УДК 004.056.5

ТЕОРЕТИЧНІ ОСНОВИ АНАЛІЗУ РИЗИКІВ ДЕРЕВА ІДЕНТИФІКАТОРІВ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

С. С. Бучик, канд. техн. наук, доц.
** Житомирський військовий інститут імені С. П. Корольова
e-mail: s_stbu@ukr.net

Викладено теоретичні основи аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів. Доведено відсутність дієвого механізму проведення процесу ризик-менеджменту в Україні на державному рівні. З урахуванням попередніх досліджень введено поняття куб Юдіна–Бучика, на основі якого фактично побудована методологія побудови класифікатора загроз державним інформаційним ресурсам («методологія подвійної трійки захисту»). У продовження тематики захисту державних інформаційних ресурсів визначено методологію оцінки ризиків безпеки інформаційно-телекомунікаційних систем та мереж у розрізі міжнародних стандартів. Здійснено постановку завдання для визначення рівня ризику державних інформаційних ресурсів з урахуванням основних характеристик, що його визначають: активів (до яких належать державні інформаційні ресурси), загроз, уразливостей, контрзаходів, з яких визначається рішення щодо захисту конкретного державного інформаційного ресурсу в разі можливого здійснення на нього атаки, переліку атак, що можуть бути здійсненні на активи.

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

In the article the theoretical bases of analysis of risks of tree of identifiers of state informative resources are expounded. The authors show the absence of effective mechanism of realization of risk process of management in Ukraine on the state level. According to the previous researches a concept of the cube of Yudina–Buchyka is entered, on the basis of it the authors built the actually methodology of construction of classifier of threats to the state informative resources (the authors enter a concept «methodology of double three of security»). In continuation of subjects of security of state informative resources the authors certain the methodology of estimation of risks of safety of the information-telecommunications systems and networks in the context of international standards. Raising of task of determination of level of risk of state informative resources taking into account basic descriptions, that characterize him, is carried out: assets (state informative resources behave to that), threats, to vulnerability, counter-measures, from that a decision is determined in relation to security of certain state informative resource in case of possible realization of attack, list of attacks that can be realized on assets.

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

Актуальність дослідження

Питання дослідження та найголовніше, практичне впровадження результатів під час побудови системи менеджменту інформаційної безпеки (СМІБ) досліджувалось багатьма авторами, зокрема за кордоном. Нажаль, у зв'язку з відсутністю в Україні сталої законодавчої бази з аналізу ризиків інформаційної безпеки (ІБ), небажанням, з незрозумілих причин, впроваджувати досвід провідних країн світу, процес побудови ІБ держави в цілому перебуває під загрозою бути не розвиненим.

Тому тематика, викладена в статті, демонструє протиріччя між існуючою реальністю та міжнародними вимогами щодо аналізу ризиків ІБ і є актуальною для сьогодення нашої молодої держави.

Аналіз останніх досліджень та публікацій

Автор статті вже торкався у своїх працях питання оцінювання ризиків ІБ.

Так у праці [1] показано один із підходів та можливість його використання для оцінки факторів ризику (у даному випадку загроз) ІБ, у праці [2] авторами запропоновано, показано та проаналізовано удосконалену методику оцінювання інформаційного ризику в автоматизованій системі (АС).

У праці [3] здійснено спробу узагальнити всі основні моделі менеджменту інформаційної системи щодо безпеки ризиків.

У праці [4] здійснено спробу аналізу менеджменту ризику ІБ у телекомунікаційних мережах.

У праці [5] розкрито алгебричні специфікації ризик-менеджменту безпеки мереж на основі по-

будови сигнатур ризиків, використання логіки предикатів та вейвлет-перетворень. Є кількість робіт, що присвячені аналізу ризиків у інформаційних системах і у ближньому зарубіжжі.

Так, у праці [6] описано процес оцінювання ризиків ІБ і розглянуто спосіб застосування когнітивно-орієнтованих моделей і схем виводу, таких як логічний висновок і семантичні мережі.

У праці [7] розкрито механізми управління ризиками ІБ відповідно до міжнародних стандартів ISO/IEC 27005 та BS 7799-3.

Мета статті — це розробка теоретичних основ аналізу та визначення ризиків інформаційної безпеки дерева ідентифікаторів державних інформаційних ресурсів (ДІР).

