УДК 65.011.3

Ігнатьєва І.Д. студентка групи 125м-16-1
Науковий керівник: Галушко С.О., ст. викладач безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

МЕТОДИ АНАЛІЗУ РИЗИКІВ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Оцінка ризику ІБ є частиною процесу менеджменту ризику і являє собою структурований процес, в рамках якого виявляють способи досягнення поставлених цілей, проводять аналіз наслідків та ймовірності виникнення небезпечних подій для прийняття рішення щодо необхідності обробки ризику. Інакше кажучи, оцінка ризику є процесом, що об'єднує ідентифікацію, аналіз ризику і порівняльну оцінку ризику. Спосіб реалізації цього процесу залежить не тільки від сфери застосування процесу ризик-менеджменту, але також і від методів оцінки ризику. Стандарт ДСТУ IEC/ISO 31010:2013 "Керування ризиком. Методи загального оцінювання ризику" є загальним для всіх областей ризику і призначений для різних цілей організації. Менеджмент ризику допомагає в прийнятті рішень в умовах невизначеності і можливості виникнення подій або обставин (планових і непередбачених), що впливають на досягнення цілей організації.

Стандарт визначає 31 метод аналізу ризиків, з яких і будуть обиратися оптимальні методи для аналізу ризиків інформаційної безпеки. Перерахуємо їх найменування: "Мозкова атака", "Структуроване чи напівструктуроване опитування", "Метод Делфі", "Переліки контрольних запитань", "Попереднє аналізування небезпечних чинників (PHA)", "Дослідження небезпечних чинників і працездатності (HAZOP)", "Аналізування небезпечних чинників і критичні точки контролю (HACCP), "Загальне оцінюванная екологічного ризику", "Структурований метод "Що - якщо" (SWIFT)", "Аналізування сценаріїв", "Аналізування впливу на діяльність (BIA)", "Аналізування першопричини (RCA)", "Аналізування видів і наслідків відмов (FMEA)", "Аналізування дерева відмов (FTA)", "Аналізування дерева подій (ETA)", "Аналізування причин і наслідків", "Аналізування причинно-наслідкових зв'язків", "Аналізування рівнів захисту (LOPA)", "Дерево рішень", "Загальне оцінювання надійності людини (HRA)", "Аналізування за схемою "краватка-метелик", "Технічне обслуговування, зорієнтоване на забезпечення безвідмовності", "Аналізування паразитних схем (SA)", "Марковське аналізування", "Імітаційне моделювання за методом Монте-Карло", "Байєсова статистика і мережі Байєса", "Криві FN", "Показники ризику", "Матриця "наслідок-ймовірність", "Аналізування витрат і вигод (CBA)", "Багатокритерійне аналізування рішень (MCDA)".

Завдання вибору методу можна розділити на 2 етапи:

1) вибір придатного методу відповідно до галузі інформаційної безпеки за допомогою оцінки;

2) вибір оптимального методу оцінки ризику.

З вище перелічених методів такі не придатні для аналізу інформаційної безпеки: "Дослідження небезпечних чинників і працездатності (HAZOP)", "Аналізування небезпечних чинників і критичні точки контролю (HACCP)", "Загальне оцінюванная екологічного ризику".

Далі розглянемо методи які стосуються кожного етапу оцінки ризиків. Для ідентифікації ризиків не підходять такі методи: "Аналізування першопричини (RCA)", "Дерево рішень", "Аналізування за схемою "краватка-метелик", "Імітаційне моделювання за методом Монте-Карло", "Байєсова статистика і мережі Байєса". Таким чином, вибір зменшується і тепер вибираємо з 23 методів.

Оптимальність методів розглядається показниками наступних властивостей:

- ресурсомісткість (необхідні ресурси: тимчасові, інформаційні та інші);
- характеру і ступеня невизначеності оцінки ризику, заснованої на доступній інформації і відповідностям цілям;
- складності проблеми і методів, необхідних для аналізу ризиків.

З таблиці А.2 Додатка А, стандарту ДСТУ IEC/ISO 31010:2013 вибираємо найоптимальніші за наведеними властивостями: “Структуроване опитування”, “Мозковий штурм” та “Переліки контрольних запитань”. Таким чином, для етапу ідентифікації ризику ми вибрали три методи, які можна комбінувати або використовувати найкращий з них.

Для етапу аналізу ризику не підходять такі методи: “Структуроване чи напівструктуроване опитування”, “Переліки контрольних запитань”, “Мозкова атака”, “Метод Делфі”, “Попереднє аналізування небезпечних чинників (PHA)”, “Імітаційне моделювання за методом Монте-Карло”, “Байєсова статистика і мережі Байєса”. Таким чином залишається 21 метод. оптимальні з них: “Структурований метод "Що - якщо", “Аналізування впливу на діяльність (BIA)”, “Аналізування першопричини (RCA)”, “Аналізування видів і наслідків відмов (FMEA)”, “Аналізування дерева подій (ETA)”, “Аналізування причинно-наслідкових зв’язків”, “Аналізування рівнів захисту (LOPA)”, “Загальне оцінювання надійності людини (HRA)”, Технічне обслуговування, зорієнтоване на забезпечення безвідмовності”, “Аналізування паразитних схем (SA)”, “Матриця “наслідок-ймовірність”.

Для порівняльної оцінки ризику не підходять такі методи: “Переліки контрольних запитань”, “Структуроване чи напівструктуроване опитування”, “Мозкова атака”, “Метод Делфі”, “Попереднє аналізування небезпечних чинників (PHA)”, “Аналізування дерева подій (ETA)”, “Аналізування причинно-наслідкових зв’язків”, “Аналізування рівнів захисту (LOPA)”, “Аналізування паразитних схем (SA)”, “Марковске аналізування”. З 21 вибираємо оптимальні, грунтуючись також на можливості отримання кількісних вихідних даних: “Аналізування дерева відмов (FTA)”, “Аналізування причин і наслідків”, “Аналізування за схемою "краватка-метелик", “Технічне обслуговування, зорієнтоване на забезпечення безвідмовності”, “Імітаційне моделювання за методом Монте-Карло”, “Байєсова статистика і мережі Байєса”.

Висновок. У цій статті було проведено відбір методів оцінки ризику інформаційної безпеки по кожному етапу загального процесу на базі стандарту ДСТУ IEC/ISO 31010:2013

Практичний досвід побудови моделі загроз інформаційній безпеці виявив, що запропонований підхід значно спрощує завдання застосування методів оцінки ризику для конкретних інформаційних систем і заданого рівня безпеки інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Смогунов В.В., Вершинин Н.Н., Авдонина Л.А.Классификация методов управления риском // Труды международного симпозиума Надежность и качество. 2009 Т. 2. С. 235-238.
2. ДСТУ IEC/ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику.