УДК 004.056

[1] **В.Г. Кононович**
Кандидат технічних наук, доцент кафедри інформаційної безпеки та передачі даних
[2] **Ю.В. Копитін**
Заступник начальника відділу забезпечення захисту інформації

[1] *Одеська національна академія зв'язку ім. О.С. Попова, Одеса*
[2] *Комунальне підприємство «Обласний інформаційно-аналітичний центр», Одеса*

МОДЕЛЮВАННЯ ПРОЦЕСІВ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Наведено моделювання процесів управління ризиками інформаційної безпеки шляхом побудови моделей ідентифікації ризиків за допомогою багатошарових графів, гіперграфів та елементів концепції мережева єдиних мереж, модернізації класичної аналітичної моделі оцінки ризиків, формування моделі обробки ризиків на основі розфарбованої мережі Петрі, презентації моделі виявлення вразливостей у процесі експлуатації системи з використанням ділових ігор, наведення інкрементної моделі побудови системи забезпечення ІБ.

Ключові слова: інформаційна безпека, інформаційно-комунікаційні технології, управління ризиками, загроза, вразливість, оцінка ризиків, обробка ризиків

Приведено моделирование процессов управления рисками информационной безопасности путем построения моделей идентификации рисков с помощью многослойных графов, гиперграфов и элементов концепции кружева единых сетей, модернизации классической аналитической модели оценки рисков, формирования модели обработки рисков на основе раскрашенной сети Петри, презентации модели выявления уязвимостей в процессе эксплуатации системы с использованием деловых игр, представления инкрементной модели построения системы обеспечения ИБ.

Ключевые слова: информационная безопасность, информационно-коммуникационные технологии, управления рисками, угроза, уязвимость, оценка рисков, обработка рисков

The paper demonstrates the modeling of information security risk management by building models of risk identification using multi-graphs, hypergraphs and elements of the concept lace of unified networks, modernization classical analytical model of risk assessment, formation the model of risk treatment based on colored Petri nets, presentation model of identification vulnerabilities in the operating system using business games, prompting incremental model construction information security system.

Keywords: information security, information and communication technology, risk management, threat, vulnerability, risk assessment, risk treatment

Постановка проблеми

Сутність діяльності будь-якої організації, незалежно від видів діяльності, організаційно-правових форм, розмірів, полягає у використанні наявних інформаційно-комунікаційних технологій та інших активів для вирішення поставлених цілей та завдань. Ця діяльність пов'язана із значною часткою невизначеності та ризиками, оскільки всі її активи можуть піддаватися різного роду загрозам. Кожна загроза в свою чергу має джерело та відповідну ймовірність реалізації. Для реалізації загроз джерела загроз використовують уразливості активів.

Знизити ці ризики можна лише до певного залишкового рівня. На сьогодні не існує механізмів, що дозволяють повністю захистити організацію від загроз та ризиків, але ризики можна істотно знизити шляхом впровадження системи управління ризиками інформаційної безпеки (ІБ). На даному етапі управління ризиками стає не лише інструментом вибору засобів захисту, обґрунтування витрат на ІБ, а й інструментом прийняття оперативних рішень [1].

Аналіз, оцінка та управління ризиками ІБ – один із ключових чинників для впровадження

стійкої, надійної та ефективної системи забезпечення інформаційної безпеки (СЗІБ). Актуальність досліджень в одній з найскладніших та ключових областей у сфері ІБ – управлінні ризиками інформаційної безпеки, пояснюється тим, що технології та методології дослідження знаходяться в стадії розвитку та не мають закінчених і готових рішень (дієздатних моделей), які б достатньо точно описували процеси аналізу та управління ризиками ІБ.

Аналіз останніх досліджень і публікацій

Одним із шляхів вирішення проблеми оцінки ризиків та вибору оптимального варіанта їх обробки є моделювання. Призначенням моделювання процесів управління ризиками інформаційної безпеки є отримання необхідної інформації для проведення аналізу на доказовій основі з метою прийняття обґрунтованих рішень стосовно того, яким чином краще забезпечувати захист активів організації від певних загроз інформаційної безпеки.

На сьогодні методики оцінювання ризиків ІБ можна умовно поділити на стандартизовані та наукові. У перших, як правило, застосовується якісний підхід з використанням різного роду таблиць зі шкалами значень ризику. Найбільш популярними та найчастіше використовуваними на практиці є методики наведені у стандартах ISO/IEC 27005:2011 [2], NIST SP800-30 [3], OCTAVE [4] та EBIOS [5]. У наукових методиках здійснюється спроба реалізації кількісного аналізу шляхом використання різноманітного математичного апарату, а саме: теорії імовірностей, теорії нечіткої логіки, імовірнісних методів, мереж Петрі, нейронних мереж тощо. Однак перші не дозволяють отримати точні результати, а другі є занадто складними для практичного застосування. Окремі аспекти аналізу та управління ризиками досліджувались у роботах О.Г. Корченко [6], В.Г. Криволапова [7], Д.О. Котенко [8], Є.Г. Новицького [9], Пітера Стефенсона [10]. Зазначимо, що у міжнародному стандарті ISO/IEC 31010 [11] наведено понад 30 підходів до аналізу та оцінки ризиків. Отже, розроблювані у цій роботі моделі, мають:

– відобразити складну структуру інформаційно-комунікаційних систем та мереж, які функціонують в організаціях, та вміти легко пристосовуватись до динамічних змін у їх структурі;

– надавати відомості, необхідні для прийняття управляючих рішень, за обмеженої кількості відомостей про об’єкт;

– за короткий проміжок часу та в умовах дефіциту бюджету організації отримувати кількісні вихідні дані.

Мета роботи

Мета – здійснити спробу підвищити зручність, швидкість, точність та інформативність оцінки ризиків ІБ, спростити процес обрання варіанта обробки ризиків шляхом побудови моделей процесу управління ризиками інформаційної безпеки.

1. Моделі ідентифікації ризиків інформаційної безпеки

Задля уникнення термінологічної плутанини у даній роботі будуть використовуватися терміни, наведені у міжнародному стандарті ISO Guide 73:2009 [12], а загальний процес управління ризиками ідентичний тому, що наведений у ISO/IEC 27005:2011 [2].

Першим заходом, який слід виконати у процесі управління ризиками інформаційної безпеки, є дослідження середовища функціонування організації, в якій проводяться роботи з побудови СЗІБ. Під час проведення дослідження необхідно:

– ідентифікувати особливості провадження внутрішніх та зовнішніх ділових процесів організації, а також приблизний прибуток (вигоду) від них;

– сформувати перелік інформації, представленої в мовній, паперовій або електронній формі, що підтримує виконання ділових процесів, визначити вимоги щодо забезпечення цілісності, конфіденційності та доступності;

– описати середовище обробки інформації, а саме: приміщення, людей (персонал та клієнтів), використовуване апаратне та програмне забезпечення та зв’язки між ними;

– визначити наявну (потенційну) кількість конкурентів, зневірених клієнтів та звільнених з роботи співробітників, які задля отримання конкурентних переваг, помсти або висловлення невдоволення, можуть здійснювати найбільш небезпечні загрози, спрямовані на нанесення навмисної шкоди установі.

Спробуємо описати моделі, які на думку авторів, дозволяють описати середовище функціонування організації з достатньою точністю для подальшого проведення оцінки ризиків та обрання варіантів їх обробки.

Враховуючи сучасну структуру інформаційно-комунікаційних систем та мереж, для опису структури сучасного середовища обробки інформації у даній роботі пропонується використовувати багатошарові графи. Детальніше про багатошарові графи можна дізнатись у роботі Д.В. Агеєва [13], в якій запропоновано використовувати їх для моделювання багатошарових телекомунікаційних систем.

Продемонструємо адаптований варіант застосування багатошарових графів для графічної ідентифікації середовища обробки інформації під час побудови СЗІБ.

Для проведення графічної ідентифікації пропонується використовувати багатошаровий граф $MLG = (G, V, E)$, який включає у себе:

– множину підграфів $G = \{G^1, \ldots, G^l, \ldots, G^L\}$, $G^l = (V^l, E^l)$, де підграф G^l описує структуру середовища обробки інформації на рівні l;

– вершини $v_i \in V$ описують елементи середовища обробки та ребра $e_k = (v_i, v_j)$, $e_k \in E$ забезпечують зв'язок елементів середовища обробки між собою.

Для моделювання елементів середовища обробки інформації виділимо наступні сім підграфів (рис.1).

1) підграф G^1- вершини якого складають приміщення (кабінети), в яких ведеться обробка інформації, використовувані заходи та засоби захисту; ребра описують зв'язки між вершинами всередині підграфу G^1, а також зв'язки між вершинами підграфу G^1, які описують приміщення (кабінети) із засобами введення/виведення інформації, які представлені у вигляді вершин рівня G^2. У випадку необхідності у підграфі можуть бути продемонстровані зв'язки з кабінетами, які розташовані поруч з приміщенням, що підлягає захисту;

2) підграф G^2– вершини якого складають засоби введення/виведення інформації в/з комп'ютерної системи або мережі, паперові носії інформації (за необхідності), засоби та заходи захисту; ребра описують зв'язки між вершинами всередині підграфу G^2, а також зв'язки між вершинами підграфу G^2 та засобами оброблення, накопичення та передавання інформації підграфу G^3.

3) підграф G^3– вершини якого складають засоби оброблення, накопичення та передавання інформації, окрім відповідних ним засобів введення/виведення (комп'ютери, ноутбуки, сервери, маршрутизатори, комутатори та інше обладнання комп'ютерної системи або мережі), засоби та заходи захисту; ребра описують зв'язки між вершинами всередині підграфу G^3, а також зв'язки між вершинами підграфу G^3 та гіпервізорами підграфу G^4;

4) підграф G^4- вершини якого складають наявні в організації гіпервізори, засоби та заходи захисту; ребра описують зв'язки між вершинами всередині підграфу G^4, а також зв'язки між вершинами підграфу G^4 та операційними системами підграфу G^5. Цей рівень в деяких організаціях може бути відсутнім взагалі.

5) підграф G^5 – вершини якого складають операційні системи, засоби та заходи захисту, позначення виходу до мережі Інтернет; ребра описують зв'язки між вершинами всередині підграфу G^5, а також зв'язки між вершинами підграфу G^5 та прикладним програмним забезпеченням підграфу G^6;

6) підграф G^6 – вершини якого складають прикладне програмне забезпечення, бази даних, засоби та заходи захисту; ребра зв'язки між вершинами всередині підграфу G^6;

7) підграф G^7– вершини якого складають користувачі та заходи захисту; ребра зв'язки між вершинами всередині підграфу G^7, а також зв'язки між вершинами підграфу G^7 з усіма іншими підграфами.

Зазначене розбиття запропоновано із потреби захисту не лише відкритої інформації, а й інформації з обмеженим доступом, та з таких міркувань:

– у підграфі G^1 захист забезпечується заходами та засобами фізичної безпеки (замки, засоби охоронно-пожежної сигналізації, системи контролю та управління доступом тощо);

– у підграфах G^2, G^3 окрім засобів фізичної безпеки використовуються інженерно-технічні засоби (генератори шуму, розв'язувальні захисні трансформатори тощо);

– у підграфах G^4, G^5, G^6– захист забезпечують механізми комп'ютерної та мережевої безпеки, а у випадку виходу до мережі Інтернет – механізми Інтернет безпеки та безпеки кіберпростору,

– у підграфі G^7– організаційні заходи кожного із згаданих видів безпеки.

Зазначимо, що в деяких випадках кількість слоїв може бути збільшено або зменшено. Так, якщо установа не планує використовувати засоби захисту від витоку технічними каналами та

каналами спеціального впливу, підграфи G^2, G^3 можна поєднати.

На рис. 1 представлено фрагмент середовища обробки інформації, де: V_1^1 – кабінет №1, V_2^1 – охоронно-пожежна сигналізація, V_3^1 – приміщення поза межами організації, V_1^2 – комплект №1 (клавіатура, маніпулятор, монітор та мережевий адаптер), V_2^2 – фізичний вихід за межі контрольованої зони (вихід до мережі Інтернет), V_1^3 – сервер, V_1^4 – гіпервізор, V_1^5 – серверна операційна система, V_2^5 – клієнтська операційна система, V_3^5 – вихід до мережі Інтернет, V_1^6 – система наповнення контенту, V_2^6 – веб-сервер, V_3^6 – система управління базами даних, V_4^6 – налаштовані механізми безпеки веб-серверу, V_5^6 – веб-браузер, V_1^7 – системний адміністратор, V_2^7 – користувач-редактор.

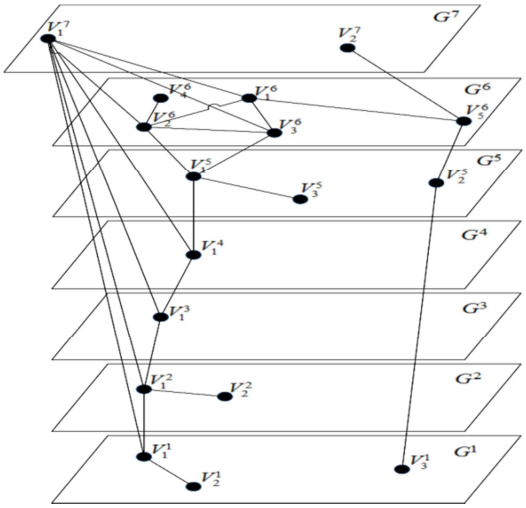

Рис. 1. Фрагмент ідентифікованого середовища обробки інформації

Показаний на рис.1 багатошаровий граф дозволяє ідентифікувати елементи середовища обробки інформації та зв'язки між ними (без відображення конкретної інформації, яка обробляється ними).

Для графічного відображення інформації, обробка якої здійснюється елементами середовища обробки інформації, поверх даного багатошарового графу побудуємо гіперграф H (рис. 2), для описання якого введемо таке: нехай – кінцева непуста множина; N – певна родина підмножин множини W. Пара (W, N) називається гіперграфом $H = (W, N)$ з множиною вершин $W = \{w\}$ та множиною ребер $N = \{n\}$, які описують ідентифіковану інформацію підтримки ділових процесів. Множину вершин W складають всі вершини багатошарового графу MLG, тобто всі елементи середовища обробки інформації. Зазначений гіперграф однозначно задається матрицею інцидентності A, елементи якої визначаються за таким правилом:

$$a_{i,j} = \begin{cases} 1, якщо H(w_i, n_j) = істина \\ 0, якщо H(w_i, n_j) = неправда \end{cases}.$$

Використання гіперграфів, детально описаних у роботі Г.Г. Омельченко [14], на етапі ідентифікації ризиків необхідне для встановлення взаємозв'язків між інформацією та елементами середовища обробки, оскільки один актив може обробляти, зберігати або передавати декілька типів інформації.

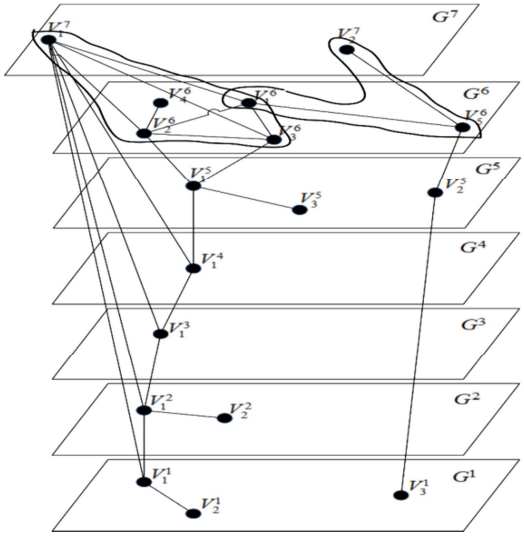

Рис. 2. Гіперграф ідентифікації активів організації

Виходячи з практичного досвіду, можна зазначити, що використання продемонстрованих багатошарових графів та гіперграфів дозволяє більш точно дослідити структуру об'єкта, на якому впроваджується СЗІБ. Однак у випадку, коли в моделі використовується значна кількість елементів, вона може стати громіздкою. У цьому випадку модель слід розбити на декілька частин залежно від функціональних доменів.

Після побудови гіперграфу поверх багатошарового графу та отримання чіткого уявлення про процес обробки кожного з видів інформації, необхідно сформувати множину комбінацій загроза/вразливість кожному з наведених елементів середовища обробки інформації.

У процесі аналізу математичних апаратів автори використали концепцію мережева єдиних мереж, яка ідеально підходить для опису поставленої задачі. Більш детально з концепцією можна ознайомитись в роботі [15].

Для спрощення відображення пропонується побудувати множину непорожніх стовбурів S, які складаються з множини непорожніх тематичних

шарів T, та до яких ребрами кріпиться множина комбінацій загроза/вразливість. S відображає окремі функціональні компоненти, T – складається із семи шарів, аналогічних мультиграфу елементів середовища обробки інформації. До кожного з цих шарів кріпиться множина наявних елементів середовища обробки комбінацій загроз/вразливостей R. У випадку, якщо імовірність реалізації комбінації загроза/вразливість залежить від реалізації іншої комбінації загроза/вразливість, будується гіпергpаф. На рис. 3 показана модель відображення загроз елементам середовища обробки інформації у вигляді стовбурів комбінацій загроза/вразливість.

2. Модель оцінки ризиків інформаційної безпеки

Продемонстровані вище графічні моделі дають змогу отримати чітке уявлення про активи організації та характерні їм загрози. В даній роботі використана класична формула оцінки ризиків R наведена у ISO/IEC 27005:2011 [2]:

$$R = T \cdot V \cdot A, \qquad (1)$$

де T – імовірність реалізації загрози;

V – величина вразливості активу;

A – цінність активу.

Спробуємо сформувати аналітичну модель оцінки ризиків, результати розрахунків якої у подальшому можуть бути використані під час побудови імітаційних моделей їх обробки.

В сучасних умовах в організаціях обробляються різні типи інформації, які під час побудови СЗІБ повинні бути чітко класифіковані. Для розрахунку ризиків за кожним видом інформації $P_{інф}$ пропонується скористатися формулою:

$$P_{інф} = I_{інф} \cdot Ч_{інфСер} \cdot (B_{інф} + B_{відн}), \qquad (2)$$

де $I_{інф}$ – імовірність реалізації хоча б однієї комбінації загроза/вразливість для певної інформації; $Ч_{інфСер}$ – середня частота реалізації певного виду загроз.

Збитки (зайві витрати) за кожним видом інформації $B_{інф}$ розраховуються за формулою:

$$B_{інф} = B_K + B_Д + B_Ю + B_P, \qquad (3)$$

де B_K – збитки від порушення конфіденційності (наслідки від появи нових конкурентів, спричинені ознайомленням з інформацією з обмеженим доступом, як результат, виникає потреба знизити ціну), оцінюються переважно керівництвом сумісно з фахівцями, які здійснюють виконання ділового процесу; $B_Д$ – збитки від порушення доступності (наслідки в результаті простоїв у роботі організації, спричинених дією загрози), оцінюються переважно керівництвом сумісно з фахівцями, які здійснюють виконання ділового процесу; $B_Ю$ – витрати на відшкодування юридичних та договірних зобов'язань, оцінюються переважно юристом сумісно з бухгалтерією; B_P – збитки репутації (відтік існуючих клієнтів внаслідок недовіри тощо), оцінюються керівництвом сумісно з керівниками всіх рівнів.

В даних розрахунках не використовуються збитки від порушення цілісності, оскільки від них переважно наносяться збитки, пов'язані з юридичними відшкодуваннями.

Середні збитки, спричинені відновленням одного елементу середовища обробки інформації, розраховуються за формулою:

$$B_{відн} = \frac{\sum_{j=1}^{n} Г^j \cdot ЗП^j + B^j_{відн.елем.}}{n}, \qquad (4)$$

де $Г$ – кількість годин необхідних на відновлення одного процесу інформаційної діяльності; $ЗП$ – середня заробітна платня фахівців (або вартість послуг сторонньої організації), залученої до виконання робіт з відновлення процесу інформаційної діяльності, оцінюється у випадку потреби оплати даних робіт; $B_{відн.елем.}$ – витрати на відновлення кожного з елементів середовища, яке забезпечує підтримку процесів інформаційної діяльності, оцінюються системними та/або мережевими адміністраторами, інженерами та іншими фахівцями сумісно з бухгалтерією.

Імовірність реалізації хоча б однієї комбінації загроза/вразливість для певної інформації розраховуються за формулою:

$$I_{інф} = 1 - \prod_{j=1}^{n} (1 - I_a^j), \qquad (5)$$

де імовірність реалізації хоча б однієї комбінації загроза/вразливість активу розраховується за формулою:

$$I_a^j = 1 - \prod_{t=1}^{n} (1 - I^t_{зва}). \qquad (6)$$

Схильність функціонального компоненту до реалізації однієї загрози пропонується розраховувати за формулою:

$$I^t_{зва} = \frac{\sum_{i=1}^{N} K_i^t \cdot B^t}{25 \cdot N}, \qquad (7)$$

де K_i^t – коефіцієнти, які описують загрозу; B^t – потенційна шкода внаслідок впливу на інформацію; N – кількість показників.