Виклад основного матеріалу

Розглянемо проблему аналізу ризику дерева ідентифікаторів ДІР, при цьому використовуватимемо методологію подвійної трійки захисту, яку автори запропонували в праці [8] (рис. 1) та принципи побудови комплексної системи захисту ДІР, які автори запропонували в праці [9].

У нижній частині рис. 1 подано куб захисту Юдіна–Бучика (процес його формування буде розкрито нижче).

Загалом менеджмент ризиків ІБ являє інтерес для більшості державних інститутів та недержавних установ, в яких активи мають цінність та впливають на репутацію.

Тому у світі йде постійна робота щодо удосконалення цього напрямку через розвиток та впровадження стандартів, специфікацій та моделей ризик-менеджменту (РМ).

Для доведення важливості впровадження РМ наведемо порівняльну таблицю впровадження стандарту ISO/IEC 27005 щодо РМ в республіці Казахстан, Білорусь, Російській Федерації, республіці Польща та Україні (див. таблицю) на державному рівні.

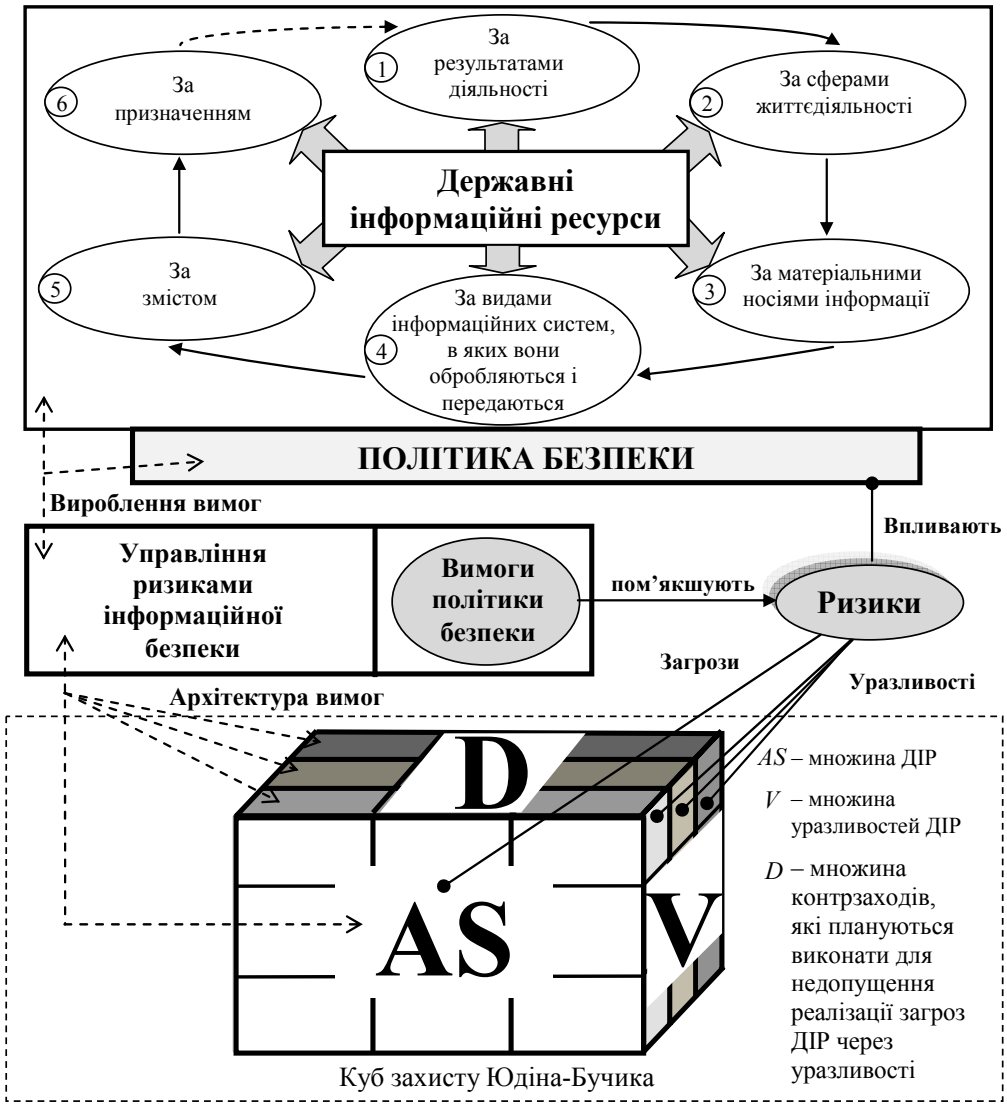

Рис. 1. Постановка проблеми аналізу ризику дерева ідентифікаторів державних інформаційних ресурсів

