УДК 342.9
DOI https://doi.org/10.32844/2618-1258.2025.1.22

РОГОЗІННІКОВА К.С.

РОЛЬ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

THE ROLE OF THE SECURITY SERVICE OF UKRAINE IN ENSURING THE STATE'S CYBERSECURITY UNDER MARTIAL LAW

У цій статті автор комплексно аналізує діяльності Служби безпеки України у сфері забезпечення кібербезпеки України в умовах повномасштабної війни росії проти України. Відповідно для цього досліджуються нормативно-правові акти, якими забезпечується важливий функціонал Служби безпеки України та її підрозділів в галузі кібербезпеки, а також виокремлено ключові аспекти, які необхідно удосконалити з урахуванням викликів сучасних кіберзагроз. Автор відводить особливе місце науковим підходам до розуміння кібербезпеки, зокрема у порівнянні з законодавчими визначеннями, що стосуються компетенцій Служби безпеки України у виявленні, попередженні та розслідуванні кібератак.

У дослідженні розглядаються випадки реальної військової кіберагресії, спрямованої проти нашої держави: атаку на телекомунікаційного оператора «Київстар» з боку хакерського угруповання ГРУ "SandWorm", а також дії, які були спрямовані на військову інфраструктуру Збройних сил України. У цьому контексті детально розглянута роль Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України у запобіганні, нейтралізації таких загроз та виявленню суб'єктів таких атак. Окремого значення набуває ефективне розслідування кіберзлочинів під час війни та притягнення винних саме до міжнародної відповідальності, які знаходяться в межах юрисдикції Міжнародного кримінального суду.

Автор погоджується з необхідністю злагодженого функціонування європейської системи кібербезпеки, а тому розглядається доцільність створення європейської кіберкоаліції як механізму колективного реагування на масштабні кіберзагрози. Зауважено про необхідність міжнародного співробітництва, обміну розвідувальними даними та уніфікації стандартів кіберзахисту з українськими союзниками.

У статті зроблений висновок, що такі явища як кібервійна та кібербезпека дуже стрімко розвиваються, у свою чергу це зумовлює необхідність адаптації державної політики до нових загроз та посилення ролі Служби безпеки України як одного з ключовий суб'єктів не лише національної системи кіберзахисту, а й загалом всієї національної безпеки. Отримані результати можуть бути використані для вдосконалення стратегічного планування у сфері кібербезпеки та підвищення ефективності державних механізмів протидії кіберзагрозам.

Ключові слова: *Служба безпеки України, кібербезпека, воєнний стан, нормативно-правове регулювання, військова кіберагресія, міжнародна відповідальність, національна безпека.*

In this article, the author comprehensively analyzes the activities of the Security Service of Ukraine in the field of ensuring the cybersecurity of Ukraine in the context of a full-scale war between Russia and Ukraine. Accordingly, the regulatory and legal acts that ensure the important functionality of the Security Service of Ukraine and its units in the field of cybersecurity are studied, and key aspects that need to be improved taking into account the challenges of modern cyber threats are also highlighted. The author

© РОГОЗІННІКОВА К.С. – кандидатка юридичних наук, доцентка кафедри правоохоронної діяльності та спеціальних юридичних дисциплін (Навчально-науковий інститут права Національного університету водного господарства та природокористування)

devotes a special place to scientific approaches to understanding cybersecurity, in particular in comparison with legislative definitions related to the competences of the Security Service of Ukraine in detecting, preventing and investigating cyber attacks.

The study examines cases of real military cyber aggression directed against our state, in particular the attack on the telecommunications operator "Kyivstar" by the GRU hacker group "SandWorm", as well as actions that were directed at the military infrastructure of the Armed Forces of Ukraine. In this context, the role of the Department of Counterintelligence Protection of State Interests in the Field of Information Security of the Security Service of Ukraine in preventing, neutralizing such threats and identifying the subjects of such attacks is considered in detail. Of particular importance is the effective investigation of cybercrimes during wartime and bringing the perpetrators to international responsibility, in particular within the jurisdiction of the International Criminal Court.