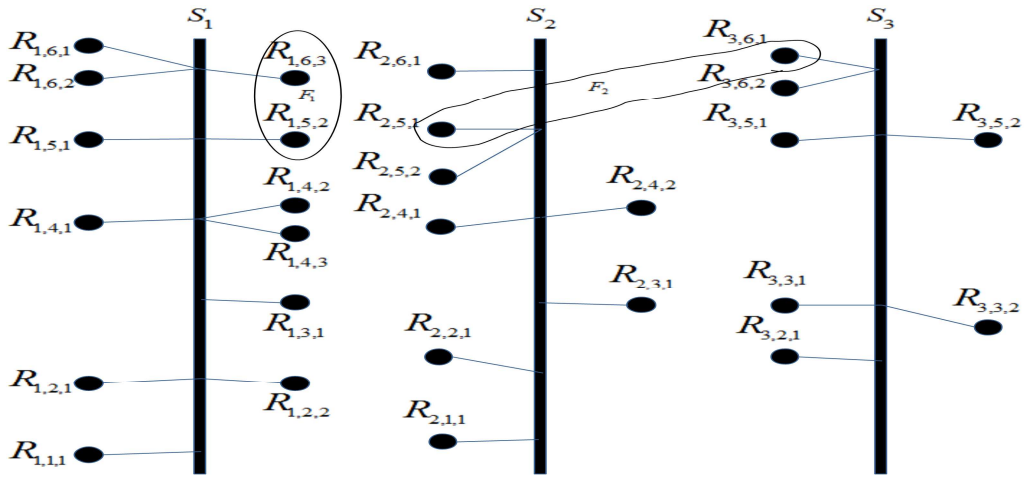

Рис. 3. Стовбури комбінацій загроза/вразливість

Наприклад, коефіцієнти поширення загрози, вмотивованості порушника тощо. Коефіцієнти та потенційна шкода приймають значення від 1 до 5.

3. Модель обробки ризиків інформаційної безпеки

Як зазначалося, на сьогодн доволі складно побудувати аналітичну модель оцінки та обробки ризиків інформаційної безпеки, яка б давала результат з достатньою точністю. Принципово іншим підходом до аналізу є імітаційне моделювання, однією із форм представлення якого є мережі Петрі.

Продемонструємо використання розфарбованих мереж Петрі, модельованих у системі CPN Tools для побудови моделі обробки ризиків інформаційної безпеки.

Модель побудовано з таких міркувань. В організаціях, внаслідок реалізації загроз безпеки, регулярно трапляються інциденти, в результаті яких наноситься шкода організації. Задля уникнення подібних інцидентів на підставі результатів оцінки ризиків організація приймає рішення, виходячи з одного з трьох варіантів: зменшення ризиків, утримання ризиків або ухилення від ризиків. У випадку обрання варіанта зменшення ризиків використовуються певні засоби захисту.

Розфарбовані мережі Петрі у моделювальній системі CPN Tools являють собою комбінацію графа мережі Петрі та мови програмування CPN ML, використовуваної для опису атрибутів елементів. Фішка розфарбованої мережі Петрі являє собою елемент абстрактного типу даних, який зазвичай називається кольором [16].

Представлена мережа Петрі (рис. 4) складається із 8 позицій та 3 переходів. Значення у позиції *A one time loss* сигналізує про кількість потенційних порушників та єдиноразові збитки від дій порушника, значення у позиції *Total loss* – загальні збитки до вжиття заходів захисту, наявність фішки у позиції *Incident detect* свідчить про факт, що інцидент виявлено через проміжок часу *IRstartTime*, фішка в позиції *Countermeasure* сигналізує про наявність заходу захисту проти загрози. Перехід *Incident response* використовується для демонстрації, що вживаються заходи для подолання інциденту, перехід *Calculatoin of losses* використовується для розрахунку загальних збитків, перехід *Risk treatment* використовується для обрання варіанта оброблення ризику.

У моделі використано три основних типи фішок: стандартний тип *REAL*, який описує рівень збитків від реалізації загроз; тип *SM*, який описує засоби захисту (а саме їх вартість та відсоток незахищеності, який залишиться після його впровадження); тип *E*, який в даній моделі використовується формально для демонстрації можливості факту виявлення інциденту безпеки.

Функція *RAvoidance* використовується для перевірки відповідності вимозі ухилення від ризиків, *RRetention* – утримання ризиків, *RReduction* – зниження ризиків.

Оголошення *IRstartTime*, яке визначає час від моменту настання інциденту до його розв'язання, тобто вживання заходів та/або засобів захисту, *RACriteria* – критерій прийняття ризиків, *Profit* – прибуток установи за певним процесом або в цілому.

Зміна *loss* описує збитки в результаті єдиноразової реалізації загрози, *lossT* – загальні збитки, які буде нанесено організації до моменту вжиття заходів захисту, *priceCM* – вартість засобів захисту інформації, *efectCM* – небезпека, яка залишиться після використання даного механізму.

У початковому стані у позиції Total loss повинна бути встановлена фішка зі значенням 1`0.0.

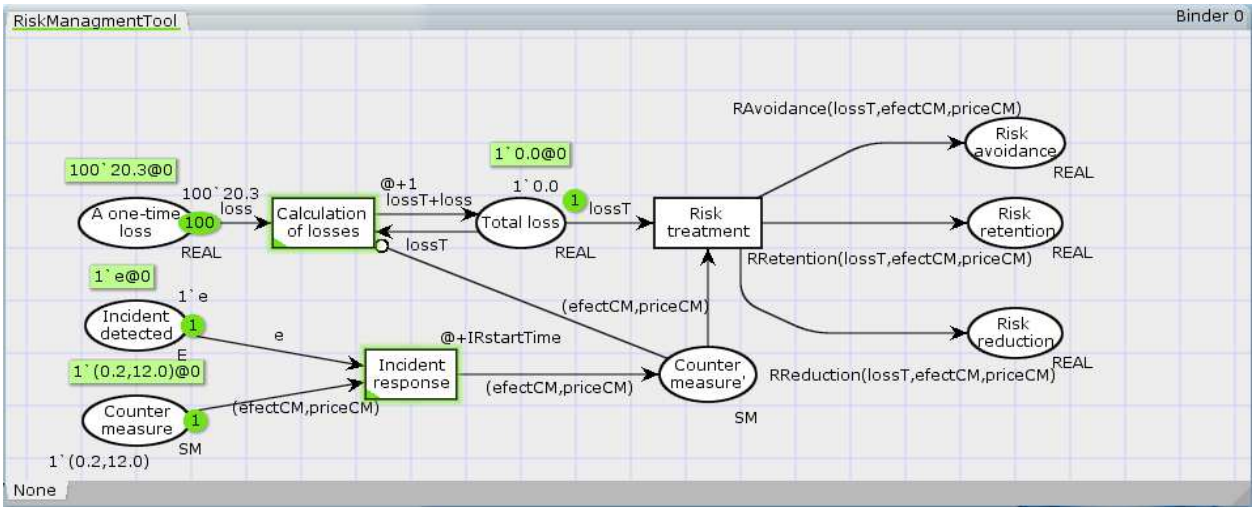

Рис. 4. Модель обробки ризиків інформаційної безпеки

Далі наведено лістинг команд, які необхідно реалізувати для функціонування цієї моделі:

colset REAL = real timed;

colset E= with e timed;

