УДК 34:004.056(477)
DOI https://doi.org/10.32782/2524-0374/2023-10/96

ПРОТИДІЯ ВПЛИВУ НА ДЕРЖАВНІ ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ ТА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ

COUNTERACTING THE IMPACT ON STATE ELECTRONIC INFORMATION RESOURCES AND CRITICAL INFRASTRUCTURE FACILITIES IN THE MILITARY CONDITIONS

Метелев О.П., д.філос. у галузі права,
завідувач спеціальної кафедри
Інститут підготовки юридичних кадрів для Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого

Плетньов О.В., к.ю.н., доцент,
професор спеціальної кафедри № 2
Інститут підготовки юридичних кадрів для Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого

У статті виокремлено шляхи протидії впливу на державні електронні інформаційні ресурси та об'єкти критичної інфраструктури в умовах воєнного стану в Україні. Автори акцентують увагу на тому, що найбільшими власниками державних реєстрів в Україні, включаючи інформацію про об'єкти критичної інфраструктури, на сьогодні є Міністерство юстиції України, Державна податкова служба України та Міністерство внутрішніх справ України, включаючи всі його підрозділи. Автори наголошують на тому, що одним із основних завдань більшості державних реєстрів є збір, зберігання та обробка інформації для прийняття державними службовцями рішень, у тому числі щодо надання публічних послуг. Проте відсутність електронної взаємодії між державними реєстрами спричиняє низку різноманітних проблем, які знижують якість надання публічних послуг, особливо в їх електронному вигляді. Відсутність оперативного доступу державного органу до інформації від його колег створює передумови для узурпації державної інформації, що підриває довіру до державних інституцій та формує корупційні ризики. Крім того, відсутність взаємодії між державними ресурсами означає необхідність дублювання даних, особливо тих, що стосуються особистої інформації. Як наслідок, відсутність електронної взаємодії не дозволяє розвивати ефективні та прозорі державні послуги для населення та бізнесу. Відсутність базової концепції державного реєстру призводить до того, що еквівалентні поля дублюються в різних реєстрах і мають однаковий пріоритет. У результаті, з одного боку, державні органи зобов'язані зберігати велику кількість інформації, зібраної кожним державним органом самостійно, що, у свою чергу, збільшує трудомісткість та економічність, необхідну для ведення державного реєстру. З іншого боку, постійно зростає ймовірність внесення помилкової інформації до державних реєстрів через серйозний вплив людського фактору на процес їх ведення. Через високу вартість модернізації дата-центрів та швидкий розвиток інформаційних технологій більшість державних дата-центрів, зокрема, тих, що відносяться до критичної інфраструктури, використовують застаріле апаратне забезпечення та потребуватимуть комплексної технологічної модернізації в найближчі роки. У цьому зв'язку автори пропонують кардинальну зміну порядку збору, зберігання, передачі й обробки інформації з використанням посилення прав доступу до баз даних, контролю трафіку, шифрування.

Ключові слова: протидія впливу, держава, електронні інформаційні ресурси, об'єкти критичної інфраструктури, воєнний стан.

The article highlights the ways of counteracting the influence on the state electronic information resources and objects of critical infrastructure in the military conditions in Ukraine. The authors emphasize that the largest owners of state registers in Ukraine, including information on critical infrastructure objects, are currently the Ministry of Justice of Ukraine, the State Tax Service of Ukraine and the Ministry of Internal Affairs of Ukraine, including all its divisions. The authors emphasize that one of the main tasks of the most state registers is collection, storage and processing of information for public officials to make decisions, including the provision of public services. However, the lack of electronic interaction between state registers causes a number of various problems that reduce the quality of public services, especially in their electronic form. The lack of operational access of a state body to information from its colleagues creates prerequisites for the usurpation of state information, which undermines trust in state institutions and creates corruption risks. In addition, the lack of interaction between government resources means the need for duplication of data, especially those related to personal information. As a result, the lack of electronic interaction does not allow development of efficient and transparent government services for population and business. The lack of a basic concept of a public register leads to the fact that equivalent fields are duplicated in different registers and have the same priority. As a result, on the one hand, state bodies are required to store a large amount of information collected by each state body independently, which, in turn, increases the time-consuming and cost-effectiveness requirement to maintain a state registry. On the other hand, the probability of entering erroneous information into state registers is constantly increasing due to the serious influence of the human factor on the process of their management. Due to the high cost of modernizing data centers and the rapid development of information technologies, most government data centers, in particular, those related to critical infrastructure, use outdated hardware and will require complex technological modernization in the coming years. Accordingly, the authors propose a radical change in the order of collection, storage, transfer and processing of information using the strengthening of access rights to databases, traffic control, encryption.

Key words: counteraction, state, electronic information resources, critical infrastructure objects, military conditions.

Постановка проблеми. В умовах повномасштабної війни, яка триває, особливого значення набуває захист і збереження державних ресурсів, баз даних органів державної влади, які містять життєво важливу інформацію, зокрема персональні дані громадян України. Не менш важлим питанням є протидія впливу ворога на об'єкти критичної інфраструктури, діяльність яких суттєво залежить від стану захищеності електронних інформаційних ресурсів. Адже це те, що в першу чергу намагається знищити ворог. Повномасштабне вторгнення Росії в Україну завдало серйозної шкоди системі водопостачання, каналізації, тепло- та електроенергії, житлу, школам і закладам охорони здоров'я.

Завдання уряду не обмежується створенням ефективної системи захисту; воно також включає заходи щодо резервного копіювання даних і швидкого відновлення, якщо це необхідно. При цьому ще у 2021 році в рамках реалізації Стратегії кібербезпеки України було підтримано рішення про створення Національного реєстру електронних інформаційних ресурсів та доручено Державній службі спеціального зв'язку та захисту інформації забезпечити його функціонування та розвиток.

Аналіз останніх досліджень. Питання забезпечення національної безпеки, включаючи захист державних інформаційних ресурсів та об'єктів критичної

інфраструктури, являють суттєвий інтерес для вітчизняних і зарубіжних вчених і практиків, зокрема, таких: Б. Браун, В. Валетчик, О. Дзьобань, М. Домарацький, Г. Ситник, В. Путятін, М. Чуї та ін. Проте надзвичайно актуальним залишається дослідження загроз державним електронним інформаційним ресурси та об'єктам критичної інфраструктури зважаючи на повномасштабне російське вторгнення на територію України.

Відповідно, **метою статті** є виокремлення шляхів протидії впливу на державні електронні інформаційні ресурси та об'єкти критичної інфраструктури в умовах воєнного стану в Україні.

Виклад основного матеріалу. Сьогодні Кабінет Міністрів України ухвалив чергову важливу постанову «Деякі питання забезпечення функціонування державних інформаційних ресурсів» від 30 грудня 2022 р. № 1500, якою передбачалося ввести в дію [5]:

– порядок роботи Національного центру резервування державних інформаційних ресурсів, який чітко визначає функції та повноваження суб'єктів Національного центр резервування державних інформаційних ресурсів. Серед них Адміністрація Державної служби спеціального зв'язку та захисту інформації, ДП «Українські спеціальні системи», Державний центр кіберзахисту, Концерн радіомовлення, радіозв'язку і телебачення та КП «Укрспецзв'язок» [2; 9; 12];

– порядок подання органами державної влади, військовими частинами, підприємствами, установами та організаціями резервних копій національних електронних інформаційних ресурсів до Національного центру резервування державних інформаційних ресурсів, а також механізм їх зберігання та доступу до них. Зокрема, цей Порядок визначає кілька видів резервного копіювання національних електронних інформаційних ресурсів, вимоги до договорів на зберігання резервних копій, вимоги щодо захисту інформації та кіберзахисту на період їх зберігання, порядок їх передачі дипломатичним установам України за кордоном під час дії воєнного стану, період їх повернення після його скасування тощо [12].

На сьогодні в Україні налічується понад 135 державних реєстрів, власниками яких є понад 40 державних органів. Наразі неможливо визначити фактичну кількість державних реєстрів через відсутність єдиного ресурсу, який би містив інформацію про всі державні реєстри, а також через відсутність юридичного визначення «державного» чи «національного» реєстру/реєстру як такого.

Найбільшими власниками державних реєстрів в Україні на сьогодні є такі:

– Міністерство юстиції України (20 реєстрів) [11];

– Державна податкова служба України (15 реєстрів) [10];

– Міністерство внутрішніх справ України, включаючи всі його підрозділи (12 реєстрів) [4].

Варто зазначити, що фінансова підтримка працездатності більшості державних реєстрів здійснюється з Державного бюджету України. Слід відзначити, що на ведення кожного з державних реєстрів Україна щорічно витрачає в середньому близько 21 млн грн. (рисунок 1) [4; 10; 11].

Діяльність державних реєстрів базується на системах управління базами даних (СУБД), серед яких найбільш популярними є наступні:

– Oracle;

– MS SQL;

– PostgreSQL (рисунок 2) [17; 18].

Одним із основних завдань більшості державних реєстрів є збір, зберігання та обробка інформації для прийняття державними службовцями рішень, у тому числі щодо надання публічних послуг. Проте відсутність електронної взаємодії між державними реєстрами спричиняє низку різноманітних проблем, які знижують якість надання публічних послуг, особливо в їх електронному вигляді. Відсутність оперативного доступу державного органу до інформації від його колег створює передумови для узурпації державної інформації, що підриває довіру до державних інституцій та формує корупційні ризики (рисунок 3) [17; 18].

Крім того, відсутність взаємодії між державними ресурсами означає необхідність дублювання даних, особливо тих, що стосуються особистої інформації. Як наслідок, відсутність електронної взаємодії не дозволяє розвивати ефективні та прозорі державні послуги для населення та бізнесу.

Наприклад, лише в рамках порівняння даних «Єдиного державного демографічного реєстру України» та «Державного реєстру актів цивільного стану України» було виявлено 80% еквівалентних нетехнологічних полів [14; 15].

Досить велика кількість рівнозначних нетехнологічних галузей спровокована відсутністю законодавчо визначеного переліку базових державних реєстрів, що використовуються як першоджерела для використання в інших інформаційних ресурсах та взаємодії державних реєстрів. Відсутність базової концепції державного реєстру призводить до того, що еквівалентні поля дублюються в різних реєстрах і мають однаковий пріоритет. У результаті, з одного боку, державні органи зобов'язані зберігати велику кількість інформації, зібраної кожним державним органом самостійно, що, у свою чергу, збільшує трудомісткість та економічність, необхідну для ведення державного реєстру. З іншого боку, постійно зростає ймовірність внесення помилкової інформації до державних реєстрів через серйозний вплив людського фактору на процес їх ведення.

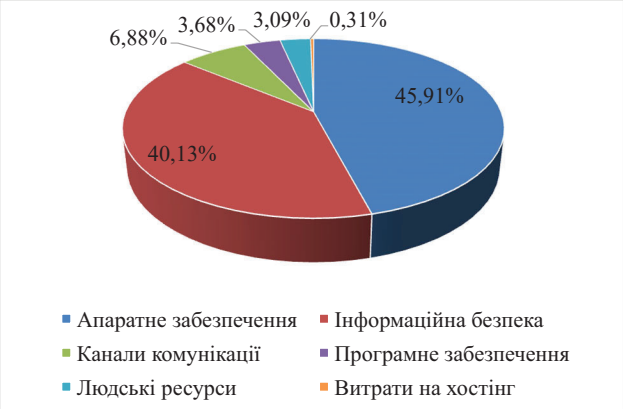

Рис. 1. Розподіл коштів Державного бюджету України на підтримку державних реєстрів України

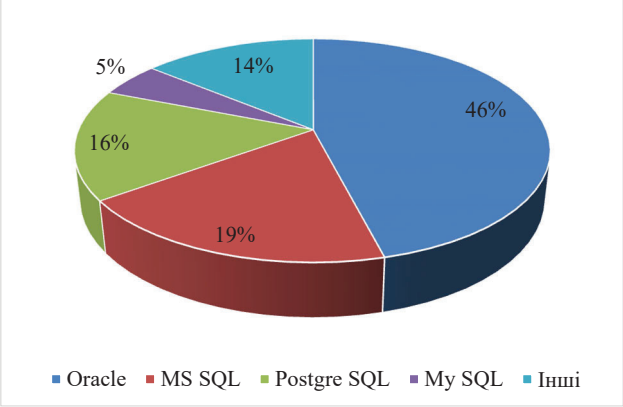

Рис. 2. Розподіл баз даних за популярністю використання в якості основи державних реєстрів