The author agrees with the need for a coordinated functioning of the European cybersecurity system, in particular, the feasibility of creating a European cyber coalition as a mechanism for collective response to large-scale cyber threats is considered. The need for international cooperation, exchange of intelligence data and unification of cyber defense standards with Ukrainian allies is noted.

The article concludes that such phenomena as cyberwar and cybersecurity are developing very rapidly, which in turn necessitates the adaptation of state policy to new threats and the strengthening of the role of the Security Service of Ukraine as one of the key actors not only of the national cyber defense system, but also of the entire national security in general. The results obtained can be used to improve strategic planning in the field of cybersecurity and increase the effectiveness of state mechanisms for countering cyber threats.

Key words: *Security Service of Ukraine, cybersecurity, martial law, regulatory and legal regulation, cyberattacks, military cyber aggression, international responsibility, national security.*

Вступ. У сучасній національній безпеці одним із ключових аспектів є кібербезпека держави. З початком повномасштабної збройної агресії проти України ми гостро відчули проблему захисту нашого кіберпростору і це питання набуло особливого значення, оскільки ворожі атаки спрямовані не лише на військові об'єкти, а й на критичну інфраструктуру, органи державної влади та інформаційний простір країни. Масштабність та системність таких атак свідчить про те, що кіберпростір став одним із основних полів ведення сучасної війни. В умовах воєнного стану держава стикається з безпрецедентними викликами у сфері кібербезпеки, що вимагає ефективного реагування та координації зусиль усіх відповідальних органів. Одну з центральних ролей у цьому процесі відіграє Служба безпеки України, яка наділена повноваженнями для запобігання, виявлення та нейтралізації загроз у кіберпросторі.

Колосовський Є. Ю. та Круць Е. М. у своєму дослідженні підкреслюють, що питання кібербезпеки в умовах воєнного стану потребує не лише ретельного аналізу, а й комплексного підходу до організації кіберзахисту держави. Вони зазначають, що здатність України ефективно протидіяти кіберзагрозам прямо впливає на її національну безпеку, збереження критичних інформаційних ресурсів та економічну стабільність. Дослідники наголошують, що успішне протистояння кіберзагрозам можливе лише за умови застосування всього арсеналу правових механізмів, спрямованих на посилення кіберзахисту. Вони акцентують увагу на тому, що безпека інформаційного простору має забезпечуватися через системний підхід на всіх рівнях державного управління, а також шляхом належного контролю руху інформаційних потоків. Одним із ключових висновків дослідників є те, що максимальний ефект у сфері кібербезпеки досягається завдяки скоординованій взаємодії всіх суб'єктів, залучених до забезпечення інформаційної безпеки держави. Для цього необхідне запровадження комплексних механізмів управління, ефективних адміністративно-правових методик та використання сучасних підходів до реалізації державної політики у сфері кіберзахисту [1, с. 403].

Науковиця Ткачук Н. А. наголошує на тому, що Служба безпеки України відіграє ключову роль у національній системі кібербезпеки, оскільки забезпечує її контррозвідувальний захист. Такий підхід визначає Службу безпеки України як системоутворюючий елемент, що здійснює протидію кіберзагрозам, які становлять небезпеку для держави. Контррозвідувальна діяльність

у сфері кібербезпеки має багатовекторний характер і спрямована насамперед на нейтралізацію кібершпигунства та кібертероризму, які можуть використовуватися як засоби ведення гібридної війни. Особливо це актуально в умовах збройного конфлікту, коли інформаційний простір України стає об'єктом цілеспрямованих атак. Окремий напрям роботи Служби безпеки України – виявлення та розкриття кіберзлочинів, наслідки яких можуть загрожувати життєво важливим інтересам держави. Йдеться не лише про несанкціоноване втручання у роботу державних органів чи критичної інфраструктури, а й про поширення деструктивного контенту, інформаційно-психологічні операції, що спрямовані на дестабілізацію суспільства. Важливою функцією є також розслідування кіберінцидентів та атак, спрямованих на державні електронні інформаційні ресурси. Особливої уваги потребує захист інформації, що має стратегічне значення, а також систем, які забезпечують функціонування органів влади та оборонного сектору. Окрім цього, Служба безпеки України виконує завдання з реагування на комп'ютерні інциденти, що можуть мати наслідки для державної безпеки. Це передбачає не лише оперативне виявлення атак, а й координацію заходів із їхнього нейтралізації та усунення наслідків [2, с. 53].

