УДК 004.054:342.72
DOI https://doi.org/10.32782/2524-0374/2024-4/116

БЕЗПЕКА ДАНИХ В ЄДИНИХ І ДЕРЖАВНИХ РЕЄСТРАХ І ЦИФРОВИХ ПЛАТФОРМАХ В УМОВАХ ВОЄННОГО СТАНУ

DATA SECURITY IN UNIFIED AND STATE REGISTERS AND DIGITAL PLATFORMS IN CONDITIONS OF MARTIAL LAW

Токарєва К.С., д.ю.н.,
доцент кафедри конституційного і адміністративного права
Національний авіаційний університет

Стаття присвячена висвітленню актуальних проблем безпеки даних в умовах воєнного конфлікту**.** Вказується на стрімкий розвиток діджиталізації в Україні та існування значної кількості державних/єдиних реєстрів та інших систем, що містять персональні дані громадян та різну конфіденційну інформацію. Зазначається, що підвищений рівень обсягу інформації в таких системах, спричинений режимом воєнного стану та сприятливими умовами для кібератак, робить державні реєстри та цифрові платформи привабливою мішенню для хакерів. Незважаючи на спроби законодавчого забезпечення кібербезпеки, відмічається, що здійснення іноземними кіберагентами масштабних атак на українські та іноземні інформаційні системи недостатньо підконтрольне. Ризики для конфіденційності та безпеки даних у реєстрах та платформах підкреслюються через приклади кібератак на супутники, урядові вебсайти та мобільні мережі. Зазначено, що такі атаки можуть призвести до дестабілізації суспільства, підриву економіки та витоку персональних даних. Порушення конституційних прав громадян в рамках недостатньої захищеності їхніх особистих даних в реєстрах є ще однією небезпекою. Окрему увагу зосереджено на проблемах, пов'язаних з функціонуванням нових реєстрів, таких як Єдиний державний реєстр призовників, військовозобов'язаних та резервістів, де конфіденційна інформація про осіб може стати об'єктом кібератак. Негативний вплив кіберзлочинності виявляється також у сфері управління майном, яке пошкоджене або знищене внаслідок воєнних дій. Ризики витоку та неправомірного використання таких даних становлять загрозу для безпеки громадян та держави в цілому. У висновках відзначається, що проблема кібербезпеки в Україні вимагає комплексного підходу, який включає в себе посилення шифрування, розробку високих стандартів безпеки, співпрацю з іншими державами та підвищення обізнаності громадян про безпечне використання даних. Зокрема, необхідно зосередити увагу на можливостях контролю над обсягом інформації про себе у державних реєстрах та платформах.

Ключові слова: безпека даних, державні реєстри, єдині реєстри, цифрові платформи, кібератаки, персональні дані, кіберзлочинність, воєнний стан, стандарти безпеки.

This article examines the pressing issues of data security in the context of the ongoing military conflict in Ukraine. It highlights the rapid development of digitalization in the country and the existence of a significant number of state and unified registries and other systems containing personal data of citizens and various confidential information. The article emphasizes that the increased volume of information in such systems, caused by the martial law regime and favorable conditions for cyberattacks, makes state registries and digital platforms an attractive target for hackers.

Despite attempts to ensure cybersecurity through legislation, the article notes that the implementation of large-scale attacks on Ukrainian and foreign information systems by foreign cyber agents remains insufficiently controlled. The risks to the confidentiality and security of data in registries and platforms are highlighted through examples of cyberattacks on satellites, government websites, and mobile networks. The article emphasizes that such attacks can lead to the destabilization of society, undermine the economy, and cause a leak of personal data.

The violation of citizens' constitutional rights due to the insufficient protection of their personal data in the registries is another highlighted danger. Particular attention is paid to the problems associated with the functioning of new registries, such as the Unified State Register of Conscripts, Military Personnel, and Reservists, where confidential information about individuals can become the target of cyberattacks.

The negative impact of cybercrime is also manifested in the area of property management that has been damaged or destroyed as a result of hostilities. The risks of leakage and misuse of such data pose a threat to the security of citizens and the state as a whole.

The article concludes that the cybersecurity problem in Ukraine requires a comprehensive approach, which includes strengthening encryption, developing high security standards, cooperating with other countries, and raising citizens' awareness of the safe use of data. In particular, it is necessary to focus on the possibilities of controlling the amount of information about oneself in state registries and platforms.

Key words: data security, State registries, Unified registries, digital platforms, cyberattacks, personal data, cybercrime, state of war martial law, security standards.

На тлі стрімкого розвитку інформаційно-комунікаційних технологій, спостерігається значне зростання ролі цифрових інструментів в управлінні даними. Дана тенденція веде до революційних змін в системах управління, стимулюючи впровадження нових єдиних та державних реєстрів, а також цифрових платформ. Однак у зв'язку зі складнощами сучасної геополітики та введеним правовим режимом воєнного стану, критична важливість забезпечення безпеки даних у таких системах стає особливо актуальною. Об'єднання зростаючої напруги та збільшеної залежності від цифрової інфраструктури підкреслює необхідність міцних механізмів для забезпечення цілісності та конфіденційності даних.

Україна, демонструючи динамічний вектор розвитку та адаптації до потреб сучасного цифрового середовища, характеризується значною активізацією процесів діджиталізації суспільних відносин. В рамках реалізації даного курсу в країні сформовано та функціонує понад двадцять реєстрів, які відіграють суттєву роль у забезпеченні результативного функціонування державних інститутів та наданні якісних публічних послуг громадянам. Інформація про деякі з реєстрів доступна на офіційному вебпорталі ДП «Національні інформаційні системи» [1]. Проте, на зазначеному вебресурсі відсутня інформація про щонайменше три реєстри, які відіграють визначну роль у суспільному житті України. Зокрема, Єдиний державний реєстр судових рішень, Єдиний реєстр досудових розслідувань та Єдиний реєстр адвокатів України є ключовими джерелами інформації для судової системи, правоохоронних органів та адвокатської спільноти в країні.

Згідно з офіційними даними Міністерства юстиції України, загальний обсяг інформації, що міститься в єдиних та державних реєстрах, становить близько 208 594 181 аркуша формату А4 [2]. Такий показник ґрунтується на аналізі 17 реєстрів, що знаходяться під управлінням зазначеного державного органу. Варто зауважити, що наведена цифра відображає лише частку загального обсягу даних, що містяться в усіх реєстрах, зважаючи на їх значну кількість.

Аналіз масштабного обсягу даних, що містяться в реєстрах, свідчить про гостру потребу в надійних механізмах

їх захисту. Сучасна геополітична ситуація призводить до значного підвищення ризиків в галузі кібербезпеки та незаконного доступу до конфіденційної інформації. Умови воєнного стану створюють сприятливі умови для здійснення кібератак, які можуть призвести до різноманітних наслідків. Зважаючи на зазначене, впровадження та забезпечення функціонування ефективних систем захисту даних є ключовим завданням держави, спрямованим на збереження конфіденційності та недоторканності інформації.

Перші кроки щодо посилення кібербезпеки в Україні були зроблені ще на початку повномасштабного вторгнення. Зокрема, парламентом було прийнято закони, які удосконалили кримінально-процесуальне законодавство у сфері кіберзлочинності [3; 4]. Хоча прийняті законодавчі акти дозволили розширити перелік кіберзлочинів, посилити відповідальність за їх вчинення та удосконалити процесуальні механізми розслідування, вони виявилися неефективними у забезпеченні захисту від кіберзагроз з боку іноземних кіберагентів.

Наприклад, дослідження хронології подій 24 лютого 2022 року свідчить про те, що масштабній військовій агресії Російської Федерації проти України передувала кібератака, спрямована на порушення роботи супутникового інтернет-сервісу Viasat. За даними міжнародних організацій, дана кібератака була ініційована з боку РФ. Вона мала значний вплив на функціонування критичної інфраструктури України, а також на доступ до інтернету для цивільних та військових користувачів. Особливістю даної атаки стало використання універсального шкідливого програмного забезпечення AcidRain, яке відрізняється від попередніх кібератак, що мали більш вузькоспрямований характер [5].

Згідно з офіційним повідомленням уряду Литовської Республіки, протягом певного періоду часу понад 130 вебсайтів державного та приватного секторів зазнали проблем з функціонуванням або стали недоступними через хакерські атаки. За даними розслідування, до атак на сайти в Німеччині, Італії, Румунії, Норвегії, Литві та США причетна хакерська група Killnet, яка оголосила «війну» десяти країнам. Характерною особливістю є те, що дані кібератаки часто синхронізуються з акціями підтримки України з боку інших держав. Окрім Killnet, проросійська хакерська група XakNet також здійснила атаку на найбільшу приватну енергетичну компанію в Україні та на вебсайти українського уряду [6].

