УДК 004.056.5

МЕТОДОЛОГІЯ АНАЛІЗУ РИЗИКІВ ДЕРЕВА ІДЕНТИФІКАТОРІВ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Сергій Бучик

У статті викладена методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів. Продемонстровано, що фактично місце аналізу ризиків інформаційної безпеки на державному рівні не визначено, що в свою чергу обумовлює актуальність проведення досліджень за вказаною тематикою. Окреслена методологія побудована на основі вперше запропонованих автором двох методів: методу визначення рівня ризику застосування певних контрзаходів щодо визначених ресурсів, яка реалізує раніше представлену автором методологію "подвійної трійки захисту"; методу кластеризації ризиків на основі транзитивного замикання бінарного відношення активів, яка дозволяє шляхом розбиття за відповідними α -рівнями отримати кластери державних інформаційних ресурсів, які згруповані за рівнями ризику. В результаті цього виникає можливість прослідити порядок об'єднання у кластери державних інформаційних ресурсів для подальшого їх аналізу, що може здійснюватись шляхом подальшого отримання оптимального α -рівня, нижче якого ризик є допустимим. Другий метод є логічним доповненням першого, причому при оцінюванні ризиків інформаційної безпеки достатньою умовою є використання лише першого методу.

Ключові слова: *державні інформаційні ресурси, ризик, ризик-менеджмент, рівень ризику, актив, загроза, уразливість, контрзахід, атака.*

Актуальність дослідження. Аналіз ризиків інформаційної безпеки (ІБ) є складовою та невід'ємною частиною системи менеджменту ІБ відповідно до стандарту ISO/IEC 27001 «Information technology – Security techniques – Information security management systems – Requirements». Аналіз, проведений автором показує, що на державному рівні в Україні не розроблено (впроваджено) даного стандарту. В Україні на практиці має місце підхід до обґрунтування вибору проекту підсистем інформаційної безпеки на базі нормативного документу технічного захисту інформації (НД ТЗІ) 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», які розроблені на базі «Канадських критеріїв безпеки комп'ютерних систем» та тісно пов'язаного з ним НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». Фактично місце аналізу ризиків ІБ на державному рівні не визначено, тому тематика, викладена в статті, є актуальною.

Аналіз останніх досліджень та публікацій. Автор у своїх працях вже звертався до тематики оцінювання ризиків ІБ. Так, у роботі [1] автором запропонована загальна модель формування системи захисту державних інформаційних ресурсів (ДІР) на основі раніше запропонованої методології "подвійної трійки захисту" [2], в якій система управління ІБ ДІР побудована за процесним підходом та з урахуванням основних етапів впровадження даної системи згідно зі стандартом ISO/IEC 27001, одним із елементів якої є модель оцінки ризиків. У [3] автором показано один із підходів та можливість його використання для оцінки факторів ризику (у даному випадку загроз) ІБ, у [4] автором запропоновано, показано та проаналізовано удосконалену методику оцінювання інформаційного ризику в автоматизованій системі. В роботі [5] здійснено спробу узагальнити всі основні моделі менеджменту інформаційної системи щодо безпеки ризиків. В роботі [6] здійснено спробу аналізу менеджменту ризику ІБ в телекомунікаційних мережах. В [7] розкриті алгебраїчні специфікації ризик-менеджменту безпеки мереж на основі побудови сигнатур ризиків, використання логіки предикатів та вейвлет перетворень. Є деяка кількість робіт, що присвячені аналізу ризиків у інформаційних системах у ближньому зарубіжжі. Так, у роботі [8] описано процес оцінки ризиків ІБ і розглянуто спосіб застосування когнітивно-орієнтованих моделей та схем виводу, таких як логічний висновок і семантичні мережі. В роботі [9] розкрито механізми управління ризиками ІБ відповідно до міжнародних стандартів ISO/IEC 27005 та BS 7799-3.

Мета статті. Метою статті є викладення методології аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів.

Виклад основного матеріалу. Виклад методології аналізу ризиків представляє собою сукупність запропонованих автором двох методів, при цьому вихідні дані першого методу є вхідними даними для другого:

I. Метод визначення рівня ризику застосування певних контрзаходів щодо визначених ресурсів;

II. Метод кластеризації ризиків на основі транзитивного замикання бінарного відношення активів.

І. Метод визначення рівня ризику застосування певних контрзаходів щодо визначених ресурсів (з урахуванням визначених атак та уразливостей ресурсів).

Визначимо для здійснення аналізу ризиків дерева ідентифікаторів ДІР наступні чотири складові:

– AS (assets) – активи, в ролі яких виступають ДІР;

– V (vulnerability) – уразливості ДІР;

– AT (attacks) – атаки на ДІР;

– D (decisions or counter-measures) – контрзаходи щодо зменшення впливу на ДІР атак через їх уразливості (засоби захисту, способи та методи захисту). Визначення даних складових лежить в рамках тієї теорії, що описана вище і не суперечить загальноприйнятим підходам до визначення складових ризику.

У відповідності до запропонованої авторами «методології подвійної трійки захисту» [2], представимо дані складові у вигляді наступних множин.

1. Множина активів ДІР

$$AS = \{AS_{nps}, AS_{ors}, AS_{its}\}, \quad (1)$$

де AS_{nps}, AS_{ors}, AS_{its} множина ДІР в яких їх захист направлений за відповідними спрямуваннями:

– нормативно-правовим (НорПС) – nps;

– організаційним (ОргС) – ors;

– інженерно-технічним (ІнжТС) – its;

1.1. Підмножини активів ДІР НорПС, ОргС, ІнжТС за властивостями інформації: к – конфіденційністю (**conf**identiality), ц – цілісністю (**int**egrity), д – доступністю (**av**ailability)

$$AS_{nps} = \{AS_{nps}^{conf}, AS_{nps}^{\text{int}}, AS_{nps}^{av}\}, \quad (2)$$

$$AS_{ors} = \{AS_{ors}^{conf}, AS_{ors}^{\text{int}}, AS_{ors}^{av}\}, \quad (3)$$

$$AS_{its} = \{AS_{its}^{conf}, AS_{its}^{\text{int}}, AS_{its}^{av}\}. \quad (4)$$

1.2. Підмножини активів ДІР НорПС за властивостями інформації (к, ц, д):

$$AS_{nps}^{conf} = \{as_{nps_1}^{conf}, as_{nps_2}^{conf}, ..., as_{nps_{confnps}}^{conf}\}, \quad (5)$$

$$AS_{nps}^{\text{int}} = \{as_{nps_1}^{\text{int}}, as_{nps_2}^{\text{int}}, ..., as_{nps_{\text{int}\,nps}}^{\text{int}}\}, \quad (6)$$

$$AS_{nps}^{av} = \{as_{nps_1}^{av}, as_{nps_2}^{av}, ..., as_{nps_{avnps}}^{av}\}, \quad (7)$$

де *confnps, intnps, avnps* – кількість ДІР НорПС за властивостями інформації (к ,ц, д).