Попри значні напрацювання у цій сфері, дійсно переконана, що окремі аспекти проблеми залишаються недостатньо висвітленими. Зокрема, потребує подальшого дослідження питання адаптації функцій Служби безпеки України до нових викликів у сфері кібербезпеки, а також її взаємодія з іншими державними та міжнародними структурами. Залишається відкритим питання удосконалення механізмів оперативного реагування на масштабні кібератаки в умовах воєнного стану, а також впровадження інноваційних технологій у протидії кіберзагрозам..

З огляду на викладене, дана стаття присвячена дослідженню ролі Служби безпеки України у забезпеченні кібербезпеки держави в умовах воєнного стану. Зокрема, розглядаються основні напрями діяльності Служби безпеки України у цій сфері, нормативно-правове регулювання її повноважень, механізми реагування на актуальні кіберзагрози та перспективи вдосконалення її діяльності в умовах сучасних викликів.

Постановка завдання. Метою даної статті є аналіз ролі Служби безпеки України у забезпеченні кібербезпеки держави в умовах воєнного стану, а саме визначення основних напрямів її діяльності, нормативно-правового регулювання повноважень та механізмів реагування на сучасні кіберзагрози.

Результати дослідження. Для ґрунтовного аналізу питання кібербезпеки важливо звернутися до її законодавчого визначення, оскільки саме нормативне розуміння цього терміна визначає межі досліджуваної проблематики та напрями державної політики у цій сфері. Закон України «Про основні засади забезпечення кібербезпеки України» містить чіткі визначення понять «кібербезпека» та «кіберзагроза», які є основоположними для розуміння механізмів захисту держави від загроз у цифровому середовищі. Згідно з частиною 5 статті 1 зазначеного закону, «кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». Це визначення охоплює широкий комплекс заходів, спрямованих на підтримку стабільного функціонування цифрового середовища, своєчасне реагування на ризики та усунення потенційних загроз. Таким чином, кібербезпека не обмежується лише технічними аспектами захисту інформації, а включає організаційні та стратегічні заходи, що забезпечують безперервний розвиток та функціонування інформаційного простору. Хоча українські науковці Л. М. Бєлкін, Ю. Л. Юринець, М. Л. Бєлкін та Є. В. Криволап розглядають поняття кібербезпеки «окремим випадком загального поняття безпеки інформації, але такої інформації, яка обертається у кіберпросторі. При цьому причиною підвищеної уваги саме до кіберзагрозам і кібербезпеки є дедалі зростаюча роль обігу інформації в комп'ютерних системах і електронно-комунікаційних мережах» [4, с. 80]. Вони акцентують свою думку на тому, що посилена увага до кіберзагроз зумовлена зростанням ролі інформаційних технологій у сучасному суспільстві. Водночас законодавче визначення кібербезпеки є ширшим і має системний характер. Порівняння наукового та правового підходів дозволяє стверджувати, що кібербезпека виходить за межі традиційного розуміння інформаційної безпеки, оскільки її порушення може мати безпосередні наслідки для економічної, оборонної та соціальної стабільності держави. Під час дії воєнного стану кіберзагрози стають частиною гібридної війни, що вимагає адаптації національної системи кіберзахисту та посилення координації між відповідними органами.

У законодавстві України можна знайти декілька понять, що стосуються ролі Служби безпеки України в національній системі безпеки. Відповідно до Закону України «Про національну безпеку України» «Служба безпеки України є державним органом спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку, здійснюючи з неухильним дотриманням прав і свобод людини і громадянина:

1) протидію розвідувально-підривній діяльності проти України;

2) боротьбу з тероризмом;

3) контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, інформаційної безпеки держави, об'єктів критичної інфраструктури;

4) охорону державної таємниці» [5].

А якщо ми досліджуємо саме її роль у забезпеченні кібербезпеки, то з цієї точки зору Служба безпеки України є одним із ключових елементів системи кібербезпеки держави, що функціонує у взаємодії з іншими суб'єктами такими як: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. Комплексне залучення цих структур дозволяє реалізовувати заходи з протидії кіберзагрозам та забезпечення стабільного функціонування державних інформаційних ресурсів [3].

Функції Служби безпеки України у сфері кібербезпеки регламентовані законодавчо, і згідно з пунктом 3 частини 2 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України», Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки» [3].

Це означає, що Служба безпеки України має широкий спектр повноважень і завдань, пов'язаних із запобіганням кіберзагрозам та боротьбою з ними. Її діяльність охоплює як превентивні заходи, такі як перевірка готовності критичної інфраструктури до потенційних атак, так і реагування на вже здійснені кібератаки та їх наслідки. Особливу увагу слід приділити контррозвідувальній складовій, яка передбачає виявлення та нейтралізацію загроз з боку іноземних спецслужб та кіберзлочинних угруповань, що здійснюють діяльність проти України та її цифрових ресурсів. У цьому контексті вважаю необхідним звернути увагу на роботу функціонального підрозділу Служби безпеки України, а саме Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України. Так, у інтерв'ю для Ukrinform начальник Департаменту кібербезпеки Служби безпеки України Ілля Вітюк наголосив, що росія протягом тривалого часу нарощувала свій кібернаступальний потенціал і після початку повномасштабної агресії активізувала кібератаки на критичну інфраструктуру України. Він зазначив, що у 2020 році було зафіксовано 800 кібератак, у 2021 році – 1400, а після лютого 2022 року кількість атак зросла до 4500 щороку. Дані, наведені І. Вітюком, підтверджують системність та стратегічний характер використання кіберагресії Російською Федерацією, що потребує комплексної протидії. З його слів, такі спроби включали використання шкідливого програмного забезпечення, розсилку фішингових повідомлень та отримання доступу до пристроїв військових через трофейні або захоплені гаджети [6].

Одним із ключових напрямів кібероборони, як зазначає Ілля Вітюк, є посилення контррозвідувальних заходів [6]. Йдеться про негласну перевірку готовності критичної інфраструктури до можливих кібератак, оперативне реагування на кіберінциденти та протидію діяльності хакерських угруповань. Такі заходи повністю відповідають компетенції Служби безпеки України, визначеній у статті 8 Закону України «Про основні засади забезпечення кібербезпеки України».

Також Ілля Вітюк повідомив, що відповідальність за атаку на «Київстар» взяло на себе хакерське угруповання SandWorm, яке відноситься до військової частини 74455 ГРУ. Незважаючи на те, що первинну заяву про атаку зробила телеграм-група «Солнцепьок», а згодом інформацію поширив канал «Джокер ДНР», Служба безпеки України визначила, що ці ресурси працюють у координації з російським ГРУ. Зі слів Іллі Вітюка, аналіз технічних характеристик атаки,

використаного програмного забезпечення та інфраструктури підтвердив, що саме SandWorm стоїть за цією операцією [6]. З позиції правового аналізу, подібну діяльність досить складно кваліфікувати, оскільки з національної точки кримінальної відповідальності такі діяння можна віднести до статті 361 та 361-1 Кримінального кодексу України [7]. Однак ми повинні розуміти, що ці дії були вчинені не просто групою незалежних хакерів, а з залученням допомоги військових та ГРУ. З цього можна стверджувати, що така діяльність порушує принципи міжнародного гуманітарного права, оскільки ця атака була направлена на цивільну інфраструктуру. Звісно, тут потрібно уточнити про ряд факторів, які ускладнюють як саме розслідування так і відповідно кваліфікацію її з точки зору міжнародного кримінального права: кібератаки – один з сучасних методів ведення війни (кібервійни), які за своїми деструктивними діями нічим не поступаються від звичайних методів війни, проте встановлення особистостей їхніх виконавців та замовників є досить значним викликом через те, що вони не знаходяться, так би мовити, на звичному полі бою, а тому зафіксувати їх набагато важче.

