УДК 621.96

М.В. Кривобок, Д. Сорока
Національний авіаційний університет
meirine@mail.ru

АЛГОРИТМ ВИЗНАЧЕННЯ З ПЕРЕЛІКУ ДАНИХ ТИХ, ЯКІ ВІДНОСЯТЬСЯ ДО КАТЕГОРІЇ ПЕРСОНАЛЬНІ ДАНІ

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

Широке впровадження інформаційних технологій робить актуальною проблему захисту інформації. До проблеми неконтрольованого поширення особливо чутлива така категорія інформації, як персональні дані. Опинившись за межами захищеної інформаційної системи, персональні дані стають доступними практично необмеженому колу користувачів і можуть бути знищені чи спотворені, а також можуть бути використані з метою нанесення шкоди особі, якої стосуються, як моральної так і матеріальної.

Питання внутрішньої безпеки інформаційних систем, зокрема і питання неконтрольованого поширення даних, на поточний час є актуальним. Це викликано стабільно зростаючою кількістю зафіксованих випадків витоку інформації у всіх країнах світу. При цьому 70-90% даних, що втрачаються, складають персональні дані (ПД), третина з яких втрачається мережевим шляхом.

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.

Виходячи з класифікації персональних даних можна виділити три групи |множин ПД:

- дані, що дозволяють однозначно ідентифікувати громадянина (А – множини даних);
- В – множини даних, які розкривають загальну інформацію, але не дозволяють однозначно ідентифікувати громадянина;
- С – множини даних, які розкривають інформацію про релігійні, расові, національні, політичні погляди, але не дозволяють однозначно ідентифікувати громадянина.

Для однозначного визначення категорії ПД, можна сформувати множини персональних даних (АВ, АС, ВС).

Таким чином, однозначно можна визначити, що:

- ПД 1 категорії є множини А і С, так як в них входять дані, що ідентифікують громадянина, а також інформація, що стосується расової, національної приналежності, політичних поглядів, релігійних і філософських переконань, стану здоров'я, інтимного життя;
- ПД 2 категорії є множини А і В, так як в них входять дані, що ідентифікують громадянина, а також несуть додаткову інформацію про нього;
- ПД 3 категорії є множина А, так як у нього входять тільки дані, що ідентифікують громадянина;
- ПД 4 категорії є множини В і С, так як вони не дають можливості ідентифікувати особу.

З наведеного можна зробити висновок, що з метою визначення відсутності персональних даних у масиві інформації достатньо переконатися у відсутності ПД групи А у цьому масиві. При виявлені у масиві інформації ПД групи А необхідно провести подальший аналіз цього масиву з метою виявлення інших персональних даних, що стосуються особи, до якої відносяться виявлені ПД групи А. При виявлені додаткових ПД необхідно встановити до якої групи вони відносяться і визначити категорію виявлених персональних даних.

Розроблено алгоритм визначення категорії ПД. При цьому за основу взято можливі комбінації класів ПД.

Науковий керівник – д.т.н., проф., П.М. Павленко