Підмножини активів ДІР ОргС за властивостями інформації (к, ц, д):

$$AS_{ors}^{conf} = \{as_{ors_1}^{conf}, as_{ors_2}^{conf}, ..., as_{ors_{confors}}^{conf}\}, \quad (8)$$

$$AS_{ors}^{\text{int}} = \{as_{ors_1}^{\text{int}}, as_{ors_2}^{\text{int}}, ..., as_{ors_{\text{int}\,ors}}^{\text{int}}\}, \quad (9)$$

$$AS_{ors}^{av} = \{as_{ors_1}^{av}, as_{ors_2}^{av}, ..., as_{ors_{avors}}^{av}\}, \quad (10)$$

де *confors, intors, avors* – кількість ДІР ОргС за властивостями інформації (к, ц, д);

Підмножини активів ДІР ІнжТС за властивостями інформації (к,ц,д):

$$AS_{its}^{conf} = \{as_{its_1}^{conf}, as_{its_2}^{conf}, ..., as_{its_{confits}}^{conf}\}, \quad (11)$$

$$AS_{its}^{\text{int}} = \{as_{its_1}^{\text{int}}, as_{its_2}^{\text{int}}, ..., as_{its_{\text{int}\,its}}^{\text{int}}\}, \quad (12)$$

$$AS_{its}^{av} = \{as_{its_1}^{av}, as_{its_2}^{av}, ..., as_{its_{avits}}^{av}\}, \quad (13)$$

де *confits, intits, avits* – кількість ДІР ІнжТС за властивостями інформації (к, ц, д).

Дані множини можуть перетинатися, так як захист певного ресурсу може здійснюватись одночасно засобами НорПС, ОргС та ІнжТС за відповідними властивостями інформації (к, ц, д), яким повинен відповідати ресурс.

2. Множина уразливостей ДІР

$$V = \{V_{nps}, V_{ors}, V_{its}\}, \quad (14)$$

де $V_{nps}, V_{ors}, V_{its}$, – множина уразливостей ДІР НорПС, ОргС та ІнжТС, які реалізуються через загрози ДІР;

2.1. Підмножина уразливостей ДІР НорПС, ОргС, ІнжТС за властивостями інформації (к, ц, д)

$$V_{nps} = \{V_{nps}^{conf}, V_{nps}^{\text{int}}, V_{nps}^{av}\}, \quad (15)$$

$$V_{ors} = \{V_{ors}^{conf}, V_{ors}^{\text{int}}, V_{ors}^{av}\}, \quad (16)$$

$$V_{its} = \{V_{its}^{conf}, V_{its}^{\text{int}}, V_{its}^{av}\}. \quad (17)$$

2.2. Підмножини уразливостей ДІР НорПС за властивостями інформації (к, ц, д):

$$V_{nps}^{conf} = \{v_{nps_1}^{conf}, v_{nps_2}^{conf}, ..., v_{nps_{confnps}}^{conf}\}, \quad (18)$$

$$V_{nps}^{\text{int}} = \{v_{nps_1}^{\text{int}}, v_{nps_2}^{\text{int}}, ..., v_{nps_{\text{int}\,nps}}^{\text{int}}\}, \quad (19)$$

$$V_{nps}^{av} = \{v_{nps_1}^{av}, v_{nps_2}^{av}, ..., v_{nps_{avnps}}^{av}\}, \quad (20)$$

де *confnps, intnps, avnps* – кількість уразливостей НорПС за властивостями інформації (к, ц, д).

Підмножина уразливостей ОргС за властивостями інформації (к ,ц, д):

$$V_{ors}^{conf} = \{v_{ors_1}^{conf}, v_{ors_2}^{conf}, ..., v_{ors_{confors}}^{conf}\}, \quad (21)$$

$$V_{ors}^{\text{int}} = \{v_{ors_1}^{\text{int}}, v_{ors_2}^{\text{int}}, ..., v_{ors_{\text{int}\,ors}}^{\text{int}}\}, \quad (22)$$

$$V_{ors}^{av} = \{v_{ors_1}^{av}, v_{ors_2}^{av}, ..., v_{ors_{avors}}^{av}\}, \quad (23)$$

де *confors, intors, avors* – кількість уразливостей ОргС за властивостями інформації (к, ц, д).

Підмножина уразливостей ІнжТС за властивостями інформації (к ,ц, д):

$$V_{its}^{conf} = \{v_{its_1}^{conf}, v_{its_2}^{conf}, ..., v_{its_{confits}}^{conf}\}, \quad (24)$$

$$V_{its}^{\text{int}} = \{v_{its_1}^{\text{int}}, v_{its_2}^{\text{int}}, ..., v_{its_{\text{int}\,its}}^{\text{int}}\}, \quad (25)$$

$$V_{its}^{av} = \{v_{its_1}^{av}, v_{its_2}^{av}, ..., v_{its_{avits}}^{av}\}, \quad (26)$$

де *confits, intits, avits* – кількість уразливостей ІнжТС за властивостями інформації (к, ц, д).

3. Множина контрзаходів

$$D = \{D_{nps}, D_{ors}, D_{its}\}, \quad (27)$$

де $D_{nps}, D_{ors}, D_{its}$ – множина контрзаходів НорПС, ОргС та ІнжТС, направлених на захист відповідних ресурсів від уразливостей;

3.1. Підмножина контрзаходів НорПС, ОргС, ІнжТС за властивостями інформації (к,ц,д)

$$D_{nps} = \left\{D_{nps}^{conf}, D_{nps}^{\text{int}}, D_{nps}^{av}\right\}, \quad (28)$$

$$D_{ors} = \left\{D_{ors}^{conf}, D_{ors}^{\text{int}}, D_{ors}^{av}\right\}, \quad (29)$$

$$D_{its} = \left\{D_{its}^{conf}, D_{its}^{\text{int}}, D_{its}^{av}\right\}. \quad (30)$$

3.2. Підмножина контрзаходів НорПС за властивостями інформації (к,ц,д):

$$D_{nps}^{conf} = \left\{ d_{nps_1}^{conf}, d_{nps_2}^{conf}, ..., d_{nps_{confnps}}^{conf} \right\}, \quad (31)$$

$$D_{nps}^{\text{int}} = \left\{ d_{nps_1}^{\text{int}}, d_{nps_2}^{\text{int}}, ..., d_{nps_{\text{int}\, nps}}^{\text{int}} \right\}, \quad (32)$$

$$D_{nps}^{av} = \left\{ d_{nps_1}^{av}, d_{nps_2}^{av}, ..., d_{nps_{avnps}}^{av} \right\}, \quad (33)$$

де *confnps, intnps, avnps* – кількість контрзаходів НорПС за властивостями інформації (к,ц, д).

Підмножина контрзаходів ОргС за властивостями інформації (к ,ц, д):

$$D_{ors}^{conf} = \left\{d_{ors_1}^{conf}, d_{ors_2}^{conf}, ..., d_{ors_{confors}}^{conf} \right\}, \quad (34)$$

$$D_{ors}^{\text{int}} = \left\{d_{ors_1}^{\text{int}}, d_{ors_2}^{\text{int}}, ..., d_{ors_{\text{int}\, ors}}^{\text{int}} \right\}, \quad (35)$$

$$D_{ors}^{av} = \left\{d_{ors_1}^{av}, d_{ors_2}^{av}, ..., d_{ors_{avors}}^{av} \right\}; \quad (36)$$

де *confors, intors, avors* – кількість контрзаходів ОргС за властивостями інформації (к ,ц, д).

Підмножина контрзаходів ІнжТС за властивостями інформації (к ,ц, д):

$$D_{its}^{conf} = \left\{d_{its_1}^{conf}, d_{its_2}^{conf}, ..., d_{its_{confits}}^{conf} \right\}, \quad (37)$$

$$D_{its}^{\text{int}} = \left\{d_{its_1}^{\text{int}}, d_{its_2}^{\text{int}}, ..., d_{its_{\text{int}\, its}}^{\text{int}} \right\}, \quad (38)$$

$$D_{its}^{av} = \left\{d_{its_1}^{av}, d_{its_2}^{av}, ..., d_{its_{avits}}^{av} \right\}; \quad (39)$$

де *confits, intits, avits* – кількість контрзаходів ІнжТС за властивостями інформації (к ,ц, д).

4. Множина атак

$$AT = \sum_{z=1}^{N} \bigcup\nolimits_{k \in \{1,...,card(AT)\}} at_k(V_z), \quad (40)$$

де $card(AT)$ потужність множини атак, N – кількість спрямувань загроз ДІР (НорПС, ОргС, ІнжТС), $at_k(V_z)$ – функція залежності k - ої атаки від уразливості ДІР за z - им спрямуванням. Необхідність введення даної залежності полягає у тому, що за рахунок зміни коефіцієнтів матриці V_z ми можемо впливати на атаку.

Позначимо матрицю контрзаходів як C. Її розмір визначається як $card(D) \times card(AS)$, тобто

$$C^1 = \left\{\left(D^1, AS^1\right) : D^1 \text{ застосовується до } AS^1\right\}$$

або

$$C^0 = \left\{\left(D^0, AS^0\right) : D^0 \text{ не застосовується до } AS^0\right\},$$

кожний елемент приймає значення 0 або 1 згідно наступного правила:

$$\forall (i, j) \in \{1,..., card(D)\} \times \{1,..., card(AS)\}$$

$$\begin{cases} C_{ij} = 1, \text{ якщо рішення } d_i \text{ застосовується до ДІР } as_j, \\ C_{ij} = 0, \text{ якщо ні.} \end{cases} \quad (41)$$

Таким чином, спираючись на визначення матриці C та попередніх міркувань, задача аналізу ризиків дерева ідентифікаторів ДІР зводиметься до знаходження такої матриці C^*, яка б оптимально задовольняла використанню за вартістю засобів захисту від атак на ДІР, що демонструє наступний ідеалізований графік (рис. 1). Зрозуміло,що даний графік може бути представлений з урахуванням третьої складової $V = \{V_{nps}, V_{ors}, V_{its}\}$– уразливості ДІР.

В зв'язку з тим, що складовими визначення рівня ризику є ймовірність успіху кожної атаки проти ДІР та вплив на нього, що характеризує збиток, доцільно ввести ще дві матриці, які характеризуватимуть вплив (збиток) І та ймовірність П успіху атаки розміром $card(AT) \times card(AS)$. Аналогічно розглянемо дві матриці I_{I} та $\mathrm{I}_{\mathrm{П}}$, де $\mathrm{I}_{\mathrm{I}_{i,k}}$ (відносно $\mathrm{I}_{\mathrm{П}_{i,k}}$) відповідає впливу прийнятого рішення d_i на ймовірність атаки at_k, для кожного (i,k) в $card(D) \times card(AT)$. Для прикладу $\mathrm{I}_{\mathrm{I}_{3,4}} = 0.85$ означає, що якщо прийнято рішення d_3, то успіх атаки at_4 на державний інформаційний ресурс зменшується на 15% від вихідного впливу.

Для того, щоб виконати умови балансу між ефективністю встановлених контрзаходів (матриць, визначених вище) та їх вартістю, введемо матрицю Γ розміром $card(D) \times card(AS)$. Для кожного $(i, j) \in \{1,..., card(D)\} \times \{1,..., card(AS)\}$, Γ_{ij} визначає вартість реалізації рішення d_i по захисту державного інформаційного ресурсу r_j.

