Вісник Національного університету “Львівська політехніка”. Серія: “Юридичні науки”
№ 2 (42), 2024

УДК 34:001.102-049.5

Ольга СКОЧИЛЯС-ПАВЛІВ
Національний університет “Львівська політехніка”,
Навчально-науковий інститут права,
психології та інноваційної освіти,
професор кафедри адміністративного
та інформаційного права,
доктор юридичних наук, професор
olha.v.skochylyas-pavliv@lpnu.ua
ORCID iD: https://orcid.org/0000-0001-6737-7628

ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

http://doi.org/10.23939/law2024.42.151

У статті розглядаються правові механізми забезпечення інформаційної безпеки. Доведено, що сьогодні як ніколи, коли в Україні йде війна, питання забезпечення інформаційної безпеки набуває особливої актуальності та значущості, оскільки інформаційний простір стає “полем бою” нарівні з воєнним фронтом. Ворожі сили активно використовують інформаційні та психологічні операції для дестабілізації ситуації всередині нашої країни, створення паніки, поширення фейків та підриву довіри до державних інституцій. У цих умовах важливою стає політика держави, яка має бути цілісною та ефективною для протидії цим загрозам. Ефективна політика держави у сфері інформаційної безпеки допоможе забезпечити стійкість суспільства до інформаційних загроз, зміцнити довіру до державних інституцій та зберегти стабільність у кризових умовах. Пропонується авторське розуміння інформаційної безпеки як стану захищеності інформаційних ресурсів та інформаційних систем, який забезпечує їхню конфіденційність, цілісність, доступність і надійність, а також захищеність від несанкціонованого доступу, розголошення, модифікації, знищення та інших форм зловживань, що можуть призвести до порушення національної безпеки, економічної стабільності та суспільного порядку. Головними складниками інформаційної безпеки, які є основою для інформаційної безпеки для держави загалом, окремих органів чи приватних підприємств, названо конфіденційність, цілісність та доступність. Основними компонентами механізму забезпечення інформаційної безпеки, на думку автора, мають бути: технічний (створення відповідної технічної інфраструктури для забезпечення функціонування інформаційної безпеки), політичний (розробка державної політики, спрямованої на забезпечення інформаційної безпеки) та правовий (прийняття якісних нормативно-правових актів, які визначатимуть всі заходи інформаційної безпеки). Ці три складники взаємодоповнюють один одного і є основними для створення ефективної системи захисту від інформаційних загроз.

Ключові слова: національна безпека; інформаційний простір; інформаційні технології; інформаційна безпека; кібербезпека; загрози інформаційній безпеці.

Постановка проблеми. Однією із найважливіших функцій держави, відповідно до Стратегії інформаційної безпеки від 28.12.2021 року, є забезпечення інформаційної безпеки [1]. Сьогодні як

ніколи, коли в Україні йде війна, питання забезпечення інформаційної безпеки набуває особливої актуальності та значущості, оскільки інформаційний простір стає "полем бою" нарівні з воєнним фронтом. Ворожі сили активно використовують інформаційні та психологічні операції для дестабілізації ситуації всередині нашої країни, створення паніки, поширення фейків та підриву довіри до державних інституцій. В цих умовах важливою стає політика держави, яка має бути цілісною та ефективною для протидії цим загрозам. Ефективна політика держави у сфері інформаційної безпеки допоможе забезпечити стійкість суспільства до інформаційних загроз, зміцнити довіру до державних інституцій та зберегти стабільність у кризових умовах.

Аналіз дослідження проблеми. Оскільки питання інформаційної безпеки, яка є частиною національної безпеки, сьогодні є одним з найважливіших у державі, то йому надається значна увага вчених та практиків. У дослідженнях І. В. Арістової, І. Р. Боднара, Б. А. Кормича, В. А. Ліпкана, Ю. Є. Максименка, В. Я. Рубана та інших проблеми інформаційної безпеки постійно перебувають у центрі уваги. Сучасні розвідки таких науковців, як В. С. Виздрик, М. Т. Гаврильців, К. І. Долженко, Л. І. Мазуренко, Т. С. Перун, О. М. Мельник, І. М. Шопіна, Є. О. Соломін та багатьох інших також присвячені різним аспектам інформаційної безпеки, її ролі та значенню в політиці держави.

