ВІННИЦЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ МИХАЙЛА КОЦЮБИНСЬКОГО

ФАКУЛЬТЕТ ПРАВА, ПУБЛІЧНОГО УПРАВЛІННЯ І МЕНЕДЖМЕНТУ

КАФЕДРА ПУБЛІЧНОГО УПРАВЛІННЯ ТА МЕНЕДЖМЕНТУ

КВАЛІФІКАЦІЙНА РОБОТА
на тему: **«ЕЛЕКТРОННЕ ВРЯДУВАННЯ В УМОВАХ ВОЕННОГО СТАНУ: ВИКЛИКИ ЦИФРОВОЇ БЕЗПЕКИ ТА ДОСТУПНОСТІ ПОСЛУГ»**

Здобувачки 4 курсу 4АПУА групи
Освітньої програми Публічне управління та адміністрування
Спеціальності 281 Публічне управління та адміністрування
Галузі знань 28 Публічне управління та адміністрування
Ступеня вищої освіти Бакалавр

Закрицької Вікторії Дмитрівни

Науковий керівник **Кононенко В.В.**,
завідувач кафедри публічного управління та менеджменту, доктор історичних наук, професор

Розширена шкала_____
Кількість балів: _____ Оцінка: ECTS _____
Голова комісії _____ _____
(підпис) (ініціали, прізвище)
Члени комісії _____ _____
(підпис) (ініціали, прізвище)
_____ _____
(підпис) (ініціали, прізвище)
_____ _____
(підпис) (ініціали, прізвище)

м. Вінниця 2026

АНОТАЦІЯ

Закрицька В.Д. Електронне врядування в умовах воєнного стану: виклики цифрової безпеки та доступності послуг. Спеціальність 281 «Публічне управління та адміністрування». – Вінницький державний педагогічний університет імені Михайла Коцюбинського, Вінниця, 2026.

У кваліфікаційній роботі досліджено особливості функціонування електронного врядування в умовах воєнного стану, а також основні виклики у сфері цифрової безпеки та доступності адміністративних послуг. Проаналізовано теоретичні засади електронного врядування, нормативно-правове забезпечення цифрової трансформації держави та особливості діяльності органів публічної влади в умовах війни.

Визначено основні проблеми функціонування електронного врядування в умовах повномасштабного вторгнення, серед яких: кібератаки на державні інформаційні ресурси, ризики витоку персональних даних, руйнування цифрової інфраструктури, обмеження доступу до державних реєстрів та нестабільний доступ до мережі Інтернет. Досліджено поняття кіберзагроз, кібератак та кібербезпеки, а також основні види цифрових загроз, що виникають у сучасних умовах.

Окрему увагу приділено питанням захисту персональних даних та правовим механізмам забезпечення інформаційної безпеки. Проаналізовано нормативно-правові акти України у сфері електронного врядування, захисту інформації, електронних комунікацій та функціонування державних реєстрів в умовах воєнного стану.

У роботі досліджено особливості надання адміністративних послуг під час війни та роль цифрових платформ у забезпеченні безперервності взаємодії громадян із державою. Визначено значення порталу та застосунку Дія у процесі цифровізації державних послуг, забезпеченні доступу до документів, соціальних виплат та адміністративних сервісів. Також проаналізовано значення відкритих даних та електронної системи публічних закупівель

Prozorro як інструментів підвищення прозорості діяльності органів влади та запобігання корупції.

За результатами дослідження встановлено, що електронне врядування в умовах воєнного стану стало важливим елементом забезпечення функціонування держави та надання адміністративних послуг громадянам. Обґрунтовано необхідність подальшого вдосконалення системи кіберзахисту, нормативно-правового регулювання та механізмів захисту персональних даних в умовах цифрової трансформації держави.

Ключові слова: електронне врядування, воєнний стан, кібербезпека, цифрова безпека, адміністративні послуги, персональні дані, діджиталізація.

Zakrytska V.D. *Electronic Governance under Martial Law: Challenges of Digital Security and Accessibility of Services*. Specialty 281 “Public Administration and Management”. – Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, 2026.

The qualification paper examines the peculiarities of electronic governance functioning under martial law, as well as the main challenges in the field of digital security and accessibility of administrative services. The theoretical foundations of electronic governance, the legal framework of the state digital transformation, and the peculiarities of public authorities’ activities during wartime are analyzed.

The study identifies the main problems of electronic governance during the full-scale invasion, including cyberattacks on state information resources, risks of personal data leakage, destruction of digital infrastructure, restrictions on access to state registers, and unstable Internet access. The concepts of cyber threats, cyberattacks, and cybersecurity are explored, along with the main types of digital threats emerging in modern conditions.

Particular attention is paid to the protection of personal data and legal mechanisms for ensuring information security. The paper analyzes Ukrainian legal

acts in the field of electronic governance, information protection, electronic communications, and the functioning of state registers under martial law.

The research also examines the peculiarities of administrative service delivery during the war and the role of digital platforms in ensuring continuous interaction between citizens and the state. The importance of the Diia portal and application in the digitalization of public services, access to documents, social payments, and administrative services is determined. The significance of open data and the electronic public procurement system Prozorro as tools for increasing transparency and preventing corruption is also analyzed.

The research findings show that electronic governance under martial law has become an important element in ensuring the functioning of the state and providing administrative services to citizens. The necessity of further improvement of cybersecurity systems, legal regulation, and mechanisms for personal data protection in the context of state digital transformation is substantiated.

Keywords: electronic governance, martial law, cybersecurity, digital security, administrative services, personal data, digitalization.

ЗМІСТ

ВСТУП

Сучасний розвиток інформаційно-комунікаційних технологій призвів до швидкої цифрової трансформації державного сектору та формування нової моделі взаємодії між громадянами, бізнесом та державою. У мирний час електронні сервіси підвищують ефективність державного управління, забезпечують оперативність надання послуг та прозорість державних процесів. Однак в умовах воєнного стану роль електронного урядування зростає: воно стає не лише інструментом комунікації та надання послуг, а й критично важливим елементом безпеки, стабільності та функціонування держави.

Актуальність теми визначається кількома ключовими факторами. По-перше, повномасштабна війна спричинила безпрецедентне зростання кількості кібератак на державні реєстри, критичну інфраструктуру та електронні сервіси. Це вимагає комплексного аналізу сучасних підходів до цифрової безпеки та оцінки їх ефективності в умовах постійних загроз. По-друге, необхідність безперервного доступу громадян до державних послуг у період масового переміщення населення, руйнування інфраструктури та обмежених можливостей фізичного контакту з органами влади вимагає гнучкості та стабільності цифрових платформ. По-третє, розвиток електронного урядування в Україні під час війни став прикладом унікального міжнародного досвіду, що поєднує інновації, ефективність та безпеку рішень, що потребують наукового осмислення.

Стан розробки наукової проблеми свідчить про значний інтерес до питань цифровізації державного управління. Теоретичні основи електронного урядування закладені в роботах таких дослідників, як М. Мескон, Т. Девенпорт, Г. Лінч, які досліджували цифрові моделі адміністративних процесів. Українські вчені – А. Семенченко, В. Брижко, Ю. Канигін, В. Фурашев – приділяли увагу питанням правового забезпечення, цифрової безпеки та організації державних електронних послуг. Питаннями

функціонування е-врядування під час воєнного стану цікавились: Горун О., Дармостук Д., Дівак А., Зайцев М., Демченко Р. В., Володченков О., Кононенко В. В., Ковальчук В., та багато інших науковців. Це свідчить про високу актуальність та важливість теми.

Теоретична значущість дослідження полягає в поглибленні розуміння сутності електронного урядування як адаптивної системи, здатної функціонувати в надзвичайних ситуаціях та збройних конфліктах. Практична значущість полягає в можливості використання отриманих результатів для вдосконалення цифрової політики України, посилення кіберстійкості державного сектору та підвищення доступності електронних послуг для населення в умовах воєнного стану.

Причинами вибору теми стали сучасні виклики цифрової безпеки, необхідність забезпечення безперервності державних електронних послуг та необхідність їх адаптації до нових умов функціонування держави. Вихідними даними були нормативно-правові акти України, статистичні дані органів державної влади, аналітичні матеріали з питань кібербезпеки та міжнародні звіти про цифрову стійкість країн, які пережили воєнні або кризові ситуації.

Метою дослідження є комплексний аналіз особливостей функціонування електронного урядування в Україні в умовах воєнного стану та визначення ключових викликів цифрової безпеки і забезпечення доступності електронних послуг.

Для досягнення мети були поставленні такі завдання:

- дослідити особливості електронного врядування в контексті функціонування держави в кризових та воєнних умовах;
- охарактеризувати нормативно-правове забезпечення електронного урядування в Україні в умовах воєнного стану;
- визначити основні види кіберзагроз для електронного врядування в умовах воєнного стану;

- встановити типові механізми захисту персональних даних в системах е-урядування;
- визначити проблеми та бар'єри для доступності адміністративних послуг для громадян під час воєнного часу;
- знайти рішення для підвищення доступності адміністративних послуг в умовах воєнного стану;
- розробити рекомендації щодо вдосконалення систем електронного врядування врядування.

Об'єктом дослідження є система електронного урядування України.

Предметом дослідження є особливості забезпечення цифрової безпеки та доступності електронних сервісів в умовах воєнного стану.

Методи дослідження базуються на використанні загальнонаукових (аналіз, синтез, узагальнення, класифікація, порівняння), теоретичних (структурно-функціональний, системний, історико-логічний методи), емпіричних (вивчення документів, статистичний та порівняльний аналіз) та спеціальних методів, зокрема системного аналізу, моделювання, методу експертної оцінки. Їх застосування забезпечило всебічність та об'єктивність отриманих результатів.

Практичне значення роботи полягає в можливості впровадження сформованих рекомендацій у діяльність органів державної влади та місцевого самоврядування, що сприятиме підвищенню кіберстійкості державних електронних систем та покращенню доступності цифрових послуг в умовах війни та інших криз.

Апробація матеріалів роботи:

- Закрицька В. Д., Кононенко В. В. Електронне врядування як інструмент підвищення рівня прозорості діяльності органів державної влади. Наука і молодь у XXI сторіччі : Зб. матеріалів конф., м. Полтава, 10 листоп. 2025 р. Полтава, 2025. С. 621–623.

- Закрицька В., Лазор О. Криза довіри до органів державної влади: як ефективна комунікація допомагає її подолати. *Розбудова доброчесності та комплаєнсу в Україні: виклики і перспективи євроінтеграції* : Зб. матеріалів Всеукр. конф. з міжнар. участю, м. Вінниця, 27 берез. 2025 р. Вінниця, 2025. С. 89–90.

Структура роботи: кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел. Робота містить таблиці та діаграми. Загальний обсяг роботи 73 сторінок.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ЗАСАДИ ФУНКЦІОНУВАННЯ ЕЛЕКТРОННОГО ВРЯДУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ

1.1. Особливості електронного врядування в умовах воєнного стану

Під час кризових ситуацій, а особливо під час воєнного стану, електронне врядування має велике значення для будь-якої держави. Адже як і в надзвичайних ситуаціях, так і в мирний час органи публічної влади мають оперативно реагувати на зміни «клімату» в державі, мають налагодити ефективну систему комунікацій з громадянами, доступ до достовірної публічної інформації та можливість для населення отримувати усі адміністративні послуги в повному обсязі, швидко та зручно [47, с.42]. Для України, яка перебуває в режимі воєнного стану, електронне врядування стало не лише інструментом покращення сервісів, а й елементом національної безпеки та стійкості державного управління.

Термін електронне врядування закріплений в декількох нормативно-правових актах. Так Концепція розвитку електронного врядування в Україні дає таке визначення: «Електронне урядування – форма 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» [77]. Також термін електронне врядування досліджував науковець Фурашев В. М. За його словами визначення словосполучення «електронне урядування”, яке надане у Концепції розвитку електронного урядування в Україні від 13 грудня 2010р. (таке ж саме визначення дає Концепція розвитку електронного врядування від 20 вересня 2017), в цілому, відповідає його сутності, але де з чим він не погоджується. А саме із визначенням основного завдання електронного врядування «формування нового типу держави». На

думку автора зміна форми та засобів здійснення державного управління, здійснення «спілкування» владних структур між собою та з населенням країни зовсім не означає зміну типу держави. Натомість пропонує наступне визначення: «Електронне урядування – форма організації державного управління, яка забезпечує підвищення ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-комунікаційних технологій, яка спрямована на максимально просте і доступне спілкування з ними фізичних та юридичних осіб, неурядових організацій та формування інформаційного суспільства» [94, с.48]. На нашу думку, термін електронне врядування доволі динамічний, тому єдино правильного визначення на усі часи не може бути, адже ІТ сфера завжди розвивається і пропонує нові способи взаємодії органів державної влади із народом.

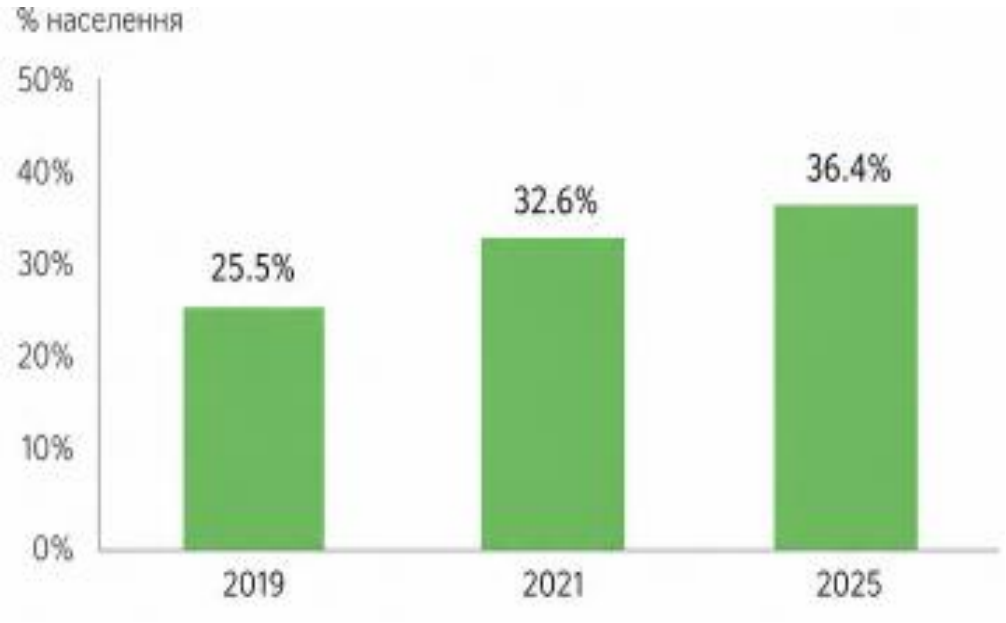
На думку науковиці Сорокіної А. стійкий державний сектор характеризується його здатністю боротися із кризовими ситуаціями, тобто мінімізацією зупинки надання державних послуг, здатністю пристосовуватись та відновлюватись [85, с.25]. І саме використання електронних сервісів забезпечує гнучкість ефективне використання державних ресурсів та оперативність управлінських дій під час шокового стану.

