УДК 340+351
DOI 10.32782/2523-4269-2024-86-45-50

**Шевчук Михайло Олександрович,**
кандидат юридичних наук,
докторант кафедри конституційного,
адміністративного та фінансового права
*(Хмельницький університет управління та права імені Леоніда Юзькова, м. Хмельницький)*
*ORCID: https://orcid.org/0000-0001-7549-6344*

# ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З УРАХУВАННЯМ СУЧАСНИХ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

*Статтю присвячено дослідженню актуальних питань правового забезпечення інформаційної безпеки. Акцентовано увагу на системі нормативно-правового регулювання інформаційної безпеки. Проаналізовано зарубіжний досвід правового регулювання інформаційної безпеки. Значна увага приділяється проблемам у практичному застосуванні правових норм в галузі інформаційної безпеки, що включає у себе організаційно-правові правові виклики. Стаття пропонує конкретні шляхи розвитку законодавства у сфері інформаційної безпеки, спрямовані на покращення ефективності захисту інформації та запобігання можливим загрозам.*
***Ключові слова:*** *інформаційна безпека, інформаційне середовище, інформація, захист інформації, забезпечення інформаційної безпеки.*

**Постановка проблеми.** Цифрова ера та стрімкий розвиток інформаційних технологій призвели не тільки до зростання обсягу і доступності інформації, але й до загроз, пов'язаних з можливістю незаконного доступу, використання та розповсюдження конфіденційної інформації. Її суттєва роль як стратегічного ресурсу в сучасному суспільстві підкреслює необхідність ефективного захисту від потенційних загроз.

Крім того, в умовах повномасштабного вторгнення Російської Федерації на територію нашої держави тема правового забезпечення інформаційної безпеки набуває ще більшої актуальності, оскільки російська агресія не лише фізично впливає на територіальну цілісність та безпеку України, але й активно використовує інформаційні канали для маніпулювання суспільною думкою, дестабілізації політичної ситуації та дезінформації громадян, що відбувається через вплив на медіа, соціальні мережі та інші канали зв'язку.

Саме тому правове забезпечення інформаційної безпеки стає невід'ємною складовою в контексті захисту національних інтересів та суверенітету. Роль ефективних правових механізмів полягає у забезпеченні захисту від кібератак, захисту конфіденційної інформації, а також у боротьбі з дезінформацією та пропагандою. Правові норми повинні визначати права та обов'язки у сфері інформаційної безпеки, а також встановлювати механізми реагування на загрози та виклики, які постають з боку зовнішніх та внутрішніх загроз.

**Аналіз останніх досліджень і публікацій.** Проблематика правового забезпечення інформаційної безпеки досліджувалася багатьма науковцями. Серед українських науковців, які досліджували дане питання, можна виділити І. Арістова, О. Баранов, К. Бєляков, В. Брижко, І. Бондар, В. Гурковського, Р. Калюжний, Б. Кормич, Т. Ткачук, В. Цимбалюк, В. Шамрай, Р. Шаповал та інші.

За останні роки відношення до інформаційної безпеки нашої держави суттєво змінилось. Насамперед трансформовано саму природу, а відповідно і стратегічний вимір концепції забезпечення інформаційної безпеки держави. При цьому інформаційна безпека України постає не як щось віртуальне, абстрактний об'єкт наукового пізнання, а як абсолютно реальна субстанція, в межах якої точаться запеклі бої, існують очевидні загрози з явними наслідками. Можемо упевнено стверджувати, що в Україні зважаючи на інформаційну війну яка ведеться росією проти нашої держави одним з найгостріших питань стає правове забезпечення стратегічної концепції інформаційної безпеки. Крім того потрібно зазначити, що всі довоєнні напрацювання в даній сфері є вагомим підґрунтям для подальшого розвитку і наукових досліджень. Однак, зміна обставин, що зумовлено сучасними реаліями загострила необхідність не лише переосмислення підходів до правової регламентації інформаційної сфери але й показала, що правова складова національної безпеки напряму залежить від безпеки в інформаційній сфері. При цьому деякі особливості правового забезпечення інформаційної безпеки в умовах воєнного стану не були предметом дослідження науковців. Тому важливим та необхідним є більш детальне вивчення даної проблематики.

