ВИТІК ПЕРСОНАЛЬНИХ ДАНИХ В ЕЛЕКТРОННОМУ УРЯДУВАННІ: РЕАЛІЇ ТА ПРОБЛЕМИ ДЕРЖАВНИХ ВЕБСАЙТІВ І ПОРТАЛІВ

LEAKAGE OF PERSONAL DATA IN ELECTRONIC GOVERNANCE: REALITIES AND PROBLEMS OF STATE WEBSITES AND PORTALS

УДК 005.4:342
DOI https://doi.org/10.32843/pma2663-5240-2020.20.20

Дмитришин М.В.
к. екон. наук, доцентка,
доцентка кафедри управління
та адміністрування
Івано-Франківський навчально-науковий
інститут менеджменту
Західноукраїнського національного
університету

Жураківська М.І.
юристка, магістрантка II курсу
Івано-Франківський навчально-науковий
інститут менеджменту
Західноукраїнського національного
університету

У статті окреслено передумови використання сучасних інформаційних технологій в електронному урядуванні й повсякденному житті людей, що зумовило виникнення проблеми захисту персональних даних в інформаційно-комунікаційних мережах і системах. Наведено приклади витоку персональних даних користувачів таких систем в Україні й за кордоном. Оцінено дії уряду й інших відповідальних органів і структур щодо вжиття заходів із ліквідації витоків, їхніх причин і забезпечення захисту інформаційно-комунікаційних систем у майбутньому. Розкрито сутність персональних даних, процесу обробки персональних даних, захисту персональних даних, інформаційної безпеки, електронного урядування та їхнє нормативно-правове трактування. Виокремлено національні інтереси України в інформаційній сфері згідно з Доктриною інформаційної безпеки України й пріоритети державної політики в інформаційній сфері. Визначено важливість електронного урядування та застосування інформаційних технологій як сучасного способу вдосконалення системи публічного управління та адміністрування. Підкреслено переважання позитивного імпакту використання інформаційних систем над можливою шкодою від їхнього функціонування та наголошено на необхідності вдосконалення захисту персональних даних у цій сфері. Схарактеризовано особливості функціонування офіційних вебсторінок органів державної влади й місцевого самоврядування, а також захист інформації в них. Проаналізовано програмні продукти й послуги, які замовляють державні органи (установи), що пов'язані із захистом персональних даних, у 2016–2020 роках. Досліджено статистику витоку персональних даних у світі й виявлено причини й винуватців таких подій. Окреслено проблеми захисту персональних даних і схарактеризовано способи протидії цьому в іноземних державах. Наведено перелік дій щодо мінімізації витоків персональних даних і покращення їх захисту. Сформульовано напрями вдосконалення системи функціонування електронного урядування в контексті захисту й збереження персональних даних в інформаційно-комунікаційних мережах.

Ключові слова: *персональні дані, витік персональних даних, електронне урядування, інформаційні ресурси, інформаційна безпека, інформаційно-комунікаційні технології, захист інформації.*

The article outlines the prerequisites for the use of modern information technologies in e-government and everyday life, which has led to the problem of personal data protection in information and communication networks and systems. Examples of leakage of personal data of users of such systems in Ukraine and abroad are given. The actions of the government and other responsible bodies and structures to take measures to eliminate leaks, their causes and ensure the protection of information and communication systems in the future were assessed. The essence of personal data, personal data processing, personal data protection, information security, e-government and their legal interpretation are revealed. The national interests of Ukraine in the information sphere in accordance with the Doctrine of Information Security of Ukraine and the priorities of the state policy in the information sphere are singled out. The importance of e-government and the use of information technologies as a modern way to improve the system of public administration and administration is determined. The predominance of the positive impact of the use of information systems over the possible damage from their operation and the need to improve the protection of personal data in this area are emphasized. The peculiarities of the functioning of the official web pages of public authorities and local governments, as well as the protection of information in them are described. The software products and services ordered by government agencies (institutions) related to personal data protection in 2016–2020 are analyzed. The statistics of personal data leakage in the world have been studied and the causes and culprits of such events have been identified. The problems of personal data protection are outlined and the ways to counteract this in foreign countries are described. The list of actions to minimize the leakage of personal data and improve their protection is given. The directions of improvement of the system of functioning of e-government in the context of protection and storage of personal data in information and communication networks are formulated.

