

Тарнавський А. М.,

*аспірант кафедри публічного управління, туризму
та готельно-ресторанної справи*

*Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна*

ЦИФРОВІЗАЦІЯ ДЕРЖАВНИХ ПОСЛУГ ТА КІБЕРЗАГРОЗИ: ВИКЛИКИ ДЛЯ РЕГІОНАЛЬНОГО УПРАВЛІННЯ В УМОВАХ ВІЙНИ ТА ПІСЛЯВОЄННОГО ВІДНОВЛЕННЯ

Цифровізація державних послуг є ключовим напрямом модернізації регіонального управління, особливо в умовах війни та післявоєнного відновлення. Впровадження електронних сервісів, таких як «Дія», е-документообіг та онлайн-реєстри, оптимізує надання адміністративних послуг, підвищує оперативність управління, зменшує бюрократію та покращує прозорість.

Електронні сервіси підвищують оперативність державного управління, що критично в умовах війни. «Дія» стала не лише платформою цифрових документів, а й інструментом координації громадян і держави. Завдяки «ЕДокументу» можна підтвердити особу без паперових документів, а через застосунок подаються заявки на компенсацію, реєстрацію внутрішньо-переміщених осіб та соціальні виплати. Автоматизація процесів значно зменшує навантаження на регіональні адміністрації [7, с. 77].

Цифрові сервіси знижують корупційні ризики, забезпечують відкритість даних та громадський контроль. У післявоєнний період вони стануть основою для управління фінансуванням, залучення інвестицій та моніторингу реконструкції [2, с. 48].

Важливим фактором є баланс між доступністю та безпекою. Надмірне спрощення автентифікації може призвести до витоку даних, тому необхідне впровадження багатофакторної автентифікації та криптографічних методів. Високий рівень довіри громадян до цифрових послуг потребує прозорих механізмів захисту даних та публічного звітування про стан кібербезпеки [1, с. 56].

Україна стала ціллю масштабних кібератак, спрямованих на підлив державних інформаційних систем, викрадення даних і порушення роботи критичних платформ. Основними загрозами є DDoS-атаки, зломи реєстрів і витоки даних (рис. 1).



Рис. 1. Основні кіберзагрози для України

Джерело: сформовано автором [3, 5, 6]

DDoS-атаки (Distributed Denial of Service). Їхня мета – виведення з ладу державних електронних сервісів шляхом перевантаження серверів фіктивними запитами для тимчасового блокування доступу громадян до онлайн-послуг [8, с. 3].

Зломи державних реєстрів є також критичною загрозою. Це може призвести до стеження за громадянами, ідентифікації критичної інфраструктури та маніпуляції державними процесами [4, с. 270].

Витоки даних можуть виникати через атаки або слабкий рівень кібербезпеки, що загрожує національній безпеці, сприяючи дезінформації, шантажу та маніпуляціям. Кіберзлочинці використовують фішинг, вразливості програмного забезпечення та соціальну інженерію для отримання персональних даних [6, с. 96].

Одним із наймасштабніших прикладів стала атака на реєстри Міністерства юстиції України (грудень 2024), що паралізувала нотаріальні та реєстраційні послуги. Наслідки атаки зачепили широкий спектр державних сервісів, зокрема реєстр актів цивільного стану, реєстр юридичних осіб та фізичних осіб-підприємців, а також реєстр речових прав на нерухоме майно [4, с. 270].

Ще одним гучним інцидентом стала атака на мобільного оператора «Київстар» у грудні 2023 року. Унаслідок масштабного злому оператор зазнав серйозного збою, що спричинило відключення мобільного зв'язку, інтернету та сервісів для мільйонів українців. Відновлення інфраструктури зайняло більше тижня, а компанія втратила близько 40% своєї мережі. Даний інцидент продемонстрував, наскільки вразливою може бути критична інфраструктура України перед добре організованими кібератаками [10, с. 189].

Фінансовий сектор став мішенню хакерів, які атакували онлайн-банкінг, платіжні системи та здійснювали DDoS-атаки, що загрожувало стабільності банківської системи. Енергетична інфраструктура також зазнала значних кібератак у 2022–2023 роках, що призводило до відключень електроенергії, створюючи ризики для промисловості, транспорту та комунальних служб, а також потенційні гуманітарні кризи [3, с. 2].