Метою статті є комплексне дослідження правових механізмів забезпечення інформаційної безпеки.

Виклад основного матеріалу. У сучасному цифровому світі інформація відіграє основну роль у всіх сферах суспільства, зокрема у політиці, економіці, військовій справі та соціальних відносинах. Однак разом із зростанням залежності від інформаційних технологій зростає й загроза їх порушення та зловживання. У зв'язку з цим питання забезпечення інформаційної безпеки для держави стає надзвичайно актуальним і важливим. Держави стикаються зі складнощами у забезпеченні безпеки своїх інформаційних ресурсів через різноманітні загрози, зокрема кібератаки, кібершпигунство, внутрішнє шпигунство та інші форми кіберзлочинності. Ці загрози можуть мати вкрай негативний вплив на державу, порушуючи національну безпеку, економічну стабільність та суспільний порядок. Вони лише посилюються в умовах воєнного стану, який запроваджений в Україні і потребують більш радикальних й ефективних заходів для протидії та належних правових механізмів її забезпечення.

Інформаційна безпека є певним елементом, складником системи національної безпеки. Підтвердженням цього є частина 1 статті 17 Конституції України, де сказано, що "захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу" [2].

Під час обговорення поняття інформаційної безпеки деякі дослідники розуміють його в досить обмеженому контексті, як сукупність апаратних і програмних засобів для забезпечення конфіденційності даних у комп'ютерних мережах. Наприклад, І. М. Сопілко вважає, що інформаційна безпека – це набір інструментів і методик, розроблених і використовуваних для захисту конфіденційної інформації від зміни, порушення, знищення і перевірки [3, с. 111].

Згідно з іншими позиціями, інформаційна безпека – це стан захищеності інформації. Так, О. М. Степко розглядає інформаційну безпеку з двох аспектів: по-перше, як захищеність внутрішньої інформації, тобто якість та надійність інформації, а також захист різних галузей інформації від розголошення і захист інформаційних ресурсів; по-друге, інформаційна безпека містить контроль над інформаційними потоками, обмеження використання провокаційної та ворожої суспільної інформації, включаючи контроль над рекламою, і захист національного інформаційного простору від зовнішньої інформаційної експансії [4, с. 91].

На думку Б. Кормича, інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави [5, с. 142].

Треба зазначити, що відповідно до Стратегії інформаційної безпеки, інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належно забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії завданню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване поширення, використання й порушення цілісності інформації з обмеженим доступом [1].

З урахуванням вищенаведених позицій вчених та законодавства можна сформулювати визначення інформаційної безпеки як стану захищеності інформаційних ресурсів та інформаційних систем, який забезпечує їхню конфіденційність, цілісність, доступність і надійність, а також захищеність від несанкціонованого доступу, розголошення, модифікації, знищення та інших форм зловживань, що можуть призвести до порушення національної безпеки, економічної стабільності та суспільного порядку.

Головними складовими частинами інформаційної безпеки, які є основою для інформаційної безпеки для держави загалом, окремих органів чи приватних підприємств, є:

– конфіденційність;

– цілісність;

– доступність [7].

Розглянемо кожну складову частину. Конфіденційність даних означає, що дані мають бути доступні лише тим, хто має авторизований доступ. Наприклад, візьмемо будь-який орган державної влади. Є інформація, яка може належати лише певним працівникам і потрібна лише для роботи. Обмеження кількості людей, які мають доступ до різних наборів даних, покращує здатність органу влади зберігати конфіденційність інформації.

Цілісність даних означає, що інформація має бути недоторканою, повною та точною. Щоб забезпечити цілісність даних, держави можуть підтримувати й оптимізувати свою IT-інфраструктуру, створювати резервні копії своїх даних і створювати план запобігання втраті даних, який захистить їх у разі серйозного порушення даних.

Доступність даних означає, що мережа, система та необхідні пристрої готові до використання за призначенням уповноваженим персоналом. Властиво, доступність даних означає здатність працівників отримати доступ до необхідних даних у будь-який момент без затримки. Є кілька факторів, які можуть перешкоджати доступу до даних навіть для авторизованих користувачів, особливо в епоху хмарних технологій, коли так багато даних розміщується за межами сайту.

Цифрова епоха стала свідком безпрецедентного зростання інформаційних загроз – від звичайної крадіжки даних або підслуховування до витонченого кібершпигунства, що фінансується національними державами. З розвитком технологій змінюється і тактика, яку застосовують кіберзлочинці. Складність інформаційної безпеки залежить від різних факторів, зокрема потенційних загроз, цінності, яку вона має, рівня чутливості інформації, перевірки та достовірності. Ось деякі з основних тенденцій в еволюції інформаційних загроз кібербезпеки, яка є частиною інформаційної безпеки і пов'язана з захистом комп'ютерних систем та мереж від витоку даних, пошкодження та крадіжки обладнання та програмного забезпечення:

Програми-вимагачі: атаки з використанням програм-вимагачів стають все більш поширеними, коли кіберзлочинці блокують системи і вимагають великі викупи або вимагають інформацію чи доступ до неї.

Вразливі пристрої: ненадійний пароль до робочих пристроїв, банальне викрадання ноутбуків чи носіїв інформації. Щоб уникнути цього, варто проводити лекції з кібергігієни в державних установах, компаніях та просто бути обізнаним кожній фізичній особі.

Атаки за допомогою штучного інтелекту (ШІ): кіберзлочинці використовують штучний інтелект і машинне навчання для створення ефективніших атак, що робить вкрай важливим для захисників впровадження штучного інтелекту для виявлення загроз. Важливо, що звичайний chat GPT чи avodocs, яким так люблять користуватися IT-юристи для використання шаблонних договорів, є open source. Тобто якщо юрист створює договір і заповнює дані в avodocs, то цей заповнений договір може бути легко викрадено, що несе загрозу клієнтам, юристу, компанії.

Положення про конфіденційність даних: нові правила конфіденційності даних, такі як GDPR і CCPA, встановлюють суворі вимоги для організацій. Їх недотримання призводить не лише до штрафних санкцій, але й створює репутаційні ризики.

Конфіденційність і захист даних: через зростаючу стурбованість щодо захисту даних окремі особи та організації стикаються з постійними проблемами щодо захисту особистої інформації, дотримання правил конфіденційності та захисту даних користувачів від несанкціонованого доступу [7].

Наведемо приклад однієї з найбільших хакерських атак, що загрожувала уряду США: Хакерська атака на SolarWinds у 2020 році.

SolarWinds – велика компанія-розробник програмного забезпечення, розташована в Талсі, штат Оклахома, яка надає інструменти керування системою для моніторингу мережі та інфраструктури, а також інші технічні послуги для сотень тисяч організацій по всьому світу. Серед продуктів компанії – система моніторингу продуктивності IT Orion. Хакери націлилися на SolarWinds, розгорнувши шкідливий код у програмному забезпеченні Orion IT для моніторингу та управління, яке використовується тисячами підприємств і державних установ у всьому світі. Злам SolarWinds став великою подією не тому, що було зламано одну компанію, а тому, що він спровокував набагато більший інцидент у ланцюзі поставок, який вплинув на тисячі організацій, також і уряд США. Під час цього зламу ймовірні державні хакери, яких Microsoft ідентифікувала як групу, відому як Nobelium (російське хакерське угруповання). Понад 30 000 державних і приватних організацій, зокрема місцеві, державні та федеральні агентства, використовують систему управління мережею Orion для управління своїми IT-ресурсами. Постраждали не лише клієнти SolarWinds. Оскільки хакерство виявило внутрішню роботу користувачів Orion, хакери потенційно могли отримати доступ до даних і мереж їхніх клієнтів та партнерів. Згідно з повідомленнями, зловмисне програмне забезпечення вразило багато компаній і організацій США. Постраждали навіть такі державні департаменти, як Міністерство внутрішньої безпеки, Державний департамент, Міністерство торгівлі та фінансів. Від цієї атаки також постраждали такі приватні компанії, як FireEye, Microsoft, Intel, Cisco і Deloitte [8].

