

УДК 342.95

ЛІСОВСЬКА Ю.П., кандидат юридичних наук.

ORCID: <https://orcid.org/0000-0001-9278-4487>.

## ДИВЕРСИФІКАЦІЯ ЯК КОДИФІКОВАНО-ЦИФРОВА СИСТЕМА АДМІНІСТРАТИВНО-ПРАВОВОГО УПРАВЛІННЯ: МІЖІНФРАСТРУКТУРНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО КАПІТАЛУ

**Анотація.** В статті досліджується диверсифікація як система адміністративно-правового управління в міжгалузевому забезпеченні діджиталізації України, яка розширює семантичний взаємозв'язок права та економіки в сучасному квантово-електронному світі. Показано диверсифікацію в якості правової політики світового порядку, що зумовлена планомерним та креативним взаємозв'язком з метою захисту правових потреб та інтересів особи, держави, а також суспільства. У роботі здійснено аналіз перспектив диверсифікації як кодифікаційно-цифрової системи адміністративно-правового управління в міжінфраструктурі інформаційного капіталу. Висвітленню диверсифікаційного механізму реалізації норм чинного законодавства у сфері захисту критичної інфраструктури і присвячена ця стаття.

**Ключові слова:** диверсифікація, діджиталізація, критична інфраструктура, квант, управління, інформаційний капітал.

**Summary.** The article examines diversification as a system of administrative and legal management in the intersectoral provision of digitalization in Ukraine, which expands the semantic relationship between law and economics in the modern quantum-electronic world. Diversification is shown as a legal policy of the world order, which is due to a planned and creative relationship to protect the legal needs and interests of the individual, the state and society. This paper analyzes the prospects of diversification as a digital codification system of administrative and legal management in the inter-infrastructure of information capital. This article is devoted to highlighting the diversification mechanism for the implementation of current legislation in the field of critical infrastructure protection.

**Keywords:** diversification, digitalization, critical infrastructure, quantum, management, information capital.

**Аннотация.** В статье исследуется диверсификация как система административно-правового управления в межотраслевом обеспечении диджитализации Украины, которая расширяет семантическую взаимосвязь права и экономики в современном квантово-электронном мире. Показана диверсификация в качестве правовой политики мирового порядка, обусловленной планомерной и креативной взаимосвязью с целью защиты правовых потребностей и интересов личности, государства, а также общества. В работе проведен анализ перспектив диверсификации как кодификационно-цифровой системы административно-правового управления в межинфраструктуре информационного капитала. Освещению диверсификационный механизм реализации норм действующего законодательства в сфере защиты критической инфраструктуры и посвящена эта статья.

**Ключевые слова:** диверсификация, диджитализация, критическая инфраструктура, квант, управление, информационный капитал.

**Постановка проблеми.** За сучасних умов актуальною категорією, яка визначає систему адміністративно-правового управління в міжгалузевому забезпеченні діджиталізації України, є диверсифікація. Саме такий якісно новий тренд міжгалузевих відносин як диверсифікація розширює семантичний взаємозв'язок права та економіки в сучасному квантово-електронному світі. При цьому фундаментальною матрицею суспільного життя у кіберпросторі є цифрова економіка як диверсифікаційна система

господарювання. Адже ця система міжгалузево забезпечує ефективне використання обмежених ресурсів, необхідних для задоволення нагальних потреб. Так, категоріальний термін “диверсифікація” як оптимальний спосіб мінімізації корупційних ризиків у сучасному кіберкапіталі використовують у багатьох сферах суспільного життя. Навіть лексико-семантичне тлумачення означеного терміну вказує на його багатоаспектність і поширеність, оскільки, на наш погляд, може бути використано в наступних значеннях: правова політика світового порядку, що зумовлена планомірним та креативним взаємозв’язком; продумана плановість та законність в міжнародній економіці; сукупність господарчих одиниць, міжнародних установ, об’єднаних структурно з метою захисту правових потреб та інтересів особи, держави, а також суспільства.

**Результати аналізу наукових публікацій.** Цієї проблематики торкалися такі вітчизняні дослідники як: О. Бригінець, А. Гриценко, М. Курко, П. Лісовський, М. Недюха, Д. Неліпа, С. Подоляка тощо. Їх фундаментальні праці стали науково-теоретичним підґрунтям вирішення проблемних питань диверсифікації як якісно нового адміністративно-правового управління цифровою економікою.

**Метою статті** є аналіз та визначення перспектив диверсифікації як кодифікаційно-цифрової системи адміністративно-правового управління в міжінфраструктурі інформаційного капіталу.

**Виклад основного матеріалу.** В сучасних умовах цифрової економіки виробництва, розподілу, обміну і споживання матеріальних благ визначаються якісно нові форми адміністративно-правового управління. Своєю чергою, правова форма диверсифікації як надання різнобічного, комбінованого та міжгалузевого характеру оптимізує та поширює виробництво різномірних товарів та надання різних інтелектуальних послуг. Це виявляється у диверсифікації як генеративно-цілісному визначенні правовою державою розміру податків, мінімізації корупційних ризиків, мінімальної заробітної плати, строку відпустки, встановлення правил квантової (радіобіокосмічної), екологічної та техногенної безпеки тощо.

***Диверсифікація як комплексна система суб’єктів управління та координації в міжгалузевих відносинах.***

Із наведеного витікає, що управління містить у собі один із видів діяльності, тобто може бути охарактеризоване як активне, динамічне явище. “Це діяльність суб’єкта, що виявляється в цілеспрямованому, організуючому впливі на об’єкт управління, здійснюваному з метою приведення його в бажаний для суб’єкта стан” [1, с. 8]. Іншими словами, диверсифікація як управлінська діяльність має генеративно-цілісний характер. Тому, саме управління в контексті диверсифікації може бути розглянуто в якості системи із спектром набору відповідних елементів, які визначають міжгалузевість її сутності. Так, Д.Д. Цабрія в своєму монографічному дослідженні “Система управління (державно-правові аспекти)”, систему управління визначає як упорядковану сукупність взаємопов’язаних елементів, які відрізняються функціональними цілями, діють автономно, але спрямовані на досягнення загальної мети” [2, с. 12].

Крім того, щодо дослідження вертифікаційних особливостей організаційно-правових основ управління варто вважати конструктивну думку вченого М.К. Якимчука, що система управління – це передусім структурно-організаційне утворення, що віддзеркалює побудову системи, характеризується складом і підлеглістю його елементів, способом їхнього зв’язку та взаємодії, єдністю елементів, об’єднаних у достатнє число підрозділів [3, с. 90]. Також обґрунтованим є методологічний підхід, згідно з яким система управління містить у собі форму реалізації взаємодії та розвитку

відносин управління, які виражаються в законах і принципах управління, а також у цілях, функціях, структурі, методах і процесі управління [4, с. 25].

З аналізу вищенаведених підходів, сутність системи управління розкривається в силу взаємодії суб'єкта та об'єкта управління, що цілеспрямовано на контроль та координацію певної галузі в суспільних відносинах. З огляду на це, як підкреслює В.М. Момот, між суб'єктом та об'єктом управління можуть встановлюватись субординаційні чи координаційні зв'язки. Адже відносини субординації – це такі відносини між суб'єктами управлінської діяльності, які виражають підпорядкованість одного суб'єкта іншому в процесі управління єдиним об'єктом. У свою чергу, відносини координації мають місце між суб'єктами управлінської діяльності, які не підпорядковані один одному, оскільки для них властивим є узгодження діяльності, поєднання зусиль під час реалізації окремих і загальних цілей [5, с. 106].

Отже, в диверсифікаційному аспекті об'єкт управління необхідно розуміти свідомо спрямований, планомірний, організований, генеративно-цілісний вплив суб'єкта управління.

### ***Диверсифікаційна природа квантових електронних ресурсів щодо кіберзахисту критичної інфраструктури.***

Основа державного управління національною системою кібербезпеки становлять Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, розвідувальні та контррозвідувальні структури, органи прокуратури, Національна поліція України, Національний банк України, паливно-енергетичний комплекс тощо.

На Службу безпеки України покладаються: попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на протидію з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів.

Аналіз положень Стратегії кібербезпеки України свідчить, що найбільш поширеними ризиками, що сприяють деструктивному впливу загроз у кіберсфері, можна вважати недостатній рівень захищеності критичної інфраструктури, безсистемність заходів кіберзахисту критичної інфраструктури, недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів тощо.

Серед основних моментів забезпечення кіберзахисту виділено доцільність таких першочергових заходів: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури та визначення критеріїв належності інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури; впровадження державного реєстру об'єктів критичної інформаційної інфраструктури; розробка вимог до кіберзахисту об'єктів критичної інфраструктури; розробка вимог до кіберзахисту об'єктів критичної інфраструктури; покладання на власників (розпорядників) об'єктів критичної інфраструктури обов'язку створення підрозділів кіберзахисту; зміцнення державно-приватного партнерства у запобіганні та локалізації кіберзагроз та захисту інформації, а також сприяння власниками (розпорядниками) об'єктів критичної інфраструктури державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту; відпрацювання належного механізму обміну інформацією між партнерами з державного та приватного сектору стосовно загроз критичній інформаційній інфраструктурі [6].

Так, координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. При цьому, Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України. Своєю чергою, Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини та громадянина; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури в банківській системі України).

Окремо варто зупинитись на тому, що законодавець дає визначення критично важливим об'єктам інфраструктури. Зокрема, в кіберпросторі під ними необхідно розуміти підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають стратегічне значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, докільля, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей. Крім того, визначено й "об'єкт критичної інформаційної інфраструктури" – це комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака, яка безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [7].

Водночас необхідно визначити, що саме завдяки положенням постанови, міністерствам, іншим центральним органам виконавчої влади разом із Службою безпеки, іншим заінтересованим державним органам передбачено подати пропозиції до переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури в цій сфері [8].

На наш погляд, диверсифікаційний механізм реалізації норм чинного законодавства у сфері захисту критичної інфраструктури вдається посилити завдяки передбаченим завданням щодо підготовки за участю Служби безпеки України законопроекту щодо розмежування кримінальної відповідальності за злочини у сфері використання комп'ютерних систем і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідного розмежування підслідності [9].

### ***Диверсифікація як міжгалузеві нормативно-правові акти трансформації цифрового порядку.***

Трансформація цифрового порядку в часи квантово-електронної епохи, що має ознаки непередбачуваності, є значним фактором впливу, в тому числі й на національну безпеку України та окремих держав. Характер цієї цифрової трансформації є складним та швидкоплинним, що зумовлює зміну загроз, які виникають. Такий стан речей вимагає адекватного реагування, зокрема – постійних змін у державній політиці на законодавчому рівні.

Державне реагування на процеси, що існують в сучасному квантово-електронному світі, стосується перманентного впливу нанотехнологій на суспільство та його інститути. Так, наприклад, в кіберсучасності існують два основні документи концептуальних засад розвитку цифровізації – схвалена розпорядженням Кабінету Міністрів України від 17.01.18 р. № 67-р "Концепція розвитку цифрової економіки та суспільства на 2018 – 2020 роки" і "Цифрова агенда України – 2020". Зазначені документи є досить ґрунтовними,

але їх зміст значною мірою презентує сучасні інформаційні технології, аніж виробляє державну стратегію.

При цьому, використання математичного моделювання за допомогою систем і методів квантової електроніки є перспективним напрямом дослідження, описання та прогнозування, зокрема як окремих агробіопроектів та явищ, такі і агроекологічних систем у цілому. Це є інструментальною основою для подальшого проведення інформаційного моніторингу агроєкосистеми, що сформувалась як диверсифікаційна система спостережень, оцінки та прогнозування станів досліджуваного об'єкта або групи об'єктів з метою прийняття раціональних управлінських рішень. Саме необхідність отримання різнобічних квантово-електронних моделей та застосування їх у агроєкосистемі обумовлена можливістю аналізувати та керувати їх станом, прогнозувати майбутні технології для підтримання ґрунтового покриву в стані, за умов якого зберігається властивість до регуляції циклів біофільних елементів, забезпечення контролю розвитку антропогенних процесів. Так, дослідження, пов'язані з розробкою науково обґрунтованої методології комплексного прогнозу екологічного стану конкретної агроєкологічної системи залежно від рівня антропогенного навантаження та рекомендацій щодо його регламентації на основі знань просторово-часових особливостей цієї системи, дозволяють з упередженням, шляхом системного моделювання складних процесів, визначити оптимальну агротехнологічну електронну карту польових робіт, оцінити наявний та спрогнозувати необхідний рівень екологічної безпеки.

Крім того, саме такі квантово-електронні модулятори як радіодальноміри є перспективними для використання також у нафтогазовій системі з метою мінімізації ризиків щодо ґрунтової поверхні земель, а саме: її аномалій, а також діагностики якості нормоконтролю щодо корозійної стійкості металевих труб. Для цього, значною мірою формують диверсифікаційну систему таких показників контролю та об'єктивних критеріїв, за допомогою яких можна відслідковувати стан та захищати екоенергетичну безпеку. На цьому етапі внаслідок недостатності необхідної інформації та потужної різноманітності явищ, що характеризують трансформацію ґрунтів залежно від комбінацій природних та антропогенних факторів, можуть виникати відповідні перешкоди. Іншими словами, квантова електронна система, що має міжгалузевий характер диверсифікації, дозволяє конструктивно визначити критерії та отримати кількісну оцінку функціонування, спрогнозувати майбутні стани екоенергосистеми, виявити її інші функціональні особливості. Адже квантова електронна система дозволяє моделювати різні можливі ситуації (навіть ситуації функціонування диверсифікаційної системи в екстремально критичних умовах, створених шляхом імітаційного моделювання).

Таке забезпечення аерокосмічного моніторингу поверхні земель за допомогою квантової електроніки дозволяє мобільно та автономно вивчати напрямки, швидкості розвитку ґрунтовних процесів та відтворення родючості ґрунту, оптимізації екологічної ситуації з врахуванням можливих наслідків. При вирішенні означених нагальних проблем необхідно враховувати ґрунтово-кліматичні умови, господарсько-економічні особливості досліджуваної екоенергосистеми, кількісний та якісний стан всіх її складових (ґрунт – рослина – зона аерації – ґрунтові води – атмосфера).

### **Висновки.**

Таким чином, стан диверсифікації як системи адміністративно-правового управління у кіберсфері є стратегічним завданням щодо забезпечення національної безпеки України. У процесі дослідження встановлено, що законодавство із зазначеного питання перебуває ще у стадії створення та становлення, що потребує подальшого удосконалення. Крім того, невизначеними залишаються передбачені ч. 2 ст. 6 Закону

України “Про основні засади забезпечення кібербезпеки України” критерії та порядок зарахування об’єктів до критичної інфраструктури, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, оскільки вони мають бути визначені Кабінетом Міністрів України, а в банківській сфері – Національним банком України.

У цьому відношенні головною метою диверсифікаційної системи керування є механізм управління нанотехнологічними впливами (та їх оптимізація) на природні процеси за умови мінімізації енерго- та ресурсовитрат, збереження довкілля, а також розробка методів прогнозу стану екоенергосистеми та її складових на різних структурних рівнях для оцінки функціонування визначення оптимального комплексу різних заходів, планування розвитку та аналізу післядій управлінських рішень або невиконання рекомендованих заходів.

### Використана література

1. Колпаков В.К. Адміністративне право України. Київ: Юрінком Інтер, 1999. 736 с.
2. Цабрия Д.Д. Система управления (государственно-правовые аспекты). Москва: Юрид. лит, 1990. 271 с.
3. Якимчук М.К. Організаційно-правові основи управління в органах прокуратури України [дисертація]. Чернівці, 2002. 470 с.
4. Долгополова М.М. Управління загальнодержавною системою забезпечення безпеки дорожнього руху: дис. ...канд. юр. наук. – (Запорізький юридичний ін-т МВС України). Харків, 2003. 229 с.
5. Момот В.М. Робота з персоналом в органах та підрозділах державної податкової адміністрації України: теоретичні та організаційно-правові засади: дис. ...канд. юр. наук. Харків: Ун-т внутр. справ, 2006. 204 с.
6. Про Стратегію кібербезпеки України: Указ Президента України “Про уведення в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року” від 15.03.16 р. № 96/2016. *Урядовий кур’єр*. 2016. № 52.
7. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. *Урядовий кур’єр*. 2017. № 215.
8. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави: Постанова Кабінету Міністрів України від 23.08.16 р. № 563. *Урядовий кур’єр*. 2016. № 168.
9. Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації”, введеного в дію Указом Президента України від 13 лютого 2017 р. № 32: Указ Президента України “Про рішення РНБО від 10 липня 2017 р.” від 30.08.17 р. № 254/20177. *Урядовий кур’єр*. 2017. № 162.
10. Лісовська Ю.П. Інформаційна безпека України: навчальний посібник. Київ: Видавничий дім “Кондор”, 2017. 199 с.
11. Лісовська Ю.П. Кібербезпека: ризики та заходи: навчальний посібник. Київ: Вид. дім “Кондор”, 2019. 272 с.
12. Лісовська Ю.П. Правова держава як кіберінфраструктурне забезпечення інформаційного капіталу: монографія. Київ: Міжрегіональна Академія управління персоналом, 2020. 252 с.
13. Литвиненко В.І., Заросило В.О., Лісовська Ю.П. Антикорупційна інфраструктура країн світу: контроль, моніторинг, представництво: навч. посіб. Київ: Видавництво Ліра-К, 2021. 200 с.