Key words: *personal data, personal data leakage, e-government, information resources, information security, information and communication technologies, information protection.*

Постановка проблеми в загальному вигляді. Досить швидко розвиваються інформаційні (цифрові) технології. Як і все цивілізоване суспільство, зокрема, органи державної влади й люди «на повну» споживають блага такого розвитку. Усе частіше суспільство використовує у своїй життєдіяльності інформаційні технології, як у державному управлінні, так і в побуті. В Україні також почало швидко розвиватись електронне урядування, а автоматизація окремих функцій і процесів публічного управління сприяла економії ресурсів і часу. Однак широкомасштабне застосування інформаційних технологій пов'язане з додатковими ризиками й загрозами щодо захисту персональних даних.

Більшість членів суспільства внаслідок масового й неконтрольованого доступу до інформаційно-комунікаційних мереж отримала доступ до великих обсягів інформації.

Як наслідок, приватність стала «відкритою», а увагу суспільства періодично привертають інформаційні скандали, що й зумовлює зацікавленість у проблематиці захисту персональних даних.

Зокрема, в січні 2020 р. увагу українського суспільства привернула подія, пов'язана з виявленням витоку персональних даних у мережі Інтернет щодо громадян, які зареєструвались на сайті career.gov.ua для проходження конкурсу на державну службу. Персональні дані громадян – копія паспорта й інші скановані документи, які особа завантажує до Єдиного порталу вакансій, – знаходились у вільному доступі.

На таку подію оперативно відреагувала Уповноважена Верховної Ради України з прав людини, давши доручення Уповноваженого працівникам Департаменту у сфері захисту персональних даних здійснити моніторинговий візит до Національного агентства України з питань державної служби, яке відповідно до законодавства здійснює адміністрування Єдиного порталу вакансій державної служби [1].

Як наслідок, у Раді національної безпеки й оборони України відбулося позачергове засідання робочої групи з реагування на кіберінциденти й протидії атакам на державні інформаційні ресурси при Національному координаційному центрі кібербезпеки (далі – НКЦК). На засіданні оперативно організовано роботу щодо виявлення вразливості, подолання її наслідків і забезпечення сталої роботи Єдиного порталу вакансій career.gov.ua Національного агентства України з питань державної служби й належного захисту персональних даних. Наголошено на важливості питань кібербезпеки в процесах цифрової трансформації держави й необхідності забезпечення органами державної влади належного кіберзахисту власних інформаційних систем [2].

Ще один витік персональних даних відбувся в травні 2020 р. У Telegram з'явився бот, який за гроші поширював персональні дані українців: інформацію з банківських реєстрів, зокрема дані з «ПриватБанку» до його націоналізації; із соцмереж, зокрема логіни й паролі з мереж «ВКонтакті» й Linkedin; із закордонних і внутрішніх паспортів; з електронної пошти; з водійських посвідчень [3].

З'явилися претензії до Міністерства цифрової трансформації України щодо витоку даних із мобільного додатка «Дія», який з'явився 6 лютого в Україні й підтягує електронну версію документів із державних реєстрів. У мобільному додатку зберігаються основні документи в цифровому вигляді, а саме: ID-картка, закордонний паспорт, студентський квиток, водійські права, техпаспорт на авто. Додаток завантажили понад два мільйони користувачів, а на початку квітня запрацював однойменний вебпортал, що є частиною проєкту «держава в смартфоні» Міністерства цифрової трансформації України й покликаний перевести в онлайн отримання більшості державних послуг.

Проте 12 травня 2020 р. на офіційному сайті Міністерства й Комітету цифрової трансформації України спростовано звинувачення щодо розповсюдження та витоку персональних даних громадян із додатка.

За фактом витоку персональних даних Нацполіцією розпочато розслідування кримінального провадження щодо несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку [4].

На жаль, це не перший і не останній випадок витоку персональних даних не лише в Україні, але й у світі.

Так, у березні 2018 р. стало відомо про найбільший витік особистих (персональних) даних користувачів Facebook: ідентифікатори, імена й номери телефонів понад 300 мільйонів користувачів просочились у глобальну мережу Інтернет [5].

Перед тим, у 2016 р., відбувся витік інформації (документів), що мав назву «Панамські папери», які розкрили масштабні міжнародні схеми ухилення від податків через секретні рахунки в офшорах [6].

Як ми бачимо, цінність інформації вже давно не співрозмірна з вартістю зазнаних збитків, навпаки, значно перевищила вартість матеріальних об'єктів, а у сфері інформаційних технологій і поготів. Розвиток інформаційно-комунікаційних технологій потребує впровадження вдалих механізмів захисту, які здатні будуть захистити права й свободи носіїв персональних даних. Інформація про особу й забезпечення захисту цієї інформації потребує неабиякої уваги з боку захисту інформації в органах державної влади й у масштабах країни в цілому.