Один із найбільш помітних і небезпечних інцидентів у сфері кібербезпеки відбувся у грудні 2023 року. Він полягав у хакерській атаці на інфраструктуру телекомунікаційного оператора Київстар в Україні. Даний оператор, вважаючись одним з найбільших національних постачальників телекомунікаційних послуг, забезпечує зв'язок для половини населення країни. Мережа Київстар зазнала технічного збою, який вплинув на функціонування мобільного зв'язку та доступу до Інтернету. Також виникли проблеми з оплатою послуг у терміналах, що працюють на базі мобільних сім-карт оператора, а також з функціонуванням інших пов'язаних систем та обладнання [7].

Особливої гостроти набувають атаки на єдині та державні реєстри, сайти Міністерства юстиції України, ДП «НАІС» та інші критичні інформаційні системи [8].

Аналізуючи два останні наведені приклади, можна визначити кілька ключових факторів, які визначають небезпеку таких атак. Перш за все, можливість *дестабілізації суспільства* виникає внаслідок порушення роботи критичної інфраструктури. Подібні атаки можуть призвести до паніки та хаосу серед населення, оскільки порушення нормального функціонування інфраструктури може спричинити серйозні соціальні наслідки. Другий аспект стосується *підриву економіки*. Такі атаки, як та, що відбулася проти мережі Київстар, можуть призвести до значних економічних збитків через припинення роботи ключових інфраструктурних систем та послуг.

Також *отримання розвідувальної інформації* становить серйозну загрозу. Кіберзлочинці, отримавши доступ до конфіденційної інформації, можуть використовувати її для планування та здійснення терористичних актів або інших злочинів. Особливо важливим є *ризик витоку персональних даних* осіб, що перебувають у лавах Збройних Сил України та їх сімей. Потенційний витік такої інформації може мати катастрофічні наслідки для військових та їх близьких, поставивши під загрозу не лише їхню конфіденційність, але й безпеку та навіть життя.

Розглядаючи останній фактор, неможливо уникнути обговорення Проекту Закону про внесення змін до деяких законодавчих актів України щодо питань проходження військової служби, мобілізації та військового обліку № 10449 від 30.01.2024 р. Вбачаємо доцільним відзначити його ст. 22, у якій передбачено функціонування Єдиного державного реєстру призовників, військовозобов'язаних та резервістів [9]. Однак реєстр породжує суперечливість, оскільки відповідно до ч. 2 ст. 6 «Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів» згода осіб, які мають бути включені до реєстру, на обробку їх персональних даних не є обов'язковою [10].

Варто додати, що нині діє проект такого Реєстру – реєстр «Оберіг». Попри відсутність інформації про чинних військовослужбовців [11], мобілізація триває, і неможливо передбачити, хто саме із зареєстрованих у цьому реєстрі осіб стане військовим у майбутньому. Отже, у рамках кібербезпеки виникає питання щодо безпеки функціонування такого реєстру.

Окрім зазначеного, питання про безпеку такого реєстру виникає через те, що наразі в ньому зберігається значна кількість особистої інформації, включаючи ПІБ, адресу проживання, дату народження, сімейний стан, інформацію про освіту, місце роботи, стан здоров'я, дані про судимість та інші [11]. Виходячи із положень ще одного законопроекту – № 10062 від 18.09.2023 р., який вже подано на підпис Президенту України, механізм отримання даних є теж дискусійним питанням. Інформація отримується з таких джерел, як органи реєстрації актів цивільного стану, Державна міграційна служби України, Державна податкова служба України, Міністерство освіти і науки України, Міністерство охорони здоров'я України, Пенсійний фонд України, Офіс Генерального прокурора та інших державних органів. При цьому не передбачено необхідності отримання згоди на обробку персональних даних для цілей реєстру [12]. Враховуючи, що згідно з Законом України «Про доступ до публічної інформації» перерахована інформація є конфіденційною [13], і згода на обробку персональних даних у такому випадку є обов'язковою. Виходячи із вищевказаного, такий реєстр обмежує основоположні права громадян. Зважаючи, що схоже положення міститься у ст. 32 Конституції України [14], такі дії є порушенням Основного Закону. Таким чином, важливо розглянути перспективи подальшого функціонування зазначеного Реєстру в рамках кібербезпеки та конституційних прав громадян.

Збройна агресія Російської Федерації проти України спричинила значні руйнування житлового фонду, інфраструктури та інших об'єктів нерухомого майна. З метою компенсації за пошкодження та знищення майна, а також для планування відновлення країни, було створено Державний реєстр майна, пошкодженого та знищеного внаслідок бойових дій, терористичних актів, диверсій, спричинених збройною агресією Російської Федерації проти України. Відповідно до ст. 14 Закону України «Про компенсацію за пошкодження та знищення окремих категорій об'єктів нерухомого майна внаслідок бойових дій …», реєстр містить інформацію про пошкоджене чи знищене майно, а також про осіб, яким завдана матеріальна шкода

внаслідок цих подій. Додатково, він фіксує процес розгляду та прийняття рішення щодо надання компенсації за зазначене пошкоджене та знищене майно, а також встановлює порядок надання фінансової підтримки (виділення коштів) на відновлення пошкодженого чи знищеного майна [15]. Втрата та крадіжка даних є однією з основних загроз, пов'язаних зі зберіганням інформації в Реєстрі. Зловмисники можуть отримати доступ до цінних персональних даних мільйонів постраждалих осіб. Такі дані становлять потенційний інструмент для здійснення різноманітних злочинних дій, включаючи ідентифікацію та націлювання на людей, що співпрацюють з урядом, планування диверсій або проведення інформаційних операцій. Крім того, існує загроза кібератак, спрямованих на сам Реєстр. Атаки цього типу можуть призвести до пошкодження або повного знищення даних, що знаходяться в системі. Подібна ситуація може серйозно ускладнити або навіть зробити неможливим процес відшкодування збитків для постраждалих, оскільки важлива інформація для реалізації компенсаційних процедур може бути втрачена.

Навіть у випадку, якщо системи єдиних реєстрів будуть надійно захищені від зовнішніх кібератак, завжди існує ризик несанкціонованого поширення конфіденційної інформації з усіх Реєстрів, у тому числі, перелічених раніше. Такий ризик може виникнути через дії внутрішніх загроз, таких як співробітники державних органів, операторів мобільних мереж та інших суб'єктів, які мають доступ до вказаних систем.

Окрім єдиних (державних) реєстрів, які містять значний масив даних, існують також різні інформаційно-комунікаційні системи. Такі системи використовуються для різних цілей, зокрема: надання державних послуг, здійснення електронних платежів, обмін інформацією, спілкування. Наприклад, Дія – це вебпортал, який використовується для отримання державних послуг в Україні [16]. Додаток містить багато персональних даних користувачів, у тому числі документів, тому він стає мішенню для кібератак. У 2022 році Дія зазнала кібератаки, яку успішно відбили. Мішенню стали також мобільні банкінгові системи – «ПриватБанк» та «Ощадбанк» [17].

Війна в Україні стимулювала створення нових інформаційних систем, таких як DREAM – цифрова екосистема для підзвітного управління відновленням [18]. Вона має на меті покращити координацію та прозорість процесів відновлення країни. DREAM містить багато конфіденційної інформації про плани та ресурси, які використовуються для відновлення України. Крім того, система містить дані про людей, котрі втратили свої домівки, вказуються адреси зруйнованих будинків, тому вона може стати об'єктом уваги хакерів.

Платформи «єДопомога», «єВідновлення» та інші, які функціонують в межах системи Дія та використовуються для координації зусиль з допомоги людям, постраждалим від війни, також потребують ретельного захисту даних [19; 20].

Висновки. Зважаючи на постійні атаки хакерів на урядові портали, реєстри, мобільні мережі та банкінги, інші інформаційно-комунікаційні платформи України, питання безпеки даних в єдиних і державних реєстрах, а також на цифрових платформах в умовах воєнного стану набуває надзвичайної важливості. Виходячи з того, що на таких платформах та реєстрах зосереджено величезну кількість персональних даних та конфіденційної інформації, включаючи дані про постраждалих від війни та військовозобов'язаних, резервістів, інформацію про територіальні громади та державні структури, наявність посилених заходів забезпечення кібербезпеки стає невідкладною необхідністю.

Потенційний ризик втрати такої конфіденційної інформації або її використання країною-терористом для здійснення диверсій, терористичних атак, шантажу чи залякування населення є значущим. Наслідки подібних сценаріїв можуть мати катастрофічні наслідки для громадян та всієї держави. Громадяни України вже переживають серйозні психологічні травми через втрату домівок, рідних, переселення та постійні ракетні атаки. Втрата даних та можливий шантаж з боку країни-агресора щодо інформації про їхніх родичів-військовослужбовців та військовозобов'язаних може значно підвищити рівень психологічної травми та відчуття загрози серед населення.

У зв'язку з вищезазначеним, ми вважаємо, що забезпечення безпеки даних на таких платформах повинно стати пріоритетом не лише для уряду України, але й для всіх держав, оскільки кіберзлочинність не має кордонів. Боротьба з нею має відбуватися у співпраці та комплексно. Зокрема, шляхом обміну досвідом, розробленням міжнародних стандартів та нормативів, технічної підтримки та спільних оперативних заходів. Крім того, варто підвищити обізнаність користувачів про правила безпечної роботи з цифровими платформами, надати можливість громадянам контролювати свої дані, які вносять до таких реєстрів та платформ. Тільки такий підхід зможе забезпечити ефективний захист даних та знизити ризики їхнього неправомірного використання в умовах воєнного конфлікту.

ЛІТЕРАТУРА

1. Реєстри. Державне підприємство «Національні інформаційні системи». URL: https://nais.gov.ua/registers (дата звернення: 08.03.2024).

2. Роз'яснення щодо функціонування та захищеності баз даних інформаційної мережі Міністерства юстиції (Єдиних та Державних реєстрів). *Міністерство юстиції України*. URL: https://minjust.gov.ua/m/str_22252 (дата звернення: 08.03.2024).

3. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15.03.2022 р. № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text (дата звернення: 21.03.2024).

4. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 р. № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 21.03.2024).

5. Війна росії проти України почалася з кібернападу на супутники. За годину до вторгнення були знищені «десятки тисяч» терміналів Viasat. *ITC.ua*. URL: https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatki-tisyach-terminaliv-viasat/ (дата звернення: 21.03.2024).

6. «Наш ворог – це ваш уряд». Як проросійські хакери створюють проблеми не тільки для України. Аналіз від WIRED. *Forbes.ua*. URL: https://forbes.ua/inside/rosiyski-khaktivisti-stvoryuyut-problemi-ne-tilki-dlya-ukraini-analiz-vid-wired-12072022-7126 (дата звернення: 21.03.2024).

7. Робимо все, щоб відновити наші сервіси після хакерської атаки. *Київстар*. URL: https://kyivstar.ua/news/id191220231000 (дата звернення: 21.03.2024).

8. На низку державних ресурсів відбувається кібератака. *Укрінформ*. URL: https://www.ukrinform.ua/rubric-technology/3683610-na-nizku-derzavnih-resursiv-vidbuvaetsa-kiberataka.html (дата звернення: 21.03.2024).

9. Картка законопроекту № 10449 від 30.01.2024. *Електронний кабінет громадянина*. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43604 (дата звернення: 21.03.2024).

10. Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів : Закон України від 16.03.2017 р. № 1951-VIII : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/1951-19#Text (дата звернення: 21.03.2024).
11. Єдиний реєстр військовозобов'язаних «Оберіг» вже працює, але його розширятимуть. *БУХГАЛТЕР.UA*. URL: https://buh.ligazakon.net/news/224766_diniy-restr-vyskovozobovyazanikh-oberg-vzhe-pratsyu-ale-yogo-rozshiryatimut (дата звернення: 21.03.2024).
12. Картка законопроекту № 10062 від 18.09.2023. *Електронний кабінет громадянина*. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/42801 (дата звернення: 21.03.2024).
13. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI : станом на 8 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 21.03.2024).
14. Конституція України : від 28.06.1996 р. № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 21.03.2024).
15. Про компенсацію за пошкодження та знищення окремих категорій обёєктів нерухомого майна внаслідок бойових дій, терористичних актів, диверсій, спричинених збройною агресією Російської Федерації проти України, та Державний реєстр майна, пошкодженого та знищеного внаслідок бойових дій, терористичних актів, диверсій, спричинених збройною агресією Російської Федерації проти України : Закон України від 23.02.2023 р. № 2923-IX : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2923-20#Text (дата звернення: 22.03.2024).
16. Дія – Державні послуги онлайн. *Офіційний вебсайт*. URL: https://diia.gov.ua/ (дата звернення: 21.03.2024).
17. Федоров: «Дія» відбила потужну кібератаку з чотирьох країн. *Радіо Свобода*. URL: https://www.radiosvoboda.org/a/news-diia-kiberataka/31705878.html (дата звернення: 21.03.2024).
18. DREAM. *Офіційний вебсайт*. URL: https://dream.gov.ua/ua (date of access: 21.03.2024).
19. єДопомога. *Офіційний вебсайт*. URL: https://aid.edopomoga.gov.ua/ (дата звернення: 21.03.2024).
20. єВідновлення. *Офіційний вебсайт*. URL: https://erecovery.diia.gov.ua/#start (дата звернення: 22.03.2024).