*colset SM=product REAL*REAL timed;*

var loss,lossT,priceCM,efectCM: REAL;

val Profit=90.0;

val RACriteria = 0.85;

val IRstartTime=9;

*fun RRetention(lossT,efectCM,priceCM)=if (lossT/Profit<=RACriteria) andalso ((lossT/Profit)<(lossT*efectCM+priceCM)/Profit) then 1`lossT else empty;*

*fun RReduction(lossT,efectCM,priceCM)=if ((lossT*efectCM+priceCM)/Profit<=RACriteria) andalso*

*((lossT/Profit)>=(lossT*efectCM+priceCM)/Profit) then 1`(lossT*efectCM+priceCM) else empty*

*fun RAvoidance(lossT,efectCM,priceCM)=if ((lossT*efectCM+priceCM)/Profit)>RACriteria*

andalso (lossT/Profit>RACriteria) then 1`lossT else empty

У таблиці наведено витяг із результатів моделювання за допомогою даної моделі обробки ризиків інформаційної безпеки.

Наведена на рис. 4 модель дає змогу організації оцінити збитки, які можуть настати через певний проміжок часу, перевірити чи задовольнятимуть вони критерію прийняття ризиків через певний обраний проміжок часу, дозволяє визначити, який варіант обробки ризиків слід обрати залежно від обраного проміжку часу.

4. Модель виявлення уразливостей в процесі експлуатації системи

У п. 1 – 3 описано, яким чином можна ідентифікувати ризики інформаційної безпеки, провести їх оцінку та обрати оптимальний варіант їх обробки. Оскільки незалежно від того наскільки якісно створена СЗІБ, в ній все одно будуть залишатись недоліки та прорахунки, які виникли в процесі проектування, розроблення або впровадження СЗІБ. Зазначимо, більшість з проблем на практиці виявляється під час експлуатації СЗІБ.

Наведемо використання ділових ігор, як методу пошуку та усунення вразливостей, що виникають під час функціонування (експлуатації) системи забезпечення інформаційної безпеки. Детальніше про використання ділових ігор в питаннях захисту інформації можна прочитати в роботі [17].

Основою пропонованої гри є метод «мозкового штурму», який є ефективним для розв'язання подібних задач. Процес проведення ділової гри складається з підготовчого та основного етапів.

Таблиця

Витяг із результатів моделювання варіантів обробки ризиків

Досліджуваний проміжок часу, умовних інтервалів часу	Єдиноразові збитки, тис. грн.	Очікуваний прибуток, тис. грн.	Коефіцієнт небезпеки	Вартість заходів захисту, тис. грн.	Загальний збиток, тис. грн.	Результат обробки ризиків
2	20.3	87.5	0.2	12.1	20.22	Зниження
17	20.3	87.5	0.2	12.1	345.1	Ухилення
1	20.3	87.5	0.2	20.5	20.3	Утримання
2	20.3	87.5	0.2	20.5	28.62	Зниження

Передбачається, що особа відповідальна за захист інформації (або особа, яка є керівником гри) в достатньому обсязі володіє відомостями про процеси інформаційної діяльності організації, а також співробітники та клієнти, які перебувають на території організації, попереджені про те, що за ними ведеться спостереження (спеціалізованим програмним забезпеченням у комп'ютерній системі та засобами відеоспостереження поза її межами).

Підготовчий етап передбачає виконання таких заходів.

1. Ініціювання процесу ідентифікації вразливостей шляхом обрання особою, відповідальною за захист інформації (або особою, яка є керівником гри) найбільш важливого(их) інформаційного(их) процесу(ів) організації, які підлягатимуть аналізу.

2. Розроблення методики виявлення вразливостей та затвердження її керівництвом. Методика включає сценарій та регламент проведення гри, перелік учасників гри, обов'язки кожного з учасників та інструкції кожному з учасників. Учасниками гри переважно є співробітники організації, відповідальні за комп'ютерну, мережеву та фізичну безпеку. В окремих випадках можуть бути залучені фахівці з інших організацій.

Перш ніж перейти до основної частини гри, за k співробітниками організації, які забезпечують виконання обраного інформаційного процесу, ведеться спостереження, під час якого кожен з учасників бере участь у l ретельно сплановних інцидентах інформаційної безпеки. Наприклад, імітація атаки методами соціальної інженерії, впровадження хибних повідомлень тощо. З метою підвищення реалістичності, до них можуть залучатися клієнти організації. Під час кожного з інцидентів співробітник може виконати одну з трьох дій:

A – прийняти правильне рішення, описане в інструкціях на систему інформаційної безпеки;

B – прийняти помилково неправильне рішення (наприклад, недостатнє навчання або неточність у інструкції);

C – виконати навмисно заборонену дію. Ці дії повинні виявити учасники на кроках 2 та 3 основного етапу гри.

3. Встановлення засобів спостереження в місцях, де відбуваються аналізовані процеси інформаційної діяльності та накопичення відомостей шляхом проведення спостереження.

Основний етап передбачає таке.

4. Доведення до учасників мети та правил гри.

5. Переглядання учасниками записів системи спостереження та формування кожним із них переліку виявлених недоліків. Примітка: учасники спостерігають не лише за правильністю дій співробітників у обраних інцидентах, а й взагалі.

6. Спілкування учасників гри зі співробітниками організації щодо виявлених неправильних або не ідентифікованих раніше небезпечних дій, з метою виявлення їх причин (клас B та C). У разі необхідності гравцями проводиться аналіз документації та налаштувань програмно-апаратних засобів.

7. Обмін інформацією між учасниками за методом «мозкового штурму» та накопичення відомостей.

8. Формування остаточного переліку вразливостей та рекомендацій щодо їх усунення, визначення небезпечності дій кожного зі співробітників (формули (8) – (11)), а також визначення критерію надійності персоналу у забезпеченні інформаційної безпеки

$$m_i^A = \frac{N_i^A}{N_i^\Sigma}, \qquad (8)$$

де m_i^A – імовірність правильного прийняття рішення i-м співробітником за l інцидентів; N_i^A – кількість правильних дій; N_i^Σ – загальна кількість інцидентів розраховується за формулою (11):

$$m_i^B = \frac{N_i^B}{N_i^\Sigma}, \qquad (9)$$

де m_i^B – імовірність прийняття ненавмисних неправильних дій; N_i^B – кількість ненавмисних неправильних дій.

$$m_i^C = \frac{N_i^C}{N_i^\Sigma}, \qquad (10)$$

де m_i^C – імовірність навмисних неправильних дій; N_i^C – кількість навмисних неправильних дій.

$$N_i^\Sigma = N_i^A + N_i^B + N_i^C. \qquad (11)$$

На основі формул (8) – (11) можна сформувати критерій ненадійності персоналу $K_{над.перс.}$, який приймає значення від 0 до 1 (1-максимально ненадійний персонал)

$$K_{над.перс.} = 1 - \frac{\sum\limits_k N_i^A}{\sum\limits_k N_i^\Sigma}. \qquad (12)$$

Ділові ігри в порівняні з іншими методами пошуку вразливостей дозволяють: виявляти недоліки системи забезпечення інформаційної безпеки, пов'язані з використанням засобів захисту інформації та виконанням заходів захисту (експлуатаційні недоліки); віднаходити елементи

середовища обробки інформації, які потребують детального аналізу причин виникнення небезпеки (можливо упущених іншими методами виявлення). Зазначений метод слід використовувати, як доповнення до інших методів пошуку вразливостей.

Як висновок, можна зазначити, що використання ділових ігор в сукупності з іншими методами пошуку вразливостей дозволить підвищити точність та якість їх ідентифікації.

5. Інкрементна модель побудови системи забезпечення інформаційної безпеки

За допомогою описаних вище моделей можливо скласти звіт про аналіз ризиків інформаційної безпеки, який міститиме відомості про перелік необхідних засобів та заходів із зазначенням пріоритетів їх впровадження. Ці відомості виступають в якості вхідних вимог до побудови (або модернізації) системи забезпечення інформаційної безпеки. Залишається лише обрати підхід до побудови системи забезпечення інформаційної безпеки.

На думку авторів, для побудови СЗІБ необхідно використовувати інкрементну модель, яка являє собою процес часткової реалізації зазначених у звіті засобів та заходів захисту, та поступового нарощення функціональних можливостей [18]. Зазначений підхід дозволить розділити загальні витрати, необхідні на побудову СЗІБ на декілька частин та прискорити процес створення системи (особливо під час модернізації, оскільки нові модулі впроваджуються частинами залежно від пріоритетів).

Зазначений підхід реалізується шляхом компонування стандартних блоків (рис. 5), завдяки яким забезпечується контроль над створенням СЗІБ. Такий підхід може бути використаний будь-якою організацією незалежно від форми власності та масштабів.

Інкрементна модель побудови системи інформаційної безпеки починається зі встановлення переліку вимог, які беруться зі звіту про аналіз ризиків, та розробки послідовності конструкцій.

Конструкції включають виконання таких заходів: укладення у разі необхідності договору з виконавцем робіт, які покладено на дану конструкцію (на схемі не відображено); розроблення технічного проекту, в якому обраним виконавцем зазначаються конкретні дії, які слід виконати; впровадження засобів та заходів захисту; експертиза засобів та заходів захисту, яка полягає перш за все в активній перевірці, якості та повноти впроваджених механізмів безпеки; введення в експлуатацію реалізованих механізмів. Формування конструкцій здійснюється залежно від зазначених у звіті пріоритетів. Причому першу конструкцію складають заходи та засоби захисту, які мають найвищий пріоритет. Примітка: паралельно можна впроваджувати заходи, описані в декількох конструкціях.

Основними перевагами використання інкрементної моделі для побудови системи інформаційної безпеки є:

– відсутність потреби заздалегідь виділяти кошти на побудову всієї системи інформаційної безпеки, оскільки спочатку створюється захист від найбільш небезпечних загроз;

– зникає потреба у формуванні громіздких технічних рішень, які майже ніколи неможливо повністю виконати;

– ризик помилкового обрання в ході аналізу заходів та засобів захисту розподіляється на декілька інкрементів;

– замовник має можливість після кожної ітерації висловити свої зауваження та скоригувати процес побудови;

Рис. 5. Процеси побудови та модернізації системи забезпечення інформаційної безпеки

– система безпеки стає більш надійною, оскільки відбувається експертиза невеликих за розміром складових;

– знижується імовірність компрометації системи, оскільки кожен виконавець володіє обмеженою кількістю відомостей про об'єкт, на якому виконуються роботи.