Аналіз останніх досліджень і публікацій. Незважаючи на те, що тема захисту персональних даних у контексті розвитку електронного урядування в Україні відносно нова, однак дослідженню окремих аспектів проблеми було присвячено праці українських науковців. Зокрема, О. Гронь досліджував проблеми захисту персональних даних у контексті сучасної комунікації [7], О. Бернадзюк – роль і місце цифрових технологій у сфері публічного управління [8], Н. Ющенко й М. Ковтун – стан і перспективи розвитку електронного уряду-

вання [9], М. Рощук – правові аспекти забезпечення безпеки інформації в процесі розвитку електронного урядування України [10].

Виділення не вирішених раніше частин загальної проблеми. Вищезазначена проблема багатогранна й комплексна, тому потребує системного дослідження причин витоку персональних даних, обставин, за яких вони трапились, оцінки наслідків витоків персональних даних, способів їх усунення та вдосконалення системи захисту даних у процесі функціонування системи електронного урядування в Україні.

Мета статті – дослідити проблему захисту персональних даних в інформаційно-комунікаційних мережах та електронному урядуванні в час інформаційного суспільства.

Виклад основного матеріалу. Стаття 2 Закону України «Про захист персональних даних» визначає персональні дані як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [11].

Поняття «персональні дані» викладено ще в деяких нормативно-правових актах, таких як Законі України «Про інформацію» [12], Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [13], Директиві 95/46/ЄС Європейського Парламенту й Ради «Про захист фізичних осіб під час обробки персональних даних і про вільне переміщення таких даних» [14].

Стаття 32 Конституції України встановлює, що ніхто не може зазнавати втручання в його особисте й сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту й прав людини [15]. Саме ця норма Конституції України є основою на предмет захисту персональних даних, від якої «відштовхуються» всі законодавчі норми.

Захист персональних даних є сукупністю правових, організаційних і технічних заходів, спрямованих на недопущення неправомірних дій із персональними даними, забезпечення їх конфіденційності, а також можливості доступу суб'єктів персональних даних до інформації про дії з їхніми персональними даними. Інститут захисту персональних даних є елементом державної системи захисту інформації, що забезпечує особисту безпеку, підтримує баланс інтересів особистості, суспільства й держави у сфері обробки інформації [16].

Інформаційна безпека є не лише самостійною складовою частиною національної безпеки, а й складником інших сфер національної безпеки держави, спрямованим на забезпечення національних інтересів у цих сферах. Це такі складові частини інформаційного середовища України, як інформаційні ресурси, інформаційна інфраструктура й інформаційні технології [17].

Крім того, згідно зі статтею 22 Закону України Про національну безпеку України Державна служба спеціального зв'язку й захисту інформації України є державним органом, призначеним для забезпечення функціонування та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту яких встановлена законом, криптографічного й технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону [18].

Доктрина інформаційної безпеки України визначає, що національними інтересами України в інформаційній сфері є:

1) життєво важливі інтереси особи:

– щодо забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

– щодо забезпечення конституційних прав людини на захист приватного життя;

2) життєво важливі інтереси суспільства й держави:

– забезпечення вільного обігу інформації, крім випадків, передбачених законом; забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;

– захищеність державної таємниці й іншої інформації, вимоги щодо захисту якої встановлені законом.

Доктрина інформаційної безпеки України визначає, що пріоритетами державної політики в інформаційній сфері мають бути:

1) щодо забезпечення інформаційної безпеки:

– створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

– розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;

2) щодо забезпечення захисту й розвитку інформаційного простору України, а також конституційного права громадян на інформацію:

– розвиток правових інструментів захисту прав людини й громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист;

3) щодо відкритості й прозорості держави перед громадянами:

– розвиток механізмів електронного урядування [19].

Визначення терміну «електронне урядування» було запроваджено в Концепції розвитку електронного урядування в Україні як форму організації державного управління, яка сприяє підвищенню ефективності, відкритості й прозорості діяльності органів державної влади й органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян.

Розвиток електронного урядування визначено одним із першочергових пріоритетів реформування системи державного управління [20].

Одним із пріоритетних завдань щодо розвитку інформаційного суспільства є надання громадянам та юридичним особам інформаційних та інших послуг шляхом використання електронної інформаційної системи «Електронний Уряд», яка забезпечує інформаційну взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій.

Єдиний вебпортал органів виконавчої влади є центральною частиною електронної інформаційної системи «Електронний Уряд», призначеною для інтеграції вебсайтів, електронних інформаційних систем і ресурсів органів виконавчої влади й надання інформаційних та інших послуг із використанням мережі Інтернет [21].

Порядком оприлюднення в мережі Інтернет інформації про діяльність органів виконавчої влади встановлено, що інформаційне наповнення, захист інформації від несанкціонованої модифікації та технічне забезпечення функціонування офіційних вебсайтів (вебпорталів) міністерств, інших центральних і місцевих органів виконавчої влади як складових частин Єдиного вебпорталу зазначені органи здійснюють самостійно [22].

Єдиний портал вакансій державної служби є складовою частиною реформи державного управління. Його мета – зробити інформацію про вакансії доступною для широкого кола людей, спростити процедуру подачі й таким чином залучити до роботи в державних структурах найкращих фахівців, що стануть агентами змін у державній службі. Портал дає можливість: відстежувати наявні вакансії; створити власний профіль; переглянути перелік документів, необхідних для участі в конкурсі на посаду, завантажити необхідні документи й подати заявку на вакансії онлайн [23].

Національне агентство України з питань державної служби (далі – НАДС) є центральним органом виконавчої влади, який забезпечує формування та реалізує державну політику у сфері державної служби, здійснює функціональне управління державною службою в органі державної влади, іншому державному органі, його апараті (секретаріаті). НАДС відповідно до покладених на нього завдань: 12^{-2}) забезпечує та здійснює розвиток, впровадження та технічне супроводження інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем і технологій у сфері, що належить до компетенції НАДС, автоматизацію процедур проведення конкурсу на зайняття посад державної служби, зокрема проведення тестування кандидатів на зайняття посад державної служби; 12^{-4}) здійснює адміністрування Єдиного порталу вакансій державної служби [24].

З цього можна зробити висновок, що на НАДС покладено обов'язок щодо здійснення інформаційного захисту Порталу вакансій державної служби. Незважаючи на це, НАДС виявилось не готовим і неспроможним у повному обсязі здійснити захист порталу на предмет витоку з нього персональних даних, у розпорядженні якого вони перебували й оброблялись.

Під обробкою персональних даних мається на увазі будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання та поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем. Усі суб'єкти відносин, пов'язаних із персональними даними, такі як володільці, розпорядники персональних даних і треті особи, зобов'язані забезпечити захист цих даних від випадкової втрати або знищення, від незаконної обробки, в тому числі незаконного знищення чи доступу до персональних даних [12].

Важливим із боку використання технології інформаційної безпеки в системах електронного урядування, проте, як показує досвід, не повністю ефективним є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

Як бачимо з вищенаведеного, законодавець зобов'язав державні органи самостійно здійснювати інформаційне наповнення, захист інформації від несанкціонованої модифікації та технічне забезпечення функціонування офіційних вебсайтів (вебпорталів). Державні органи (установи) замовляють програмні продукти й послуги в різних приватних фірм. Дані офіційного порталу (2020 рік) оприлюднення інформації про публічні закупівлі України вебпорталу Публічних закупівель Прозорро [25] з 2016 року наведено в таблиці 1.

Надавачами таких послуг, як правило, є товариства з обмеженою відповідальністю, фізичні особи-підприємці, приватні підприємства. Обсяги, види й суми вражають. Державні кошти освоюють приватні структури, оскільки відсутній державний орган, який би міг надавати такі послуги. Зокрема, розробляв би програмний продукт щодо захисту інформаційних ресурсів (вебсайтів, порталів) органів державної влади від неправомірних дій стосовно витоку й захисту інформації.

Залишається відкритим питання, хто саме винен у витоку персональних даних, унаслідок чиїх неправомірних дій стаються витоки.

Згідно зі статистикою, кількість випадків витоку даних у США у 2019 році (1 473), збільшилась на 17 відсотків у порівняні із загальною кількістю у 2018 році (1 257), про що повідомляє Identity Theft Resource Center – неприбуткова організація, що фіксує порушення використання персональних даних [26].

За даними Експертно-аналітичного центру InfoWatch (проводять дослідження витоків конфіденційної інформації), у 2019 році число скомпрометованих записів персональних даних майже вдвічі перевищило світове населення. Це означає, що багато людей могли неодноразово ставати жертвами витоків персональних даних через різні інциденти. Складова частина витоку даних становить: 74,8% – персональні дані, 10,78% – платіжна інформація, 10,50% – комерційна таємниця та ноу-хау, 4,50% – державна таємниця.

