УДК 004.056.5

АНАЛІЗ СТАТИСТИЧНИХ ДАНИХ ЩОДО ВИКОРИСТОВУВАНИХ В ОРГАНІЗАЦІЯХ ЗАСОБІВ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Іванчук Т.С., ЛДУ БЖД
НК – Кухарська Н.П., к. ф.-м. н., доцент, ЛДУ БЖД

Дослідження "Лабораторії Касперського" [1] виявили, що до найбільш популярних у 2014 році засобів забезпечення інформаційної безпеки IT-інфраструктури в організаціях, незалежно від їх розміру, належать антивірусні програми (ними користувалися близько 60 % опитаних респондентів) та регулярне оновлення програмного забезпечення (ПЗ) і встановлення виправлень (патчів) (53 %). Інші засоби використовувалися рідше: контроль додатків (38 %), шифрування інформації на робочих станціях працівників організації та на знімних носіях (по 23 %). Зауважимо, і антивірусне ПЗ, і оновлення програм, і системи шифрування даних вже декілька років входять до складу стандартного набору інформаційної безпеки (ІБ). Їх рівень проникнення високий, і, відповідно, з кожним роком респонденти все рідше включають їх в список заходів, що були вперше застосовані за досліджуваний період.

Серед нових заходів, вжитих організаціями у 2014 році для забезпечення ІБ, – впровадження систем для захисту фінансових транзакцій (36 % респондентів), технологій захисту мобільних пристроїв (31 %), засобів підтримки працездатності веб-сервісів і захисту від DDoS-атак (28 %). Також, 24 % респондентів вказали на ще один новий для них засіб безпеки – застосування систем для захисту від витоку даних (Data Loss/Leakage Protection, DLP). У той же час, результати цих досліджень свідчать: з внутрішніми інцидентами ІБ протягом року зіткнулися 87 % організацій; майже чверть (24 %) таких інцидентів привели до втрати конфіденційної інформації (КІ). До ключових ризиків всередині організацій "Лабораторія Касперського", зокрема, віднесла: незнання працівниками правил IT-безпеки, що привели до випадкових витоків даних (36 %), зумисне розкриття працівниками КІ (23 %). Інциденти, пов'язані з неналежним обміном інформацією через мобільні пристрої (електронну пошту, SMS і т.д.) становлять 21 %, і майже стільки ж (20 %) – інциденти, спричинені втратою чи крадіжкою мобільних пристроїв працівників.

На основі цих результатів опитувань, можна зробити такі висновки:

- Спостерігається розрив між високим рівнем небезпеки внутрішніх загроз і засобами, що застосовуються для їх запобігання. На фоні внутрішніх загроз організаціями перебільшено ризики вірусних, хакерських і спамерських атак, котрі ефективно попереджаються доступними сьогодні технологіями.
- Всебічний аналіз ролі персоналу у забезпеченні безпеки КІ організацій свідчить про зростаючу актуальність вирішення проблеми внутрішніх витоків.

Аналізуючи вище наведені статистичні дані, виокремимо основні причини такого стану справ:

- Недостатня увага посадових осіб організацій, підприємств та інших структурних утворень щодо забезпечення захисту КІ, а деколи відсутність такої уваги взагалі.
- Має місце серйозний розрив між усвідомленням необхідності запобігання загрозам витоку КІ і реалізацією засобів, методів і заходів, використовуваних для їх захисту.
- Перешкоди, які змушені переборювати організації у процесі запобігання внутрішніх загроз, значною мірою пов'язані з відсутністю необхідних фінансових засобів.

ЛІТЕРАТУРА

1. Информационная безопасность бизнеса [Электронный ресурс]. – Режим доступа : http://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf