Система оцінювання ризиків інформаційної безпеки – «РИЗИК-КАЛЬКУЛЯТОР»

УДК 621.395.7 (043.2)

Світлана Казмірчук[1], Єгор Часновський[2]

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

У забезпеченні надійності процесів обробки інформації та досягненні необхідного рівня інформаційної безпеки (ІБ) особливе місце займає управління ризиками порушення базових характеристик безпеки ресурсів інформаційних систем (РІС), таких як конфіденційність, цілісність і доступність. Ризики ІБ, що виникають в результаті інформаційної діяльності, можна моніторити за допомогою їх оцінювання в процесі функціонування інформаційної системи (ІС). Це дозволить визначити коректні, фінансово безпечні шляхи реалізації бізнес-процесів на підприємстві, в якому функціонує ІС. Про важливість вирішення даного завдання свідчить, зокрема, прийняття низки державних і міжнародних стандартів у цій галузі (ISO / IEC 27001, ISO / FDIS 31000 та ін.).

Однак, на даний момент більшість існуючих систем оцінювання ризиків (ОР) ІБ потребують підтримки експерта, що пов'язано з додатковими фінансовими і тимчасовими витратами. Тому актуальним є розробка таких систем, які дозволять автоматизувати процес ОР ІБ, наприклад, шляхом використання необхідних для роботи параметрів з відповідних баз даних (БД), наприклад, CVSS метрик.

Метою даної роботи є розробка системи ОР ІБ, що дозволяє мінімізувати участь експерта і максимально автоматизувати процес формування необхідних для оцінювання параметрів.

Для реалізації поставленої задачі пропонується створення системи ОР ІБ – «РИЗИК-КАЛЬКУЛЯТОР». Така система, на базі синтезу систем ОР безпеки РІС, основаних на логіко-лінгвістичному підході, аналітико-синтетичній кортежній моделі та якісно-кількісному методі ОР ІБ, шляхом використання CVSS оцінок, які представляються в існуючих БД, дозволить автоматизувати процес ОР в режимі реального часу, а також за запитом користувача трансформувати еталонні лінгвістичні змінні (ЛЗ) і не привертати для цього експертів відповідної предметної області. Окрім цього, система включає функцію редагування вбудованих метрик, використовуючи вбудований CVSS калькулятор версії 3.0.

Структурно-параметрична модель запропонованої системи складається з двох базових компонент, що відображають підсистеми обробки первинних (ППОД) і вторинних даних (ПВОД). Опишемо склад кожної з підсистем, побудова яких здійснюється відповідно до методології якісно-кількісного методу ОР ІБ. Підсистема ППОД призначена для первинної обробки початкових величин і включає в себе модуль ініціалізації вхідних даних (МІД), а також модулі формування (МФЕ) і перетворення (МПЕ) еталонних значень. Підсистема ПВОД, використовуючи CVSS метрики, здійснює перетворення первинних параметрів, що надходять з ППОД з метою формування остаточних

оцінок ступеня ризику (СР). Вона складається з модуля зважування оціночних параметрів (МРП) і їх коригування (МКП), а також модулів оцінки СР (МСР) і генерації звіту (МГЗ).

В якості вхідних даних можуть використовуватися, наприклад, результати роботи програми для перевірки системи на проникнення (Penetration test). Таке програмне забезпечення, як правило, виконує аналіз зазначеного об'єкта, виконуючи пошук вразливостей його РІС в кіберпросторі (згідно ISO / IEC 27032: 2012 року під кіберпростором можемо розуміти складну сутність, яка реально існує у вигляді глобальної сукупності процесів взаємодії людей, програмного забезпечення і сервісів Інтернет в мережах, але яка при цьому ніяк не проявляється в будь-якої відомої, матеріальній формі).

Таким чином, формується список у вигляді множини вразливостей РІС досліджуваного об'єкта. Для отримання множини РІС і множини відповідних уразливостей в МІД виконується обробка отриманого зі спеціалізованого програмного забезпечення (рівня - Penetration test), відповідного звіту, який містить в собі інформацію про РІС і вразливості з зазначеними CVSS метриками. Далі, здійснюється ініціалізація списку вразливостей і РІС, для подальшої передачі в МФЕ. В результаті роботи МІД на вхід МФЕ надходять всі ідентифіковані об’єкти РІС з вказаними вразливостями та їх CVSS метриками.

У разі необхідності можливе корегування CVSS метрик за допомогою МКП, в якому реалізується їх перевизначення за рахунок вбудованого CVSS-калькулятора версії 3.0. Скореговані параметри CVSS метрики, B, T, E передаються назад в МРП.

Дані з МРП надходять до МСР, де на основі 10 етапу якісно-кількісного методу ОР ІБ, для кожної уразливості, реалізується оцінювання СР уразливості, а також обчислюється середнє значення СР для кожного РІС. Далі, на основі розрахованого значення СР уразливості та середнього значення СР кожного РІС і побудованих еталонів в ППОД, відбувається процес дефазифікації, який пов'язаний з формуванням структурного параметру СР кожної уразливості і дозволяє отримати числові значення СР і його лінгвістичну інтерпретацію.

На основі МГЗ, з врахуванням результатів роботи ППОД та ПВОД, генерується звіт по оцінкам СР, який включає РІС, лінгвістичні еквіваленти СР кожної вразливості та графічну інтерпретацію результатів.

Таким чином, була розроблена структурно-параметричну модель системи ОР ІБ - «РИЗИК-КАЛЬКУЛЯТОР», яка, за рахунок структурних компонент підсистем, формування первинних і вторинних даних, а також складових їх модулів ініціалізації вхідних даних, формування і перетворення еталонних значень, зважування оціночних параметрів і їх коригування, оцінювання СР і генерації звіту, в яких реалізовані запропоновані методи (якісно-кількісний, оцінювання на основі баз даних вразливостей, інкрементування та декрементування порядку лінгвістичних змінних), дозволяє забезпечити високу гнучкість і зручність при ОР безпеки РІС без участі експертів відповідної предметної області.

Науковий керівник – д-р. т. наук, доцент кафедри БІТ, Казмірчук С.В.