За світовою статистикою майже пропорційно поділені неправомірні дії порушника щодо витоку інформації, як внутрішнього, так зовнішнього, які стали причиною витоку (46,4% – внутрішній порушник, 53,6% – зовнішній злочинець). А сукупний обсяг даних, скомпрометованих через внутрішні витоки, У 2019 році склав 9,87 млрд записів. Уперше за весь час спостережень обсяг записів, скомпрометованих через внутрішні витоки, перевищив аналогічний показник для витоків зовнішніх.

До недавнього часу серед дослідників була поширена думка, що найнебезпечнішими для володільців інформації є дії зовнішніх зловмисників – хакерські атаки. Феномен внутрішніх витоків набув нового значення: за обсягом скомпрометованих даних внутрішні витоки не тільки зрівнялись, а й удвічі перевищили зовнішні витоки. Очевидна небезпека внутрішніх витоків змусила серйозно переглянути підходи до захисту інформації, насамперед персональних даних і платіжної інформації.

Стосовно розподілу внутрішніх витоків по винуватцю, найактуальнішою протягом останніх років виглядає проблема так званого «при-

Таблиця 1

Програмні продукти й послуги, які замовляють державні органи (установи), що пов'язані із захистом персональних даних [25]

№	Назва послуги	Кількість тендерів	Код
1	Послуги, пов'язані з програмним забезпеченням.	48191	72260000-5
2	Послуги з програмування та консультаційні послуги з питань програмного забезпечення.	69690	72260000-7
3	Послуги у сфері інформаційних технологій, консультування, розроблення програмного забезпечення, послуги мережі інтернет і послуги з підтримки.	129392	72000000-5
4	Послуги з розробки пакетів програмного забезпечення.	3111	72210000-0
5	Послуги у сфері управління даними.	23625	72300000-8
6	Послуги з обробки даних.	18436	72310000-1
7	Послуги з розробки системного й користувацького програмного забезпечення.	113	72211000-7
8	Послуги, пов'язані з роботою з електронними таблицями.	59	72311000-8
9	Послуги з перетворення даних.	14	72311100-9
10	Послуги з розробки прикладного програмного забезпечення.	530	72212000-4
11	Послуги з розробки галузевого програмного забезпечення.	55	72212100-0

вілейованого користувача» – співробітника, чиї права доступу до інформації, оброблюваної в компанії, практично не обмежені, водночас контроль дій такого співробітника не організований або здійснюється не в повному обсязі.

Як правило, до привілейованих користувачів відносять топменеджмент (керівників) компаній та організацій, системних адміністраторів і прирівняних до них співробітників (у тому числі офіцерів безпеки).

Такий аналіз дає підстави припускати, що витік персональних даних із державних інформаційних ресурсів приблизно на 50% стається з вини працівників (внутрішніх порушників) того чи іншого державного органу, що містить і певний відсоток вини керівництва. Також немала частка витоку персональних даних траплялась із вини підрядника (партнера), а саме через неякісний програмний продукт, послуги, пов'язані з програмним забезпеченням, послуги у сфері інформаційних технологій, консультування, розроблення програмного забезпечення, послуг мережі інтернет і послуги з підтримки.

На жаль, захищеність персональних даних українських громадян лишається «відкритою», оскільки в Україні досі відсутній регуляторний орган, який би ефективно наглядав за дотриманням законодавства у сфері захисту персональних даних. Закон України «Про захист персональних даних» залишив відкритим питання щодо дієвого механізму шляхом системного контролю за виконанням щодо захисту персональних даних. Хоча стаття 22 Закону України «Про захист персональних даних» [11] передбачає, що контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснюють такі органи, як Уповноважений, суди, проте ефективність цього закону залишається низькою, а притягнути до відповідальності того, хто «зливає» або «сприяє зливу» бази персональних даних, дуже важко.

Уповноважений має, зокрема, такі повноваження у сфері захисту персональних даних: складати протоколи про притягнення до адміністративної відповідальності й направляти їх до суду у випадках, передбачених законом. Кіберполіція розслідує кримінальні правопорушення, зокрема щодо витоку персональних даних із Державних реєстрів.

Відповідно до даних Єдиного державного реєстру судових рішень [28], налічується така кількість судових рішень щодо порушення законодавства у сфері захисту персональних даних у порядку статті 188-39 Кодексу про адміністративні порушення України:

– 13 за 6 місяців 2020 року;
– 16 за 2019 рік;
– 20 за 2018 рік;
– 18 за 2017 рік.

Уповноважений законодавчо обмежений самостійно притягувати до відповідальності винних осіб, лише зі зверненням до суду, що своєю чергою затягується в часі.

