УДК 342.6+341.1/.8
https://doi.org/10.34142/23121661.2025.41.02
orcid.org/0000-0003-1921-3041

В.В. Марченко

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ДІЇ РЕЖИМУ ВОЄННОГО СТАНУ: КОНСТИТУЦІЙНО-ПРАВОВИЙ ТА МІЖНАРОДНИЙ АСПЕКТИ

V. Marchenko

ENSURING INFORMATION SECURITY UNDER THE CONDITIONS OF MARTIAL LAW: CONSTITUTIONAL, LEGAL, AND INTERNATIONAL ASPECTS

Анотація. У статті досліджуються проблеми та законодавча база щодо забезпечення інформаційної безпеки під час дії режиму воєнного стану. Оскільки сучасні конфлікти все більше переходять у цифрову сферу, захист важливої інформаційної інфраструктури, боротьба з дезінформацією та захист національної безпеки стають ключовими пріоритетами. В ній досліджуються конституційно-правові та міжнародні аспекти інформаційної безпеки, розглядається роль міжнародно-правових інструментів та механізмів співпраці у протидії кіберзагрозам. Особлива увага приділяється застосуванню європейського законодавства, міжнародних конвенцій з кібербезпеки та регіональних угод, наголошуючи на їх важливості для сприяння скоординованій відповіді на виклики, спричинені збройними конфліктами в цифровій сфері. Наголошується на важливості міцної законодавчої бази, міжнародної співпраці та технологічних рішень для забезпечення інформаційної безпеки під час воєнного стану. Підкреслюючи відповідність України стандартам ЄС щодо захисту даних, в ній наголошує на необхідності міцної правової бази, міжнародного співробітництва та технологгічних рішень для забезпечення безпеки, довіри та цифрової трансформації, сприяючи інтеграції у глобальне інформаційне суспільство.

Ключові слова: інформаційна безпека, воєнний стан, кібербезпека, міжнародна співпраця, глобальна безпека.

Abstract. The article provides a thorough analysis of the challenges and legislative frameworks associated with ensuring information security during martial law. As modern conflicts increasingly extend into the digital domain, safeguarding critical information infrastructure, combating disinformation, and protecting national security emerge as essential priorities. The study explores constitutional, legal, and international aspects of information security, addressing the delicate balance between maintaining security and upholding fundamental rights, including freedom of expression, access to information, and privacy.

The constitutional analysis focuses on provisions applicable during martial law, offering insights into the legal basis for implementing information security measures. The legal dimension focuses on operational mechanisms such as cybersecurity strategies, legislative frameworks, and the roles of government agencies in mitigating information-related risks. The article evaluates the effectiveness of existing national legislation and policies, identifies shortcomings, and proposes reforms to enhance resilience against information threats during martial law.

At the international level, the study examines the role of global legal instruments and cooperative mechanisms in addressing cyber threats. Particular attention is paid to European legislation, international cybersecurity conventions, and regional agreements, highlighting their significance in enabling a coordinated response to the challenges posed by armed conflicts in the digital sphere.

The article emphasizes the importance of robust legislative frameworks, international collaboration, and technological solutions in ensuring information security during martial law. It underscores the need for Ukraine to align its legislative framework with European Union standards on data protection and information security. By adhering to EU directives, Ukraine aims to strengthen trust, resilience, and digital transformation, thereby protecting national interests, complying with global norms, and advancing its integration into the global information society.

Keywords: information security, martial law, Cybersecurity, international cooperation, global security

Постановка проблеми. В умовах дії режиму воєнного стану в Україні інформація функціонує як критично важливий стратегічний ресурс. За цих умов її роль стає ще більш важливою, оскільки вона зазнає постійних змін не лише щодо свого обсягу, але й щодо своєї точності, надійності та стратегічної цінності. Ефективне управління, розповсюдження та захист інформації безпосередньо впливають на національну безпеку, прийняття рішень і суспільну мораль, підкреслюючи її подвійну природу як активу, так і як потенційної загрози під час кризи.

