УДК 004.056: 004.942: 343.1

ВІТАЛІЙ ВІКТОРОВИЧ НОСОВ

к.т.н. доцент професор кафедри захисту інформації ХНУВС

ЗАСТОСУВАННЯ ПОНЯТТЯ "СЦЕНАРІЇ РИЗИКІВ" ДЛЯ СЗІ ОВС УКРАЇНИ У КОНТЕКСТІ СИСТЕМНОГО ПІДХОДУ COBIT®5

У базових державних стандартах із захисту інформації [1, 2, 3] та інших вітчизняних нормативно-методичних документах регламентується визначати та оцінювати для інформації, що захищається, окремі складові інформаційних ризиків: загрози, джерела загроз, ймовірність прояви загроз та очікувану шкоду від їх реалізації, окрему модель загроз. Ці оцінки використовуються при розробленні адекватної системи захисту інформації.

Якщо постулювати необхідність застосування системного мислення та системного підходу при створенні життєздатної системи захисту інформації [4], то представляється доцільним взяти до уваги підходи, що реалізовані у проекті COBIT®5, які є сукупністю взаємопов'язаних методологій та стандартів в галузі управління, аудиту і IT безпеки, розроблених світовою спільнотою фахівців під егідою міжнародної асоціації ISACA (Information System Audit and Control Association, Асоціація з управління і аудиту інформаційної системи).

У методиці [5] бази знань COBIT®5, на відміну від [1, 2, 3], пропонується інтегрований підхід до розгляду складових інформаційних ризиків, де використовується поняття "сценарії ризиків", яке поєднує в собі усі відповідні складові і дозволяє системно виходити на основну мету IT безпеки - надання можливості організації виконувати свої функції (створення цінностей для зацікавлених сторін) при мінімізації ресурсних затрат і виникаючих супутніх IT ризиків (певне поєднання імовірності небажаних подій в IT із їх наслідками).

ОВС України, згідно [6], утворено з метою формування та реалізації державної політики у сфері захисту прав і свобод людини та громадянина, власності, інтересів суспільства і держави від злочинних посягань. Зацікавленими сторонами (на різних рівнях системи), для яких ОВС створює цінності, є людина, суспільство і держава. На інформаційні технології (IT)

спирається уся діяльність ОВС, а значить загальні ризики для ОВС у значній мірі визначаються IT ризиками. IT ризики для ОВС можна поділити на дві категорії: (а) зупинка зростання підтримки цільової діяльності ОВС і (б) втрата вже досягнутого рівня IT підтримки цієї діяльності (рис. 1).

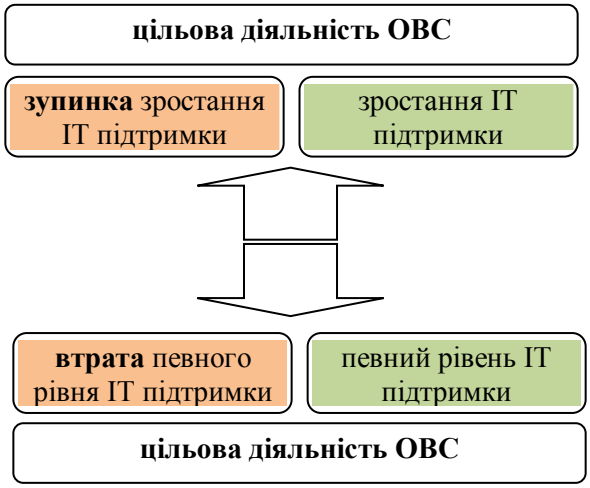

Рис. 1. Категорії IT ризиків ОВС

У рамках системи IT безпеки (системи захисту інформації) ОВС потрібні стратегічне керування (governance) та операційне управління (management) IT ризиками, які потребують створення відповідних структур та процесів за методиками [7, 8].

Рис. 2. Структура сценарію ризику

Сценарії ризиків для ОВС повинні представляти собою опис імовірних подій, що можуть вплинути на процес захисту прав і свобод людини та громадянина, власності, інтересів суспільства і держави від злочинних

посягань. Вплив імовірних подій може бути як позитивним, так і негативним. Структуру сценарію ризику можна представити як на рис. 2.

Сценарії ризиків можуть бути отримані двома різними шляхами (рис. 3):

- *зверху-вниз,* аналізувати задачі основної діяльності ОВС і визначати сценарії найбільш релевантних і імовірних ІТ ризиків, які впливають на виконання цих задач;
- *знизу-уверх,* виходити із відомого переліку типових сценаріїв ІТ ризиків, з якого вибирати найбільш релевантні та уточнювати їх у відповідності із особливостями конкретних ІТ різних підрозділів ОВС. Методика [5] містить потрібний перелік типових сценаріїв ІТ ризиків.

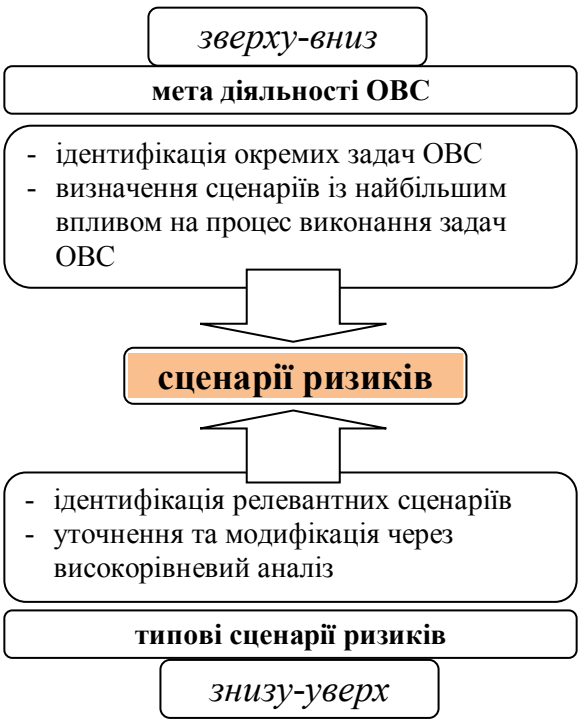

Рис. 3. Шляхи отримання сценаріїв ризику

Таким чином, використання нового поняття "сценарії ризиків" у контексті системного підходу COBIT®5 при створенні життєздатної системи захисту інформації ОВС дозволить поставити процеси захисту інформації у залежність від процесів основної цільової діяльності ОВС.

Список використаних джерел: **1**. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423 - Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=38883&cat_id=38838. – Назва з екрана. **2.** ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту

України від 19.12.96 р. № 511. - Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=38911&cat_id=38836. – Назва з екрана. **3.** ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. №200. - Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=38934&cat_id=38836. – Назва з екрана. **4.** Носов В.В. Системний підхід у забезпеченні інформаційної безпеки / В.В. Носов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2010. – № 1 (20). – С. 92-97. **5.** Risk Scenarios Using COBIT® 5 for Risk. ISACA. 2014. - Режим доступу: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/risk-scenarios-using-cobit-5-for-risk.aspx. – Назва з екрана. **6.** Указ Президента України "Про затвердження Положення про Міністерство внутрішніх справ України" від 6 квітня 2011 р. № 383/2011. - Режим доступу: http://zakon2.rada.gov.ua/laws/show/383/2011. – Назва з екрана. **7.** The Risk IT Framework. ISACA. 2009. - Режим доступу: http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework_fmk_Eng_0610.pdf. – Назва з екрана. **8.** The Risk IT Practitioner Guide. ISACA. 2009. - Режим доступу: http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Practitioner-Guide_res_Eng_0610.pdf. – Назва з екрана.