УДК 004.056.5

ФОРМАЛІЗОВАНЕ ПРЕДСТАЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СПРИЧИНЕНИХ ПЕРСОНАЛОМ

Іванчук Т.С.

Кухарська Н.П., ЛДУ БЖД, доцент, канд. фіз.-мат. наук

ЛДУ БЖД

Забезпечення безпеки конфіденційної інформації (КІ) завжди було і залишається однією з важливих проблем захисту інформації. У результаті її витоку зазнає значного матеріального і морального збитку не тільки власник КІ, але і держава у цілому.

Це пов'язано з очевидними і цілком об'єктивними закономірностями, які мають місце у сучасних непростих умовах інформаційних взаємовідносин. Проведені Аналітичним центром InfoWatch дослідження[1] демонструють доволі стійку тенденцію до збільшення кількості випадків витоку КІ. Аналіз статистичних данихпоказує: у 2014 році 73 % витоків КІ були наслідком впливу внутрішніх загроз на автоматизовану інформаційну систему, її відносно самостійні структурні елементи.У розподілі за характером дій порушника у 81 % випадках зафіксований "класичний" витік – втрата контролю над інформацією.12 % усіх витоків конфіденційних даних зв'язано з неправомірним використанням інформації, до якої працівники мали легітимний доступ. У таких випадках, як правило, мова йде про фінансове шахрайство банківських працівників. 7 % зареєстрованих інцидентів класифіковано як порушення, що пов'язаніз отриманням несанкціонованого доступу до інформації (перевищення прав доступу, маніпуляція з інформацією, котра не потрібна працівнику для виконання службових обов'язків)У 2014 році внутрішні зловмисники майже не використовували такі канали передачі інформації, як мобільні пристрої (0,2 %), знімні носії (2,0 %), електрону пошту (1,2 %), паперові документи (4,9 %). "Просунутий" зловмисник став обізнаним: сучасні засоби контрою дають змогу успішно перехопити передачу КІ перерахованими каналами і через те не ризикувавдаремно.Водночас, зауважимо, частка витоків не завжди відображає розмір небезпеки, пов'язанийз конкретним каналом. Цілком очевидно, достатньо одного випадку витоку критично важливої інформації, наприклад, каналом "Електронна пошта", щоб організація стикнулася з багатомільйонними втратами.

Ризики спричинені персоналом є окремою групою ризиків інформаційної безпеки (ІБ) організації, позаяк, спектр причин і умов їх реалізації доволі широкий. Опишемо ризики, джерелом яких є персонал, у вигляді факторної моделі – системи причин й умов, що сприяють їх реалізації (рис. 1).

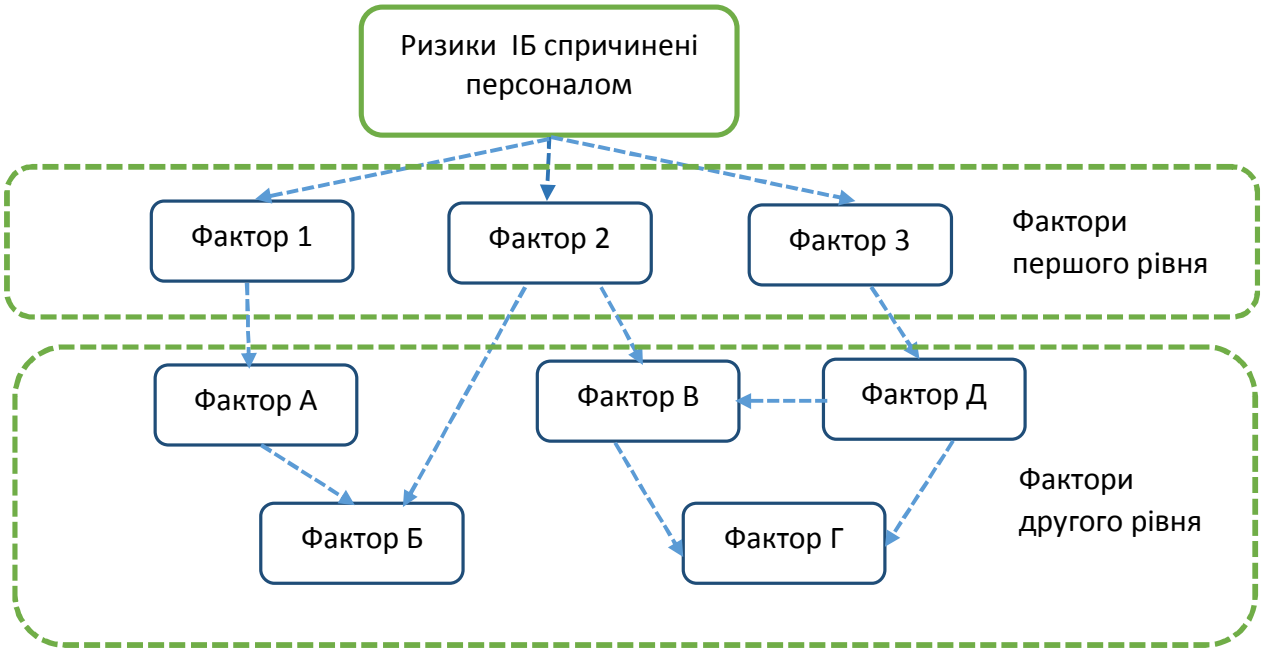

Рис.1. Узагальнена структура факторної моделі ризиків ІБ, джерелом яких є персонал

Виокремимо два рівні факторів:

- Фактори ризику другого рівня – явища, котрі можуть оброблятися (оцінюватися, управлятися) організацієюкожен зокрема, між факторами цієї групи існують багаточисленні зв’язки, можливі цикли як позитивного, так і негативного зворотного зв’язку.
- Фактори ризику першого рівня безпосередньо впливають на реалізацію ризиків від персоналу, вони консолідують вплив всієї множини факторів ризику другого рівня і дають змогу спростити роботу з моделлю. Зв'язки всередині групи факторів першого рівня відсутні.

Фактори ризику першого рівня деталізуються через систему факторів ризику другого рівня – більш дрібних (і через те більш зрозумілих) явищ, що сприяють реалізації загроз ІБ від персоналу. Відзначимо, що деякі фактори другого рівня можуть повторюватися для декількох факторів першого рівня, оскільки впливають на них одночасно.

На основі використання запропонованої моделі підвищення захищеності організації щодо загроз ІБ від персоналуможе бути досягнуто шляхом оцінювання та контролю з боку організації факторів ризику другого рівня.

ЛІТЕРАТУРА

1. Глобальное исследование утечек конфиденциальной информации в 2014 году [Электронный ресурс]. – Режим доступа : http://www.infowatch.ru/report2014