УДК 621.96

Т.В. Німченко, к.т.н.

КРИТЕРІЙ ВИЗНАЧЕННЯ З ПЕРЕЛІКУ ДАНИХ ТИХ, ЩО ВІДНОСЯТЬСЯ ДО КАТЕГОРІЇ ПЕРСОНАЛЬНІ

Національний авіаційний університет, Київ
e-mail: fiona54@ukr.net

У роботі розглянуто критерій визначення з переліку даних таких, які відносяться до категорії персональних даних. Наведено класифікацію категорій персональних даних.

***Ключові слова**:, захист інформації, інформаційна безпека, персональні дані, загрози*

Вступ і постановка задачі

Інформаційні технології мають широке застосування при обробці даних, а також при їх обміні між різними користувачами. Такі процеси охоплюють не тільки окрему організацію або її структури, які виступають у вигляді внутрішніх користувачів, але й зовнішніх користувачів. За таких умов, з урахуванням все більш широкого використання інформаційних технологій, виникають проблеми захисту інформаційних ресурсів, включаючи і дані, що обробляються або передаються. Тому питанням інформаційної безпеки приділяється значна увага.

Проблема захисту інформаційних ресурсів особливо важлива з точки зору захисту персональних даних. Такий захист передбачає мінімізацію втрат, які виникають при реалізації загроз безпеки персональних даних з відповідними наслідками – фізичної, матеріальної та фінансової шкоди суб'єкту персональних даних. Тому в останній час питанням захисту персональних даних приділяється значна увага у багатьох країнах світу. Питання захисту персональних даних є актуальними для операторів інформаційних систем та фахівців з інформаційної безпеки. Також виникає проблема автоматичного визначення інформаційною системою з переліку даних тих, які відносяться до категорії персональні дані.

Основна частина

Інформаційні загрози за своєю актуальністю посідають друге місце серед основних загроз бізнесу, таких як економічна нестабільність, промисловий шпіонаж, викрадення інтелектуальної власності, нанесення шкоди репутації, тощо. Встановлено, що питання внутрішньої безпеки інформаційних систем, зокрема і питання неконтрольованого поширення даних, на поточний час є актуальними [1 –5].При цьому близько 90% даних, що втрачаються, складають персональні дані (ПД), частина з яких втрачається мережевим шляхом. Приблизно однакові частки втрати персональних данихспостерігаються за рахунок навмисних дій співробітників компаній, так і через їх необережність.

Серед інформаційних загроз виділяють дві основні групи загроз: внутрішні та зовнішні [3]. До зовнішніх загроз відносять загрози, які виникають та якими керують за межами інформаційних систем (ІС), відносно ресурсів яких вони спрямовані. Внутрішні загрози виникають безпосередньо в межах ІС. Вони можуть надходити від технічного обладнання, недосконалих програмних засобів та персоналу.

Проблема внутрішніх загроз інформаційній безпеці викликана незахищеністю від них ІС організацій і установ та відсутністю ефективного рішення протидії таким загрозам. Практично на усіх підприємствах використовуються програмні і/або апаратні засоби захисту, які призначені для боротьби із зовнішніми загрозами і досить ефективно їм протистоять. Що стосується засобів захисту від внутрішніх загроз, то тільки дуже незначна частина компаній їх використовує, хоча необхідність у цих засобах об'єктивно існує.

Встановлено, що не існує жодного визначеного переліку даних, які однозначно відносяться до категорії персональних даних. Також встановлено, що основним критерієм, який визначає приналежність певних даних до категорії ПД, є характерна таким даним властивість ідентифікувати за ними особу, до якої вони відносяться. Теоретично це можливо за умови, якщо всі особи, в рамках наявної інформації, унікальні та є хоча б одна особа, якій відповідають наведені дані. Очевидно, що ймовірносна оцінка відповідності даних певній особі могла б бути шля-

хом визначення переліку даних, які можна кваліфікувати як персональні. Але така процедура нормативно не передбачена чинними документами. Класифікацію ПД наведено на рис.1

Рис. 1 – Класифікація персональних даних

Також склад і структура ПД у кожному конкретному випадку можуть бути різними. Дані, які можна віднести до категорії персональних даних визначаються не їх складом чи переліком, а в першу чергу тим, чи можна за цими даними ідентифікувати особу, до якої вони відносяться, чи ні. При цьому, у залежності від складу ПД, кількості осіб, яких вони стосуються та району, що охоплюють, ПД можуть відноситись до одної з чотирьох категорій (класів ризику).

Щодо можливого характеру загрози для збереження цілісності та конфіденційності персональних даних, які обробляються у відповідних базах та ІС, а також необхідності впровадження відповідних заходів безпеки даних, персональні дані діляться на чотири класи ризику:

*Клас ризику 4:*ризик відсутній. Персональні дані, що обробляються, вже знаходяться у вільному доступі, і вважається, що використання таких персональних даних не містить ризиків для суб'єктів персональних даних, для їх захисту не потрібні жодні спеціальні заходи безпеки;

*Клас ризику 3***:** незначний рівень ризику. В цьому класі у випадку втрати або несанкціонованого чи неналежного доступу до персональних даних особи наслідки для неї є такими, що для їх запобігання буде достатньо використовувати звичайні (стандартні) заходи захисту інформації. До цієї групи відносяться бази даних бухгалтерії та відділу кадрів невеликих підприємств, бібліотек, комунальних організацій, а також клієнтські бази торгівельних та сервісних організацій (із певними виключеннями);

*Клас ризику 2:*середній рівень ризику. У цьому класі втрата або неавторизоване чи неналежне використання персональних даних суб'єкта може спричинити додаткові негативні наслідки. До баз персональних даних цього класу відносяться бази, що містять дані про особисте життя громадян, расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, бази даних, що містять або можуть містити опосередковану інформацію про світоглядне переконання, статеве життя чи здоров'я (наприклад, бази абонентів телекомунікаційних компаній, інтернет-сервіс провайдерів тощо). Для таких баз даних може бути необхідним проведення незалежної оцінки вжитих заходів щодо захисту персональних даних.

*Клас ризику 1:*високий рівень ризику. У випадку, якщо несанкціоновані дії із персональними даними можуть мати серйозні наслідки для суб'єкта персональних даних, для їх захисту повинні бути впроваджені належні засоби захисту, а також обов'язково проводитися незалежна оцінка таких заходів.

Припустимо, що особу можна ідентифікувати за умови, якщо певному набору даних відповідає достатньо вузьке коло осіб, яке легко локалізується для подальшого уточнення. При цьому в процесі локалізації та уточнення можуть бути використані виключно загальнодоступні джерела та засоби.

На основі наведених класів ризику ПД можна виділити чотири категорії персональних даних, які умовно відповідають даним, включеним до певних класів ризику (рис.2) [2, 3]. До четвертої категорії відносяться знеособлені та загальнодоступні дані, до третьої категорії відносяться ідентифікаційні дані. Очевидно, що поширення таких даних не може завдати відчутної шкоди особі, до якої вони відносяться. Третя категорія даних ніякої інформації про особу не несе, а дані, що відносяться до четвертої категорії вже загальнодоступні. Звідси випливає, що захисту від несанкціонованого поширення підлягають дані першої та другої категорії.

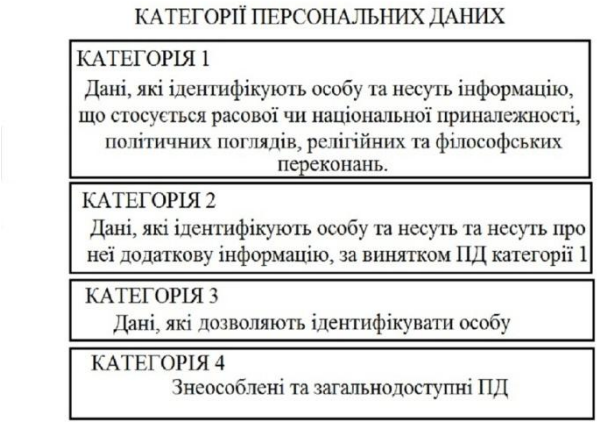

Рис. 2 – Категорії персональних даних

На основі такого розмежування ПД можна представити у вигляді наступних категорій:

ІД– групи даних, що дозволяють однозначно ідентифікувати громадянина;

ДЗІ– групи даних, які розкривають загальну інформацію, але не дозволяють однозначно ідентифікувати громадянина: ДЗІ;

ДОЧ– групи даних, які розкривають інформацію про релігійні, расові, національні, політичні погляди, але не дозволяють однозначно ідентифікувати громадянина: ДОЧІ.

Елементи розглянутих типів ПД представлені в табл.1.

Таблиця 1

Тип даних	Елемент	Найменування елемента
ІД	1	Прізвище, ім'я, по батькові
	2	Дані, що характеризують фізіологічні особливості, та за якими можна встановити особу
	3	Паспортні дані
	4	Дані свідоцтва про народження
	5	Дані водійського посвідчення
	6	Адреса місця проживання
ДЗІ	1	Дані про освіту
	2	Дані про трудову діяльність
	3	Дані про трудову книжку
	6	Дані з трудового договору
	4	Дані про заробітню плату
	5	Дані з наказів по особовому складу
	6	Дані про атестацію
	7	Дані з матеріалів службових розслідувань
	8	Дані про підвищення кваліфікації
	9	Дані про проходження професійної перепідготовки
	10	Дані про військовий облік
	11	Дані про доходи
	12	Дані про майно
	13	Дані про індивідуальні номери платника податків
	14	Дані страхового свідоцтва
	15	Дані про сімейний стан та склад сім'ї
	16	Дані про пільги
ДОЧ	1	Дані про здоров'я
	2	Дані про расову приналежність
	3	Дані про національну приналежність
	4	Дані про політичні погляди
	5	Дані про релігійні переконання
	6	Дані про інтимне життя

Для однозначного визначення належності даних до категорії ПД, використовуючи дані табл.1, можна сформувати множини персональних даних, представлені на рис.2. У результаті аналізу можливих варіантів об'єднання груп даних (рис.3.) видно, що до категорії ПД будуть відноситись дані, до складу яких входять елементи з груп ІД та ДОЧ і ІД та ДЗІ. Такі дані будуть відповідно відноситись до 1 та 2 класу ризику ПД. Дані до яких входять елементи з підгруп ДІО та ДПУ також будуть персональними та будуть відноситись до 3 класу ризику. Дані, до яких входять елементи груп ДЗІ та ДОЧ можуть бути віднесеними до 4 класу ризику, тому що вони є знеособленими. Такі дані не потребують захисту.

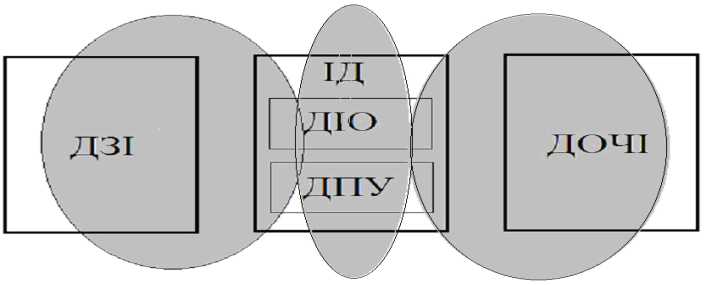

Рис. 3. – Групи персональних даних

При цьому до переліку даних, які віднесені до категорій 1 та 2, входять персональні дані групи ІД, або такі персональні дані, за якими однозначно можна ідентифікувати особу.

Отримані результати показали, що з метою визначення відсутності персональних даних у масиві інформації, що підлягає обробці, достатньо будувати алгоритм її обробки з визначенням відсутності ПД групи ІД у цьому масиві. При виявлені у масиві інформації, що підлягає обробці, групи ІД необхідно проводити подальший аналіз даних з метою виявлення інших ПД, що стосуються особи, до якої відносяться виявлені ПД групи ІД. При виявлені додаткових ПД необхідно встановлювати до якої групи вони відносяться, з наступним визначенням категорії виявлених ПД.

Висновки

Розроблено критерій визначення категорії ПД. При цьому за основу взято можливі комбінації класів ПД. ПД 4 категорії є дані групи ДОЧ та ДОЧІ, так як вони не дають можливості ідентифікувати особу. ПД 3 категорії є данні групи ІД, так як у неї входять тільки дані, що ідентифікують громадянина. ПД 2 категорії є дані груп ІД та ДЗІ, так як в них входять дані, що ідентифікують громадянина, а також несуть додаткову інформацію про нього. ПД 1 категорії є множини ІД і ДОЧ, так як в них входять дані, що ідентифікують громадянина, а також інформація, що стосується расової, національної приналежності, політичних поглядів, релігійних і філософських переконань, інтимного життя, стану здоров'я.

Список літературних джерел

1. Закон України “Про захист персональних даних”від01.06.2010 № 2297-VI (Редакція станом на 09.06.2013).

2. Марков А.П. Проблемы и решения по защите персональных данных в информационных системахперсональных данных [Текст] / А.П. Марков, Б.И. Сухинин // Компьютерная безопасность. - Улан-Уде: ВСГТУ. - 2009. – №5. – с. 20 – 27.

3. Коржов В.В. Защита персональных данных: проблемы и пути решения [Текст]/ В.В.Коржов // Открытые системы. – 2010. - №10. – С. 11.

4. Рытов М.Ю. Автоматизация проектирования систем защиты персональных данных в органах исполнительной власти/ М.Ю. Рытов, О.М. Голембиовская//Информация и безопасность. – 2011. – №3. –с.591 – 593.

5. Аверченков В.И.Формализация процесса выбора состава средств обеспечения безопасности на объекте защиты/ В.И.Аверченков, М.Ю.Рытов, Т.Р.Гайнулин//Вестник компьютерных и информационных технологий.- 2010. – № 11.- с. 45 – 50.