Рис. 3. Розподіл державних реєстрів за принципом розміщення

Інформаційне навантаження державних реєстрів часто є фрагментарним (раптовим), коли не всі поля, розроблені реєстрами, фактично заповнені. Це, у свою чергу, викликає обмеження у функціональності реєстру, що блокує можливість отримати з нього достовірні та повні дані. Як правило, фрагментація зумовлена відсутністю оцифрованої інформації за певний період часу до створення реєстру. Варто зазначити, що наразі існують окремі випадки електронної взаємодії, особливо в державних реєстрах Державної податкової служби України, Міністерства юстиції України, Міністерства внутрішніх справ України та Пенсійного фонду України [4; 10; 11; 13]. Такі обміни даними базуються на різноманітних і здебільшого застарілих технологіях, які не є стандартними і можуть використовуватися виключно двома державними органами без будь-якої систематичної процедури. Факт такої взаємодії свідчить про розуміння необхідності обміну даними для прийняття швидких рішень на основі достовірних даних. Переважна більшість поточних взаємодій використовує поле «Номер облікової картки платника податків» або «ІПН» як ідентифікатор підключення. З метою уніфікації зазначених взаємодій Державне агентство з питань електронного урядування в Україні у 2017 році запровадило національну систему електронної взаємодії державних інформаційних ресурсів, яка забезпечила рівні стандарти обміну даними для державних органів.

Ефективна система взаємодії державних реєстрів, як і будь-яка державна політика, має ґрунтуватися на ідеології «користувачевоцентризму», коли держава сама має служити інтересам своїх громадян шляхом всебічної підтримки пріоритетів їх прав, свобод та інтересів. Отже, існує потреба впровадити модель, за якої держава самостійно отримує персональні дані за допомогою персонального цифрового ідентифікатора, а не змушує особу збирати пов'язані дані особисто, пересуваючись по різних державних установах. На даний момент основною перешкодою на шляху реалізації вищезазначеної моделі є відсутність загального та популярного уніфікованого національного персонального цифрового ідентифікатора. Жоден із нині існуючих унікальних ідентифікаторів, які використовуються в державних реєстрах, не забезпечує 100% охоплення населення від народження людини до її смерті. Наприклад, до Державного реєстру виборців вносяться відомості про осіб, які досягли 18 років, і базуються на сукупності персональних даних, таких як ім'я та прізвище, дата та місце народження, серія та номер паспорта тощо. Державні реєстри, які належать Пенсійному фонду України та Фіскальна служба України має свої унікальні персональні ідентифікатори, такі як номер облікової картки платника податків та номер картки державного реєстру загальнообов'язкового державного соціального страхування, які, на жаль, не є обов'язковими (особа може відмовитися), і не охоплюють частину неповнолітніх громадян, які становлять 14% населення України [4; 10; 11; 13].

Водночас зусиллями Державної міграційної служби України у 2015 році було створено Єдиний державний демографічний реєстр України, який ініціював поширення унікального номера запису в Єдиному державному демографічному реєстрі (УНЗР). Цей номер є єдиним персональним ідентифікатором, від якого неможливо відмовитися, і він призначається людині один раз після народження (під час реєстрації народження) і не може бути змінений протягом усього життя. УНЗР – це 14-значне число, в якому зашифрована інформація про стать і дату народження людини.

Можна прогнозувати, що для того, щоб охопити УНЗР все населення, знадобиться не менше 12 років. Звичайно, цей термін неприйнятний, і Державна міграційна служба України робить усе можливе, щоб його скоротити, активізуючи роботу з видачі документів, що посвідчують особу. Важливість УНЗР полягає в тому, що цей номер має стати основою для розробки абсолютно нової системи державних інформаційних ресурсів. Це може допомогти побудувати інформаційні зв'язки, які дозволять поширювати персональні дані між державними реєстрами без необхідності отримання конкретних документів самою особою. Це означає, що людина буде носити унікальний номер від народження, і він буде автоматично вноситися до інших реєстрів, коли людина виростає. За все життя інформація про кожного з користувачів потрапляє в середньому до 16 державних реєстрів, і пов'язані дані про людину кілька разів вносяться в один і той же державний реєстр на різних етапах життя. Така процедура завжди вимагає від збору певного пакету документів знову і знову, незважаючи на те, що останні могли неодноразово подаватись до інших державних реєстрів [3].

Щодо протидії негативного ворожого впливу на об'єкти критичної інфраструктури слід зазначити, що відновлення та захист критичної інфраструктури підвищить енергетичну безпеку та покращить послуги водопостачання, очищення стічних вод та енергоефективності в громадах.

Сприятиме довгостроковому сталому розвитку та переходу до зеленої енергетики в Україні.

У грудні 2022 року Європейський Союз та Nefco оголосили ініціативу щодо реконструкції та ремонту критичної комунальної інфраструктури в Україні. Основними цілями акції є відновлення критично важливої муніципальної інфраструктури в місцевих громадах, сильно пошкоджених під час військових дій, які тепер перебувають під контролем українського уряду, надання базових муніципальних послуг для жителів та підвищення надійності та безпеки водо-, тепло- та електроенергії, постачання та очищення стічних вод, оскільки війна триває.

Загалом 12 сильно постраждалих міст і селищ міського типу Київської області, які не мають внутрішніх ресурсів для проектування та реалізації реконструкції критичної інфраструктури, уклали угоди з Nefco на отримання грантове фінансування від ЄС. Підтримані громади – це: Бородянка, Борщагівка, Димер, Дмитрівка, Гостомель, Ірпінь, Іванків, Калинівка, Немішаєве, Пісківка, Славутич та Велика Димерка.

Залежно від критичних потреб у реконструкції, визначених для кожного проекту, у громадах будуть реалізовані наступні заходи: ремонт та модернізація систем теплопостачання; ремонт систем водопостачання; ремонт та модернізація систем очищення стічних вод [20].

Підтримані проекти, пов'язані з критичною інфраструктурою, спрямовані не лише на відновлення пошкодженої інфраструктури, а й на її модернізацію та значне підвищення енергоефективності.

На додаток до цієї діяльності наразі впроваджено додаткові програми, що фінансуються ЄС, включаючи підтримку модернізації систем водопостачання, впровадження заходів з енергоефективності в громадських будівлях і мережах вуличного освітлення, а також будівництво, реконструкцію та оновлення громадських будівель для забезпечення нагальних житлових потреб для внутрішньо переміщених осіб. Отже, з метою протидії впливу на державні електронні інформаційні ресурси та об'єкти критичної інфраструктури в умовах воєнного стану слід, у першу чергу, забезпечити належний захист баз даних, які є основою державних реєстрів.

Бази даних стають корисними лише за умови доступу до них, але цей доступ має бути захищеним. Перший рівень захисту баз даних надають брандмауери, які забороняють доступ за умовчанням. Єдиний трафік, дозволений через брандмауер, має надходити від певних програм, веб-серверів або користувачів, яким потрібен доступ до даних, і без особливої потреби брандмауер повинен забороняти базі даних ініціювати вихідні з'єднання.

Прямий доступ до бази даних слід обмежити або заборонити, якщо сценарій використання це дозволяє. Зміни правил брандмауера повинні контролюватися процедурами управління змінами та ініціювати сповіщення для моніторингу безпеки [17; 18].

Організації можуть розгортати спеціалізовані засоби баз даних, які включають спеціальні брандмауери. Організації з більш обмеженими ресурсами можуть просто розгорнути посилену версію брандмауера операційної системи сервера бази даних.

Найменша можлива кількість користувачів, програм і інтерфейсів прикладного програмування повинна мати доступ до бази даних. Будь-який доступ має надаватися лише після авторизації мережі або програми, і навіть тоді весь доступ має ґрунтуватися на принципі найменших привілеїв і надаватися протягом найменшого можливого часу. Цю найкращу практику можна розділити на три підкатегорії: авторизація користувача, привілейований доступ і використання баз даних для розробки та операцій.

Контроль доступу до бази даних здійснює системний адміністратор. Адміністратор надає дозволи, визначені ролями та шляхом додавання облікових записів користувачів до цих ролей бази даних. Наприклад, роль безпеки на рівні рядків обмежує доступ для читання та запису до рядків даних на основі ідентичності користувача, членства в ролі або контексту виконання запиту.

Спеціалізовані рішення безпеки бази даних можуть забезпечити централізоване управління ідентифікаторами та дозволами, мінімізувати зберігання паролів і активувати політики ротації паролів. Комплексне управління доступом може бути непрактичним для невеликих організацій, але залишається важливим управляти дозволами за допомогою ролей або груп, а не окремих користувачів.

Адміністратори також повинні посилити правила доступу до бази даних:

– нульові паролі не повинні бути дозволені;

– тимчасові інсталяційні файли, які можуть містити паролі, слід видалити;

– облікові записи за замовчуванням слід видалити, якщо вони не потрібні, або змінити паролі з налаштувань за замовчуванням;

– потрібно вимагати унікальні ідентифікатори для всіх користувачів для відстеження та реєстрації;

– користувачі та програми повинні використовувати окремі облікові записи;

– неактивні користувачі повинні бути відключені або видалені;

– підвищені привілеї бази даних слід реєструвати, повідомляти про них та потенційно створювати сповіщення системи безпеки;

– групи користувачів і права доступу слід періодично переглядати;

– облікові записи повинні автоматично блокуватися після кількох невдалих входів, як правило, рекомендовано шість невдалих спроб входу.

Адміністратори повинні мати лише мінімальні повноваження, необхідні для виконання необхідних завдань, і лише протягом періоду, який їм потрібен. Привілейований доступ має надаватися тимчасово та постійно скасовуватися. Більші організації автоматизують управління доступом за допомогою програмного забезпечення для управління привілейованим доступом, що, в свою чергу, надає авторизованим користувачам тимчасовий пароль, реєструє дії та запобігає передачі паролів.

Подібно до того, як сервер має бути захищений, база даних також має бути захищена, щоб запобігти простим атакам і експлойтам. Зміцнення бази даних залежить від типу платформи бази даних, але загальні кроки включають посилення захисту паролем і контроль доступу, захист мережевого трафіку і шифрування конфіденційних полів у базі даних.

Усі невикористані або непотрібні служби або функції бази даних слід видалити або вимкнути, щоб запобігти нерозпізнаному використанню. Усі елементи управління безпекою бази даних, які надає база даних, мають бути ввімкнені. Деякі з них буде ввімкнено за замовчуванням, а інші можуть мати певні причини для вимкнення, але кожен із них слід оцінити та задокументувати всі причини вимкнення елементів управління. За можливості адміністратори можуть увімкнути безпеку на рівні рядків і динамічне маскування конфіденційних даних.

Адміністратори також повинні постійно перевіряти дані, щоб виявити конфіденційні дані з метою визначення, чи потрібно змінити відокремлені таблиці або застосувати додатковий захист.

Адміністратори повинні постійно контролювати та перевіряти журнали баз даних, дані та діяльність, зокрема:

– журнали входу користувачів, особливо спроб і невдалих входів;

– заблоковані облікові записи (через надмірну кількість невдалих спроб входу);

– підвищення привілеїв бази даних;

– вилучення, копіювання або видалення даних бази даних (особливо масштабні зміни або вилучення);

– доступ до конфіденційних або регламентованих даних (може знадобитися для відповідності);

– створення нового облікового запису.

Перевірки часто можуть виявити аномальну активність, а групи безпеки можуть створювати сповіщення безпеки про критичні події, щоб попередити команди безпеки або ввімкнути інформацію про безпеку та управління подіями. Моніторинг активності бази даних і програмне забезпечення для моніторингу цілісності файлів може надавати спеціалізовані сповіщення безпеки незалежно від власних функцій журналювання та аудиту бази даних.

Хоча перевірки можуть виявити зловмисну активність, що триває, організаціям не слід чекати атак, щоб перевірити розгортання своїх баз даних. Постачальники баз даних слід стежити за оновленнями баз даних з мінімальною затримкою.

Бази даних структурують дані, але дані, що містяться в базі даних, також потребують захисту. Перший крок вимагає, щоб організація зберігала лише захищені дані. Усунення надмірних даних або видалення непотрібної історичної інформації може мінімізувати ризик.

Далі потрібно навмисно контролювати дані. Надмірність захищених даних повинна бути усунена в усій системі, і, де це можливо, слід уникати виходу захищених даних за межі системи запису. Функції хешування можна застосовувати до захищених елементів даних перед збе-

реженням даних, необхідних для цілей зіставлення поза системою. Усюди, де це можливо, захищені дані, такі як інформація про стан здоров'я чи номери кредитних карток, слід відокремлювати від особистої інформації.

Шифрування також слід застосовувати для додаткового захисту. Багато постачальників пропонують рішення для шифрування даних у стані спокою, даних у дорозі або навіть даних у використанні. Деякі інструменти шифрування навіть дозволяють обробляти та шукати дані без дешифрування, щоб дані завжди залишалися зашифрованими та захищеними.

Деякі постачальники хмарних технологій, наприклад Oracle, роблять шифрування збережених даних за замовчуванням або надають інструменти керування ключами шифрування, наприклад, сховище ключів Azure. Однак організації самі несуть відповідальність за забезпечення належного захисту і передачу даних.