**Метою статті** є аналіз особливостей правового забезпечення інформаційної безпеки з урахуванням повномасштабного вторгнення Російської Федерації в Україну та його впливу на національну безпеку та цифрові інформаційні ресурси.

**Виклад основного матеріалу.** Інформаційна безпека стала однією з найбільш актуальних проблем у сучасному цифровому світі. Перед владою кожної розвиненої держави постає завдання забезпечити ефективне правове регулювання цієї сфери для захисту як індивідуальних прав і свобод громадян, так і національних інтересів. На сьогодні інформаційна безпека не обмежується лише захистом даних від несанкціонованого доступу. Вона охоплює також проблеми кібертеро-

ризму, кібершпигунства, дезінформації та інші аспекти цифрової безпеки. Відповідно, правове регулювання в цій сфері має включати законодавство, спрямоване на попередження таких загроз, виявлення порушень і відповідальне покарання винних.

Ефективне правове регулювання інформаційної безпеки передбачає наявність чітких і конкретних нормативних актів, які визначають права та обов'язки суб'єктів цієї сфери, процедури виявлення та реагування на інциденти, а також механізми міжнародного співробітництва у цій галузі.

Завдяки правовому регулюванню можна забезпечити необхідний рівень забезпечення безпеки в інформаційному просторі, уникнути переважання інтересів держави над правами громадян або навпаки. Крім того, воно сприяє розвитку технологічних інновацій та стимулює розвиток безпечного цифрового середовища для всіх користувачів.

Дослідження нормативно-правового регулювання дозволить нам визначити ключові правові акти, що визначають правила та принципи функціонування системи інформаційної безпеки держави, а також оцінити ефективність їх впровадження та виконання.

Як зазначає Є. І. Лапінська, нормативна база інформаційної безпеки виконує три основні функції: 1. Регулює взаємовідносини між суб'єктами інформаційної безпеки, визначає їх права обов'язки та відповідальність. 2. Нормативно забезпечує дії суб'єктів інформаційної безпеки на всіх рівнях, а саме – людини, суспільства, держави. 3. Встановлює порядок застосування різних сил і засобів забезпечення інформаційної безпеки [1, с. 64].

Не заперечуючи позицію авторки, варто зазначити, що нормативна база інформаційної безпеки також виконує ряд інших важливих завдань, які сприяють зміцненню та забезпеченню безпеки інформації на всіх рівнях. По-перше, це забезпечення соціальної відповідальності. Нормативна база може стимулювати суб'єкти інформаційної безпеки до вжиття заходів з підвищення свідомості щодо ризиків та загроз для інформаційної безпеки. По-друге, це створення механізмів контролю та нагляду. Нормативна база може передбачати створення органів або механізмів контролю, які забезпечують відповідність суб'єктів інформаційної безпеки встановленим стандартам та вимогам. По-третє, це профілактика та реагування на інциденти. Нормативна база може включати положення щодо розробки планів профілактики та реагування на інциденти інформаційної безпеки.

На сьогодні розробка та вдосконалення законодавчої бази інформаційної безпеки є необхідним заходом, що задовольняє найпершу потребу у захисті інформації при розвитку соціально-економічних, політичних, військових напрямів діяльності кожної держави. Нормативну базу щодо забезпечення інформаційної безпеки доцільно розглядати з урахуванням існуючої ієрархії нормативних актів.

