несанкціонованого доступу. Використання телекомунікаційних технологій для забезпечення незаконних операцій «традиційними» організованими злочинними угрупуваннями також є одним із чинників їх переформатування відповідно до мережевої моделі, як це має місце і в легальних транснаціональних корпораціях.

Специфіка природи злочинних організацій, що діють у кіберпросторі, ставить додаткові вимоги перед правоохоронними органами, але й створює додаткові можливості, що можуть використовуватися і для організації протидії «традиційній» злочинності, що використовує комп'ютерні технології для здійснення протиправних акцій.

Стратегія «роїння» як напрям ведення військового протистояння може розповсюджуватися і на сферу протидії організованій злочинності, причому не лише у контексті діяльності кримінальних структур, але й в організації роботи правоохоронних органів. Це, у свою чергу, потребує не лише розробки нової парадигми правоохоронної діяльності, а й ставить нові вимоги до рівня підготовки співробітників компетентних органів, що повинні мати відповідні навички автономної діяльності, прийняття самостійних рішень та швидкого реагування на зміни у обстановці.

Література: ***1.*** *Про Концепцію державної політики у сфері боротьби з організованою злочинністю: Указ Президента України від 21 жовтня 2011 року №1000/2011. – Урядовий кур'єр від 29.10.2011 — № 201.* ***2.*** *Закону України «Про організаційно-правові основи боротьби з організованою злочинністю». [Електронний ресурс]. – Режим доступу: http://www.rada.com.ua* ***3.*** *Кримінальний кодекс України.[Електронний ресурс]. – Режим доступу: http://www.rada.com.ua* ***4.*** *Конвенція ООН проти транснаціональної організованої злочинності. 2000 р.[Електронний ресурс]. – Режим доступу: http://www.rada.com.ua* ***5.*** *McClure G. The Role of Interpol in Fighting Organized Crime /481 International Criminal Police Review (2000) – Interpol. [Електронний ресурс]. – Режим доступу: http://www.interpol.int/Public/Publications/ICPR/ICPR481_1.asp* ***6.*** *Family Cities, AmericanMafia.com [Електронний ресурс]. – Режим доступу: http://www.americanmafia.com/ 26_Family_Cities.html* ***7.*** *Castelli B. The Globalization of the Drug Trade. – Apr. 1999. [Електронний ресурс]. – Режим доступу: http://www.unesco.org/most/sourdren.pdf* ***8.*** *Shelley L., Director, Center for Transnational Organized Crime and Corruption, Testimony Before the House Committee on International Relations. – October 1, 1997. [Електронний ресурс]. – Режим доступу: http://www.fas.org/irp/congress/1997_hr/h971001ls.htm.* ***9.*** *Brenner S. W. Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships / North Carolina Journal of Law & Technology. –Volume 4, Issue 1: Fall 2002. – 50 p. [Електронний ресурс]. – Режим доступу: http://www.rand.org/publications/MR/MR880.* ***10.*** *Теория оперативно-розыскной деятельности: Учебник. 2-е изд., перераб. и доп./Под ред. К. К. Горяинова, В. С. Овчинского, Г. К. Синилова. – М.: ИНФРА-М, 2012. – Х., 690 с.* ***11.*** *Arquilla J. In Athena's Camp: Preparing for Conflict in the Information Age/ J.Arquilla, D. Ronfeldt. – 1997.* ***12.*** *Arquilla J. David Ronfeldt, Swarming and the Future of Conflict / J.Arquilla, D. Ronfeldt. – 2000. [Електронний ресурс]. – Режим доступу: http://www.rand.org/publications/DB/DB311.pdf*

УДК 35.078:342.738

ДЕЯКІ ПРАКТИЧНІ АСПЕКТИ РЕАЛІЗАЦІЇ ЗАХОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ЇХ ОБРОБКИ В ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ) СИСТЕМАХ

Олексій Мервінський, *Микола Щербак

*Державна служба захисту персональних даних, *ТОВ «Data Protection Development»*

Анотація **В статті обгрунтовуються вимоги щодо системи захисту персональних даних (ПД) в Україні такого рівня, щоб не існувало протиріччя між положеннями європейських директив і вимогами правових і нормативних документів системи ТЗІ України.**

Аннотация **В статье обосновываются требования относительно системы защиты персональных даннях (ПД) в Украине такого уровня, чтобы не существовало противоречия между положениями европейских директив и требованиями правовых и нормативных документов системы ТЗИ Украины.**

Summary **In the article requirements are studied in relation to the system of the personal data protection (PD) in Ukraine in such way that there were not be any contradiction was not between positions of europian directives and requirements of legal documents of Ukraine and native normative documents of the system TID**.

Ключові слова: кримінологічна **безпека, злочинність, причинність, управління ризиками, оцінювання ризиків.**

I Вступ

В країнах Євросоюзу визнання заходів, які можна вважати адекватними для забезпечення захисту персональних даних (ПД), віднесено до компетенції уповноважених державних органів. Загальноєвропейський підхід у цьому напрямі полягає в тому, що уповноважені державні органи з питань захисту персональних даних пропонують володільцям ПД самостійно визначати відповідні засоби захисту.

Згідно зі статтею 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [1] передбачено, що інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в інформаційно-телекомунікаційній (інформаційній) системі (ІТС/АС) із застосуванням комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю.

Директивою 95/46/ЄС Європарламенту та Ради Європи [2] юридичні, нормативні та технічні вимоги, які регламентують забезпечення захисту ПД, щодо прав фізичних осіб та законних інтересів юридичних осіб, повинні бути чітко збалансованими. Дані заходи не повинні нести володільцю ПД великі фінансові навантаження на створення систем захисту ПД, але при цьому мати належний (достатній) рівень захисту ІТС/АС володільця. Якою ж має бути система захисту ПД в Україні щоб не суперечити положенням європейських директив і вимогами правових і нормативних документів системи ТЗІ України?

II Основна частина

Відповідно до пп. 2 статті 5 Закону України «Про захист персональних даних» [3] за режимом доступу персональні дані визначено як інформацію з обмеженим доступом. Законом України «Про інформацію» [4] (ст. 21) визначено, що до інформації з обмеженим доступом відноситься конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Для створення КСЗІ з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Наказом Міністерства юстиції України № 3659/5 [5] встановлено типовий (мінімальний) перелік робіт (Типовий порядок), які необхідно реалізувати володільцю ПД під час організації заходів – зокрема із захисту ПД. Цей порядок передбачає застосування ІТС/АС мережевого захисту від несанкціонованого доступу під час обробки ПД, впровадження процедур авторизації працівників, забезпечення антивірусного захисту, а також використання технічних засобів безперебійного живлення елементів АС, яка здійснює обробку ПД.

Другий розділ [5] присвячений питанням обробки ПД у складі АС системи. У пункті 2.2 цього документу зазначається, що обробка ПД в АС може здійснюватись із застосуванням засобів мережевого захисту від несанкціонованого доступу під час обробки ПД.

Загалом, до засобів мережевого захисту відносяться:

- міжмережеві екрани — для блокування атак з зовнішнього середовища. Вони керують проходженням мережевого трафіку відповідно до встановлених володільцем (розпорядником) правил захисту. Як правило, міжмережеві екрани встановлюються на вході мережі і розділяють внутрішні (приватні) та зовнішні (загального доступу) мережі;
- системи виявлення втручань — для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу «відмова в обслуговуванні». Використовуючи спеціальні механізми системи виявлення втручань здатні попереджувати шкідливі дії, а це дозволяє значно знизити час простою АС внаслідок атаки і витрати на підтримку працездатності мережі;
- засоби створення віртуальних приватних мереж — для організації захищених каналів передачі даних через незахищене середовище забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування;
- засоби аналізу захищеності — для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації. Їх застосування дозволяє попередити можливі атаки

на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

Проте, застосування жодного із зазначених засобів не є необхідною умовою включення їх до складу КСЗІ, що **може** створюватися в ІТС/АС на виконання вимог Закону України [1] «Про захист інформації в інформаційно-телекомунікаційних системах».

