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

Ключові слова: персональні дані, цілісність персональних даних, автоматизована система, інформаційна система Збройних Сил України.

Постановка проблеми. На сьогодні почастішали спроби направлених атак на сервери державних підприємств та установ, із метою отримання певних персональних даних фізичних осіб для подальшого розповсюдження, або заподіяння шкоди конфіденційній безпеці. Тим часом спостерігається активне створення міжнародних просторових соціальних, інформаційних систем, обіг особистої конфіденційної інформації в яких потребує їх 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 небезпек у контексті використання ними особистих даних під час 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, та створення відповідного програмного забезпечення. Цим питанням присвячені роботи таких вітчизняних фахівців, 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, що зазначеною проблематикою займалася значна кількість науковців, багато її аспектів нині залишаються малодослідженими або потребують доопрацювання, особливо в контексті правового врегулювання питань захисту персональних даних та вдосконалення організаційної системи захисту даних для забезпечення національної безпеки. Більшість досліджень за цією тематикою здійснювались для запобігання порушень щодо цілісності персональних даних, тобто проводився аналіз технічних недоліків у системі захисту, як правило вже після здійснення злочинних кібератак.

Метою статті є обґрунтування раціональних рішень щодо захисту персональних даних в інформаційних системах Збройних Сил України на основі аналізу досвіду розвинутих країн з питань захисту персональних даних в інформаційних системах для його подальшого використання.

Виклад основного матеріалу. У Збройних Силах (ЗС) України з 2006 року впроваджується Єдина система управління адміністративно-господарськими процесами ЗС України (ЄСУ АГП). Зокрема, впроваджені функціональні підсистеми "Майно" та "Житло" Єдиної системи управління адміністративно-господарськими процесами Збройних Сил України, що містять персональні даннні військовослужбовців. Ця інформація потребує захисту від втручання з боку будь-яких осіб. Ці данні можуть бути ідентифіковані. Тобто відповідно до українського законодавства та міжнародного права, такі відомості фактично є "*персональними даними*", які визначають невід'ємну частину приватного життя людини [2-3].

Вагомий досвід з питань щодо необхідності захисту права на приватне життя людини під час спілкування в різних інформаційних системах, зокрема, в соціальних мережах, отримано англійськіми та американськими вченими-дослідниками. Британський дослідник Артур Міллер зазначає, що "Потенційні порушення недоторканності приватного життя можуть

спонукати відмовитися від інформаційних систем. Тому глобальний успіх у розвитку та поширенні інформаційних систем залежить від прийняття відповідних заходів захисту персональних даних користувачів" [5]. Це висловлення англійського вченого є одним із визначальних під час формування підходів до захисту персональних даних в соціальних мережах. У нашій державі прийнято Закон України "Про захист персональних даних", який визначає вимоги до обробки та захисту персональних даних, зокрема і в інформаційно-телекомунікаційних мережах [2].

Загалом, в Європейських державах правовий захист персональних даних 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 до захисту персональних даних, запроваджені Конвенцією Ради Європи № 108 під час їх обробки в автоматизованій системі [3] та докладніше розвинуті у Директиві Європейського Парламенту та Ради 95/46/ЄС про захист користувачів інформаційних систем під час обробки цими системами персональних даних і вільним обігом цих даних в системі [6]. Питанням захисту персональних даних в інтернет-середовищі, зокрема в соціальних мережах, 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 персональних даних в телекомунікаційних системах ("Берлінська група") [7].

В основі підходу до захисту та обробки персональних даних лежать відповідні базові принципи щодо їх збору, обробки, зберігання та передачі. Отже персональні дані мають бути:

- оброблені чесно і встановленим законним порядком;
- зібрані для визначених, чітких і законних цілей і надалі не оброблятися у спосіб, несумісний з цими цілями;
- достовірними, відповідними і не надлишковими щодо визначених законних цілей, заради яких вони збираються для подальшого їх використання;
- 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);
- збережені в тій формі, яка дає змогу встановити особу-суб'єкт даних (державні органи встановлюють відповідні гарантії для персональних даних, які зберігаються протягом встановлених термінів);
- оброблені з дотриманням прав фізичної особи та гарантувати право на доступ до власних даних;
- оброблені з дотриманням законодавчих вимог захисту конфіденційної інформації;
- відповідно захищені при передачі за межі країни, з дотриманням міжнародних стандартів щодо закордонного поширення персональних даних.

Ці базові принципи підходу до побудови системи захисту були прийняті ще в 90-х роках з врахованням інтересів ряду країн світу. Нині деякі правові норми розвинутих країн містять імплементований перелік аналогічних принципів у національному законодавстві або посилаються на згадану Конвенцію Ради Європи внутрішнім вітчизняним законодавством. Сучасні інформаційні технології щодня удосконалюються, активізуються соціальні мережі, значною мірою змінюються методи і процеси збирання та обробки персональних даних (далі – ПД). На сьогодні 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 персональних даних" провела дослідження на тему: "Як забезпечити прозорість та відкритість обробки персональних даних на веб-ресурсах" [10]. У ході громадського дослідження виявлено, що найчастіше персональні дані з використанням веб-ресурсів обробляються саме в рамках таких процесів:

- заповнення користувачами інтернет-ресурсів наданих 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 (ст. 6, 11 Закону України "Про захист персональних даних") факт реєстрації особи в соціальній мережі є обов'язковим елементом та за

згодою клієнта (користувача), із подальшою обробкою (використанням) його персональних даних певною соціальною мережею. Проте велика кількість соціальних мереж не дотримується певних правових умов для обробки персональних даних, а отже фактично у незаконний спосіб обробляють ці дані та передають їх іншим установам. У ході проведеного дослідження з'ясовано, що в багатьох соціальних мережах, доступних широкому загалу, реєстрація проводиться із врахуванням введення особистих даних, відповідно до яких користувач може бути ідентифікований, а саме: ПІБ; географічне місцезнаходження, місце навчання; телефонні контакти тощо.