Конституційні норми є основою правового забезпечення інформаційної безпеки в більшості країн. Відповідно до ст. 17 Основного Закону України захист суверенітету й територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу [2], тому актуальним для України є проведення динамічних, обґрунтованих та комплексних реформ, які мають забезпечити модернізацію держави в контексті залучення кращого світового досвіду, що, своєю чергою, передбачає ефективне впровадження досягнень теорії та практики державного управління в сфері забезпечення національної безпеки, особливо в контексті тих викликів, з якими стикнулася Україна починаючи з 2014 року [3]. Закріплення інформаційної безпеки на конституційному рівні відображає визнання її стратегічного значення для суспільства.

Міжнародне співробітництво у сфері інформаційної безпеки визнається ключовим елементом забезпечення стійкості та безпеки в цифровому просторі. У цьому контексті, угоди та конвенції, укладені між державами та іншими суб'єктами міжнародного права, відіграють важливу роль у встановленні міжнародних стандартів та принципів щодо захисту інформаційної безпеки. Особливе місце в системі нормативно-правових актів щодо забезпечення інформаційної безпеки займають міжнародно-правові акти, зокрема: Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних [4]; Конвенція про кіберзлочинність [5]; Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних [6]; Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру [7].

Законодавчий рівень нормативно-правових актів представлений цілою низкою фундаментальних законів. Основу інформаційного законодавства складають такі закони: «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги», «Про Національну поліцію», «Про національну інфраструктуру геопросторових даних», «Про доступ до публічної інформації», «Про основні засади забезпечення кібербезпеки України» тощо.

У 2014 році виконуючий обов'язки Президента України, голова Верховної Ради України Олександр Турчинов підписав Указ № 449/2014 про рішення РНБО від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [8].

Цей документ відображав важливість та актуальність питань інформаційної безпеки в контексті змін в політичному, економічному та соціальному житті країни, що виникли у зв'язку з подіями Революції Гідності та подальшими наслідками. Такі кроки свідчили про необхідність адаптації законодавства до нових реалій та зміцнення захисту інформаційних ресурсів держави в умовах ростучих загроз з боку зовнішніх і внутрішніх акторів.

З метою забезпечення інформаційної безпеки в Україні Указом Президента України від 25.02.2017 р. була затверджена «Доктрина інформаційної безпеки України» [9]. В сучасних умовах війни 18 березня 2022 року прийнято рішення РНБО «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», в якому визначено, що в умовах воєнного стану реалізація єдиної інформаційної політика є пріоритетним питанням національної безпеки» [10].

Загалом, підзаконні нормативно-правові акти щодо інформаційної безпеки відіграють вирішальну роль у системі правового регулювання даної сфери. Вони встановлюють конкретні правила, процедури та стандарти, які допомагають реалізувати загальні принципи та цілі, визначені на рівні стратегічного керівництва. Ці акти забезпечують системність та конкретність у діяль-

ності органів влади, підприємств та інших суб'єктів, що сприяє ефективному впровадженню стратегічних заходів і політики у галузі інформаційної безпеки. Такий підхід дозволяє забезпечувати високий рівень захищеності інформаційних ресурсів та зменшувати ризики виникнення загроз у цій сфері, що є критичним для національної безпеки та стабільності держави.

Незважаючи на наявність такого законодавства, існують відомі проблеми у практичному застосуванні правових норм в галузі інформаційної безпеки. Однак єдності у шляхах якісної трансформації інформаційного законодавства України серед дослідників цієї проблематики не існує, що є логічним, зважаючи на складність, динаміку та масштабність сучасних інформаційних процесів, які відбуваються в умовах становлення національної правової системи [11, с. 252].

З метою забезпечення стабільності та безпеки в інформаційному просторі держави всього світу звертають увагу на розвиток ефективних правових механізмів, спрямованих на захист інформаційної інфраструктури та особистих даних громадян.

Наприклад, у 2015 році в Сполучених Штатах Америки був прийнятий Закон про кібербезпеку, спрямований на підвищення рівня інформаційної безпеки за допомогою розширення обміну даними щодо кібербезпеки між урядовими структурами та фірмами-виробниками. Основні положення закону спрощують компаніям обмін особистою інформацією з урядом, особливо в сучасних умовах кіберзагроз. Закон також передбачає створення системи федеральних агентств для отримання інформації щодо загроз від приватних компаній [12]. Прийняття подібного Закону відображає тенденцію до збільшення співпраці між урядом і приватним сектором для боротьби з кіберзагрозами. Це підкреслює важливість інтеграції та співпраці між різними суб'єктами для ефективного захисту від кібератак.

Загалом, в розвинених державах велика увага приділяється розробці законодавства та створенню національних служб з захисту прав людини. В США провідну роль у сфері комп'ютерних злочинів відіграє Федеральне Бюро Розслідувань (ФБР), яке в рамках штатів встановило правила боротьби з комп'ютерною злочинністю. Крім того, діє Центральне Розвідувальне Управління (ЦРУ), яке забезпечує безпеку комп'ютерних комунікацій шляхом моніторингу спілкування [13]. Така співпраця між різними структурами в США сприяє покращенню загальної кібербезпеки країни та забезпечує захист від кіберзагроз на різних рівнях, що є критичним для збереження національної безпеки та захисту інформаційної сфери в умовах зростаючих кіберзагроз.

Інтеграція України до Європейського Союзу сьогодні є однією з найважливіших стратегічних цілей, які визначають розвиток держави на сучасному етапі. З моменту оголошення наміру набуття повноцінного членства в ЄС, Україна активно здійснює реформи на шляху до відповідності стандартам Європейського Союзу в різних сферах життя, включаючи інформаційну безпеку.

Аналіз законодавства держав-членів Європейського Союзу стосовно інформаційної безпеки є важливим етапом в підготовці України до інтеграції до ЄС, оскільки це сприятиме гармонізації національного законодавства з європейськими стандартами та підвищенню ефективності заходів з захисту інформації в країні.

Розробка правового регулювання та узгодження відповідних стандартів забезпечення інформаційної безпеки, включаючи безпеку інформаційних технологій, в країнах Європейського Союзу розпочалася значно раніше, ніж в Україні, тому воно має системний і досконалий характер. Крім того, нормативне регулювання забезпечення інформаційної безпеки в ЄС є більш чітким і структурованим: передусім чітко визначені основні поняття і категорії, надано перелік відповідних загроз інформаційній безпеці, таких як особисті дані особи та інше.

Наприклад, правове регулювання інформаційної безпеки у Німеччині характеризується детальною розробкою системи різних видів інформації з обмеженим доступом, чіткі формулювання їх понять у федеральному законодавстві. Відповідно до Закону «Про перевірку безпеки» [14] до системи секретної інформації входять державна таємниця та відомча таємниця, охорона яких, на відміну від інших видів таємниць, що стосуються конфіденційної сфери приватних осіб, обумовлена інтересами зовнішньої безпеки держави.

Національна інформаційна політика Польщі спрямована на побудову вільного відкритого суспільства, впровадження концепції вільного транскордонного обігу інформації, забезпечення прав людини. Ключову роль у забезпеченні кібернетичної безпеки відіграє Агентство внутрішньої безпеки, яке у 2013 році розробило Стратегію кібербезпеки Польщі та ініціювало створення Центру криптології при Міністерстві національної оборони, на який покладено завдання щодо захисту інформації, кібероборони та проведення наступальних кібероперацій [15].

У контексті дослідження правового регулювання інформаційної безпеки в країнах Європи відзначається важливість системного та комплексного підходу до захисту інформації та забезпечення кібербезпеки. Зазначені приклади свідчать про впровадження відповідної законодавчої бази, спрямованої на створення відкритих, демократичних суспільств, які гарантують права та свободи громадян у цифровому просторі.

Німецьке правове середовище відрізняється детальним розробленням системи класифікації інформації з обмеженим доступом, що сприяє ефективному контролю за розголошенням державних таємниць. Це вказує на серйозний підхід до захисту конфіденційної інформації та збереження національної безпеки. У Польщі вагомий акцент робиться на розробці стратегій кібербезпеки та створенні спеціалізованих структур для забезпечення захисту інформації та проведення відповідних кібероперацій. Це свідчить про прагнення підвищити рівень кібербезпеки в країні та зберегти національну безпеку в умовах постійної кіберзагрози.