Недоліки, характерні інкрементній моделі, викладені в роботі [19] є несуттєвими, оскільки процесу впровадження заходів та засобів захисту передує детальна оцінка ризиків.

Висновки та перспективи подальших досліджень

Практична значущість даного дослідження полягає в тому, що наведені моделі процесів управління ризиками ІБ дають можливість зручно, швидко та точно отримати цілісну картину ситуації відносно ризиків ІБ організації незалежно від її розмірів, приймати оптимальні управлінські рішення стосовно обробки ризиків. Представлені моделі у сукупності відтворюють процес управління ризиками ІБ, наведений у міжнародному стандарті ISO/IEC 27005:2011.

Запропоновані моделі дозволять отримувати науково-обґрунтовані організаційно-технічні рішення, впровадження яких сприятиме: підвищенню рівня ІБ організації та захисту її активів від множини зовнішніх та внутрішніх загроз, своєчасному виявленню вразливостей, зменшенню потенційних наслідків від реалізації загроз та зниженню ймовірності їх виникнення у майбутньому, мінімізації збитків, усуненню інцидентів та неприйнятних ризиків.

У перспективі подальших досліджень передбачається віднаходження шляху модернізації мережі Петрі таким чином, щоб вона могла самостійно (за мінімальної участі людей) приймати рішення стосовно обрання того чи іншого варіанта захисту із множини можливих.

Список літератури

1. *Динамическое управление состоянием безопасности [Електронний ресурс]. – Режим доступу: \www/ URL: www.arinteg.ru/about/publications/press /dinamicheskoe-upravlenie-sostoyaniem-bezopasnosti-131209.html. – Загол. з екрану.*
2. *ISO/IEC 27005:2011. Information technology - Security techniques - Information security risk management (second edition) [Текст]. – Введ. 2011-05-19. – Женева, 2011. – 68 с.*
3. *NIST Special Publication 800-30. Guide for Conducting Risk Assessments [Текст]. – Gaithersburg, 2012. – 95 с.*
4. *Richard A. Caralli Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process [Текст]:/ Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson. – Hanscom AFB, 2007. – 154 с.*
5. *EBIOS Méthode de gestion des risques [Текст]. – Париж, 2010. – 95 с.*
6. *Корченко А.Г. Методы анализа и оценки рисков потерь государственных информационных ресурсов [Електронний ресурс]:/ Корченко А.Г., Щербина В.П., Казмирчук С.В. – Режим доступу: \www/ URL: archive.nbuv.gov.ua/portal/natural/Zi/2012_1/20.pdf*
7. *Криволапов В.Г. Комплексная методика моделирования рисков информационной безопасности открытых систем [Текст]: автореф. дис. канд. техн. наук / Криволапов В.Г. – М., 2009. - 23 с.*
8. *Котенко Д.О. Метод оценки риска информационной безопасности на основе сценарного логико-вероятностного моделирования [Текст]: автореф. дис. ... канд. техн. наук / Котенко Д.О. – С.-Пб., 2010. – 16 с.*
9. *Новицкий Е.Г. Управление рисками нарушения информационной безопасности при стратегическом планировании: На примере крупной диверсифицированной информации [Текст]: дис. канд. техн. наук/ Новицкий Е.Г. – М., 1999. – 76 с.*
10. *Peter R., Stephenson A. Formal Model for Information Risk Analysis Using Colored Petri Nets [Електронний ресурс]. – Режим доступу: \www/ URL: http://www.researchgate.net/publication/228909435_A_formal_model_for_information_risk_analysis_using_colored_petri_nets.*
11. *IEC/ISO 31010:2009. Risk management – Risk assessment techniques [Текст]. – Женева, 2009. – 90 с.*
12. *ISO Guide 73:2009. Risk management – Vocabulary [Текст]. – Женева, 2009. – 15 с.*
13. *Агеев Д.В. Моделирование современных телекоммуникационных систем многослойными графами [Електронний ресурс]. – Режим доступу: \www/ URL: http://pt.journal.kh.ua/2010/1/1/101_ageyev_simulation.pdf.*
14. *Омельченко Г.Г. Гиперграфовые модели и методы решения дискретных задач управления в условиях неопределенности [Текст]: дис канд. фізико-математичних наук/ Омельченко Г.Г. – Черкесск, 2004. – 161 с.*
15. *Тихомиров А.А. Кружево единых сетей: Теоретические основы [Електронний ресурс]. – Режим доступу: \www/ URL: http://www.myshared.ru/slide/355663/*
16. *Зайцев Д.А. Исследование эффективности технологии MPLS с помощью раскрашенных сетей Петри [Електронний ресурс]/ Зайцев Д.А., Сакун А.Л. – Режим доступу: \www/ URL: http://teka.rulitru.ru/docs/2/1025/conv_1/file1.pdf.*
17. *Копитін Ю.В. Ділові ігри як метод підготовки фахівців з інформаційної безпеки [Електронний ресурс]/ Шиліна Н.Є, Копитін Ю.В. – Режим доступу: \www/ URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/4218.*
18. *ISO/IEC TR 15271-1:2010. Information technology - Guide for ISO/IEC 12207 (Software Life Cycle Processes) [Текст]. – Введ. 2010-10-01. – Женева, 2010. – 76 с.*
19. *Обзор моделей жизненного цикла разработки программного обеспечения [Електронний ресурс]. – Режим доступу: \www/ URL: http://www.itlab.unn.ru /MiniProjects/LCM/Conspect.doc.*

Стаття надійшла до редколегії 23.10.2013

Рецензент: д-р техн. наук, проф. А.А. Кобозєва, Одеський національний політехнічний університет, Одеса.