

УДК 342.9

DOI <https://doi.org/10.51989/NUL.2025.1.28>

ЦИФРОВІЗАЦІЯ НОТАРІАТУ ТА ДЕРЖАВНИХ РЕЄСТРІВ В УКРАЇНІ: НЕЗАХИЩЕНІСТЬ СИСТЕМИ ТА НЕОБХІДНІСТЬ ПЕРЕГЛЯДУ АДМІНІСТРАТИВНО-ПРАВОВОЇ ПОЛІТИКИ

Письменний Олександр Олександрович,
orcid.org/0009-0009-1065-3922
адвокат Ради адвокатів Дніпропетровської області,
аспірант
Дніпровського державного університету внутрішніх справ



Стаття присвячена розгляду деяких питань упровадження цифрових технологій у нотаріальну діяльність. Нотаріат в Україні постійно перебуває в динаміці розвитку та вдосконалення, що проявляється у змінах як системи, так і особливостей діяльності нотаріусів.

У статті зосереджено увагу на необхідності поступового введення нових форм і технологій у нотаріальну діяльність з метою гарантованої всебічної допомоги учасникам цивільних правовідносин. У процесі дослідження висвітлено окремі проблемні аспекти процедури впровадження та функціонування електронного нотаріату в Україні. Розглянуто доцільність запровадження та нормативного закріплення електронного нотаріату в Україні. Розглянуто актуальні зміни законодавства про нотаріат, пов'язані з розвитком електронного цивільного обороту.

Стаття присвячена характеристиці особливостей проблемних питань цифровізації нотаріату в умовах дії правового режиму воєнного стану в Україні. Актуальність даного питання пояснюється тим, що в сучасних умовах розвитку інформаційних технологій і їх практичного застосування в системі нотаріату маємо можливість отримувати якісно, оперативно та прозоро широкий спектр послуг, що надаються органами нотаріату в умовах дії правового режиму воєнного стану в Україні.

Одним із надважливих напрямів нотаріальної діяльності є допомога громадянам у реалізації їхніх законних прав у частині здійснення ними нотаріальних реєстраційних дій.

Наголошено на необхідності модернізації українського нотаріату та його погодження з європейськими стандартами. Установлено, що запровадження електронного нотаріату в рамках формування технологічної інфраструктури для гарантування безпеки та стабільності правовідносин в умовах електронного цивільного обороту переводить на новий рівень якість надання нотаріальних послуг і безпеку юридично значущих відомостей. Досліджено доцільність запровадження електронної форми документування, яка сприятиме спрощенню роботи нотаріусів. Також у процесі дослідження звернено увагу на те, що впровадження електронної системи нотаріату в Україні має відповідати всім установленим вимогам про захист інформації, бути забезпечене необхідними засобами захисту.

Автор доходить висновку, що для коректного функціонування електронного нотаріату робота електронного реєстру нотаріальних дій з іншими електронними реєстрами та сервісами, що діють, які застосовуються під час учинення нотаріальної дії, має бути узгодженою та технічно сумісною. Запропоновано внести зміни до чинного Закону України «Про нотаріат» – закріпити чіткий перелік нотаріальних дій, які можна буде вчиняти через електронні сервіси.

Ключові слова: цифровий нотаріат, цифровізація нотаріату, державні реєстри, кібербезпека, адміністративне право, хакерські атаки, цифрове управління, адміністративно-правове регулювання, Національна поліція.

Pysmennyi Olexsandr. Digitalization of notaries and state registries in Ukraine: system insecurity and the need to revise administrative law policy

The article is devoted to the consideration of some issues of the implementation of digital technologies in notarial activity. The notary in Ukraine is constantly in the dynamics of development

and improvement, which is manifested in changes both in the system itself and in the specifics of the activities of notaries.

The article focuses on the need for the gradual introduction of new forms and technologies in notarial activity in order to guarantee comprehensive assistance to participants in civil legal relations. In the course of the study, some problematic aspects of the procedure for the introduction and functioning of the electronic notary in Ukraine were highlighted. The expediency of introducing and normative consolidation of electronic notary in Ukraine is considered.

The expediency of introducing and normative consolidation of electronic notary in Ukraine is considered. Current changes in notary legislation related to the development of electronic civil turnover are considered.

The article is devoted to the characteristics of the problematic issues of digitization of the notary under the conditions of the legal regime of martial law in Ukraine.

The relevance of this issue is explained by the fact that in the modern conditions of the development of information technologies and their practical application in the notary system, we have the opportunity to receive qualitatively, quickly and transparently a wide range of services provided by the notary authorities in the conditions of the legal regime of martial law in Ukraine.

One of the most important areas of notarial activity is assistance to citizens in exercising their legal rights in terms of notarial registration.

The need to modernize the Ukrainian notary and bring it into line with European standards was emphasized. It was established that the introduction of electronic notary as part of the formation of a technological infrastructure to ensure the security and stability of legal relations in the conditions of electronic civil turnover brings the quality of notarial services and the security of legally significant information to a new level.

The expediency of introducing an electronic form of documentation, which will facilitate the work of notaries, has been investigated. Also, during the study, attention was drawn to the fact that the implementation of the electronic notary system in Ukraine must meet all established requirements for information protection and be provided with the necessary means of protection.

The author comes to the conclusion that for the correct functioning of the electronic notary, the work of the electronic register of notarial acts with other active electronic registers and services, which are used when performing a notarial act, must be coordinated and technically compatible.

It is proposed to make changes to the current Law of Ukraine "On Notaries" in the form of establishing a clear list of notarial actions that can be performed through electronic services.

Key words: *digital notary, digitization of notary, state registers, cyber security, administrative law, hacker attacks, digital management, administrative and legal regulation, National Police.*

Метою статті є проведення аналізу правових проблем цифровізації нотаріату та державних реєстрів, оцінювання рівня їхньої захищеності, а також формулювання конкретних рекомендацій щодо змін у правовому регулюванні цифрових сервісів, висвітлення проблеми законотворчої діяльності під час воєнного стану, недосконалості нашої правової системи та спроба визначити шлях вирішення цієї проблеми практичними напрацюваннями.

Саме тому актуальним є питання щодо можливості держави вироблення заходів із пристосування законодавства, пов'язаного із цифровізацією, до умов воєнного часу, з метою подальшого захисту прав учасників даного виду правовідносин.

Ю. Бисага [1], З. Журавльова у своїх публікаціях висвітлюють переваги впровадження електронного нотаріату, зокрема

створення єдиних електронних реєстрів і запровадження нотаріальних документів із QR-кодами, що значно спрощує процес пошуку інформації та мінімізує ризики шахрайства. В. Марченко [1], А. Ли́ла-Барська досліджують питання кібербезпеки в нотаріальній діяльності, наголошуючи на необхідності використання сучасних технологій захисту інформації, як-от системи на базі машинного навчання, для забезпечення електронного документообігу. Їхні статті також містять практичні рекомендації щодо підвищення цифрової грамотності нотаріусів і впровадження комплексних програм навчання.

Проте, незважаючи на наявність досліджень за цією темою, більшість питань щодо вільного цифрового простору в діяльності нотаріату залишаються відкритими в умовах воєнного стану й зазнають нововведень у законодавчих актах.

Постановка проблеми. Цифровізація державних послуг – це один із ключових пріоритетів реформування правової системи України. Електронні реєстри, цифровий документообіг і автоматизація нотаріальних процесів мали б забезпечити зручність, уніфікованість, швидкість і надійність надання адміністративних послуг. Однак, як показала практика, упровадження цифрових сервісів без належного захисту створює більше загроз, ніж можливостей.

Груднева кібератака 2024 р. на реєстри Міністерства юстиції України стала яскравим доказом системної проблеми – відсутності ефективних механізмів кібербезпеки. Масштабний злам державних реєстрів поставив під загрозу майнові права громадян, правомірність нотаріальних дій і загальну стабільність цифрового управління державою.

Ця ситуація вказує на критичну необхідність перегляду адміністративно-правової політики щодо цифровізації державних реєстрів, оскільки поточна система виявилася нездатною протидіяти загрозам. Незахищеність державних реєстрів як основна загроза цифровізації є важливою проблемою.

Фактичний стан державних реєстрів відображає українську систему цифрових державних реєстрів, яка формується з метою оптимізації роботи державних органів і забезпечення зручного доступу до інформації.