В Україні на сьогодні існують деякі проблеми, які, на нашу думку, потребують уваги та вирішення:

1. Недостатня адаптація законодавства до швидкого темпу технологічного розвитку. Інновації у сфері інформаційних технологій можуть швидко змінюватись, що вимагає постійного оновлення правових актів для ефективного реагування на нові виклики та загрози.

2. Недостатня координація між різними органами влади у сфері кібербезпеки. Відсутність централізованого механізму управління та координації може ускладнювати ефективне реагування на кіберзагрози та події.

3. Низький рівень кіберграмотності в суспільстві. Багато громадян та бізнесів не мають достатньої обізнаності щодо загроз кібербезпеці та методів їх запобігання.

4. Недостатня ефективність механізмів виявлення та розслідування кіберзлочинності. Удосконалення

механізмів співпраці між правоохоронними органами та іншими структурами може сприяти більш успішному протидії кіберзлочинності.

На сьогодні в Україні існує необхідність врахування сучасних реалій, пов'язаних з війною Російської Федерації проти нашої держави, і прийняття Концепції інформаційної безпеки України, яка комплексно врегулювала б цю сферу відносин. Перш ніж прийняти таку Концепцію, необхідно визначити питання, які регулюватимуться в ній. На наш погляд, у цій Концепції має бути закріплено таке: державна політика у сфері забезпечення інформаційної безпеки, заходи захисту інформації, види та джерела загроз у сфері інформаційної безпеки, першочергові заходи щодо забезпечення інформаційної безпеки.

Загалом, розвиток законодавства у сфері інформаційної безпеки має великий потенціал у забезпеченні високого рівня захисту інформації та кібербезпеки. Такі перспективи повинні включати:

1. Адаптація до технологічного прогресу. Законодавство повинно постійно оновлюватися та адаптуватися до нових технологічних відкриттів та загроз. Регулярне оновлення правових актів дозволить враховувати сучасні тенденції та забезпечувати ефективний захист інформації.

2. Міжнародне співробітництво. Удосконалення міжнародного співробітництва та приєднання до міжнародних конвенцій та угод допоможе Україні зміцнити своє позиціонування у глобальному кіберпросторі та ефективно протидіяти транскордонним кіберзагрозам.

3. Забезпечення кібербезпеки в критичних секторах. Важливо розвивати законодавство, спрямоване на захист критично важливих інфраструктур, таких як енергетика, транспорт, медицина тощо, щоб зменшити ризики кібератак та забезпечити неперервність функціонування.

4. Збільшення кіберграмотності. Розвиток законодавства, спрямованого на підвищення рівня кіберграмотності серед населення та підприємств, є важливим кроком у забезпеченні ефективного захисту інформації та кібербезпеки.

5. Створення спеціалізованих органів управління. Важливо розглядати можливість створення спеціалізованих органів управління, які б займалися координацією та моніторингом діяльності в галузі кібербезпеки.

Отже, розвиток законодавства у сфері інформаційної безпеки має багато перспектив, які можуть сприяти забезпеченню стійкого та безпечного інформаційного середовища для усіх учасників суспільства.

**Висновки.** У світі, де інформація стала одним із найцінніших ресурсів, правове забезпечення інформаційної безпеки стає важливою складовою для захисту прав та інтересів громадян, підприємств та держави в цілому. Правове забезпечення інформаційної безпеки базується на комплексі міжнародних угод та національних нормативно-правових актів, спрямованих на захист конфіденційності, цілісності та доступності інформації.

Незважаючи на наявність відповідного законодавства, практичне застосування правових норм у сфері інформаційної безпеки стикається з численними проблемами.

