УДК 519.711.3:343.98

Кульчицький О. С.;
Грицюк В. В.;
Зотова І. Г.

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Визначення нормативно-правових аспектів захисту персональних даних в інформаційних системах Збройних Сил України

Резюме. Проаналізовані проблемні питання, пов'язані з цілісністю персональних даних при обробці та передачі інформації в розподіленій інформаційний системі управління адміністративно-господарськими процесами Збройних Сил України. Проведено аналіз аспектів забезпечення захисту від посягань на цілісність персональної інформації в інформаційних системах розвинутих держав.

Ключові слова: персональні дані, цілісність персональних даних, інформаційна система, інформаційна система ЗС України.

Постановка проблеми. На даний час зросли спроби направлених атак на сервери державних підприємств та установ, зі спробою отримати певну персональну інформацію про фізичних осіб, а також заподіяти шкоду конфіденційній безпеці, а саме отримати персональну інформацію з подальшим розповсюдженням. В той же час спостерігається активне створення міжнародних просторових інформаційних систем, обіг особистої конфіденційної інформації в яких потребує її захисту. Важливого значення нині набуває законодавчий контроль за розвитком електронного середовища, захисту інформації в інформаційних системах.

Використання інформаційних систем управління ресурсами та прийняття рішень крім зручності у користуванні приховують велику кількість всіляких небезпек в контексті використання ними особистих даних при реєстрації користувачів [1].

Аналіз останніх досліджень і публікацій. В Україні у фахових виданнях досліджені питання як розробки, так і вдосконалення керівних документів і положень щодо захисту персональних даних (далі – ПД), та створення відповідного програмного забезпечення. Цим питання присвячені роботи таких вітчизняних фахівці, як Т. Костецької, М. Щербатюка, В. Брижко, та інших [11,12]. Серед зарубіжних вчених слід відзначити роботи А. Міллера, Р. Холлборга та І. Вельдера[4,5].

Незважаючи на те, що зазначеною проблематикою займалася значна кількість науковців, багато її аспектів нині залишаються малодослідженими або потребують доопрацювання, особливо в контексті правового врегулювання питань захисту ПД та вдосконалення організаційної системи захисту даних для забезпечення національної безпеки. Більшість досліджень за даною тематикою здійснювались для запобігання порушень щодо цілісності ПД, тобто проводився аналіз технічних недоліків в системі захисту, як правило вже після здійснення злочинних кібератак.

Метою статті є обґрунтування оптимальних рішень **щодо захисту ПД в інформаційних системах ЗС України** на основі аналізу досвіду розвинутих країн з питань захисту ПД в інформаційних системах.

Виклад основного матеріалу. У ЗС України з 2006 року розробляється єдина система управління адміністративно-господарськими процесами ЗС України (ЄСУ АГП ЗСУ). Зокрема впроваджені функціональні підсистеми "Майно" та "Житло" ЄСУ АГП ЗСУ, що містять персональні данні військовослужбовців. Така інформація потребує захисту від посягань на її конфіденційність. За допомогою цих даних будь-яка особа може бути ідентифікована та у разі неправомірного використання цієї інформації діяльність особи може бути скомпрометована. Тобто відповідно до українського законодавства та міжнародного права, такі відомості фактично є "*персональними даними*", які визначають невід'ємну частину приватного життя людини [2-3].

Англійськими та американськими вченими-дослідниками досліджене питання щодо необхідності захисту права на приватне

життя людини під час інформаційного обміну в різних інформаційних системах. Кожен користувач має право на приватність, так вважає британський дослідник Артур Міллер та зазначає, що "Потенційні порушення недоторканності приватного життя може спонукати їх відмовитися від використання інформаційних систем. Тому глобальний успіх в розвитку та поширенню інформаційних систем залежить від прийняття відповідних заходів захисту ПД користувачів" [5]. Це висловлення англійського вченого є одним з визначальних при формуванні підходів до захисту ПД в інформаційних системах. В нашій державі прийнято Закон України "Про захист персональних даних", який визначає вимоги щодо обробки та захисту ПД, в тому числі і в інформаційно-телекомунікаційних мережах [2].

Загалом, в Європейських державах правовий захист ПД охоплює майже два десятки загальноєвропейських конвенцій, директив та рекомендацій, кожна країна ЄС видала свої базові нормативно-законодавчі акти, приймалися конкретні закони щодо роботи з персональними даними у різних сферах діяльності.

Положення які відображають вимоги щодо захисту ПД, запроваджені Конвенцією Ради Європи № 108 під час їх обробки в автоматизованій системі [3] та більш докладніше розвинуті у Директиві Європейського Парламенту та Ради 95/46/ЄС про захист користувачів інформаційних систем під час обробки цими системами ПД і вільним обігом цих даних в системі [6]. Питанням щодо захисту ПД в інформаційних системах, присвячені й інші рекомендаційні документи різних європейських установ:

- рекомендації фахівців робочої групи, яка функціонує відповідно до статті 29 Директиви 95/46/ЄС (WP 39 –"Приватність в мережі Інтернет);
- рекомендації фахівців міжнародної робочої групи з питань захисту ПД в телекомунікаційних системах ("Берлінська група") [7].

В основі підходу щодо захисту та обробки ПД лежать відповідні базові принципи щодо їх збору, обробки, зберігання та передачі. Отже ПД мають:

- оброблятися чесно і встановленим законним порядком;
- збиратися для визначених, чітких і законних цілей і надалі не оброблятися у спосіб, несумісний з цими цілями;
- бути достовірними, відповідними і не надлишковими відносно визначених законних цілей, заради яких вони збираються для подальшого їх використання;
- бути точними і, за необхідністю обновлятися (слід вжити всіх законних заходів для гарантій безпеки їх цілісності та достовірності, з урахуванням цілей, заради яких вони використовуються, обробляються, стираються або виправляються);
- зберігатися в тій формі, яка дозволяє встановити особу-суб'єкт даних, (державні органи встановлюють відповідні гарантії для ПД, які зберігаються протягом встановлених термінів);
- оброблятися з дотриманням прав фізичної особи, гарантувати право на доступ до власних даних;
- оброблятися з дотриманням законодавчих вимог захисту конфіденційної інформації;
- не передаватися за межі країни без відповідного захисту, а якщо і передаватись, то з дотриманням міжнародних стандартів стосовно закордонного поширення ПД.

Вказані базові принципи підходу до побудови системи захисту були прийняті ще в 90-роках та враховані інтереси ряду країн світу. На сьогодні деякі правові норми розвинутих країн містяться в імплементованому переліку аналогічних принципів у національному законодавстві або посиланнях на вищезгадану Конвенцію Ради Європи внутрішнім вітчизняним законодавством. Сучасні інформаційні технології щодня удосконалюються, значною мірою змінюються методи і процес збирання та обробки ПД, обмеження доступу до них. На сьогоднішній день продовжує удосконалюватись багатофункціональне інформаційне середовище, в якому зростають вимоги до подальшого захисту ПД, а старі методи та підходи стають вже неефективними.

У жовтні 2012 року, за ініціативи Всеукраїнської громадської організації було прийнято Декларацію "За недоторканність приватного життя в мережі Інтернет", до якої приєдналась низка провідних національних телекомунікаційних компаній, а в лютому 2013 року "Українська асоціація захисту ПД" провела дослідження на тему: "Як забезпечити прозорість та відкритість обробки ПД на веб-ресурсах" [10]. В ході громадського дослідження виявлено, що найчастіше ПД з використанням веб-ресурсів обробляються саме в рамках таких процесів як:

- заповнення користувачами анкет;
- реєстрація та подальша авторизація логіну та паролю;

- реєстрація за визначеним обліковим записом соціальної мережі;

- надання користувачем своєї електронної адреси або телефонного номера для зворотного зв'язку.

З точки зору вітчизняного законодавства (статті 6, 11 Закону України "Про захист ПД") факт реєстрації особи в інформаційній системі є обов'язковим елементом та за згодою клієнта (користувача), із подальшою обробкою (використанням) його ПД певною інформаційною системою. Проте, велика кількість інформаційних систем не дотримується певних правових умов для обробки ПД, а отже фактично у незаконний спосіб обробляють ці дані та передають їх іншим установам. У ході проведеного дослідження з'ясовано, що в багатьох інформаційних системах та мережах, доступних широкому загалу, реєстрація проводиться із врахуванням введення особистих даних, відповідно до яких користувач може бути ідентифікований, а саме:

1) ПІБ;

2) географічне місцезнаходження, місце навчання тощо;

3) телефонні контакти.

Усі дані про особу заповнюються суб'єктом ПД без попередження про їх можливе подальше використання за час функціонування інформаційної системи. З одного боку, можна уникнути цієї проблеми шляхом введення недостовірних відомостей, але фактично дана соціальна мережа являється більшою мірою утилітою, яку використовують з метою розваги, проте, якщо ж особа має намір створити персональну сторінку з метою спілкування чи з іншою метою, обов'язковими умовами якої є зазначення "правдивих відомостей", за якими вона може бути ідентифікована, то тут виникає проблемна правова ситуація.

З метою вирішення такої проблеми пропонуємо ввести опцію, суть якої буде зводитись до того, що в процесі реєстрації особи в інформаційній системі обов'язковим початковим етапом стане відповідь фізичної особи на запитання: "Чи згодні ви, що в процесі функціонування вашої персональної сторінки в інформаційній системі можлива обробка ваших ПД?", та визначення відповідальності власників інформаційних систем за її зберігання та недоторканість. З одного боку, це дозволить уникнути поширення даних про особу, яка цього завідомо не бажає, шляхом її фактичного попередження, з іншого – це сприятиме практичній уніфікації національного законодавства України, та змусить власників інформаційних систем більш відповідальніше відноситись до захисту та зберігання наданої інформації. Інший проблемний аспект забезпечення приватності в інформаційних системах – неможливість повністю та остаточно видалити свої дані із особистої сторінки в соціальної мережі. Така проблема порушує так зване особисте право фізичної особи у сфері захисту ПД – "право бути повністю видаленим з мережі" але не дає нам змогу знайти та відстежити злочинців. Ці питання покладаються на відповідні державні органи.

Так зване "право бути повністю видаленим з мережі" існувало в Європі з 1995 року в усіх країнах-членах ЄС (з прийняттям базової Директиви 95/46/ЄС). Кожний користувач будь якої інформаційної системи може вимагати видалити свої дані у будь-який момент. Але навпаки, існують і певні рамки, обмеження. Наприклад, якщо особисті дані використовуються з метою свободи слова та самовираження у засобах масової інформації, і, зрозуміло, якщо в цьому випадку є певна правова неузгодженість, а також, якщо держава або приватна компанія має право обробляти ці дані відповідно до визначеної законної мети їх обробки або узгодження з відповідною особою. Тож обмеження існують, хоча в цілому права фізичної особи мають бути гарантовані, якщо немає підстав для подібних обмежень. На відповідне "право бути повністю видаленим з мережі" приділено чималу увагу у проекті нового Загального регламенту ЄС із захисту ПД, який наразі проходить широке громадське слухання в установах ЄС, в якому від адміністратора безпеки системи до користувача вимагається вироблення чіткого, послідовного правового і технічного механізму реалізації цього права.

Необхідно також врахувати, що Директивою 97/66/ЄС Європарламенту та Ради Європи [8] юридичні, нормативні та технічні вимоги, які регламентують забезпечення захисту ПД, прав фізичних осіб та законних інтересів юридичних осіб повинні бути чітко сформульовані та не створювати перешкод для розвитку у сфері захисту інформації. Досягнення такого балансу є можливим за умови визначення обмеженої та обґрунтованої кількості вимог, що не перешкоджають розвитку новітніх технологій та належному функціонуванню баз ПД. Також, відповідно до вимог Директив Європарламенту та Ради Європи [6, 8] власники інформаційних систем за сприяння Уповноваженого державного органу з питань захисту ПД повинні здійснювати співробітництво в процесі

впровадження та розвитку відповідних технологій для надання гарантій захисту прав фізичних осіб. В усіх розвинутих країнах визнання заходів, які можна вважати адекватними для забезпечення захисту, віднесено до компетенції уповноважених державних органів з питань захисту ПД, в тому числі й шляхом відповідних публікацій та оприлюднень.

Для вирішення цих проблем запропонований підхід за яким уповноважені державні органи з питань захисту ПД пропонують власникам інформаційних систем, де зберігаються особисті данні, самостійно визначати заходи щодо захисту з урахуванням існуючих небезпек:

- можливих ризиків, пов'язаних з обробкою та зберіганням даних в інформаційних системах;
- природа та обсяги порушників, які втручаються в інформаційні системи;
- вартості заходів, щодо впровадження систем захисту в інформаційних системах;
- характеристика та можливості інформаційних систем де циркулює інформація, тощо.

Насамперед, у більшості випадків від власників інформаційних систем, де циркулює особиста інформація не вимагається застосування спеціальних заходів захисту, зокрема загальноприйнятих (описаних в стандартах ISO/IEC 27001). У більшості випадків акцентується увага на наявність кваліфікованих адміністраторів систем управління захистом ПД (в установах, організаціях) та навчання персоналу, при обробці та зберіганні ПД.

Наша держава робить важливі кроки у вирішенні та подоланні проблемних питань та реалізації права на захист ПД. Так у рекомендаціях парламентських слухань на тему "Законодавче забезпечення розвитку інформаційного суспільства в України", затверджених постановою Верховної Ради України від 03.07.14 р. № 1565-VII), міститься рекомендація Уряду України - "забезпечити у середніх загальноосвітніх школах викладення предмету (теми) щодо правил роботи в інформаційних системах (соціальних мережах), участі у загальних форумах, захисту ПД та мережевої етики з урахуванням сучасного стану розвитку інформаційних систем". Ефективність цих рекомендацій Урядом України можна буде оцінити лише після певного проміжку часу.

Слід зазначити, що на сьогодні підтвердження відповідності комплексних систем захисту інформації (далі – КСЗІ) в інформаційних системах, в Україні здійснюється за результатами державної експертизи, у встановленому законодавством порядку. Власники (розпорядники) інформаційних систем, які задовольняють критеріям, визначеним у пункті 1.6 Положення про державну експертизу в сфері технічного захисту інформації [9] з урахуванням змін [10], мають право вільного вибору щодо застосування будь-якого з можливих варіантів (способів) проведення державної експертизи КСЗІ. Проте з урахуванням положень Директив Європарламенту та Ради Європи доцільно розширити перелік інформаційних систем щодо яких можливо застосовувати цю процедуру.

Висновки. Державне законодавство України у сфері захисту ПД постійно реформується з урахуванням досвіду та кращих практичних напрацювань країн ЄС з метою забезпечення якісного рівня захисту ПД.

Засоби та методи використання ПД в неправомірних цілях швидко розвиваються та удосконалюються, саме тому нехтування виконанням заходів захисту ПД, які обробляються в інформаційних системах відомчого призначення може призвести до виникнення умов для неправомірних дій з даною інформацією.

Заходи захисту ПД, механізми, створення органів, відповідальних за захисту ПД слід планувати та здійснювати на упередження неправомірних дій. Слід підкреслити, що захист ПД в усіх сферах національної безпеки держави слід об'єднати під єдине керівництво.

Приведені базові принципи щодо їх збору, обробки, зберігання та передачі дадуть змогу суттєво знизити ризики від витоку інформації, порушення її цілісності та доступності.

Запропонований підхід у сфері захисту ПД дасть змогу підвищити ефективність СЗІ перспективних інформаційних систем відомчого призначення у сферах медицини, логістики, надлишкового військового майна, зокрема функціональної підсистеми "Житло" Єдиної системи управління адміністративно-господарськими процесами Збройних Сил України, в якій згідно технічних вимог обробляється конфіденційна інформація (ПД).

Подальші дослідження доцільно зосередити на пошуку найоптимальніших шляхів вирішення освітлених питань у напрямку захисту особистих даних в корпоративних мережах - з метою забезпечення ефективного захисту ПД користувачів інформаційних систем, запровадження розробки корпоративних кодексів, які будуть

відігравати важливу роль у розвитку національного законодавства у різних сферах з обробки та передачі ПД.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Радкевич О. П. Конфіденційність персональної інформації в соціальних мережах // Вісник Вищої ради юстиції – 2012. – № 3(11). – С. 215-224.
2. Про захист персональних даних: Закон України від 01.06.10р.No 2297-VI // Офіційний вісник України – 2010. – № 49. – 199 с.
3. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28.01.81 р. № 108 // Офіційний вісник України. – 2011. – № 1. – 701 с.
4. Hallborg R.B. Principles of Liberty and Right to Privacy // Law and Philosophy. – 1986. – № 5. – P. 13-20.
5. Arthur R. Reviving territorial privacy in the pervasive computing era. 12 червня 2016 г. Режим доступу:https://www. linkedin.com/pulse/reviving-territorial-privacy-pervasive-computing-era-quentin-baltus
6. Про захист фізичних осіб при обробці персональних даних і вільним обігом цих даних: Директива Європейського парламенту та Ради 95/46/ЄС від 24.10.85 р. – Режим доступу : www.zakon.rada.gov.ua/laws/show/994_242
7. Про захист осіб у зв'язку з обробкою даних у інформаційних магістралях: Рекомендації Ради Європи R(99)5від 09.11.99 р. – Режим доступу: //www.medialaw.kiev.ua/laws/laws_international/105/
8. Директива 97/66/ЄС Європейського Парламенту і Ради "Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі" від 15 грудня 1997 року.
9. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р., № 22.
10. НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформаційних від несанкціонованого доступу".
11. Брижко В. М. Про упорядкування законодавства України із захисту персональних даних / Брижко В. М. // Правова інформатика. – 2008. – № 1(17). – С. 20-34.
12. Костецька Т.А. Інформаційне право України ; навчальний посібник / Костецька Т. А. – К. : Київ. нац. торгово-економічний університет. – 2009. –170 с.

Стаття надійшла до редакції 08.02.2017

Кульчицький А. С.;
Грицюк В. В.;
Зотова И. Г.

Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев

Определение нормативно-правовых аспектов защиты персональных данных в информационных системах Вооружённых Сил Украины

Резюме. Проанализированы проблемные вопросы, связанные с целостностью персональных данных при обработке и передаче информации в распределённой информационной системе управления административно-хозяйственными процессами Вооружённых Сил Украины. Проведен анализ аспектов обеспечения защиты от посягательств на целостность персональной информации в информационных системах развитых государств.

Ключевые слова: персональные данные, целостность персональных данных, автоматизированная система, информационная система ВС Украины.

A. Kulchitsky;
V. Hrytsiuk;
I. Zotova

Center for Military and Strategic Studies National Defence University of Ukraine named after Ivan Chernyhovsky, Kyiv

Determination of normatively-legal aspects of protection of the personal data is in the informative systems of the Armed Forces of Ukraine

Resume. Analysed problem questions related to integrity of the personal data at treatment and information transfer in the distributed informative system of management the administrative processes of the Armed Forces of Ukraine. The analysis of aspects of providing of protecting is conducted from trenching upon integrity of the personal information in the informative systems of the developed states.

Keywords: the personal data, integrity of the personal data, CAS, informative system AF Ukraine.