Що ж стосується української практики у сфері загроз і викликів інформаційній безпеці, то розглянемо це питання через призму війни. Якщо проаналізуємо, яка ж була хронологія подій у повномасштабному вторгненні, то буде помітно як постійно, ледь не щомісяця здійснюються атаки на українські системи з метою викрадення інформації. Одна з заяв НАТО 28 лютого 2022 року звучала: “Кібератака на державу-члена НАТО може спричинити дію статті 5 (пункт про колективну оборону), заявив офіційний представник НАТО на тлі занепокоєння, що хаос у кіберпросторі навколо вторгнення росії в Україну може поширитися на інші території”. Військовий альянс упродовж багатьох років чітко давав зрозуміти, що серйозна кібератака може спровокувати дію пункту, але такий сценарій поки що був переважно гіпотетичним [9].

Розглянемо, які інформаційні небезпеки були в перші дні повномасштабного вторгнення. 25 лютого: фішингові атаки, ймовірно, від білоруських хакерів спрямовані проти українських військовослужбовців [10]; фейки про “перевірки” від СБУ, нібито СБУ вимагає від українців перейти за

посиланням, через що згодом ворог хоче отримати доступ до акаунтів українців та дуже багато іншого, про що сповіщає урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA [11].

Загалом, на думку дослідників, Україна має всі шанси та можливості в досягненні технологічного лідерства, оскільки має для цього всю потрібну базу. Досягнення в сфері ШІ, належного захисту інформації, вплинуть на національну оборону і безпеку, ґрунтуючись на революційних змінах у трьох сферах – військовій, інформаційній та економічній. Наприклад, у військовій сфері доступні комерційні технології, які використовують штучний інтелект, такі як безпілотні літальні апарати, зокрема ударні, безпілотні літальні апарати різних діапазонів, крилаті ракети з автоматичним визначенням цілей. Ці технології можуть надати доступ до нових засобів високоточного завдання ударів, зокрема на великі відстані. Іншим прикладом є технологія машинного навчання, яка може автоматизувати аналіз супутникових зображень і забезпечити кіберзахист. У сфері інформаційної та кібернетичної безпеки штучний інтелект значно розширить можливості збору та аналізу даних, реагування на кіберінциденти, а також створення агрегованих даних. Під час розв'язання завдань розвідки це означатиме врахування більшого числа джерел об'єктивної інформації, а також джерел дезінформації та інформаційних впливів [12, с. 149].

О. М. Степко вважає, що розв'язання проблеми забезпечення безпеки інформації в державі потребує розв'язання таких широкомасштабних завдань, як розроблення теоретичних засад безпеки інформації та нормативно-правової бази, яка регламентує вирішення усіх аспектів забезпечення безпеки інформації, створення системи органів, що відповідають за безпеку інформації та вирішення питань керування захистом інформації та її автоматизації, покращення виробництва засобів захисту інформації й організація підготовки відповідних фахівців [4, с. 90].

Основні загрози та виклики у сфері інформаційної безпеки держав, підприємств і просто фізичних осіб зростають прямопропорційно зі швидкістю розвитку видів атак на бази даних, сервіси та архіви. Навіть найбільш захищені сфери, такі як політика та оборона держав, стають цілями зловмисників, які намагаються викрасти інформацію.

Російсько-українська війна наочно демонструє, що інформація може бути використана як засіб масового впливу. У цьому контексті необхідно розробити ефективний механізм, який гарантуватиме інформаційну безпеку України. На нашу думку, основними компонентами цього механізму мають бути:

Технічний аспект – створення відповідної технічної інфраструктури для забезпечення функціонування інформаційної безпеки.

Політичний аспект – розробка державної політики, спрямованої на забезпечення інформаційної безпеки.

Правовий аспект – прийняття якісних нормативно-правових актів, які визначатимуть всі заходи інформаційної безпеки.

Ці три складові частини взаємодоповнюють одна одну і є основними для створення ефективної системи захисту від інформаційних загроз.

Крім того, треба звернути увагу на практичні аспекти, які сприятимуть забезпеченню інформаційної безпеки в державі. Насамперед це щоденне об'єктивне ознайомлення з новинами та іншою інформацією за допомогою державних інтернет-видань, медіа та звернень до громадськості. Регулярне подання інформації про основні події, особливо під час періоду війни, допомагає розсіяти чутки та розкрити фейки. Також важливо навчати громадян основ критичного мислення, розпізнавання дезінформації та фейків, а також безпеки в інтернеті. Не менш важливим є захист свободи слова та інформаційних прав громадян на доступ до інформації і конфіденційність даних, водночас забезпечуючи прозорість та відповідальність у роботі медіа та інших інформаційних платформ.

Висновки. Отже, у контексті сучасних трансформаційних змін суспільства, геополітичної обстановки та воєнного стану в Україні, практика застосування забезпечення інформаційної без-

пеки виявляється надзвичайно важливою. Завдяки розумінню та ефективному застосуванню різноманітних методів і стратегій, держава може ефективно протидіяти дезінформації, кібератакам та іншим інформаційним загрозам. Зокрема, потрібно зосередитися на підвищенні кібербезпеки, освіті та обізнаності громадян, розвитку правової бази та міжнародному співробітництві. Тільки шляхом комплексного підходу і впровадження відповідних заходів можна забезпечити ефективну інформаційну безпеку, особливо в умовах війни, зберігаючи свободу слова та інформаційні права громадян.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 15 жовтня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

2. Конституція України від 28 червня 1996 року. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80#Text

3. Сопілко І. М. (2021). Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник*. 2021. № 2 (59). С. 110–115.

4. Степко О. М. (2011). Аналіз головних складових інформаційної безпеки держави. *Науковий вісник Національного авіаційного університету*. 2011. Том 1. № 3. С. 90–99.

5. Кормич Б. А. (2004). Організаційно-правові основи політики інформаційної безпеки України: дис. ... д-ра юрид. наук: 12.00.07 / Національний ун-т внутрішніх справ. Х., 2004. URL: http://www.disslib.org/orhanizatsiyno-pravovi-osnovy-polityky-informatsiynoyi-bezpeky-ukrayiny.html

6. DOT Security. What Are the 3 Components of Information Security. 24.10. 2023. URL: https://dotsecurity.com/insights/blog-what-are-the-components-information-security

7. Rabeya Islam Rima. Cyber security in modern world. 14.01.2024. URL: https://www.educative.io/answers/what-are-some-challenges-in-information-security

8. Saheed Oladimeji, Sean Michael Kerner. SolarWinds hack explained: Everything you need to know. 03.11.2023. URL: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

9. Пірсон Дж., Лендей Дж. (2022). Кібератака на НАТО може активувати положення про колективну оборону – офіційно. 28.02.2022. URL: https://www.reuters.com/world/europe/cyberattack-nato-could-trigger-collective-defence-clause-official-2022-02-28/

10. Мастерс Дж. Російсько-українська війна: кібератака – Хронологія кінетичної війни. 26.01.2024. URL: https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion

11. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA. Офіційна Facebook-Сторінка. URL: https://www.facebook.com/UACERT

12. Шевченко А. І. (2023). Стратегія розвитку штучного інтелекту в Україні: монографія. Київ, 2023. С. 305. URL: https://jai.in.ua/archive/2023/ai_mono.pdf

13. Мазуренко Л. І. (2022). Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія "Питання політології"*. 2022. Випуск 42. URL: https://periodicals.karazin.ua/politology/article/view/22088/20387

REFERENCES

1. ***Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy*** vid 15 zhovtnia 2021 roku "Pro Stratehiiu informatsiinoi bezpeky". (2021, October 15) [On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On Information Security Strategy"]. Retrieved from: https://zakon.rada.gov.ua/laws/show/685/2021#Text [In Ukrainian].

2. ***Konstytutsiia Ukrainy*** (1996, June 28) [Constitution of Ukraine]. Retrieved from: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text [In Ukrainian].

3. Sopilko, I. M. (2021). ***Informatsiina bezpeka ta kiberbezpeka: porivnialno-pravovyi aspekt*** [Information security and cyber security: a comparative legal aspect]. *Yurydychnyi visnyk*. No. 2 (59). P. 110–115 [In Ukrainian].

4. Stepko, O. M. (2011). ***Analiz holovnykh skladovykh informatsiinoi bezpeky derzhavy***. [Analysis of the main components of information security of the state]. *Naukovyi visnyk Natsionalnoho aviatsiinoho universytetu*. Tom 1. No. 3. P. 90–99 [In Ukrainian].

5. Kormych, B. A. (2004). ***Orhanizatsiino-pravovi osnovy polityky informatsiinoi bezpeky Ukrainy*.** [Organizational and legal foundations of information security policy of Ukraine]. Doctor's thesis. Kharkiv. Retrieved from: http://www.disslib.org/orhanizatsiyno-pravovi-osnovy-polityky-informatsiynoyi-bezpeky-ukrayiny.html [In Ukrainian].

6. ***DOT Security.*** What Are the 3 Components of Information Security (24.10.2023). Retrieved from: https://dotsecurity.com/insights/blog-what-are-the-components-information-security [In English].

7. Rabeya Islam Rima. ***Cyber security in modern world*** (14.01.2024). Retrieved from: https://www.educative.io/answers/what-are-some-challenges-in-information-security [In English].

8. Saheed Oladimeji, Sean Michael Kerner. ***SolarWinds hack explained: Everything you need to know***" (03.11.2023). Retrieved from: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know [In English].

9. Pirson, Dz., Lendei, Dz. ***Kiberataka na NATO mozhe aktyvuvaty polozhennia pro kolektyvnu oboronu – ofitsiino***" (28.02.2022). Retrieved from: https://www.reuters.com/world/europe/cyberattack-nato-could-trigger-collective-defence-clause-official-2022-02-28/

10. Masters, Dz. **Rosiisko-ukrainska viina: kiberataka – Khronolohiia kinetychnoi viiny** (26.01.2024). Retrieved from: https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion [In Ukrainian].

11. Uriadova komanda reahuvannia na kompiuterni nadzvychaini podii Ukrainy CERT-UA. Ofitsiina Facebook-Storinka. Retrieved from: https://www.facebook.com/UACERT [In Ukrainian].

12. Shevchenko, A. I. (2023). ***Stratehiia rozvytku shtuchnoho intelektu v Ukraini:*** monohrafiia [Strategy for the development of artificial intelligence in Ukraine]. Kyiv, 305 p. Retrieved from: https://jai.in.ua/archive/2023/ai_mono.pdf [In Ukrainian].

13. Mazurenko, L. I. (2022). ***Informatsiina bezpeka v umovakh rosiisko-ukrainskoi viiny: vyklyky ta zahrozy***.[Information security in the conditions of the Russian-Ukrainian war: challenges and threats]. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina. Seriia* "*Pytannia politolohii*". Vypusk 42. Retrievedfrom: https:// periodicals.karazin.ua /politology/ article/view/ 22088/20387 [In Ukrainian].

Дата надходження: 15.04.2024 р.

Olha SKOCHYLIAS-PAVLIV
Lviv Polytechnic National University,
Educatinoal and Rasearch Institute of Law,
Psychology and Innovative Education,
Professor of the Administrative
and Information Law Department,
Doctor of Law, Professor
olha.v.skochylyas-pavliv@lpnu.ua
ORCID iD: https://orcid.org/0000-0001-6737-7628

LEGAL MECHANISMS FOR ENSURING INFORMATION SECURITY IN UKRAINE

The article considers the legal mechanisms for ensuring information security. It has been proven that today, more than ever, when there is a war in Ukraine, the issue of ensuring information security becomes especially relevant and significant, as the information space becomes a "battlefield" on a par with the war front. Enemy forces actively use informational and psychological operations to destabilize the situation inside our country, create panic, spread fakes and undermine trust in state institutions. In these conditions, the state's policy becomes important, which should be integral and effective in

countering these threats. An effective state policy in the field of information security will help ensure society's resilience to information threats, strengthen trust in state institutions, and maintain stability in crisis conditions. The author's understanding of information security is offered as a state of security of information resources and information systems, which ensures their confidentiality, integrity, availability and reliability, as well as protection against unauthorized access, disclosure, modification, destruction and other forms of abuse that may lead to a violation of national security, economic stability and social order. The main components of information security, which are the basis for information security for the state as a whole, individual bodies or private enterprises, are called confidentiality, integrity and availability. The main components of the mechanism for ensuring information security, in the opinion of the author, should be: technical (creation of appropriate technical infrastructure to ensure the functioning of information security), political (development of state policy aimed at ensuring information security) and legal (adoption of high-quality normative legal acts that will determine all information security measures). These three components complement each other and are key to creating an effective system of protection against information threats.

Key words: national security; information space; information technologies; information security; cyber security; threats to information security.