В умовах війни та посилення кібератак на державні установи України особливо актуальним є питання зміцнення кібербезпеки регіонального управління. Захист інформаційних систем регіональних адміністрацій вимагає комплексного підходу, що включає впровадження резервних систем, навчання персоналу та застосування сучасних технологій захисту даних.

Одним із основних заходів забезпечення кіберстійкості є впровадження резервних реєстрів та систем зберігання даних. Це дозволяє швидко відновити доступ до критично важливої інформації у разі злому основних реєстрів або атак на інфраструктуру, як це було після кібератаки в грудні 2024 року [4, с. 271–272].

Низька цифрова грамотність службовців підвищує вразливість регіональних систем управління. Навчальні програми з кібербезпеки допоможуть зменшити ризики атак і витоку даних. Законодавство України передбачає фінансування таких заходів, зокрема створення відділів кібербезпеки в регіональних адміністраціях. Обов'язкові аудити безпеки дозволять виявляти вразливості та запобігати атакам [9, с. 43–44]. Додатковий захист забезпечує багатофакторна автентифікація із біометрією та одноразовими кодами [1, с. 56].

Захист конфіденційних даних забезпечується криптографічним шифруванням, яке запобігає викраденню та підміні інформації. Додатково використання файрволів і систем виявлення загроз дозволяє аналізувати трафік і вчасно ідентифікувати спроби злому державних серверів [1, с. 56].

Додатково необхідно запровадити механізми контролю за дотриманням кібербезпекових стандартів у місцевих адміністраціях. Це передбачає обов'язкову сертифікацію державних ІТ-систем та створення єдиної національної системи реагування на кіберінциденти [5, с. 29].

Цифровізація державних послуг модернізує регіональне управління, підвищуючи ефективність, прозорість і доступність, особливо в умовах війни. Електронні сервіси, такі як «Дія», спрощують адміністративні процеси, знижують бюрократію та корупційні ризики. Водночас кіберзагрози вимагають комплексного захисту: багатофакторної автентифікації, шифрування даних, навчання персоналу та створення резервних систем. Кіберстійкість критичної інфраструктури та створення відділів кібербезпеки є ключовими для ефективного управління.

Список використаних джерел:

1. Артёмова А. Ю., Ташлицький С. А. Роль кібербезпеки у цифровій трансформації державних підприємств. 2024. 53 с.
2. Белова І., Гомотюк А., Ярощук О. Цифрова трансформація управлінських та бізнес-процесів в Україні під час воєнного стану. *Економічний аналіз*. 2024. Том 34. № 1. С. 42–52. DOI: 10.35774/econp2024.01.042.
3. Дорогий Я. Ю., Цуркан В. В. Кібербезпека критичної інфраструктури під час військової загрози. 2024.
4. Котенок А. Г., Оніщенко Б. Кібербезпека та державні реєстри неухомості. 2025.
5. Кравцов О. В. Децентралізація і локалізація в контексті формування цифрової моделі стійкості. *Дніпровський науковий часопис публічного управління, психології, права*. 2025. № 5. С. 27–34. DOI: 10.51547/ppr.dp.ua/2024.5.3.
6. Крет О., Крет Р., Кундеус О. Система кібербезпеки як складова національної безпеки держави. *Grani*. 2024. Т. 27, № 5. С. 92–99. DOI: 10.15421/172496.
7. Пендальчук Є. В. Роль інформаційно-комунікаційних технологій у політичній комунікації: вплив цифрових платформ на маніпулювання громадською думкою. *Modern scientific journal (Сучасний науковий журнал)*. 2024. № 5 (3). С. 61–69. DOI: 10.36994/2786-9008-2024-5-9.
8. Ткач В. О. Вплив цифрових інструментів і кіберзахисту на розбудову Української державності та інтеграцію в світові освітні і технологічні процеси. *Forestry education and science: current challenges and development prospects*. 2024. October 23-25; Lviv, Ukraine. DOI: 10.36930/conf150.5.36.
9. Ткачук Д., Миколайчук М. Вартісний аналіз ресурсів як складова створення бюджетної стратегії задля забезпечення кібербезпеки в органах місцевого самоврядування України. *Collection of scientific papers «SCIENTIA»*. 2023. August 25; Zagreb, Croatia. С. 42–45.
10. Храмов С., Опірський І. Аналіз сучасного стану кібератак в Україні під час війни. *Ukrainian information security research journal*. 2024. Т. 26, № 1. С. 214–222. DOI: 10.18372/2410-7840.26.18842.