Обсяг доступної інформації зростає в геометричній прогресії, збільшується різноманітність і складність її джерел, постійно розробляються інноваційні методи отримання, обробки та поширення інформації. Одночасно зростає кількість користувачів, які покладаються на інформаційні ресурси, інтегруючи інформацію практично в усі сфери соціального, економічного та політичного життя. Однак, поряд із цими досягненнями, в умовах воєнного стану та протистояння російській агресії, сучасне інформаційне середовище відзначається значними ризиками. Це, зокрема, суспільна вразливість до шкідливої або маніпулятивної інформації, поширеність шахрайства, промислове шпигунство в електронних мережах і тривожне зростання кіберзлочинності. Такі виклики вимагають надійних структур для захисту цілісності, безпеки та конфіденційності інформації.

Актуальність усунення цих ризиків підкреслюється в основних нормативних актах, наприклад, у «Концепції розвитку електронного урядування в Україні» [1], яка визначає інформаційну безпеку та конфіденційність як один із

фундаментальних принципів електронного урядування. Цей принцип наголошує на захисті даних в електронних системах від несанкціонованого доступу, забезпеченні їх доступності, цілісності та конфіденційності.

На практиці Україна запровадила кілька законодавчих заходів для посилення інформаційної безпеки, що прямо виходить з Конституції України, яка закладає основи інформаційної безпеки в державі. Стаття 32 гарантує захист персональних даних, підкреслюючи заборону несанкціонованого збирання, зберігання, використання чи поширення конфіденційної інформації про фізичних осіб. Стаття 17 висвітлює відповідальність держави за забезпечення безпеки свого інформаційного простору [2]. Закон України «Про основні засади кібербезпеки в Україні» (2017) [3] встановлює комплексну основу для захисту критичної інформаційної інфраструктури країни та визначає обов'язки різних зацікавлених сторін, включаючи державні органи, приватні підприємства та громадян, у боротьбі з кіберзагрозами. Наприклад, Національний координаційний центр з кібербезпеки [4], що діє при Раді національної безпеки і оборони України, відіграє ключову роль у впровадженні заходів із кібербезпеки. Центр здійснює моніторинг кіберзагроз, координує національні заходи реагування на кіберінциденти та співпрацює з міжнародними партнерами для підвищення стійкості інформаційної інфраструктури України.

На міжнародному рівні Україна є активним учасником Будапештської конвенції про кіберзлочинність (2001) [5], провідного міжнародного договору, спрямованого на гармонізацію національного законодавства, удосконалення методів розслідування та сприяння міжнародній співпраці у боротьбі з кіберзлочинністю. Через цю структуру Україна співпрацює з такими організаціями, як Європол та Інтерпол, щоб протидіяти транснаціональним кіберзагрозам.

Крім того, такі практичні заходи, як створення захищених центрів обробки даних, розробка зашифрованих протоколів зв'язку та регулярні аудити критично важливих інформаційних систем, демонструють відданість України забезпеченню інформаційної безпеки. Наприклад, державні ініціативи, такі як платформа «Дія», яка об'єднує численні публічні сервіси в єдиний цифровий інтерфейс, включають розширені протоколи безпеки для захисту даних користувачів від несанкціонованого злому.

Метою даної статті є комплексне дослідження багатоаспектних елементів забезпечення інформаційної безпеки в умовах дії режиму воєнного стану. Це передбачає аналіз правових, технічних та організаційних заходів, які наразі діють для забезпечення конфіденційності, цілісності та доступності інформації. Крім того, стаття має на меті виявлення прогалини та розробку дієвих рекомендацій щодо вдосконалення загальної системи безпеки, узгодженої з міжнародними стандартами та національними нормативними актами.

Аналіз наукових джерел. Питання інформаційної безпеки України, в тому числі в умовах дії режиму воєнного стану, перспектив розвитку, методологіч-

ного та теоретичного підґрунтя досліджуваної проблеми висвітлювалося в наукових працях таких авторів, як: Дубов Д.В. [6], Золотар О. О. [7], Кавин С. Я. [8], Килимник І. І. [9], Левченко О. В. [10], Пархоменко-Куцевіл О. І. [11], Семенченко А.І. [12], Ткачук Т. Ю. [13], Шемчук В. В. [14] та інші. Інтерпретація інформаційної безпеки Дубовим Д.В. висвітлює її сутність як здатність нейтралізувати шкідливий вплив різних видів соціальної інформації. Дослідник визначає безпеку або як відсутність загрози, або як здатність надійно захиститися від неї. У цьому контексті захист інформації розуміється як активний процес, спрямований на запобігання несанкціонованим діям з інформацією в системі [6]. Отже, небезпечними визнаються інформаційні впливи, які призводять до дестабілізуючих наслідків або посягають на інтереси особи, суспільства, держави. На думку А. І. Семенченка і В. М. Дрешпака до загроз інформаційної безпеки слід віднести такі, як: порушення конфіденційної інформації, порушення цілісності інформації та порушення доступності інформації [12, с.23].

