

## **ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМАХ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ**

Інформаційні системи обробки персональних даних (ІСОПД) за структурою є локальними інформаційними системами, які функціонують у складі корпоративних інформаційних систем. Вони складаються з програмних та апаратних засобів обробки інформації, а також мережних каналів обміну даними. При цьому, досить часто, в якості каналу передачі даних між елементами системи використовується мережа інтернет. Така структура організації комп'ютеризованих систем обробки персональних даних (ПД), маючи суттєві переваги з точки зору вартісної складової побудови та експлуатації системи, передбачає необхідність впровадження ефективних систем захисту ПД, що обробляються системою, у відповідності до вимог чинного законодавства.

Виявлення потенційних загроз безпеці інформації та порушників інформаційної безпеки є обов'язковою умовою при розробці та впровадженні систем захисту інформації. До потенційних загроз інформаційній безпеці можна віднести наступні загрози.

Перехоплення даних. Наведений тип загрози може бути застосований у каналах передачі даних та бути направлений на незаконне використання інформації, спотворення та пошкодження її цілісності, а також на її несанкціоноване поширення.

Несанкціонований доступ до інформаційних ресурсів. Крім спотворення інформації, її копіювання, вилучення чи неправомірного поширення, такий тип загрози може нанести шкоду елементам інформаційної системи;

Загроза зі сторони штатних співробітників, які мають легальний доступ до ресурсів корпоративної інформаційної системи. Вилучення, знищення, спотворення та несанкціоноване поширення інформації може виникнути в результаті реалізації таких загроз;

Загроза втрати носія інформації та засобів її обробки. Загрози можуть бути спрямованими на знищення, спотворення, копіювання та неправомірне використання і поширення інформації.

Порушниками інформаційної безпеки і безпеки ПД, можуть бути як фізичні особи, так і організації. Таких порушників можна поділити на зовнішніх, до яких відносяться зловмисники які намагаються отримати доступ до інформаційних ресурсів, знаходячись поза межами захищеної інформаційної системи, та внутрішніх, які є легальними користувачами корпоративної інформаційної системи, в тому числі вони можуть бути і операторами ІСОПД. Загрози інформаційній безпеці можуть реалізовуватись внаслідок як навмисних так і ненавмисних дій внутрішніх порушників. Неуважність та некомпетентність оператора можуть бути причинами виникнення загроз безпеці інформації. Помста, матеріальна вигода, задоволення нездорових амбіцій – список можливих

мотивацій навмисних дій зловмисників, які можуть привести до порушення цілісності конфіденційної інформації.

Приведені загрози інформаційній безпеці в повній мірі можна віднести і до ПД. При впровадженні систем захисту інформації при обробці ПД особливої уваги потребує попередження несанкціонованого поширення таких даних мережевими каналами, адже ПД передаються мережевими каналами і каналами інтернет. До таких каналів передачі даних вони можуть надходити як санкціоновано, так і несанкціоновано, внаслідок дій внутрішніх порушників. А отже системи попередження несанкціонованого витоку ПД мережевими каналами повинні розрізняти санкціоновані та несанкціоновані надсилання таких даних.

*Науковий керівник – к.т.н., доц., Т.В. Німченко*