АДМІНІСТРАТИВНЕ ТА ФІНАНСОВЕ ПРАВО

УДК 343.9:004.056.5
DOI https://doi.org/10.32782/2408-9257-2025-2-7

Біленець Д. А.,
кандидат юридичних наук, доцент,
доцент кафедри цивільного, господарського права
та приватно-правових дисциплін
Чернівецького навчально-наукового юридичного інституту
Національного університету «Одеська юридична академія»
https://orcid.org/0000-0003-0866-0698

ІНФОРМАЦІЙНА БЕЗПЕКА У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ: РОЛЬ КІБЕРПІДРОЗДІЛІВ НАЦПОЛІЦІЇ ТА СБУ

INFORMATION SECURITY IN THE FIELD OF STATE SECRETS PROTECTION: THE ROLE OF CYBER UNITS OF THE NATIONAL POLICE AND THE SECURITY SERVICE OF UKRAINE

У статті здійснено системний правовий аналіз забезпечення інформаційної безпеки у сфері охорони державної таємниці в умовах зростаючих кіберзагроз та воєнного стану. Визначено, що законодавче регулювання в Україні базується на комплексі нормативно-правових актів, які визначають повноваження органів безпеки, розподіляють відповідальність за збереження інформації з обмеженим доступом та встановлюють механізми реагування на інциденти, пов'язані з витоками державної таємниці. Окрему увагу приділено ролі Служби безпеки України як основного суб'єкта контррозвідувального захисту інформаційного простору, а також функціоналу кіберпідрозділів Національної поліції України, що дедалі активніше залучаються до розслідування кіберінцидентів, пов'язаних із поширенням, викраденням або знищенням секретної інформації.

У публікації окреслено наявні прогалини у правовому регулюванні міжвідомчої взаємодії між СБУ та НПУ, зокрема у частині оперативного обміну класифікованими даними, реагування на загрози в реальному часі, стандартизації електронного документообігу в умовах воєнного стану. Досліджено функціональні обмеження кіберпідрозділів поліції, що, не маючи формального доступу до держтаємниці, фактично виконують ключові технічні завдання в системі цифрового захисту. Визначено, що в умовах цифровізації, гібридної війни та загроз інформаційного тероризму необхідним є нормативне унормування функціонального симбіозу між правоохоронною та контррозвідувальною гілками безпекового сектору.

Особливу увагу приділено міжнародному досвіду, зокрема моделям реагування на кіберінциденти, запровадженим у країнах НАТО. Аналіз показує, що для України імплементація концепції «whole-of-government» є не лише питанням стратегічного вибору, а й практичної необхідності. Запровадження єдиної системи управління IT-ризиками та уніфікованих протоколів дій під час надзвичайних подій дозволить зміцнити стійкість державної інформаційної інфраструктури, мінімізувати втрати у разі кіберзагроз та забезпечити стабільність державного управління в умовах гібридної агресії.

Ключові слова: *інформаційна безпека, державна таємниця, Служба безпеки України, Національна поліція України, кіберзагрози, цифрова інфраструктура, режим секретності, управління IT-ризиками.*

The article provides a comprehensive legal analysis of information security assurance within the sphere of protecting state secrets amid growing cyber threats and martial law conditions. It is established that legislative regulation in Ukraine is grounded in a set of interrelated normative legal acts that define the powers of security agencies, delineate responsibility for safeguarding classified information, and outline mechanisms for responding to incidents involving the leakage of state secrets. Particular attention is devoted to the role of the Security Service of Ukraine as the main counterintelligence actor in the information security domain, as well as to the functions of cyber units of the National Police of Ukraine, which are increasingly involved in investigating cyber incidents related to the dissemination, theft, or destruction of classified information.

The publication highlights existing legal gaps in the interagency cooperation framework between the SSU and the NPU, especially regarding the operational exchange of classified data, real-time threat response, and the standardization of electronic document workflow under wartime conditions. The article examines the functional limitations of police

cyber units which, despite lacking formal access to state secrets, effectively perform key technical tasks within the national digital security system. It is emphasized that under conditions of digitalization, hybrid warfare, and information terrorism threats, there is an urgent need for legislative consolidation of the functional symbiosis between law enforcement and counterintelligence branches of the security sector.

