УДК 683.1
Олексій Олександрович ДЕРЕВЯГІН,
кандидат юридичних наук, старший науковий співробітник,
доцент кафедри оперативно-розшукової діяльності та розкриття злочинів факультету № 2
Харківського національного університету внутрішніх справ
ORCID: https://orcid.org/0000-0003-1622-5549

АЛГОРИТМ ПРОВЕДЕННЯ ОЦІНКИ БЕЗПЕКИ ТА ЗАХИЩЕНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Перед початком оцінювання програмного забезпечення (далі – ПЗ) кожному оцінювачу необхідно детально ознайомитись з усією нормативною базою, яка стосується даного питання.

Під час проведення оцінки безпеки та захищеності ПЗ необхідно дотримуватися певної методології та структури. Методологія оцінки характеристик безпеки та захищеності ПП у відповідності зі стандартом ДСТУ ISO/IEC 14598 «Інформаційні технології. Оцінювання програмного продукту» в загальному виді можна представити так:

- розробка вихідних вимог для проведення оцінювання (визначення цілей випробувань; вибір характеристик, субхарактеристик, вибір метрик, визначення їхніх необхідних значень);
- визначення методики оцінювання характеристик якості ПЗ, встановлення рівнів пріоритету метрик, виділення критеріїв для проведення вимірювань;
- планування й проектування процесу оцінки характеристик якості в життєвому циклі ПЗ;
- проведення вимірювань для оцінювання; порівняння результатів із критеріями й вимогами;
- узагальнення й оцінка результатів.

Для кожної характеристики якості рекомендується сформувати шкалу вимірювань з виділенням необхідних, припустимих і незадовільних значень.

Відповідно до вищевикладеної методології та матеріалів стандарту ISO/ IEC 9126 «Software engineering – Product quality» можна описати процес оцінювання у вигляді покрокової процедури, орієнтованої на використовування узагальненої моделі якості, представленої в даному стандарті:

1) Формування вимог до оцінювання;
2) Специфікація оцінювання;
3) Проектування оцінювання;
4) Виконання оцінювання.

Відповідно до цієї структури оцінювач, під час проведення оцінки безпеки та захищеності програмного продукту, повинен:

1) Сформулювати ціль оцінювання – перевірка відповідності програмного продукту вимогам безпеки та захищеності;

2) Ідентифікувати вид продукту, тобто визначитися з тим, що він собою представляє, в якій сфері та галузі буде використовуватись і з якою метою, які до нього ставляться вимоги і таке інше. Відповідно до цього формуються певні вимоги до самого процесу оцінювання;

3) Визначитися з характеристиками та субхарактеристиками якості, які він буде використовувати в процесі оцінювання. Крім субхарактеристик «безпека» та «захищеність» можливе використання й інших характеристик, пов'язаних з ними. (відповідно до стандарту ISO/IEC 9126-1: 2001 Software Engineering – Product Quality – Part 1: Quality model);

4) Визначитися із складом метрик безпеки та захищеності, які використовуватимуться в процесі оцінювання. Їх перелік та способи обчислення визначається серіями міжнародних стандартів ISO/IEC TR 9126-2:2003 Software Engineering – Product Quality – Part 2: External metrics, ISO/IEC TR 9126-3:2003 Software Engineering – Product Quality – Part 3: Internal metrics, ISO/IEC TR 9126-4:2004 Software Engineering – Product Quality – Part 4: Quality in use metric;

5) Встановити рівні пріоритету метрик безпеки та захищеності, тобто впорядкувати їх за значимістю та назначити відповідні вагові коефіцієнти;

6) Визначитися з критеріями оцінювання. Відповідно до документації програмного забезпечення та вимог, що до нього ставляться встановити кількісні значення субхарактеристик і метрик, яким повинно відповідати програмне забезпечення, що оцінюється;

7) Визначитися з планом оцінювання. З'ясувати на кого розрахована оцінка: розробника, замовника чи незалежного оцінювача;

8) Виміряти кількісні показники метрик та субхарактеристик «безпека» та «захищеність». Перед цим визначитися з формулами та методикою їх обчислення;

9) Порівняти виміряні показники з встановленими до процесу оцінювання значеннями (з встановленим критерієм);

10) На основі аналізу отриманих результатів оцінювання субхарактеристик якості «захищеність» та «безпека» сформувати експертний висновок про ступінь відповідності ПЗ вимогам захищеності та безпеки, який повністю залежить від характеристики оцінюваного ПЗ, вимог, які до нього ставляться, сфери його застосування, повноти та ймовірності процесу оцінювання, а також особи оцінювача.

Висновок. Запропонований алгоритм проведення оцінки безпеки та захищеності програмного забезпечення (ПЗ) відповідає вимогам Законів України «Про Інформацію», «Про наукову і науково-технічну експертизу», «Про захист інформації в інформаційно-телекомунікаційних системах», а також відповідно до міжнародних стандартів ISO/IEC 9126 «Software engineering - Product quality» і ISO/IEC 14598 «Software engineering - Product evaluation» та адаптованих до них ДСТУ ISO/IEC 14598 «Інформаційні технології. Оцінювання програмного продукту» та має на меті допомогти оцінювачу програмного продукту ефективно провести експертизу щодо встановлення факту відповідності програмного забезпечення вимогам безпеки та захищеності.

Одержано 19.10.2018