Система оцінювання ризиків інформаційної безпеки в режимі реального часу

УДК 621.395.7 (043.2)

Світлана Казмірчук[1], Єгор Часновський[2], Олександр Корченко

Національний авіаційний університет, [1]sv.kazmirchuk@gmail.com, [2]egor.chasnovskii@gmail.com

Враховуючи, що більшість активів підприємств перебувають у цифровому вигляді, загроза несанкціонованого доступу через цифровий пристрій і його програмне забезпечення безсумнівно має грати ключову роль при побудові системи менеджменту інформаційної безпеки (ІБ) підприємства та оцінюванні ризиків (ОР) ІБ.

Для визначення уразливостей ІБ досліджуваної інформаційної системи на тепер існує ряд методів ОР ІБ, які допомагають організаціям оцінювати свої ризики, впроваджувати відповідні заходи безпеки для їх усунення та дотримуватися вимог щодо управління ризиками ІБ. Однак, більшість існуючих методів ОР ІБ вимагають роботи експерта відповідної предметної області та не передбачають функціоналу проведення ОР ІБ в режимі реального часу. Тому актуальним є питання розробки системи ОР ІБ, яка дозволить отримувати результати ОР ІБ в режимі реального часу з актуальними даними шляхом синхронізації CVSS метрик з відомими відкритими базами даних уразливостей ІБ.

Метою даної роботи є розробка системи ОР ІБ, що дозволить реалізовувати оцінювання в режимі реального часу без залучення експертів відповідної предметної області. Для досягнення поставленої мети необхідно реалізувати наступну задачу – удосконалити існуюче структурне рішення системи ОР ІБ за рахунок введення в підсистему формування вхідних даних (ПФВД) модуля ідентифікації уразливостей (МІВ) та модуля синхронізації CVSS метрик БД уразливостей NIST (МСБД).

Модуль МСБД виконує підключення до зазначеної БД, порівнює хеш-значення попередньо завантаженого meta-файлу з файлом, що знаходиться на сервері NIST. У разі не співпадіння хеш-значення локального файлу з файлом на сервері відбувається оновлення локального файлу з уразливостями відповідного року, що дозволяє отримувати актуальні дані з наявних на цільовій системі. Модуль МІВ виконує сканування цільової системи, записуючи у спеціальний службовий файл всю інформацію про наявне встановлене програмне забезпечення. Після етапу сканування відбувається пошук відсканованого ПЗ у CVSS файлах уразливостей, що були попередньо підготовлені МСБД. У випадку, якщо наявне ПЗ має уразливості, дані про неї з XML файлу записуються у спеціальний список.

Таким чином, було удосконалено структурне рішення системи ОР ІБ в режимі реального часу, за рахунок введення в ПФВД модулів МІВ та МСБД, які дозволять реалізувати ОР ІБ в режимі реального часу без залучення експертів відповідної предметної області.