Основними реєстрами нотаріальної діяльності є:

- Державний реєстр речових прав на нерухоме майно;
- реєстри, що увійдуть до Єдиної державної електронної системи е-нотаріату;
- Реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань.

Проблема в тому, що всі ці системи мають централізовану архітектуру без належного багаторівневого кіберзахисту. Як наслідок, кібератака 2024 р. змогла зупинити їхню роботу, що призвело до паралізації нотаріальної та реєстраційної діяльності всіх сервісних центрів із надання послуг громадян. І це спричинило колапс в діяльності державного механізму, увесь процес реєстрації більшості послуг був

заблокований, що насамперед порушує права громадян.

Під час глибокого дослідження цього питання акцентую увагу на основних вразливих аспектах реєстрів. Аналіз причин успішного злому державних реєстрів показує такі ключові проблеми:

- відсутність національної політики кібербезпеки реєстрів;
- реєстри розроблялися як окремі системи, без комплексного підходу до безпеки;
- відсутність єдиного органу, відповідального за моніторинг атак і реагування на інциденти;
- недосконала система доступу до реєстрів надала можливість входу до системи через зламани сертифікати доступу;
- використання застарілих методів автентифікації;
- централізація та відсутність резервних механізмів;
- атака на центральну систему реєстрів автоматично паралізує всю систему;
- відсутність резервних автономних серверів, які могли б забезпечити безперервність роботи.

Акцентуємо увагу на тому, що натеper за адміністрування реєстрів відповідає ДП «НАІС», яке підпорядковане Міністерству юстиції України. Проте саме Міністерство юстиції не має належних інструментів для гарантування кібербезпеки, що робить ситуацію ще більш критичною.

На думку В. Марченка, впровадження цифрового нотаріату – неминучий процес для України. Однак для його ефективного функціонування потрібні системні дії, спрямовані на використання цифрових технологій як на користь професії, так і на користь наших громадян. Це дозволить оновити нотаріальний процес, зробити його більш зручним і зрозумілим, інтегрує нотаріуса у транснаціональні правовідносини та дасть можливість зміцнити позиції професії [1].

Система національного нотаріату перебуває в постійному процесі динамічного розвитку, що потрібно враховувати під час дослідження. Натеper у нотаріальній діяльності досить активно використовуються можливості електронних технологій, зокрема, для здійснення професійної діяльності нотаріуси мають доступ до Єди-

ного реєстру нотаріусів, Єдиного реєстру спеціальних бланків нотаріальних документів, Державного реєстру обтяжень рухомого майна, Спадкового реєстру, Єдиного реєстру довіреностей, Державного реєстру речових прав на нерухоме майно, Державного реєстру актів цивільного стану громадян, Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців і громадських формувань. Однак Е-нотаріат передбачає комплексне застосування електронних технологій [2, с. 42].

Держава створює різного роду реєстри та бази даних з метою забезпечення ефективного функціонування різних сфер суспільного життя. Ці реєстри та бази даних є важливим інструментом для збору, зберігання і оброблення інформації, яка потрібна для ухвалення рішень, контролю та надання різного роду послуг громадянам. Однією з головних причин створення реєстрів і баз даних є забезпечення ефективного контролю над різними процесами всередині державного управління. Наприклад, державні реєстри щодо населення дозволяють вести облік громадян, установлювати їхні права й обов'язки, а також забезпечувати доступ до соціальних послуг і допомоги. Такі реєстри також допомагають уникнути подвійного обліку, шахрайства та незаконного заволодіння майном громадян.

Окрім того, державні реєстри та бази даних допомагають забезпечити ефективне функціонування системи охорони здоров'я, освіти, соціального захисту й інших галузей. Завдяки цим реєстрам можна вести облік медичних даних, освітніх досягнень, соціальних пільг та інших важливих показників, що дозволяє забезпечити якісне надання послуг і аналізувати стан суспільства для ухвалення ефективних рішень. Також реєстри та бази даних є важливим інструментом для забезпечення взаємодії між різними державними органами й організаціями. Вони дозволяють обмінюватися інформацією, координувати дії та виконувати різні адміністративні процедури швидко й ефективно. Отже, створення реєстрів і баз даних є важливим елементом державного управління, який допомагає забезпечити ефективну роботу державних структур, контроль за процесами та надання послуг громадянам.

На жаль, не можна надати точну кількість реєстрів і баз даних, що існують в Україні, оскільки їхня кількість постійно змінюється і залежить від різних чинників, як-от законодавчі зміни, реформи та потреби державних органів. Україна має велику кількість реєстрів і баз даних, які охоплюють різні сфери життя, як-от населення, здоров'я, освіта, соціальний захист, фінанси, юстиція, багато інших. Державні органи й організації ведуть свої власні, так звані внутрішні реєстри та бази даних для забезпечення своєї діяльності та надання послуг громадянам.

Зі збільшенням кількості реєстрів і дій, які відбуваються у віртуальному полі, без попереднього паперового оформлення заяви чи клопотань щодо запитуваної послуги паралельно збільшується і кількість незаконних дій, які здійснюються або умисно особами, що мають сертифікований доступ до вказаних баз даних, що ст. 362 Кримінального кодексу України окреслено як злочин, або не навмисно, особами, які внаслідок неуважності або необізнаності порушили правила ведення відповідного реєстру, що затверджені належним чином і здебільшого оформленні як нормативно-правовий акт.

Така структура контролю не є поодиноким, але не розповсюджена на весь абсолютно інформаційний простір України як держави.

Загалом, контроль кібербезпеки державою є необхідним для захисту національної безпеки, особистих даних громадян, боротьби з кіберзлочинністю та забезпечення ефективного функціонування цифрового суспільства.

Проблема захисту реєстрів є відкритим питанням, наявність значних проблем нам проілюстровано кібератакою у грудні 2024 р. Коли було зламано доступ до реєстрів Мінюсту і майже 2 місяці не працювала система. Ця ситуація продемонструвала нам, що система державних реєстрів в Україні є вразливою, а поточні підходи до цифровізації не враховують основних принципів кібербезпеки.

Зупинимось більш детально на організації захисту даних, що містяться в реєстрах. Відповідно до наказу Міністерства внутрішніх справ України від 30 жовтня 2012 р. № 988 «Про організацію діяль-

ності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС» [4] основним завданням Управління є участь у формуванні та забезпеченні реалізації державної політики щодо запобігання та протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, мереж електрозв'язку, а також іншим кримінальним правопорушенням, учиненим з їх використанням.

Проаналізували опубліковані звіти про результати роботи Департаменту кіберполіції Національної поліції України у 2022–2023 рр.

У 2022 р. припинено діяльність 23 організованих груп і злочинних організацій, що діяли в кіберпросторі. До складу зазначених угруповань входив 81 учасник (23 – організатори, 51 – активний виконавець), якими вчинено 269 кримінальних правопорушень (зокрема, 240 тяжких і особливо тяжких), із яких: шахрайств – 178, 59 – у сфері використання електронно-обчислювальних машин, 12 – у сфері обігу наркотичних засобів, 3 – за ст. 255 (Створення, керівництво злочинною спільнотою, а також участь у ній) Кримінального кодексу України, 2 крадіжки, 3 – у сфері господарській діяльності (легалізації (відмивання) майна, одержаного злочинним шляхом), 1 привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем. Також у 2022 р. кіберполіцейськими здійснювалось супроводження 5 тис. кримінальних правопорушень, виявлено 2,3 тис. кіберзлочинів, повідомлено про підозру 1 тис. особам за вчинення 2,3 тис. кримінальних правопорушень. Затримано понад 100 кіберзлочинців, задокументовано та притягнуто до відповідальності 30 педофілів і 10 хакерів. До суду з обвинувальними актами скеровано 2,7 тис. кримінальних правопорушень за обвинуваченням 840 осіб [9].