Таблиця

Порівняльна характеристика впровадження стандартів РМ

Назва міжнародного стандарту	Впровадження в республіці Казахстан	Впровадження в РФ	Впровадження в республіці Білорусь	Впровадження в республіці Польща	Впровадження в Україні
ISO/IEC 27005:2011. Information technology – Security techniques – Information security risk management	**Так** СТ РК ISO/IEC 27005-2013 Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности	**Так** ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности	**Так** СТБ ISO/IEC 27005-2012 Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности	**Так** PN-ISO/IEC 27005:2014-01 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji	**Ні**

Даний аналіз показує, що на державному рівні в Україні не розроблено (впроваджено) даного стандарту, що регламентував би питання РМ.

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».

У цілому, аналізуючи світовий простір міжнародних стандартів [8], на практиці при обґрунтуванні проекту інформаційної безпеки організацій отримано два підходу: перший засновано на перевірці відповідності рівня захищеності інформаційно-телекомунікаційної системи (ІТС) вимогам одного із стандартів в галузі ІБ (як вказано вище в Україні це здійснюється на основі НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99, в Російській Федерації та у більшості європейських країн — відповідно з ISO/IEC 15408 — Загальних критеріїв безпеки інформаційних технологій і т. д.). У даному випадку як критерій ефективності виступають сумарні витрати на виконання визначених функціональних вимог:

$$\sum_{i=1}^{n} C_i \to \min ,$$

де C_i — витрати на *i*-й засіб захисту.

Основний недолік цього підходу полягає в тому, що в разі, коли необхідний рівень захищеності чітко не заданий (наприклад, через законодавчі вимоги) визначити «найбільш ефективний» рівень захищеності ІТС досить складно.

Другий підхід пов'язано з оцінкою та управлінням ризиками, що містить в собі оцінювання розміру збитків, очікуваних від інцидентів, пов'язаних з інформаційною безпекою (наприклад, протягом року). Потім здійснюється оцінка того, як засоби та заходи забезпечення безпеки впливають на зниження ризику та здійснюється розрахунок їх вартості. Нажаль, в Україні даний підхід офіційно згідно НД ТЗІ не використовується.

Життєвий цикл методології оцінки ризиків безпеки інформаційно-телекомунікаційних систем та мереж можна представити наступною схемою (рис. 2) [4].

На рис. 2 суцільними лініями відображено процес по управлінню ризиками. Стрілками показано відношення між одинадцятьма процесами методології оцінки ризиків безпеки інформаційно-телекомунікаційних систем та мереж (ІТСМ).

Кожен з процесів являє собою частину діяльності, необхідну для проведення сукупності РМ процесів.

Якщо два підпроцеси поєднані/з'єднані суцільною лінією, то вихід першого є входом для другого. З іншого боку, на рис. 2 пунктирною лінією представлені деякі процеси, які є специфічними для даної методології.

Надамо короткий огляд одинадцятим представленим процесам.

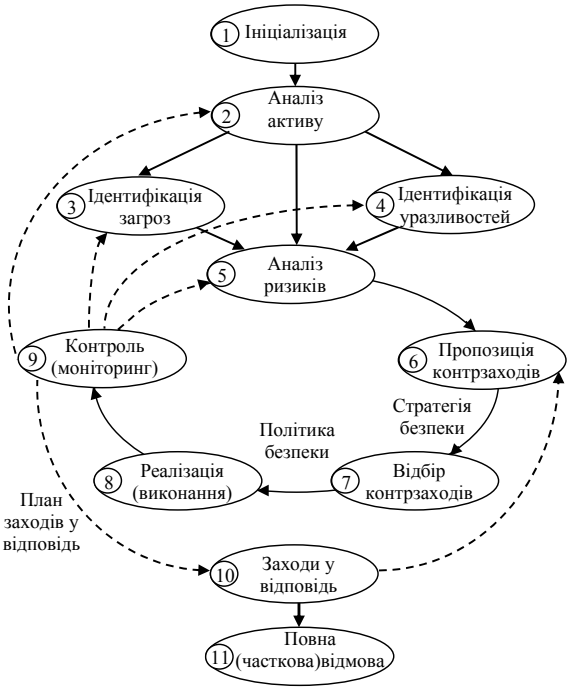

Рис. 2. Методологія оцінки ризиків безпеки інформаційно-телекомунікаційних систем та мереж

