьому процесі. Протягом дослідження ми торкнемося досвіду України в протистоянні зовнішнім кіберзагрозам (особливо за час повномасштабної російсько-української війни) та реакції міжнародного співтовариства на нові кібервиклики.

**Аналіз останніх досліджень і публікацій.** Питанням кіберпростору та кібербезпеки займається багато вітчизняних дослідників, серед яких можна виділити Грубі Т., Кононенко В., Здоровко С., Сабадишина Ю., Корольова А., Білоусова М., Тіщенко В., Логвиненко Є.

Виходячи з цього, **метою статті** є дослідження ролі міжнародного співтовариства в галузі кібертовариства та досвід України у протистоянні сучасним кіберзагрозам.

**Виклад основного матеріалу.** Міжнародне співробітництво в галузі кібербезпеки є ключовим фактором у забезпеченні стабільності та захисту інформаційних просторів усього світу. Оскільки кіберзагрози не знають кордонів, спільна дія і обмін інформацією між країнами стають необхідністю. Міжнародні організації та угоди сприяють встановленню спільних стандартів та механізмів відповіді на кібератаки, забезпечуючи тим самим кращий захист кіберпростору та національних інтересів кожної країни. Співробітництво в цій сфері важливо не лише для запобігання кіберзагрозам, але й для виявлення та розслідування інцидентів, що сталися вже.

Сьогодні, коли в нашій державі Україні 10 років йде війна, і не лише конвенційними засобами та методами, а й у тому числі на інформаційному фронті, участь у міжнародному процесі має вкрай важливе значення. Враховуючи те, що Україна, як одна з країн, яка щоденно веде активну боротьбу з кіберзагрозами та вже має чималий досвід й знання у галузі кібербезпеки, вплив на формування міжнародних стандартів та норм, спрямованих на забезпечення кібербезпеки, а також роль України у світовій кібербезпеці надзвичайно важлива. А сприяння у розробці та впровадженні міжнародних ініціатив може мати далекосяжний вплив на світовий кіберландшафт.

Слід зазначити, що у сфері ефективного забезпечення інформаційної безпеки існують три основні аспекти: люди, процеси та технології. Згідно зі Стратегією кібербезпеки Європейського Союзу [1], прийнятої у 2013 році, передбачено «зміцнення співпраці між державним та приватним секторами, а також розробку концептуальних документів для створення єдиної підходової парадигми в Європейському Союзі стосовно організації та проведення інформаційних операцій в рамках Стратегії «Спільної оборони і політики безпеки». Серед головних завдань, визначених у Стратегії кібербезпеки ЄС, можна виділити наступне: значне зниження рівня кіберзлочинності в країнах Європейського Союзу; розвиток політики кіберзахисту в країнах-членах Європейського Союзу та розвиток індустрії та технологічних ресурсів для забезпечення кібербезпеки.

У Стратегії визначено необхідність розвитку та фінансування національних центрів протидії кіберзлочинності та надано рекомендації щодо принципів, якими повинна керуватися політика

кібербезпеки в межах Європейського Союзу і на міжнародному рівні. Враховуючи це, передбачалося створення системи органів і агентств для протидії кіберзагрозам на загальноєвропейському рівні.

Також Стратегія підкреслює активну роль Європейського Союзу у забезпеченні захисту країн-членів організації, державних установ та громадян від кіберзлочинності. Одним з конкретних результатів цієї діяльності було створення Європейського центру протидії кіберзлочинності. Кіберпростір, разом з іншими фізичними просторами, вважається одним з театрів воєнних операцій. Спостерігається тенденція до створення кіберзбройних сил, завданнями яких є не лише захист критичної інформаційної інфраструктури від кібератак, але й проведення превентивних операцій у кіберпросторі, включаючи вимкнення критично важливих об'єктів противника через руйнування інформаційних систем, які керують цими об'єктами [1].

Ефективна система кібербезпеки невід'ємно пов'язана з наявністю ефективної нормативно-правової бази. У цьому контексті важливо зазначити значення Указу Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [2] від 26.08.2021 року. Цей Указ відповідає стратегії і передбачає створення максимально вільного, безпечного, відкритого і стабільного кіберпростору в інтересах захисту прав людини.

У сучасних умовах, коли Україна перебуває в стані воєнного конфлікту, це питання стає актуальним для всіх громадян, а не лише ІТ-фахівців. Знання цифрової грамотності, дотримання цифрового етикету і правил кібергігієни важливі для всіх. Під час початку війни, ІТ-фахівці з різних частин країни приєдналися до кіберполіції та успішно припинили агресію. Це призвело до вимкнення критично важливих інформаційних систем окупанта завдяки координації зусиль.

Також варто згадати, що серед міжнародних організацій, які визнають безпеку однією з основних цілей, НАТО внесла найбільший внесок у зміну політики стосовно інформаційної безпеки. Організація встановила центри в країнах-членах як багатонаціональні інститути, спрямовані на розробку стратегій цифрової безпеки, поліпшення міжнародної співпраці, впровадження наукових розробок у боротьбі з цифровими загрозами, обмін досвідом забезпечення інформаційної безпеки між країнами-членами та партнерами. В даний час, Центр кібербезпеки НАТО успішно функціонує в Естонії. Слід відзначити, що він не є складовою структурою збройних сил НАТО і фінансується завдяки сприянню держав-спонсорів та внескам держав-членів НАТО [4, с. 244–248].

Україна активно співпрацює з міжнародними партнерами в галузі кібербезпеки, набуваючи доступ до міжнародного досвіду та сучасних методів реагування на кіберінциденти. Заходи, спрямовані на зміцнення довіри у кіберпросторі та співпрацю з ЄС, НАТО та іншими міжнародними організаціями, сприяють підвищенню кібербезпеки та відповідають національним інтересам України. У цьому контексті, Україна бере участь у Форумі команд реагування на інциденти інформаційної безпеки FIRST, що об'єднує групи CERT у країнах Європи [5, с. 42–48].

Щодо досвіду України – це не пусті слова. Тільки за минулий 2022 рік Україна відбила понад 1,5 мільйона кібератак на українську енергетичну галузь [6]. З метою вдосконалення забезпечення захисту національного кіберпростору Україна робить багато локальних нововведень. Одним із найсвіжіших можна виділити програму Bug Bounty, яку 16 травня 2023 Уряд ухвалив розроблений фахівцями Держспецзв'язку «Порядок проведення Bug Bounty» для державних установ та приватних компаній [8]. Bug Bounty – це програма яка дає можливість легально тестувати системи й мережі на наявність вразливостей, а власникам приватного сектору – значно підвищувати рівень кіберзахисту систем шляхом усунення таких вразливостей. Тепер процес виявлення потенційних слабкостей повинен здійснюватися через Bug Bounty. Замовник, який є власником інформаційної системи, самостійно запускає таку програму, публікуючи її оголошення та встановлюючи фінансовий винагородний фонд або інші види заохочень.

З метою захисту інформації Кабінетом Міністрів України в травні 2023 року було затверджено Порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж [8], який визначає механізм здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (далі - пошук потенційної вразливості системи). Іншими словами відтепер власник бізнесу, підприємства або державна установа, що хоче перевірити свою інформаційну систему на вразливості має можливість скористатися механізмом легально оголосити про

дозвіл зламати чи знайти слабкість в її інформаційній технології. А пошуком будуть займатися спеціалісти з приватного сектору. Як результат – інформаційна технологія проходить «випробування вогнем», а виконавці цього випробування отримують за це справедливу винагороду.

**Висновок.** Міжнародний та європейський досвід та співробітництво в галузі кібербезпеки є критично важливим аспектом забезпечення сучасної світової безпеки, оскільки кіберзагрози не зупиняються на національних кордонах і можуть миттєво впливати на держави та глобальну інфраструктуру. У цьому контексті Україна грає важливу роль у світовій кібербезпеці. По-перше, Україна, яка стала об'єктом масштабних кібератак, набула значного досвіду у відстоюванні та реагуванні на кіберзагрози. Цей досвід виявився вельми корисним для інших країн, які також стикаються з подібними проблемами. Україна активно ділиться своїми знаннями та інформацією про кіберзагрози з міжнародним співтовариством, сприяючи підвищенню світової кібербезпеки. По-друге, Україна активно приєднується до міжнародних ініціатив та програм, спрямованих на зміцнення кібербезпеки. Вона бере участь у спільних проектах з міжнародними організаціями, такими як Організація з безпеки і співробітництва в Європі (ОБСЄ), Європейський Союз (ЄС) та Північноатлантичний альянс (НАТО), співпрацюючи у сфері кібербезпеки та сприяючи розвитку спільних стратегій. По-третє, Україна активно взаємодіє з міжнародними організаціями і спільнотами для зміцнення довіри у кіберпросторі. Ця співпраця сприяє обміну інформацією, розробці спільних стандартів та підвищенню стійкості глобального інтернету до кіберзагроз.

Україна, будучи активним учасником міжнародних ініціатив та маючи великий досвід у галузі кібербезпеки, продовжує грати важливу роль у зміцненні світової кібербезпеки та сприяє створенню безпечнішого кіберпростору для всіх країн.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**


1. Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade. Council of the European Union. Brussels, 9 March 2021. № 6722/21.
2. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» № 447/2021 від 26 серпня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 15.01.2024).
3. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших. Інформаційна довідка. Європейський інформаційно-дослідницький центр.
4. Кононенко В.П, Здоровко С.С., Корольова А.Є. Інформаційна безпека як стан. Науковий вісник Ужгородського Національного Університету, Серія ПРАВО. Випуск 76: частина 2023. С. 244–248.
5. Грубі Т.В. Світові та вітчизняні практики в сфері кібербезпеки: виклики сучасност. Збірник матеріалів Міжнародної науково-практичної конференції «Інформаційна безпека: сучасний стан, проблеми та перспективи» [Електронний ресурс] / [за заг. ред. О.В. Віннічук]. Кам'янецьПодільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. С. 42–48.
6. Торік відбили понад 1,5 мільйона кібератак на українську енергетичну галузь» – Укрінформ, 2023, https://www.ukrinform.ua/rubric-technology/3729720-torik-vidbili-ponad-15-miljona-kiberatak-na-ukrainsku-energeticnu-galuz.html (дата звернення: 15.01.2024).
7. В Україні дозволили організовувати Bug Bounty. Що це змінить і як працюватиме. URL: https://dou.ua/lenta/news/bug-bounty-in-ukraine/ (дата звернення: 15.01.2024).
8. Постанова КМУ «Порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» № 497 від 16 травня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#Text (дата звернення: 15.01.2024).
9. Тіщенко В.О., Логвиненко Є.С. Правові засади забезпечення кібербезпеки в умовах воєнного стану. Протидія кіберзлочинності та торгівлі людьми: зб. матеріалів міжнар. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.). Вінниця: ХНУВС, 2023. С. 71–73.
10. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2023. № 9 (вересень). 351 с.