У 2023 р. скеровано до суду кримінальні провадження щодо протиправної діяльності 42 організованих груп і злочинних організацій, що діяли в кіберпросторі. До складу зазначених угруповань входив 191 учасник, якими вчинено 731 кри-

мінальне правопорушення (зокрема, 547 тяжких і особливо тяжких), із яких: 438 шахрайств, 20 крадіжок, 12 за ст. 255 (Створення, керівництво злочинною спільнотою, а також участь у ній) Кримінального кодексу України, 11 сутенерств, 3 привласнення, розтрата майна, 46 – у сфері господарської діяльності, 33 – у сфері використання електронно-обчислювальних машин, 14 – у сфері службової діяльності, 7 – у сфері обігу наркотичних засобів, 147 – інші. Також у 2023 р. кіберполіцейськими здійснювалось супроводження понад 6,4 тис. кримінальних правопорушень, виявлено 3,6 тис. кіберзлочинів, повідомлено про підозру 1,7 тис. особам за вчинення 3,7 тис. кримінальних правопорушень. До суду з обвинувальними актами скеровано 4 тис. кримінальних правопорушень за обвинуваченням 1,3 тис. осіб [7; 8].

Логічним є факт, що з розвитком комп'ютерних технологій кількість злочинів стає дедалі більше. Навіть стовідсоткове розкриття злочинів не зменшить їхньої кількості, бо статистика розкриття злочинів не є протидією їх скоєнню.

Завданням держави є убезпечення громадян, із цим завданням держава частіше не справляється, ніж навпаки, оскільки в кожного є приклад, як ошукують людей шляхом розсилки фішингових листів. Так, наприклад, щодня від нотаріальної палати України надходять повідомлення про фішингову розсилку на офіційні електронні поштові скриньки нотаріусів листів зі шкідливими програмним вкладенням, метою якого є отримання несанкціонованого доступу до реєстрів, що перебувають у користуванні нотаріусів. Трохи дивною є рекомендація для нотаріусів не відкривати такі листи, або відкривати їх спочатку на мобільному пристрої, або не переглядати пошту на комп'ютерах, де встановлено реєстри. Тобто замість вирішення питання захисту реєстрів фаєрволом від фішингу, нотаріусам рекомендують просто придбати окремий комп'ютер для реєстрів. Тобто вирішити проблему не можуть, а лише радять ситуативні методи, якими нотаріус сам себе має захищати від дій правопорушників, хоча в Законі України «Про нотаріат» такі функції в нотаріусів відсутні.

З огляду на проблеми сучасності, в Україні на кожний новий електронний реєстр чи державну базу даних створюється свій керівний чи контролюючий орган, що ніяк не покращує кримінальний простір у цифровому полі, тому неминучим стає утворення на базі Міністерства цифрової трансформації багаторівневої Національної служби цифрового простору, з аналітичною, контролюючою та правозахисною метою, щоб усім цифровим простором держави опікувався один орган. Створення одного органу, що працюватиме, який опікуватиметься вирішенням різних питань, може мати декілька переваг для громадян.

Саме тому одним із можливих способів захисту інформації в державних реєстрах є впровадження сучасних технологій криптографічного захисту даних. Це передбачає використання шифрування для збереження конфіденційності даних і електронних підписів для забезпечення цілісності й автентичності інформації. Криптографічні алгоритми можуть ускладнити доступ до даних для несанкціонованих осіб і зменшити ризик незаконних змін.

Окрім того, важливо гарантувати фізичну безпеку серверів і баз даних, де зберігається інформація реєстру. Це може передбачати використання контрольно-пропускних систем, відеоспостереження і обмеження доступу до приміщень із серверами лише для авторизованих осіб.

Також необхідно регулярно проводити аудит безпеки, щоб виявляти потенційні вразливості та вживати заходів для їх усунення. Це може включати перевірку наявності оновлень програмного забезпечення, перевірку наявності відповідних політик доступу, а також проведення незалежних перевірок зовнішніми експертами.

Отже, захист інформації в державних реєстрах потребує комплексного підходу. Упровадження сучасних технологій криптографічного захисту, фізична безпека, регулярний аудит і освіта співробітників можуть сприяти забезпеченню надійного захисту реєстру та запобіганню незаконному доступу до нього.

Держава повинна контролювати кібербезпеку в Україні з кількох причин.

Захист національної безпеки: кібератаки можуть спричинити значну шкоду національній інфраструктурі й економіці,

а також порушити роботу важливих галузей, як-от енергетика, транспорт, фінанси та комунікації. Держава має відповідальність за захист своїх громадян та інфраструктури від кіберзагроз і гарантування національної безпеки.