Утім, питання щодо визначення змісту інформаційної безпеки, її трансформації в умовах дії режиму воєнного стану та сучасної війни залишаються малодослідженими.

Виклад основного матеріалу. На сучасному етапі розвитку суспільства і держави законодавець наполегливо наголошує на критичному питанні інформаційної безпеки в контексті інформаційного суспільства та електронного урядування. Цей наголос відображає зростаючу важливість безпечних та ефективних систем управління інформацією, зокрема, оскільки цифрові технології стають невід'ємною частиною процесів управління. Крім того, прагнення України отримати повноправне членство в Європейському Союзі вимагає узгодження її правової бази з європейськими принципами, нормами та стандартами в управлінні інформаційним суспільством та захисті даних.

Процес узгодження зумовлений необхідністю гармонізувати українське законодавство з правовими стандартами ЄС, які ґрунтуються на міцній нормативно-правовій основі, розробленій для забезпечення безпеки даних, конфіденційності та ефективного функціонування електронних комунікаційних систем. Орієнтирами для цієї гармонізації стали кілька ключових нормативних актів:

1) Директива 95/46/ЄС (24.10.1995 р.) [15] про захист осіб щодо обробки персональних даних і про вільне переміщення таких даних. Ця директива встановлювала фундаментальні принципи захисту даних, включаючи прозорість, обмеження цілей і мінімізацію даних. Незважаючи на те, що у 2018 році її замінив Загальний регламент про захист даних (GDPR) [16], її принципи залишаються невід'ємною частиною чинного законодавства ЄС про захист даних і є основоположним керівництвом для приведення українського законодавства в норму;

2) Директива 98/34/ЄС (22.06.1998 р.) [17] про встановлення процедури надання інформації у сфері технічних стандартів і правил. Ця директива наголошує на гармонізації технічних стандартів і важливості прозорості технічних регламентів, що безпосередньо підтримує сумісність систем в рамках єдиного цифрового ринку;

3) Директива 1999/93/ЕС (13.12.1999 р.) [18] про рамки Співтовариства для електронних підписів. Ця директива забезпечує правову основу для визнання електронних підписів, забезпечення їх дійсності та сприяння їх використанню в електронних транзакціях. Україна активно імплементувала подібні положення, зокрема через Закон України «Про електронну ідентифікацію та електронні довірчі послуги» (2017), який відповідає стандартам ЄС;

4) Директива 2002/21/ЕС (7.08.2002 р.) [19] про загальну нормативну базу для електронних комунікаційних мереж і послуг (Рамкова Директива). Ця директива встановлює загальну основу для регулювання електронних комунікаційних мереж і послуг, спрямованих на сприяння конкуренції, забезпечення захисту споживачів і заохочення інновацій;

5) Конвенція № 108 Ради Європи (28.01.1981 р.) [20] про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Як сторона, яка підписала цю конвенцію, Україна зобов'язана вживати заходів, що забезпечують законну обробку персональних даних, надалі наближаючи свою практику до європейських стандартів.

Україна зробила значні кроки для інтеграції європейських стандартів у своє національне законодавство. Наприклад, Закон України «Про захист персональних даних» (2010) [21] було розроблено у відповідь на вимоги Директиви 95/46/ЄС та Конвенції № 108, що містить ключові принципи захисту даних, такі як згода, прозорість і відповідальність.

Так само Закон України «Про електронні комунікації» (2020) [22] відображає положення Директиви 2002/21/ЕС, встановлюючи нормативну базу для електронних комунікаційних мереж і послуг, сприяючи конкуренції та захищаючи права споживачів.

