

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ВІД ВИТОКУ МЕРЕЖЕВИМИ КАНАЛАМИ

Актуальність проблеми захисту персональних даних обумовлена законодавчими актами України та відповідними документами міжнародного співтовариства. Проведений аналіз інформації показує, що близько 80% компаній у світі мали інциденти з безпеки персональних даних, у тому числі і з необережності своїх співробітників. Тому захисту персональних даних приділяється значна увага [1]. У випадку обробки персональних даних електронними засобами з використанням мережових технологій може виникати загроза їх витоку за межі захищеного інформаційного простору установи. Такі загрози можуть виникати з необережності співробітників, які мають до них доступ. Для захисту персональних даних можливо застосовувати існуючі системи інформаційної безпеки. Однак, існуючі системи орієнтовані тільки на захист від зовнішніх загроз. Робота подібних систем направлена, в основному, на попередження несанкціонованого доступу до інформаційних ресурсів.

Під час електронної обробки інформації, яка у своєму складі має персональні дані, спрямованість систем захисту інформації зміщується в сторону внутрішніх загроз. Це підтверджується даними компанії InfoWatch.

Для обміну та обробки персональних даних використовуються різноманітні технології передачі даних, зокрема системи електронної пошти, миттєвих повідомлень, WEB-технологій, ftp-з'єднання та ін.

З проаналізованої інформації видно, що навіть у організаціях, які мають власну розвинену інформаційну інфраструктуру, співробітники досить часто у своїй роботі використовують сервіси передачі даних від сторонніх операторів в силу їх більшої зручності. Це, в свою чергу, створює реальну загрозу витоку персональних даних за межі інформаційного простору установи чи організації мережевими каналами, у тому числі і з необережності співробітників даної установи. Попередження витоку персональних даних зумовлює необхідність постановки задачі контролю каналів їх передачі. Це вимагає створення технології та систем, які передбачають моніторинг інформації, що передається каналами, та виявляють у даній інформації персональні дані. При цьому технології повинні виявляти персональні дані в інформації, що передається.

Проаналізувавши існуючі методи та підходи видно, що створення оптимальних технологій захисту персональних даних базується на поєднанні існуючих методик контекстного аналізу інформації з урахуванням форматів їх передачі, а також алгоритмів реагування на виявлені спроби передачі персональних даних. Отже необхідне формування та підтримка спеціальних баз даних, які дозволять проводити аналіз і реалізацію алгоритмів виявлення та реагування несанкціонованої передачі інформації.