1 Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації

УДК 351.9; 621.321

ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ВИМОГ ЗАКОНОДАВСТВА В СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Олексій Мервінський, Андрій Ніколаєв
Державна служба України з питань захисту персональних даних

Анотація: **Розглянуті питання відповідальності за порушення законодавства про захист персональних даних з позицій захисту прав людини та основні фактори, що визначають умови настання відповідальності володільців або розпорядників баз персональних даних за їх дії, які пов'язані з реальною суттєвою шкодою, завданою фізичній особі внаслідок незаконного доступу до її персональних даних та незаконною обробкою цих даних.**
Summary: **Considered questions of responsibility for violation of legislation about the protection of the personal data from positions of defence of human rights, and basic factors, which determine the terms of offensive of responsibility of proprietors or managers of bases of the personal information for their actions, which are related to the real substantial harm a physical person as a result of illegal access to its personal information and illegal processing of these data.**
Ключові слова: **Захист персональних даних, відповідальність за порушення вимог, реєстрація персональних даних.**

I Вступ

З 1 січня 2011 року вступив в силу прийнятий Верховною Радою України Закон України «Про захист персональних даних» [1], який базується на основних принципах Директиви Європейського Парламенту та Ради ЄС від 24 жовтня 1995 року щодо захисту прав приватних осіб стосовно обробки персональних даних та вільного переміщення таких даних. Такій події передувала ратифікація 6 липня 2010 року базових європейських стандартів у сфері захисту персональних даних, зокрема Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї щодо органів нагляду та транскордонних потоків даних. Таким чином Україна взяла на себе зобов'язання імплементувати їх положення в національне законодавство України.

Проте наразі в засобах масової інформації та Інтернет-виданнях розповсюджується ціла низка статей та публікацій, в яких коментується процедура вступу в дію цього Закону та Закону про відповідальність за порушення вимог законодавства в сфері захисту персональних даних [2]. Подана у цих статтях інформація спотворюється як за змістом (мов би закон покликаний вирішити проблему масового залучення до відповідальності володільців баз персональних даних з незалежних від них причин), так і у підходах до питань відповідальності (за умов відсутності належного правового врегулювання на рівні підзаконних актів, яке б урегулювало весь процес підготовчої роботи, що мала передувати процесу реєстрації баз персональних даних).

Незважаючи на те, що «вилка» санкцій є достатньо широкою, визначення протиправності дій у більшості випадків насамперед пов'язується з фактом конкретних порушень прав конкретного громадянина – суб'єкта персональних даних. Оскільки Закон [2] спрямований виключно на захист прав людини, то питання відповідальності за порушення законодавства про захист персональних даних насамперед слід тлумачити з огляду на дії або бездіяльність, що спричинили реальну суттєву шкоду фізичній особі внаслідок незаконного доступу до її персональних даних та незаконної обробки цих даних.

II Основна частина

Серед усього переліку статей Закону [2] найбільш важливою нормою можна вважати статтю 182 Кримінального кодексу України [3] "Порушення недоторканності приватного життя», яка передбачає відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації. Крім того пункт 2 цієї статті, передбачає

посилення відповідальності за вчинення тих самих дій повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи. У примітці до згаданої статті чітко зазначено, що «Істотною шкодою у цій статті, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян".

Далі за «ступенем захисту від втручання в особисте життя» слідує стаття 188^{39} Кодексу України про адміністративні правопорушення [4] «Порушення законодавства у сфері захисту персональних даних», яка стосується питань:

- неповідомлення або несвоєчасного повідомлення суб'єкта персональних даних про його права у зв'язку з включенням його персональних даних до бази персональних даних, мету збору цих даних та осіб, яким ці дані передаються;
- недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних у базі персональних даних, що призвело до незаконного доступу до них.

Особлива важливість зазначених статей пов’язана з тим, що вони покликані унеможливити зловживання та незаконне використання персональних даних, що могло б завдати шкоди суб’єкту персональних даних - людині.

Слід виділити за ступенем значущості також статтю 188^{40} Кодексу України про адміністративні правопорушення щодо невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних. Бо тільки на останньому місці у цій статі передбачається відповідальність з ухилення від державної реєстрації бази персональних даних та неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних. Це пов’язано з тим, що ухилення від реєстрації само по собі, зазвичай, не завдає шкоди суб’єкту персональних даних, але створює передумови для інших порушень.

У контексті встановлення відповідальності за ухилення від державної реєстрації бази персональних даних також необхідно підкреслити те, що відповідно до законодавства реєстрація баз персональних даних здійснюється за заявочним принципом, який полягає насамперед у тому, що володілець бази персональних даних самостійно визнає факт наявності персональних даних, усвідомлює необхідність забезпечення законної обробки та законного доступу до даних про фізичну особу, про що ставить відмітку у відповідному розділі заяви на реєстрацію бази персональних даних.

Також слід звернути увагу на розмір штрафів. За ухилення від державної реєстрації бази персональних даних максимальною санкцією є накладання штрафу у розмірі до тисячі неоподатковуваних мінімумів доходів громадян. У той же час, максимальною санкцією за неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про його права у зв'язку з включенням його персональних даних до бази персональних даних, мету збору цих даних та осіб, яким ці дані передаються, є накладання штрафу у розмірі «лише» до чотирьохсот неоподатковуваних мінімумів доходів громадян. Але, якщо дію цих норм розглянути на практиці, ситуація буде виглядати дещо інакше.

Розглянемо приклад, коли на підприємстві є дві бази персональних даних – працівників і контрагентів. У базі працівників містяться персональні дані 15 осіб, а у базі контрагентів – 100. Підприємство не зареєструвало свої бази персональних даних та не здійснило повідомлення суб’єктів. чиї персональні дані містяться в згаданих базах. За цих умов ризики, які несе підприємство у разі його перевірки на предмет дотримання вимог законодавства про захист персональних даних, мають становити:

- за ухилення від державної реєстрації баз персональних даних (1 000 неоподатковуваних мінімумів доходів громадян за кожну з баз персональних даних) максимальна санкція становитиме 2 000 неоподатковуваних мінімумів доходів громадян;
- за неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних (400 неоподатковуваних мінімумів доходів громадян за кожного з 115 суб’єктів, чиї персональні дані містяться у базах) максимальна санкція становитиме 46 000 неоподатковуваних мінімумів доходів громадян.

Окремо слід виділити питання, які були висвітлені у коментарях Державної служби України з питань захисту персональних даних (ДСЗПД) і які стосувалися питань щодо умов, за яких буде порушуватися питання стосовно притягнення до адміністративної та кримінальної відповідальності в сфері захисту персональних даних:

1. До ДСЗПД повинна бути надіслана скарга від фізичної особи, або певного володільця чи розпорядника баз персональних даних, включених до Плану перевірок дотримання вимог законодавства про захист персональних даних на відповідний період. При цьому скарга має бути підкріплена документами, що підтверджують порушення у сфері захисту персональних даних
2. На підставі скарги або Плану ДСЗПД буде проведено перевірку володільців та (або) розпорядників баз персональних даних щодо дотримання ними вимог законодавства про захист персональних даних, в

результаті якої буде надано припис про усунення порушень. В разі невиконання припису ДСЗПД складає адміністративний протокол, який потім передається до суду.

3. Після вступу в силу Закону [2] у разі виявлення під час перевірки порушень, передбачених статтями Кодексу України про адміністративні правопорушення, буде складатись адміністративний протокол, а у разі виявлення порушень, передбачених статтями Кримінального кодексу України, матеріали перевірки будуть передаватись правоохоронним органам.

4. Тільки наявність адміністративного протоколу, складеного представниками ДСЗПД, є підставою для проведення відповідного судового засідання та прийняття рішення про накладення адміністративного стягнення, передбаченого Кодексом України про адміністративні правопорушення, на підставі якого володільцем бази персональних даних сплачується штраф.

5. Ухиленням від державної реєстрації бази персональних даних не вважатиметься факт подачі володільцем бази персональних даних заяви про реєстрацію бази персональних даних до ДСЗПД до 1 липня 2012 року.

6. Єдиним органом виконавчої влади, на який Законом покладено завдання щодо контролю за додержанням вимог законодавства про захист персональних даних, є ДСЗПД, а рішення про адміністративне стягнення прийматиме лише суд.

Працівниками ДСЗПД завершено розробку проекту «Положення про порядок здійснення контролю у сфері захисту персональних даних» відповідно до Закону України «Про основні принципи державного нагляду (контролю) у сфері господарчої діяльності» [5]. Зазначений документ конкретизує значну кількість питань діяльності щодо практичного застосування вимог законодавства про відповідальність у сфері захисту персональних даних, визначення фактів порушень та притягнення до відповідальності порушників.