Special attention is paid to international experience, particularly to cyber incident response models implemented in NATO member states. The analysis reveals that for Ukraine, the adoption of a "whole-of-government" approach is not only a matter of strategic alignment but also of practical necessity. The introduction of a unified IT risk management system and standardized emergency response protocols will enhance the resilience of the national information infrastructure, minimize potential losses from cyber threats, and ensure the continuity of public administration under conditions of hybrid aggression.

Key words: *information security, state secrets, Security Service of Ukraine, National Police of Ukraine, cyber threats, digital infrastructure, secrecy regime, IT risk management.*

Постановка проблеми. У контексті збройної агресії Російської Федерації проти України проблема захисту державної таємниці набула нових масштабів і трансформувалась у критично важливий аспект національної безпеки. Зростання кіберзагроз, поширення фішингових атак, втручання у телекомунікаційні системи та використання інформаційно-психологічного впливу вимагають перегляду традиційного підходу до охорони інформації з обмеженим доступом.

Особливої актуальності набуває питання узгодження дій між Службою безпеки України, яка є головним контррозвідувальним суб'єктом у сфері державної таємниці, та кіберпідрозділами Національної поліції України, які виконують оперативно-технічні функції у сфері реагування на інциденти в кіберпросторі. Відсутність чітких юридичних механізмів обміну інформацією, розмежування повноважень і регламентації спільних дій створює загрозу розмиття відповідальності та зниження ефективності державного контролю за збереженням таємної інформації.

Метою статті є комплексне дослідження правових засад функціонування системи інформаційної безпеки у сфері охорони державної таємниці в Україні, з акцентом на аналізі ролі та повноважень ключових суб'єктів – зокрема Служби безпеки України та кіберпідрозділів Національної поліції. У фокусі перебуває нормативне регулювання допуску до секретної інформації, реагування на кіберінциденти, виявлення та нейтралізація загроз, спричинених як зовнішніми, так і внутрішніми чинниками. Особливу увагу приділено взаємодії між правоохоронними та спеціальними органами в умовах гібридної війни, необхідності адаптації законодавства до цифрових реалій та формуванню дієвої моделі протидії витокам інформації в умовах збройного конфлікту.

Проблематика забезпечення інформаційної безпеки у сфері охорони державної таємниці набуває дедалі більшої актуальності в українському правничому дискурсі, що зумовлено як збройною агресією Російської Федерації, так і цифровою трансформацією сектору безпеки. Наукове підґрунтя становлять праці О.Г. Семенюка, який досліджує ознаки державної таємниці як предмета злочину, М.В. Гончарова – щодо концептуального розуміння інформаційної безпеки, а також С.Б. Гордієнка, який аналізує управління ІТ-ризиками на об'єктах критичної інфраструктури.

У фахових публікаціях все частіше висвітлюються аспекти взаємодії СБУ та кіберпідрозділів Нацполіції в умовах воєнного стану, наприклад у монографії О.В. Левченка щодо державної стратегії у сфері інформаційної безпеки. Нормативно-правову базу становлять закони України «Про державну таємницю», «Про основні засади забезпечення кібербезпеки України», «Про національну безпеку України» та інші акти, що визначають режим доступу до секретної інформації та функціональну компетенцію профільних органів. На сьогодні тема активно досліджується в контексті кіберзагроз, гібридних впливів та інтеграції у стандарти НАТО, що підтверджує її стратегічне значення для національної безпеки України.

Основний виклад матеріалу. Правове регулювання інформаційної безпеки в Україні у сфері охорони державної таємниці базується на системі взаємопов'язаних нормативно–правових актів, що охоплюють як спеціалізовані органи безпеки, так і загальні правила поводження з інформацією з обмеженим доступом.

Основу становить Закон України «Про державну таємницю», який визначає її як вид таємної інформації, розголошення якої може зашкодити національній безпеці, та закладає правові засади її охорони, зокрема в умовах цифровізації [1].