1. *Ініціалізація.* Даний процес має за мету підготовку РМ проекту, оцінку його вартості та визначення плану заходів по управлінню ризиками.

2. *Аналіз активів.* Метою цього процесу є збірання інформації про систему, яка аналізу-ється.

3. *Ідентифікація загроз.* Цей процес напрямлений на виявлення атак, які загрожують системі, відповідно до класифікації загроз.

4. *Ідентифікація уразливостей.* На цьому рівні здійснюється виявлення недоліків та порушення безпеки системи, що аналізується.

5. *Аналіз ризиків.* Метою даного процесу є виявлення ризиків, які можуть загрожувати активам системи, що аналізується, на підставі виявлених уразливостей та загроз.

6. *Пропозиція контрзаходів.* На цьому рівні пропонується стратегія пом'якшення виявлених ризиків.

7. *Відбір контрзаходів.* Мета даного процесу — визначити політику безпеки, яка буде адаптована до системи, що аналізується, для зниження рівня небезпеки.

8. *Реалізація (виконання).* На цьому рівні обрані контрзаходи безпеки реалізуються відповідно до політикою безпеки.

9. *Контроль (моніторинг).* Мета цього процесу — підтримання системи, що аналізується на рівні безпеки, якій прийнятний. Моніторинг активності може викликати необхідність повторного виконання деяких процесів, якщо це необхідно.

10. *Заходи у відповідь.* Даний процес направлений на те, щоб здійснювати реагування безпекою відповідно до плану заходів у відповідь.

11. *Повна (часткова) відмова.* Цей процес вказує на повну відмову системи або дестабілізацію базових процесів.

Отже, бачимо, що даний підхід має спільні риси з видами діяльності, які пов'язані з менеджментом інформаційної безпеки за стандартом ISO/IEC 27005:2011 [10], що в загальному вигляді являє собою такий процес: встановлення контексту; оцінка ризику; обробка ризику; прийняття ризику; обмін інформацією відносно ризику; моніторинг та перегляд ризику.

Оцінка ризику дерева ідентифікаторів ДІР полягає у визначенні його рівня (кількісної або якісної величини) та порівняння цього рівня з максимально припустимим (прийнятним) рівнем, а також, можливо, з рівнем інших ризиків. Класично, відповідно до ISO/IEC 27005:2011 рівень ризику визначається комбінуванням двох величин: *імовірності події та розмирів її наслідків.* Подія полягає у реалізації загрози державному інформаційному ресурсу, яка реалізує уразливості ресурсу для впливу на нього та порушення його безпеки (для ДІР відповідно до методології «подвійної трійки захисту» [8] розуміють властивості інформації: конфіденційність — захист від несанкціонованого ознайомлення; цілісність — актуальність та несуперечність ДІР, їх захищеність від несанкціонованої зміни; доступність — можливість за час, що прийнятний, отримати доступ до ДІР). У праці [8] авторами наведено механізм атаки ДІР. В інтерпретації до оцінки ризиків та з урахуванням вищесказаного наведемо механізм визначення рівня ризику ДІР (рис. 3).

Рис. 3. Механізм визначення рівня ризику ДІР

Таким чином, кількісне визначення величини ризику ДІР відповідно зі стандартом ISO/IEC 27005:2011 та інтерпретацією рис. 3 можна виразити такою формулою:

$$R_{\text{ДІР}} = P_{\text{з\_ДІР}} \times S_{\text{ДІР}}, \quad (1)$$

де $P_{\text{з\_ДІР}}$ — імовірність успішної реалізації загрози ДІР відносно до ресурсу з використанням уразливості та нанесення збитку державній установі; $S_{\text{ДІР}}$ — наслідки реалізації загрози ДІР (збиток через цінність ресурсу).

Імовірність успішної реалізації загрози $P_{\text{з\_ДІР}}$ визначають так:

$$P_{\text{з\_ДІР}} = P_{\text{рз\_ДІР}} \times V, \quad (2)$$

де $P_{\text{рз\_ДІР}}$ — імовірність того, що загроза відносно до ДІР буде реалізовуватися (успішність або неуспішність реалізації загрози визначається величиною уразливості); V — імовірність того, що у випадку реалізації загрози відносно до ДІР ця загроза буде реалізована успішно, з використанням даної уразливості, в зв'язку з чим безпека активу порушуватиметься (визначені вище властивості інформації) та державна установа понесе певний збиток.

Таким чином, кількісне визначення величини ризику ДІР буде визначатися з урахуванням (1) і (2):

$$R_{\text{ДІР}} = P_{\text{рз\_ДІР}} \times V \times S_{\text{ДІР}}. \quad (3)$$

Наочно механізм визначення рівня ризику ДІР з урахуванням (3) можна подати так (рис. 4).

Для визначення величини ризику використовують оціночні кількісні значення, які отримують шляхом експертних оцінок, прогнозування, а також на основі статистичних даних.

Розмір збитку зазвичай визначається в грошових одиницях, величина уразливості приймає значення в діапазоні від 0 до 1, а ймовірність загрози є цілим позитивним числом, яке визначає кількість спроб реалізації загроз, що очікують за визначений період часу.

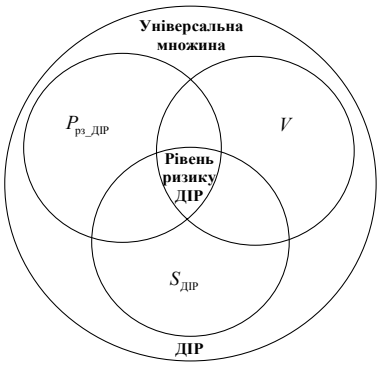

Рис. 4. Механізм визначення рівня ризику ДІР

Для розрахунку ризиків зручно використовувати період часу, якій дорівнює одному року.

У цьому випадку величина ризику відповідає середньорічним збиткам організації, що прогнозуються в результаті інцидентів безпеки (Annual Loss Expectancy — ALE) [7].

Український сегмент міжнародного дерева ідентифікаторів об'єктів OID (object identifier tree) авторами розглядався в праці [8] та у зв'язку з малою кількістю об'єктів в ньому (саме українського сегменту) та відсутністю систематичного наповнення, в праці [8] авторами здійснена спроба описати ієрархічну гілку кодів вузлів для наповнення Національного реєстру Українського сегменту міжнародного дерева ідентифікаторів об'єктів на базі структури системи судів загальної юрисдикції.

Таким чином, виникає необхідність: по-перше здійснювати наповнення даного дерева, у якому містяться ДІР та по-друге захищати його від несанкціонованих дій.

У даній статті зупинимося на розгляді методології оцінки ризиків ДІР, що містяться в українському сегменті міжнародного дерева ідентифікаторів OID.

Для вирішення цього завдання використаємо підхід щодо мережевого управління ризиками ІБ, який представлений в праці [5].

Таким чином, визначимо для здійснення аналізу ризиків дерева ідентифікаторів ДІР такі 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 у рамках теорії, яка була описана вище і не суперечить загальноприйнятим підходам щодо визначення складових ризику.

Відповідно до запропонованої авторами «методології подвійної трійки захисту» [8], представимо дані складові у вигляді таких множин.

1. Множина активів ДІР

$$AS = \{AS_{nps}, AS_{ors}, AS_{its}\},$$

де AS_{nps}, AS_{ors}, AS_{its} множина ДІР в яких їх захист напрямлений 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)

$$AS_{nps} = \{AS_{nps}^{conf}, AS_{nps}^{\text{int}}, AS_{nps}^{av}\};$$
$$AS_{ors} = \{AS_{ors}^{conf}, AS_{ors}^{\text{int}}, AS_{ors}^{av}\};$$
$$AS_{its} = \{AS_{its}^{conf}, AS_{its}^{\text{int}}, AS_{its}^{av}\}.$$

