УДК 044.56.5 (043.2)

ОЦІНКА ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В ТРАНСПОРТНІЙ ГАЛУЗІ

Аль-Амморі Алі[1], Сергій Заворотний[2]

Національний транспортний університет, [1]ammourilion@ukr.net

[2]seregazavorotnyi@gmail.com

В процесі експлуатації інформаційних систем (ІС) транспортної галузі, можливе виникнення умов, які непередбачені розробником, при проектуванні систем захисту інформації (СЗІ). Оцінка ефективності захисту інформації повинна обов'язково мати як розрахунковий так і ймовірнісний характер. Методологія оцінки повинна включати систему нормативних документів, що містять кількісні, вимірювані показники ефективності СЗІ, та забезпечить вимоги як замовників так і проектувальників. Необхідність обґрунтування оптимальних значень показників ефективності, що враховує цільове призначення інформаційної системи транспортної галузі є актуальним та дуже важливим питанням в наукових колах. Для вирішення проблеми пропонується використовувати системний підхід. Саме кількісне визначення ефективності може розглядатися як основа для вирішення проблеми.

Мета дослідження полягає в виконанні аналізу нормативно-методичного забезпечення оцінки ефективності захисту інформації в транспортній галузі.

Статистика атак на ІС в транспортній галузі, вказує на негативну тенденцію вразливості ІС до атак та проникнень в інформаційні бази та системи. Атаки реалізуються на складові автоматизованих систем керування (АСК), системи SCADA та HMI (людино-машинний інтерфейс).

Засоби захисту інформації (ЗЗІ), відповідно до чинних норм та правил, підлягають обов'язковій сертифікації. Однак, сертифікація не є досконалим інструментом і в кращому випадку перевіряють лише 85% від всіх можливих засобів, а зазвичай навіть 60-70%.

Об'єктивне підтвердження ефективності СЗІ є складним процесом, що може ускладнюватися недосконалістю існуючої нормативної бази, а також принциповій різниці інженерії ІТ від традиційної. Як приклад, фахівцями галузі відзначається недостатність систем нормативних показників інформаційної безпеки та критеріїв ефективності СЗІ.

Нормативні документи щодо оцінки безпеки ІТ практично не містять конкретних методик, внаслідок чого різниця між загальними деклараціями та конкретним інструментарієм щодо реалізації та контролю їх положень достатньо велика. Виходячи з призначення, методична база повинна охоплювати всі критично важливі аспекти забезпечення та перевірки виконання вимог, що висуваються до СЗІ в транспортній галузі. У методичному плані визначення ефективності СЗІ повинно полягати у виробленні висновку щодо придатності способу дій персоналу або пристосованості технічних засобів до досягнення мети захисту інформації на основі вимірювання відповідних показників, наприклад, при функціональному тестуванні.

Відповідно до сучасної теорії оцінки ефективності систем, якість будь-якого об'єкта, у тому числі і СЗІ, проявляється лише в процесі цільового функціонування, тому найбільш об'єктивним є оцінювання ефективності застосування. Процедури випробувань, сертифікації або ліцензування не повністю усувають невизначеність властивостей СЗІ або її окремих елементів і не враховують випадковий характер атак. Тому об'єктивною характеристикою якості СЗІ може бути лише ймовірність, що характеризує ступінь можливостей конкретної СЗІ при заданому комплексі умов.

У сучасних нормативних документах з інформаційної безпеки використовується класифікаційний підхід. Ймовірнісні методи також знайшли широке поширення у практиці забезпечення безпеки інших прикладних областях. Відповідно до цих методів рівні гарантій безпеки СЗІ трансформуються на довірчі ймовірності відповідних оцінок показників.

Узагальнені дані про можливі показники ефективності наведено у таблиці 1.

Таблиця 1

Можливі показники ефективності СЗІ та критерії ефективності СЗІ

Вимоги до СЗІ	Види показників ефективності СЗІ
Початок та закінчення випадків	Ймовірність випадку
Досягнення необхідних характеристик	Ймовірність досягнення результату не менше необхідного рівеня
Не встановлені	1. Математичне очікування результату 2. Дисперсія результату
Концепція ефективності СЗІ	Критерії ефективності
Придатність	1. Прийнятний результат 2. Допустимий результат
Оптимальність	1. Найкращий результат 2. Найкращий середній результат

Висновок. Нормативно-методичної бази в сфері інформаційної безпеки, що використовується в транспортної галузі не відповідає сучасним вимогам інформаційної безпеки. Для визначення необхідного рівень безпеки СЗІ, потрібно виконувати оцінку ефективності СЗІ за рахунок показників, які мають ймовірнісний характер.

Змістовні результати з оцінювання ефективності систем захисту, можуть бути отримані при системному підході. Кількісна оцінка ефективності СЗІ є сучасним ефективним методом на відміну від якісних методів.