Information Technology and Cyber Defence as Important Elements of National Security

UDC: 32.01.04 DOI: https://doi.org/10.15421/172521

Kazmiruk Dmytro
Ph.D. Student, https://orcid.org/0009-0006-5763-1665, dmitrokazmiruk4@gmail.com
Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)

Abstract

Relevance. The relevance of the article is due to the growing threats to national security in the context of globalisation and digitalisation. Modern challenges, including hybrid warfare and cyber threats, require effective strategies and measures to protect information resources.

The purpose: to identify the key modern challenges to information security in the context of digitalisation and globalisation, as well as to develop recommendations for improving the effectiveness of cyber defence to ensure national security.

Results. Ensuring information security is becoming a priority for public policy due to the growing importance of information and the development of new technologies that pose challenges to national security, in particular in the context of hybrid warfare. It is determined that an effective national security strategy must take into account geopolitical, technological and social factors, as well as the development of cybersecurity through digital transformation and modernisation of information infrastructure. Important areas include improving the regulatory framework, raising the level of information literacy and active cooperation with international partners to establish cyber defence.

Conclusions. In today's globalised and digitalised world, information security is gaining strategic importance for national security. Challenges posed by hybrid threats and cyber conflicts require a comprehensive approach to information security at all levels. The development of a stable information policy that takes into account political, economic and geopolitical factors is key to preserving national interests. The balance between openness of information and its security is important, especially in democratic countries. The integration of digital technologies provides new opportunities for strengthening cybersecurity, but faces challenges from institutional changes, financial constraints and foreign policy threats.

Keywords: information security, cybersecurity, hybrid warfare, digital transformation, national security, information technology, digitalisation

Інформаційні технології та кібернетичний захист як важливі елементи національної безпеки

Казмірук Дмитро
Київський національний університет імені Тараса Шевченка (Київ, Україна)

Анотація

Актуальність. Актуальність статті обумовлена зростаючими загрозами для національної безпеки в умовах глобалізації та цифровізації. Сучасні виклики, зокрема гібридні війни та кіберзагрози, вимагають ефективних стратегій і заходів для захисту інформаційних ресурсів.

Мета дослідження: виявити ключові сучасні виклики інформаційної безпеки в умовах цифровізації та глобалізації, а також розробити рекомендації щодо підвищення ефективності кіберзахисту для забезпечення національної безпеки.

Результати. Забезпечення інформаційної безпеки стає пріоритетом для державної політики через зростання важливості інформації та розвитку нових технологій, що створюють виклики для національної безпеки, зокрема в умовах гібридної війни. Визначено, що для ефективної стратегії національної безпеки необхідно враховувати геополітичні, технологічні та соціальні фактори, а також розвиток кібербезпеки через цифрову трансформацію та модернізацію інформаційної інфраструктури. Важливими напрямками є удосконалення нормативно-правової бази, підвищення рівня інформаційної грамотності та активна співпраця з міжнародними партнерами для налагодження кіберзахисту.

Висновки. У сучасних умовах глобалізації та цифровізації інформаційна безпека набуває стратегічного значення для національної безпеки. Виклики, пов'язані з гібридними загрозами та кіберконфліктами, вимагають комплексного підходу до забезпечення захисту інформації на всіх рівнях. Розробка стабільної інформаційної політики, що враховує політичні, економічні та геополітичні фактори, є ключовою для збереження національних інтересів. Важливим є баланс між відкритістю інформації та її безпекою, особливо в демократичних країнах. Інтеграція цифрових технологій надає нові можливості для зміцнення кібербезпеки, але стикається з викликами інституційних змін, фінансових обмежень і зовнішньополітичних загроз.

Ключові слова: інформаційна безпека, кібербезпека, гібридна війна, цифрова трансформація, національна безпека, інформаційні технології, діджиталізація

Стаття надійшла / Article arrived: 11.01.2025 Схвалено до друку / Accepted: 25.02.2025

Вступ.