У сучасних умовах складних та динамічних процесів інформатизації, що відбуваються у контексті розвитку національної правової системи, відсутність єдності щодо якісної трансформації інформаційного законодавства в Україні є логічною. Це обумовлено низкою чинників, серед яких варто виокремити недостатню адаптацію законодавства до швидкого темпу технологічного розвитку, недостатню координацію між органами влади у сфері кібербезпеки, низький рівень кіберграмотності в суспільстві та неефективність механізмів виявлення та розслідування кіберзлочинності.

Урахування сучасних реалій, пов'язаних із загрозою з боку Російської Федерації та вирішення вищезазначених проблем можуть бути досягнуті через прийняття та реалізацію Концепції інформаційної безпеки України. Важливо, щоб у такій Концепції було закріплено державну політику у цій сфері, заходи захисту інформації, види та джерела загроз, а також першочергові заходи для забезпечення інформаційної безпеки.

Розвиток законодавства у галузі інформаційної безпеки має потенціал у забезпеченні високого рівня захисту інформації та кібербезпеки через адаптацію до технологічного прогресу, міжнародне співробітництво, захист критичних секторів, підвищення кіберграмотності та створення спеціалізованих органів управління. Такий розвиток законодавства відкриває перспективи для створення стійкого та безпечного інформаційного середовища для всіх учасників суспільства.

**Список використаних джерел**

1. Лапінська Є. І. Основні питання законодавства України у сфері інформаційної безпеки. *Науковий вісник Міжнародного гуманітарного університету*. 2019 № 39. С. 64–67.

2. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

3. Нестерович В. Ф. Громадські протести на окремих територіях Українського Донбасу протягом весни 2014 року: причини та наслідки. *Віче*. 2014. № 21. С. 14–17.

4. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, ратифікована згідно із Законом України № 2438–VI від 06.07.2010 р. URL: http://zakon1.rada.gov.ua/cgi–bin/laws/main.cgi?nreg=994_326 (дата звернення: 19.02.2024 р.).

5. Конвенція про кіберзлочинність ратифікована згідно із Законом України № 2824–IV від 07.09.2005 р. URL: http://zakon1.rada.gov.ua/cgi–bin/laws/main.cgi?nreg=994_575 (дата звернення: 19.02.2024 р.).

6. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних, ратифікований згідно із Законом України № 2438–VI від 06.07.2010 р. URL: http://zakon1.rada.gov.ua/cgi–bin/laws/main.cgi?nreg=994_363 (дата звернення: 20.02.2024 р.).

7. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, ратифікований Законом України № 23–V від 21.07.2006 р. URL: http://zakon.rada.gov.ua/cgi–bin/laws/main.cgi?nreg=994_687 (дата звернення: 20.02.2024 р.).

8. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Указ Президента України від від 01.05.2014 № 449/2014. URL: https://zakon.rada.gov.ua/laws/show/449/2014#Text (дата звернення: 20.02.2024 р.).

9. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 47/2017. URL: https://zakon.rada.gov.ua/go/47/2017 (дата звернення: 20.02.2024 р.).

10. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19 березня 2022 року № 152/2022. URL: https://zakon.rada.gov.ua/go/152/2022 (дата звернення: 21.02.2024 р.).

11. Нижник Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навчальний посібник. Н.Р. Нижник, Г.П. Ситник, В.Т. Білоус. Ірпінь : Акад. ДПС України, 2000. 304 с.

12. Taplin Ruth. Managing Cyber Risk in the Financial Sector: Lessons from Asia, Europe and the USA (Routledge Studies in the Growth Economies of Asia). Routledge, 2016, p. 167-169. URL: https://www.routledge.com/Managing-Cyber-Risk-in-the-Financial-Sector-Lessons-from-Asia-Europe-and/Taplin/p/book/9781138477179 (дата звернення: 21.02.2024 р.).

