УДК 343.3
DOI https://doi.org/10.24144/2788-6018.2025.01.110

ПРОБЛЕМНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Топчій В.В.,
доктор юридичних наук., професор,
Заслужений юрист України,
директор навчально-наукового інституту права
Державного податкового університету
ORCID: 0000-0002-1726-9028

Бодунова О.М.,
доктор юридичних наук., доцент,
завідувач кафедри правничої лінгвістики
Державного податкового університету
ORCID: 0000-0001-9179-5985

Топчій В.В., Бодунова О.М. Проблемні питання забезпечення кібербезпеки в Україні.
У статті розглянуто проблемні питання забезпечення кібербезпеки в Україні. Встановлено, що кіберзлочинність є глобальною проблемою, яка постійно еволюціонує, і потребує скоординованих зусиль на національному та міжнародному рівнях. Для ефективного запобігання кіберзлочинам держави, включаючи Україну, розробляють і впроваджують різноманітні стратегії, програми та заходи, зокрема розробка середньострокових програм запобігання, посилення міжнародного співробітництва та рівня обізнаності населення у сфері кібергігієни тощо. Україна рухається у правильному напрямку, але ефективне запобігання кіберзлочинів вимагає постійної модернізації та адаптації до нових викликів. Співпраця держави, громадянського суспільства та міжнародних партнерів є ключем до успіху у цьому питанні.

З метою усунення вищенаведених загроз та з метою фомування цілісної стратегії кібербезпеки в Україні визначено та проаналізовано нормативно-правове підґрунтя.

Зазначено, що під час першого місяця війни в Україні парламент оперативно прийняв законопроєкти, спрямовані на вдосконалення процедур і правових основ притягнення кіберзлочинців до кримінальної відповідальності. Ці зміни були необхідними для ефективної протидії зростаючим кіберзагрозам, які стали особливо актуальними в умовах війни. Запровадження відповідальності за кіберзлочини, вчинені в умовах війни, є необхідним для забезпечення національної безпеки та захисту суспільних інтересів України. Такі дії не лише підривають критичну інфраструктуру та інформаційну безпеку, але й можуть використовуватись агресором як інструмент гібридної війни.

Доведено, що для того, щоб комплексно вирішувати питання запобігання злочинності у сфері кіберзлочинності, Україні потрібно ввести додаткові нормативно-правові акти, що будуть орієнтовані не лише на реагування на кіберзагрози, але й на більш ефективне попередження кіберзлочинності.

Окрім цього, встановлено необхідність впровадження відповідальності за вищезазначені кримінальні правопорушення, вчинені під час воєнного стану. За такі протиправні дії повинні передбачатися суворі санкції, оскільки обставини в країні вимагають цього. Особа, яка завдає шкоди національним інтересам України у кіберпросторі й у такий спосіб допомагає агресору в цій війні, повинна нести відповідальність аналогічно воєнним злочинцям.

Ключові слова: кібербезпека, кіберзлочинність, кримінальний кодекс, кримінальні правопорушення, цифрове середовище, кіберзахист, запобігання

Topchii V.V., Bodunova O.M. Problematic issues of ensuring cybersecurity in Ukraine.
The article examines the problematic issues of cybersecurity in Ukraine. It is established that cybercrime is a global problem that is constantly evolving and requires coordinated efforts at the national and international levels. In order to effectively prevent cybercrime, states, including Ukraine, develop and implement various strategies, programmes and measures, including the development of medium-term prevention programmes, strengthening international cooperation and public awareness in the field of cyber hygiene, etc. Ukraine is moving in the right direction, but effective cybercrime prevention requires constant modernisation and adaptation to new challenges. Cooperation between the state, civil society and international partners is key to success in this regard.

In order to address the above threats and to formulate a comprehensive cybersecurity strategy in Ukraine, the legal framework has been identified and analysed.

It is noted that during the first month of the war in Ukraine, the Parliament promptly adopted bills aimed at improving the procedures and legal framework for bringing cybercriminals to criminal liability. These changes were necessary to effectively counteract the growing cyber threats that have become particularly relevant in a time of war. The introduction of liability for cybercrime committed in times of war is necessary to ensure national security and protect the public interest of Ukraine. Such actions not only undermine critical infrastructure and information security, but can also be used by the aggressor as a tool of hybrid warfare.

It is proved that in order to comprehensively address the issue of preventing cybercrime, Ukraine needs to introduce additional regulations that will focus not only on responding to cyber threats, but also on more effective prevention of cybercrime.

In addition, it is necessary to introduce liability for the above criminal offences committed during martial law. Such unlawful acts should be subject to severe sanctions, as the circumstances in the country require it. A person who harms the national interests of Ukraine in cyberspace and thus assists the aggressor in this war should be held liable in the same way as war criminals.

Key words: cybersecurity, cybercrime, criminal code, criminal offences, digital environment, cyber defence, prevention

Постановка проблеми. Використання цифрового середовища повинне відповідати законодавчим нормам і етичним стандартам, адже кожна дія може мати серйозні наслідки. Гармонізація зусиль громадян, суб'єктів господарювання та державних органів є ключовим чинником ефективного кіберзахисту, особливо в умовах воєнного стану. Спільна робота на всіх рівнях дозволяє забезпечити скоординованість дій, швидке реагування на загрози та стійкість кіберпростору [1].

Кіберзлочинність є глобальною проблемою, яка постійно еволюціонує, і потребує скоординованих зусиль на національному та міжнародному рівнях. Для ефективного запобігання кіберзлочинам держави, включаючи Україну, розробляють і впроваджують різноманітні стратегії, програми та заходи, зокрема розробка середньострокових програм запобігання, посилення міжнародного співробітництва та рівня обізнаності населення у сфері кібергігієни тощо. Україна рухається у правильному напрямку, але ефективне запобігання кіберзлочинів вимагає постійної модернізації та адаптації до нових викликів. Співпраця держави, громадянського суспільства та міжнародних партнерів є ключем до успіху у цьому питанні.

На сьогодні у нашій країні відсутній єдиний підхід до створення загальної системи запобігання злочинності у сфері кібербезпеки, який є необхідним кроком для захисту суспільства та держави в умовах зростання кіберзагроз. Така система повинна базуватися на комплексному підході, який охоплює всі аспекти кібербезпеки. Так, для створення ефективної системи захисту в кіберпросторі необхідно інтегрувати освітні, технічні та організаційні заходи. Саме тому обрана нами тема дослідження є актуальною., особливо під час війни, коли кількість кіберзагроз зростає кожного дня.

Метою цього дослідження є вивчення та узагальнення проблемних аспектів забезпечення кібербезпеки в Україні під час воєнного стану та визначення можливих напрямів їх усунення.

Стан опрацювання проблематики. Питання забезпечення кібербезпеки розглядалися багатьма науковцями. Зазначеним питанням приділяли увагу такі дослідники як О.М. Бандурка, В.В. Василевич, В.В. Голіна, Б.М. Головкін, А.П. Закалюк, О.М. Литвинов, В.В. Марков, М.І. Сащенко, В.О. Туляков, І.В. Жук, Я.В. Левківська та інші.

Виклад основного матеріалу. Варто почати з того, що збільшення кількості кіберзлочинів є комплексною проблемою, яка має як загальні, так і спеціальні причини, зокрема:

1) висока завантаженість правоохоронних органів. Причинами цього є обмеженість ресурсів правоохоронних органів, які змушені розглядати широкий спектр правопорушень та нестача спеціалістів, здатних розслідувати кіберзлочини. Наприклад, 2021 року було виявлено близько 299 160 кримінальних правопорушень [2].

2) анонімність та глобальний характер кіберзлочинів. Така ситуація пов'язана з можливістю приховування особи через VPN, Tor та інші засоби анонімізації, а також географічною розподіленістю злочинців, яка ускладнює юрисдикційні питання.

3) стрімкий технологічний прогрес. Так, постійно впроваджуються нові технології, які кіберзлочинці активно експлуатують.

4) брак кібергігієни. Причиною цього є недостатня обізнаність користувачів про безпечну поведінку в Інтернеті та відсутність відповідальності за недотримання кібергігієни.

З метою усунення вищенаведених загроз та з метою фомування цілісної стратегії кібербезпеки в Україні сформоване нормативно-правове підгрунтя. Закон України «Про основи забезпечення

кібербезпеки України» забезпечує чітке визначення основних термінів і завдань у сфері кібербезпеки. Ця концепція є основою для створення ефективної системи протидії загрозам у кіберпросторі та гарантує захист життєво важливих інтересів держави й суспільства. Згідно з цим Законом, кібербезпека - це захист життєво важливих інтересів людини, громадянина, суспільства і держави в умовах кіберпростору, що сприяє постійному розвитку інформаційного суспільства та цифрового комунікаційного середовища. Ця концепція спрямована на безперервне виявлення, запобігання та нейтралізацію реальних та потенційних загроз національній безпеці України у кіберпросторі. Кіберзахист – це комплекс організаційних, правових, інженерно-технічних заходів, включаючи заходи криптографічного та технічного захисту інформації. Ці заходи призначені для попередження кіберінцидентів, виявлення та захист від кібератак, а також для відновлення стабільності та надійності функціонування комунікаційно-технологічних систем. Кіберзлочинність (комп'ютерна злочинність) визначається як суспільно небезпечне кримінально протиправне діяння в кіберпросторі або через його використання, за яке передбачена відповідальність за законом України або яке визнається кримінальним парвопорушенням за міжнародними договорами України [3].

У зв'язку з зазначеним сьогодні в Україні разом з докорінними змінами у зовнішньому та внутрішньому безпековому середовищі, появою нових викликів та загроз в умовах гібридної війни активно реформується сектор безпеки і оборони з урахуванням специфіки кіберпростору. Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020, є важливим документом, який визначає пріоритети та шляхи зміцнення безпеки держави, зокрема в умовах гібридної війни та з урахуванням специфіки кіберпростору [4].

Основними напрямами Стратегії національної безпеки України у сфері кібербезпеки є:

1) захист критичної інфраструктури, що реалізується шляхом визначення та посилення захисту об'єктів, важливих для функціонування держави, таких як енергетичні системи, транспорт, зв'язок, фінансовий сектор;

2) розвиток технологій, зокрема інвестування у створення та впровадження сучасних технологій для моніторингу, виявлення та нейтралізації кіберзагроз та вдосконалення криптографічного захисту даних;

3) посилення кібергігієни шляхом підвищення обізнаності населення про основи кіберзахисту;

4) інтеграція з міжнародними стандартами, зокрема посилення співпраці з країнами-партнерами для обміну досвідом та технологіями, впровадження міжнародних стандартів, таких як ISO/IEC 27001 тощо.

З метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави окремим документом розроблена і затверджена Указом Президента України від 14 травня 2021 року № 447/2021 Стратегія кібербезпеки України [4].

Указ Президента України від 13 лютого 2017 року № 32/2017, який затвердив рішення Ради національної безпеки і оборони України від 29 грудня 2016 року, відображає актуальність і важливість питання кібербезпеки для захисту національних інтересів. Документ спрямований на нейтралізацію загроз у кіберпросторі, зокрема щодо об'єктів критичної інфраструктури.

Цей указ став одним із перших стратегічних документів, який комплексно підійшов до вирішення проблем кібербезпеки в Україні. Він заклав основу для створення національної системи захисту в кіберпросторі та впровадження сучасних технологій, необхідних для протидії новим викликам [5].

У Кримінальному кодексі України кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку закріплено в розділі 16 [6]. Деякі норми щодо превенції містяться в Конституції України, в Кримінальному процесуальному кодексі України, проте вони є більш декларативними і потребують подальшого опрацювання та вдосконалення.

Проте у законодавстві присутня невизначеність термінів у сфері кібербезпеки, що є суттєвою проблемою, яка впливає на ефективність запобігання кіберзлочинності, координацію дій між органами влади та правове регулювання. Такі кроки є важливими для створення єдиного підходу до вирішення цієї проблеми. Чітке визначення термінів дозволить забезпечити єдність у правозастосуванні та спростить роботу правоохоронних органів, прокуратури та судів.

Ми пропонуємо основні поняття у сфері кібербезпеки визначати таким чином:

Кіберпростір – сукупність цифрових мереж і систем, що дозволяють передавати, обробляти та зберігати інформацію.

Кіберзлочин – кримінально протиправні дії, спрямовані на порушення безпеки інформаційних систем або використання їх для незаконних цілей.

Кібератака – спроба несанкціонованого доступу, руйнування, маніпулювання або знищення інформаційних ресурсів.

Об'єкти критичної інфраструктури – об'єкти, порушення функціонування яких може призвести до значних економічних, екологічних, соціальних або політичних наслідків.

Окрім цього, потребує удосконалення чинне законодавство в контексті імплементації міжнародних стандартів. Зокрема, імплементація Конвенції про кіберзлочинність (Будапештської конвенції) є важливим кроком для України у зміцненні правових і процедурних механізмів боротьби з кіберзлочинністю. Особливої уваги потребує виконання статей, які стосуються збору, збереження та розкриття комп'ютерних даних і руху інформації. Доцільно внести до чинного законодавства положення таких статей:

Стаття 16 – Термінове збереження комп'ютерних даних, які зберігаються: ця стаття передбачає впровадження процедур, які дозволяють правоохоронцям наказувати тимчасове збереження даних, налагодження співпраці з провайдерами інтернет-послуг.