Провідну роль у забезпеченні режиму секретності закон закріплює за Службою безпеки України, що координує всі заходи з допуску, контролю й захисту державної таємниці [2]. Водночас окремі функції оперативного реагування на порушення режиму доступу до неї покладено на інші органи, зокрема Національну поліцію, яка діє в межах Закону України «Про Національну поліцію» [3].

Семенюк О. зазначив, що істотною властивістю державної таємниці, як предмета злочину, є обов'язкова наявність її специфічних ознак, без встановлення яких не може бути вирішено питання про притягнення особи до кримінальної відповідальності за вчинення злочинів у сфері охорони державної таємниці, кваліфікацію цих діянь та призначення покарання [4, с. 85].

Взаємозв'язок між інформаційною безпекою та державною таємницею набуває особливої актуальності в умовах цифровізації державного управління, електронного документообігу та розвитку телекомунікаційних технологій. У цьому контексті важливу роль відіграє Закон України «Про захист інформації в інформаційно-комунікаційних системах», який містить технічні та криптографічні вимоги до захисту даних, визначає правила роботи з конфіденційною інформацією та встановлює юридичну відповідальність за порушення режиму її обробки в електронному середовищі [5].

Науковець Гончаров М. акцентує увагу на тому, що державна політика забезпечення інформаційної безпеки повинна базуватися на наукових і методологічних розробках, систематизованих і об'єднаних в єдину концепцію. Вона може бути представлена як сукупність національних цілей, інтересів і цінностей; стратегії та тактики управлінських рішень і методів їх реалізації, що розробляються та реалізуються державною владою [6, с. 34].

Комплексне регулювання у цій сфері доповнюється Законом України «Про інформацію», який класифікує інформацію за режимом доступу, визначає обов'язки володільців щодо збереження, передачі та поширення даних і прямо визнає захист інформації елементом національної безпеки [7].

В умовах воєнного стану актуалізується необхідність посиленого контролю за інформаційними потоками, зокрема впровадження додаткових обмежень щодо обігу чутливої інформації та її поширення в мережі Інтернет.

Закон України «Про правовий режим воєнного стану» передбачає обмеження права на інформацію та зобов'язання державних органів встановлювати спеціальні правила доступу до інформації, що може містити державну таємницю або стосуватися обороноздатності, мобілізації, діяльності Збройних сил [8].

Комплексне регулювання інформаційної безпеки в Україні здійснюється відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», який встановлює принцип міжвідомчої взаємодії всіх суб'єктів сектору безпеки і оборони – зокрема СБУ, Національної поліції, Держспецзв'язку та НКЦК – з метою забезпечення цілісності, доступності та захисту інформації, у тому числі такої, що становить державну таємницю [9].

Окреме значення має Стратегія інформаційної безпеки, затверджена Указом Президента України, яка визначає стратегічні напрями державної політики у сфері кіберзахисту, зокрема в частині реагування на загрози, захисту критичної інфраструктури та координації дій державних органів у разі витоку охоронюваної законом інформації [10].

Важливо відзначити роль Закону України «Про національну безпеку України», де встановлено, що забезпечення інформаційної безпеки держави – один із пріоритетів сектору безпеки і оборони. Відповідно до закону, СБУ і інші органи зобов'язані реалізовувати політику у сфері захисту інформаційних ресурсів, протидіяти технічним розвідкам та інформаційно-психологічному впливу, у тому числі в цифровому середовищі [11].

Українське законодавство у сфері інформаційної безпеки та охорони державної таємниці формує узгоджену правову базу, що визначає компетенції державних органів, механізми допуску до секретної інформації та порядок реагування у разі її витоку або загрози.

Водночас цифровізація та воєнний стан вимагають не лише наявності нормативних актів, а й постійного оновлення їх змісту та підвищення ефективності ключових суб'єктів – передусім Служби безпеки України та Національної поліції. Центральну роль у цій системі відіграє саме СБУ, яка відповідає за контррозвідувальні заходи, допуск до державної таємниці та контроль за дотриманням режимно-секретних вимог. Відповідні повноваження закріплені, зокрема, у статтях 6-8 Закону України «Про державну таємницю» [1] та Законі України «Про Службу безпеки України» [2].