13. Baron R.M.F. A critique of the international cybercrime treaty./Comm-Law Conspectus, 2002, N.10, p. 263–278.

14. Gesetz uber die Voraussetzungen und das Verfahren von Sicherheitsuberprufungen des Bundes und den Schutz von Verschlus– ssachen (Sicherheitsuberprufungsgesetz SUG. URL: http://www.gesetze-im-internet.de/s_g/BJNR086700994.html (дата звернення: 21.02.2024 р.).

15. Across Europe? Nations Mold Cyber Defenses. URL: http://archive.defensenews.com/article/20130709/DEFREG01/307090008/ Across-Europr-Nations-Mold-Cyber-Defenses (дата звернення: 21.02.2024 р.).

**References**

1. Lapins′ka, Y.E. (2019). Osnovni pytannya zakonodavstva Ukrayiny u sferi informatsiynoyi bezpeky [Basic issues of Ukrainian legislation in the field of information security]. Naukovyy visnyk Mizhnarodnoho humanitarnoho universytetu – Scientific Bulletin of the International Humanitarian University. № 39. S. 64–67 [in Ukrainian].

2. Konstytutsiya Ukrayiny: pryynyata na p″yatiy sesiyi Verkhovnoyi Rady Ukrayiny 28 chervnya 1996 roku [The Constitution of Ukraine]. Vidomosti Verkhovnoyi Rady Ukrayiny. 1996. № 30. St. 141 [in Ukrainian].

3. Nesterovych, V.F. (2014). Hromads′ki protesty na okremykh terytoriyakh Ukrayins′koho Donbasu protyahom vesny 2014 roku: prychyny ta naslidky [Public protests in certain territories of the Ukrainian Donbas during the spring of 2014: causes and consequences]. *Viche*. № 21. S. 14–17 [in Ukrainian].

4. Konventsiya pro zakhyst osib u zv′yazku z avtomatyzovanoyu obrobkoyu personal′nykh danykh [The Convention on the Protection of Individuals in Connection with Automated Processing of Personal Data] ratyfikovana zhidno iz Zakonom Ukrayiny № 2438–VI vid 06.07.2010. Retrieved from: http://zakon1.rada.gov.ua/cgi–bin/laws/main.cgi?nreg=994_326 (data zvernennya: 19.02.2024) [in Ukrainian].

5. Konventsiya pro kiberzlochynnist′ [The Convention on Cybercrime] ratyfikovana z·hidno iz Zakonom Ukrayiny № 2824–IV vid 07.09.2005. Retrieved from: http://zakon1.rada.gov.ua/cgi–bin/laws/main.cgi?nreg=994_575 (data zvernennya: 19.02.2024) [in Ukrainian].

6. Dodatkovyy protokol do Konventsiyi pro zakhyst osib u zv′yazku z avtomatyzovanoyu obrobkoyu personal′nykh danykh shchodo orhaniv nahlyadu ta transkordonnykh potokiv danykh [Additional Protocol to the Convention on the Protection of Individuals in Connection with Automated Processing of Personal Data Regarding Supervisory Authorities and Cross-Border Data Flows], ratyfikovanyy z·hidno iz Zakonom Ukrayiny № 2438–VI vid 06.07.2010. Retrieved from: http://zakon1.rada.gov.ua/cgi–bin/laws/main.cgi?nreg=994_363 (data zvernennya: 20.02.2024) [in Ukrainian].

7. Dodatkovyy protokol do Konventsiyi pro kiberzlochynnist′, yakyy stosuyet′sya kryminalizatsiyi diy rasyst·s′koho ta ksenofobnoho kharakteru, vchynenykh cherez kompyuterni systemy [Additional Protocol to the Convention on Cybercrime, which concerns the criminalization of racist and xenophobic acts committed through computer systems], ratyfikovanyy Zakonom Ukrayiny № 23–V vid 21.07.2006 r. Retrieved from: http://zakon.rada.gov.ua/cgi–bin/laws/main.cgi?nreg=994_687 (data zvernennya: 20.02.2024) [in Ukrainian].

8. Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 28 kvitnya 2014 roku «Pro zakhody shchodo vdoskonalennya formuvannya ta realizatsiyi derzhavnoyi polityky u sferi informatsiynoyi bezpeky Ukrayiny [On measures to improve the formation and implementation of state policy in the field of information security of Ukraine]: Ukaz Prezydenta Ukrayiny vid vid 01.05.2014 № 449/2014. Retrieved from: https://zakon.rada.gov.ua/laws/show/449/2014#Text (data zvernennya: 20.02.2024) [in Ukrainian].

9. Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 29 hrudnya 2016 roku «Pro Doktrynu informatsiynoyi bezpeky Ukrayiny» [On the Information Security Doctrine of Ukraine]: Ukaz Prezydenta Ukrayiny vid 25 lyutoho 2017 roku № 47/2017. Retrieved from: https://zakon.rada.gov.ua/go/47/2017 (data zvernennya: 20.02.2024) [in Ukrainian]

10. Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 18 bereznya 2022 roku «Shchodo realizatsiyi yedynoyi informatsiynoyi polityky v umovakh voyennoho stanu» [Regarding the implementation of a unified information policy under martial law]: Ukaz Prezydenta Ukrayiny vid 19 bereznya 2022 roku № 152/2022. Retrieved from: https://zakon.rada.gov.ua/go/152/2022 (data zvernennya: 21.02.2024) [in Ukrainian].

11. Nyzhnyk, N.R. (2000). Natsional′na bezpeka Ukrayiny (metodolohichni aspekty, stan i tendentsiyi rozvytku): navchal′nyy posibnyk [National security of Ukraine (methodological aspects, state and trends of development): study guide]. N.R. Nyzhnyk, H.P. Sytnyk, V.T. Bilous. Irpin′: Akad. DPS Ukrayiny, 304 s. [in Ukrainian].

12. Taplin Ruth. Managing Cyber Risk in the Financial Sector: Lessons from Asia, Europe and the USA (Routledge Studies in the Growth Economies of Asia). Routledge, 2016, p. 167–169. Retrieved from: https://www.routledge.com/Managing-Cyber-Risk-in-the-Financial-Sector-Lessons-from-Asia-Europe-and/Taplin/p/book/9781138477179 (data zvernennya: 21.02.2024) [in English].

13. Baron, R.M.F. (2002). A critique of the international cybercrime treaty./Comm-Law Conspectus, N. 10, p. 263–278 (data zvernennya: 21.02.2024) [in English].

14. Gesetz uber die Voraussetzungen und das Verfahren von Sicherheitsuberprufungen des Bundes und den Schutz von Verschlus– ssachen (Sicherheitsuberprufungsgesetz SUG. Retrieved from: http://www.gesetze-im-internet.de/s_g/BJNR086700994.html (data zvernennya: 21.02.2024) [in German].

15. Across Europe? Nations Mold Cyber Defenses. Retrieved from: http://archive.defensenews.com/article/20130709/DEFREG01/307090008/ Across-Europr-Nations-Mold-Cyber-Defenses (data zvernennya: 21.02.2024) [in English].

**Shevchuk Mykhailo,**
PhD in Law,
Doctoral Student at the Department of Constitutional,
Administrative and Financial law
*(Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi)*
*ORCID: https://orcid.org/0000-0001-7549-6344*

## FEATURES OF LEGAL ENSUREMENT OF INFORMATION SECURITY TAKING INTO ACCOUNT CURRENT THREATS TO NATIONAL SECURITY

*The article is devoted to the study of current issues of legal provision of information security. Attention is focused on the system of normative and legal regulation of information security. The foreign experience of legal regulation of information security is analyzed. Considerable attention is paid to problems in the practical application of legal norms in the field of information security, which includes organizational and legal legal challenges. The article offers specific ways of developing legislation in the field of information security aimed at improving the effectiveness of information protection and preventing possible threats.*

***Key words:*** *information security, information environment, information, information protection, ensuring information security.*

Надіслано до редколегії 26.02.2024