Стаття 17 – термінове збереження і часткове розкриття даних про рух інформації, яка охоплює не лише збереження даних, але й їх часткове розкриття для встановлення джерела або адресата інформації.

Стаття 19 – обшук і арешт комп'ютерних даних, які зберігаються, яка надає повноваження правоохоронцям здійснювати обшуки, вилучення та збереження комп'ютерних даних у рамках розслідування.

Стаття 20 – збирання даних про рух інформації у реальному масштабі часу, що передбачає впровадження технологій для перехоплення та аналізу руху інформації.

Стаття 21 – перехоплення даних змісту інформації: це положення, які дозволяють здійснювати перехоплення інформації із забезпеченням відповідних судових дозволів.

Варто зазначити, що запобігання кіберзлочинності вимагає не лише нормативно-правового забезпечення, але й стратегічного підходу, який враховує короткострокові, середньострокові та довгострокові цілі. Це забезпечує системний захист інформаційних ресурсів, ефективну протидію кіберзлочинам і притягнення до відповідальності осіб, які розробляють та використовують кримінально протиправні схеми.

Основними засадами такого підходу до запобігання кіберзлочинності є:

1. Створення та вдосконалення законодавства у сфері кібербезпеки та протидії кіберзлочинності.
2. Удосконалення кримінального та адміністративного законодавства для забезпечення належного покарання за кіберзлочини.
3. Введення стандартів захисту інформаційних ресурсів, обов'язкових для державних установ та приватного сектору.
4. Розробка стратегій кіберзахисту та впровадження сучасних технологій для виявлення та попередження кіберзагроз;
5. Створення спеціалізованих підрозділів, такі як підрозділи кіберполіції, центри реагування на кіберінциденти (CERT) тощо.
6. Підготовка фахівців з кібербезпеки, організація тренінгів для співробітників правоохоронних органів і суддів щодо специфіки кіберзлочинів;
7. Участь у міжнародних програмах боротьби з кіберзлочинністю, спільні операції з іншими країнами для розкриття міжнародних кіберзлочинних угруповань.
8. Просвітницькі кампанії серед населення для підвищення обізнаності про кіберзагрози.
9. Інвестиції в модернізацію технологічної бази для забезпечення стійкості до нових видів загроз.
10. Співпраця з приватним сектором для виявлення осіб, причетних до створення шкідливого програмного забезпечення.

Сьогодні не можна оминати увагою й інформаційну війну, яка ведеться росією проти України.

Під час першого місяця війни в Україні парламент оперативно прийняв законопроєкти, спрямовані на вдосконалення процедур і правових основ притягнення кіберзлочинців до кримінальної відповідальності. Ці зміни були необхідними для ефективної протидії зростаючим кіберзагрозам, які стали особливо актуальними в умовах війни.

1. Зміни до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» стосовно поліпшення досудового розслідування за гарячими слідами та боротьби з кібератаками, № 2137-IX від 15.03.2022.
2. Зміни до Кримінального кодексу України щодо ефективної протидії кіберзлочинності під час воєнного стану, № 2149-IX від 24.03.2022.

Закон України № 2149-IX є одним із ключових нормативно-правових актів, спрямованих на підвищення рівня національної кібербезпеки, створення ефективної системи захисту від кіберзагроз і адаптацію національного законодавства до сучасних викликів у сфері кіберзлочинності.

Проте, з огляду на ці зміни, виникають питання щодо трансформації термінології та встановленні посиленої відповідальності за інші види кримінальних правопорушень у сфері кібербезпеки.

У новій версії до попередніх визначень були додані такі норми:

1. Дії, визначені частинами першою або другою цієї статті, якщо вони становлять витік, втрату, підроблення, блокування даних, спотворення процесу обробки даних або порушення установленого порядку його керівництва (стаття 361 Кримінального кодексу України), представляють нову правову конструкцію, проте в залежності від тлумачення вихідної структури у попередньому варіанті).
2. Заходи, передбачені частинами першою або другою цієї статті, якщо вони (...) призводять до створення небезпеки серйозних технічних аварій або екологічних проблем, загрози життю чи здоров'ю людей або інших серйозних наслідків (частина 4 статті 361 Кримінального кодексу України).
3. Дії, визначені частинами третьою або четвертою цієї статті, які вчиняються під час воєнного стану (частина 5 статті 361 Кримінального кодексу України) [6].

Введення нового законодавства, спрямованого на регулювання кібербезпеки та запобігання кіберзлочинності під час війни, є вкрай важливим для захисту національних інтересів України. В умовах кіберагресії та зростаючої кількості злочинів у сфері інформаційних технологій це дозволяє забезпечити безпеку держави та громадян, а також створює умови для ефективного реагування на нові виклики.

Запровадження відповідальності за кіберзлочини, вчинені в умовах війни, є необхідним для забезпечення національної безпеки та захисту суспільних інтересів України. Такі дії не лише підривають критичну інфраструктуру та інформаційну безпеку, але й можуть використовуватись агресором як інструмент гібридної війни.

Отже, ситуація з регулюванням кібербезпеки в Україні демонструє важливі кроки в бік інтеграції цієї сфери в загальну правову систему. Однак існують прогалини в законодавстві щодо запобігання злочинності в сфері кібербезпеки.

Для того, щоб комплексно вирішувати питання запобігання злочинності у сфері кіберзлочинності, Україні потрібно ввести додаткові нормативно-правові акти, що будуть орієнтовані не лише на реагування на кіберзагрози, але й на більш ефективне попередження кіберзлочинності. На нашу думку, це включає:

1) розробку окремого закону, що регламентуватиме специфіку запобігання кіберзлочинності;

2) удосконалення координації між правоохоронними органами, державними установами та приватним сектором у боротьбі з кіберзлочинами;

3) програму навчання та сертифікації фахівців у сфері кібербезпеки та кіберправосуддя.

Окрім цього, доведено необхідність впровадження відповідальності за вищезазначені кримінальні правопорушення, вчинені під час воєнного стану. За такі протиправні дії повинні передбачатися суворі санкції, оскільки обставини в країні вимагають цього. Особа, яка завдає шкоди національним інтересам України у кіберпросторі й у такий спосіб допомагає агресору в цій війні, повинна нести відповідальність аналогічно воєнним злочинцям [7].

У зв'язку з цим, запропоновано внести зміни до ст. 361 Кримінального кодексу України, виклавши ч. 5 у такій редакції: «Дії, передбачені частиною третьою або четвертою цієї статті, вчинені під час дії воєнного стану, – караються позбавленням волі на строк від десяти до п'ятнадцяти років або довічним позбавленням волі з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років» [7].

Також необхідно додати кваліфікуючу ознаку «вчинення кримінального правопорушення в умовах воєнного стану» до ряду статей Кримінального кодексу, зокрема: ст. 361^{-1} «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут», ст. 361^{-2} «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації», ст. 363^{-1} «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку».

Висновки. Забезпечення кібербезпеки в Україні є актуальним завданням у контексті зростання кіберзагроз, пов'язаних із війною, активізацією хакерських атак і поширенням кіберзлочинності. Відповідно до сучасних викликів, Україна реалізує низку стратегічних та оперативних заходів для забезпечення кібербезпеки.

Основними напрямами забезпечення кібербезпеки в Україні є:

1) розробка законодавчих актів, спрямованих на конкретні аспекти запобігання кіберзлочинності;

2) інвестиції в інфраструктуру кібербезпеки;
3) розширення міжнародної співпраці у сфері боротьби з кіберзлочинністю;
4) зміцнення освітніх програм для підготовки кадрів у сфері кіберзахисту;
5) створення регіональних центрів кібербезпеки для оперативного реагування на загрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Єрема М., Борисенко А., Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. Офіційний сайт «LIGAЗакон». URL: https://jurliga.ligazakon.net/ analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.
2. Єдиний звіт про кримінальні правопорушення по державі за жовтень 2021 року. Статистична інформація Офісу Генерального прокурора. URL: https://old.gp.gov.ua/ua/stst2011.html?dir_id=114140&libid=100820&c=edit&_c=fo#.
3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII // Сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/ aws/show/2163-19#Text.
4. Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020. Офіційний сайт представництва Президента України. URL: https://www.president.gov.ua/documents/3922020-35037
5. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення РНБО від 29 грудня 2016 року. Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/n0015525-16#Text.
6. Кримінальний кодекс України: Закон України від 05 квіт. 2001 р. № 2341-III / База даних «Законодавство України» / ВР України. URL: http://zakon4.rada.gov.ua/laws/show/2341-14.
7. Бодунова О.М. Кримінологічні засади запобігання злочинності у сфері інформаційних технологій: дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». Ірпінь, Державний податковий університет, 2024. 433 с.