Функції системи управління інформаційною безпекою

УДК 004[056.53+413.4]

Володимир Мохор[1], Василь Цуркан[2]

ІПМЕ ім. Г.Є. Пухова НАН України, [1]v.mokhor@gmail.com,
КПІ ім. Ігоря Сікорського,[2]v.v.tsurkan@gmail.com

Забезпечення конфіденційності, цілісності та доступності інформації в організації досягається завдяки реалізуванню функцій системою управління інформаційною безпекою. Вони реалізуються з огляду на наявність вхідних і вихідних даних, обмежень і механізмів. Тому для формалізування її функцій використано графічну нотацію функціонального моделювання IDEF0 (Integrated Computer Aided Manufacturing Definition).

Метою даної роботи є формалізування функцій системи управління інформаційною безпекою в організації.

Функції системи управління інформаційною безпекою формалізуються функціональним блоком. Кожна сторона такого блоку характеризується своїм призначенням: ліва – вхідні дані, права – вихідні дані, верхня – обмеження, нижня – механізми, виклики. Водночас визначається мета та точка зору функціонального моделювання системи управління інформаційною безпекою. Зокрема, метою є забезпечення конфіденційності, цілісності та доступності інформації. Тоді як точкою зору визначаються організація, а також внутрішні (вище керівництво, персонал) та зовнішні зацікавлені сторони. Важливість виокремлення зацікавлених сторін обумовлена тим, що з їхнього боку можливе встановлення важливих вимог для забезпечення інформаційної безпеки.

При розгляданні діяльності управління інформаційною безпекою як функції верхнього рівня виокремлюються такі вхідні дані: інформаційні активи, відомості про інформаційні активи, відомості про організацію. За результатами зазначеної діяльності отримуємо збереженість властивостей інформаційних активів (конфіденційність, цілісність, доступність) з прийнятним рівнем ризику. Управління інформаційною безпекою обмежується зовнішніми та внутрішніми обставинами організації; вимогами зацікавлених сторін до забезпечення інформаційної безпеки, а також інтерфейсами та залежностями між діями в організації. Цей перелік уточняється виокремленням критеріїв оцінювання і прийняття ризику інформаційної безпеки. Як механізми розглядаються внутрішні та зовнішні зацікавлені сторони, метод оцінювання ризику інформаційної безпеки; виклик – загальна система управління організацією. Декомпозиція діяльності управління інформаційною безпекою відображена, наприклад, такими функціями: встановлення обставин діяльності організації, встановлення зобов'язань вищого керівництва організації, планування, функціонування, оцінювання ефективності, вдосконалювання системи управління інформаційною безпекою.

Отже, такий підхід дозволяє, по-перше, формалізувати функції системи управління інформаційною безпекою у графічній нотації IDEF0. По-друге, серед них виокремити функцію верхнього рівня як діяльність з управління інформаційною безпекою. По-третє, для кожної них задати вхідні та вихідні дані, обмеження, механізми та виклики. Як наслідок, по-четверте, встановити функціональні межі системи управління інформаційною безпекою.