Необхідно також врахувати, що Директивою 97/66/ЄС Європарламенту та Ради Європи [6] юридичні, нормативні та технічні вимоги, які регламентують забезпечення захисту ПД, прав фізичних осіб та законних інтересів юридичних осіб повинні бути чітко збалансованими та **не створювати перешкод для розвитку ринку**. 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 [2, 6] володільці ПД за сприяння Уповноваженого державного органу з питань захисту персональних даних повинні здійснювати співробітництво в процесі впровадження та розвитку відповідних технологій там, де це необхідно для надання гарантій захисту прав фізичних осіб. В країнах Євросоюзу 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.

Загальноєвропейський підхід у цьому напрямі полягає в тому, що уповноважені державні органи з питань захисту ПД **пропонують володільцям** ПД **самостійно визначати** відповідні заходи захисту з урахуванням насамперед:

- можливого рівня ризику, пов'язаного з обробкою ПД в АС;
- природи та обсягів ПД, що обробляються в АС;
- вартості робіт, щодо впровадження заходів захисту в АС;
- характеристик АС володільців та/або розпорядників ПД, тощо.

Проте, у більшості випадків від володільців ПД не вимагається застосування спеціальних заходів захисту, окрім загальноприйнятих (описаних зокрема в стандартах ISO/IEC 27001 [7]). У більшості випадків акцентується увага на необхідності наявності на підприємстві (установі, організації) відповідної системи управління захистом ПД та навчання персоналу, який організовує роботу, пов'язану із захистом ПД при їх обробці.

У зв'язку з цим варто наголосити на тому, що з метою застосування положень Закону «Про захист персональних даних» [3] та Типового положення [5], забезпечення ефективного захисту прав суб'єктів ПД, сприянню додержанню законодавства, враховуючи специфіку обробки ПД у різних сферах, можуть розроблятися корпоративні кодекси поведінки (кодекси практики) з обробки ПД, які можуть системно розкривати основні правила обробки і захисту ПД.

Остаточний вибір конкретних заходів захисту, технічних рішень та стандартів, якими необхідно керуватися, архітектур ІТС та АС залишається в межах компетенції володільця ПД. Так само в компетенції володільця знаходиться й безпосередня оцінка ризиків порушень безпеки даних.

Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу врегульовані нормативним документом системи технічного захисту інформації (НД ТЗІ) 2.5-004-99 [8]. Деякі питання щодо захисту персональних даних, зокрема послуги ідентифікації та автентифікації, можна розглядати відповідно до функціонального критерію «Спостереженість» цього документу. Інші послуги, які становлять предмет послуг спостереженості і керованості, відповідно до НД ТЗІ 2.5-004-99 згідно з вимогами Типового порядку необхідно вживати виважено та помірковано.

Так, на відміну від вимог НД ТЗІ 2.5-004-99 (зовнішній аналіз, захищений журнал, сигналізація про небезпеку, детальна реєстрація, аналіз в реальному часі), Типовим порядком чітко прописані всі можливі дії, які можуть здійснюватися в АС щодо реєстрації:

- результатів ідентифікації та/або автентифікації працівників;
- дії з обробки ПД;
- факту встановлення ознаки «Підтвердження надання згоди на обробку персональних даних» за допомогою управляючих елементів веб-ресурсів, інтерфейсів користувача програмного забезпечення.

Всі зазначені Типовим порядком дії щодо захисту ПД при їх обробці в АС значно звужують питання, які складають вимоги щодо спостереженості та контролю за діями користувачів або легальністю доступу, передбачені зазначеними критеріями НД ТЗІ 2.5-004-99. А питання керованості, зокрема достовірного каналу, самотестування, визначення спроможності комплексу засобів захисту (КЗЗ) виконувати свої функції, цілісність комплексу засобів захисту навіть не передбачаються Типовим порядком.

Слід зазначити, що Типовим порядком взагалі не передбачається необхідність створення КЗЗ в базах ПД при їх обробці у складі АС.

Проте, забезпечення конфіденційності ПД може бути здійснено через реалізацію функціональних послуг спостереженості відповідно до НД ТЗІ 2.5-005-99 [9] «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

Особливо слід наголосити на тому, що передбачені НД ТЗІ 2.5-004-99 [8] питання розподілу обов'язків взагалі не враховують розподіл обов'язків з урахуванням питань захисту ПД та завдань відповідальної особи або структурного підрозділу, які організовують роботу, пов'язану із захистом ПД при їх обробці на підприємстві (установі, організації) відповідно до закону.

