https://orcid.org/0000-0001-5329-889X
https://orcid.org/0000-0003-1236-287X
https://orcid.org/0000-0001-6991-0617

УДК 004.02:004.5:004.6 351.863.1

О.В. НЕСТЕРЕНКО[*], І.Є. НЕТЕСІН[**], В.Б. ПОЛІЩУК[**]

МЕТОД ОБЧИСЛЕНЬ У ЗАДАЧАХ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

[*]Національна академія управління, м. Київ, Україна
[**]Український науковий центр розвитку інформаційних технологій, м. Київ, Україна

Анотація. *В умовах постійних проявів агресії у різних сферах діяльності, що є однією з найгостріших проблем сьогодення, набувають усе більшої актуальності заходи на їх упередження. Це у свою чергу вимагає вдосконалення методичного забезпечення підтримки прийняття рішень щодо забезпечення безпеки та протидії атакам різного роду. На сучасному етапі характерною рисою управління у сфері безпеки все ще залишаються занадто повільне виявлення інцидентів та визначення масштабів їх розвитку. Методологічна складність процедур оцінювання ризиків безпеки та відповідних обчислень обумовлена нестачею на ринку відповідних методик, програмних засобів і технологій, що ускладнює створення автоматизованих засобів підтримки прийняття рішень. У даному дослідженні пропонується універсальний метод, що базується на формалізованій моделі відображення взаємозв'язку об'єктів (ресурсів), націлених на них загроз та очікуваних ризиків. В основу такої моделі покладена бінарна схема «загроза – об'єкт», яка має вираз у вигляді дводольного графа. Модель передбачає розподіл графа на підграфи. У відповідності з моделлю безпеки з повним перекриттям будується третій набір, що відповідає механізмам захисту. Одночасне застосування елементів онтологічних описів підвищує рівень конкретності методу та більш чіткого уявлення щодо стану середовища. Для проведення обчислень запропоновано матричний підхід, який тісно пов'язаний із графовими моделями. Наведені схеми технологічної реалізації отриманих рішень на основі офісних застосунків та побудови відповідної інформаційно-аналітичної системи. Запропонований метод може застосовуватись у автоматизованих системах у багатьох сферах діяльності.*

Ключові слова: *безпека, ризик, онтологія, матриці, графи, інформаційно-аналітична система.*

Abstract. *In conditions of constant displays of aggression in various fields of activity, which is one of the most acute problems of our time, corresponding preventive measures are becoming increasingly important. In its turn, it requires the improvement of the methodological support for decision-making to ensure security and counter various kinds of attacks. At the present stage, the remaining slowness of identification of incidents and determining the scale of their development is a characteristic feature of security management. Methodological complexity of the procedures for assessing security risks and corresponding calculations is stipulated by the lack of appropriate methods, software and technologies on the market, which complicates the development of automated decision support tools. This paper offers a universal method based on a formalized model of the relationship between objects (resources), aimed at them threats and expected risks. This model is based on the «threat – object» binary scheme expressed in a bipartite graph and provides for the division of the graph into subgraphs. There is built another (third) set that corresponds to the safety model with full overlap and protection mechanisms as well. Simultaneous utilization of the elements of ontological descriptions increases the level of the method concreteness and a clearer understanding of the environment state. A matrix approach, which is closely related to graph models, is proposed for computations. The article provides some schemes of technological implementation of the obtained solutions based on office applications and designing a corresponding information and analytical system. The proposed method can be applied in automated systems in many fields of activity.*

Keywords: *security, risk, ontology, matrices, graphs, information and analytical system.*

DOI: 10.34121/1028-9763-2021-3-47-59

1. Вступ

У наш час однією з найгостріших проблем є прояви агресії. Хоча вважається, що агресія є атрибутивною властивістю людини і належить до необхідних біологічних механізмів виживання. Її прояви деструктивності, що все більше поширюються і в індивідуальному, і в суспільному житті, становлять суттєву загрозу розвитку людини і людства та поглиблюють суспільну кризу [1]. Одним із найбільш наочних прикладів негативних виразів агресії може слугувати поширення інцидентів кібербезпеки. Зі збільшенням кількості ланок з'єднань в Інтернеті сильнішають можливості кіберзлочинців щодо проникнення шкідливого програмного забезпечення в комп'ютерні системи, які функціонують у різних галузях. Усе відчутніше зростає схожість закономірностей розвитку вірусних кібератак та розвитку біологічних епідемій [2]. Водночас ми вже є свідками й переростання останніх у світові пандемії, природа яких залишається остаточно не з'ясованою. Почастішали випадки терористичних актів та вуличної злочинності. Тому питання вироблення ефективних засобів протидії агресії в контексті зміцнення безпеки та можливостей застосування сучасних методів захисту набувають усе більшої актуальності. Особливо важливим це є у сферах оборони та надзвичайних ситуацій.

У таких умовах забезпечення безпеки та протидії атакам різного роду, що охоплюють різні сфери діяльності, потребує заходів на упередження та вдосконалення підтримки прийняття відповідних рішень [3, 4]. Водночас виявлення інцидентів та визначення масштабів їх розвитку все ще залишається занадто повільним. Особливе занепокоєння викликає й той факт, що значна частина атак виявляється взагалі несподіваними. Частка нових невідомих атак, так званих атак «нульового дня», постійно множиться. Це пояснюється значною мірою й об'єктивними чинниками. Як би швидко не зростала кількість технологій захисту, множина видів атак завжди буде більшою.

Масштаб проблеми досяг такого розмаху, що просто реагувати на безпекові інциденти є недостатнім. Потрібні системи управління безпекою, без якої громадяни, підприємства та організації, міста і країни залишаться беззахисними перед навалою різних атак. Важливими складовими такої системи є засоби підтримки прийняття рішень, що зокрема забезпечують упереджувальні заходи та прогнозування реалізації й розвитку атак. Разом із тим необхідно зазначити, що на цей час не існує більш-менш універсальної методики, адекватної різним сферам застосування. Чимало управлінців не звертають уваги на важливість робіт з оцінки ризиків безпеки у сфері практичної діяльності, у тому числі й у зв'язку з нестачею на ринку відповідних методик, програмних засобів і технологій, що у свою чергу ускладнює й створення автоматизованих засобів підтримки прийняття рішень.

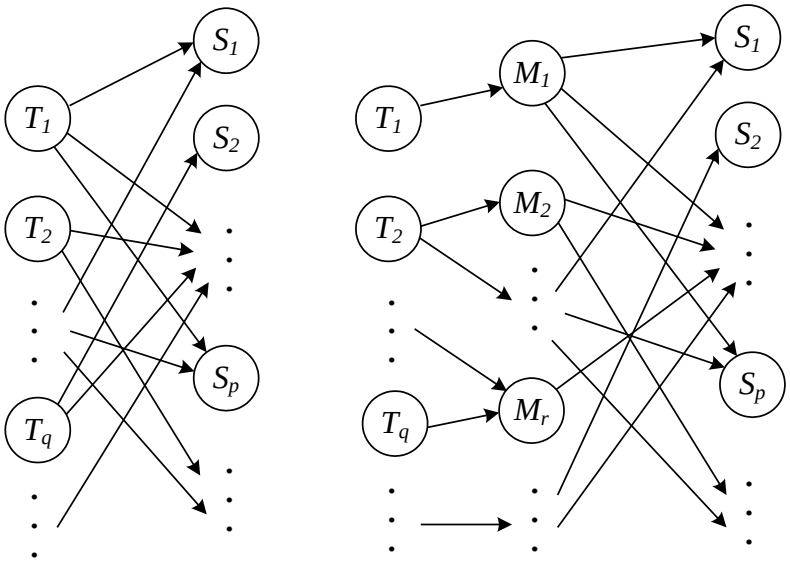
Метою даної статті є пропонування універсального методу проведення обчислень на основі формалізованої моделі, що відображає взаємозв'язок об'єктів (ресурсів), націлених на них загроз та очікуваних ризиків, та який може застосовуватись в автоматизованому режимі у багатьох сферах діяльності.

2. Постановка задачі та класифікація понять

Переважну більшість інцидентів (атак) у різних сферах можна представити у вигляді бінарної схеми «загроза» → «об'єкт», яка може мати вираз у вигляді дводольного графа $G_{TS}=(V(T,S),\ E(T,S))$ (рис. 1*а*). У цьому графі множини вершин його часток $T \cup S = V(T,S), T \cap S = \varnothing$, та множина ребер $E(T,S)$, в якому ребро $(T_q, S_p) \in E(T,S)$, якщо є загроза T_q об'єкту S_p.

Під загрозою тут будемо розуміти будь-які обставини або події, що виникають у зовнішньому середовищі та які можуть бути причиною нанесення збитків деяким об'єктам.

У свою чергу об’єкт – це категорія, що стосується сутностей, на які спрямовано загрозливу дію.



а) *б*)

Рисунок 1 – Бінарна схема «загроза» → «об’єкт»: а) дводольний граф «загроза» → «об’єкт»; б) тридольний граф із механізмами захисту)

У загальному випадку з наведеної моделі витікає необхідність застосування протидії, тобто захисту від впливу загроз, насамперед від загроз, наслідком реалізації яких може бути неприпустимо високий чи високий рівень шкоди. Такі загрози зазвичай мають комплексний, тобто одночасний вплив на декілька властивостей захищеності. Подібні загрози прийнято називати найбільш суттєвими (найбільш небезпечними).

Виявлення найбільш суттєвих загроз та високого рівня шкоди (збитків), нанесених об’єкту, є основою для визначення потрібних контрзаходів для забезпечення припустимої захищеності, необхідних для захисту засобів, підсистем, функцій захисту (узагальнюючи назвемо механізмами захисту), що дає змогу будувати відповідні моделі систем захисту.

У відповідності з відомою моделлю безпеки з повним перекриттям [4], яка будується виходячи з тези, що система безпеки повинна мати принаймні один засіб для забезпечення безпеки на кожному можливому шляху дії загрози на об’єкт, в моделі, що пропонується (рис. 1*б*), з’являється третій набір $M = \{M_1, M_2, ..., M_r, ...\}, r = 1, 2, ...$, якщо відповідає механізмам захисту. В ідеальному випадку кожен механізм M_r повинен усувати деяке ребро (T_q, S_p). На практиці ж M_r виконує функцію «бар’єру», забезпечуючи деяку міру опору спробам реалізації загрози. Включення в модель множини M перетворює граф G_{TS} у тридольний граф $G_{TMS} = (V(T, M, S), E(T, M), E(M, S))$.

З метою забезпечення підтримки рішень необхідно визначити найбільш імовірні властивості захищеності об’єктів, які порушуються внаслідок впливу загроз, тобто здійснити ідентифікацію у вигляді переліку загроз із констатацією відповідності властивостям захищеності об’єктів. Для цього потрібна певна класифікація. Визначення термінів і понять (концептів), що відносяться до якоїсь області, а також відношень між ними, є основою онтологічного підходу, що потребує враховувати різні формально-методологічні вимоги, критерії та оцінки. Серед основних із них є необхідність структурування термінів і понять та побудова інформаційної й функціональної моделей предметної області (ПдО) [5]. Зазвичай такі класифікації набувають вигляду таксономій тематичних онтологій ПдО.

Отже, основним безпековим поняттям є загроза (*Threat*), яка може викликати появу нештатних ситуацій, об'єкт захисту (*Object of safety*) та засоби (механізми) захисту (*Means/mechanisms of safety*) (рис. 2).

Рисунок 2 – Онтологія комплексу понять і зв'язків безпекового середовища

Очевидно, основною задачею, що має розв'язуватись, є вибір механізмів захисту (*Choice of safety Mechanisms*). Але при цьому на практиці зазвичай існує проблема оцінки вартості реалізації вибраних механізмів захисту та пріоритетності їх реалізації. Для цього традиційно відомим є визначення оцінки ризиків (*Risk Assessment*), яка випливає з імовірності здійснення (реалізації) загроз та рівня шкоди (збитків) від ураження об'єктів. Враховуючи важливість проведення прогностичного аналізу вразливостей об'єктів та перебігу загрозливих процесів, до комплексу понять необхідно віднести й розв'язання задач прогностичного моделювання (*Prognostic Modeling*).

3. Онтологічні описи предметної області безпекового середовища

Дослідження показують, що створення графових моделей безпекового середовища для визначення впливів різного типу загроз та захищеності об'єктів свідчить про зручність їх застосування, надаючи ефективний інструмент менеджерам і розробникам засобів захисту [6–10]. Одночасне застосування елементів онтологічних описів підвищує рівень конкретності моделі та більш чіткого уявлення щодо стану середовища. Для проведення моніторингу та аналізу безпекового середовища зазвичай використовуються експертні методи, які можуть бути підтримані відповідною базою знань, сформованою, наприклад, на основі онтологій наявних у ПдО об'єктів, можливих загроз, які можуть бути спрямовані на об'єкти, а також задіяних (у разі їх наявності) механізмів захисту [11]. Як атрибутивні характеристики концептів цих онтологій визначаються експертні оцінки цінності об'єктів (наприклад, як характеристика (рівень) збитку у разі ураження об'єкта), ймовірностей або можливостей реалізації кожної загрози та характеристик відповідних механізмів захисту (ефективності, вартості, комплексності тощо). Побудова БЗ є досить важливим заходом, адже опис об'єктів і загроз є задачею слабоформалізованою, особливо з точки зору знаходження можливих зв'язків між ними.

Щоб забезпечити експертну діяльність у виявленні можливих атак та запобіганні ним, необхідні структуровані формати для опису інцидентів. Це є серйозною проблемою, оскільки від читабельності і зрозумілості задокументованої інформації багато в чому зале-

жать успіх і ефективність вкладу експертів у процес прийняття рішень. У цьому сенсі для аналізу інформації важливу роль відіграє графічна візуалізація.

В останні десятиліття в умовах поліваріантності сценаріїв розвитку явищ і процесів вагомим інструментом підтримки прийняття рішень стали матричні методи. Цьому посприяли можливості матричних методів, пов’язані з побудовою абстрактно-логічних розумових конструкцій, проведенням розрахунків і зручною візуалізацією [12, 13]. Водночас матричні методи значною мірою корельовані і з графовими моделями.

Зазвичай отримані у процесі досліджень моделі реалізуються в інформаційних технологіях для забезпечення практичного застосування. Для комп’ютерного програмування як онтологічні моделі, так і матричне подання даних і зв’язків є достатньо зручним і наочним. Матрична методологія дозволяє увесь процес розв’язання задач прогностичного моделювання, оцінювання ризиків та прийняття рішень щодо вибору механізмів захисту представити як послідовність трансформацій пов'язаних між собою матриць, що містять дані щодо характеристик основних понять і відношень між ними.

Використовуючи цю методологію, представимо вихідні матриці загального випадку середовища безпеки онтографом, показаним на рис. 3.

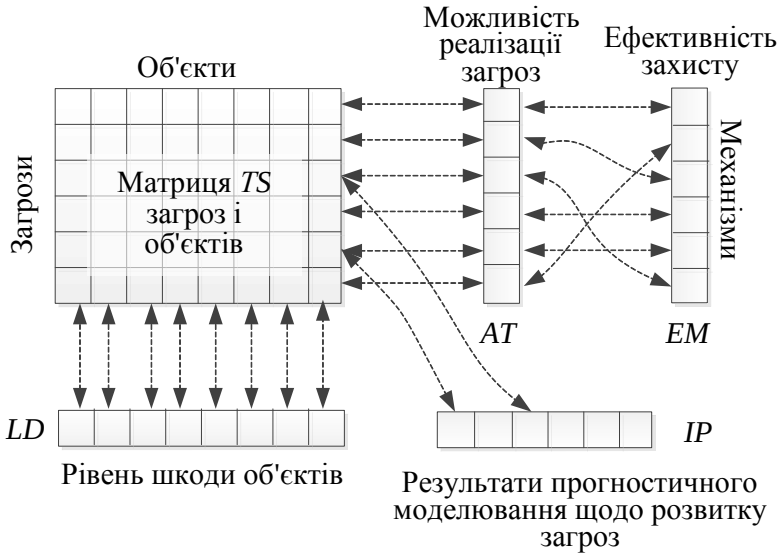


Рисунок 3 – Онтологія вихідних матриць середовища безпеки

Основною (вихідною) матрицею є матриця $||TS||_Q^P$ «загроз-об’єктів» розміром $(P \times Q)$, яка показує взаємозв’язок між цими сутностями. Також онтологія вихідних матриць включає в себе ще чотири окремих вектори характеристик: $||AT||_1^P$ – загроз, $||LD||_Q^1$ – об’єктів, $||EM||_1^R$ – механізмів захисту та $||IP||_Q^1$ – результатів прогностичного моделювання.

У процесі первинного аналізу ПдО формуються списки об’єктів, загроз і можливих механізмів захисту. Матриця $||TS||_Q^P$ є бінарною матрицею і заповнюється як матриця бісуміжності дводольного графа G_{TS}. Вектори-стовпці $||AT||_1^P$ і $||EM||_1^R$ і вектори-рядки $||LD||_Q^1$ та $||IP||_P^1$ містять значення відповідних характеристик.

Наведений підхід не є складним за своєю суттю і може бути достатньо легко реалізований відповідними програмними засобами. Проблема може полягати лише у тому, що кількість об’єктів, а також, можливо, і загроз, які потрібно досліджувати, може бути досить значною. У такому випадку побудова графа G_{TMS} є нетривіальною задачею, зважаючи

на складність зв'язків графа G_{TS}. Тому питання щодо формального опису переліку усіх об'єктів та загроз потребує окремої уваги.

Одним із підходів щодо полегшення вирішення проблеми може бути пошук на графі G_{TS} компонентів зв'язності, тобто таких його підграфів $G_i = (V_i, E_i)$, що $G_{TS} = \bigcup G_i$, але $V_i \bigcap V_j = \varnothing$ та $E_i \bigcap E_j = \varnothing$, $i, j = 1, 2, ..., i \neq j$, у той час як у будь-якому G_i будь-які вершини u та v з'єднані простим ланцюгом. Для знаходження компонент зв'язності можливо застосувати відомі алгоритми пошуку у глибину і пошуку в ширину, використання механізмів рекурсії, фарбування вершин або ребер тощо [14].

У разі, якщо граф зв'язний, ці ж алгоритми у процесі свого виконання знаходять розділяючі ребра, так звані «мости», що з'єднують двозв'язні блоки графа [15]. У цьому випадку вершина графа (з числа загроз одного із блоків), яка інцидентна ребру моста, розділяється на дві вершини. Новостворена вершина з'єднується з другим блоком у другій вершині моста, а саме ребро моста видаляється. Таким чином, блоки графа перетворюються у компоненти зв'язності без порушення початкових відносин між загрозами і об'єктами у графі G_{TS}.

У результаті таких перетворень будується блочно-діагональна матриця [16], що відповідає цьому графу, в якій кожний матричний блок буде матрицею бісуміжності $\| TS_i \|_{Q_i}^{P_i}$ відповідної дводольної компоненти зв'язності, де Q_i та P_i – відповідно кількість об'єктів і загроз, які на них націлені, у підграфі G_i.

Тепер, розглядаючи отримані підграфи G_i, які як частини графа G_{TS} поступаються йому за розміром, визначення необхідних механізмів захисту з набору M, очевидно, значно спрощується.

Треба зауважити, що сильна зв'язність графа G_{TS} (якщо спочатку у ньому немає декількох компонентів зв'язності або мостів) не є обмеженням для застосування запропонованого підходу. У такому випадку можна застосувати нескладний алгоритм знаходження реберних розрізів графа шляхом підсумовування по модулю 2 відповідних рядків матриці бісуміжності, а далі з кінцевими вершинами ребер розрізу діяти аналогічно вершинам мосту.

4. Рішення щодо оцінювання параметрів і характеристик загроз, збитків і ризиків

Застосування кількісних методів експертного оцінювання, що потребує необхідності чіткого математичного та логічного обґрунтування, нерозривно пов'язане з поєднанням теоретичного розуміння проблеми і набору евристичних правил для її вирішення. Як показує практика, універсальних евристичних правил і практичних прийомів не існує. Правила, вироблені на основі знань, специфічних для певної ПдО, є, зазвичай, ефективними лише у споріднених галузях.

Рішення щодо вибору і оцінювання параметрів і характеристик загроз, збитків і ризиків, яке пропонується на основі вищенаведеної формалізованої моделі, передбачає:

1) вибір і співвіднесення вимірювальних шкал;

2) оцінювання відносного рівня збитків від реалізації атак на основі відносної цінності ресурсів;

3) оцінювання можливості здійснення загроз;

4) оцінювання ризиків від реалізації загроз;

5) вибір механізмів захисту, виходячи із сутності загроз і відповідної функціональності механізмів захисту.

У відповідності з запропонованим підходом на основі побудованої графової моделі захищеного середовища експертами здійснюються формування вихідних матриць і попе-

редній вибір механізмів захисту за схемою, показаною на рис. 4. Матриці призначені для опису зв'язків між елементами графової моделі.

Граф G_{TS} описується матрицею TS, виділені компоненти зв'язності (підграфи G_i) описуються матрицями TS_i. Далі на основі онтологічного опису механізмів захисту шляхом їх добору з урахуванням заданих загроз формується матриця *TM*.

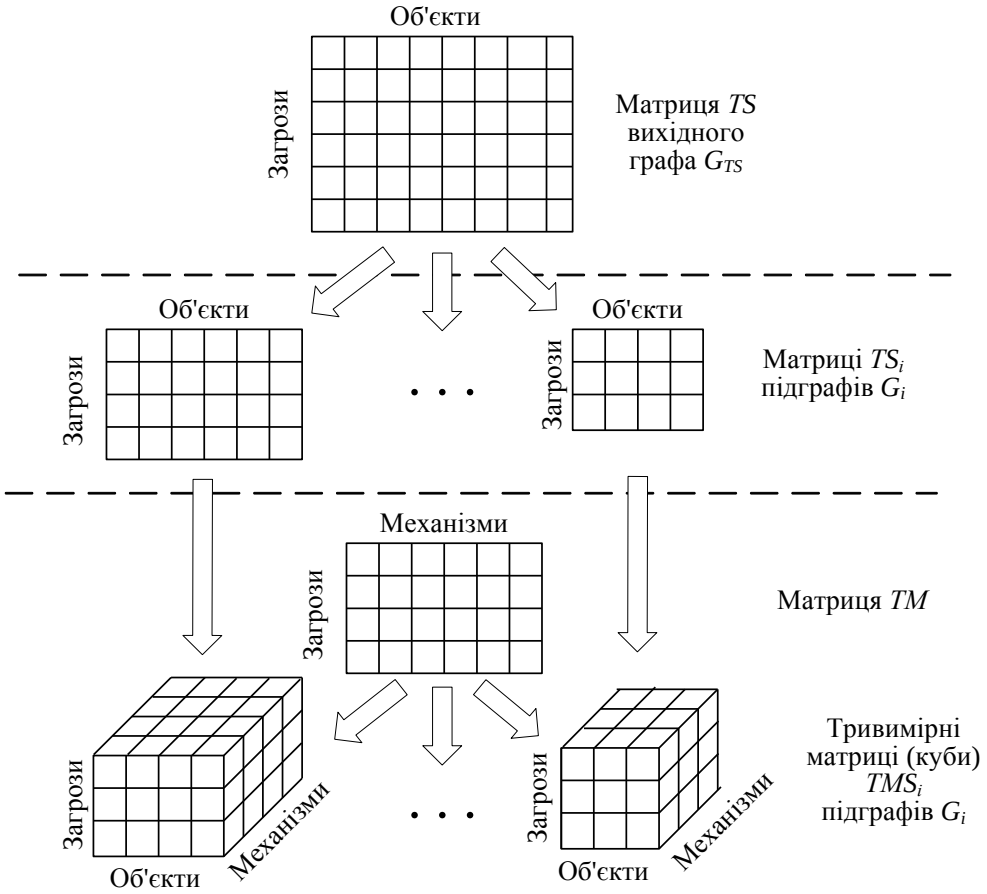


Рисунок 4 – Матричні трансформації на основі графової моделі

Наступним кроком є побудова тридольних графів компонентів зв'язності з урахуванням запропонованих механізмів захисту та опис їх відповідними тривимірними матрицями (кубами) TMS_i.

Процес проведення подальших розрахунків оцінювання ризиків на основі матричного подання показано на рис. 5.

Для розрахунків використовуються вектори характеристик загроз, об'єктів, механізмів захисту, а також результатів прогностичного моделювання. Різноманітні кількісні і якісні оцінки цих характеристик переводяться експертами до кількісного (бального) виміру за певними умовними схемами. Наприклад, можливості здійснення загроз подаються за такою схемою: незначна можливість – 1 бал, низька – 3, висока – 7, дуже висока – 9 балів. Для оцінок збитку (рівень шкоди) об'єктів більш доцільно використовувати іншу бальну шкалу: низький збиток – 20 балів, середній – 50, високий – 70, неприпустимо високий – 90 балів; відповідно для оцінки ефективності механізмів захисту: середня – 50, висока – 70, значна – 90, що відповідає поданню у відсотках. Результати прогностичного моделювання доцільно представити у вигляді коефіцієнтів k_h підвищення стійкості системи об'єктів захисту у разі застосування певних організаційно-технічних заходів протидії щодо можли-

вого майбутнього розвитку загроз [2]. Інтервал значень коефіцієнтів k_h, що характеризують важливість заходів для підвищення захищеності ресурсів, встановлюється від 0,9 (дуже висока важливість) до 0,1 (низька важливість). Якщо на етапі прогностичного моделювання певні заходи визначити не вдалося, $k_h = 0$.