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

$$AS_{nps}^{conf} = \{as_{nps_1}^{conf}, as_{nps_2}^{conf}, ..., as_{nps_{confnps}}^{conf}\};$$
$$AS_{nps}^{\text{int}} = \{as_{nps_1}^{\text{int}}, as_{nps_2}^{\text{int}}, ..., as_{nps_{\text{int}\,nps}}^{\text{int}}\};$$
$$AS_{nps}^{av} = \{as_{nps_1}^{av}, as_{nps_2}^{av}, ..., as_{nps_{avnps}}^{av}\},$$

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

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

$$AS_{ors}^{conf} = \{as_{ors_1}^{conf}, as_{ors_2}^{conf}, ..., as_{ors_{confors}}^{conf}\};$$
$$AS_{ors}^{av} = \{as_{ors_1}^{av}, as_{ors_2}^{av}, ..., as_{ors_{avors}}^{av}\};$$
$$AS_{ors}^{\text{int}} = \{as_{ors_1}^{\text{int}}, as_{ors_2}^{\text{int}}, ..., as_{ors_{\text{int}\,ors}}^{\text{int}}\},$$

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

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

$$AS_{its}^{conf} = \{as_{its_1}^{conf}, as_{its_2}^{conf}, ..., as_{its_{confits}}^{conf}\};$$
$$AS_{its}^{\text{int}} = \{as_{its_1}^{\text{int}}, as_{its_2}^{\text{int}}, ..., as_{its_{\text{int}\,its}}^{\text{int}}\};$$
$$AS_{its}^{av} = \{as_{its_1}^{av}, as_{its_2}^{av}, ..., as_{its_{avits}}^{av}\},$$

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

Дані множини можуть перетинатися, оскільки 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

$$V = \{V_{nps}, V_{ors}, V_{its}\}$$

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)

$$V_{nps} = \{V_{nps}^{conf}, V_{nps}^{\text{int}}, V_{nps}^{av}\};$$
$$V_{ors} = \{V_{ors}^{conf}, V_{ors}^{\text{int}}, V_{ors}^{av}\};$$
$$V_{its} = \{V_{its}^{conf}, V_{its}^{\text{int}}, V_{its}^{av}\},$$

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

$$V_{nps}^{conf} = \{v_{nps_1}^{conf}, v_{nps_2}^{conf}, ..., v_{nps_{confnps}}^{conf}\}$$
$$V_{nps}^{\text{int}} = \{v_{nps_1}^{\text{int}}, v_{nps_2}^{\text{int}}, ..., v_{nps_{\text{int}\,nps}}^{\text{int}}\}$$
$$V_{nps}^{av} = \{v_{nps_1}^{av}, v_{nps_2}^{av}, ..., v_{nps_{avnps}}^{av}\}$$

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

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

$$V_{ors}^{conf} = \{v_{ors_1}^{conf}, v_{ors_2}^{conf}, ..., v_{ors_{confors}}^{conf}\};$$
$$V_{ors}^{\text{int}} = \{v_{ors_1}^{\text{int}}, v_{ors_2}^{\text{int}}, ..., v_{ors_{\text{int}\,ors}}^{\text{int}}\};$$
$$V_{ors}^{av} = \{v_{ors_1}^{av}, v_{ors_2}^{av}, ..., v_{ors_{avors}}^{av}\},$$

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

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

$$V_{its}^{conf} = \{v_{its_1}^{conf}, v_{its_2}^{conf}, ..., v_{its_{confits}}^{conf}\};$$
$$V_{its}^{\text{int}} = \{v_{its_1}^{\text{int}}, v_{its_2}^{\text{int}}, ..., v_{its_{\text{int}\,its}}^{\text{int}}\};$$
$$V_{its}^{av} = \{v_{its_1}^{av}, v_{its_2}^{av}, ..., v_{its_{avits}}^{av}\},$$

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

3. Множина контрзаходів

$$D = \{D_{nps}, D_{ors}, D_{its}\}$$

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):

$$D_{nps} = \{D_{nps}^{conf}, D_{nps}^{\text{int}}, D_{nps}^{av}\};$$
$$D_{ors} = \{D_{ors}^{conf}, D_{ors}^{\text{int}}, D_{ors}^{av}\};$$
$$D_{its} = \{D_{its}^{conf}, D_{its}^{\text{int}}, D_{its}^{av}\}.$$