Актуальність статті зумовлена швидким розвитком технологій та інформаційних процесів, які створюють нові виклики для національної безпеки. У сучасному світі інформаційна безпека є не лише технологічною, але й стратегічною складовою, що вимагає оперативного реагування на постійно змінювані умови глобальних і внутрішніх загроз. Гібридні війни, кібератаки та маніпуляції інформацією стають все більш поширеними методами тиску на держави, що вимагає від них розробки ефективних стратегій і заходів для захисту від таких загроз. Крім того, інтеграція цифрових технологій у державне управління та суспільне життя підвищує важливість кібербезпеки, що ставить перед країнами завдання забезпечення належного рівня захисту інформаційних ресурсів. Враховуючи зазначене, розгляд питань забезпечення інформаційної безпеки в умовах глобалізації та цифрової трансформації є надзвичайно актуальним і важливим для сучасного етапу розвитку національних і міжнародних безпекових систем.

Мета дослідження: виявити ключові сучасні виклики інформаційної безпеки в умовах цифровізації та глобалізації, а також розробити рекомендації щодо підвищення ефективності кіберзахисту для забезпечення національної безпеки.

Аналіз попередніх публікацій. Наукові дослідження теми інформаційних технологій та кібернетичного захисту як важливих елементів національної безпеки показують, що ці технології стають ключовими у протидії сучасним загрозам. Миколюк (2022) акцентує на важливості стратегічного підходу до кіберзахисту в умовах гібридної війни, підкреслюючи роль інформаційних технологій у державному управлінні. Житко (2017) розглядає розвиток кібербезпеки в Україні в умовах війни, відзначаючи необхідність вдосконалення нормативно-правової бази та співпраці між державними органами, приватним сектором і науковими установами.

Грищук і Даник (2016) досліджують термінологічні аспекти кібербезпеки, вказуючи на потребу у створенні єдиного термінологічного апарату для ефективної боротьби з кіберзагрозами. Мазур (2024) зауважує необхідність покращення правового регулювання кібербезпеки в Україні. Савченко (2023) наголошує на ключовому значенні кібербезпеки у забезпеченні ініормаційної безпеки держави. Куйбіда, Карпенко та Наместнік (2018) акцентують на важливості цифрової трансформації для забезпечення кібербезпеки, зазначаючи, що вона повинна охоплювати всі рівні державного управління. Свердлик (2022) наголошує на ключовому значенні кіберзахисту інформації та кібергігієни при користуванні мережею інтернет, в тому числі для працівників державних органів.

Нікітін і Кульчицький (2019) підкреслюють важливість партнерства між державними органами та приватним сектором для розробки ефективних методів захисту в умовах цифрової трансформації. Денісенко (2023) звертає увагу на роль інформаційно-комунікаційних технологій у публічному управлінні та їх значення для безпеки. Вовк (2024) зауважує, що до публічного управління забезпеченням кібербезпеки має бути обов'язково включено ефективні методи серед яких: розвідка загроз, машинне навчання, поведінкова аналітика, архітектура нульової довіри, управління ризиками. Ці дослідження підкреслюють важливість комплексного підходу до інтеграції ІТ у національну безпеку через розвиток цифрової трансформації, вдосконалення нормативно-правової бази та ефективну співпрацю між різними секторами.

Результати дослідження.

Проблематика інформаційної безпеки набуває особливої актуальності в умовах значного зростання обсягів і значення інформації, яке відбувається в останні роки. Це зростання супроводжується суттєвим збільшенням числа суб'єктів інформаційних відносин і споживачів інформації. Враховуючи ці фактори, забезпечення інформаційної безпеки стає одним із пріоритетних напрямків державної політики. Підвищення ролі інформації в глобалізованому світі, разом із розвитком сучасних технологій, створює нові виклики для національної безпеки. Зокрема, це стосується і загострення гібридної інформаційної війни, яку протягом багатьох років ведуть проти нашої держави. У такому контексті забезпечення інформаційної безпеки набуває не лише технологічного, а й стратегічного значення, вимагаючи комплексного підходу до вирішення проблем, що виникають у цій сфері. Тому важливо здійснювати активні та системні заходи для мінімізації загроз інформаційної безпеки на всіх рівнях.

Інформаційна безпека є однією з пріоритетних сфер відповідальності сучасної держави, що визначає її здатність до захисту власних національних інтересів та ефективної протидії різноманітним загрозам, як внутрішнім, так і зовнішнім. У цьому контексті розробка та впровадження стабільної та сучасної інформаційної політики є основою для забезпечення національної безпеки. Для її ефективної реалізації необхідно враховувати цілу низку об'єктивних чинників, серед яких важливими є політико-економічна та геополітична ситуація на міжнародній арені, загальна тенденція до діджиталізації ключових сфер життєдіяльності, розвиток інформаційних технологій, а також необхідність захисту національних інтересів в умовах активного ведення інформаційної війни з країною-агресором (Миколюк, 2022).

Рівень розвитку та безпеки інформаційного простору країни є важливими системоутворюючими факторами, що прямо впливають на стан національної безпеки, включаючи політичну, економічну, соціальну, воєнну та інформаційну складові. Урахування цих факторів є необхідним для формування стратегії

національної безпеки, яка має на меті забезпечення стабільності та стійкості держави в умовах глобальних та локальних загроз.

Особливу увагу варто приділити тенденціям, що спостерігаються на міжнародній арені, де відкритість даних і доступ до інформації стають важливими аспектами державної політики. Проте, у різних країнах підхід до цього питання може значно варіюватися. У авторитарних режимах інформаційна політика характеризується суворою централізацією та контролем, що визначає чіткі та обмежені сфери доступу до інформації. Натомість у демократичних державах цей процес супроводжується значною участю різних суб'єктів, що створює ситуацію напруженості та дискусійності. Важливим є досягнення балансу між відкритістю інформації та її безпекою, що є складним завданням для урядів. Окремі дослідники зазначають, що в умовах серйозної загрози національній безпеці демократичні держави можуть втратити заявлені цінності прозорості та відкритості, оскільки забезпечення безпеки в таких випадках може вимагати значних обмежень у доступі до інформації.

Потреба в ефективному захисті інформаційних ресурсів сприяє зближенню демократичних та авторитарних підходів до регулювання цієї сфери, що зумовлює зміну акцентів у бік централізації та керованості інформацією (Anderson, 2011; Rosenzweig, 2013). Така трансформація веде до виникнення внутрішнього конфлікту, що поступово загострюється на тлі розвитку глобальної мережі Інтернет. З одного боку, повна прозорість, властива демократичним нормам, виступає як протилежність державній таємниці та секретності, які є необхідними для певних сфер, таких як національна безпека чи оборона, і в яких інтереси виконавчої влади можуть вимагати особливого контролю. Однак, враховуючи поточну геополітичну ситуацію та зростання рівня конфліктів і загроз на глобальному рівні, можна стверджувати, що більшість урядів нині віддають пріоритет забезпеченню безпеки критично важливої інформації перед її широким розповсюдженням (McChesney, 1996). Так, наприклад, переглядається доцільність публікації в відкритому доступі інформації щодо переміщення озброєнь, яка раніше була доступна у формі електронної звітності.

Сучасні реалії, зокрема загострення гібридної війни в інформаційному просторі, значно підвищили актуальність питань удосконалення кібербезпеки в Україні. Хоча вже вжито низку важливих заходів, таких як затвердження "Стратегії кібербезпеки України", прийняття Закону "Про основні засади забезпечення кібербезпеки України" та ратифікація "Конвенції про кіберзлочинність" (Житко, 2017), залишається необхідність подальшого розвитку в цьому напрямку. Особливо це стосується чіткого визначення меж застосування кіберпростору в умовах військових конфліктів. Незважаючи на значний прогрес у розробці методології кібербезпеки, який доводить, що елементами кіберборотьби є кіберзахист, кіберрозвідка та кібервплив, термінологічний апарат, сформований на основі нормативно-правових актів і керівних документів, ще не дозволяє офіційно визнавати це у відповідних документах (Грищук, & Даник, 2016).

Крім того, важливим напрямком є розвиток інформаційного суспільства в Україні, оскільки воно є основою для ефективної реалізації державної інформаційної політики. Для цього необхідно оновити застарілу нормативно-правову базу в інформаційній сфері, підвищувати рівень комп'ютерної та інформаційної грамотності серед населення, активно впроваджувати новітні методи навчання, а також забезпечувати загальний доступ до Інтернету. Хоча робота в цих напрямках вже ведеться, темпи її реалізації все ще не відповідають вимогам часу, що ставить під загрозу конкурентоспроможність країни в інформаційній сфері на міжнародному рівні.

Ефективна кібербезпека не може бути досягнута без належної цифрової трансформації державних інститутів та адаптації провідних інформаційних і цифрових технологій для використання в сфері національної безпеки. Сучасний етап розвитку цифрових технологій супроводжується появою численних визначень цифрової трансформації, кожне з яких акцентує увагу на різних аспектах цього процесу, проте мало хто з них враховує комплексний підхід, який передбачає інтеграцію стратегічного партнерства між усіма зацікавленими сторонами, одночасну розробку цифрових послуг, програмного забезпечення, а також оцінку рівня цієї трансформації. Так, В. С. Куйбіда, О. В. Карпенко та В. В. Наместнік визначають цифрову трансформацію як процес змін у природі людини, її мисленні, життєдіяльності та управлінні, спричинений використанням цифрових технологій (Куйбіда, Карпенко, & Наместнік, 2018). Ю. О. Нікітін та О. І. Кульчицький уточнюють, що цифрова трансформація є процесом переходу до нових способів діяльності, який здійснюється через впровадження цифрових технологій та сервісів, що ґрунтується на стратегічному партнерстві усіх учасників і передбачає одночасну розробку програмного забезпечення, оцінку рівня цифрової трансформації та її інтеграцію у національні стратегії (Нікітін, & Кульчицький, 2019).

Процес цифрової трансформації активно підтримується в Україні загальною тенденцією до діджиталізації більшості сфер життєдіяльності громадян. Діджиталізація, як комплекс сучасних інструментів і процесів, є якісно новим етапом у розвитку інформаційно-комунікаційних технологій, які трансформують усі сфери суспільного життя. Термін «діджиталізація» в перекладі з англійської означає «оцифрування», «цифровізація» або

«перетворення в цифрову форму» (Струтинська, 2019). У цьому контексті діджиталізація виступає не лише як технологічний процес, а й як важливий фактор, що забезпечує інтеграцію інформаційних технологій у різні аспекти функціонування державних інституцій, зокрема в сфері безпеки, що є ключовим для розвитку кіберзахисту та забезпечення національної безпеки.

У сучасних трансформаційних умовах значно посилюється інтеграція технологічних, економічних та соціальних функцій держави, що обумовлює появу нових підходів до управління і взаємодії між державою та громадянами. Новітня цифрова трансформація спричиняє виникнення якісно нової форми інституційної взаємодії, в межах якої відбувається активне впровадження інформаційно-комунікаційних технологій. Взаємозв'язок та взаємодія суб'єктів публічного управління, які опосередковуються цифровізацією, викликають нові інституційні вимоги, зокрема до здобуття сучасних інформаційних технологій учасниками управлінського процесу та їх адаптації до нових форм комунікації (Денісенко, 2023). Це дозволяє говорити про якісну трансформацію функцій держави, яка вже включає в себе інноваційні підходи до управління в умовах цифровізації.

Проте, поряд із позитивними змінами, що супроводжують цифрову трансформацію, існують суттєві виклики та протидіючі фактори. Серед них виділяються проблеми інституційного середовища, фінансові обмеження та зовнішньополітичні загрози, які ставлять під сумнів стабільність і існування української державності в умовах постійного зовнішнього тиску. У цьому контексті важливо зазначити, що, попри значні досягнення у сфері цифровізації, на шляху до повної інтеграції інформаційних технологій у державне управління ще залишаються певні проблеми, які потребують системного вирішення.