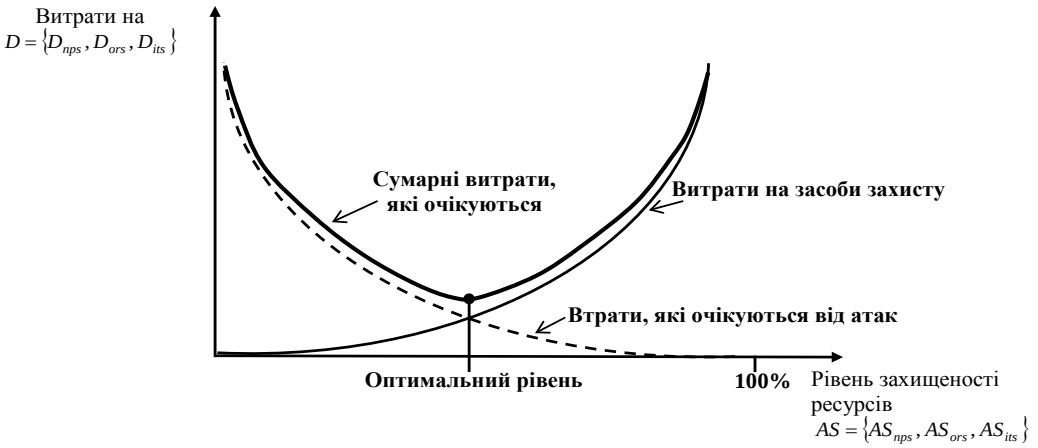

Рис. 1. Ідеалізований графік залежності витрат на захист від рівня захисту

Ці матриці необхідні для кількісної оцінки контрзаходів безпеки ДІР. За допомогою операторів $*$ та $\cdot$, які визначають поелементне та класичне множення, функції, які описують оптимізацію процесу аналізу ризику, можуть бути представлені наступним чином:

$$f_1(C) = \left\| \mathrm{I}_{\Pi} \cdot (\Pi * \mathrm{M}) \right\|, \quad (42)$$

$$f_2(C) = \left\| \mathrm{I}_{\mathrm{I}} \cdot (\mathrm{I} * \mathrm{M}) \right\|, \quad (43)$$

$$f_3(C) = \left\| C * \Gamma \right\|, \quad (44)$$

де $*$ – означає поелементне множення матриць;

$\| \ \|$ – норма $card(AT) \times card(AS)$.

Враховуючи множини (1,14,27) функції (42 - 44) представимо наступним чином:

$$f_1(C) = \left\| f_{1_{nps}}(C_{1_{nps}}) + f_{1_{ors}}(C_{1_{ors}}) + f_{1_{its}}(C_{1_{its}}) \right\|, \quad (45)$$

$$f_2(C) = \left\| f_{2_{nps}}(C_{2_{nps}}) + f_{2_{ors}}(C_{2_{nps}}) + f_{2_{its}}(C_{2_{nps}}) \right\|, \quad (46)$$

$$f_3(C) = \left\| f_{3_{nps}}(C_{3_{nps}}) + f_{3_{ors}}(C_{3_{ors}}) + f_{3_{its}}(C_{3_{its}}) \right\|. \quad (47)$$

З урахуванням підмножин (2-4) розкриємо складові функції (45):

$$f_{1_{nps}}(C_{1_{nps}}) = f_{1_{nps}}^{conf}(C_{1_{nps}}^{conf}) + f_{1_{nps}}^{\mathrm{int}}(C_{1_{nps}}^{\mathrm{int}}) + f_{1_{nps}}^{av}(C_{1_{nps}}^{av}), \quad (48)$$

$$f_{1_{ors}}(C_{1_{ors}}) = f_{1_{ors}}^{conf}(C_{1_{ors}}^{conf}) + f_{1_{ors}}^{\mathrm{int}}(C_{1_{ors}}^{\mathrm{int}}) + f_{1_{ors}}^{av}(C_{1_{ors}}^{av}), \quad (49)$$

$$f_{1_{its}}(C_{1_{its}}) = f_{1_{its}}^{conf}(C_{1_{its}}^{conf}) + f_{1_{its}}^{\mathrm{int}}(C_{1_{its}}^{\mathrm{int}}) + f_{1_{its}}^{av}(C_{1_{its}}^{av}). \quad (50)$$

З урахуванням підмножин (15-17) розкриємо складові функції (46):

$$f_{2_{nps}}(C_{2_{nps}}) = f_{2_{nps}}^{conf}(C_{2_{nps}}^{conf}) + f_{2_{nps}}^{\mathrm{int}}(C_{2_{nps}}^{\mathrm{int}}) + f_{2_{nps}}^{av}(C_{2_{nps}}^{av}), \quad (51)$$

$$f_{2_{ors}}(C_{2_{ors}}) = f_{2_{ors}}^{conf}(C_{2_{ors}}^{conf}) + f_{2_{ors}}^{\mathrm{int}}(C_{2_{ors}}^{\mathrm{int}}) + f_{2_{ors}}^{av}(C_{2_{ors}}^{av}), \quad (52)$$

$$f_{2_{its}}(C_{2_{its}}) = f_{2_{its}}^{conf}(C_{2_{its}}^{conf}) + f_{2_{its}}^{\mathrm{int}}(C_{2_{its}}^{\mathrm{int}}) + f_{2_{its}}^{av}(C_{2_{its}}^{av}). \quad (53)$$