Підвищення рівня загроз у кіберпросторі стимулювало СБУ до модернізації підходів. Відомство сформувало внутрішні кіберструктури, що безпосередньо відповідають за виявлення, попередження і нейтралізацію кібератак. На сьогодні особливе місце посідає Ситуаційний центр забезпечення кібербезпеки при СБУ, який виконує роль оперативного командного вузла, у тому числі в режимі воєнного часу [12]. Центр збирає інформацію про кіберінциденти, координує дії із суміжними органами (CERT-UA, Нацполіція, НКЦК), здійснює оперативний аналіз вразливостей у державних ІТ-системах.

Служба безпеки України здійснює перевірки органів державної влади на відповідність вимогам щодо захисту державної таємниці та в разі виявлення порушень видає приписи про усунення недоліків. Найбільш вразливими залишаються локальні мережі з недостатнім шифруванням або відсутністю сертифікованого ПЗ [13]. При цьому важливо оцінювати не лише наявність у СБУ формальних повноважень, а й реальну здатність діяти проактивно в умовах цифрової трансформації. Відсутність відкритої аналітики щодо результатів контррозвідувальних заходів ускладнює об'єктивну оцінку ефективності роботи служби. Водночас позитивним є посилення співпраці СБУ з партнерами НАТО та ЄС – зокрема, участь у спільних навчаннях, як-от «Cyber Coalition», що сприяє вдосконаленню оперативного реагування на складні кібератаки.

Роль Служби безпеки України у сфері захисту державної таємниці виходить далеко за межі технічного забезпечення – ключовим чинником залишається людський фактор, зокрема витоки даних через недбалість персоналу, недостатній контроль ІТ-постачальників або навмисне розголошення відомостей. У зв'язку з цим СБУ має системно вдосконалювати внутрішні процедури, забезпечувати якісний відбір кадрів, розвивати міжвідомчу взаємодію та формувати професійну культуру роботи з інформацією з обмеженим доступом. Як системоутворюючий суб'єкт у цій сфері, СБУ повинна постійно адаптувати свої підходи до умов багаторівневих, у тому числі прихованих, кіберзагроз, модернізуючи інфраструктуру, підвищуючи прозорість у допустимих межах та забезпечуючи оперативну реакцію завдяки підтримці з боку держави.

У системі інформаційної безпеки України вагоме місце займають кіберпідрозділи Національної поліції, які з 2015 року функціонують як окремий оперативний блок із власною компетенцією у сфері боротьби з кіберзлочинністю. Їхні повноваження закріплені як у Законі України «Про Національну поліцію», так і в підзаконних нормативних актах, включаючи положення про Департамент кіберполіції та функціональні інструкції [3]. Основним завданням є виявлення, попередження та припинення правопорушень, пов'язаних із використанням цифрових технологій, комп'ютерних мереж і телекомунікацій.

Хоча Національна поліція не має прямого мандату на охорону державної таємниці, кіберпідрозділи дедалі частіше залучаються до розслідування інцидентів, пов'язаних із витоками секретної або конфіденційної інформації, зокрема через фішинг, злам систем або шкідливе ПЗ. Особливо небезпечними є випадки, що стосуються об'єктів критичної інфраструктури чи органів, які обробляють інформацію з грифом «таємно». У таких випадках кіберполіція виконує роль першої оперативної ланки: фіксує інцидент, розпочинає кримінальне провадження, проводить обшуки, цифрову експертизу, а далі – співпрацює з СБУ у межах статей 328, 330, 361 Кримінального кодексу України [14].

Після початку повномасштабної війни проти України з 2022 року кіберпідрозділи Національної поліції значно активізували діяльність із захисту державних інформаційних ресурсів, у тому числі електронних сервісів, банківських систем, інфраструктури ЗСУ та органів дер-

жавної влади. За офіційними даними Департаменту кіберполіції, лише у 2023 році було виявлено та ліквідовано понад 15 тисяч кіберінцидентів, частина з яких стосувалася інформації, що могла містити елементи державної таємниці [15].

Попри те, що поліція не має прямих повноважень у сфері охорони держтаємниці, її кіберпідрозділи де-факто виконують ряд критичних функцій у сфері реагування на цифрові загрози. Через відсутність формалізованих механізмів доступу до класифікованої інформації вони нерідко діють у «сірій зоні» – оперативно, але поза межами закріпленої юрисдикції.

З початку повномасштабного вторгнення у лютому 2022 року Україна фіксує інтенсивне зростання кібератак на урядові вебпортали, військові системи зв'язку та інформаційні ресурси об'єктів критичної інфраструктури. Значна частина з них супроводжувалась використанням шкідливого ПЗ типу Wiper, компрометацією електронної пошти та облікових записів держслужбовців. Метою атак були системи, що зберігають інформацію про державні контракти, оборонні закупівлі та пересування військ, тобто дані, які часто підпадають під режим державної таємниці [16].

У відповідь на ці загрози в умовах воєнного стану держава оперативно оновила нормативно–правову базу протидії кіберінцидентам, запровадила розпорядження РНБО, підзаконні акти та постанови уряду, які врегульовують міжвідомчу координацію та реагування [17]. У центральній ролі тут виступає CERT-UA як технічний центр раннього реагування. Паралельно СБУ розширила контррозвідувальні заходи, зокрема зосередившись на блокуванні інформаційно–психологічних операцій, які несуть загрозу національній безпеці. Лише у 2023 році СБУ нейтралізувала понад 4 тис. Онлайн-ресурсів, що поширювали дезінформацію або сприяли викраденню чутливої інформації [13].

Якщо раніше витоки державної таємниці здебільшого виникали через недбале поводження зі службовими документами або діяльність шпигунських мереж, то сьогодні основна загроза змістилась у цифрове середовище – зокрема через фішинг, підроблені домени органів влади, заражені зовнішні носії чи шкідливі оновлення програмного забезпечення. Попри розвиток технічного захисту, критичною залишається потреба в підготовці персоналу, чіткій інституційній взаємодії та швидкій комунікації. Держава вже здійснила низку кроків у напрямі підвищення кіберстійкості – зокрема, впровадила резервне копіювання державних даних, залучила міжнародну експертизу та активізувала навчання службовців.

Водночас стратегічна безпека вимагає не лише реагування на атаки, а й формування сталої культури інформаційного захисту на всіх рівнях – від центральних органів до фронтових підрозділів. У цьому контексті особливої актуальності набуває оновлення підходів до класифікації інформації: коли обставини вимагають оперативної дії, а інфраструктура не забезпечує режим секретності, необхідним є впровадження автоматизованих систем шифрування та розширення дозволених технічних засобів для умов воєнного стану, за умови їх сертифікації Держспецзв'язку.

Як слушно зауважує Левченко О.В., «у гібридній війні проти України Росія здійснює надпотужний деструктивний інформаційний вплив на всі сфери функціонування нашої країни, створюючи реальні інформаційні загрози і завдаючи відчутних збитків державі і суспільству» [18, с. 2].

Кіберзагрози в умовах збройного конфлікту є багатовекторними: вони охоплюють як класичні спроби втручання в системи збереження даних, так і гібридні атаки, що поєднують кіберзлочинність із психологічним впливом. Україна відповідає на ці виклики системно, хоча й у складних обставинах. Необхідною умовою збереження державної таємниці є не лише технічна модернізація, а й формування цілісної доктрини реагування на надзвичайні кіберінциденти, адаптованої до умов реального бойового часу.

Ефективне забезпечення інформаційної безпеки у сфері охорони державної таємниці неможливе без налагодженої міжвідомчої взаємодії, яка в Україні реалізується через координацію діяльності Служби безпеки України, Національної поліції, Державної служби спеціального зв'язку та захисту інформації та Національного координаційного центру кібербезпеки при РНБО. Оскільки кожен із цих

органів виконує окрему функцію у сфері кібер-захисту, постає потреба в оперативному обміні інформацією, погодженні дій у разі інцидентів, а також у чіткому розподілі відповідальності за правоохоронні та контррозвідувальні заходи [16].