У Типовому порядку також вживається термін *«відмова в обслуговуванні»*, який є близьким до терміну «стійкість до відмов» як послуга, що є складовою критерію «Доступності», і який є більш широким у тому значенні, що гарантує доступність комп'ютерної системи (в контексті зазначеного документу НД ТЗІ) після відмови її компонента і тому потребує невиправданих додаткових витрат володільців та/або розпорядників ПД на його реалізацію.

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, НД ТЗІ 2.5-004-99 [8] містить обов'язкові критерії гарантій, що дозволяють оцінити коректність реалізації послуг. Зазначені критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, випробування КЗЗ, середовища функціонування і експлуатаційної документації.

В цих критеріях вводиться сім рівнів гарантій (Г-1, ..., Г-7), які є ієрархічними. Ієрархія рівнів гарантій відображає поступово наростаючу міру впевненості в тому, що реалізовані в АС послуги дозволяють протистояти певним загрозам. Механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи. Все зазначене свідчить про те, що зазначені критерії гарантій є надзвичайно надмірними стосовно обробки ПД в складі АС.

Саме тому зазначені критерії можуть застосовуватися до всього спектру комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та інші, але не можуть бути застосовані для оцінювання надійності впроваджених механізмів захисту від незаконного доступу та незаконної їх обробки під час обробки ПД в базах персональних даних.

Значна увага у Типовому порядку в питаннях обробки ПД в складі АС приділяється питанням ідентифікації, автентифікації та авторизації. Порівняно з аналогічними заходами зазначених вище критеріїв, де ці питання розглядаються як ідентифікація і автентифікація при обміні, але винятково за умови створення КЗЗ, автентифікація відправника (захист від відмови авторства) та отримувача (захист від відмови від одержання) у Типовому порядку зазначені процедури значно спрощені.

У критеріях НД ТЗІ рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації (зовнішня, одиночна або множинна ідентифікація і автентифікація), а обов'язковою умовою Критеріїв є забезпечення можливості однозначного підтвердження протоколу автентифікації незалежною третьою стороною, що реалізовується. А це також виходить поза межі сфери дії Закону «Про захист персональних даних» та відповідних нормативно-правових актів.

Відповідно до вимог Типового порядку ідентифікація є початковою процедурою надання доступу до системи. Після неї здійснюється автентифікація та авторизація. Ідентифікація дозволяє користувачу, або процесу, який діє від імені певного користувача, повідомити своє ім'я за допомогою унікального параметру — ідентифікатора (наприклад, логін), який є відомим іншій стороні.

У разі успішної ідентифікації відбувається автентифікація. Шляхом автентифікації інша сторона переконується, що суб'єкт саме той, за кого він себе видає (використовується пароль у випадку парольної автентифікації або інший параметр, наприклад, цифровий підпис). Один із способів автентифікації полягає у попередній ідентифікації на основі ідентифікатора користувача (логіна – реєстраційного імені користувача) і пароля — певної конфіденційної інформації, знання якої передбачає володіння певним ресурсом в мережі. Отримавши введений користувачем логін і пароль, комп'ютер порівнює їх зі значеннями, які зберігаються в спеціальній захищеній базі даних і, у випадку успішної автентифікації, проводить авторизацію з подальшим допуском користувача до роботи в системі.

Одночасно з використанням традиційної автентифікації за допомогою пароля за необхідності використовується паралельно багатофакторна автентифікація — на основі двох чи більше факторів. У цьому випадку для автентифікації використовується не лише інформація, яка є відомою користувачеві, а й інші додаткові фактори, наприклад:

- властивість, якою володіє суб'єкт (біометрична автентифікація);
- знання – інформація, яку знає суб'єкт (парольна автентифікація);

- володіння – річ, або унікальний предмет, яким володіє суб'єкт (токен, смарт-карта або криптографічний сертифікат).

Особливого значення автентифікація набуває при доступі до таких Інтернет-сервісів, як: електронна пошта; веб-форуми; соціальні мережі; Інтернет-банкінг; платіжні системи; корпоративні сайти; Інтернет-магазини. Позитивним результатом автентифікації є авторизація користувача, тобто надання йому прав доступу до ресурсів, визначених для виконання його завдань. Залежно від важливості ресурсу, для доступу до нього можуть застосовуватися різні методи автентифікації: базова автентифікація, дайджест автентифікація, автентифікація по пред'явленню цифрового сертифікату, використання смарт-карт і USB-ключів, децентралізована автентифікація, відстежування автентифікації самим користувачем, багатофакторна автентифікація.

Авторизація передбачає керування рівнями та засобами доступу користувача авторизації до об'єкта, захищеного авторизацією, як в фізичному розумінні (доступ до кімнати готелю за карткою), так і в галузі цифрових технологій (наприклад, автоматизована система контролю доступу) та ресурсів системи залежно від ідентифікатора і пароля користувача або надання певних повноважень (особі, програмі) на виконання деяких дій у системі обробки даних).

Одночасно з мінімально необхідним обов'язковим використанням паролів, що регулярно змінюються, Директиви Європарламенту та Ради Європи [2, 6] також вимагають регулярного перегляду прав доступу. Але в різних країнах ЄС деякі аспекти щодо впровадження елементів захисту ПД реалізуються по-різному.

Щодо підтвердження відповідності КСЗІ в ІТС/АС слід зазначити, що на сьогодні підтвердження відповідності в Україні здійснюється за результатами державної експертизи в порядку, встановленому законодавством, або шляхом декларування (для випадку оброблення інформації про ПД в автоматизованій системі класу "1"). Власники (розпорядники) ІТС, 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 ІТС/АС щодо яких можливо застосовувати процедуру декларування.

У майбутньому, ініціативою ЄС є прагнення щодо створення Єдиного законодавства в сфері захисту ПД за принципом «Один Контитент – Один Закон». Це прагнення виходить з аналізу регулювання питань із захисту ПД громадян протягом останніх 18 років. Директива Європарламенту та Ради Європи [2] містить 12 сторінок. У Німеччині вона була перенесена у формі закону про захист даних, яка складає 60 сторінок. І якщо взяти ці 60 сторінок і помножити на 27 держав-членів ЄС, то може скластися уявлення про те, що термін "складності регулювання" означає на практиці. ЄС прагне замінити цю «гору паперу» на один закон, який буде діяти в усій Європі.

ІІІ Висновки

Національне законодавство у сфері захисту ПД в Україні увібрало і продовжує вбирати в себе передовий досвід та кращі практики країн ЄС з метою забезпечення визнання рівня захисту персональних даних в Україні адекватним і таким, що відповідає вимогам ЄС.

Доцільно розширити перелік ІТС/АС, для яких відповідність КСЗІ вимогам нормативних документів з технічного захисту інформації здійснюється безоплатно уповноваженим центральним органом виконавчої влади з питань захисту інформації шляхом аналізу відомостей декларації.

З метою застосування положень Закону «Про захист персональних даних» [3] та Типового положення [5], забезпечення ефективного захисту прав суб'єктів ПД, сприянню додержанню законодавства, враховуючи специфіку обробки ПД у різних сферах, слід запровадити можливість розробляти корпоративні кодекси поведінки (кодекси практики) з обробки ПД.

Література: ***1****. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»* ***2.*** *Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних, Директива 95/46/ЄС Європейського Парламенту і Ради Європи від 24 жовтня 1995 р.* ***3****. Закон України «Про захист персональних даних»* ***4.*** *Закон України «Про інформацію»* ***5.*** *Про затвердження Типового порядку обробки персональних даних у базах персональних даних, наказ Мінюста від 30.12.2011 № 3659/5.* ***6****. 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* **7.** *Стандарт* ISO/IEC 27001 **8.** *НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р., № 22;* ***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.*** *НД ТЗІ 3.7-003-05 "Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі", затвердженому наказом ДСТСЗІ СБУ від 8 листопада 2005 року № 125* ***12.*** *Положення про державну експертизу в сфері технічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 16 травня 2007 року № 93, зареєстрованим в Міністерстві юстиції України 16 липня 2007 року за № 820/14087* ***13.*** *"Про затвердження змін до Положення про державну експертизу в сфері технічного захисту інформації", наказ Адміністрації Держспецзв'язку від 10 жовтня 2012 року № 567 зареєстрованим 6 листопада 2012 року Міністерством юстиції України за № 1863/22175*