

digital environment, minimising the risks of system compromise and data leakage. Scientific research confirms that ZTS implementation significantly reduces the likelihood of successful attacks through the use of multi-factor authentication, micro-segmentation and continuous threat monitoring.

– At the same time, the implementation of Zero Trust requires significant financial and organisational resources, including infrastructure upgrades, staff training and the creation of adaptive access policies. This underscores the need for cross-sectoral cooperation, in particular between government agencies, the private sector and academia, which will synergistically strengthen cyberspace resilience at the national level.

– Further research should be aimed at improving behavioural analysis algorithms and evaluating the effectiveness of Zero Trust Security in specific critical infrastructure sectors. In the long run, this concept will become the basis for global cyber defence standards, which will help minimise threats in the global digital space.

1. National Institute of Standards and Technology (NIST). Zero Trust Architecture: Special Publication 800-207. 2020. 60 c.
2. Kindervag J. No More Chewy Centers: Introducing the Zero Trust Model of Information Security. Forrester Research, 2010. 16 c.
3. Zero Trust Deployment Guide for Microsoft Azure Active Directory. *Microsoft Security Blog*. URL : <https://www.microsoft.com/security/blog/zero-trust-deployment-guide>.
4. Zero Trust Maturity Model. *Cybersecurity & Infrastructure Security Agency (CISA)*. URL : <https://www.cisa.gov/zero-trust-maturity-model>.



Андрій КОРЕНЕВ

доцент кафедри
адміністративно-правових дисциплін
та публічного управління
Дніпровського державного
університету внутрішніх справ
(м. Дніпро, Україна),
кандидат юридичних наук

<https://orcid.org/0000-0001-8611-8998>

**АДМІНІСТРАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ: ВИКЛИКИ
ТА ПЕРСПЕКТИВИ**

Адміністративно-правове забезпечення інформаційної безпеки в Україні є складною системою, яка містить нормативно-правові акти, інституційні механізми та державну політику, спрямовану на захист інформаційного простору країни. Ця система регулює правові відносини, що виникають у сфері створення, обробки, зберігання та поширення інформації, а також протидію кіберзагрозам і дезінформації. Основою правового регулювання сфери інформаційної безпеки є Конституція України, яка закріплює принципи захисту державного суверенітету та територіальної цілісності, а також гарантує свободу слова та доступ до інформації. У ст. 17 Основного закону визначено, що забезпечення інформаційної безпеки є невід'ємною складовою національної безпеки, а ст. 34 передбачає можливість обмеження інформаційних прав громадян у випадках, пов'язаних із загрозою національній безпеці або громадському порядку.

Ключову роль у правовому забезпеченні інформаційної безпеки відіграють спеціальні законодавчі акти, які регулюють цю сферу. Зокрема, Закон України «Про національну безпеку України» встановлює стратегічні засади державної політики у сфері безпеки, включаючи інформаційну безпеку; Закон України «Про інформацію» визначає правові основи інформаційних відносин, регулює доступ до інформації та встановлює механізми її захисту; Закон України «Про доступ до публічної інформації» гарантує громадянам право отримувати інформацію, яка перебуває у розпорядженні державних органів; Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи державної політики у сфері кібербезпеки, регламентує заходи

із запобігання та протидії кіберзлочинності, встановлює основні принципи функціонування національної системи кіберзахисту [1, с. 345–349].

Окрім законодавчих актів, важливу роль у забезпеченні інформаційної безпеки відіграють державні органи, які здійснюють контроль та координацію заходів у цій сфері. Центральним органом державного управління, відповідальним за координацію діяльності у сфері національної безпеки, є Рада національної безпеки і оборони України, яка розробляє та реалізує державну політику в інформаційній сфері. Значну роль відіграє Служба безпеки України, яка займається контррозвідальним захистом у сфері інформаційної безпеки, а також здійснює оперативні заходи щодо виявлення та нейтралізації загроз у кіберпросторі.

Державна служба спеціального зв'язку та захисту інформації України відповідає за технічний захист інформації та безпечне функціонування державних інформаційних ресурсів. Національна поліція України, зокрема підрозділи кіберполіції, здійснює заходи щодо протидії кіберзлочинності та несанкціонованому доступу до інформації [2, с. 65–70]. У 2021 р. в межах Міністерства культури та стратегічних комунікацій України було створено Центр стратегічних комунікацій та інформаційної безпеки, який займається аналізом інформаційного середовища, протидією дезінформації та забезпеченням координації державних органів у сфері стратегічних комунікацій.

Незважаючи на сформовану систему адміністративно-правового регулювання інформаційної безпеки, Україна стикається з низкою викликів, які ускладнюють реалізацію державної політики в цій сфері. Одним із головних викликів є стрімкий розвиток інформаційних технологій, що створює нові загрози для кібербезпеки та інформаційного суверенітету держави. Недостатня адаптація законодавства до сучасних викликів та цифрових загроз може призводити до прогалин у правовому регулюванні та недостатньої ефективності заходів із захисту інформації [3, с. 167–172].

Іншою проблемою є слабка координація між державними органами, відповідальними за інформаційну безпеку. Відсутність єдиної політики, дублювання повноважень і розрізненість дій органів державної влади ускладнюють реалізацію ефективних заходів з управління інформаційною безпекою. Також існує проблема забезпечення балансу між захистом національних інтересів та дотриманням прав людини, зокрема права на свободу вираження поглядів та доступу до інформації. Неправильне або надмірне обмеження доступу до інформації може призводити до порушення демократичних стандартів та викликати суспільний резонанс [4, с. 50–58].

Перспективи розвитку адміністративно-правового регулювання інформаційної безпеки в Україні пов'язані з необхідністю вдосконалення законодавчої бази з урахуванням сучасних загроз і міжнародних стандартів. Важливим напрямом є розробка та впровадження нових законодавчих актів, які б комплексно регулювали відносини у сфері кібербезпеки та інформаційної безпеки. Особливо актуальним є питання гармонізації українського законодавства із законодавством Європейського Союзу та стандартами НАТО, що дозволить ефективніше інтегрувати Україну у світову систему кіберзахисту та інформаційної безпеки.

Посилення інституційної спроможності державних органів у сфері інформаційної безпеки також є необхідним кроком. Це включає запровадження єдиної системи управління інформаційною безпекою, розподіл функцій між органами державної влади, а також забезпечення ефективної взаємодії між ними. Необхідно впровадити прозорі механізми моніторингу та оцінки ефективності заходів у сфері інформаційної безпеки, що дозволить своєчасно виявляти ризики та загрози та оперативно реагувати на них.

Одним із перспективних напрямів є підвищення цифрової грамотності населення та забезпечення належного рівня освіти у сфері кібербезпеки. Це дозволить громадянам та організаціям краще захищати свої інформаційні ресурси та зменшить ризики кібератак. Крім того, необхідно посилити міжнародну співпрацю у сфері інформаційної безпеки, оскільки кіберзагрози мають глобальний характер, і ефективна боротьба з ними потребує спільних зусиль міжнародної спільноти.

Таким чином, для ефективного забезпечення інформаційної безпеки в Україні необхідно здійснити комплекс заходів, спрямованих на вдосконалення адміністративно-правового регулювання, посилення інституційної спроможності державних органів, розширення міжнародної співпраці та підвищення рівня цифрової безпеки громадян. Вирішення цих питань сприятиме зміцненню інформаційного суверенітету держави, створенню ефективної системи кіберзахисту та забезпеченню балансу між національними інтересами та демократичними цінностями у сфері інформаційної безпеки.

1. Бліхар М. М. Адміністративно-правове забезпечення інформаційної безпеки в інтернет-просторі. *Науковий вісник Ужгородського національного університету*. Серія : Право. 2021. № 67. С. 345–349.
2. Олійник О. В. Адміністративно-правові засоби забезпечення інформаційної безпеки. *Юридичний вісник*. 2015. № 1 (34). С. 65–70.
3. Остапенко О., Баїк О. Адміністративно-правова природа інформаційної безпеки. *Вісник Національного університету «Львівська політехніка»*. Серія : Юридичні науки. 2021. № 3 (31). С. 167–172.
4. Баран М. В. Інформаційна безпека як предмет адміністративно-правового регулювання. *Соціально-правові студії*. 2021. № 3 (13). С. 50–58.



Ксенія КОСЯЧЕНКО

доцент кафедри
цивільно-правових дисциплін
ННІ права та інноваційної освіти
Дніпровського державного
університету внутрішніх справ
(м. Дніпро, Україна),
кандидат юридичних наук
<https://orcid.org/0000-0002-1380-218X>

**ДІДЖИТАЛІЗАЦІЯ ПОДАТКОВИХ ПОСЛУГ В УКРАЇНІ:
ВПЛИВ НА АДМІНІСТРУВАННЯ ПОДАТКІВ
ТА ПІДВИЩЕННЯ ПРОЗОРОСТІ**

Податкова система є однією з фундаментальних складових економічної системи будь-якої держави, а її мобільність та відповідність вимогам сучасності виступають невід'ємним фактором зовнішнього розвитку. Діджиталізація податкових послуг являє собою ключовий етап реформування податкової системи України. Впровадження цифрових технологій у сфері адміністрування податків спрямоване на підвищення ефективності роботи державних органів, зменшення бюрократичного навантаження на платників податків та створення прозорих умов для ведення бізнесу. Цифрові інструменти, серед яких електронний кабінет платника податків, автоматизовані системи обліку та електронні звіти, дозволяють не лише полегшити процес податкового адміністрування, але й мінімізувати ризики корупції, сприяючи зростанню рівня довіри до держави. У тезах досліджується вплив діджиталізації на податкове адміністрування в Україні та її роль у підвищенні прозорості фінансових процесів.

Зосереджуючись на темі дослідження, спочатку слід окремо проаналізувати поняття діджиталізації, адміністрування податків та концепцію підвищення прозорості податкових процесів в Україні.

Цифрові технології та цифровізація права, зокрема в Україні, є важливою темою, яка активно обговорюється серед юристів та науковців через значний вплив таких технологій на економічні та суспільні правовідносини. Цей процес охоплює не лише правові аспекти, а й соціальні, економічні та політичні трансформації, пов'язані з використанням новітніх технологій [3, с. 70–71]. Докладніше розглядаючи дефініцію діджиталізації, зазначимо, що це поняття є неологізмом, що увійшов в українську мову відносно нещодавно і є транслітерацією англійського слова «digitalization». Зазначений термін почав активно використовуватися в українській мові протягом останніх десяти років на тлі світового технологічного прогресу. Зростання обсягів використання інформаційних технологій, Інтернету, смартфонів та інших цифрових пристроїв сприяло необхідності впровадження цифрових рішень у сфері державного управління, бізнесу та освіти [1, с. 128].

Офіційне використання терміна набуло популярності після запуску проєкту «Дія» («Держава і я») у 2019 р., метою якого стало спрощення доступу громадян до державних послуг через цифрові платформи [2]. Поняття діджиталізації стало ключовим в контексті реформ, спрямованих на впровадження електронного урядування та цифрової економіки в Україні.

Щодо адміністрування податків, відповідна термінологія чітко окреслена на законодавчому рівні у підпункті 14.1.1-1 п. 14.1.1 ст. 14 Податкового кодексу України: