УДК 349
DOI 10.33244/2617-4154.4(21).2025.52-60

А. С. Розпаченюк,
аспірант,
Університет митної справи та фінансів
email: rozpachenyukand@gmail.com
ORCID ID 0009-0008-2833-6709

ЕЛЕКТРОННЕ ВРЯДУВАННЯ ТА ПРАВОВІ ГАРАНТІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Сучасна система державного управління України, що базується на використанні інформаційних технологій, перебуває у процесі активного розвитку та вдосконалення. Попри складні умови воєнного стану, постійні обстріли цивільної інфраструктури та численні кіберзагрози, країна зуміла уникнути управлінського колапсу завдяки широкому впровадженню електронного урядування. Електронні адміністративні послуги, зокрема через портал «Дія», забезпечили громадянам доступ до соціальних виплат, реєстрації пошкодженого майна та інших сервісів навіть за умов переміщення органів влади й руйнування інфраструктури.

Метою статті є дослідження правових засад і механізмів забезпечення інформаційної безпеки держави в умовах розвитку електронного врядування, аналіз сучасних тенденцій цифровізації управлінських процесів, визначення ключових гарантій захисту інформаційних ресурсів, окреслення основних ризиків і проблем, а також формулювання напрямів удосконалення законодавства та практики його застосування з урахуванням значення інформаційної культури й етичних стандартів для ефективного функціонування електронного врядування.

Водночас актуальною проблемою залишається недосконаліть законодавчої бази у сфері кібербезпеки: дублювання функцій державних органів, відсутність ефективної координації та спеціалізованих судових процедур. Це ускладнює оперативне реагування на кіберінциденти й взаємодію держави з приватним сектором. Нормативні акти, що регулюють електронне врядування, починаючи з Указу Президента України 2005 року та Концепції розвитку е-урядування, заклали правові основи для прозорості, відкритості та ефективності управління.

Особливого значення набуває інформаційна безпека як складова національної безпеки. Вона розглядається як стан захищеності, комплекс організаційних заходів та постійний процес протидії загрозам. Наукові підходи (Гурковський, Шевчук) акцентують на захисті життєво важливих інтересів громадян і держави, а також на потребі активних заходів інформаційного впливу. У воєнний час питання кіберзахисту та захисту персональних

даних стають критично важливими, адже системи ідентифікації в «Дії» чи банківських додатках підвищують ризики несанкціонованого доступу.

Отже, електронне урядування в Україні поєднує правові, організаційні й технічні механізми, що забезпечують безперервність державного управління, доступність послуг і захист інформаційних ресурсів навіть у надзвичайних умовах, формуючи цілісну систему взаємодії держави та громадян.

Ключові слова: *інформаційна безпека, правове забезпечення інформаційної безпеки, електронне урядування, правові гарантії, діджиталізація управлінських процесів.*

Постановка проблеми. Сучасна система державних органів і застосування інформаційних технологій в управлінській діяльності на рівні держави та органів місцевого самоврядування ще далека від ідеалу. Цьому є підтвердження, й воно зумовлене рядом чинників. Проте потрібно зазначити, що Україна є одним із лідерів побудови належної державної системи електронного врядування навіть у такий складний час – час воєнного стану. Безперечно, постійні обстріли цивільної інфраструктури держави створюють проблеми щодо належного розвитку як технічної сторони системи електронного урядування, так і розвитку окремих елементів у системі державного управління. Але варто зазначити, що саме через широке запровадження елементів надання адміністративних послуг в електронному вигляді вдалось уникнути колапсу в системі державного управління, в наданні адміністративних послуг громадянам, постраждалим унаслідок військової агресії, внутрішньо переміщеним особам та іншим категоріям осіб.

Цілком погоджуємося з думкою О. В. Євсюкової та М. С. Кисельова, що «разом із перевагами цифровізації існують і значні виклики, серед яких – кібербезпека, захист персональних даних, цифрова нерівність серед населення, а також необхідність удосконалення нормативно-правової бази. Подолання цих викликів потребує комплексного підходу, зокрема інвестування в розвиток цифрової інфраструктури, впровадження міжнародних стандартів безпеки та підвищення рівня цифрової грамотності громадян» [6].

Аналіз останніх публікацій. Питання дослідження правових засад і механізмів забезпечення інформаційної безпеки держави в умовах розвитку електронного врядування є предметом активного дослідження вітчизняних науковців, серед яких О. О. Золотар, Н. Б. Новицька, А. М. Новицький, О. В. Євсюкова та М. С. Кисельов.