Щодо кібербезпеки, то сутність кіберборотьби включає кілька основних аспектів. По-перше, це постійний захист власної кіберінфраструктури, який здійснюється на регулярній основі, а також активний захист у разі кібернападів з боку противника. До того ж, важливими складовими є розвідка кіберінфраструктури супротивника для виявлення вразливих точок та здійснення впливу на його інфраструктуру з метою нейтралізації загроз. Проте, існуючі дефініції понять «кіберзахист», «кіберрозвідка» та «кібервплив» не повною мірою визначають їхнє відношення до кіберборотьби, що ускладнює чітке розуміння цього процесу в контексті офіційної стратегії. Наприклад, визначення кіберрозвідки на даний момент обмежується лише розвідувальними органами України, що не відповідає сучасним викликам, які потребують більш широкого підходу до кібербезпеки (Горгуленко, 2024).

Загалом, сучасні військові конфлікти, зокрема російсько-українська війна, показали, що кіберборотьба є постійним елементом міжнародних відносин як у мирний час, так і під час збройних конфліктів. Кіберборотьба переростає у кіберпротиборство, що характеризується двостороннім впливом, послідовністю та тісним зв'язком з військовими операціями в інших доменах (сухопутний, повітряний, морський), що робить кібероперації важливою складовою частиною сучасної війни. Це підкреслює необхідність не лише вдосконалення національної кібербезпеки, але й розробки міжнародних стандартів кібербезпеки для забезпечення ефективного реагування на кіберзагрози в умовах збройних конфліктів.

Для подальшого посилення кібернетичного захисту і, як наслідок, національної безпеки країни, необхідно врахувати ряд рекомендацій. По-перше, необхідно інтегрувати цифрові технології в усі сфери національної безпеки, що включає впровадження інноваційних інформаційно-комунікаційних технологій в управлінські процеси. Це дозволить створити ефективну систему реагування на кіберзагрози та забезпечить своєчасну і адекватну відповідь на виклики в кіберпросторі.

По-друге, важливо сформувати стратегічне партнерство між державними органами, приватним сектором та науковими установами, яке сприятиме розробці нових цифрових послуг та оцінці рівня цифрової готовності країни до кіберзагроз. Це дасть змогу досягти комплексного підходу у цифровій трансформації та зміцнити кібербезпеку.

По-третє, потрібно постійно вдосконалювати нормативно-правову базу в сфері кібербезпеки, розробляючи чіткі стандарти для кіберзахисту, кіберрозвідки та кібервпливу. Це дозволить створити єдині правила гри для всіх учасників процесу кібербезпеки та забезпечить правову основу для боротьби з кіберзагрозами.

По-четверте, важливим є підвищення рівня комп'ютерної та інформаційної грамотності серед населення та органів влади, що допоможе зменшити кількість людських помилок та уразливостей. Це забезпечить більш ефективне реагування на кіберзагрози та збільшить загальну кіберстійкість країни.

По-п'яте, потрібно впроваджувати інноваційні методи кіберзахисту, зокрема використовуючи штучний інтелект і машинне навчання для моніторингу та захисту кіберпростору країни. Це дозволить швидко виявляти кіберзагрози та нейтралізувати їх на ранніх етапах.

По-шосте, необхідно посилювати співпрацю з міжнародними партнерами, обмінюючись інформацією та координуючи дії для ефективного реагування на глобальні кіберзагрози. Це сприятиме створенню єдиного міжнародного

фронту протидії кіберзлочинності та кібертероризму.

По-сьоме, потрібно постійно модернізувати національну кіберінфраструктуру, адаптуючи її до нових технологічних викликів і забезпечуючи надійний захист критичної інфраструктури. Це дозволить країні підтримувати високий рівень кібербезпеки та забезпечувати стабільність у цифровому середовищі.

Висновки.

У сучасних умовах глобалізації та інформаційної революції питання інформаційної безпеки набувають особливої ваги, оскільки зростання обсягів інформації та розвиток технологій створюють нові виклики для національної безпеки, зокрема в контексті гібридних загроз і кіберконфліктів. Інформаційні війни, дезінформація, маніпуляції громадською думкою через соціальні мережі та кібератаки на критичну інфраструктуру стають інструментами сучасних конфліктів, що посилює потребу в ефективних механізмах захисту.

У цих умовах інформаційна безпека стає не лише технологічною, але й стратегічною складовою національної безпеки, що вимагає комплексного підходу до її забезпечення на всіх рівнях. Розробка стабільної інформаційної політики, яка враховує політичні, економічні та геополітичні фактори, є необхідною для захисту національних інтересів у ситуаціях глобальних загроз. Особливо важливим є досягнення балансу між відкритістю інформації та її безпекою, що стає особливо актуальним у демократичних країнах у контексті загострення загроз для національної безпеки. Захист свободи слова та водночас протидія інформаційним атакам є критично важливими для збереження демократичних інститутів та суспільної стабільності. Паралельно з цим, інтенсивний розвиток цифрових технологій та їх впровадження в усі сфери управління надають нові можливості для зміцнення кібербезпеки та національної безпеки в цілому. Використання штучного інтелекту, технологій блокчейну, біометричних систем і хмарних рішень може значно підвищити рівень безпеки даних та державних інформаційних систем.

Проте необхідно зазначити, що повна інтеграція цифрових технологій в державні структури стикається з низкою викликів, зокрема у сфері інституційних змін, фінансових обмежень і зовнішньополітичних загроз. Успішна цифровізація державного управління потребує системного підходу, включаючи оновлення законодавчої бази, вдосконалення механізмів захисту персональних даних та посилення кіберграмотності серед державних службовців. Враховуючи всі ці фактори, надзвичайно важливо продовжувати розвивати стратегії кібербезпеки, удосконалювати нормативно-правову базу та посилювати міжнародну співпрацю для ефективного протистояння новітнім кіберзагрозам. Україна активно інтегрується в європейські та світові ініціативи у сфері кібербезпеки, що сприяє зміцненню її позицій у боротьбі з кіберагресією. Розвиток інформаційного суспільства та цифрова трансформація повинні стати основою для підвищення рівня безпеки, підвищуючи інформаційну та комп'ютерну грамотність серед населення та органів влади, що дозволить країні зберегти стабільність і конкурентоспроможність в умовах сучасних загроз. Створення національних програм із кібербезпеки, підтримка стартапів у сфері технологічного захисту та розширення міжнародного співробітництва можуть стати ключовими інструментами у формуванні ефективної системи інформаційної безпеки в умовах цифрової епохи.

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

Вовк, А. (2024). Сучасні проблеми публічного управління забезпеченням кібербезпеки в Україні. *Публічне управління: концепції, парадигма, розвиток, удосконалення*, 8, 28-35.

Горгуленко, В. (2024). Військово-теоретичне обґрунтування рекомендацій стосовно розвитку термінологічного апарату в сфері кіберборотьби. *Сучасні інформаційні технології у сфері безпеки та оборони*, 3(51), 11-28.

Грищук, Р. В., & Даник, Ю. Г. (2016). *Основи кібернетичної безпеки*. (Монографія). Житомир: ЖНАЕУ.

Денісенко, В. А. (2023). Концептуальні аспекти цифрової трансформації як визначального фактора підвищення ефективності забезпечення національної безпеки в Україні. Правові новели. *Науковий юридичний журнал*, 21(2), 184-189.

Житко, А. О. (2017). Кібервійна як складова гібридної війни. Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення. *Всеукраїнська науково-практична конференція*. Маріуполь: ДонДУУ. (с. 263-266).

Куйбіда, В. С., Карпенко, О. В., & Наместнік, В. В. (2018). Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. *Інформаційні технології*, 1, 5-10.