З метою максимально повного висвітлення питання відповідальності володільців баз персональних даних насамперед необхідно також чітко висвітлити їх обов'язки щодо захисту персональних даних, що кореспондуються з правами суб'єкта персональних даних.

Умови можливого настання відповідальності володільців або розпорядників баз персональних даних доцільно розподілити (для кращого розуміння) у наступні групи:

1. Умови настання відповідальності за вчинення дій, пов'язаних з персональними даними без згоди суб'єкта персональних даних:

- обробка персональних даних без конкретних і законних цілей, що визначаються за згодою суб'єкта персональних даних;
- зміна визначеної мети обробки персональних даних без згоди суб'єкта персональних даних;
- використання, поширення персональних даних без згоди суб'єкта;
- необґрунтоване посилання на забезпечення інтересів національної безпеки, економічного добробуту та прав людини при використанні та поширенні персональних даних без згоди суб'єкта;
- визначення строків зберігання персональних даних без згоди суб'єкта персональних даних.

Крім того, Закон [5] чітко визначає дії володільця або розпорядника бази персональних даних, які визначаються умовами згоди суб'єкта персональних даних, окрім випадків, передбачених іншими законами України:

- обсяги персональних даних, які можуть бути включені до бази персональних даних;
- порядок доступу до персональних даних третіх осіб;
- повідомлення про передачу персональних даних третій особі протягом десяти робочих днів.

Окремо слід зазначити те, що ДСЗПД веде Державний реєстр баз персональних даних, який надає можливість кожному громадянину отримати інформацію щодо внесених до нього записів, знати про місцезнаходження баз персональних даних, їх призначення та найменування, місцезнаходження та/або місце проживання (перебування) володільця чи розпорядника цієї бази.

2. Умови настання відповідальності за порушення вимог щодо забезпечення законності обробки персональних даних:

- без згоди суб'єкта персональних даних або без наявності відповідного дозволу на обробку персональних даних, який надається володільцю бази персональних даних відповідно до закону, виключно для здійснення його повноважень;
- обробка персональних даних без згоди суб'єкта з необґрунтованим посиланням на необхідність захисту життєво важливих інтересів суб'єкта персональних даних;
- неотримання згоди суб'єкта персональних даних на обробку його персональних даних з посиланням на необхідність захисту життєво важливих інтересів суб'єкта персональних даних у час, коли отримання такої згоди стало можливим. Важливим при цьому є те, що при наданні суб'єктом персональних даних згоди на обробку його персональних даних він має право внести застереження стосовно обмеження права на обробку своїх персональних даних;

- ненадання працівникам дозволу на використання персональних даних лише суворо відповідно до їхніх професійних чи службових або трудових обов'язків;
- не доведення до працівників вимоги щодо не припущення розголошення ними у будь-який спосіб персональних даних, які їм було довірено, або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків;
- не доведення до працівників вимоги стосовно того, що це зобов'язання є чинним після припинення ними діяльності, пов'язаної з персональними даними.

3. Умови настання відповідальності за невиконання або неналежне виконання процедур, пов'язаних з формулюванням мети обробки персональних даних:

- не внесення чіткого формулювання мети обробки персональних даних до відповідних нормативно-правових чи статутних документів;
- неповідомлення суб'єкта персональних даних протягом десяти робочих днів з дня включення його персональних даних до бази персональних даних про мету збору даних виключно в письмовій формі.

4. Умови настання відповідальності за недотриманням вимог щодо точності та достовірності персональних даних, які збираються та обробляються у базах персональних даних:

- невиконання заходів щодо оновлення персональних даних у разі необхідності;
- невнесення змін до персональних даних на підставі вмотивованої письмової вимоги суб'єкта персональних даних;
- ігнорування вимоги щодо невідкладного внесення змін до персональних даних, які не відповідають дійсності з моменту встановлення невідповідності;
- обробка відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи.

5. Умови настання відповідальності за формування складу та змісту персональних даних у базі персональних даних:

- невідповідність складу та змісту персональних даних визначеній меті їх обробки;
- надмірність персональних даних – збирання та обробку персональних даних, що не відповідають визначеній меті їх обробки;
- обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, а також даних, що стосуються здоров'я чи статевого життя, окрім випадків, передбачених Законом.