Варто зазначити, що підтвердженням важливості цих кейсів не лише для України, а й для світової спільноти є те, що прокурор Міжнародного кримінального суду Карім Хан офіційно визнав можливість кваліфікації таких дій як воєнних злочинів. Відзначу, що його думка привертає увагу до кіберзлочинів під час ведення війни і того, що вони можуть мати той самий руйнівний ефект, як і, наприклад, збройні напади, але без фізичної присутності агресора [8]. Кібератаки, що здійснюються на критичну інфраструктуру, можуть так само призвести до втрат людських життів, порушень прав людини та знищення цінної інформації. Враховуючи ці ризики, питання включення кіберзлочинів до міжнародного кримінального права стає надзвичайно важливим. І хоча Римський статут на сьогодні не містить конкретних положень щодо кіберзлочинів, це відкриває можливості для розвитку та напрацювання нових правових норм, які будуть враховувати загрози, які несуть за собою новітні методи ведення війни.

У цьому контексті досвід України у боротьбі з кіберзлочинністю має стати важливим внеском у міжнародну практику притягнення до відповідальності за відповідні воєнні злочини. Україна, як країна, що зазнала і продовжує зазнавати численних кібератак з боку агресора, зокрема на державні установи, критичну інфраструктуру та громадян, має унікальний досвід виявлення, розслідування та протидії таким загрозам. Важливу роль у цьому процесі, як ми з'ясували, відіграють спеціальні підрозділи, які займаються кібербезпекою та протидією кібертероризму. Тому досвід Служби безпеки України у знешкодженні таких кіберзагроз та розслідуванні кібератак може стати основою для розробки міжнародних стандартів розслідування кіберзлочинів, що матимуть прямі наслідки для захисту прав людини та забезпечення міжнародної безпеки. Загалом, такі заяви дають позитивні сигнали про рішучість та готовність міжнародної спільноти до боротьби з кіберзлочинністю як елементом воєнних дій.

До речі, вважаю за необхідне погодитися з пропозицією Н. Ткачук, керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО, яка акцентувала увагу на необхідності консолідації міжнародних зусиль у сфері кібербезпеки шляхом створення європейської кіберкоаліції. Вона підкреслила, що нинішня кібервійна, яка є безпрецедентним явищем у світовій історії, демонструє критичну важливість злагоджених дій усіх суб'єктів кібербезпеки. За її словами, Україна вже продемонструвала високу стійкість власної кіберінфраструктури, що стало можливим завдяки ефективній взаємодії між державними органами, сектором безпеки, бізнесом і громадянським суспільством [9]. Втім, враховуючи зростання масштабності й складності кібератак, необхідним є створення структурованого міжнародного механізму, який би забезпечував обмін оперативною інформацією, розвідувальними даними та уніфікацію стандартів кіберзахисту на рівні європейських країн.

На думку Н. Ткачук, європейська кіберкоаліція повинна включати не лише механізми спільного аналізу кіберзагроз, а й розробку координаційних протоколів реагування як на національному, так і на міжнародному рівні [9]. Повністю підтримую цю пропозицію через те, що дозволить створити дієву систему стримування загроз у кіберпросторі та зміцнить здатність держав протидіяти кіберагресії. Важливим аспектом такої співпраці є розширення стратегічного партнерства між країнами та посилення кібердипломатії, що забезпечить превентивний захист критичної інформаційної інфраструктури. Повністю підтримую таку ініціативу, оскільки її реалізація сприятиме зміцненню кібербезпеки України та інтеграції нашої держави в європейську систему кіберзахисту. Особливу роль у цьому процесі повинна відігравати Служба безпеки України, яка володіє необхідними компетенціями та ресурсами для координації заходів у сфері кібербезпеки. Саме Служба безпеки України має стати ключовим суб'єктом забезпечення провідної

ролі України у міжнародних кібернетичних ініціативах, що сприятиме як зміцненню національної безпеки, так і підвищенню авторитету нашої країни у сфері глобального кіберзахисту.

Висновки. Стрімкий розвиток інформаційних технологій зумовив не лише розширення можливостей кібербезпеки, а й загострення кіберзагроз, що стали невід'ємною складовою сучасних військових конфліктів. Україна зіткнулася з безпрецедентним рівнем кіберагресії, що здійснюється російською федерацією та спрямована на підрив критичної інфраструктури, військових інформаційних систем та цивільного сектору. Аналіз діяльності Служби безпеки України в цій сфері доводить її ключову роль у забезпеченні кіберзахисту держави, виявленні та нейтралізації загроз, а також формуванні доказової бази для притягнення винних до відповідальності. Особливо важливим є визнання міжнародною спільнотою, зокрема прокурором Міжнародного кримінального суду, факту того, що кібератаки на цивільну інфраструктуру можуть бути кваліфіковані як воєнні злочини. Це створює додаткові правові механізми для міжнародного переслідування злочинців та притягнення до відповідальності не лише виконавців, а й організаторів таких атак.

В умовах воєнного стану національна система кібербезпеки має функціонувати на принципах тісної взаємодії між Службою безпеки України, Міністерством оборони України, Державною службою спеціального зв'язку та захисту інформації, Національною поліцією, Генеральним штабом Збройних сил України та розвідувальними органами. Координація їхніх дій, оперативний обмін інформацією та впровадження сучасних технологій кіберзахисту дозволять ефективніше протидіяти новим викликам.

Підсумовуючи, можна стверджувати, що перспективи подальшого вдосконалення кібербезпеки в Україні мають базуватися на таких ключових напрямах: розвиток законодавчої бази з урахуванням новітніх кіберзагроз, посилення міжнародної співпраці у сфері кіберзахисту, впровадження сучасних механізмів кіберконтррозвідки та формування ефективної системи підготовки спеціалістів у сфері кібербезпеки. Всі ці заходи сприятимуть підвищенню рівня кіберзахисту держави та її стійкості перед сучасними загрозами.

Список використаних джерел:

1. Колосовський Є. Ю., Круць Е. М. Сучасний стан кібербезпеки україни в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. № 12. С. 402-405.

2. Ткачук Н. А. Роль і місце Служби безпеки України в національній системі кібербезпеки. the Journal of Eastern European Law / Журнал східноєвропейського права. 2017. № 44. С. 50-57.

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради Україн.* 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 25.03.2025).

4. Бєлкін Л. М., Юринець Ю. Л., Бєлкін М. Л., Криволап Є. В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років. *Scientific Works of National Aviation University. Series: Law Journal "Air and Space Law"*. № 3(64). 2022. С. 78-86.

5. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради України.* 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 25.03.2025).

6. Ukrinform. Ілля Вітюк, начальник Департаменту кібербезпеки СБУ. *Укрінформ – актуальні новини України та світу.* URL: https://www.ukrinform.ua/rubric-ato/3848169-illa-vituk-nacalnik-departamentu-kiberbezpeki-sbu.html (дата звернення: 25.03.2025).

7. Кримінальний кодекс України: Кодекс України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України.* 2001. № 25-26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 25.03.2025).

8. Ukrinform. Кіберзлочини можуть підпадати під юрисдикцію МКС – прокурор Хан. *Укрінформ – актуальні новини України та світу.* URL: https://www.ukrinform.ua/rubric-world/3816924-kiberzlocini-mozut-pidpadati-pid-urisdikciu-mks-prokuror-han.html (дата звернення: 25.03.2025).

9. Н. Ткачук: Необхідно розглянути можливість створення європейської кіберкоаліції для спільного реагування у випадку масштабних кібератак. – Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/ua/Diialnist/6074.html (дата звернення: 25.03.2025).