Усі дані про особу заповнюються суб'єктом персональних даних без попередження про їх можливе подальше використання за час функціонування особистої сторінки в соціальній мережі. З одного боку, можна уникнути цієї проблеми шляхом введення недостовірних відомостей, але фактично ця соціальна мережа є 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 розв'язання такої проблеми пропонуємо ввести опцію, суть якої буде зводитись до того, що в процесі реєстрації особи в соціальній мережі обов'язковим початковим етапом стане відповідь фізичної особи на запитання: "Чи згодні ви, що в процесі функціонування вашої персональної сторінки в будь-якої соціальній мережі можлива обробка ваших персональних даних?", та визначення відповідальності власників соціальних мереж за її зберігання та недоторканість. З одного боку, це дасть змогу 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 соціальних мереж відповідальніше відноситись до захисту та зберігання наданої інформації. Інший проблемний аспект забезпечення приватності в соціальних мережах – неможливість повністю та остаточно видалити свої дані з особистої сторінки в соціальній мережі. Така проблема порушує так зване особисте право фізичної особи у сфері захисту персональних даних – "право бути повністю видаленим з мережі", але не дає 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 соціальної мережі 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 персональних даних, 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 згідно з 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 персональних даних 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, у тому числі й шляхом відповідних публікацій та оприлюднень.

Для розв'язання 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 таких існуючих небезпек:

- можливих ризиків, пов'язаних з обробкою та зберіганням даних в автоматизованих системах (далі – АС);

- природа та обсяги порушників, які втручаються в АС;

- вартості заходів, щодо впровадження систем захисту в АС;

- характеристика та можливості АС, де циркулює інформація тощо.

Насамперед, у більшості випадків від власників АС, де циркулює особиста інформація не вимагається застосування спеціальних заходів захисту, зокрема загальноприйнятих (описаних в стандартах ISO/IEC 27001). У більшості випадків акцентується увага на наявності кваліфікованих адміністраторів систем управління захистом ПД систем (в установах, організаціях) та навчанні персоналу, під час обробки та зберігання ПД.

Наша держава робить важливі кроки у розв'язанні та подоланні проблемних питань та реалізації права на захист персональних даних в соціальних мережах. Так, у рекомендаціях парламентських слухань на тему: "Законодавче забезпечення розвитку інформаційного суспільства в Україні", затверджених постановою Верховної Ради України від 03.07.14 р. № 1565-VII), є рекомендація Уряду України - "забезпечити у середніх загальноосвітніх школах викладення предмету (теми) з правил роботи у соціальних мережах, участі у загальних форумах, захисту персональних даних 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 інформаційно-телекомунікаційних системах/автоматизованих системах (далі – ІТС/АС), в Україні здійснюється за результатами державної експертизи, у встановленому законодавством порядку. Власники (розпорядники) ІТС, які задовольняють критеріям, визначеним у п. 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 ІТС/АС відповідно до яких можливо застосовувати цю процедуру.

Висновки. Державне законодавство України у сфері захисту ПД продовжує переймати передовий досвід та кращі практичні здобутки країн ЄС з метою забезпечення якісного рівня захисту персональних даних.

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

Заходи захисту ПД, механізми, створення органів, відповідальних за захисту ПД слід планувати та здійснювати на упередження неправомірних дій. Підкреслимо, що захист персональних даних 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 ІТС/АС 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 (персональні дані).

Подальші дослідження доцільно зосередити на пошуку оптимальніших шляхів розв'язання висвітлених питань у таких напрямах:

- загальноосвітній – використання Урядом України вже існуючих рекомендацій провідних країн);

- правовий – активна позиція уповноваженої Верховною Радою України особи з прав людини щодо проведення інформаційних семінарів, надання чітких практичних рекомендацій, публікацій до широкого відома результатів перевірок інформаційних систем з питань захисту персональних даних;

- захист персональних даних в корпоративних мережах - з метою забезпечення ефективного захисту ПД користувачів АС, запровадити можливість розробляти корпоративні кодекси, які будуть важливими в сприянні державою законодавства, у різних сферах, з обробки та передачі даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Раджевич О.П. Конфіденційність персональної інформації в соціальних мережах// Вісник Вищої ради юстиції.–2012.–No 3(11).–С. 215-224.
2. Про захист персональних даних: Закон України від 01.06.10р.No 2297-VI // Офіційний вісник України. – 2010. –No 49.–С.199.
3. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28.01.81 р. No 108 // Офіційний вісник України. –2011. – No 1. –С. 701.

4. Hallborg R.B. Principles of Liberty and Right to Privacy // Law and Philosophy. –1986. –No 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 /В. М. Брижко // Правова інформатика. -2008. - №1(17). – С.20-34.
12. Костецька Т.А. Інформаційне право України ; навчальний посібник. /. Т. А. Костецька. - К.:- Київ. нац. торгово.-економічний. Університет. - 2009. – С. 170.

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. Проанализированны 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.