Ключову координаційну функцію виконує Національний координаційний центр кібербезпеки, створений у 2016 році, до складу якого входять представники СБУ, НПУ, Міноборони, Генштабу, Держспецзв'язку, Служби зовнішньої розвідки та інших суб'єктів сектору безпеки. Завдяки такій структурі забезпечується швидке прийняття рішень у кризових ситуаціях, запуск протоколів реагування та ефективний обмін технічною й аналітичною інформацією [9].

Станом на 2024 рік, модель співпраці між СБУ та кіберпідрозділами НПУ є комбінованою: Служба безпеки України здійснює контррозвідувальні функції, пов'язані із захистом державної таємниці, тоді як кіберполіція – первинне технічне забезпечення розслідувань, вилучення цифрових доказів, аналіз шкідливого програмного забезпечення, блокування доступу до ворожих серверів.

У разі виявлення фактів витоку інформації, що має ознаки державної таємниці, матеріали передаються за підслідністю до СБУ, однак фактичну оперативно-технічну частину часто реалізують підрозділи Нацполіції. Це приклад функціональної симетрії, за якої взаємодія без жорсткої централізації дозволяє досягати високих результатів. З огляду на це, особливої актуальності набуває потреба у чітко структурованому підході до управління ІТ-ризиками на об'єктах критичної інформаційної інфраструктури, що передбачає формування спільної робочої групи, ранжування загроз та впровадження оптимальних стратегій реагування, включно з прийняттям, передачею чи уникненням ризику.

Як наголошує С.Б. Гордієнко, «рішення щодо реагування на ризики потребують ретельного розгляду та врахування всіх без виключення та приниження значущості ризиків безпеки», а ефективне реагування потребує «співвіднесення вартості реалізації заходів з вигодами, що від них отримуються» [19].

Гнучка модель міжвідомчої взаємодії між СБУ та НПУ довела свою ефективність у ситуаціях оперативного реагування, проте на рівні нормативного врегулювання така співпраця залишається фрагментарною. Відсутність чітко закріплених механізмів інформаційної взаємодії, зокрема у сфері охорони державної таємниці, створює ризики дублювання функцій або, навпаки, утворення комунікаційних розривів під час кризових інцидентів.

Наразі затримання адміністраторів ворожих ресурсів або учасників кібершахрайських схем відбувається спільними силами, але юридичне підґрунтя для таких дій закріплене лише на рівні наказів або внутрішніх розпоряджень, що не гарантує стабільності координації. Ускладнення викликає також обмежена можливість оперативного обміну класифікованою інформацією між установами – чинні внутрішні режимні приписи часто не дозволяють передавати комп'ютерні докази чи технічні файли без багаторівневих погоджень, що значно знижує ефективність у так званому «вікні реакції». У цьому контексті доцільно ініціювати розробку єдиного стандарту міжвідомчого електронного документообігу для критично чутливої інформації.

У контексті триваючої збройної агресії та зростання кіберзагроз міжнародні стандарти реагування на інформаційні інциденти за моделлю "whole-of-government" заслуговують особливої уваги, оскільки забезпечують уніфікований підхід до координації дій усіх суб'єктів сектору безпеки. Як показує досвід країн НАТО – Литви, Естонії, Польщі – навіть незначні загрози в цифровому середовищі автоматично опиняються під контролем централізованих органів кіберзахисту.

Для України така модель є не лише стратегічно бажаною, але й функціонально необхідною. Проте її ефективна імплементація потребує перегляду правового статусу регіональних структур обробки інцидентів, унормування їх повноважень та впровадження єдиної інфраструктури міжвідомчого управління ризиками. Тільки за умови інституційної сумісності, технологічної інтегрованості та правової визначеності можлива стійка та результативна система охорони державної таємниці в умовах гібридної війни.