Як відомо, володільцем найбільшої кількості персональних даних є держава, тому саме до неї висуваються найсуворіші вимоги щодо їх збереження та уникнення поширення у випадках, коли це не передбачається згодою особи. Очевидно, що витік інформації з державних баз даних лише посилює недовіру до держави й створює відчуття незахищеності перед внутрішніми й зовнішніми загрозами. Таким чином, ми не можемо говорити про захист персональних даних приватними особами, якщо навіть державні бази даних перебувають під загрозою. На жаль, забезпечити абсолютний захист персональних даних наразі не може жодна держава у світі, проте особа може обмежити обсяг тих відомостей, на обробку яких вона надає згоду [29].

Прикладом ефективного механізму захисту персональних даних є Європейський Союз, де з 25 травня 2018 року почав діяти новий Закон про захист конфіденційних даних. GDPR – General Data Protection, що в перекладі означає загальний регламент роботи. Такий нормативний акт Європейського Союзу, який підлягає до виконання на території всіх держав-учасниць, стосується правил поводження з персональними даними. Регламент зачіпає будь-яку дію щодо роботи з персональними даними, а саме збору, зберігання, передачі.

Закон передбачає великі штрафи для компаній-порушників: за порушення основних принципів обробки даних; порушення правил передання персональних даних, ігнорування заборони наглядового органу на обробку даних; порушення прав суб'єкта тощо. Передбачено накладення штрафу у розмірі 4% від загального річного обороту підприємства або 20 млн євро (залежно від того, яка сума буде більшою). За порушення порядку повідомлення про інцидент, відсутність співробітника із захисту даних, де це необхідно, незаконну обробку персональних даних дитини тощо передбачено менші, проте не менш істотні штрафи – 10 млн євро, або 2% від загального річного обороту підприємства [30].

Регламент встановлює також вищі стандарти безпеки на захист інформації, вимагає відповідних організаційних і технічних дій. Зокрема, норми Регламенту орієнтовані на забезпечення принципів прозорості, підзвіт-

ності й захисту прав громадян, серед ключових є такі:

– розпорядник (обробник) інформації зобов'язаний повідомити відповідному органу влади про інцидент порушення безпеки персональної інформації протягом 72 годин та якомога швидше всіх суб'єктів інформації;

– портативність даних – суб'єкт інформації має право отримати від розпорядника свої персональні дані в машинозчитуваному форматі й передати їх до іншого розпорядника;

– право на доступ – суб'єкт інформації має право звертатись до розпорядника з питаннями: яка інформація, пов'язана з ним, зберігається / обробляється, з якою метою, в який спосіб і де саме, а розпорядник зобов'язаний безкоштовно надати цифрову копію всієї збереженої персональної інформації на вимогу;

– право на забуття – суб'єкт інформації має право вимагати в розпорядника інформації припинення будь-якої обробки, зберігання та подальшого розповсюдження всіх персональних даних;

– відповідальні за безпеку інформації співробітники – Регламент також змінює порядок зберігання записів для великих організацій, що займаються збереженням та обробкою персональних даних у великих об'ємах і на постійній основі [30].

Є підстави вважати, що у зв'язку зі значними розмірами штрафів і запровадженням нових вимог щодо збору, зберігання та передачі зафіксовано падіння витоку персональних даних у 2018 році. Жорсткі правила щодо забезпечення безпеки інформації допоможуть ефективніше захистити персональні дані й дисциплінувати порушників. Варто аналогічні норми запровадити в українському законодавстві щодо захисту персональних даних.

Ураховуючи прагнення України до Євроінтеграції, було б доцільно провести аналогічні кроки щодо захисту персональних даних, такі як у Регламенті, а саме, як зазначає Infowatch:

Крок 1. Провести аудит персональних даних і задокументувати весь процес обробки персональних даних [31].

Крок 2. Визначити законні підстави для обробки персональних даних.

Крок 3. Розробити політику з обробки й захисту персональних даних.

Крок 4. Призначити відповідальних за захист персональних даних.

Крок 5. Провести оцінку інформаційних ризиків, у тому числі оцінку впливу на захист персональних даних (DPIA).

Крок 6. Забезпечити права суб'єктів даних.

Крок 7. Упровадити систему обробки запитів суб'єктів даних.

Крок 8. Упровадити необхідні заходи щодо захисту персональних даних.

Крок 9. Реалізувати безпечне транскордонне передання персональних даних.

Крок 10. Розробити й упровадити процес реагування на інциденти [27].