Впровадження платформи «Дія», ініціативи цифрового урядування України демонструє практичне застосування цих нормативних баз. Платформа використовує передові системи електронного підпису та безпечні протоколи зв'язку, що забезпечує дотримання Директиви 1999/93/ЕС та принципів GDPR. Крім того, поточні законодавчі реформи України щодо захисту даних та електронного урядування підтримуються програмами технічної допомоги ЄС, такими як ініціатива EU4Digital [23], яка сприяє узгодженню цифрових політик і стандартів між Україною та ЄС.

Ключову роль у формуванні та реалізації державної політики інформаційної безпеки відіграє Державна служба спеціального зв'язку та захисту

інформації України [24]. До її обов'язків входить криптографічний та технікний захист інформації, охорона державних інформаційних ресурсів, забезпечення безпечного функціонування систем електронного документообігу в державних установах та органах місцевого самоврядування. Крім того, вона контролює розробку та застосування електронних цифрових підписів, забезпечуючи їх безпечне використання та сприяючи їх прийняттю в державних установах і органах місцевого самоврядування. Ці зусилля підкріплюються нормативними актами, зокрема Законом України «Про електронну ідентифікацію та електронні довірчі послуги» (2017 р.) [25], який приводить систему електронного цифрового підпису України у відповідність до Регламенту ЄС (Регламент eIDAS № 910/2014) [26], що полегшує взаємодію в електронних транзакціях.

Варто відзначити роботу Міністерства цифрової трансформації України, яке бере активну участь у визначенні пріоритетних напрямів інформатизації та забезпеченні інформаційної безпеки держави. Одним із важливих завдань є інтеграція безпечних інформаційно-комунікаційних технологій у діяльність органів виконавчої влади, включаючи сприяння безпечному електронному документообігу. Йдеться про впровадження системи «Трембіта», яка підтримує безпечний та ефективний обмін даними між державними органами, та вдосконалення цифрових публічних послуг через портал «Дія». Ці ініціативи демонструють застосування законодавчих повноважень для сприяння прозорості та ефективності при одночасному захисті конфіденційної інформації.

Інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства, держави, що забезпечує запобігання заподіянню шкоди. Відповідно можна визначити низку проблем, які впливають на інформаційну безпеку держави, а саме:

а) неповнота, несвоєчасність або недостовірність інформації. Наприклад, забезпечення доступу громадян і державних органів до своєчасної та точної інформації є критично важливим, особливо в ситуаціях екстреного реагування;

б) в умовах негативного інформаційного впливу боротьба з дезінформацією та шкідливим контентом є пріоритетом держави. Наприклад, Україна співпрацює з ЄС для протидії онлайн-кампаніям дезінформації через такі ініціативи, як Оперативна робоча група зі стратегічних комунікацій (англ. East StratCom Task Force), яка працює над виявленням і викриттям російських наративів дезінформації;

в) негативні наслідки використання інформаційно-комунікаційних технологій. Так, враховуючи ризики кібератак і зломів, в Україні була прийнята Стратегія кібербезпеки України [27], яка встановлює механізми реагування на загрози, пов'язані з інформаційно-комунікаційними технологіями, і їх пом'якшення;

г) несанкціоноване розповсюдження, використання та порушення цілісності, конфіденційності та доступності інформації. Так, Закон України «Про захист персональних даних» [21] забезпечує законну та безпечну обробку персональних даних, узгоджуючи з глобальними стандартами, такими як Загальний регламент ЄС щодо захисту даних (GDPR) [16].

Хоча українське законодавство передусім розглядає інформаційну безпеку як питання захисту життєво важливих інтересів людини, суспільства та держави, це поняття можна розглядати й з іншого боку.

По-перше, інформаційна безпека передбачає розгортання передових технологій, таких як блокчейн для безпечного керування даними або штучний інтелект для виявлення загроз. Наприклад, в Україні досліджується технологія блокчейн [28] для безпечного керування реєстром власності, забезпечення цілісності та прозорості даних.

По-друге, інформаційна безпека лежить в основі економічної ста більності, захищаючи інтелектуальну власність і конфіденційні бізнес-дані. Національний координаційний центр кібербезпеки співпрацює з приватними структуррами для забезпечення безпеки критичної економічної інфраструктури.

По-третє, прагнення України до європейської інтеграції вимагають дотримання стандартів ЄС щодо інформаційної безпеки, сприяння довірі та співпраці в транскордонних цифрових взаємодіях. Участь у таких структурах, як ініціатива EU4Digital, є прикладом цього зобов'язання.

По-четверте, інформаційна безпека також перетинається із забезпеченням права на приватне життя та свободу інформації. Діяльність Уповноваженого Верховної Ради України з прав людини щодо моніторингу практик захисту даних підкреслює цей вимір.

Інформаційна безпека передбачає усунення ризиків, які можуть призвести до шкоди або втрат через ненадійність, неповноту або несвоєчасність інформації. Вона також поширюється на пом'якшення ризиків, пов'язаних з несанкціонованим використанням інформаційних технологій та доступом до державних електронних ресурсів. Ключові елементи включають: забезпечення доступу до конфіденційної інформації лише уповноваженим особам і гарантія того, що інформаційні ресурси залишаються доступними для законного використання, особливо в критичних операціях.

Для національного урядування та державного управління інформаційна безпека є центральною темою. Вона охоплює розробку та впровадження комплексних стратегій для забезпечення безпечного електронного урядування. Наприклад, Закон України «Про основні засади кібербезпеки в Україні» [3] встановлює інституційні основи безпеки кіберпростору. Ухвалення Національної програми інформатизації [29] визначає пріоритет інтеграції безпечних цифрових рішень у державне управління, що відповідає міжнародним стандартам.

Ефективні механізми інформаційної безпеки повинні вирішувати першочергові та нові ризики в електронному урядуванні. Ці механізми охоплюють набір принципів, методів і засобів, спрямованих на безпечне надання, отримання, передачу, використання, зберігання та захист інформації в системах електронних документів.

Важливого значення в умовах режиму воєнного стану набуває інформаційна безпека в електронному документообігу, що потребує багатовимірного підходу, який включає такі елементи:

1) правові, які встановлюють правову базу для безпечної електронної взаємодії;

2) технічні, що захищають конфіденційні дані в електронних системах;

3) кадрові, що покращують спроможність урядовців керувати захищеними системами електронних документів;

4) фінансові: асигнування з державного бюджету на реалізацію стратегій кібербезпеки демонструють пріоритетність інформаційної безпеки;

5) методологічні, тобто рекомендації Кабінету Міністрів України щодо безпечного використання систем електронного документообігу, які стандартизують практику в органах виконавчої влади.

Сучасна інформаційна сфера стикається з різноманітними комплексними та динамічними ризиками та загрозами інформаційній безпеці, які загрожують людині, суспільству та державі.

Ці загрози можна класифікувати на основі їх природи та впливу на інформацію, системи даних і основні права користувачів:

1. Крадіжка інформації та захищених даних: несанкціонований доступ і викрадання даних, включаючи комерційну таємницю, особисті дані та державну таємницю.

2. Знищення інформації та програмного забезпечення: навмисні дії з видалення або пошкодження даних і програмного забезпечення, критичного для роботи технічних систем.

3. Незаконне перехоплення інформації: несанкціоноване прослуховування комунікацій або передачі даних, що порушує конфіденційність.

4. Модифікація інформації та програмного забезпечення: несанкціонована зміна даних або програмного забезпечення з метою маніпулювання результатами або ненадійності систем.

5. Незаконне використання інформації та програмного забезпечення: використання інформації та запатентованого програмного забезпечення без дозволу для отримання особистої або фінансової вигоди.

6. Порушення або виведення з ладу комп’ютерів і мереж: цілеспрямовані атаки з метою вимкнення або погіршення функціональності ІТ-систем.

7. Приховування інформації: приховування або нерозголошення важливої інформації, яка зачіпає інтереси окремих осіб, суспільства чи держави.

8. Порушення прав на персональні дані: несанкціонований збір, зберігання та неправомірне використання персональних даних, що порушує конфіденційність і основні права.

Загрози інформаційній безпеці в сучасному цифровому світі охоплюють широкий спектр викликів, від технічних порушень до ерозії основних прав. Комплексна законодавча та нормативна база України, узгоджена з міжнародними стандартами, спрямована на пом'якшення цих ризиків шляхом поєднання превентивних заходів, можливостей реагування на інциденти та міжнародного співробітництва. Постійно адаптуючись до нових загроз, таких як кампанії з дезінформації та передові кібератаки, держава забезпечує захист критичних інформаційних активів, цілісність систем і прав своїх громадян.

На основі викладеного матеріалу можна окреслити деякі практичні рекомендації.

По-перше, для забезпечення інформаційної безпеки, особливо для держави, яка перебуває під постійною загрозою, необхідна надійна правова база. Є сенс включити захист кіберпростору та інформаційну безпеку як пріоритет національної безпеки до Конституції України. Наприклад, Естонія змінила свої закони після неодноразових кібератак, щоб підвищити стійкість держави.

По-друге, на законодавчому рівні закріпити визначення критичної інформаційної інфраструктури, покарання за кіберзлочини та обов'язкове звітування про порушення безпеки.

По-третє, запровадити суворіші правила для запобігання кампаніям дезінформації, особливо тим, які спрямовані на дестабілізацію державних структур. Наприклад, Закон Німеччини «Про захист прав користувачів у соціальних мережах» (NetzDG) [30] забезпечує основу для боротьби з незаконним вмістом у соціальних мережах.

По-четверте, впровадити систему виявлення загроз на основі штучного інтелекту для ідентифікації, аналізу та реагування на загрози в реальному часі [28].

По-п'яте, для забезпечення цілісності даних і захисту конфіденційних комунікацій вкрай необхідним є впровадження технології блокчейну. На теперішній час вже є позитивні напрацювання в цій сфері, наприклад, система електронного урядування Естонії ефективно використовує блокчейн для кібербезпеки.

По-шосте, людський фактор часто є найслабшою ланкою кібербезпеки. Нарощування потенціалу та підвищення обізнаності є життєво важливими. Для цього необхідно проводити обов'язкове навчання для урядовців і військовослужбовців щодо найкращих практик кібербезпеки та пом'якшення їх загроз. Важливим є наукове та дослідницьке співробітництво для розробки навчальних програм з кібербезпеки та сприяння інноваціям у цій галузі.

По-сьоме, глобальні виклики вимагають спільних рішень. Міжнародне партнерство посилює можливості інформаційної безпеки [28].

Є необхідність розширити двосторонні та багатосторонні угоди щодо обміну розвідданими, спільного аналізу загроз і скоординованої реакції на кіберінциденти, а також створити механізми для ефективної співпраці в розслідуванні та переслідуванні кіберзлочинів, включаючи угоди про екстрадицію кіберзлочинців. Крім того, важливим є зміцнення регіональних альянсів, таких як ОБСЄ або Стратегія кібербезпеки Європейського Союзу, для покращення координації та спільного використання ресурсів і співпраця з міжнаціональними технологічними компаніями, щоб використовувати їхній досвід та інфраструктуру для захисту критично важливих систем.

Висновки. Динамічний характер інформації в умовах воєнного стану підкреслює її стратегічну цінність і вимагає комплексних заходів для пом'якшення пов'язаних ризиків. Впровадження надійної правової бази, активна участь у міжнародних угодах і розгортання передових технологічних рішень є важливими для захисту інформаційних ресурсів. Ці зусилля не лише захищають національні інтереси, але й зміцнюють довіру та стійкість у швидкозмінному цифровому ландшафті.

Гармонізація законодавчої бази України зі стандартами ЄС у сфері управління інформацією та захисту даних є не просто технічною вимогою, а стратегічним імперативом інтеграції країни до європейської спільноти [31]. Прийнявши та імплементувавши такі директиви, як щодо захисту персональних даних, електронних підписів та комунікаційних мереж, Україна будує міцну правову основу, яка забезпечує як інформаційну безпеку, так і відповідність європейським нормам, зміцнюючи довіру та співпрацю в епоху цифрових технологій. Інституційна та законодавча база інформаційної безпеки в Україні відображає багатовимірний підхід, який відповідає на виклики цифрової ери. Використовуючи технологічний прогрес, сприяючи міжнародній співпраці та дотримуючись світових норм, Україна прагне зміцнити свою екосистему інформаційної безпеки. Ці зусилля не лише захищають державні ресурси та суспільні інтереси, але й відповідають ширшим цілям цифрової трансформації та інтеграції у глобальне інформаційне суспільство.

Література

1. Про схвалення Концепції розвитку електронного урядування в Україні / https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text (дата звернення: 23.12.2024). **2.** Конституція України / https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 23.12.2024). **3.** Про основні засади кібербезпеки в Україні / https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 23.12.2024). **4.** Про Національний координаційний центр кібербезпеки / https://zakon.rada.gov.ua/laws/show/242/2016#Text(дата звернення: 23.12.2024). **5.** Конвенція про кіберзлочинність / https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 23.12.2024). **6.** Дубов Д.В. Основи електронного урядування. Навчальний посібник / Д.В. Дубов, С.В. Дубова – К.:

Центр навчальної літератури, 2006. – 176 с. **7.** Золотар О. О. Досвід правового забезпечення інформаційної безпеки в країнах Східного партнерства ЄС (Молдова, Грузія). Lex Portus. 2017. № 3 (5). С. 70–80. 251. **8.** Кавин С. Я. Правові засади забезпечення кібербезпеки в державах – членах Європейського Союзу. Актуальні проблеми держави і права. 2020. № 8. С. 51–58. **9.** Килимник І. І. Інформаційне суспільство та інформаційна безпека. Нові виклики та шляхи подолання інформаційних загроз. Науковий вісник Ужгородського нац. ун-ту. 2023. № 76. С. 53–57. **10.** Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія /О. В. Левченко. Житомир: Видавець ПП "Євро-Волинь", 2021. 172 с. **11.** Пархоменко-Куцевіл О. І. Проблеми забезпечення інформаційної безпеки під час здійснення військових операцій та бойових дій. Публічне управління і адміністрування в Україні. 2022. № 8. С. 177–181. **12.** Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А. І. Семенченка, В. М. Дрешпака. – К., 2017. Частина 13: Захист інформації в системах електронного урядування / [О. М. Хошаба]. – К.: ФОП Москаленко О.М., 2017. – 72 с. **13.** Ткачук Т. Ю. Забезпечення інформаційної безпеки: досвід окремих країн Східної Європи. Інформація і право. 2017. № 4. С. 62–72. **14.** Шемчук В. В. Загрози інформаційній безпеці: проблеми визначення та подолання. Експерт: парадигми юридичних наук і державного управління. 2020. № 1. С. 285–296. **15.** Директива 95/46/ЄС / https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 22.10.2024). **16.** Загальний регламент про захист даних / https://gdpr-text.com/uk/ (дата звернення: 04.01.2024). **17.** Директива 98/34/ЄС https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31998L0034 (дата звернення: 29.12.2024). **18.** Директива 1999/93/EC / https://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri= celex%3A31999L0093 (дата звернення: 02.01.2025). **19.** Директива 2002/21/EC / https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0021 (дата звернення: 02.01.2025). **20.** Конвенція № 108 Ради Європи / https://zakon.rada.gov.ua/laws/show/ 994_ 326#Text (дата звернення: 02.01.2025). **21.** Про захист персональних даних / https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 03.01.2025). **22**. Про електронні комунікації / https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 03.01.2025). **23.** Ініціатива EU4Digital / https://eufordigital.eu/ (дата звернення: 03.01.2025). **24.** Про Державну службу спеціального зв'язку та захисту інформації України / https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 02.01.2025). **25.** Про електронну ідентифікацію та електронні довірчі послуги / https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 02.01.2025). **26.** Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC / https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32014R0910 (дата звернення: 03.01.2025). **27.** Стратегія кібербезпеки України / https://zakon.rada.gov.ua/laws/show/ 447/ 2021#n12 (дата звернення: 04.01.2025). **28.** *Volodymyr Marchenko. Blockchain technologies in information security / Scientific Center of Innovative Researches, Relationship between public administration and business entities management-2022 /* https://conf.scnchub.com/index.php/RPABM/RPABM-2022/paper/view/412 (дата звернення: 04.01.2025). **29.** Положення про формування та виконання Національної програми інформатизації / https://zakon.rada.gov.ua/laws/show/ 119-2024-%D0%BF#Text (дата звернення: 04.01.2025). **30.** Закон Німеччини «Про захист прав користувачів у соціальних мережах» / https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/NetzDG_engl.pdf?__blob=publicationFile& (дата звернення: 04.01.2025). **31.** *Volodymyr Marchenko.* The evolution of information Security framework in Ukraine : European integration and legal perspectives. URL: https://conf.scnchub.com/index.php/ICEAF/ICEAF-2024/paper/view/806/256 (дата звернення: 04.01.2025).