

СИСТЕМИ ПОПЕРЕДЖЕННЯ ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ МЕРЕЖЕВИМИ КАНАЛАМИ

Удосконалення політики інформаційної безпеки персональних даних є одним із важливих завдань захисту інформації в мережових каналах у всьому світі.

Потрібно сказати, що коло таких проблем є набагато ширше ніж можна собі уявити. Оскільки персональні дані кожного з нас чи то медичного, фінансового характеру, не кажучи вже про ті, що ми використовуємо у своїх візитках є або можуть бути об'єктом використання в автоматизованій системі обробки, ми, користуючись Інтернетом там залишаємо велику кількість своїх персональних даних, яку пізніше не можна видалити чи змінити. І що головне використання наших даних нічим не обмежене і не врегульоване тобто фактично, такі дані залишаються не захищеними. І вони безперешкодно можуть використовуватись з метою впливу на наш вибір чи то економічний, чи то політичний – будь-який, можуть впливати на наші переконання і думки або використовуватись якимось іншим чином. Такі бази даних постійно вдосконалюються, уніфікуються і з кожним разом зачіпають приватне життя кожної людини все сильніше і сильніше.

Що ж говорячи про закон “про захист персональних даних” то проаналізувавши його, ми не отримаємо чіткої відповіді, про відповідальність за порушення прав на захист наших персональних даних. Тому важливо є, саме зменшити витік персональних даних і створити систему попередження витоку особистої інформації в мережу, де захистити та контролювати її ми просто не зможемо. І після чого цією інформацією зможе оперувати будь-хто і в будь яких цілях.

В основі ідеї системи попередження витоку персональних даних мережевими каналами є створення системи, яка призначена для запобігання витоків конфіденційної інформації через електронну пошту, соціальні мережі, інтернет-пейджери і будь-які інші мережеві канали передачі даних. Яка б дозволяла контролювати і архівувати: переписку в корпоративній електронній пошті; листи і вкладення, що відсилаються через сервіси веб-пошти; спілкування в соціальних мережах, на форумах і блогах; повідомлення інтернет-пейджерів; файли, що передаються по FTP. Адже саме через вище вказані процеси може відбуватись витік персональних даних. Для виявлення конфіденційних даних у повідомленнях система попередження даних використовує гібридний аналіз - комплекс сучасних технологій детектування, які з високою точністю визначають рівень конфіденційності переданої інформації та категорію документів з урахуванням особливостей бізнесу, вимог галузевих стандартів і законодавства України, СНД, Європи та США. Якщо пояснити простими словами, коли користувач захоче надіслати інформацію під яка є секретною або належить до персональної, система попередить клієнта про це.

Налаштування даної системи дозволяють призначити різну реакцію на виявлення підозрілих повідомлень : їх можна заблокувати , пропустити з повідомленням офіцера безпеки або помістити в карантин для ручної перевірки. Після кожної реакції системи, всі дії архівуються та зберігаються, що дозволяє розглянути особу відправника та одержувача, дані які надсилались та інше. Такий архів є незамінним інструментом для аналізу , проведення внутрішніх розслідувань і профілактики витоків. Таким чином, Українське право у галузі захисту персональних даних, що пройшло через довгий шлях становлення, продовжує свій розвиток. Більше 70% українців згідно з соціологічними опитуваннями стурбовані станом захисту особистої інформації в Інтернеті, тому розвиток законодавства у даній сфері залишається одним з найбільш актуальних питань для України.

Науковий керівник – ст. викл., І.М. Мужик