СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПІДПРИЄМСТВА ТА ОЦІНКА ЇЇ ЕФЕКТИВНОСТІ

Гріненко Т.О., Шаповал М.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Впровадження нових елементів технологічної інфраструктури має великий спектр ризиків, що пов'язані з обробкою персональних даних. Питання захисту персональних даних постає особливо гостро для державних установ та організацій, які в силу своєї діяльності збирають й обробляють відомості про фізичну особу. Відповідно до Законів України «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах» персональні дані повинні захищатись від несанкціонованого доступу, модифікації та розповсюдження.

Метою доповіді є обґрунтування вимог до систем захисту персональних даних для інформаційних (автоматизованих) систем, порядку проведення робіт з розробки системи захисту персональних даних підприємства та оцінки ефективності такої системи.

Для забезпечення інформаційної безпеки необхідно використовувати комплексний підхід, тобто необхідно систематизувати усі заходи щодо захисту персональних даних у п'ять рівнів захисту: нормативно-правовий, організаційний, інженерно-технічний, апаратний та апаратно-програмний. Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації [1].

Мінімізувати неконтрольоване поширення інформації за межі інформаційних систем, у яких вона обробляється, можна шляхом впровадження систем протидії внутрішнім загрозам чотирьох класів: системи моніторингу та аудиту; системи автентифікації; системи, що реалізує засоби шифрування; системи виявлення і попередження витоку інформації (DLP-системи) [2].

Процес обробки та захисту персональних даних повинен ґрунтуватися на підході, який передбачає систематичне оцінювання ризиків, які можуть виникнути для суб'єктів відносин, пов'язаних з персональними даними. Управління ризиками полягає в описі всіх процесів роботи з даними усередині й ззовні організації, що дозволить проводити пошук найбільш вразливих місць у системі захисту інформації.

Список літератури

1. НД ТЗІ 3.7-003-05 – Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. [Електрон. ресурс]: – Режим доступу: https://tzi.com.ua/downloads/3.7-003-2005.pdf.

2. Гулак Г.М., Козачок В.А., Складанний П.М., Бондаренко М.О., Вовкотруб Б.В. Системи захисту персональних даних в сучасних інформаційно- телекомунікаційних системах. *Сучасний захист інформації*. 2017. Т. 30. №2. С. 65-70. DOI: http://nbuv.gov.ua/UJRN/szi_2017_2_12.