Висновки. Таким чином, можна констатувати, що переважна більшість державних реєстрів на даний момент знаходяться на державних майданчиках тих органів, які відповідають за їх обслуговування. Через високу вартість модернізації дата-центрів та швидкий розвиток інформаційних технологій більшість державних дата-центрів використовують застаріле апаратне забезпечення та потребуватимуть комплексної технологічної модернізації в найближчі роки. Що стосується безпеки даних, то лише 60% державних реєстрів мають сертифіковані комплексні системи захисту інформації. Це створює великий ризик для конфіденційності даних, що зберігаються в недостатньо захищеному середовищі. Аналогічна ситуація спостерігається на об'єктах критичної інфраструктури. Відповідно, ключовою передумовою протидії впливу на державні електронні інформаційні ресурси та об'єкти критичної інфраструктури в умовах воєнного стану має стати кардинальна зміна порядку збору, зберігання, передачі й обробки інформації з використанням посилення прав доступу до баз даних, контролю трафіку, шифрування. Саме зазначені дії дозволять забезпечити якісний захист інформації в межах державних інформаційних ресурсів, зокрема, на рівні об'єктів критичної інфраструктури.

ЛІТЕРАТУРА

1. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. Безпека інформації. 2013. Т. 19. № 2. С. 120.
2. Державне підприємство «Українські спеціальні системи». URL: https://uss.gov.ua/.
3. Державна міграційна служба України. URL: https://dmsu.gov.ua/.
4. Державна податкова служба України. URL: https://tax.gov.ua/
5. Деякі питання забезпечення функціонування державних інформаційних ресурсів: Постанова Кабінету Міністрів України від 30 грудня 2022 р. № 1500. URL: https://zakon.rada.gov.ua/laws/show/1500-2022-%D0%BF#Text.
6. Дзьобань О. П. Національна безпека в умовах соціальних трансформацій: методологія дослідження та забезпечення: монографія. Харків: Константа, 2006. 440 с.
7. Додонов О. Г., Путятін В. Г., Валетчик В. О. Інформаційно-аналітична підтримка прийняття управлінських рішень у кризових ситуаціях. Реєстрація, зберігання і обробка даних. 2006. Т. 8. № 1. С. 37–54.
8. Домарацький М. Б. Особливості категоріювання об'єктів критичної інформаційної інфраструктури. Фінансова система та економічна безпека: стан, проблеми, ефективність: збірник тез наукових робіт учасників міжнародної науково-практичної конференції для студентів, аспірантів та молодих учених. – Київ : Аналітичний центр «Нова Економіка», 2019. Ч. 2. С. 91–92.
9. Коцерн радіомовлення, зв'язку та телебачення. URL: https://www.rrt.ua/.
10. Міністерство внутрішніх справ України. URL: https://mvs.gov.ua/.
11. Міністерство юстиції України. URL: https://minjust.gov.ua/.
12. Національний центр резервування державних інформаційних ресурсів. URL: https://uss.gov.ua/natsionalnyj-tsentr-rezervuvannya-derzhavnyh-informatsijnyh-resursiv-2/.
13. Пенсійний фонд України. URL: https://www.pfu.gov.ua/.
14. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20 листопада 2012 року № 5492-VI. URL: https://ips.ligazakon.net/document/T125492?an=718.
15. Про державну реєстрацію актів цивільного стану: Закон України від 1 липня 2010 року № 2398-VI. URL: https://zakon.rada.gov.ua/laws/show/2398-17#Text.
16. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України №447/2021. URL: https://www.president.gov.ua/documents/4472021-40013.
17. Романюк О. Н., Савчук Т. О. Організація баз даних та знань. Вінниця: ВДТУ, 2001.
18. Руденко В. Д. Бази даних в інформаційних системах: навч. посібник. Київ: Фенікс, 2010. 240 с.
19. Ситник Г. П., Олуйко В. М., Вавринчук М. П. Національна безпека України: теорія і практика. Київ: Кондор, 2007. 616 с.
20. Critical infrastructure being repaired in 12 Ukrainian communities. URL: https://www.nefco.int/news/critical-infrastructure-being-repaired-in-12-ukrainian-communities/.
21. Manyika J., Chui M., Brown B., Bughin J., Dobbs R., Roxburgh C. & Hung A. Big data techniques and technologies. Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute, 2011. P. 27–31.