Після повномасштабного вторгнення електронне урядування зіткнулося із багатьма проблемами: зруйнування інфраструктури, нестабільне підключення до інтернету, ризики викрадення персональних даних громадян та кібератаки на державні ресурси, не достатнє правове регулювання.

Також є актуальною проблема цифрової грамотності населення. Велика частина громадян, переважно люди похилого віку, не володіють базовими навичками користування онлайн-ресурсами. Проте, якщо проаналізувати статистичні дані Мінцифри та «Дія.Освіта», рівень цифрової грамотності в Україні в порівнянні з 2019 роком значно зріс (діаграма 1.1. та 1.2.).

Діаграма 1.1.

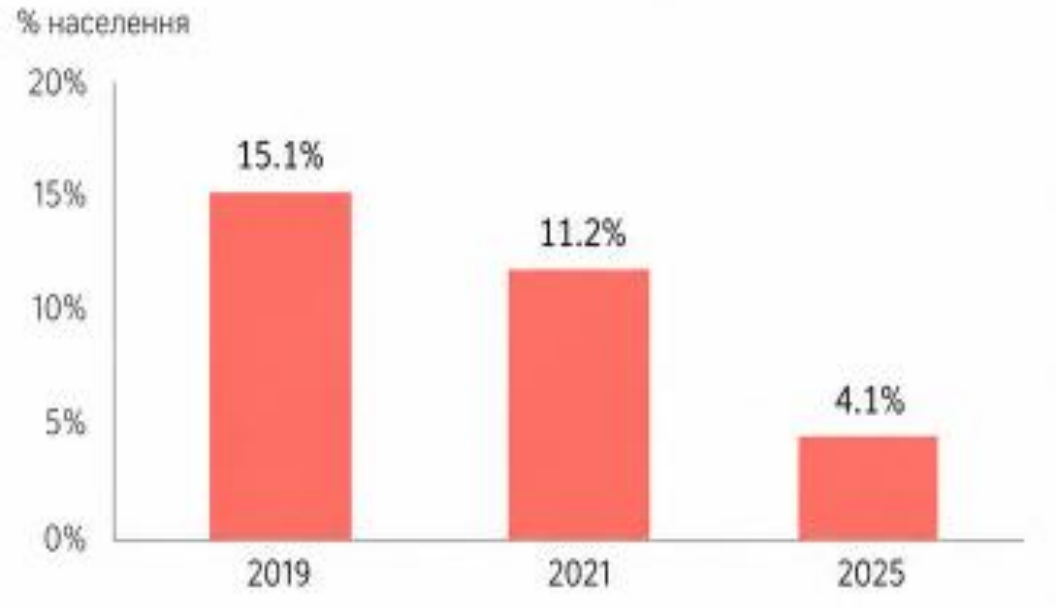
Рівень володіння цифровими навичками вище середнього



Діаграма сформована на основі джерел: [40], [41], [42].

Діаграма 1.2.

Відсоток населення без цифрових навичок

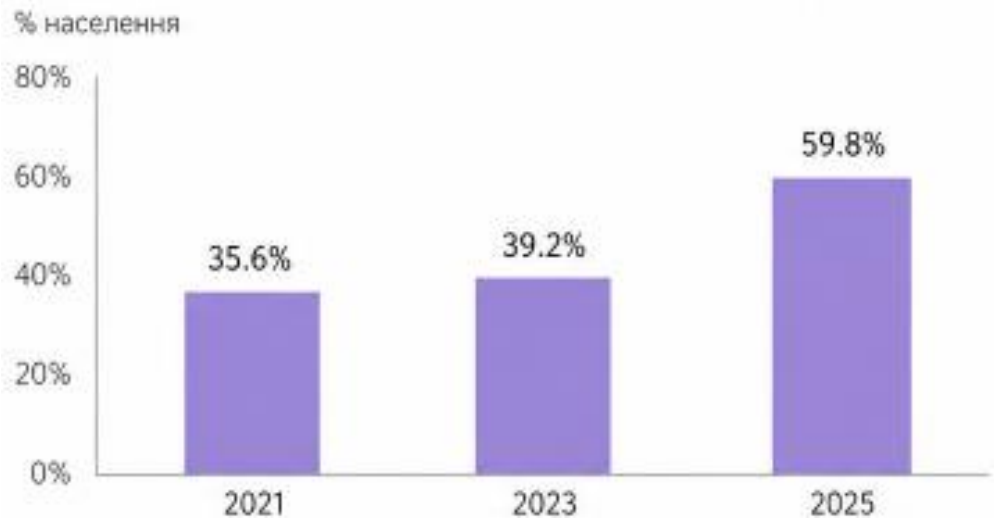


Діаграма сформована на основі джерел: [40], [41], [42].

Також важливим для нашого дослідження є показник досвіду користування державними онлайн послугами (діаграма 1.3.).

Діаграма 1.3.

Динаміка користування державними онлайн послугами



Діаграма сформована на основі джерел: [40], [41], [42]

З огляду на вище наведені дані можна сказати, що воєнний стан вплинув на рівень цифрової грамотності населення України. Тому що, в умовах, які склались люди змушені були навчитись користуватись онлайн ресурсами для того, щоб отримати ту чи іншу послугу. Оскільки електронні сервіси працюють навіть під час повітряних тривог, що не можна сказати про фізичні устнови.

Щодо проблеми кібербезпеки, то для уникнення кібератак на державні реєстри та вебресурси, було прийнято рішення обмежити до них доступ.

Основні обмеження стосувалися:

- державних реєстрів; доступ до Єдиного державного реєстру (ЄДР) та Державного реєстру речових прав на нерухоме майно було суттєво обмежено. Це ускладнило виконання багатьох адміністративних і юридичних процедур, зокрема операцій на ринку нерухомості;
- веб-сайтів державних органів; деякі офіційні веб ресурси, наприклад, сайт Державної казначейської служби, були тимчасово закриті або функціонували з обмеженнями для захисту даних;
- реєстру судових рішень; доступ до Єдиного державного реєстру судових рішень було закрито для загального доступу 24 лютого 2022 року

задля захисту інформації від потенційних кібератак і приховування чутливих даних [24, с.218].

На думку М. Сливки, надання якісних та зрозумілих електронних адміністративних послуг має значну кількість переваг:

- скорочення випадків зловживання своїм становищем службовими особами;
- зменшення затрати часу на подання документів та написання заяв; швидкий доступ до актуальної інформації щодо необхідної адміністративної послуги;
- забезпечення умов для розвитку бізнесу;
- відсутність спілкування зі службовою особою та перебування у відповідних державних органах, оскільки в період карантину це є актуальним та зменшує кількість інфікованих осіб;
- прозорість та швидкість оплати адміністративних послуг [83, с.197].

Публікація вийшла у 2021 році, коли існували карантинні обмеження, але і під час воєнного стану ці переваги є актуальними. Наприклад, скорочення випадків зловживання службовим становищем є дуже важливим у наш час, оскільки корупційні ризики можуть зростати через спрощені або надзвичайні процедури. Автоматизація процесів і мінімізація людського чинника сприяють підвищенню доброчесності управлінських рішень.

Також важливо зменшити витрат часу на подання документів та оформлення заяв, особливо для ВПО, військовослужбовців, волонтерів та громадян, які перебувають за кордоном.

Вагомою перевагою є і швидкий доступ до актуальної інформації щодо адміністративних послуг. В умовах постійних змін законодавства та процедур, які властиві для воєнного стану, важливо швидко інформувати громадян.

Особливо важливо зменшити кількість особистого спілкування з посадовими особами та відвідування державних органів з міркувань безпеки,

оскільки це зменшує скупчення людей у потенційно небезпечних місцях, з огляду на постійні ворожі атаки.

В умовах воєнного стану діджиталізація з амбітної реформи стала життєвою необхідністю. Уряд України спрямував цифрові проєкти на підтримку обороноздатності та забезпечення базових потреб населення. Додаток «Дія» став одним із ключових інструментів, що надав громадянам можливість отримувати важливі послуги навіть під обстрілами та у вимушеній евакуації. Від подання заявки на допомогу внутрішньо переміщеним особам до оформлення документів та доступу до електронних сервісів [27, с. 46]. На сьогодні за даними Мінцифри додатком «Дія» користуються 23,7 млн українців, де доступні 33 цифрові документи та 242 послуги [56].

Також були розгорнуті та посилені цифрові системи для управління надзвичайними ситуаціями, координації гуманітарної допомоги та обліку пошкодженої інфраструктури. Завдяки хмарним технологіям значну частину державних реєстрів вдалося зберегти та захистити від ворожих кібератак, забезпечивши цілісність даних та безперебійність роботи [27, с.46].

Особливої уваги потребує проблема корупції як в мирний час так і в умовах війни. Для України це питання є болючим.

Рівень корупції можна прослідкувати за допомогою міжнародних показників, таких як от Індекс сприйняття корупції (Corruption Perceptions Index, CPI) від Transparency International. Він формується на основі оцінок міжнародних установ та показує рівень сприйняття корупції. Держави оцінюються за стобальною шкалою, де 0 – найбільший рівень корупції, а 100 – найменший [31]. За даними Transparency International у 2025 році Україна отримала 36 балів та посіла 104 місце зі 182. Це доволі високий рівень корупції і нам є над чим працювати [□].

В контексті цієї проблеми варто розглянути яку роль відіграє електронне врядування в запобіганні корупційним явищам. На думку

Кононенко В.В. та Дзавелюк М.В. інструменти електронного врядування допомагають громадянам швидко та прозоро отримувати публічні послуги, запобігаючи можливим спробам зловживання владою з боку чиновників. Оскільки у цифровому просторі набагато легше відслідкувати усі дії, що можна використовувати як для попередження корупції так і для її виявлення [37, с. 133]. В іншій своїй роботі Кононенко В.В. наголошує на тому, що держави з високим рівнем цифровізації менш корумповані, оскільки зникає суб'єктивний фактор із рішень чиновників. Також науковець акцентує на тому, що війна не призвела до погіршення відносин між державою і громадянами, а дала поштовх для освоєння нових можливостей [88, с. 278].

З цього випливає, що за допомогою електронного врядування забезпечується високий рівень прозорості діяльності органів влади і довіри громадян до державних інститутів. Це можна побачити проаналізувавши деякі статистичні дані. Наприклад, за результатами щорічного опитування КМІС, проведеного у 2024 році за підтримки ПРООН, 84 % українців позитивно оцінили досвід користування е-послугами, що на 5 % більше, ніж у 2023 році [28, с. 621]. Це свідчить про постійний розвиток електронного врядування, про зручність цифрових сервісів, а головне про довіру до них. За даними Transparency International Україна, у межах програми «Прозорі міста» середній рівень прозорості муніципалітетів у 2024 році зріс із 42,2 % до 45,4 %. Лідерами стали Чернівці (84,5 бала), Вінниця (81 бал) та Луцьк (76 балів) [28, с. 622]. Це демонструє поступове впровадження принципів відкритості та цифрової підзвітності навіть в умовах воєнного стану.

Інструментом для забезпечення прозорості державної влади є реєстр електронних декларацій. У 2024–2025 роках НАЗК розпочало 1534 перевірки декларацій, з яких 78 % уже завершено. Порушення не були виявлені лише у 0,9 % випадків (11 декларацій). Це свідчить про наявність значних проблем із дотриманням антикорупційного законодавства та необхідність удосконалення системи контролю [28, с. 622].

Для того, аби підвищити рівень довіри до органів влади, громадяни повинні мати інформацію про їх діяльність у повному обсязі, а головне, щоб ці дані були правдивими [29, с.89]. Що є дуже актуально в умовах воєнного стану, адже якщо громадяни не будуть довіряти органам влади, то не зможуть ефективно взаємодіяти. Виходячи із цієї тези варто розглянути явище відкритих. Вони сприяють розвитку демократії в країні, рівного доступу до публічної інформації, довіри до влади. Україна впроваджує політику відкритості державного сектору згідно із принципами Міжнародної хартії відкритих даних (Open Data Charter) [7, с. 32]. До основних принципів, за якими здійснюється оприлюднення наборів відкритих даних відносять такі:

- відкритість за замовчуванням;
- оперативність;
- доступність і використання;
- порівняння та інтероперабельність ;
- покращене урядування і залучення громадян;
- інклюзивний розвиток та інновації [49].

Поняття «відкриті дані» закріплено в Законі України «Про доступ до публічної інформації». Встановлено, що відкриті дані – це інформація, яка оброблена електронними засобами, має вільний та безоплатний доступ [67]. Основними характеристиками є доступність для усіх громадян, формат, який дозволяє автоматизовану обробку, відсутність фінансових обмежень, обмежень щодо авторських прав [7, с. 32].

Інструментом, що підвищує прозорість та відкритість органів влади на сьогодні в Україні є електронна платформа публічних закупівтль Prozorro. Вона надає вільний доступ до інформації про державні закупівлі. Це в свою чергу дозволяє антикорупційним органам виявляти та запобігати корупційним проявам. На платформі доступні усі етапи процесу закупівель від оголошення тендеру до укладення договору. Також система Prozorro надала нові можливості не лише для виявлення корупції, а й для проведення аналізу

ефективності закупівель, оскільки потрібна інформація завжди є доступно [7, с.33].

Міжнародні установи, зокрема Світовий банк, позитивно оцінили платформ. Та рекомендували використовувати Prozorro для закупівель у сфері відбудови, надавши поради для адаптації системи під свої правила. Першим замовником стало Міністерство охорони здоров'я, яким було організовано закупівлю на створення структурованої кабельної системи в лікарні «Охмадит» [96, с. 350].

На думку науковця Р. Була відкриті дані за умови ефективного використання, дають можливість оптимізувати діяльність органів влади шляхом аналізу великого масиву інформації. Що забезпечує прийняття якісних рішень, які базуються на реальних даних [7, с.33]. Набори даних, які мають бути оприлюднені зафіксовані у Постанові Кабінету Міністрів України «Про затвердження переліку наборів даних, які підлягають оприлюдненню у формі відкритих даних» [69]. Деякі з них наведені у таблиці 1.1

Таблиця 1.1

Перелік наборів даних, які підлягають оприлюдненню у формі відкритих даних

Структура / орган	**Приклади наборів даних, що підлягають оприлюдненню**
Верховна Рада України	інформація про пленарні засідання; інформація про законопроекти; стенограми та порядки денні пленарних засідань; інформація про народних депутатів України; господарсько-фінансова діяльність Верховної Ради України
Конституційний Суд України	акти Конституційного Суду України; порядки денні органів Конституційного Суду України; інформація

	про конституційні скарги та подання; акти з організаційних питань
Вища рада правосуддя	рішення Вищої ради правосуддя; інформація про автоматизований розподіл справ; реєстр повідомлень суддів про втручання у здійснення правосуддя; інформація про притягнення суддів до дисциплінарної відповідальності
Центральна виборча комісія	інформація про результати виборів; дані про виборчі дільниці; фінансові звіти виборчих фондів; відомості про кандидатів
Національний банк України	структура власності банків; офіційний курс гривні; дані фінансової звітності банків; інформація з Державного реєстру банків; показники валютного ринку України
Офіс Генерального прокурора	звіт про роботу прокурора; єдиний звіт про кримінальні правопорушення; єдиний звіт про осіб, які вчинили кримінальні правопорушення
Міністерство юстиції України	Єдиний державний реєстр юридичних осіб; Єдиний реєстр нотаріусів; Єдиний реєстр боржників; Єдиний реєстр приватних виконавців
Міністерство внутрішніх справ України	місця розміщення камер автоматичної фіксації порушень; перелік суб'єктів охоронної діяльності; перелік суб'єктів, що мають ліцензії на діяльність зі зброєю
Міністерство економіки України	інформація про публічні закупівлі; реєстри ліцензіатів; класифікатор професій; реєстр індустріальних парків; дані про державну підтримку сільського господарства

Міністерство фінансів України	інформація про використання публічних коштів; державний бюджет України; інформація щодо державного боргу; інформація про розподіл субвенцій
Міністерство охорони здоров'я України	Державний реєстр лікарських засобів; медична статистична звітність; перелік лікарських засобів, що підлягають реімбурсації; ліцензійний реєстр МОЗ
Міністерство освіти і науки України	реєстр суб'єктів освітньої діяльності; реєстр документів про освіту; реєстр сертифікатів ЗНО; дані щодо вступу до закладів вищої освіти
Міністерство оборони України	інформація про втрати живої сили та техніки противника; перелік операторів протимінної діяльності
Міністерство енергетики України	дані звіту Ініціативи прозорості видобувних галузей; фактичні обсяги видобутку природного газу; показники діяльності підприємств державного сектору економіки

Таблиця сформована на основі джерела: [69].

Особливу роль у цифровізації відіграє платформа data.gov.ua – єдиний державний веб-портал відкритих даних в Україні. Станом на 2026 рік на сайті опубліковано 38696 наборів даних [52].

На сьогодні гостро постало питання легітимності влади в Україні, оскільки завершився строк повноважень Президента України та парламенту. І хоча Конституцією передбачено, що під час воєнного стану можуть бути обмежені права громадян зокрема і виборче право, це питання доволі дискусійне. Якщо говорити про вибори в звичному для нас режимі за допомогою паперових бюлетенів та виборчих дільниць, то вони скоріше неможливі. Тому що ніхто не може гарантувати безпеку під час їх проведення, з огляду на постійні ракетні атаки. Ще однією причиною є реалізація виборчого права військовослужбовцями, оскільки вони не можуть покидати

позиції будь-коли, а організувати виборчу дільницю на лінії фронту не можливо.

Тому логічним є застосування інструментів електронної демократії, що на нашу думку тісно пов’язана із електронним врядуванням, а саме е-голосування. Порівняно з традиційними методами, всі форми е-голосування мають переваги. Зокрема, вони забезпечують ширший доступ до виборчого процесу, дозволяючи брати участь громадянам, які перебувають за межами країни або з об’єктивних причин не можуть фізично з’явитися на дільницю. Серед інших переваг – оперативність обробки результатів, яка дає змогу отримати їх майже миттєво, зниження витрат на друк, транспортування та логістику, а також мінімізація людського фактора, що зменшує ризик помилок під час підрахунку голосів.

Особливо під час воєнного стану ці переваги є вагомими, та звучать як вирішення проблеми, але не все так однозначно. Існує багато ризиків. По-перше, відсутні абсолютні гарантії захищеності системи від зовнішнього втручання або кібератак. По-друге, постає питання довіри виборців до результатів голосування, зокрема впевненості у правильності підрахунку голосів та їх врахуванні. Важливим є і механізм підтвердження виборцем факту свого волевиявлення. Окрім цього, актуальною залишається проблема забезпечення таємниці голосування, адже необхідно гарантувати, що інформація про вибір громадянина не стане доступною третім особам [6]. Тому, на нашу думку, е-голосування це дуже перспективна сфера розвитку держави, але вона потребує належного технічного та правового підґрунтя.

Отже, в умовах воєнного стану електронне врядування стало необхідною складовою функціонування держави, забезпечуючи безперервність надання послуг і ефективну взаємодію влади з громадянами. Воно дозволило адаптувати систему управління до кризових умов та частково компенсувати обмеження, пов’язані з безпековою ситуацією.

Дослідження показало, що попри значні виклики, зокрема кіберзагрози, технічні обмеження та проблеми цифрової грамотності, рівень використання електронних сервісів суттєво зріс. Це свідчить про їхню затребуваність і ефективність, а також про поступове формування цифрової культури в суспільстві.

Водночас електронне врядування відіграє важливу роль у підвищенні прозорості діяльності органів влади та зменшенні корупційних ризиків. Однак подальший розвиток цієї сфери, зокрема впровадження е-голосування, потребує комплексного підходу з урахуванням питань безпеки, довіри та правового регулювання.

1.2. Нормативно-правове забезпечення електронного врядування та цифрової безпеки в умовах воєнного стану в Україні

Основним видом забезпечення електронного врядування є його нормативно-правова база, що фіксує головні ідеї, цілі, завдання, напрями розвитку та засоби його впровадження.

Основні засади щодо державної політики у сфері розвитку інформаційного суспільства та інформатизації, розбудови електронного врядування закріплені в низці нормативно-правових актів, зокрема в Законах України «Про інформацію» (1992), «Про науково-технічну інформацію» (1993), «Про захист персональних даних» (2010), «Про захист інформації в інформаційно-телекомунікаційних системах» (1994), «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» (2007), «Про електронні документи та електронний документообіг» (2003), «Про електронні комунікації» (2020), «Про електронну ідентифікацію та електронні довірчі послуги» (2017), «Про медіа» (2022) та ін [51, с.258].

Варто розглянути Закон України «Про звернення громадян», що забезпечує громадянам України можливості для участі в управлінні

державними і громадськими справами, для впливу на поліпшення роботи органів державної влади і місцевого самоврядування, підприємств, установ, організацій незалежно від форм власності, для відстоювання своїх прав і законних інтересів та відновлення їх у разі порушення.

У цьому контексті слід зазначити про Закон України «Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції» [64], який стосується важливих змін розбудови електронного врядування, зокрема стосовно збільшення інструментів втілення прав громадян відносно звернення до органів влади із застосуванням сучасних ефективних засобів (електронне звернення, електронна петиція) [51, с.259]. Таким чином, підвищується рівень відкритості діяльності органів влади й налагоджується комунікація з громадянами. В умовах режиму воєнного стану між органами публічної влади та суспільством ефективна взаємодія є дуже важливою.

У процесі розвитку електронного врядування важливу роль відіграє Закон України «Про доступ до публічної інформації», що встановлює порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень [67]. Цей закон був доповнений ст. 10-1 Закон України «Про внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних», що закріпила поняття «відкриті дані» [59]. Це дозволило державі публікувати інформацію онлайн, без звернень громадян, що підвищує рівень прозорості та підзвітності.

Але під час воєнного стану постала проблема кібератак на онлайн ресурси, тому доступ до публічної інформації було дещо обмежено. Відповідно до указу Президента № 64/2022, Кабінетом Міністрів України було прийнято Постанову № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» [19].

Постановою були визначені певні заходи, для забезпечення безпеки та ефективності управління інформаційними ресурсами й електронними системами в час війни:

- постанова передбачає можливість розміщення державних інформаційних ресурсів та публічних електронних реєстрів на хмарних ресурсах або в центрах обробки даних, розташованих за межами України [19]. Це сприяє забезпеченню інформаційної доступності та захисту даних у воєнний період;
- для забезпечення цілісності й конфіденційності державних інформаційних ресурсів було дозволено створення резервних копій, зберігання їх у зашифрованому вигляді за межами країни, а також в ізольованих сегментах центрів обробки даних;
- з метою забезпечення контролю та захисту критичних інформаційних ресурсів під час воєнного варто було зупинити та обмежити роботу інформаційних систем, електронних реєстрів та комунікаційних систем [19].

Внаслідок запровадження воєнного стану було обмежено доступу до Державної казначейської служби [35, с.68]. Урядовою постановою від 24 березня 2022 року № 364 були внесені зміни щодо питань регулювання державної реєстрації та функціонування реєстрів у воєнний період [65]. Згідно з цими змінами, інформація з реєстрів може надаватися через державних реєстраторів, нотаріусів та адміністраторів центрів надання адміністративних послуг, розташованих у межах адміністративно-територіальних одиниць, не включених до переліку обмежених зон [35, с.69].

Також було припинено доступ до Єдиного державного реєстру судових рішень (ЄДРСР). Ці заходи були спрямовані для захисту реєстру від кібератак, захисту інформації про суддів та судові рішення від знищення або можливого використання окупантами [35, с. 69]. На сьогодні реєстр значно посилено у сфері кіберзахисту, доступ до нього відновлено для всіх користувачів з 20

червня 2022 року. Однак Державна судова адміністрація України може обмежувати доступ до реєстру у випадку виявлення загроз кібербезпеці [57];

- також було заборонено використання хмарних ресурсів та/або центрів обробки даних, що розташовані на тимчасово окупованих територіях, або тих, що належать державі-агресору [65], це свідчить про спрямованість на захист державної інформації та персональних даних громадян;

Також під час воєнного стану змін зазнали й інші нормативно правові акти та було введено в дію нові, наприклад:

- Закон України «Про хмарні послуги» визначає правові відносини, що виникають при наданні хмарних послуг, та встановлює особливості використання хмарних послуг органами державної влади, органами влади Автономної Республіки Крим, органами місцевого самоврядування, військовими формуваннями [78, с.8]. Стаття 8 цього закону зазначає, що надавачу хмарних послуг заборонено використовувати технічні засоби, що розташовані та тимчасово окупованій території або на території держави-агресова.

- Закон України «Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів» [60] спрямований на підвищення кіберзахисту державних інформаційних ресурсів і об’єктів критичної інформаційної інфраструктури. Забезпечує можливість створення резервних копій інформаційних ресурсів за межами країни [35, с.70]. Зміни стосувались законів «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про публічні електронні реєстри» .

- Закон України «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». спрямований на забезпечення стабільної роботи електронних

комунікаційних мереж в умовах воєнного стану. Ним посилено централізоване управління електронними комунікаціями шляхом надання обов'язкової сили розпорядженням національного центру оперативно-технічного управління, а також запроваджено механізм виключення постачальників з реєстру у разі їх невиконання. Водночас передбачено скорочення строків консультацій під час прийняття регуляторних рішень, що забезпечує оперативність управління без повної відмови від прозорих процедур. Окремі норми закону спрямовані на захист інформаційної безпеки та спрощення використання технічного обладнання з метою швидкого відновлення електронних комунікаційних мереж. Загалом зазначені зміни відображають адаптацію державного регулювання електронних комунікацій до умов воєнного стану та підвищують ефективність управління критичною цифровою інфраструктурою [63].

- Закон України «Про внесення змін до деяких законодавчих актів України щодо забезпечення умов для відновлення та розвитку електронних комунікаційних мереж» [62]. Основна мета цього закону – створення умов для розвитку та відновлення зв'язку в Україні під час дії воєнного стану та у післявоєнний період [35, с.70].
- Закон України «Щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації» [61] спрямований на прискорену інтеграцію України до Єдиного цифрового ринку ЄС. Забезпечує взаємне визнання кваліфікованих електронних підписів та печаток, що спрощує електронну взаємодію між Україною та ЄС.

Узагальнюючи, нормативно-правове забезпечення електронного врядування в Україні є комплексним і охоплює регулювання інформаційної сфери, електронних послуг та кібербезпеки. В умовах воєнного стану воно було оперативно адаптоване через прийняття нових актів і внесення змін до чинного законодавства.

Основна увага зосереджена на захисті державних інформаційних ресурсів, забезпеченні безперервності їх функціонування та використанні сучасних технологій, зокрема хмарних рішень. Водночас зберігається орієнтація на відкритість, доступ до інформації та розвиток електронної взаємодії з громадянами.

Висновки до Розділу 1

Узагальнюючи результати дослідження, викладені в першому розділі, доцільно зазначити, що електронне врядування в умовах воєнного стану стало критично важливий елемент забезпечення функціонування держави, її стійкості та безпеки. Воно виконує не лише сервісну функцію, а й стає складовою національної безпеки, забезпечуючи безперервність надання адміністративних послуг, ефективну комунікацію між владою та громадянами, а також підтримку управлінських процесів у кризових умовах.

Аналіз особливостей функціонування електронного врядування засвідчив, що його розвиток у воєнний період відбувається під впливом як значних викликів, так і нових можливостей. З одного боку, суттєвими обмеженнями виступають кіберзагрози, руйнування інфраструктури, обмеження доступу до державних реєстрів та проблеми цифрової нерівності. З іншого боку, саме ці обставини стимулювали прискорену цифровізацію, зростання рівня цифрової грамотності населення та підвищення попиту на електронні послуги.

Встановлено, що електронне врядування відіграє вагому роль у підвищенні прозорості діяльності органів публічної влади та зниженні корупційних ризиків завдяки автоматизації процесів, мінімізації людського фактора та можливості цифрового контролю. Водночас реалізація окремих перспективних інструментів, зокрема електронного голосування, потребує комплексного підходу, який має враховувати питання кібербезпеки, довіри суспільства та належного правового забезпечення.

Дослідження нормативно-правової бази показало, що в Україні сформовано розгалужену систему правового регулювання електронного врядування, яка охоплює сфери інформаційних відносин, електронних комунікацій, захисту персональних даних та кібербезпеки. В умовах воєнного стану ця система зазнала оперативної адаптації шляхом прийняття спеціальних нормативних актів і внесення змін до чинного законодавства. Ключовими напрямами таких змін стали забезпечення безперервності функціонування інформаційних систем, посилення кіберзахисту, впровадження хмарних технологій та тимчасове обмеження доступу до окремих інформаційних ресурсів з метою їх захисту.

Отже, електронне врядування в Україні в умовах воєнного стану характеризується високою динамічністю розвитку, адаптивністю до кризових викликів та стратегічною значущістю для держави. Подальший його розвиток має бути спрямований на вдосконалення правового регулювання, зміцнення кібербезпеки, подолання цифрової нерівності та впровадження інноваційних цифрових інструментів із урахуванням вимог безпеки та довіри суспільства.

РОЗДІЛ 2
ВИКЛИКИ ЦИФРОВОЇ БЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО ВРЯДУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ

2.1. Характеристика основних кіберзагроз електронному врядуванню в умовах воєнного стану

Як зазначалось, електронне врядування це форма організації державної влади, що використовує інформаційно-комунікаційні технології. А з початком повномасштабного вторгнення цифровий простір України зіштовхнувся з рядом небезпек, тобто кіберзагроз, що унеможливлює ефективне використання електронного врядування .

Для аналізу цього питання варто розпочати із визначення таких термінів : кіберзагроза, кібератака та кібербезпека. Тлумачення цих термінів можна знайти у Законі України «Про основні засади забезпечення кібербезпеки України». Так, кіберзагроза згідно із Законом – це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів. Кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах та інші [75]. Отже кіберзагроза – це можливість чи намір спричинити шкоду, а кібератака – це уже конкретні дії що втілюють цю загрозу.

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 і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [75].

Але єдиного підходу до визначення кібербезпеки немає, до прикладу, В. Н. Фурашев пояснює поняття «кібербезпеки» як сукупність здібностей людини, народу та держави, стосовно запобігання та усунення, свідомого, прямого негативного впливу інформації [93, с.163]. Д. О. Ширяєв відзначає, що кібербезпека є складною проблемою і для того аби захистити свою цифрову інфраструктуру, потрібно постйно розробляти нові технолоігї [34, с. 403]. У свою чергу, Л. М. Бєлкін, Ю. Л. Юринець, М. Л. Бєлкін, Є. В. Криволап вважають , що кібербезпека це частина загального поняття безпеки інформації [86, с.80]. Таким чином, кібербезпека поєднує правовий, технологічний, соціальний та безпековий виміри, що зумовлює різноманітність її визначень у науковій та нормативній площині.

Кіберзагрози з якими Україна стикається на сьогодні, можна розділити на 4 види (таблиця 2.1.)

Таблиця 2.1. Види кіберзагроз

Кіберзагроза	**Характеристика**
Деструктивні атаки	Передбачають використання програм-руйнівників (wiper), як-от HermeticWiper, WhisperGate. Метою цих атак є виведення з ладу систем управління, баз даних та пошкодження об’єктів критичної інфраструктури.
Фішингові атаки	Наприклад, від імені державних органів розповсюджуються фішингові

	листи, підроблені застосунки з метою збору персональних даних або проникнення в інформаційні системи.
Кібершпигунство	Довготривале проникнення у комп'ютерні мережі з метою збору даних, ураження комунікаційних систем або підготовки до фізичних атак.
Інформаційно-психологічні операції	Дезінформація, поширення фейкових повідомлень, deepfake-відео, маніпуляція громадською думкою через Telegram-канали, Інтернет та соціальні мережі.

Таблиця сформована на основі джерела [9, с.133]

Згідно з аналітичним звітом Державної служби спеціального зв'язку та захисту інформації України за перше півріччя 2025 року, кількість кіберінцидентів зросла на 17% порівняно з попереднім періодом [12, с. 9]. Загалом за 2025 рік порівняно із 2024 роком кількість кібератак підвищилась на 37% про це повідомила керівниця служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО Наталія Ткачук [91]. Це свідчить не лише про зростання інтенсивності атак, але й про системний характер кібероперацій проти України.

Найбільш ураженими залишаються:

- місцеві органи влади (34% зафіксованих атак);
- сектор безпеки та оборони (23%);
- урядові організації (19%);
- енергетичний сектор (4%) [12, с. 10].

Важливим джерелом для оцінки сучасних кіберзагроз у сфері електронного врядування є звіти Агентства Європейського Союзу з кібербезпеки (ENISA – European Union Agency for Cybersecurity). У звіті ENISA Threat Landscape for Public Administration 2024 проаналізовано основні

загрози, які спрямовані на органи державної влади країн Європейського Союзу.

Згідно зі звітом, публічний сектор (тобто органи державної влади, місцевого самоврядування та урядові цифрові сервіси) входить до числа найбільш атакованих секторів, 38,2 % усіх інцидентів були спрямовані саме на публічну адміністрацію [3].

Тобто як в Україні так і у ЄС органи влади є найбільш атакованими, але під час воєнного стану це явище набуває системного характеру.

У таблиці 2.1. наведені найбільш поширені та давно відомі види кібератак, але Держспецзв'язку у своєму звіті наводить низку нових:

- атаки типу «Zero Click» (у перекладі – «нульова взаємодія»). Це атаки, які не потребують жодних дій з боку користувача. Тобто для зараження системи достатньо лише відкриття електронного листа [12, с. 16]. ENISA підкреслює, що такі вразливості є особливо небезпечними для посадових осіб державного сектору. Для України в умовах воєнного стану ця загроза є критичною, оскільки вона може використовуватися для: стеження за державними службовцями, збору розвідувальної інформації, підриву управлінських процесів [3].
- у звіті фіксується перехід зловмисників до тактики «Steal & Go» (у перекладі – «викрав і пішов»). Це означає, що шкідливе програмне забезпечення не закріплюється надовго в системі, а швидко викрадає необхідні дані та зникає [12, с. 5]. Стилер (від англ. stealer), або ж викрадач – один із видів шкідливого програмного забезпечення, яке збирає інформацію на комп'ютері й надсилає її хакерам[13] .
- у звіті також зазначено ознаки використання штучного інтелекту (тобто програм, здатних генерувати код або тексти автоматично) для створення шкідливих скриптів. Це ускладнює аналіз та підвищує варіативність атак. Таким чином, цифрові загрози стають більш автоматизованими та масштабованими [12, с. 13].

В умовах воєнного стану кількість і складність кібератак зростає, тому ефективний кіберзахист є необхідною умовою стабільного функціонування електронного врядування та захисту державних інформаційних ресурсів.

Отже, у підрозділі встановлено, що кіберзагрози в умовах воєнного стану мають серйозний вплив на функціонування електронного врядування. Розгляд основних понять дозволив зрозуміти, що кіберзагроза – це потенційна небезпека, тоді як кібератака є її безпосереднім проявом у вигляді конкретних дій, спрямованих на порушення роботи інформаційних систем.

З’ясовано, що поряд із традиційними видами кібератак, такими як фішинг, кібершпигунство чи деструктивні атаки, з’являються нові, більш складні загрози. До них належать атаки без участі користувача («zero-click»), швидке викрадення даних («steal & go»), а також використання штучного інтелекту для створення шкідливих програм. Це свідчить про те, що кіберзагрози постійно розвиваються і стають більш небезпечними.

Статистичні дані показують, що найбільше атак спрямовано на органи державної влади, що пояснюється їхньою важливістю для функціонування держави. В умовах війни такі атаки мають не лише технічний, а й стратегічний характер, оскільки можуть впливати на стабільність управління та довіру громадян.

2.2. Захист персональних даних та конфіденційності в системах е-урядування в умовах воєнного стану

Під час воєнного стану захист персональних даних став одним із ключових елементів національної безпеки, оскільки поширились кібератаки на державні реєстри, що містять власне персональні дані громадян.

Варто розглянути саме поняття персональних даних. Закон України «Про захист персональних даних» дає таке визначення цьому поняттю: «персональні дані – відомості чи сукупність відомостей про фізичну особу,

яка ідентифікована або може бути конкретно ідентифікована»[70]. Таке ж визначення зафіксовано й у Законі України «Про інформацію» [73]. Європейське законодавство також має своє визначення. Так, п. 1 ст. 4 Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС» закріплює, що «персональні дані» означають будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»). Фізична особа, яку можна ідентифікувати, – це особа, яку можна ідентифікувати прямо чи опосередковано, зокрема за такими ідентифікаторами, як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної ідентичності такої фізичної особи [80].

Якщо порівняти закріплені поняття в українському та європейському законодавстві, то можна зробити висновок, що українське законодавство визначає персональні дані у більш загально, зосереджуючись на ключовому елементі – можливості ідентифікації особи. Натомість європейський підхід є значно ширшим: він не лише фіксує сам факт можливості ідентифікації, але й деталізує способи та ознаки, за якими вона здійснюється [54, с.431].

Персональні дані також можна класифікувати за певними критеріями (таблиця 2.2.)

Таблиця 2.2. Класифікація персональних даних

Критерій класифікації	**Вид даних**
За сферою використання	звичайні персональні дані; персональні дані працівників; персональні дані публічних осіб; персональні дані військовослужбовців та осіб, які

	беруть участь у збройному конфлікті (у тому числі волонтерів); персональні дані призовників, військовозобов'язаних і резервістів; медичні персональні дані (дані про стан здоров'я, генетичні дані); персональні дані, що використовуються у цифровому середовищі.
За можливістю поширення	відкриті персональні дані; конфіденційні персональні дані.
За ступенем втручання у приватне життя особи	звичайні персональні дані; чутливі (особливо чутливі) персональні дані.
За правовим режимом захисту	персональні дані, що обробляються в умовах звичайного правового режиму; в умовах надзвичайного стану; в умовах воєнного стану.
За підставами обробки	персональні дані, обробка яких здійснюється за згодою суб'єкта персональних даних; персональні дані, обробка яких здійснюється без згоди суб'єкта на підставах, визначених законом.
За метою обробки	персональні дані, що обробляються з метою забезпечення охорони здоров'я; персональні дані, що використовуються для ведення військового обліку призовників, військовозобов'язаних та резервістів; персональні дані, обробка яких здійснюється для захисту життєво важливих інтересів суб'єкта персональних даних або інших осіб.

Таблиця сформована на основі джерел: [54, с.432], [80]

Доцільно зазначити, що відповідно до Закону України «Про критичну інфраструктуру» захист персональних даних належить до сфер, які функціонально пов'язані з національною системою захисту критичної інфраструктури [74]. Це свідчить про те, що система захисту персональних даних має самостійне значення та водночас перебуває у тісному взаємозв'язку із забезпеченням національної безпеки держави.

З метою посилення інформаційної безпеки 18 березня 2022 року Рада національної безпеки і оборони України ухвалила рішення щодо реалізації єдиної інформаційної політики в умовах воєнного стану, яке було введене в дію Указом Президента України від 19 березня 2022 року №152/2022. У цьому рішенні підкреслюється, що в умовах воєнного стану забезпечення єдиної інформаційної політики розглядається як одне з пріоритетних завдань у сфері національної безпеки [97].

Особливості правового режиму функціонування інформаційних систем, у тому числі тих, що містять персональні дані, були визначені постановою Кабінету Міністрів України від 12 березня 2022 року №263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем та публічних електронних реєстрів в умовах воєнного стану» [19]. Згідно з цією постановою на період дії воєнного стану держателі державних реєстрів, до яких належать органи державної влади, а також державні та комунальні підприємства, установи й організації, мають право вживати додаткових заходів для захисту інформації. Зокрема, передбачено можливість розміщення державних інформаційних ресурсів і публічних електронних реєстрів на хмарних ресурсах або у центрах обробки даних, що знаходяться за межами України, створення додаткових резервних копій реєстрів, а також тимчасового обмеження або призупинення їх роботи з метою забезпечення безпеки даних [54, с.429].

Крім того, у 2025 році було прийнято постанову Кабінету Міністрів України «Деякі питання оперативно-технічного управління електронними

комунікаційними мережами в умовах надзвичайної ситуації, надзвичайного або воєнного стану» від 24 січня 2025 року №75. У зазначеному нормативному акті визначено, що система оперативно-технічного управління електронними комунікаційними мережами може функціонувати у двох режимах: звичайному та надзвичайному, що дає змогу забезпечити безперервність роботи мереж та належний рівень їх захисту в умовах кризових ситуацій [23].

У контексті забезпечення національної безпеки держави мають право запроваджувати спеціальні режими захисту персональних даних у період воєнних дій [54, с. 429]. В умовах збройного конфлікту суттєво зростає кількість кібератак, спрямованих на об’єкти критичної та військової інфраструктури. Такі атаки можуть спричинити несанкціонований доступ до інформації, що, у свою чергу, створює ризики витоку персональних даних та їх подальшого використання противником у власних цілях [32].

Під станом захищеності персональних даних розуміють юридично гарантований рівень безпеки персональної інформації, за якого забезпечуються її конфіденційність, цілісність і доступність, а також дотримуються права суб’єктів персональних даних щодо їх збирання, обробки, зберігання та передачі. Такий стан передбачає впровадження відповідних організаційних і технічних заходів, спрямованих на запобігання несанкціонованому доступу, розголошенню, зміні або знищенню персональних даних відповідно до вимог чинного законодавства [54, с.429].

Важливу роль у забезпеченні кіберзахисту державних інформаційних ресурсів відіграє система виявлення вразливостей і реагування на кіберінциденти та кібератаки, функціонування якої координується Державним центром кіберзахисту Державної служби спеціального зв’язку та захисту інформації України. Основним завданням цієї системи є здійснення централізованого моніторингу кіберзагроз, виявлення підозрілої активності в інформаційних системах, а також оперативне реагування на кіберінциденти, що можуть становити загрозу для безпеки державних інформаційних ресурсів.

Система забезпечує збір та аналіз телеметричної інформації про події інформаційної безпеки, що дає змогу своєчасно виявляти потенційні загрози та запобігати їх негативним наслідкам [53].

За результатами моніторингу у 2025 році було опрацьовано понад 17 тисяч подій інформаційної безпеки, серед яких зафіксовано 730 кіберінцидентів різного рівня складності. Значна частина таких інцидентів була пов’язана з використанням шкідливого програмного забезпечення, основною метою якого є отримання несанкціонованого доступу до інформаційних систем та встановлення прихованого контролю над ними [25]. Подібні атаки можуть призводити до втрати облікових записів, зараження інформаційних систем шкідливим програмним забезпеченням, а також до незаконного отримання конфіденційної інформації.

Особливу небезпеку становлять кібератаки, що здійснюються організованими групами або так званими кластерами кіберзагроз, діяльність яких спрямована на проведення кіберрозвідки та викрадення інформації. Оскільки в інформаційних системах цих установ обробляються значні обсяги персональних даних громадян, успішні кібератаки можуть призвести до їх витоку та подальшого використання у протиправних цілях [25].