З урахуванням підмножин (28-30) розкриємо складові функції (47):

$$f_{3_{nps}}(C_{3_{nps}}) = f_{3_{nps}}^{conf}(C_{3_{nps}}^{conf}) + f_{3_{nps}}^{\mathrm{int}}(C_{3_{nps}}^{\mathrm{int}}) + f_{3_{nps}}^{av}(C_{3_{nps}}^{av}), \quad (54)$$

$$f_{3_{ors}}(C_{3_{ors}}) = f_{3_{ors}}^{conf}(C_{3_{ors}}^{conf}) + f_{3_{ors}}^{\mathrm{int}}(C_{3_{ors}}^{\mathrm{int}}) + f_{3_{ors}}^{av}(C_{3_{ors}}^{av}), \quad (55)$$

$$f_{3_{its}}(C_{3_{its}}) = f_{3_{its}}^{conf}(C_{3_{its}}^{conf}) + f_{3_{its}}^{\mathrm{int}}(C_{3_{its}}^{\mathrm{int}}) + f_{3_{its}}^{av}(C_{3_{its}}^{av}). \quad (56)$$

З урахуванням підмножин (5-13) розкриємо складові функцій (48-50):

$$f_{1_{nps}}^{conf}(C_{1_{nps}}^{conf}) = \sum_{i=1}^{confnps} f_{1_{nps_i}}^{conf}(C_{1_{nps_i}}^{conf}), \quad (57)$$

$$f_{1_{nps}}^{\mathrm{int}}(C_{1_{nps}}^{\mathrm{int}}) = \sum_{j=1}^{\mathrm{int}\, nps} f_{1_{nps_j}}^{\mathrm{int}}(C_{1_{nps_j}}^{\mathrm{int}}), \quad (58)$$

$$f_{1_{nps}}^{av}(C_{1_{nps}}^{av}) = \sum_{n=1}^{avnps} f_{1_{nps_n}}^{av}(C_{1_{nps_n}}^{av}), \quad (59)$$

$$f_{1_{ors}}^{conf}(C_{1_{ors}}^{conf}) = \sum_{i=1}^{confors} f_{1_{ors_i}}^{conf}(C_{1_{ors_i}}^{conf}), \quad (60)$$

$$f_{1_{ors}}^{\mathrm{int}}(C_{1_{ors}}^{\mathrm{int}}) = \sum_{j=1}^{\mathrm{int}\, ors} f_{1_{ors_j}}^{\mathrm{int}}(C_{1_{ors_j}}^{\mathrm{int}}), \quad (61)$$

$$f_{1_{ors}}^{av}(C_{1_{ors}}^{av}) = \sum_{n=1}^{avors} f_{1_{ors_n}}^{av}(C_{1_{ors_n}}^{av}), \quad (62)$$

$$f_{1_{its}}^{conf}(C_{1_{its}}^{conf}) = \sum_{i=1}^{confits} f_{1_{its_i}}^{conf}(C_{1_{its_i}}^{conf}), \quad (63)$$

$$f_{1_{its}}^{\text{int}}(C_{1_{its}}^{\text{int}}) = \sum_{j=1}^{\text{int}\,its} f_{1_{its_j}}^{\text{int}}(C_{1_{its_j}}^{\text{int}}), \quad (64)$$

$$f_{1_{its}}^{av}(C_{1_{its}}^{av}) = \sum_{n=1}^{avits} f_{1_{its_n}}^{av}(C_{1_{its_n}}^{av}). \quad (65)$$

З урахуванням підмножин (18-26), (31-39) складові функцій (51-53), (54-56) розкриваються аналогічним чином як і (57-65).

Припущення. Якщо атака at_k направлена на уразливість v_l та дана уразливість присутня в активі as_j, то атака at_k може бути здійснена проти активу as_j.

Звідси, як висновок можна визначити матрицю $\mathbf{M}$, яка буде визначати ступінь впливу атаки $at_k(v_l)$ на актив as_j.

Матриця $\mathbf{M}$ гарантує, що лише можлива атака приймається до уваги при оцінці ефективності встановлених контрзаходів. Фактично, якщо рішення не дає реалізувати атаку, вона не має позитивного впливу на систему, якщо відсутній актив, проти якого направлена атака.

Матриця $\mathbf{M}$ може бути представлена як добуток двох матриць $\mathbf{E}$ (розміром $(card(AT)\times card(V))$ та $\mathbf{P}$ (розміром $(card(V)\times card(AS))$, що приймають значення від 0 до 1 за наступними правилами:

$$\forall (k,l) \in \{1,...,card(AT)\}\times\{1,...,card(V)\}$$

$$\begin{cases} \mathrm{E}_{kl} \to 1 \text{ якщо атака } a_k \text{ направлена на уразливість } v_l \\ \mathrm{E}_{kl} \to 0 \text{ якщо ні.} \end{cases}$$

$$\forall (k,j) \in \{1,...,card(V)\}\times\{1,...,card(AS)\}$$

$$\begin{cases} \mathrm{P}_{lj} \to 1 \text{ якшо уразливість } v_l \text{ присутня в активі } r_j \\ \mathrm{P}_{lj} \to 0 \text{ якщо ні.} \end{cases}$$

$\mathbf{E}$ може бути побудована з використанням загальновідомих баз даних атак. $\mathbf{P}$ можна заповнити, якщо використати різні механізми виявлення уразливостей в активах та відповідно до ДІР з використанням класифікатора загроз [2].

На відміну від [7], де функції (42-44) використовуються з оператором $\boxtimes c$, даний оператор у вказаному випадку не використовуємо, у зв'язку з тим, що при подальшому розгляді його змісту використовуються матриці $\mathbf{M}_1$ та $\mathbf{M}_2$, місце яких в даній роботі (див.[7]) не визначено та втрачає сенс.

Матриці, які утворюються у вигляді функцій $f_1(C)$, $f_2(C)$, $f_3(C)$, мають розмір $card(D)\times card(AS)$.

У наведеному вище аналізі ми припустили, що основні компоненти, набори та матриці відомі. На практиці збір цих даних потребує спеціальних процедур та обладнання.

Підмножина AS складається із описаних активів та може бути визначена шляхом відвідування сайтів або сервісів.

Підмножина V є уразливостями бібліотек, які можуть бути побудовані з використанням захищених баз даних з відомими уразливостями. Також може використовуватися експерт для виявлення уразливостей, які пов'язані з людським фактором.

Підмножину атак AT отримуємо із системи виявлення вторгнень. Більш того, атаки представляють собою дерева атак, які вперше введені Б. Шнайером в [10]. Наше завдання полягає у тому, щоб визначити та оцінити можливі наслідки подій, які виникнуть у разі появи основних атак.

Атаку, яка може бути направлена на ресурс, оцінюють за допомогою механізмів аналізу ризиків. Це завдання є найскладнішим, у зв'язку з тим, що різні види потенційних впливів пов'язуватимуться з розміром збитку в грошовому еквіваленті.

Однією із найбільш важливих задач є визначення ймовірності атаки, оскільки це впливатиме на якість проведеного аналізу ризику.

Також оцінка успішності прийнятих контрзаходів проти атак, що регламентуються матрицями $\mathbf{I}_\mathbf{I}$ та $\mathbf{I}_\mathbf{\Pi}$, залежатиме від людського фактора (втручання людини).

Ці три останніх положення демонструють, що такі процеси можуть бути автоматизовані достатньо легко, при цьому людський фактор залишається основною складовою циклу управління ризиками.

Функції f_1 та f_2 дозволяють оцінити ефективність матриці C, а в f_3 приведена вартість рішень. Так як, відповідно до [6], перед авторами

стоїть задача розподілу визначених способів та методів захисту ресурсів від атак, для оптимального розподілу можна скористатися методами теорії лінійного програмування. Для цього кожний елемент матриці C прийматиме значення від 0 до 1 згідно наступного правила:

$$\forall (i,\ j) \in \{1,...,card(D)\} \times \{1,...,card(AS)\}$$

$$\begin{cases} C_{ij} \to 1, \text{ якщо рішення } d_i \text{ найкращим чином може бути застосовано до ДІР } as_j, \\ C_{ij} \to 0, \text{ якщо ні.} \end{cases}$$

Таким чином, завдання полягатиме у визначенні оптимальних значень матриці C_{ij}^* з урахуванням функцій (42-44).

На практиці стоїть завдання мінімізації цих функцій:

$$\begin{cases} f_1(C) \to \min \\ f_2(C) \to \min \\ f_3(C) \to \min \end{cases}.$$

Для отримання оптимального розв'язання задачі аналізу ризику інформаційної безпеки, скористаємось мультиплікативний критерієм [11].

Мультиплікативний критерій оптимальності реалізує принцип справедливої відносної поступки і полягає у наступному: справедливим слід вважати такий компроміс, коли відносне зниження одного критерію не перевищує відносного (не прив'язаного до величини першого критерію) перевищення іншого критерію.

Математично мультиплікативний критерій базується на перемножуванні часткових критеріїв оптимальності.

Функціонал, що забезпечує формування оптимального розв'язку за мультиплікативним критерієм якості має вигляд

$$f^*(C) = \prod_{m=1}^{n} f_m(C) \Rightarrow_{\min}^{\max}, \qquad (66)$$

де $f^*(C)$ – оптимальне значення параметра, який оптимізується; $f_m(C)$ – приватні критерії якості; $m = \overline{1,n}$ – параметр, який характеризує кількість часткових функцій якості.

Таким чином, з урахуванням функцій (42-44) та (66)

$f^*(C) = \left\| \mathrm{I}_{\Pi} \cdot (\Pi * \mathrm{M}) \right\| \cdot \left\| \mathrm{I}_{\mathrm{I}} \cdot (\mathrm{I} * \mathrm{M}) \right\| \cdot \left\| C * \Gamma \right\| = C \cdot f_{opt}$,

де $f_{opt} = f_1(C) \cdot f_2(C) \cdot \Gamma$.

Після чого ми отримуємо узагальнену оптимальну матрицю $f^*(C)$ з невідомими елементами матриці C, яку необхідно оптимізувати до C^* таким чином, щоб цільова функція $f^*(C) \to 1$, так як всі події щодо закриття від атак ресурсів певними способами та методами повинні утворювати повну групу подій. Таким чином ми приходимо до збалансованої задачі лінійного програмування, яка полягатиме у тому, щоб при $f^*(C) \to 1$ та $\sum C_{ij} f_{opt}^{ij} \le \sum f_{opt}^{ij}$ при $0 \le C_{ij} \le 1$ отримати оптимальні значення C_{ij}^*, які і визначатимуть рівень ризику застосування певних контрзаходів щодо визначених ресурсів (з урахуванням визначених атак та уразливостей ресурсів).

II. Метод кластеризації ризиків на основі транзитивного замикання бінарного відношення активів.

У відповідності з першим методом ми отримали рівні ризику застосування певних контрзаходів щодо визначених ресурсів (з урахуванням визначених атак та уразливостей ресурсів), тобто вихідна матриця має розмір $card(D) \times card(AS)$.

Визначимо отриману матрицю, як матрицю об'єктів-ознак, де в якості об'єктів виступають ресурси (активи) AS, а в якості ознак – розподілені по ресурсам контрзаходи D.

В зв'язку з тим, що відповідно до формул (42-44) в попередньому методі, ми мали місце з нормованими значеннями, то відпадає необхідність здійснювати нормування елементів матриці.

Для отримання бінарного відношення, необхідно отримати матрицю близькості L_E, елементи якої визначаємо як міжточкові відстані за наступною формулою (використаємо Евклідову відстань) [12], але з урахуванням того, що елементами матриці є ступінь захисту певного контрзаходу відповідного ресурсу, то для визначення саме ризику не захисту даного ресурсу віднімемо отримане значення від 1:

$$l_{E_{ij}} = 1 - \sqrt{\frac{1}{n} \sum_{k=1}^{n} (d_{ik} - d_{jk})^2}.$$

Для визначення α-рівнів на основі транзитивного замикання відношення схожості визначається відношення еквівалентності, яке може бути у відповідності з теоремою декомпозиції представлено наступним чином [13]:

$$L_E = \bigcup_{\alpha} L_{E_\alpha}. \qquad (67)$$

Таке представлення дає можливість побудувати так зване, декомпозиційне дерево, яке достатньо точно відображає структуру відношення схожості або групування (кластеризацію) елементів, які побудовані з використанням їх транзитивних відстаней від інших елементів.

Таким чином, після побудови декомпозиційних дерев розглядаються α - рівні отриманих відношень еквівалентності.

Транзитивне замикання відношення схожості, визначається тим, що:

1) $\forall(x,x)\in E\times E:\mu_{L_E}(x,x)=1$ – властивість рефлексивності,

2) $\forall(x,y)\in E\times E:\mu_{L_E}(x,y)=\mu_{L_E}(y,x)$ – властивість симетрії

отримано відношення еквівалентності виходячи із визначення транзитивного замикання, яким називається відношення $\tilde{L}_E$, що визначається наступним чином:

$$\tilde{L}_E = L_E{}^1 \cup L_E{}^2 \cup ... \cup L_E{}^k \cup ...,$$

де відношення $L_E{}^k$ визначається рекурсивно.

Таким чином, якщо L_E – відношення в $E\times E$, то $L_E{}^2 = L_E \circ L_E$ і буде визначатися функцією корисності:

$$\mu_{L_E{}^2}(x,z)=\max_y\left[\min\left(\mu_{\tilde{L}_E}(x,y),\mu_{\tilde{L}_E}(y,z)\right)\right],$$

де

$$x,y,z\in E.$$

В результаті отримання за (67) відповідних α - рівнів ми отримуємо кластери ДІР, які згруповані за рівнями ризику. В результаті цього є можливість прослідкувати порядок об'єднання у кластери ДІР для подальшого їх аналізу. Використавши алгоритм, який представлено автором в [13], отримуємо оптимальний α - рівень, нижче якого ризик є допустимим.

Основні результати. До основних результатів досліджень, викладених у статті, можна віднести вперше представлену автором методологію аналізу ризиків дерева ідентифікаторів ДІР. Така методологія побудована на основі вперше запропонованих автором двох методів: методу визначення рівня ризику застосування певних контрзаходів щодо визначених ресурсів, що реалізує раніше представлену автором методологію "подвійної трійки захисту"; методу кластеризації ризиків на основі транзитивного замикання бінарного відношення активів, що дозволяє шляхом розбиття за відповідними α-рівнями отримати кластери ДІР, які згруповані за рівнями ризику. В результаті цього вдається можливим прослідкувати порядок об'єднання у кластери державних інформаційних ресурсів для подальшого їх аналізу, що може бути проведено шляхом подальшого отримання оптимального α-рівня, нижче якого ризик є допустимим. Другий метод є логічним доповненням першого, причому при оцінюванні ризиків інформаційної безпеки достатньою умовою є використання лише першого методу. В основі даних теоретичних викладок лежить теорія матричних обчислень, теорія множин, лінійного програмування.

Автором в статті не ставилось за мету проведення економізації вартості рішень у сфері розробки систем захисту інформації на базі ризикового підходу та адаптації законодавчої бази захисту інформації в Україні до міжнародних стандартів серії ISO 2700х. Основним результатом даної статті автор вважає формування системи стандартизації ДІР власної оригінальної методології, що зрозуміло не протирічить міжнародним стандартам, використовуючи особистий досвід та результати наукових досліджень представлених в серії статей та монографій групи науковців та викладення теоретичних основ оптимізації системи захисту ДІР.

Висновок. В результаті проведених досліджень автором представлено методологію аналізу ризиків дерева ідентифікаторів ДІР, що дозволяє здійснювати аналіз ризиків безпеки не тільки ДІР, а й інформаційно-телекомунікаційних систем та мереж у розрізі існуючих міжнародних стандартів. Наведений механізм, на думку автора, є з одного боку максимально доступним і простим, з іншого – втілює все краще, що реалізовано у міжнародних стандартах.

В подальшому автор бачить динамічний розвиток даної теорії у розрізі її практичного застосування в органах державного управління.

ЛІТЕРАТУРА

[1]. Юдін О. К. Загальна модель формування системи захисту державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик, О. В. Фролов // Наукоємні технології. – 2015. – № 4 (28). – С. 332-337.

[2]. Юдін О. К. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія / Юдін О. К., Бучик С. С. – К. : НАУ, 2015. – 214 с.

[3]. Бучик С.С. Оцінка функціональних профілів загроз державним інформаційним ресурсам / С. С. Бучик // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. – Житомир: ЖВІ ДУТ, 2014. – Вип. 9. – С. 146-155.

[4]. Бучик С. С. Методика оцінки інформаційних ризиків в автоматизованій системі / С. С. Бучик,

С. В. Мельник // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. – Житомир: ЖВІ, 2015. – Вип. 11. – С. 33-43.

[5]. N. Mayer, "Model-Based Management of Information System Security Risk", Namur, Belgium, 2009, ISBN : 978-2-87037-640-9.

[6]. Jihene Krichene. Managing Security Projects in Telecommunication Networks : To obtain Diploma of Doctor in Information and Communications Technology / Krichene Jihene. – Tunis: 2008. – 204 p.

[7]. M. Hamdi, X. Boudriga, "Algebraic Specification of Network Security Risk Management'" First ACM Workshop on Formal Methods in Security Engineering, Washington D.C., 2003.

[8]. Плетнёв П. В. Алгебраический подход к оценке информационной безопасности / П. В. Плетнёв, И. В. Лёвкин / Известия алтайского государственного университета. – 2010. – №1-2. – С.124-127. – Режим доступа: http://cyberleninka.ru/article/n/algebraicheskiy-podhod-k-otsenke-informatsionnoy-bezopasnosti.

[9]. Астахов А. М. Искусство управления информационными рисками / А. М. Астахов. – М.: ДМК Пресс, 2010. – 312 с.

[10]. Bruce Schneier, "Secrets and Lies: Digital Security in a Networked World", John Wiley & Sons, ISBN: 0471253111, 2001.

[11]. Бучик С. С. Системи підтримки прийняття рішень: конспект лекцій / С. С. Бучик, С. О. Кондратенко, О. О. Писарчук. – Житомир: ЖВІРЕ, 2006. – 168 с.

[12]. Мандель И. Д. Кластерный анализ / И. Д. Мандель. – М.: Финансы и статистика, 1988. – 176с.

[13]. Б. М. Герасимов Алгоритм визначення α - рівня нечіткого відношення / Б. М. Герасимов, С. С. Бучик, О. С. Кондратенко // Збірник наукових праць ВІТІ НТУ України "КПІ". – К.: ВІТІ НТУУ "КПІ", 2005. – Вип. 3. – С.8-12.

REFERENCES

[1]. Yudin O., Buchyk S., Frolov O. (2015) "Zagalna model formuvannya sistemi zahistu derzhavnih informatsiynih resursiv", Science-based technologies, №4(28), pp.332-337.

[2]. Yudin O., Buchyk S. Derzhavni informatsiyni resursi. Metodologiya pobudovi klasifikatora zagroz : monografiya, K: NAU, 2015, 214 p.

[3]. Buchik S.S. (2015) "Otsinka funktsionalnih profiliv zagroz derzhavnim informatsiynim resursam", Problemi stvorennya, viprobuvannya, zastosuvannya ta ekspluatatsiyi skladnih informatsiynih sistem : zb. nauk. prats, Zhitomir: ZhVI DUT, Vip. 9, pp. 146-155.

[4]. Buchik S., Melnik S. (2015) "Metodika otsinki informatsiynih rizikiv v avtomatizovaniy sistemi" Problemi stvorennya, viprobuvannya, zastosuvannya ta ekspluatatsiyi skladnih informatsiynih sistem : zb. nauk. prats, Zhitomir: ZhVI, Vip. 11, pp. 33-43.

[5]. N. Mayer, "Model-Based Management of Information System Security Risk", Namur, Belgium, 2009, ISBN : 978-2-87037-640-9.

[6]. Jihene Krichene. Managing Security Projects in Telecommunication Networks : To obtain Diploma of Doctor in Information and Communications Technology / Krichene Jihene. – Tunis: 2008. – 204 p.

[7]. M. Hamdi, X. Boudriga, "Algebraic Specification of Network Security Risk Management'" First ACM Workshop on Formal Methods in Security Engineering, Washington D.C., 2003.

[8]. PletnYov P., Lyovkin I. (2010) "Algebraicheskiy podhod k otsenke informatsionnoy bezopasnosti" Izvestiya altayskogo gosudarstvennogo universiteta, №1-2, pp. 124-127. – Rezhim dostupa: http://cyberleninka.ru/article/n/algebraicheskiy-podhod-k-otsenke-informatsionnoy-bezopasnosti.

[9]. Astahov A. M. Iskusstvo upravleniya informatsionnyimi riskami, M.: DMK Press, 2010, 312 p.

[10]. Bruce Schneier, "Secrets and Lies: Digital Security in a Networked World", John Wiley & Sons, ISBN: 0471253111, 2001.

[11]. Buchik S., Kondratenko S., Pisarchuk O. Sistemi pidtrimki priynyattya rishen : konspekt lektsiy, Zhitomir: ZhVIRE, 2006, 168 p.

[12]. Mandel I. Klasternyiy analiz, M.: Finansyi i statistika, 1988, 176 p.

[13]. Gerasimov B., Buchik S., Kondratenko S. (2005) "Algoritm viznachennya α-rivnya nechitkogo vidnoshennya", Zbirnik naukovih prats VITI NTU Ukraine "KPI", K.: VITI NTUU "KPI", Vip. 3, pp. 8-12.

МЕТОДОЛОГИЯ АНАЛИЗА РИСКОВ ДЕРЕВА ИДЕНТИФИКАТОРОВ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В статье представлена методология анализа рисков дерева идентификаторов государственных информационных ресурсов. Продемонстрировано, что фактически место анализа рисков информационной безопасности на государственном уровне не определенно, что в свою очередь обусловливает актуальность проведения исследований за указанной тематикой. Очерченная методология построена на основе впервые предложенных автором двух методах: методе определения уровня риска применения определенных контрмер относительно определенных ресурсов, который реализует ранее представленную автором методологию "двойной тройки защиты"; методе кластеризации рисков на основе транзитивного замыкания бинарного отношения активов, который позволяет путем разбиения за соответствующими α-уровнями получить кластеры государственных информационных ресурсов, которые сгруппированы за уровнями риска. В результате этого возникает возможность проследить порядок объединения в кластеры государственных информационных ресурсов для дальнейшего их анализа, который может

осуществляться путем дальнейшего получения оптимального α-уровня, ниже которого риск является допустимым. Второй метод является логическим дополнением первого, причем при оценивании рисков информационной безопасности достаточным условием является использование лишь первого метода.

Ключевые слова: государственные информационные ресурсы, риск, риск-менеджмент, уровень риска, угроза, уязвимость, контрмероприятия, атака.

THE METHODOLOGY OF ANALYSIS OF RISKS OF TREE THAT IDENTIFIERS THE STATE INFORMATIVE RESOURCES

In the article the methodology of analysis of risks of tree of identifiers of state informative resources is shown. The actually place of analysis of risks of the informative safety at the state level is not certain, that stipulates the actuality of the realization of researches after this subject. This methodology is built on the basis of the first offered by the author two methods : the method of determination of level of risk of application of certain counter-measures in relation to certain resources, which will realize the methodology of "double three of defence" presented by the author before; the method of clusterization of risks on the basis of the transition shorting of binary relation of assets, which allows by division after corresponding α - by levels to get the clusters of state informative resources, which are grouped after the levels of risk. After that there is a possibility to trace the order of association in the clusters of state informative resources for their further analysis that can be conducted by the further receipt of optimal α - level, below which a risk is possible. The second method is logical addition of the first, thus at the evaluation of risks of informative safety a sufficient condition is the use only of the first method.

Key words: state informative resources, risk, risk management, risk level, asset, threat, vulnerability, counter-measure, attack.

Бучик Сергій Степанович, кандидат технічних наук, доцент, начальник кафедри автоматизованих систем управління Житомирського військового інституту імені С. П. Корольова.
E-mail: s_stbu@ukr.net

Бучик Сергей Степанович, кандидат технических наук, доцент, начальник кафедры автоматизированных систем управления Житомирского военного института имени С.П. Королева.

Buchyk Sergii, PhD in Eng., chief of department of automated control the system the Zhitomir Military Institute of the name of S.P. Korolyova.