Метою статті є дослідження правових засад і механізмів забезпечення інформаційної безпеки держави в умовах розвитку електронного врядування, аналіз сучасних тенденцій цифровізації управлінських процесів, визначення ключових гарантій захисту інформаційних ресурсів, окреслення основних ризиків і проблем, а також формулювання напрямів удосконалення законодавства та практики його застосування з урахуванням значення інформаційної культури й етичних стандартів для ефективного функціонування електронного врядування.

Виклад основного матеріалу. Впровадження електронних систем забезпечення державного врядування як загальнодержавної політики надало можливість відкрито вести діалог на рівні громадянина та органів державного управління і місцевого самоврядування. Водночас кібератаки на інформаційно комунікаційні системи державних

органів показали потребу в налагодженні дієвої системи інформаційної безпеки та її нормативно-правового забезпечення.

Практична проблема зумовлена критичними недоліками чинного законодавства України у сфері кібербезпеки, які виявляються в несистемності нормативно-правового регулювання, дублюванні функцій різних державних органів і відсутності ефективних механізмів координації їхньої діяльності. Існуюча правова база не забезпечує адекватного реагування на сучасні кіберзагрози, оперативного обміну інформацією про кіберінциденти та ефективної взаємодії між державним і приватним секторами. Проблеми правозастосовної практики охоплюють недостатню підготовленість правоохоронних органів до розслідування кіберзлочинів, неадекватність санкцій за кіберправопорушення та відсутність спеціалізованих судових процедур для розгляду справ у сфері кібербезпеки [1].

Правовою підставою розвитку електронного врядування в Україні є ряд нормативних документів, що ухвалювалися задля створення належних правових підстав задоволення потреб суспільства й держави в розробці, впровадженні та подальшому вдосконаленні новітніх інформаційних технологій у відносинах держави й громадян.

Ще 2005 року з метою створення належних умов для прискорення економічного та соціального розвитку України, суттєвого поліпшення умов життя людей, забезпечення відкритості й прозорості функціонування органів державної влади та органів місцевого самоврядування, реалізації конституційних прав громадян в інформаційній сфері було ухвалено Указ Президента України, яким передбачалось організацію роботи з надання юридичним та фізичним особам адміністративних послуг на основі використання електронної інформаційної системи «Електронний уряд» [2].

У Концепції розвитку електронного урядування в Україні, зокрема, визначено поняття електронного урядування як форми організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян [3].

Електронне урядування в Україні на сучасному етапі напряму пов’язане із проблематикою, ускладненою воєнним часом, веденням активних бойових дій на території держави, потребою в забезпеченні безперервного, постійного та своєчасного функціонування всіх ланок державного управління. Саме електронне урядування як новітня система надала можливість у складних умовах війни, які зумовили переміщення органів державної влади та місцевого самоврядування на нові місця своєї діяльності за повного або часткового руйнування інфраструктури, обмеження доступу громадян до державних установ та отримання адміністративних послуг, забезпечити реальну державну управлінську функцію, водночас самі державні послуги перейшли на новий рівень і стали більш доступними та ефективнішими.

Застосування електронного урядування у воєнний період дало змогу оперативно ухвалювати управлінські рішення, забезпечивши швидкий обмін інформацією в електронному вигляді, забезпечити електронний документообіг між усіма гілками влади й реально запровадити електронний документообіг у значній частині взаємодії

органів влади та громадян держави. Саме яскравим прикладом взаємодії держави та реальної підтримки громадян у складний час є надання послуг через портал «Дія». Зокрема, надаються послуги щодо соціальних виплат, допомоги внутрішньо переміщеним особам, реєстрації пошкодженого майна, державних виплат підтримки. Усі операції здійснюються в електронному вигляді за допомогою мережі «Інтернет», електронного документообігу та застосування порталу чи мобільного додатка «Дія».

Водночас потрібно розуміти і важливість проведення захисту системи від несанкціонованих, негативних, кібернетичних впливів на роботу інформаційних систем державних органів. На сьогодні питання інформаційної безпеки держави, її інформаційних ресурсів, систем стоїть на такому самому високому рівні, як і загальновійськова безпека держави.

Ряд нормативних актів спрямовано на створення належного правового поля застосування різних інструментів державного впливу на процеси забезпечення інформаційної безпеки та належного функціонування інформаційно-комунікаційних систем. Так, задля належного функціонування системи електронно комунікаційних мереж України, створення належних умов протидії в умовах дії воєнного стану нормативно закріплено положення про те, що Національний центр оперативно-технічного управління електронними комунікаційними мережами України в умовах надзвичайного або воєнного стану видає розпорядження щодо оперативно-технічного управління електронними комунікаційними мережами, які є обов'язковими для виконання постачальниками електронних комунікаційних мереж та/або послуг. Під час дії воєнного стану на підставі звернення регуляторний орган може ухвалити рішення про вилучення з реєстру постачальників електронних комунікаційних мереж і послуг тих постачальників, які не виконали розпорядження. У такому разі припиняється обмін інформацією з мережами суб'єкта господарювання, якого вилучено з реєстру постачальників електронних комунікаційних мереж і послуг [4].

Досліджуючи поняття інформаційної безпеки як правового інституту в загальній системі права України, варто зазначити про те, що це поняття трактується із різним підходом як вченими, так і законодавцем.

Так, В. Гурковський, аналізуючи поняття «інформаційна безпека», визначає інформаційну безпеку як суспільні відносини, пов'язані із захищеністю життєво важливих інтересів людини й громадянина, суспільства та держави від реальних і потенційних загроз в інформаційному просторі, що є важливою умовою збереження й примноження духовних і матеріальних цінностей державотворчої нації, її існування, самозбереження та прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантування, охорони, захисту і відстоювання її національних інтересів [7].

В. Шатун та О. Гладун трактують інформаційну безпеку як стан забезпечення захищеності національних інтересів України у сфері інформації від загроз, що можуть виникати для особи, суспільства та держави. До таких загроз вони відносять неповноту чи несвоєчасність інформації, її несанкціоноване поширення та використання, деструктивний інформаційний вплив, а також негативні наслідки функціонування інформаційних технологій [9, с. 175].

Проаналізувавши різні підходи до визначення категорії «інформаційна безпека», які дають змогу комплексно та системно зрозуміти це явище, М. О. Шевчук пропонує розглядати інформаційну безпеку як перманентний процес діяльності компетентних органів, спрямований на запобігання та протидію загрозам в інформаційній сфері через застосування активних заходів інформаційного впливу, а також сукупність умов для такої діяльності, що може реалізовуватися та контролюватися впродовж тривалого часу. Інформаційна безпека як ключова складова національної безпеки, на його думку, містить такі пріоритетні напрями: забезпечення захисту інформаційного простору та забезпечення безпеки культурного генофонду людства в умовах глобалізації [8].

Звертаючись до нормативного осмислення категорії «інформаційна безпека», потрібно констатувати, що чинне законодавство України не містить її розгорнутого дефінітивного визначення. Водночас нормативно-правові акти, які регламентують сферу інформаційної безпеки, послідовно інтерпретують її крізь призму ширшої концепції національної безпеки, розглядаючи як органічну складову останньої.

Таблиця 1

Постанова Кабінету Міністрів України «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури»	Інформаційна безпека – це стан захищеності, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та/або технологічних систем, конфіденційність, цілісність і доступність електронних інформаційних ресурсів, а також забезпечується своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз штатного режиму функціонування таких систем і ресурсів, несанкціонованого втручання в їх роботу
Закон України «Про основні засади забезпечення кібербезпеки України»	Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі; кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на захист від кіберзагроз, забезпечення кібербезпеки, стійкості, цілісності, доступності та конфіденційності інформаційних ресурсів у кіберпросторі, а також здатності інфраструктури до їх обробки
Закон України «Про інформацію»	Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї
Закон України «Про захист інформації в інформаційно-комунікаційних системах»	Захист інформації в системі – діяльність, спрямована на запобігання порушенню цілісності, конфіденційності й доступності інформації в системі

Продовження таблиці 1

Закон України «Про електронні комунікації»	Безпека мереж і послуг – здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, що надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги
Постанова Національного банку України «Про затвердження Положення про захист інформації та кіберзахист учасниками платіжного ринку»	Інформаційна безпека – збереження конфіденційності, цілісності та доступності інформації
Постанова Національного банку України «Про затвердження Положення про вимоги до системи управління кредитною спілкою»	Інформаційна безпека – комплекс організаційних заходів кредитної спілки, програмних і техніко-технологічних засобів, що функціонують на всіх організаційних рівнях кредитної спілки та забезпечують захист інформації від випадкових та/або навмисних загроз, наслідком реалізації яких може стати порушення доступності, цілісності, конфіденційності інформації щодо діяльності кредитної спілки або її клієнтів
Постанова Національного банку України «Про затвердження Положення про організацію системи внутрішнього контролю в банках України та банківських групах»	Інформаційна безпека – комплекс організаційних заходів банку, програмних і техніко-технологічних засобів, що функціонують на всіх організаційних рівнях банку та забезпечують захист інформації від випадкових та/або навмисних загроз, наслідком реалізації яких може стати порушення доступності, цілісності, конфіденційності інформації щодо діяльності банку або його клієнтів
Проєкт Закону України від 28.05.2014 № 4949 «Про засади інформаційної безпеки України»	Інформаційна безпека –- стан захищеності життєво важливих інтересів людини й громадянина, суспільства та держави, у разі якого запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій

Водночас у Законі України «Про захист інформації в інформаційно-комунікаційних системах» визначено, що державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, у системах, об'єктах критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, мають оброблятися в авторизованих системах з безпеки або через отримання сертифіката відповідності стандарту інформаційної безпеки, виданого органом з оцінки відповідності [5].

Висновки. Отже, у нормативних актах інформаційна безпека розглядається як стан захищеності, як комплекс організаційних заходів, як збереження конфіденційності, як діяльність, як здатність протистояти діям, що становлять загрозу.

У поєднанні із загальними вимогами, що ставляться до державних органів та органів місцевого самоврядування в питаннях дотримання інформаційної безпеки під час здійснення своєї діяльності, бачимо значне зростання державних послуг, що надаються в електронному вигляді.

У сфері електронного врядування окремим питанням стоїть особливість ідентифікації особи та захист персональних даних. У додатку «Дія», «Резерв», у банківських інтернет-додатках задіяні системи ідентифікації особи та підтверджені документи в електронній формі. Це підвищує ризик щодо доступу до такої інформації та відповідно до несанкціонованого доступу до персональних даних.

Підсумовуючи, потрібно зазначити, що в Україні сформовано правову базу щодо забезпечення електронного урядування та належної інформаційної безпеки, кібербезпеки й захисту інформації. У поєднанні із адміністративними заходами, управлінськими рішеннями створюють цілісну систему забезпечення громадян держави відповідними адміністративними послугами за допомогою інтернет, належні умови діяльності всіх гілок влади в державі навіть у складних умовах воєнного стану, забезпечують оперативне прийняття рішень на всіх рівнях задля забезпечення потреб населення, створюють спрощені або спеціальні процедури отримання електронних державних послуг.

Крім того, державні інформаційні ресурси є основними джерелами надання достовірної інформації, джерелом отримання кризових повідомлень (наприклад, повідомлень про повітряну тривогу), основним засобом формування інформаційної стійкості суспільства до загроз, формування національної системи інформаційної безпеки держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мазепа С. Кібербезпека в Україні: сучасні виклики та шляхи вдосконалення законодавчого регулювання. *Актуальні проблеми правознавства.* 2025. № 2 (42). С. 164–171.

2. Про першочергові завдання щодо впровадження новітніх інформаційних технологій : Указ Президента України від 20 жовтня 2005 року № 1497/2005. URL : https://zakon.rada.gov.ua/laws/show/1497/2005#Text

3. Про схвалення Концепції розвитку електронного урядування в Україні : розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. URL : https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text

4. Про внесення змін до Закону України «Про електронні комунікації» щодо підвищення ефективності організації роботи постачальників електронних комунікаційних мереж та/або послуг в умовах воєнного стану : Закон України 3 травня 2022 року № 2240-IX. URL : https://zakon.rada.gov.ua/laws/show/2240-20#Text

5. Про захист інформації в інформаційно-комунікаційних системах : Закон України 5 липня 1994 року № 80/94-ВР, в редакції від 20.04.2025. URL : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

6. Євсюкова О. В., Кисельов М. С. Механізми надання публічних послуг у цифровій державі: виклики та перспективи. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Публічне управління та адміністрування.* 2025. Том 36 (75), № 1. С. 63–70.

7. Гурковський В. І. Безпека як об'єкт правовідносин в умовах глобального інформаційного суспільства. *Правова інформатика*. 2010. № 2 (26). С. 72–77.

8. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського університету. Серія: Право* / голов. ред. Ю. М. Бисага. Ужгород, 2023. Т. 2, вип. 78. С. 134–139. Бібліогр. : с. 139 (8 назв). URL : http://visnyk-pravo.uzhnu.edu.ua/article/view/285994/280058

9. Шатун В. Т. Інформаційна безпека – невід'ємна складова національної безпеки України. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія».* 2016. Т. 267, вип. 255. С. 174–180.

REFERENCES

1. Mazepa S. Kiberbezpeka v Ukraini: suchasni vyklyky ta shliakhy vdoskonalennia zakonodavchoho rehuliuvannia. *Aktualni problemy pravoznavstva.* 2025. № 2 (42). S. 164–171.

2. Pro pershocherhovi zavdannia shchodo vprovadzhennia novitnikh informatsiinykh tekhnolohii : Ukaz Prezydenta Ukrainy vid 20 zhovtnia 2005 roku № 1497/2005. URL : https://zakon.rada.gov.ua/laws/show/1497/2005#Text

3. Pro skhvalennia Kontseptsii rozvytku elektronnoho uriaduvannia v Ukraini : rozporiadzhennia Kabinetu Ministriv Ukrainy vid 20 veresnia 2017 r. № 649-r. URL : https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text

4. Pro vnesennia zmin do Zakonu Ukrainy "Pro elektronni komunikatsii" shchodo pidvyshchennia efektyvnosti orhanizatsii roboty postachalnykiv elektronnykh komunikatsiinykh merezh ta/abo posluh v umovakh voiennoho stanu : Zakon Ukrainy 3 travnia 2022 roku № 2240-IX. URL : https://zakon.rada.gov.ua/laws/show/2240-20#Text

5. Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh : Zakon Ukrainy 5 lypnia 1994 roku № 80/94-VR, v redaktsii vid 20.04.2025. URL : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

6. Ievsiukova O. V., Kyselov M. S. Mekhanizmy nadannia publichnykh posluh u tsyfrovii derzhavi: vyklyky ta perspektyvy. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia : Publichne upravlinnia ta administruvannia.* 2025. Tom 36 (75). № 1. S. 63–70.

7. Hurkovskyi V. I. Bezpeka yak obiekt pravovidnosyn v umovakh hlobalnoho informatsiinoho suspilstva. *Pravova informatyka.* 2010. № 2 (26). S. 72–77.

8. Shevchuk M. O. Do pytannia henezy poniattia informatsiinoi bezpeky yak skladovoi natsionalnoi bezpeky. *Naukovyi visnyk Uzhhorodskoho universytetu. Seriia: Pravo* / holov. red. Yu. M. Bysaha. Uzhhorod, 2023. T. 2, vyp. 78. S. 134–139. Bibliohr. : s. 139 (8 nazv). URL : http://visnyk-pravo.uzhnu.edu.ua/article/view/285994/280058

9. Shatun V. T. Informatsiina bezpeka – nevidiemna skladova natsionalnoi bezpeky Ukrainy. *Naukovi pratsi Chornomorskoho derzhavnoho universytetu imeni Petra Mohyly kompleksu «Kyievo-Mohylianska akademiia».* 2016. T. 267, vyp. 255. S. 174–180.

A. S. Rozpachenuk. E-GOVERNANCE AND LEGAL GUARANTEES OF STATE INFORMATION SECURITY

The modern system of public administration in Ukraine, based on the use of information technologies, is in the process of active development and improvement. Despite the difficult conditions of martial law, constant shelling of civilian infrastructure, and numerous cyber threats, the country has managed to avoid administrative collapse thanks to the widespread implementation of e-governance. Electronic administrative services, particularly through the "Diia" portal, have ensured citizens' access to social benefits, registration of damaged property, and other services even under conditions of relocation of government bodies and destruction of infrastructure.

The purpose of the article is to study the legal foundations and mechanisms for ensuring state information security in the context of e-governance development, to analyze current trends in the digitalization of administrative processes, to identify key guarantees for the protection of information resources, to outline major risks and problems, and to formulate directions for improving legislation and its application, taking into account the importance of information culture and ethical standards for the effective functioning of e-governance.

At the same time, an urgent problem remains the imperfection of the legislative framework in the field of cybersecurity: duplication of functions among state bodies, lack of effective coordination, and absence of specialized judicial procedures. This complicates prompt responses to cyber incidents and the interaction between the state and the private sector. Regulatory acts governing e-governance, starting with the Presidential Decree of 2005 and the Concept of e-governance development, laid the legal foundations for transparency, openness, and efficiency of public administration.

Information security acquires particular importance as a component of national security. It is considered as a state of protection, a set of organizational measures, and a continuous process of countering threats. Scholarly approaches (Gurkovskyi, Shevchuk) emphasize the protection of vital interests of citizens and the state, as well as the necessity of active measures of informational influence. In wartime, issues of cyber defense and protection of personal data become critically important, since identification systems in "Diia" or banking applications increase the risks of unauthorized access.

Thus, e-governance in Ukraine combines legal, organizational, and technical mechanisms that ensure the continuity of public administration, accessibility of services, and protection of information resources even under extraordinary conditions, forming a holistic system of interaction between the state and its citizens.

Keywords: *information security, legal support of information security, e-governance, legal guarantees, digitalization of administrative processes.*

Стаття надійшла до редколегії 7 листопада 2025 року