Мазур, Я. П. (2024). Правові основи регламентації кібербезпеки. *Науковий вісник Ужгородського національного університету. Серія: Право*, 3(85), 11-15.

Миколюк, А. (2022). Публічне управління інформаційною безпекою: діджиталізація та інформаційна війна. *Право та державне управління*, 1, 156-161.

Нікітін, Ю. О., & Кульчицький, О. І. (2019). Цифрова парадигма як основа визначень: цифровий бізнес, цифрове підприємство, цифрова трансформація. *Маркетинг і цифрові технології*, 3(4), 77-87.

Савченко, В. А. (2023). Забезпечення стійкості кібероборони держави в умовах збройного конфлікту. *Сучасний захист інформації*, 3, 6-11.
Свердлик, З. (2022). Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві. *Український журнал з бібліотекознавства та інформаційних наук*, 10, 175-188.
Струтинська, І. В. (2019). Дефініції поняття «цифрова трансформація». *Економіка та управління підприємствами*, 48-2, 91-96.
Anderson, J. (2011). *Public policymaking*. Wadsworth Publishing.
McChesney, R. W. (1996). The Internet and U. S. communication policy-making in historical and critical perspective. *Journal of Communication*, 46, 98-124.
Rosenzweig, P. (2013). *Cyber warfare: How conflicts in cyberspace are challenging America and changing the world*. Praeger Publishers.

REFERENCES

Anderson, J. (2011). *Public policymaking*. Wadsworth Publishing.
Denisenko, V. A. (2023). Conceptual aspects of digital transformation as a determining factor in improving the effectiveness of national security in Ukraine. *Legal novels. Scientific legal journal*, 21(2), 184-189.
Gorgulenko, V. (2024). Military-theoretical substantiation of recommendations for the development of terminology in the field of cyber warfare. *Modern Information Technologies in the Field of Security and Defence*, 3(51), 11-28.
Grishchuk, R. V., & Danik, Y. G. (2016). Fundamentals of cyber security. (Monograph). Zhytomyr: ZhNAEU.
Kuibida, V. S., Karpenko, O. V., & Namestnik, V. V. (2018). Digital governance in Ukraine: basic definitions of the conceptual and categorical apparatus. *Information Technologies*, 1, 5-10.
Mazur, Y. P. (2024). Legal foundations of cybersecurity regulation. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 3(85), 11-15.
McChesney, R. W. (1996). The Internet and U. S. communication policy-making in historical and critical perspective. *Journal of Communication*, 46, 98-124.
Mykoliuk, A. (2022). Public management of information security: digitalisation and information warfare. *Law and Public Administration*, 1, 156-161.
Nikitin, Y. O., & Kulchytskyi, O. I. (2019). Digital paradigm as a basis for definitions: digital business, digital enterprise, digital transformation. *Marketing and digital technologies*, 3(4), 77-87.
Rosenzweig, P. (2013). *Cyber warfare: How conflicts in cyberspace are challenging America and changing the world*. Praeger Publishers.
Savchenko, V. A. (2023). Ensuring the stability of the state's cyber defense in conditions of armed conflict. *Modern Information Protection*, 3, 6-11.
Strutynska, I. V. (2019). Definitions of the concept of ‘digital transformation’. *Economics and management of enterprises*, 48-2, 91-96.
Sverdlyk, Z. (2022). Cybersecurity and cyberdefense: issues on the agenda in Ukrainian society. *Ukrainian Journal of Library and Information Sciences*, 10, 175-188.
Vovk, A. (2024). Modern problems of public management of cybersecurity in Ukraine. *Public administration: concepts, paradigm, development, improvement*, 8, 28-35.
Zhytko, A. O. (2017). Cyberwar as a component of hybrid warfare. Ukrainian society in the conditions of war: current challenges and prospects for peacebuilding. *All-Ukrainian scientific and practical conference*, (pp. 263-266). Mariupol: DonDUU.