Інформаційні технології щільно інтегрувалися у сферу урядування, оскільки застосування таких технологій дало можливість підвищити ефективність автоматизації деяких функцій і механізмів публічного управління шляхом економії часу й інших ресурсів, унаслідок чого створюються умови для доступності, відкритості й прозорості діяльності суб'єктів публічного права. Проте обсяги й масштаби застосування таких технологій у державному управлінні щільно пов'язані із загрозами й ризиками, що несуть у собі можливості цих технологій.

Часто витік персональних даних трапляється через халатність персоналу, невідповідність рівня підготовки працівників чи недостатню увагу органів публічної влади до захисту інформації та супроводу вебсайтів, а також низькою цифровою грамотністю українців у цілому.

Висновки. Вищезазначене дає підстави вважати, що зі стрімким розвитком інформаційних технологій необхідно приділити особливу увагу захисту інформації на вебпорталах і вебсайтах органів державної влади.

По-перше, на часі створення державного органу, який розробляє програмне забезпечення щодо захисту персональних даних (натепер цим займаються лише приватні установи, продукт яких купують державні установи, які є замовниками таких послуг), або посилення відповідальності за неякісний захист виготовленої програми.

По-друге, внести зміни щодо виплати у вигляді відшкодування (компенсації) за витік персональних даних особі, чиї дані були неправомірно «злиті» (натепер лише передбачена адміністративна відповідальність за зверненням уповноваженої з прав людини щодо статей 188-39 і 188-40 Кодексу України про адміністративні правопорушення від ста до двохсот неоподатковуваних мінімумів доходів громадян на посадових осіб, від двохсот до чотирьохсот неоподатковуваних мінімумів доходів громадян на громадян – суб'єктів підприємницької діяльності (від 340 до 6800 грн – мізерний штраф в контексті порушення прав людини)).

По-третє, призначити в органі осіб, які відповідальні за захист персональних даних (натепер є лише уповноважені особи за надання відповідей за публічною інформацією), на аналог вимог у Регламенті.

По-четверте, провести навчання з працівниками, які опрацьовують персональні дані, й передбачити відповідальність за дії особи, внаслідок яких стався витік інформації

По-п'яте, прописати норму, де орган, який у процесі діяльності володів персональними даними, повинен автоматично знищувати їх після обробки (для прикладу: 1) особа звертається до банку із заявкою про отримання кредиту (долучає паспорт, код і так далі), а банк відмовляє у видачі, проте персональні дані залишають у володінні банку, хоча логічно, щоб дані знищувались; 2) особа звертається із заявою на конкурс на посаду, аналогічно, долучає копії документів із персональними даними, конкурс не пройшла, дані в органі зберігаються, а їх слід знищити).

По-шосте, розробити механізм, за якого власник персональних даних мав би можливість самостійно знищувати, переглядати, змінювати персональні дані, які подає.

По-сьоме, створити єдину базу персональних даних, з якої б уповноважені особи відповідних органів самостійно у випадку потреби отримували персональні дані особи, на певний час і на виконання певної дії (для прикладу: 1) коли відповідна особа заходить у Державний реєстр речових прав на нерухоме майно, в якому фіксується посекундний вхід особи в реєстр і всі дії; 2) коли особа звертається з відповідною заявою про отримання кредиту, участі в конкурсі, звернення на отримання відповідних соціальних виплат, отримання субсидії, призначення пенсії та інше, орган, до якого звертаються, самостійно б генерував із такої бази необхідні дані).

Ключовою проблемою витоку персональних даних є відсутність централізованого захисту, оскільки кожен орган «точково» здійснює самостійний захист свого вебсайту чи вебпорталу. Витік персональних даних насамперед є проблемою не локального характеру, тобто не лише одного з державних органів влади, а цілком глобального характеру в розрізі забезпечення інформаційної безпеки національних інтересів України. Отже, це потребує комплексних дій стосовно централізованого захисту вебсайтів і вебпорталів органів державної влади, оскільки інформаційна безпека є складовою частиною державної безпеки.

ЛІТЕРАТУРА:

1. Повідомлення про витік персональних даних кандидатів на посади державної служби: перевіряємо інформацію та обставини. *Уповноважений Верховної Ради України з прав людини* : вебсайт. URL: http://www.ombudsman.gov.ua/ua/page/secretariat/press-office/pr/ (дата звернення: 26.10.2020).

2. НКЦК оперативно організував роботу щодо забезпечення сталої роботи порталу career.gov.ua і належного захисту персональних даних. *Рада національної безпеки і оборони України* : вебсайт. URL: https://www.rnbo.gov.ua/ua/Diialnist/3464.html (дата звернення: 26.10.2020).

3. Солонина Є.О. Злив персональних даних українців: що сталося і як захиститися. *Радіо Свобода* : вебсайт. URL: https://www.radiosvoboda.org/a/zlyv-danyx-i-diya/30610626.html (дата звернення: 26.10.2020).

4. Нацполіція розпочала кримінальне провадження за фактом витоку інформації про персональні дані громадян. *Національна поліція* : вебсайт. URL: https://www.npu.gov.ua/news/ (дата звернення: 26.10.2020).

5. Bischoff P. Report: 267 million Facebook users IDs and phone numbers exposed online (UPDATE: now 309 million). URL: https://www.comparitech.com (Last accessed: 26.10.2020).

6. Panama papers. URL: https://panamapapers.sueddeutsche.de/en/ (Last accessed: 26.10.2020).

7. Гронь О.В., Погореленко А.К. Проблеми захисту персональних даних у контексті сучасної комунікації. *Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство*. 2018. Вип. 19 (1). С. 102–108.

8. Берназюк О.О. Роль та місце цифрових технологій у сфері публічного управління. *Підприємництво, господарство і право.* 2017. № 10. С. 166–170.

9. Ющенко Н.В., Ковтун М.В. Електронне урядування в Україні: стан та перспективи розвитку. *Причорноморські економічні студії.* 2019. Вип. 38. С. 152–157.

10. Рощук М.В. Розвиток електронного урядування в Україні: правовий аспект забезпечення безпеки інформації. *Безпека інформації.* 2018. Т. 24. № 1. С. 17–22.

11. Про захист персональних даних : Закон України від 01 червня 2010 р. № 2297-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 26.10.2020).

12. Про інформацію : Закон України від 02 жовтня 1992 р. № 2657-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 26.10.2020).

13. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи № 108 від 28 січня 1981 р. *База даних «Законодавство України».* URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 26.10. 2020).

14. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 р. *База даних «Законодавство України».* URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 26.10.2020).

15. Конституція України : Закон України від 28 червня 1996 р. №254к/96-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 26.10.2020).

16. Єсімов С.С. Захист персональних даних у контексті розвитку динамічних систем. *Науковий вісник державного університету внутрішніх справ*. 2013. № 3. С. 198–207.

17. Інформаційна безпека особистості, суспільства, держави : підручник / Я.М. Жарков, М.Т. Дзюба, І.В. Замаруєва та ін. Київ : Видавничо-поліграфічний центр «Київський університет», 2008. 274 с.

18. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 26.10.2020).

19. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 р. № 47/2017 / Президент України. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 26.10.2020).

20. Про схвалення Концепції розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text (дата звернення: 26.10.2020).

21. Про заходи щодо створення електронної інформаційної системи «Електронний Уряд» : Постанова Кабінету Міністрів України від 24 лютого 2003 р. № 208 / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/208-2003-%D0%BF#Text (дата звернення: 26.10.2020).

22. Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади : Постанова Кабінету Міністрів України від 4 січня 2002 р. № 3 / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/3-2002-%D0%BF#Text (дата звернення: 26.10.2020).

23. Програма «Електронне врядування задля підзвітності влади та участі громади» (EGAP) : вебсайт. URL: https://egap.in.ua (дата звернення: 26.10.2020).

24. Про затвердження Положення про Національне агентство України з питань державної служби : Постанова Кабінету Міністрів України від 1 жовтня 2014 р. № 500 / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/500-2014-%D0%BF#Text (дата звернення: 26.10.2020).

25. Портал prozorro.gov.ua : вебпортал. URL: https://prozorro.gov.ua/ (дата звернення: 26.10.2020).

26. Identity Theft Resource Center. URL: https://www.idtheftcenter.org (Last accessed: 26.10.2020).

27. Експертно-аналітичний центр InfoWatch : вебсайт URL: https://www.infowatch.ru (дата звернення: 26.10.2020).

28. Єдиний державний реєстр судових рішень. http://www.reyestr.court.gov.ua (дата звернення: 26.10.2020).

29. Фісун В.В. Проблеми захисту персональних даних: досвід України та інших країн. *Юридична Газета* : вебсайт. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html (дата звернення: 26.10.2020).

30. Регламент європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). *База даних «Законодавство України».* URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 26.10.2020).

31. GDPR: General чи все-таки Global? *Вісник МСФЗ* : вебсайт. URL: https://msfz.ligazakon.ua/ua/magazine_article/FZ001542 (дата звернення: 26.10.2020).