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

$$D_{nps}^{conf} = \{d_{nps_1}^{conf}, d_{nps_2}^{conf}, ..., d_{nps_{confnps}}^{conf}\};$$
$$D_{nps}^{\text{int}} = \{d_{nps_1}^{\text{int}}, d_{nps_2}^{\text{int}}, ..., d_{nps_{\text{int}\,nps}}^{\text{int}}\};$$

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

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

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

$$D_{ors}^{conf} = \left\{ d_{ors_1}^{conf}, d_{ors_2}^{conf}, ..., d_{ors_{confors}}^{conf} \right\};$$

$$D_{ors}^{\text{int}} = \left\{ d_{ors_1}^{\text{int}}, d_{ors_2}^{\text{int}}, ..., d_{ors_{\text{int}\,ors}}^{\text{int}} \right\};$$

$$D_{ors}^{av} = \left\{ d_{ors_1}^{av}, d_{ors_2}^{av}, ..., d_{ors_{avors}}^{av} \right\},$$

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

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

$$D_{its}^{conf} = \left\{ d_{its_1}^{conf}, d_{its_2}^{conf}, ..., d_{its_{confits}}^{conf} \right\};$$

$$D_{its}^{\text{int}} = \left\{ d_{its_1}^{\text{int}}, d_{its_2}^{\text{int}}, ..., d_{its_{\text{int}\,its}}^{\text{int}} \right\};$$

$$D_{its}^{av} = \left\{ d_{its_1}^{av}, d_{its_2}^{av}, ..., d_{its_{avits}}^{av} \right\},$$

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

4. *Множина атак*

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

де $card(AT)$ потужність множини атак; N — кількість спрямувань загроз ДІР (НорПС, ОргС, ІнжТС); $at_k(V_z)$ — функція залежності k-ї атаки від уразливості ДІР за z-м спрямуванням.

Необхідність введення даної залежності полягає у тому, що за рахунок зміни коефіцієнтів матриці V_z можемо впливати на атаку.

Розкриємо для наочності куб Юдіна–Бучика відповідно до введених позначень.

Початковий куб, який наведено з множини $\{AS, V, D\}$ (рис. 5, *а*) відповідно до пунктів 1, 2, 3, буде представлено так (рис. 5, *б*). Надалі відповідно до пунктів 1.1, 2.1, 3.1 маємо наступне розкриття попередніх кубів (рис. 5, *в*). Надалі відповідно до пунктів 1.2, 2.2, 3.2 отримуємо простір кубів (рис. 5, *г*).

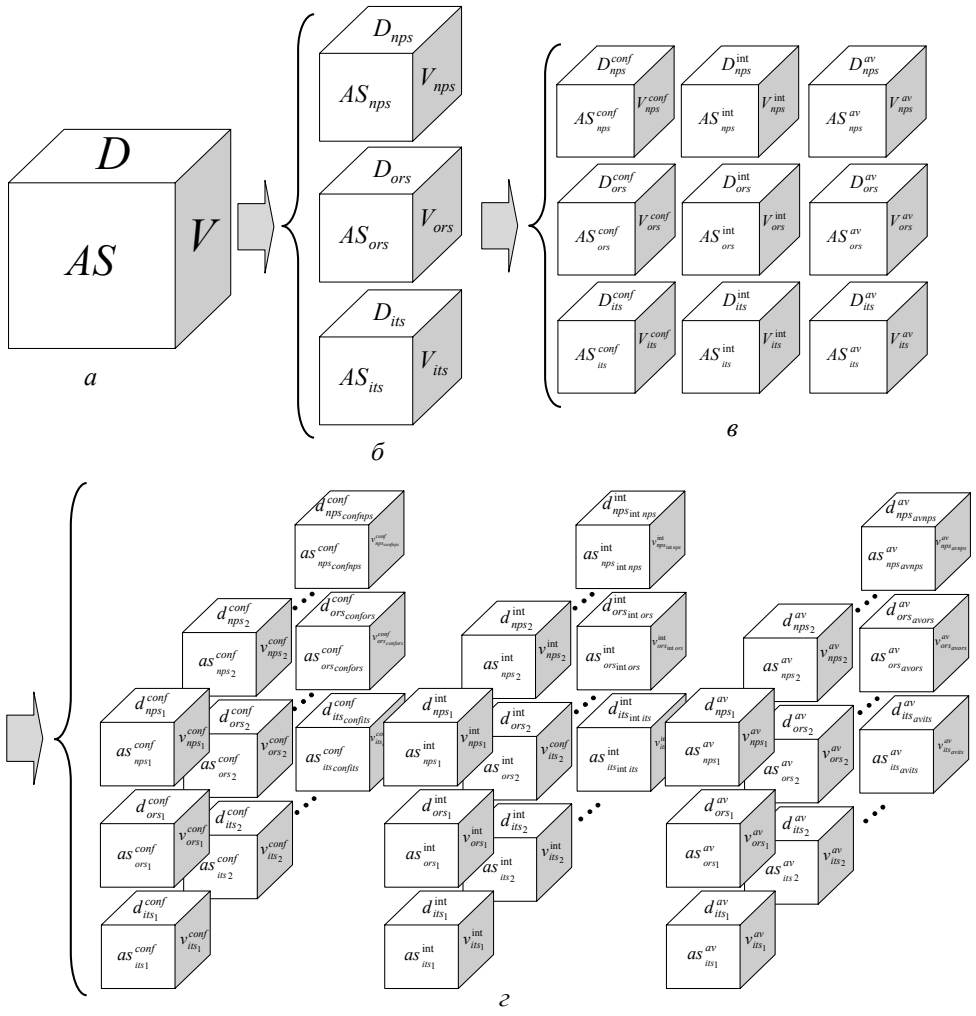

Рис. 5. Пошарове розкриття кубу Юдіна–Бучика

Основні результати

До основних результатів статті можна віднести проведений аналіз щодо відсутності в Україні на державному рівні дієвого механізму аналізу ризиків інформаційної безпеки. Введено поняття куб Юдіна–Бучика та здійснено на його основі постановку проблеми аналізу ризику дерева ідентифікаторів державних інформаційних ресурсів, визначено методологію оцінки ризиків безпеки інформаційно-телекомунікаційних систем та мереж у розрізі міжнародних стандартів. Представлено в оригінальній авторській інтерпретації теоретичні основи аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів, базовим поняттям якого виступає розроблена авторами в попередніх дослідженнях методологія «подвійної трійки захисту».

Висновок

У результаті проведених досліджень щодо теоретичних основ аналізу ризиків безпеки не тільки ДІР, а і ІТСМ у розрізі існуючих міжнародних стандартів в Україні на державному рівні необхідно запровадити дієвий механізм ризик-менеджменту, якій на сучасному етапі розвитку фактично відсутній. Даний механізм з одного боку має бути максимально доступним і простим, з другого боку — втілювати все краще, що реалізовано у міжнародних стандартах, особливо на тлі сучасного розвитку Україні як європейської держави та необхідності швидкої адаптації до стандартів країн Європейського Союзу.

У подальшому, автор бачить динамічний розвиток даної теорії у розрізі детального розкриття механізму визначення рівня ризику державних інформаційних ресурсів з урахуванням основних характеристик, які його визначають.

ЛІТЕРАТУРА

1. *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.

2. *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.

3. *N. Mayer*. “Model-Based Management of Information System Security Risk”, Namur, Belgium, 2009, ISBN : 978-2-87037-640-9.

4. *Jihene Krichene*. Managing Security Projects in Telecommunication Networks : To obtain Diploma of Doctor in Information and Communications Technology / Krichene Jihene. — Tunis: 2008. — 204 p.

5. **M. Hamdi**, X. Boudriga, “Algebraic Specification of Network Security Risk Management"” First ACM Workshop on Formal Methods in Security Engineering, Washington D.C., 2003.

6. *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.

7. *Астахов А. М*. Искусство управления информационными рисками / А. М. Астахов. — М. : ДМК Пресс, 2010. — 312 с.

8. *Юдін О. К*. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія / О. К. Юдін, С. С. Бучик. — К. : НАУ, 2015. — 214 с.

9. *Юдін О. К*. Принципи побудови комплексної системи захисту державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Наукоємні технології. — 2015. — № 1 (25). — С. 15–20.

10. *Информационная* технология — Методы и средства обеспечения безопасности — Менеджмент риска информационной безопасности : ISO/IEC 27005 : 2011 [Электронный ресурс]. — Режим доступа: https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf.

Стаття надійшла до редакції 21.01.2016