Захист особистої інформації громадян: у сучасному цифровому світі, де особиста інформація зберігається та передається онлайн, важливо забезпечити захист цієї інформації від несанкціонованого доступу та використання. Держава повинна встановлювати правила та норми, які регулюють збір, зберігання і оброблення особистих даних громадян, а також забезпечувати їх виконання та захист. Особливо зважаючи на той факт, що громадянин України не може відмовитись на законодавчому рівні від цифровізації його даних.

Боротьба з кіберзлочинністю: кіберзлочинність, як-от хакерство, шахрайство та крадіжка ідентичності, стає все більш поширеною та складною проблемою. Держава повинна мати ефективні механізми для виявлення, розслідування та покарання кіберзлочинців, а також для запобігання таким злочинам через упровадження відповідного законодавства та заходів.

Регулювання та стандартизація: держава має важливу роль у встановленні стандартів і норм для кібербезпеки в різних секторах, як-от фінанси, охорона здоров'я та комунікації. Це допомагає забезпечити єдність і взаємодію між різними суб'єктами та забезпечити високий рівень захисту від кіберзагроз.

Кібербезпека є глобальною проблемою, і співпраця між державами є важливою для ефективної боротьби з кіберзагрозами. Держава повинна активно співпрацювати з міжнародними організаціями й іншими країнами для обміну інформацією, досвідом і ресурсами в галузі кібербезпеки.

З огляду на проблеми сучасності в Україні на кожний новий електронний реєстр чи державну базу даних створюється свій керівний чи контролюючий орган, що ніяк не покращує кримінального простору в цифровому полі, тому неминучим стає утворення на базі Міністерства цифрової трансформації багаторівневої Національної служби цифрового простору з аналітичною, контролюючою та правозахисною

метою, щоб усім цифровим простором держави опікувався один орган. Створення одного органу, що працюватиме, який опікуватиметься вирішенням різних питань, може мати декілька переваг для громадян:

1. Ефективність, що передбачає ефективне та швидке вирішення питань. Координація між різними органами може потребувати багато часу та зусиль, тоді як один орган може працювати більш злагоджено та швидко.

2. Наявність одного органу, який відповідає за різні питання, що зручно для громадян, оскільки вони можуть звертатися до одного місця для отримання необхідної допомоги чи інформації. Це зменшує необхідність у складних процедурах і пересаді з одного органу до іншого.

3. Зменшення бюрократії, оскільки одним працюючим органом можна спростити процеси та зменшити бюрократичні перешкоди. Це може полегшити доступ громадян до послуг і зменшити час, необхідний для їх отримання.

4. Об'єднання різних органів в один може дозволити ефективніше використовувати ресурси, як-от бюджет, персонал і технології. Це може допомогти забезпечити кращу якість послуг і використання публічних ресурсів.

Звичайно, існують ситуації, коли різні органи можуть мати специфічні компетенції та функції, що потребують окремої уваги. У такому разі важливо забезпечити ефективну співпрацю та координацію між різними органами, щоб гарантувати найкращі результати для громадян.

Але держава Україна вже має позитивний досвід у створенні об'єднаної платформи, яка стала у пригоді багатьом громадянам, ця платформа називається «Дія», тож логічним постає питання, чому не можна створити таку саму платформу для контролю за діяльністю цифрового простору держави.

Посягання на діяльність державних реєстрів, як-от Реєстр речових прав на нерухоме майно, може мати серйозні наслідки для суспільства та громадян. Основні ризики – незаконні зміни власників об'єктів нерухомості, підробка документів, втрата даних або навіть можливість використання реєстру для шахрайства та злочинних дій.

Одним із можливих способів захисту інформації в державних реєстрах є впровадження сучасних технологій криптографічного захисту даних. Це передбачає використання шифрування для збереження конфіденційності даних і електронних підписів для забезпечення цілісності й автентичності інформації. Криптографічні алгоритми можуть ускладнити доступ до даних для несанкціонованих осіб і зменшити ризик незаконних змін.

Окрім того, важливо гарантувати фізичну безпеку серверів і баз даних, де зберігається інформація реєстру. Це може передбачати використання контрольно-пропускних систем, відеоспостереження і обмеження доступу до приміщень із серверами лише для авторизованих осіб.

Також необхідно регулярно проводити аудит безпеки, щоб виявляти потенційні вразливості та вживати заходів для їх усунення. Це може передбачати перевірку наявності оновлень програмного забезпечення, перевірку наявності відповідних політик доступу, а також проведення незалежних перевірок зовнішніми експертами.

Нарешті, важливо забезпечити освіту та свідомість співробітників, які працюють із державними реєстрами. Інструктажі та навчання з питань кібербезпеки можуть допомогти усвідомити ризики та навчити працівників виявляти та запобігати можливим атакам.

Загалом, захист інформації в державних реєстрах потребує комплексного підходу. Упровадження сучасних технологій криптографічного захисту, фізична безпека, регулярний аудит і освіта співробітників можуть сприяти забезпеченню надійного захисту реєстру та запобіганню незаконному доступу до нього.

Висновки. З огляду на виявлені недоліки, державна політика щодо цифровізації повинна змінитися в таких напрямках:

- перегляд адміністративно-правової політики у сфері цифровізації;
- створення Національної служби кібербезпеки реєстрів;
- упровадження багаторівневої автентифікації. Необхідно запровадити: біометричну ідентифікацію для доступу до реєстрів; блокчейн-системи для перевірки достовірності внесених даних;

- децентралізація реєстрів і створення резервних серверів. Запровадження незалежних серверів з автономним доступом дозволить уникнути паралічу системи в разі атаки;

- посилення відповідальності за недбале адміністрування реєстрів;

- запровадження кримінальної і адміністративної відповідальності для посадовців, які допустили незахищеність державних цифрових сервісів.

Потрібен повний перегляд адміністративно-правової політики у сфері цифровізації. Без цього будь-яке подальше розширення цифрових послуг буде супроводжуватися критичними ризиками для держави та громадян.

Пріоритетними завданнями є: створення єдиного органу захисту реєстрів, упровадження технологій багаторівневого кіберзахисту, посилення відповідальності за порушення у сфері цифровізації.

Орган захисту реєстрів має відповідати за:

- моніторинг атак на всі державні реєстри;

- оперативне реагування на спроби зламу;

- сертифікацію архітектури реєстрів;

- координацію між Мін'юстом, ДП «НАІС» і кіберполіцією.

Незахищеність реєстрів створює ризики для права власності, нотаріальних дій і загалом для функціонування державного управління. У статті проаналізовано адміністративно-правові аспекти цифровізації, виявлено ключові проблеми захисту реєстрів і запропоновано заходи щодо реформування політики регулювання цифрової інфраструктури України. Тільки системний підхід дозволить зробити цифрову інфраструктуру України надійною та стійкою до загроз.

ЛІТЕРАТУРА:

1. Марченко В., Желтухін Є. Нотаріат у фокусі реформ. *Юридична газета online*. URL: <http://jur-gazeta.com/interview/notariat-u-fokusireform.html> (дата звернення: 25.08.2021).

2. Цивільний кодекс України : Закон України № 435-IV від 16 січня 2003 р. / *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення: 28.04.2023).

3. Деякі питання нотаріату в умовах воєнного стану : постанова Кабінету Міністрів України від 28.02.2022 р. № 164. URL: <https://zakon.rada.gov.ua/laws/show/164-2022-п#Text> (дата звернення: 26.04.2023).

4. Пронотаріат : Закон України від 02.09.1993 р. № 3425-XII. URL: <https://zakon.rada.gov.ua/laws/show/3425-12> (дата звернення: 26.04.2023).

5. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. URL: <https://www.president.gov.ua/documents/constitution>.

6. Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень : Закон України. *Відомості Верховної Ради України*. 2004. № 51. Ст. 553. URL: <https://zakon.rada.gov.ua/laws/show/1952-15#Text>.

7. Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень : постанова Кабінету Міністрів України від 25 грудня 2015 р. № 1127. URL: <https://zakon.rada.gov.ua/laws/show/1127-2015-п#Text>.

8. Звіт про результати роботи Департаменту кіберполіції Національної поліції України у 2023 р. URL: <https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u-roczni-969/>.

9. Річні звіти Національної поліції України. URL: <https://www.npu.gov.ua/diynalnist/zvitnist/richni-zviti>.