6. Умови настання відповідальності за невиконання вимог, пов'язаних з державною реєстрацією бази персональних даних:

- неповідомлення суб'єкта персональних даних протягом десяти робочих днів з дня включення його персональних даних до бази персональних даних про його права, визначені Законом, та осіб, яким передаються його персональні дані, виключно в письмовій формі;
- неповідомлення ДСЗПД про кожну зміну відомостей, необхідних для реєстрації відповідної бази, не пізніш як протягом десяти робочих днів з дня настання такої зміни.

7. Умови настання відповідальності за дії, пов'язані з обробкою персональних даних:

- умисне приховування, ненадання чи несвоєчасне надання, що призвели до випадкової втрати, знищення, пошкодження;
- знищення персональних даних в базах персональних даних у випадках, що не передбачені Законом;
- неповідомлення протягом десяти робочих днів суб'єкта персональних даних про зміну чи знищення персональних даних або обмеження доступу до них, а також не здійснення відповідного повідомлення суб'єктів відносин, пов'язаних із персональними даними, яким ці дані було передано;
- оброблення персональних даних у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, у строк, не більший, ніж це необхідно відповідно до їх законного призначення;

8. Умови настання відповідальності за ненадання або несвоєчасне надання суб'єкту персональних даних доступу до його персональних даних, що містяться у відповідній базі персональних даних:

- відстрочення доступу суб'єкта персональних даних до своїх персональних даних;
- ненадання суб'єкту персональних даних можливості реалізовувати право безоплатного одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними, без зазначення мети запиту;
- ігнорування запиту суб'єкта персональних даних на предмет його задоволення;
- ненадання відповіді на запит суб'єкта персональних даних протягом більше десяти робочих днів з дня його надходження;

- неповідомлення протягом десяти робочих днів особи, яка подала запит, що запит буде задоволено, або направлення відмови у наданні відомостей із зазначенням підстави з посиланням на конкретний нормативно-правовий акт;
- недотримання строків безоплатного задоволення запиту суб'єкта персональних даних (більше ніж тридцять календарних днів) щодо надання відповіді про те, чи зберігаються його персональні дані у відповідній базі персональних даних, а також надання змісту його персональних даних, які зберігаються та джерела отримання цих відомостей;
- ненадання інформації суб'єкту персональних даних про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані, що містяться у відповідній базі персональних даних;
- невиконання вимоги, що у разі відстрочення доступу до персональних даних третіх осіб, допускається у разі, якщо необхідні дані не можуть бути надані протягом тридцяти календарних днів з дня надходження запиту (проте, загальний термін вирішення питань, порушених в запиті, не може перевищувати сорока п'яти календарних днів);
- неповідомлення суб'єкта персональних даних у письмовій формі про відстрочення з роз'ясненням порядку оскарження такого рішення із зазначенням: прізвища, ім'я та по-батькові посадової особи, дати відправлення повідомлення, причини відстрочення та строку, протягом якого буде задоволено запит.

9. Умови настання відповідальності за відсутність умов для захисту персональних даних у базі персональних даних:

- незабезпечення захисту персональних даних від незаконного доступу до них;
- незабезпечення цілісності персональних даних у базі персональних даних;
- незабезпечення відповідного режиму доступу до персональних даних;
- не визначення структурного підрозділу або відповідальної особи, яка організовує роботу, пов'язану з захистом персональних даних при їх обробці;
- незабезпечення фізичною особою, яка володіє персональними даними, особистого захисту баз персональних даних.

10. Умови настання відповідальності за порушення вимог при поширенні (розповсюдженні, реалізації, передачі) відомостей про фізичну особу з урахуванням того, що виконання вимог встановленого режиму захисту персональних даних забезпечує сторона, що поширює ці дані:

- розголошення відомостей стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними;
- надання доступу до персональних даних третій особі, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення вимог Закону або неспроможна їх забезпечити;
- надання права на використання персональних даних без створення відповідних умов для захисту цих даних та перевірки вжитих заходів стороною, якій передаються персональні дані, створених нею заходів щодо забезпечення вимог Закону;
- доручення обробки персональних даних розпоряднику володільцем без укладання з розпорядником договору в письмовій формі;
- обробка персональних даних розпорядником не відповідно до чітко встановленої мети обробки персональних даних та в обсягах, що були визначені в умовах укладеного договору;
- використання відомостей про особисте життя фізичної особи – як чинник, що підтверджує чи спростовує її ділові якості.

III Висновки

Питання відповідальності за порушення законодавства про захист персональних даних насамперед слід тлумачити виключно з позицій захисту прав людини. Особлива важливість статей Закону України [2] пов'язана з тим, що вони покликані унеможливити зловживання та незаконне використання персональних даних, що могло б завдати шкоди суб'єкту персональних даних - людині. До основних факторів, що визначають умови настання відповідальності володільців або розпорядників баз персональних даних, доцільно віднести їх дії, які пов'язані з:

- персональними даними без згоди суб'єкта персональних даних;
- порушенням вимог щодо забезпечення законності обробки персональних даних;
- невиконанням або неналежним виконанням процедур, пов'язаних з формулюванням мети обробки персональних даних;
- недотриманням вимог щодо точності та достовірності персональних даних, які збираються та обробляються у базах персональних даних;
- порушенням формування складу та змісту персональних даних у базі персональних даних;

- невиконанням вимог, пов'язаних з державною реєстрацією бази персональних даних;
- порушенням порядку обробки персональних даних;
- ненаданням або несвоєчасним наданням суб'єкту персональних даних доступу до його персональних даних, що містяться у відповідній базі персональних даних;
- відсутністю умов для захисту персональних даних у базі персональних даних;
- порушенням вимог при поширенні (розповсюдженні, реалізації, передачі) відомостей про фізичну особу з урахуванням того, що виконання вимог встановленого режиму захисту персональних даних забезпечує сторона, що поширює ці дані.

Література: ***1.*** *Закон України «Про захист персональних даних» від 01. 06. 2010 р.* ***2.*** *Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» від 02. 06. 2011 р.* ***3.*** *Кримінальний кодекс України від 05. 04. 2001 р.* ***4.*** *Кодекс України про адміністративні правопорушення від 07. 12. 1984 р.* ***5.*** *Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» від 05. 04.2007 р.*

УДК 654.924

ОСОБЕННОСТИ ОЦЕНКИ ПРОДОЛЖИТЕЛЬНОСТИ НЕСАКЦИОНИРОВАННОГО ПРОНИКНОВЕНИЯ НА ОХРАНЯЕМЫЙ ОБЪЕКТ

Владимир Волхонский
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Аннотация: **Анализируются особенности оценки продолжительности несанкционированного проникновения. Маршрут проникновения представляется суммой переходов через зоны и препятствия. Анализируется продолжительность проникновения и методика получения оценки этой продолжительности.**
Summary: **Special features of unauthorized penetration duration are analyzed. Penetration route is represented as sum of crossing. Penetration duration is analyzed and method of duration estimation is offered.**
Ключевые слова: **Система безопасности, продолжительность проникновения, вероятность.**

Введение

Один из важнейших вопросов создания систем безопасности (СБ) состоит в оценке эффективности разрабатываемой системы. Решению задач анализа и оценки эффективности СБ посвящено достаточно большое количество работ, например, [1 – 3]. При этом неизбежно возникает вопрос оценки продолжительности несанкционированного проникновения (НП) на объект обеспечения безопасности, необходимой для сравнения со временем реакции СБ на несанкционированное проникновение [1, 2]. Недостатками существующих подходов является недостаточная степень учета вероятностных характеристик процесса проникновения на объект и взаимосвязи упомянутых характеристик с особенностями объекта. Целью настоящей работы является анализ особенностей объекта и процесса проникновения, влияющих на аппроксимацию закона распределения продолжительности несанкционированного проникновения.

I Анализ процесса НП

При НП нарушитель перемещается по объекту по определенному маршруту [1], выбираемому из тех или иных соображений. Например, минимальных затрат времени или минимума возможности быть обнаруженным. Можно говорить о двух основных типах элементов объекта, преодолеваемых при НП. Это, во-первых, зоны, прохождение которых определяется главным образом их геометрическими размерами и скоростью движения нарушителя и, во-вторых, препятствиями или физическими барьерами, преодоление которых требует дополнительных затрат времени, зависящих от конструкции препятствия, квалификации нарушителя и его оснащенности.

Реальные объекты имеют обычно достаточно большое количество зон и препятствий. Т. е. можно говорить о том, что имеют место совокупности $\mathbf{Z}$ зон z_i и $\mathbf{D}$ препятствий d_i.

Процесс выполнения НП можно проиллюстрировать диаграммой на рис. 1. На этом рисунке обозначены