Отже, в умовах воєнного стану захист персональних даних набув особливого значення, оскільки державні інформаційні системи стали одними з основних об’єктів кібератак. Було встановлено, що держава запровадила додаткові механізми захисту інформаційних ресурсів, зокрема резервне копіювання даних, використання хмарних технологій та посилений моніторинг кіберзагроз.

Водночас зростання кількості кіберінцидентів свідчить про необхідність постійного вдосконалення систем кіберзахисту та забезпечення належного рівня конфіденційності персональних даних у системах електронного врядування.

Висновки до розділу 2

Отже, в умовах воєнного стану питання цифрової безпеки систем електронного врядування набули особливого значення, оскільки саме інформаційний простір став одним із ключових напрямів протистояння. Повномасштабне вторгнення спричинило суттєве зростання кількості кібератак на органи державної влади, державні реєстри, електронні комунікаційні мережі та інші об’єкти критичної інформаційної інфраструктури. Це створило додаткові ризики для стабільного функціонування державного управління та надання електронних послуг громадянам.

У ході дослідження було з’ясовано, що сучасні кіберзагрози характеризуються не лише збільшенням кількості атак, а й зміною їх характеру. Поряд із традиційними формами кібератак активно застосовуються новітні технології та автоматизовані механізми впливу, що ускладнює процес виявлення та нейтралізації загроз. Особливу небезпеку становлять атаки, спрямовані на отримання доступу до державних інформаційних ресурсів та персональних даних громадян, оскільки це може призвести не лише до технічних порушень у роботі систем, а й до негативних наслідків для національної безпеки держави.

Також встановлено, що в умовах воєнного стану захист персональних даних є важливою складовою функціонування систем електронного врядування. Розвиток цифрових сервісів і збільшення обсягів інформації, що обробляється державними інформаційними системами, потребують належного рівня правового, організаційного та технічного захисту. Саме тому держава була змушена оперативно адаптувати механізми кіберзахисту до нових умов, зокрема шляхом резервного копіювання державних реєстрів, використання хмарних технологій, посилення моніторингу кіберзагроз та вдосконалення систем реагування на кіберінциденти.

РОЗДІЛ 3.

ДОСТУПНІСТЬ АДМІНІСТРАТИВНИХ ПОСЛУГ ТА ШЛЯХИ ЇЇ ЗАБЕЗПЕЧЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

3.1. Проблеми доступності адміністративних послуг в умовах воєнного стану

Термін адміністративна послуга в українському законодавстві з'явився в період розвитку концепції сервісної держави. Головним завданням якої є забезпечення доступних і якісних послуг громадянам . Іншими словами можна сказати, що сервісна держава – це держава послуг, обов'язком якої є служіння народу [84, с. 421]. Особливо ця концепція важлива під час воєнного стану, адже життя не зупинилось, люди народжуються, помирають, одружуються, хтось опинився в складних обставинах і потребує соціальної допомоги. І тому держава змушена пристосовуватись до нових умов, для того, щоб забезпечити безперервність надання адміністративних послуг.

Варто зазначити, що до визначення поняття надання послуг органами публічної влади було багато підходів. Такі послуги називали «публічними», «виконавськими», « державними», «управлінськими». Згодом науковці почали використовувати термін «адміністративні послуги», оскільки він передає владно-правовий характер цього процесу та вказує на суб'єкт, який надає такі послуги [84, с. 422].

Остаточно термін «адміністративна послуга» зафіксував Закон України «Про адміністративні послуги». Згідно із ним: « адміністративна послуга – результат здійснення владних повноважень суб'єктом надання адміністративних послуг за заявою фізичної або юридичної особи, спрямований на набуття, зміну чи припинення прав та/або здійснення обов'язків такої особи відповідно до закону» [58]. Також стаття 4 Закону визначає основні принципи, на основі яких здійснюється надання таких послуг:

- верховенства права, у тому числі законності та юридичної визначеності;
- стабільності;
- рівності перед законом;
- відкритості та прозорості;
- оперативності та своєчасності;
- доступності інформації про надання адміністративних послуг;
- захищеності персональних даних;
- раціональної мінімізації кількості документів та процедурних дій, що вимагаються для отримання адміністративних послуг;
- неупередженості та справедливості;
- доступності та зручності для суб'єктів звернень [58].

Але у період воєнного стану, проблематичним стало дотримання таких принципів як: своєчасність , доступність, прозорість та стабільність [39, с.241]. Оскільки Законом України «Про правових режим воєнного стану» статтею 8 встановлено тимчасові обмеження конституційних прав і свобод людини і громадянина [76].

Основними проблемами в перші тижні війни стали: встановлення особи, оскільки багато документів були втрачені; зупинка реєстрації бізнесу, транспортних засобів, нерухомості через припинення роботи відповідних реєстрів; неможливість реєстрації місця проживання; окремою проблемою стали хакерські атаки на державні реєстри; багато громадян переїхали зі своїх міст в інші частини України, ставши внутрішньо переміщеними особами, що в свою чергу підвищило попит на адміністративні послуги, що стосуються підтримки таких громадян [8].

З 24 лютого 2022 року змінились процедури надання адміністративних послуг. Перший нормативно-правовий акт який яскраво демонструє зміни в процедурах – це постанова КМУ від 28 лютого 2022 року «Про зупинення строків надання адміністративних послуг та видачі документів дозвільного

характеру», наразі втратила чинність [72]. Ця постанова є прикладом ситуаційного управління, оскільки процес надання адміністративних послуг повністю залежав від безпекової ситуації.

Також важливим є наказ Міністерства Юстиції України «Про впорядкування відносин з державної реєстрації народження та отримання документів про народження в умовах воєнного стану» [66]. Наказом було значно спрощено процедуру реєстрації новонароджених та видачі відповідних документів , а саме: на територіях бойових дій, реєстрація може здійснюватися лише за заявою у довільній формі, шляхом надсилання копій документів електронною поштою; свідоцтво про народження можна отримати у електронному вигляді, а оригінал у будь-якому відділі ДРАЦС; встановлений порядок реєстрації новонароджених за кордоном; дозволено отримувати такі документи родичам [84, с. 423].

Змін зазнала і процедура реєстрації шлюбу, постановою КМУ від 07.03.2022 «Деякі питання державної реєстрації шлюбу в умовах воєнного стану» (на даний час втратила чинність), було дозволено реєструвати шлюб без присутності одного з наречених, якщо той є військовослужбовцем [17]. Акт про укладення шлюбу може скласти безпосередній командир (керівник) військовослужбовця або поліцейського. Без особистої присутності наречених через відеозв'язок. Акт про укладення шлюбу може скласти керівник медзакладу, в якому перебувають або працюють один або двоє наречених. У присутності двох наречених та свідків. Також один із наречених може доєднатися через відеозв'язок [89, с. 102].

Було продовжено термін дії водійських посвідчень згідно із постановою КМУ від 03.03.2022 «Деякі питання допуску водіїв до керування транспортними засобами» [18], закордонних паспортів постановою КМУ від 28.02.2022 «Деякі питання внесення інформації до паспорта громадянина України для виїзду за кордон» [15].

Постанова КМУ від 06.03.20222 «Деякі питання державної реєстрації та функціонування єдиних та державних реєстрів, держателем яких є Міністерство юстиції, в умовах воєнного стану» дозволила громадянам здійсювати реєстраційні дії в будь-якому доступному органі, здійснювати такі процедури на підставі електронних документів, також встановлено, що реєстрація благодійних організацій та організацій, що допомагають Збройним Силам України здійснюється без сплати адміністративного збору [16].

Також не можливо не розглянути проблеми безпеки, які суттєво вплинули на зміни в сфері адміністративних послуг. На тимчасово окупованих територіях та в зонах бойових дій була частково, або повністю припинена робота органів публічної влади. Зрозуміло, що надання адміністративних послуг стало неможливим. Для того аби забезпечити громадянам доступ до таких послуг, органи влади було переміщено на безпечні території та запроваджено дистанційні роботи і онлайн-послуги [48, с.75]. Що для нашої теми є ключовим аспектом, оскільки саме в цей період електронне врядування відіграло ключову роль, вирішивши питання доступності послуг за допомогою онлайн-сервісів, які детальніше розглянемо пізніше. Також під час повітрних тривог центри надання адміністративних послуг, для того аби організувати безпечні умови для персоналу припиняють роботу, що унеможливлює дотримання вище наведених принципів доступності та стабільності.

Також гостро постали кадрові проблеми, оскільки багато кваліфікованих працівників змушені були виїздити за кордон, або залишились на тимчасово окупованих територіях. Кадрова спроможність публічної адміністрації у зв’язку із цим знизилась. Зросло навантаження на тих працівників, котрі залишились [48, с.76].

У своєму звіті голова НАДС Наталія Алюшина навела статистичні дані, щодо кадрової ситуації державної служби, яка слалась у 2022 році з початком воєнного стану (таблиця 3.1.)

Таблиця 3.1.

Вплив воєнного стану на кадрових склад державної служби

Показник	**Кількість**
Звільнено	25602 державних службовці
Призначено на посади	20297
Виїхали за кордон	5355, з них 3992 – жінки
Перебували на окупованих територіях	4713
Загинуло	108
Поранено	80
Зникло безвісти	205

Таблиця сформована на основі джерела [5].

Особливо критичною проблема доступності стала для людей з особливими потребами та старшого покоління. Через призупинення роботи адміністративних центрів люди залишились без можливості оформити важливі документи [39, с.241].

У таких умовах особливої актуальності набуває розвиток електронних сервісів як альтернативного інструменту забезпечення доступу громадян до адміністративних послуг. Практика воєнного часу засвідчила, що цифровізація публічного управління стала необхідною умовою функціонування держави.

Підтвердженням цього є результати дослідження Transparency International Ukraine в межах програми «Прозорі міста», яке у 2025 році було спрямоване на оцінку рівня розвитку електронних сервісів у муніципалітетах України відповідно до європейських стандартів. Дослідження охопило низку обласних центрів, зокрема Київ, Львів, Харків, Дніпро та інші, і дозволило комплексно оцінити стан цифрової інфраструктури на місцевому рівні.

За результатами аналізу встановлено, що середній рівень розвитку електронних сервісів становить близько 49,8 %, це свідчить, що більшість

громад мають низький рівень цифрової зрілості. Найвищі показники показали такі міста як Київ та Львів, а найнижчі Полтава та Чернігів [79].

Важливо зазначити, що попри складні безпекові умови, більшість органів місцевого самоврядування забезпечують функціонування базових електронних сервісів. Зокрема, у більшості міст доступні онлайн-запис до центрів надання адміністративних послуг, сервіси електронних петицій, системи моніторингу громадського транспорту та інші інструменти взаємодії з громадянами [79]. Це свідчить про адаптацію публічної адміністрації до умов воєнного стану.

Отже, запровадження воєнного стану суттєво вплинуло на систему надання адміністративних послуг в Україні та поставило перед публічною адміністрацією нові виклики. Тимчасове припинення роботи державних реєстрів, обмеження доступу до органів влади, кадрові втрати, переміщення населення та постійні безпекові загрози ускладнили дотримання основних принципів надання адміністративних послуг, зокрема доступності, стабільності, своєчасності та відкритості. Водночас саме кризові умови стали поштовхом до адаптації процедур надання послуг та прискорення процесів цифровізації публічного управління.

Держава була змушена оперативно реагувати на нові потреби суспільства шляхом внесення змін до нормативно-правового регулювання, спрощення окремих адміністративних процедур та розширення можливостей дистанційного отримання послуг. Особливого значення набули електронні сервіси, які забезпечили безперервність взаємодії громадян з органами влади навіть в умовах активних бойових дій та переміщення населення. Саме розвиток електронного врядування дозволив частково компенсувати обмеження, пов’язані з фізичною недоступністю адміністративних установ.

Разом із тим результати досліджень свідчать, що рівень розвитку електронних сервісів у різних громадах залишається нерівномірним. Це вказує на необхідність подальшого вдосконалення цифрової інфраструктури,

підвищення цифрової грамотності населення та забезпечення рівного доступу громадян до електронних адміністративних послуг, особливо для людей старшого віку та осіб з інвалідністю.

3.2. Е-сервіси як рішення для підвищення доступності адміністративних послуг в умовах воєнного стану

Окресливши проблеми, з якими стикнулася сфера надання адміністративних послуг під час війни, варто розглянути, які є рішення цих питань, як все ж таки держава змогла взаємодіяти із громадянами в таких умовах.

Онлайн-сервіси в цьому контексті відіграли ключову роль, дали можливість без фізичної присутності та під час повітряних тривог, надавати громадянам електронні послуги та інформувати їх.

Ще до війни у 2019 році Президентом України був представлений проєкт «Держава в смартфоні», що передбачав підвищення рівня якості та швидкості надання адміністративних послуг онлайн. Він реалізується через платформу «Дія», що є інтегрованою цифровою системою, яка дозволяє громадянам отримувати державні послуги без фізичної взаємодії із службовцями, тобто онлайн. Працювати портал почав у 2020 році та об’єднав понад 100 державних послуг, наприклад, подання податкових декларацій, оформлення соціальної допомоги, реєстрацію бізнесу, доступ до цифрових документів [10, с.170].

Відповідно до п. 1 «Положення про Єдиний державний вебпортал електронних послуг», затвердженого Постановою КМУ «Питання Єдтного державного вебпотралум електронних послуг та Реєстру адміністративних послуг», портал «Дія» визначається як державна інформаційно-комунікаційна система, що забезпечує доступ до електронних публічних послуг, адміністративних сервісів та інформаційних ресурсів у цифровій формі.

Згідно з п. 4 зазначеного Положення, основною метою функціонування порталу є реалізація права громадян на доступ до електронних публічних послуг, а також забезпечення взаємодії між фізичними і юридичними особами та органами державної влади без необхідності особистого звернення.

Відповідно до п. 5 Положення, портал «Дія» виконує низку основних завдань. Зокрема, до них належить надання електронних публічних послуг, у тому числі комплексних послуг, автоматизація процесів обробки інформації, забезпечення доступу до державних реєстрів, а також можливість отримання користувачами результатів адміністративних процедур в електронній формі. Окремо передбачено забезпечення електронного листування між користувачами та суб'єктами надання послуг, що підвищує оперативність комунікації.

Згідно з п. 6 Положення, портал «Дія» забезпечує функціональні можливості електронної ідентифікації та автентифікації користувачів, що дозволяє підтверджувати особу через електронні засоби без фізичної присутності. Також передбачено використання кваліфікованого електронного підпису, автоматичне заповнення заяв, перевірку даних, а також формування електронних відображень документів, які можуть використовуватися користувачами у цифровому форматі.

Тут варто зупинитись на понятті використання кваліфікованого електронного підпису. КЕП створюється на основі кваліфікованого сертифіката електронного підпису, є надійним засобом для підтвердження автентичності електронних документів та відповідності документа вимогам законодавства. Використовують КЕП у сферах, де велику роль відіграють питання безпеки наприклад: фінансові угоди, договори та угоди між компаніями, які підлягають нотаріальному посвідченню та/або державній реєстрації та при здійсненні правосуддя.

Відповідно до п. 8 Положення, користувачі порталу мають право безоплатно отримувати доступ до електронних послуг, зберігати цифрові

документи, подавати заяви, отримувати інформацію про стан розгляду звернень, а також користуватися функціями інформаційної підтримки. Таким чином, портал виступає інструментом забезпечення доступності адміністративних послуг у цифровому середовищі.

Згідно з п. 10 та п. 11 Положення, власником Порталу є держава в особі Міністерства цифрової трансформації України, яке забезпечує його розвиток, функціонування та захист інформаційних даних. Технічне адміністрування здійснюється державним підприємством «ДІЯ», яке відповідає за технічну реалізацію, модернізацію та безпеку системи.

Окремо, відповідно до п. 14 Положення, Портал «Дія» є інтегрованою системою, яка об’єднує різні цифрові компоненти, зокрема мобільний застосунок, електронний кабінет користувача, державні реєстри та інші інформаційні підсистеми, що забезпечують комплексне функціонування цифрових сервісів [55]. Положення детально характеризує портал «Дія» та дає можливість зрозуміти механізм та сутність його роботи.

Однією з перших послуг була можливість реєстрації транспортних засобів та отримання посвідчення водія в електронному вигляді [10, с. 170]. Згодом у «Дії» стали доступні послуги із різних сфер життя: освіта, охорона здоров’я, сім’я, соціальний захист, безпека та правопорядок, підприємництво, нерухомість, будівництво.

Зрозуміло, що портал був не ідеальним відразу і мав свої недоліки. Такі як складний механізм ідентифікації та авторизації, труднощі із залученням та використанням. Це вплинуло на те , що спочатку громадяни не довіряли цьому застосунку і не користувались ним [11, с. 176]. Але постійне вдосконалення його та ситуація в країні змінили ставлення громадян до онлайн-послуг.

В умовах повномасштабної війни особливого значення набуло подальше функціональне розширення цифрової платформи Дія, яка фактично трансформувалася із інструменту зручного доступу до адміністративних

послуг у критично важливий механізм забезпечення безперервності державного управління та комунікації з громадянами.

Станом на 2025 рік в «Дії» доступно понад 160 послуг, які надають громадянам та бізнесу (талиця 3.1.) створено 6,3 млн кабінетів та 23,7 млн користувачів [90].

Таблиця 3.1.

Доступні послуги в застосунку «Дія»

Громадянам	**Бізнесу**
Довідки та витяги	Земля, будівництво, нерухомість
Ліцензії та дозволи	Підприємництво
Здоров’я	Створення бізнесу
Пенсії, пільги та допомога	Дія.City
Репарації: міжнародний реєстр збитків	Ліцензії та дозволи
Земля, будівництво, нерухомість	Витяги та довідки
Сім’я	Бронювання
Підприємництво	Розмінування
ЄВідновлення	

Таблиця сформована на основі джерела: [14].

З огляду на масове переміщення населення, втрату або знищення паперових документів, а також обмежений доступ до фізичних центрів надання адміністративних послуг, цифрові документи, доступні у застосунку, набули особливої практичної значущості [10, с. 171]. Вони забезпечують можливість ідентифікації особи та підтвердження її правового статусу незалежно від місця перебування, що є критично важливим в умовах нестабільності та постійної зміни безпекової ситуації.

Тут варто розглянути поняття єДокумент. Постановою КМУ від 10.03.2022 року «Деякі питання застосування єДокумента в період дії воєнного стану» було закріплено, що єДокумент це документ, що посвідчує особу в період дії воєнного стану, у формі відображення в електронній формі інформації, що ідентифікує особу та міститься в паспорті громадянина України та/або в паспорті громадянина України для виїзду за кордон, та/або в посвідченні водія.

Стаття 6 Порядку застосування єДокумента в період дії воєнного стану встновила набір даних, який містить єДокумент: назва документа;

- реквізити (назва, серія та/бо номер) паспорта громадянина України або паспорта громадянина України для виїзду за кордон, або посвідчення водія;
- прізвище, власне ім’я, по батькові (за наявності) особи українською мовою та латинськими літерами;
- стать;
- громадянство (за наявності);
- дата народження;
- відцифрований образ обличчя особи (за наявності);
- реєстраційний номер облікової картки платника податків з Державного реєстру фізичних осіб - платників податків (за наявності);
- адреса зареєстрованого місця проживання та дата реєстрації (за наявності) [21].

Паралельно з цим держава оперативно адаптувала електронні сервіси до нових викликів, впроваджуючи інструменти, спрямовані на вирішення актуальних проблем громадян. Зокрема, було реалізовано можливість подання інформації про пошкоджене або зруйноване майно, оформлення статусу безробітного, отримання відповідних компенсацій, а також доступ до програм фінансової підтримки, у тому числі міжнародної допомоги для внутрішньо переміщених осіб [10, с.172]. Важливо, що значна частина цих процедур була

максимально автоматизована, що дозволило мінімізувати бюрократичні бар'єри та скоротити час отримання послуг.

Крім того, функціонал платформи було розширено у напрямі забезпечення громадянської участі та мобілізації ресурсів суспільства. Зокрема, реалізовано можливість здійснення фінансових внесків на підтримку обороноздатності держави та надання гуманітарної допомоги [11, с.178]. Такий підхід свідчить про еволюцію електронних сервісів від інструментів адміністративного обслуговування до повноцінної цифрової екосистеми взаємодії держави і суспільства.

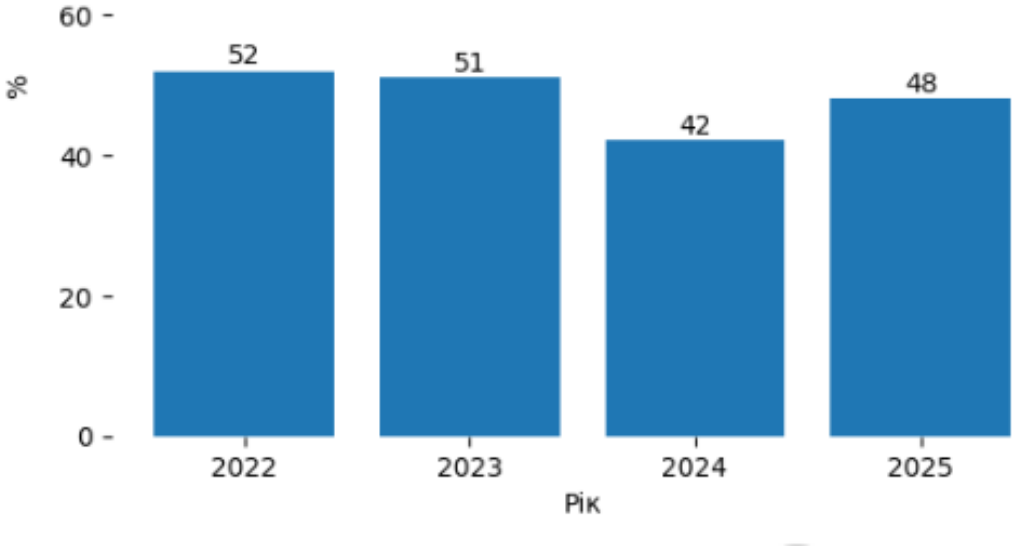
Отже з цього випливає, що «Дія» є дуже гнучким застосунком, що швидко адаптується до різних умов: «почалася пандемія COVID19 – запустили ковід-сертифікати про вакцинацію в Дії, які були офіційно визнані в ЄС, почалася війна і люди почали масово виїжджати із зони бойових дій без грошей та документів – запустили в Дії цифровий єДокумент та можливість у кілька кліків подати заяву про отримання виплат для ВПО, людям потрібно відбудовувати зруйноване під час війни житло – запустили послугу єВідновлення» – Михайло Федоров [14].

Для того аби краще зрозуміти рівень користування «Дією» варто проаналізувати щорічні звіти всеукраїнських опитувань, проведеними Київським міжнародним інститутом соціології на замовлення Програми розвитку ООН в Україні у партнерстві із Міністерством цифрової трансформації.

Перше на що варто звернути увагу – це відсоток користувачів «Дія» (діаграма 3.1.)

Діаграма 3.1.

Скільки відсотків українців використовують «Дія»



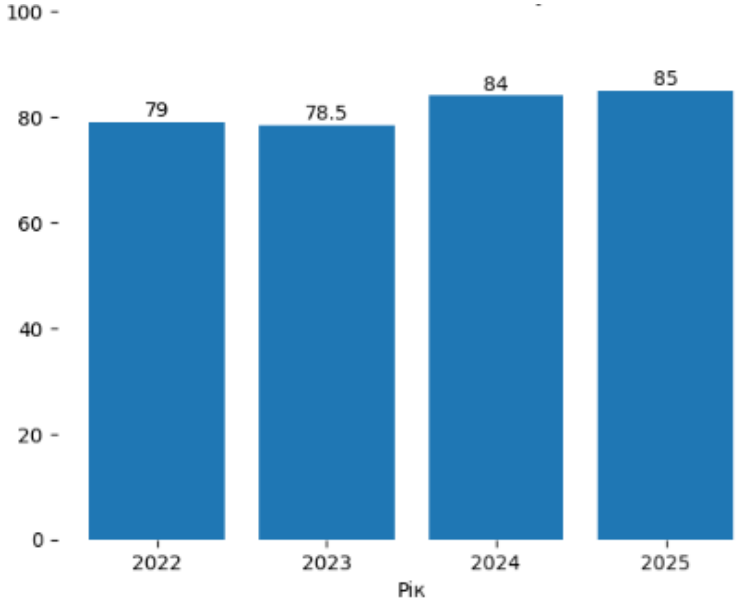
Діаграма сформована за допомогою штучного інтелекту, на основі джерел: [43], [44], [45], [46].

Загалом динаміка є стабільною і показує високий рівень зацікавленості громадян у цьому додатку.

Далі потрібно розглянути рівень задоволення користуванням додатком «Дія» (діаграма 3.2.)

Діаграма 3.2.

Позитивна оцінка «Дія» у %



Діаграма сформована за допомогою штучного інтелекту, на основі джерел: [43], [44], [45], [46].

З цього видно, що рівень задоволеності доволі високий і постійно зростає. Це зумовлено тим, що «Дія» завжди розвивається і додає нові послуги для громадян.

Однією з найбільш соціально значущих комплексних електронних послуг в Україні є сервіс «єМалятко», що функціонує в межах державної платформи цифрових послуг. Його запровадження є важливим етапом цифрової трансформації системи державного управління, оскільки спрямоване на спрощення процедур, пов'язаних із народженням дитини, та мінімізацію адміністративного навантаження на громадян.

Сутність послуги полягає в реалізації принципу «єдиного звернення», відповідно до якого за однією електронною заявою батьки можуть ініціювати отримання комплексу адміністративних послуг, необхідних після народження дитини [26]. Такий підхід дозволяє уникнути багаторазового звернення до різних органів державної влади та суттєво скорочує часові й організаційні витрати заявників.

Функціонально «єМалятко» забезпечує можливість одночасного отримання до десяти державних послуг, які надаються різними державними органами. Серед них виділяються базові (обов'язкові) та додаткові (опційні) послуги.

До базових належать: державна реєстрація народження дитини, визначення її походження, реєстрація в Державному реєстрі фізичних осіб-платників податків, визначення громадянства України та присвоєння унікального номера запису в Єдиному державному демографічному реєстрі, а також внесення інформації про дитину до електронної системи охорони здоров'я. Ці послуги формують первинний адміністративно-правовий статус новонародженої дитини [26].

Також варто розглянути послуги у соціальній сфері. Мова йде про Програму «єПідтрика», послуги якої доступні на порталі «Дія». У період воєнного стану Урядом України було запроваджено механізми фінансової

підтримки населення через програму «єПідтримка». Зокрема, у 2022 році передбачалася одноразова виплата у розмірі 6500 гривень для громадян, які втратили частину заробітної плати або можливість здійснювати трудову чи підприємницьку діяльність унаслідок бойових дій [84, с.423].

Окремим напрямом державної підтримки стало надання щомісячної допомоги внутрішньо переміщеним особам. Виплати призначалися громадянам, які були змушені залишити місце проживання через бойові дії або тимчасову окупацію територій Автономної Республіки Крим, міста Севастополя, а також низки областей України, що постраждали внаслідок збройної агресії. Допомога надавалася особам, інформація про яких була внесена до Єдиної інформаційної бази даних про внутрішньо переміщених осіб. Розмір щомісячних виплат становив 3000 гривень для дітей та осіб з інвалідністю і 2000 гривень для інших категорій внутрішньо переміщених осіб [84, с. 242].

Також у 2025 році надавалась послуга «Зимова єПідтримка», якою скористалось дуже багато українців. Лише за першу добу подали 2,5 мільйони заявок у «Дії». «Зимова єПідтримка стала наймасовішою послугою за всю історію. Лише за першу добу ми отримали 2,5 мільйони заявок у Дії, а за три місяці роботи програми –12 мільйонів заявок. Це також найшвидша послуга з отримання коштів у світі. Кілька кліків у Дії – і українці отримали допомогу від держави, яку можна витратити на певні товари та послуги, а також задонатити на підтримку Сил оборони» – зазначив Михайло Федоров [1].

Отже, в умовах воєнного стану електронні сервіси стали одним із найважливіших інструментів забезпечення доступності адміністративних послуг для населення. Через обмеження роботи державних установ, постійну небезпеку та масове переміщення громадян саме цифрові технології дозволили підтримувати безперервний зв’язок між державою та суспільством. У таких умовах платформа «Дія» фактично перетворилася не лише на сервіс

для отримання документів чи довідок, а й на важливий механізм реалізації державної політики в кризовий період.

3.3. Напрями вдосконалення електронного врядування та практичні рекомендації щодо забезпечення доступності адміністративних послуг в умовах воєнного стану

Підчас війни держава стикнулись із низкою нових проблем: кібератаки, пошкодження інфраструктури, цифрова нерівність, переміщення населення, необхідність взаємодіяти із громадянами дистанційно. І виходячи із цього актуальним є розробка рекомендацій для удосконалення електронного врядування.

На нашу думку варто впровадити адаптивне управління кіберризиками. Тобто прогнозування сценаріїв кібератак, передбачення потенційних загроз та розробка механізмів реагування на різні типи кіберінцидентів. Науковець Горун О.Ю. у своїй статті виокремив напрями вдосконалення системи кіберзахисту України, науковець рекомендує розробити протоколи кібербезки, що будуть містити алгоритми дій у різних випадках, а також під час відключень електроенергії чи втрати доступу до цифрових систем [64, с. 134]. Важливо для забезпечення кіберстійкості є і розвиток системи кіберосвіти. Потрібно впровадити обов’язкове навчанням кібергігієні для державних службовців, працівників сектору безпеки, а також для пересічних громадян.

Неврегульованим залишається питання кримінальної відповідальності за скоєні кіберзлочини. Потрібно внести відповідні зміни до Кримінального кодексу України та Закону України «Про основні засади забезпечення кібербезпеки України» [64, с. 135].

Також важливим аспектом є інституційне забезпечення, оскільки в Україні немає окремого спеціалізованого органу з питань кібербезпеки, доцільно було б його створити.

Для того аби підвищити кіберстійкість систем електронного врядування в Україні варто розвивати міжнародне співробітництво щодо захисту державних цифрових ресурсів та інфраструктури. Міжвідомча робоча група з питань залучення міжнародної допомоги у сфері кібербезпеки підтримала ряд проєктів Державного центру кіберзахисту Держспецзвязку, в межах міжнародної ініціативи «Талліннський механізм» [30]. Головною метою цих проєктів є забезпечення захисту державних інформаційних систем від кібератак та безперервності функціонування.

Підтримку отримали 4 проєкти. В рамках першого будуть оцінювати стан захищеності інформаціно-комунікаційних систем державних органів через проведення тестування на проникнення [30]. Це десть змогу побачити вразливості ресурсів та завчасно усунути можливі ризики несанкціонованого доступу. Наступна ініціатива присвячена захищеному доступу органів влади до Інтернету. Тут планується оновлення технічного обладнання та посилення захисту від мережевих атак та кіберінцидентів. Також підтримали проєкт, що стосується розвитку систем резервного зберігання державних інформаційних ресурсів. Планується розширення обсягів сховищ резервних копій та захищеної передачі великих об’ємів даних між резервними майданчиками [30].

Якщо говорити про нормативно-правове забезпечення електронного врядування то спостерігається його фрагментарність, оскільки механізми його функціонування закріпленні у багатьох різних документах, часто шляхом внесення змін у вже існуючий нормативно-правовий акт. Тому для підвищення ефективності електронного врядування, що особливо важливо під час воєнного стану, варто створити окремий закон, наприклад, «Про

електронне врядування» чи кодекс який би комплексно закріплював усі аспекти пов’язані із цифровізацією держави.

Ці думки також висвітленні у роботі Стиранка М.Б.. Науковець пропонує створити Цифровий кодекс України, в якому буде закріплено: засади регулювання цифрових прав; гарантії особистої цифрової свободи; правила обробки та управління даними у публічних інформаційних ресурсах і реєстрах; порядок емісії цифрових активів; режим збирання, використання й захисту персональних даних; регулювання обробки й управління даними, що створюються або зберігаються коштом державних і місцевих бюджетів; правила функціонування цифрових платформ та екосистем і нормативної взаємодії суб’єктів приватного та публічного права; порядок збирання і зберігання біометричних даних та застосування технологій біометричної ідентифікації [87]. На нашу думку кодекс варто доповнити положеннями про функціонування систем електронного врядування під час воєнного стану та використання штучного інтелекту для обробки даних.

Щодо питання розвитку цифрової інфраструктури, то перше що потребує вдосконалення це теле-комунікаційна інфраструктура. Оскільки під час повномасштабного вторгнення значна частина такої інфраструктури була знищена, виникли проблеми з інтернет покриттям, що у свою чергу обмежує доступ до електронних публічних послуг. Тому важливо розбудовувати інтернет-інфраструктуру, щоб доступ до мережі мали усі населені пункти. Також варто оновити матеріально-технічну базу органів місцевого самоврядування та ЦНАПів, оскільки у багатьох вона є застарілою.

Важливо також постійно розвивати цифрову грамотність громадян. Хоча динаміка в цій сфері є позитивною і з кожним роком кількість населення, що не володіє цифровими навичками все менша, технології не стоять на місці, впроваджуються все нові й нові методи взаємодії держави із громадянами. Тому потрібно впроваджувати освітні програми як для громадян так і для державних службовців та посадових осіб органів місцевого самоврядування.

Оскільки до цього часу є посадовці які не володіють потрібними знаннями з електронного врядування.

Тепер перейдемо до адаптації е-сервісів для людей з особливими потребами. Це люди із порушення слуху, зору, опорно-рухового апарату, людей похилого віку. Тут варто розглянути Міжнародні рекомендації, щодо доступності веб-ресурсів для ус9595іх груп користувачів WCAG (Web Content Accessibility Guidelines) 2.1.. У настановах закріплено, що потрібно адаптовувати інтерфейси для програм екранного читання, використовувати контрастні кольорові системи, надавати можливість змінювати масштаб тексту, додавати голосову навігацію та субтитри для відеоматеріалів, а також спростити режим користування сервісами [50].

Перспективним напрямом розвитку е-врядування є інтеграція штучного інтелекту для обробки даних та прийняття рішень. Це питання досліджує багато науковців. Так М. Холод, Н. Костенюк, О. Воронов вважають, що використання штучного інтелекту в публічному управлінні допоможе автоматизувати рутинні операції, швидше опрацьовувати великі об’єми інформації, робити стратегічні прогнози, наприклад, передбачити наслідки реформ ще до їх впровадження [95, с. 310]. Це збільшить рівень прозорості, оскільки рішення будуть прийматись шляхом заданих алгоритмів, без людського фактора.

І.С. Арделян, Х.В. Плецян визначають, що основною метою впровадження штучного інтелекту в публічному управління є допомога в різних його сферах. Наприклад: розподіл хворих у сфері охорони здоров’я, встановлення кількості безробітних, розробка маршрутів для безпілотників, відповіді на звернення громадян, відслідкування шахрайства, прийняття рішення, що стосуються соціальної допомоги [4, с. 4]. Це свідчить про те, що використовувати штучний інтелект можна в різний спосіб та в різних сферах.

Важливим аспектом в цьому напрямі є нормативно-правове регулювання впровадження штучного інтелекту. Науковиця Л.О. Сімонцева у

своїй статті аналізує європейський підхід у цій сфері. Загальний регламент про захист даних (GDPR) фіксує базові норми, щодо автоматизованої обробки персональних даних. Також визначає, що будь-яка особа має право на перегляд рішення людною, а не лише алгоритмами, якщо це рішення має правові наслідки чи є дуже важливим для неї. Наступний документ – це Регламент про штучний інтелект (AI Act), для систем штучного інтелекту, що використовуються у високо ризикованих сферах: соціальні послуги, використання публічних ресурсів, контроль та правозастосування. В цих випадках регламент встановлює високі вимоги прозорості, якості даних, документації, закріплює обов'язковість проведення перевірок таких систем. Рекомендація ЮНЕСКО щодо етики ШІ встановлює, що штучний інтелект у публічному управлінні повинен допомагати збільшити доступність послуг, має бути спрямованим не лише на спрощення процедур, економію часу чи ресурсів, а й на соціальне благо. Також закріплює для держави обов'язок контролю, створення процедур етичної оцінки та залучення різних груп стейкхолдерів для розробки правил користування штучним інтелектом [82].

В Україні нормативно-правова основа в цьому аспекті є не розвиненою. Важливо не лише вносити зміни до законів чи постанов, а розробити власний регламент щодо використання штучного інтелекту, щоб врегулювати усі сторони цього процесу.

Корисним використання штучного інтелекту є на перспективу післявоєнної відбудови. Цим питанням цікавились Н. Костенюк та О. Воронов. У своїй роботі вони визначили, що держава після війни стикнеться із рядом проблем, що стосуються відновлення інфраструктури, соціальної та економічної сфери. І в цьому контексті системи штучного інтелекту допоможуть відновити реєстри населення, розподілити гуманітарну допомогу та інші ресурси, спрогнозувати бюджет на відновлення інфраструктури [38].

Отже, електронне врядування в Україні є доволі розвиненим, але все таки має певні недоліки, тому ми пропонуємо впроваджувати механізми

адаптивного управління кіберзагрозами, для ефективного усунення та передбачення проблем, також допрацювати законодавство в сфері електронного врядування та кіберзахисту, а саме розробити окремі нормативно-правові акти. Також потрібно модернізувати матеріально-технічну базу, особливо в місцевих органах влади та теле-комунікаційну інфраструктуру, а саме забезпечити стабільний доступ до мережі Інтеренет для усіх територій. Важливо підвищувати рівень цифрової грамотності громадян шляхом освітніх програм. На нашу думку особливо чутливим є питання інклюзивності е-послуг, тому пропонуємо адаптувати веб-сервіси для людей з особливими потребами, тобто додавати субтитри до відеоматеріалів, додати голосовий супровід, використовувати контрастні кольори та надавати можливість масштабувати текст. Перспективним напрямом розвитку е-врядування вважаємо використання штучного інтелекту, особливо в період післявоєнної відбудови.

Висновки до розділу 3

Отже, забезпечення доступності адміністративних послуг в умовах воєнного стану стало одним із важливих напрямів діяльності держави, адже саме від ефективності системи публічного управління залежала можливість громадян реалізовувати свої права в кризових умовах.

Дослідження показало, що в умовах воєнного стану значна частина процедур була спрощена, а електронний формат став одним із основних способів взаємодії громадян з органами влади. Це дало можливість забезпечити безперервність надання послуг навіть в умовах безпекових обмежень, переміщення населення та нестабільної роботи окремих державних установ.

Водночас війна продемонструвала, що цифровізація публічного управління має не лише технологічне, а й стратегічне значення. Електронні сервіси забезпечили оперативність державного реагування та підтримку населення, однак одночасно виявили проблеми нерівномірного цифрового

розвитку громад і складності доступу до онлайн-послуг для окремих категорій населення.

Таким чином, досвід України засвідчив, що поєднання цифрових технологій, нормативної гнучкості та оперативного реагування органів влади стало необхідною умовою забезпечення доступності адміністративних послуг і стабільного функціонування держави в умовах воєнного стану.

Важливо не зупинятись на досягнутому, а постійно розвивати системи е-врядування, реагувати на слабкі зони та проваджувати нові технології.

ВИСНОВКИ

У кваліфікаційній роботі здійснено комплексне дослідження особливостей функціонування електронного врядування в Україні в умовах воєнного стану, а також проаналізовано виклики цифрової безпеки та проблеми забезпечення доступності адміністративних послуг. Отримані результати дали змогу виконати поставлені завдання та сформулювати такі висновки:

- електронне врядування забезпечує безперервність діяльності органів публічної влади, підтримує взаємодію держави з громадянами та дозволяє надавати адміністративні послуги навіть в умовах бойових дій, руйнування інфраструктури й масового переміщення населення. Водночас встановлено, що воєнний стан прискорив цифровізацію державного управління та підвищив рівень використання електронних сервісів населенням.
- в Україні сформована комплексна система правового регулювання у сфері інформаційних відносин, електронних комунікацій, захисту персональних даних та кібербезпеки. Після початку повномасштабного вторгнення законодавство було оперативно адаптоване до нових умов шляхом прийняття спеціальних нормативно-правових актів і внесення змін до чинного законодавства. Основна увага держави була зосереджена на забезпеченні безперервності функціонування державних інформаційних систем, посиленні кіберзахисту, використанні хмарних технологій та захисті державних реєстрів.
- визначено основні види кіберзагроз: деструктивні атаки, фішингові атаки, кібершпигунство, інформаційно-психологічні операції Дослідження показало, що поряд із традиційними видами атак активно поширюються нові форми кіберзагроз, зокрема атаки типу «zero-click», технології швидкого викрадення даних («steal & go») та використання штучного інтелекту для створення шкідливого програмного забезпечення.

- ефективний захист персональних даних забезпечується завдяки комплексному поєднанню правових, організаційних і технічних заходів. До основних механізмів належать шифрування даних, багаторівнева автентифікація користувачів, резервне копіювання інформації, обмеження доступу до державних реєстрів, використання хмарних технологій та постійний моніторинг кіберінцидентів
- до ключових проблем доступності адміністративних послуг віднесено руйнування цифрової та енергетичної інфраструктури, нестабільний доступ до мережі Інтернет, тимчасове обмеження доступу до державних реєстрів, низький рівень цифрової грамотності окремих категорій населення, а також труднощі отримання послуг внутрішньо переміщеними особами, громадянами на тимчасово окупованих територіях та особами, які перебувають за кордоном. Встановлено, що воєнний стан значно посилив потребу у дистанційних формах взаємодії громадян із державою.
- важливу роль у забезпеченні доступності послуг відіграють цифрові платформи та електронні сервіси, насамперед портал і застосунок «Дія». Саме завдяки розвитку електронних сервісів громадяни отримали можливість дистанційно оформлювати документи, отримувати соціальну допомогу та користуватися іншими адміністративними послугами незалежно від місця перебування. Також встановлено, що важливими інструментами забезпечення прозорості діяльності органів влади та запобігання корупції залишаються відкриті дані та електронна система публічних закупівель Prozorro.
- були розроблені рекомендації щодо вдосконалення нормативно-правової бази в сфері кібербезпеки та е-врядування, а саме створення окремих нормативно-правових актів, адаптація веб-ресурсів для людей з особливими потребами, модернізація матеріально-технічної бази органів влади. Встановлено, що перспективними напрямами є взаємодія із міжнародними організаціями та інтеграція штучного інтелекту в публічному управлінні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 14,4 млн українців скористалися Зимовою єПідтримкою – це наймасовіша програма в історії України. *Дія*. URL: https://diia.gov.ua/news.

2. Corruption perceptions index. *Transparency international the global coalition against corruption*. URL: https://www.transparency.org.

3. European union agency for cybersecurity. ENISA sectorial threat landscape. 2025. 42 p.

4. Адрелян І., Плецан Х. Методи застосування штучного інтелекту для аналізу соціально-економічних даних у публічному управлінні. *Публічне управління і політика*. 2025. № 5. С. 1–11.

5. Алюшина Н. Публічний звіт голови НАДС. Киїів, 2023. 44 с.

6. Андрій Магера. Електронне голосування для України – перспектива далекого майбутнього. Але точно не сьогодні. *Центр політико правових-реформ*. URL: https://pravo.org.ua.

7. Була Р. Роль відкритих даний у розвитку цифрової держави. *Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління*. 2025. № 1. С. 31–38.

8. Вплив війни на сферу адміністративних послуг та рекомендації на майбутнє. *UPLAN*. URL: https://uplan.org.ua.

9. Горун О. Кіберзагрози України в умовах агресії РФ. Інформація і право. 2025. № 3. С. 131–139.

10. Дармостук Д. Цифрові платформи для надання державних послуг: досвід України та світу. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. № 9. С. 168–175.

11. Дембіцький С., Злобіна О., Костенко Н. Українське суспільство в умовах війни : монографія. Київ : Ін-т соціології НАН України, 2022. 410 с.

12. Державна служба спеціального зв’язку та захисту інформації України. Російські кібер-операції аналітика за І півріччя 2025 року. Київ, 2025. 24 с.

13. Державна служба спеціального зв'язку та захисту інформації України. Що таке програма-стилер, якої шкоди вона може завдати комп'ютеру?. URL: https://www.cip.gov.ua/ua/faqs/sho-take-programa-stiler-yakoyi-shkodi-vona-mozhe-zavdati-komp-yuteru.

14. Державні послуги онлайн. Дія. URL: https://diia.gov.ua/.

15. Деякі питання внесення інформації до паспорта громадянина України для виїзду за кордон : Постанова від 28.02.2022 № 170-2022-п. URL: https://zakon.rada.gov.ua.

16. Деякі питання державної реєстрації та функціонування єдиних та державних реєстрів, держателем яких є Міністерство юстиції, в умовах воєнного стану : Постанова від 06.03.2022 № 209-2022-п. URL: https://zakon.rada.gov.ua.

17. Деякі питання державної реєстрації шлюбу в умовах воєнного стану : Постанова від 07.03.2022 № 213-2022-п. URL: https://zakon.rada.gov.ua.

18. Деякі питання допуску водіїв до керування транспортними засобами : Постанова від 03.03.2022 № 184-2022-п. URL: https://zakon.rada.gov.ua.

19. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану : Постанова від 12.03.2022 № 263. URL: https://zakon.rada.gov.ua

20. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки : Постанова від 23.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-п#Text.

21. Деякі питання застосування єДокумента в період дії воєнного стану : Постанова від 10.03.2022 № 248-2022-п. URL: https://zakon.rada.gov.ua.

22. Деякі питання надання допомоги в рамках Програми "єПідтримка" : Постанова від 09.12.2021 № 1272-2021-п. URL: https://zakon.rada.gov.ua.

23. Деякі питання оперативно-технічного управління електронними комунікаційними мережами в умовах надзвичайної ситуації, надзвичайного або воєнного стану : Постанова від 24.01.2025. URL: https://zakon.rada.gov.ua/laws/show/75-2025-п#Text.

24. Дівак А. Електронне урядування в умовах воєнного стану : перспективи цифровізації кризового управління. *Юридичний науковий електронний журнал*. 2025. № 2. С. 217–220.

25. ДЦКЗ Держспецзв'язку. Про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (СВВ) за 2025 рік. 2025. 7 с.

26. єМалятко. Дія. URL: https://diia.gov.ua.

27. Зайцев М., Демченко Р. В., Володченков О. Діджиталізація публічного управління в умовах воєнного стану та повоєнного відновлення. *Вісник ПДАУ (Публічне управління та адміністрування)*. 2025. № 3. С. 44–48.

28. Закрицька В. Д., Кононенко В. В. Електронне врядування як інструмент підвищення рівня прозорості діяльності органів державної влади. Наука і молодь у XXI сторіччі : Зб. матеріалів конф., м. Полтава, 10 листоп. 2025 р. Полтава, 2025. С. 621–623.

29. Закрицька В., Лазор О. Криза довіри до органів деражваної влади: як ефективна комунікація допомагає її подолати. *Розбудова доброчесності та комплаєнсу в Україні: виклики і перспективи євроінтеграції* : Зб. матеріалів Всеукр. конф. з міжнар. участю, м. Вінниця, 27 берез. 2025 р. Вінниця, 2025. С. 89–90.

30. Затверджено чотири проєкти Держспецзв'язку для реалізації в межах Талліннського механізму. *Державна служба спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/news/zatverdzheno-chotiri-proyekti-derzhspeczv-yazku-dlya-realizaciyi-v-mezhakh-tallinnskogo-mekhanizmu.

31. Індекс сприйняття корупції–2025. *Transparency international Ukraine*. URL: https://ti-ukraine.org.

32. Кірієнко В. Захист персональних даних як аспекту національної безпеки в умовах збройного конфлікту. Юридичний науковий електронний журнал. 2024. № 1. С. 398–400.

33. Ковальчу В. Адаптація надання адміністративних послуг до умов воєнного стану. *Юридичний вісник*. 2024. № 1. С. 273–281.

34. Колосовський Є., Круць Є. Сучасний стан кібербезпеки України в умовах воєнного періоду. Юридичний науковий електронний журнал. 2023. № 12. С. 402–406.

35. Кондратьєва К. Значення правового регулювання е-врядування для національної безпеки України в умовах воєнного стану. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*. 2024. Т. 2, № 16. С. 68–72.

36. Кондратьєва К. Портал "Дія" як ефективний інструмент е-врядування під час війни. Публічна політика і державне управління в умовах війни : Зб. матеріалів конф., м. Вінниця. 2024. С. 82–86.

37. Кононенко В.В., Дзевелюк М.В. Технології електронної демократії у роботі органів місцевого самоврядування в україні як інструменти запобігання корупції. Розбудова доброчесності та комплаєнсу в Україні: виклики і перспективи євроінтеграції : збірник матеріалів Всеукраїнської конференції з міжнародною участю (м. Вінниця, 27 березня 2025 р.). Вінниця : ТОВ «Друк», 2025. 310 с. С. 133-136. 167.

38. Костенюк Н., Воронов О. Можливості оптимізації публічного управління України за допомогою штучного інтелекту: перспективи для післявоєнної відбудови. *Теоретичні та прикладні питання державотворення*. 2025. № 34. С. 148–155.

39. Кравцов Д. Актуальні проблеми під час воєнного стану у сфері надання адміністративних послуг. *Київський часопис права.* 2025. № 2. С. 239–242.

40. М-во цифрової трансформації України. Дослідження цифрової та ШІ - грамотності в Україні. 2025. 102 с. URL: https://osvita.diia.gov.ua.

41. М-во цифрової трансформації України. Цифрова грамотність населення України. 2019. 211 с. URL: https://osvita.diia.gov. .

42. М-во цифрової трансформації України. Цифрова грамотність населення України. 2021. 134 с. URL: https://osvita.diia.gov.ua/uploads/0/2625-doslidzenna_2021_ukr.pdf.

43. М-во цифрової трансформації. Думки і погляди населення України щодо державних електронних послуг. 2022. 58 с.

44. М-во цифрової трансформації. Думки і погляди населення України щодо державних електронних послуг. 2024. 67 с.

45. М-во цифрової трансформації. Думки і погляди населення України щодо державних електронних послуг. 2025. 58 с.

46. М-во цифрової трансформації. Думки і погляди населення України щодо електронних державних послуг. 2026. 56 с.

47. Медведенко І. Електронне врядування: міжнародний досвід та перспективи для України. *Український економічний часопис*. 2024. № 6. С. 52–58.

48. Мельник В. Особливості надання адміністартивних послуг органами публічної адміністрації в умовах дії правового режиму воєнного стану: організаціно-правовий аспект. *Приватне та публічне право*. 2024. № 1. С. 74–80.

49. Міжнародна хартія відкритих даних. *Верховна Рада України*. URL: https://data.rada.gov.ua.

50. Міжнародні настанови із вебдоступності WCAG 2.1 відтепер доступні українською. *UNDP*. URL: https://www.undp.org.

51. Міляєва М., Сліпчук Ю. Сучасний стан нормативно-правового забезпечення розбудови електронного врядування в Україні. *Право та державне управління*. 2024. № 2. С. 257–268.

52. Набори даних. *Дія*. URL: https://data.gov.ua/dataset.

53. Оперативний центр реагування на кіберінциденти. *Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України*. URL: https://scpc.gov.ua/uk/soc.

54. Пальчик М., Шкрібляк К., Березделький Ю. Актуальні проблеми захисту персональних даних як напряму забезпечення національної безпеки України в умовах війни. Електронне наукове видання «Аналітично-порівняльне правознавство». 2025. № 6. С. 425–435.

55. Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг : Постанова від 04.12.2019 № 1137-2019-п. URL: https://zakon.rada.gov.ua.

56. Прес-офіс М-ва. Від стартапу до ІТ-компанії: як Мінцифра побудувала найзручнішу цифрову державу. *Міністерство цифрової трансформації України*. URL: https://thedigital.gov.ua.

57. Пресслужба ДСА України. Державна судова адміністрація України в тестовому режимі відновила доступ до ЄДРСР. *Державна судова адміністрація України*. URL: https://dsa.court.gov.ua .

58. Про адміністративні послуги : Закон України від 06.09.2012 № 5203-VI. URL: https://zakon.rada.gov.ua.

59. Про внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних : Закон України від 09.04.2015 № 319-VIII. URL: http://zakon.rada.gov.ua .

60. Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів : Закон України від 15.03.2022 № 2130-IX. URL: https://zakon.rada.gov.ua .

61. Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації : Закон України від 01.12.2022 № 2801-IX. URL: https://zakon.rada.gov.ua .

62. Про внесення змін до деяких законодавчих актів України щодо забезпечення умов для відновлення та розвитку електронних комунікаційних мереж : Закон України від 16.08.2022 № 2530-IX. URL: https://zakon.rada.gov.ua .

63. 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 від 03.05.2022 № 2240-IX. URL: https://zakon.rada.gov.ua .

64. Про внесення змін до Закону України "Про звернення громадян" щодо електронного звернення та електронної петиції : Закон України від 02.07.2015 № 577-VIII. URL: http://zakon.rada.gov.ua .

65. Про внесення змін до постанови Кабінету Міністрів України від 6 березня 2022 р. № 209 : Постанова від 24.03.2022 № 364. URL: https://zakon.rada.gov.ua .

66. Про впорядкування відносин з державної реєстрації народження та отримання документів про народження в умовах воєнного стану : Наказ від 03.09.2022 № z1009-22. URL: https://zakon.rada.gov.ua.

67. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua .

68. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua.

69. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних : Постанова від 21.10.2015 № 835-2015-п. URL: https://zakon.rada.gov.ua.

70. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua.

71. Про звернення громадян : Закон України від 01.10.1996 № 393/96-ВР. URL: http://zakon.rada.gov.ua .

72. Про зупинення строків надання адміністративних послуг та видачі документів дозвільного характеру : Постанова від 28.02.2022 № 165-2022-п. URL: https://zakon.rada.gov.ua.

73. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

74. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua.

75. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua.

76. Про правовий реим воєнного стану : Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua.

77. Про схвалення Концепції розвитку електронного урядування в Україні : Розпорядж. від 20.10.2017. URL: https://zakon.rada.gov.ua .

78. Про хмарні послуги : Закон України від 17.02.2022 № 2075-IX. URL: http://zakon.rada.gov.ua .

79. Прозорі міста. Електронні сервіси: як міста проходять євротест на прозорість?. *TrancparentCities*. URL: https://transparentcities.in.ua.

80. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) : Регламент від

27.04.2016 № 984_008-16. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

81. Роз'яснення законодавства у сфері ЕДП. *Центральний засвідчувальний орган*. URL: https://czo.gov.ua.

82. Сімонцева Л. Штучний інтелект та автоматизоване прийняття рішень у публічному управління в умовах євроінтеграції. *Таврійський науковий вісник*. 2025. № 6. С. 90–101.

83. Сливка М., Гінда А. Правове регулювання надання електронних адміністративних послуг. *Вісник Національного університету "Львівська політехніка"*. 2021. № 3. С. 195–202.

84. Соловйова О., Ковальчук Д., Кундій А. Адміністративні послуги в умовах воєнного стану в Україні. *Юридичний науковий електронний журнал*. 2022. № 5. С. 421–425.

85. Сорокіна А. Цифровізація як фактор підвищення економічної стійкості державного сектору. *Держава та економіка*. 2025. № 5. С. 24–38.

86. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020–2021 років / Л. Бєлкін та ін. Scientific works of national aviation university series: law journal «air and space law». 2022. Т. 3, № 64. С. 78–86.

87. Стиранка М. Нормативне регулювання використання цифрових сервісів якінструменту здійснення електронного урядування. *Київський часопис права.* 2026. № 1. С. 270–277.

88. Тимошенко Т. А., Кононенко В. В. Реалізація концепції сервісної держави як один із механізмів запобігання корупції. Розбудова доброчесності та комплаєнсу в Україні: виклики і перспективи євроінтеграції : збірник матеріалів Всеукраїнської конференції з міжнародною участю (м. Вінниця, 27 березня 2025 р.). Вінниця : ТОВ «Друк», 2025. С. 277-279.

89. Тихонова Д. Адміністративні послуги під час воєнного стану. *Poltava Law Review*. 2023. № 2. С. 40–58.

90. Ткаліч О. Сьогодні українцям у порталі "Дія" доступні вже понад 160 державних послуг, а у 2026 очікується ще більше нововведень. *Соцпортал*. URL: https://socportal.info/ua.

91. Торчинець М. 6 тисяч кібератак проти України здійснили у 2025 році, на 37% більше ніж у попередньому – РНБО. ain. URL: https://ain.ua/2026/02/20/za-2025-rik-proti-ukrayini-zdiisnili-priblizno-6000-kiberatak/.

92. Федоров М. Дія – державні послуги онлайн. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua.

93. Фурашев В. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162–175.

94. Фурашев В. Суть та визначення поняття "електронне урядування". *Правова інформатика*. 2012. Т. 3, № 35. С. 46–50.

95. Холод М., Костенюк Н., Воронов О. Перспективи використання штучного інтелекту в публічному управлінні : вплив на ефективність надання адміністративних послуг, процес ухвалення управлінських рішень та цифрому трансформацію. *Теоретичні та прикладні питання державотворення*. 2024. № 32. С. 307–314.

96. Шульган І., Слобода Н. Електронна система Prozorro як ефективний інструмент боротьби з корупцією. *Вісник Національного університету "Львівська політехніка"*. 2024. № 4. С. 348–364.

97. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану : Рішення від 18.03.2022. URL: https://zakon.rada.gov.ua.