Висновки. Забезпечення інформаційної безпеки у сфері охорони державної таємниці

в Україні потребує комплексного, міжвідомчого підходу, що враховує як традиційні форми загроз, так і нові виклики кіберпростору. Аналіз чинного законодавства засвідчує, що нормативна база загалом охоплює ключові напрями захисту секретної інформації, однак її ефективність залежить від узгодженої взаємодії Служби безпеки України, кіберпідрозділів Національної поліції, Держспецзв'язку та Національного координаційного центру кібербезпеки.

В умовах воєнного стану роль кіберпідрозділів як оперативної ланки реагування на інциденти інформаційного витоку суттєво зростає. Разом з тим, відсутність формалізованих механізмів доступу до класифікованої інформації, а також недосконаліть нормативного забезпечення міжвідомчої координації ускладнюють ефективне реагування на загрози.

Подальше вдосконалення системи охорони державної таємниці має ґрунтуватися на стандартизації процедур управління ризиками, впровадженні електронного документообігу для критично чутливої інформації та розвитку професійної культури серед посадових осіб, що працюють з інформацією з обмеженим доступом. Необхідним також є посилення аналітичної спроможності СБУ, розширення інституційної взаємодії з НАТО/ЄС та адаптація міжнародних підходів у сфері кіберзахисту до українських реалій.

ЛІТЕРАТУРА:

1. Про державну таємницю : Закон України від 21 січня 1994 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855–12

2. Про Службу безпеки України : Закон України від 25 березня 1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229–12

3. Про Національну поліцію : Закон України від 2 липня 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580–19

4. Семенюк О. Г. Державна таємниця як предмет злочину. *Інформація і право*. 2016. № 4 (19). С. 85–94. URL: http://il.ippi.org.ua/article/view/272983

5. Про захист інформації в інформаційно–комунікаційних системах : Закон України від 5 липня 1994 р. № 80/94–ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94–вр

6. Гончаров М. В. Дослідження поняття «інформаційна безпека». *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Вип. 82, ч. 1. С. 34–37. URL: https://visnyk–juris–uzhnu.com/wp–content/uploads/2024/05/6.pdf

7. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657–XII. URL: https://zakon.rada.gov.ua/laws/show/2657–12

8. Про правовий режим воєнного стану : Закон України від 12 травня 2015 р. № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389–19

9. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19 (дата звернення: 18.05.2025).

10. Про Стратегію інформаційної безпеки : Указ Президента України від 28 грудня 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021 (дата звернення: 18.05.2025).

11. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469–19

12. Вдовін І. О. Організаційно–правові засади реалізації інформаційної безпеки України : дис. … канд. юрид. наук. URL: https://uacademic.info/ua/document/0424U000144

13. Служба безпеки України : Офіційний вебсайт. URL: https://ssu.gov.ua

14. Кримінальний кодекс України : Закон України від 5 квітня 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341–14 (дата звернення: 18.05.2025).

15. Кіберполіція України: Офіційний вебсайт. URL: https://cyberpolice.gov.ua (дата звернення: 18.05.2025).

16. Національний координаційний центр кібербезпеки. Офіційний сайт.URL: https://cip.gov.ua/ua

17. Про затвердження Плану заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки України: розпорядження Кабінету Міністрів України від 19 грудня 2023 р. № 1163–р. URL: https://www.kmu.gov.ua/npas/pro–zatverdzhennia–planu–zakhodiv–na–20232024–roky–z–realizatsii–stratehii–kiberbezpeky–ukrainy–i191223–1163 (дата звернення: 18.05.2025).

18. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія. Житомир : Видавець ПП «Євро-Волинь», 2021. 172 с. URL: https://sprotyvg7.com.ua/wp–content/uploads/2022/12/inform–bezpeka.pdf

19. Гордієнко С. Б. Актуальні питання управління IT–ризиками на об'єктах критичної інформаційної інфраструктури. *Телекомунікаційні та інформаційні технології*. 2022. № 1. С. 29–35. URL: https://tit.dut.edu.ua/index.php/telecommunication/article/view/2412