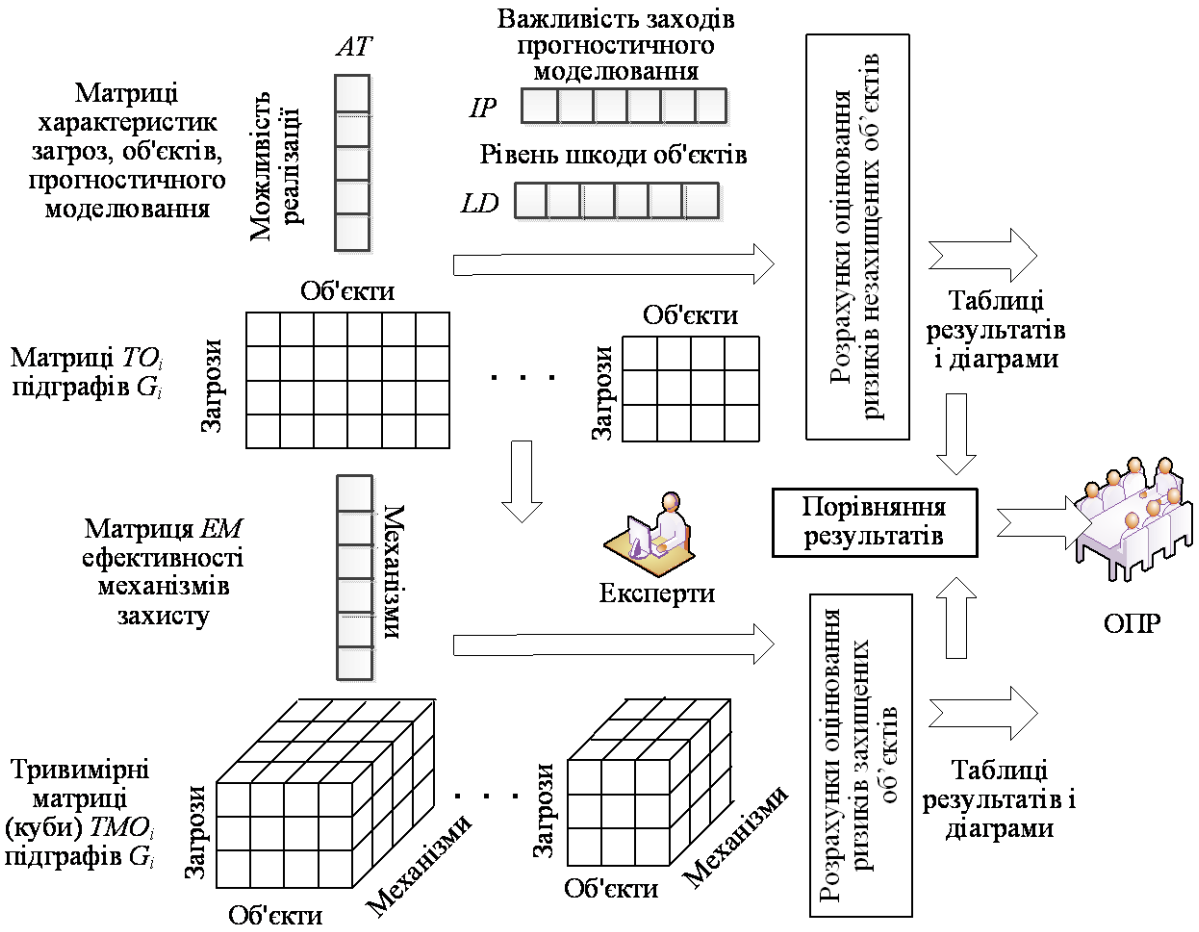


Рисунок 5 – Матричне подання розрахунку оцінювання ризиків

Розрахунки проводяться для кожного підграфа на основі матриць TS_i для з'ясування рівня ризику незахищених об'єктів.

Спочатку обчислюється вектор $\| CTS_i \|_1^Q$ сумарної оцінки можливості здійснення усіх загроз для кожного об'єкта підграфа G_i:

$$\| CTS_i \|_1^Q = (\| TS_i \|_{Q_i}^{P_i})^{\mathrm{T}} \times \| AT \|_1^{P_i}, \qquad (1)$$

де символ «$^{\mathrm{T}}$» означає транспонування матриці.

Після цього вектор $\| CTS_i \|_1^Q$ нормується і в результаті отримуємо вектор ${}^{\mathrm{N}}\| CTS_i \|_1^Q$.

Далі обчислюється вектор $\| RTS_i \|_{Q_i}^1$ відносних оцінок ризиків по кожному об'єкту підграфа G_i як добуток Адамара нормованого вектора ${}^{\mathrm{N}}\| CTS_i \|_1^Q$ на підвектор $\| LD \|_{Q_i}^1$ оцінок можливих збитків по кожному об'єкту цього підграфа:

$$\| RTS \|_{Q_i}^1 = ({}^{\mathrm{N}}\| CTS_i \|_1^{Q_i})^{\mathrm{T}} \circ \| LD \|_{Q_i}^1 . \qquad (2)$$

Відносний ризик R_i підграфа G_i буде дорівнювати сумі елементів вектора $\| RTS \|^1_{Q_i}$, нормованої по всіх таких векторах:

$$R_i = \oplus \| RTS_i \|^1_{Q_i} / \sum_i \oplus \| RTS_i \|^1_{Q_i}, \quad (3)$$

де $\oplus$ означає підсумовування елементів вектора.

На підставі цих даних, а також результатів прогностичного моделювання робиться висновок щодо пріоритетності застосування механізмів захисту для відповідних об'єктів від націлених на них потенційних загроз.

Тридольні графи на базі підграфів G_i будуються експертним шляхом. Їм відповідають тривимірні матриці $\| TMS_i \|^{Q_{i_{R_{i_{P_i}}}}}$, з яких виділяються вектори $\| MS_i \|^1_{Q_i}$, які, з використанням вектора $\| EM \|^R_1$, заповнюються значеннями $\left(1 - \frac{F_r}{100}\right)$, де F_r – ефективність r-го механізму захисту. Також, з використанням вектора *IP*, створюються вектори $\| IPS_i \|^1_{Q_i}$ з відповідними елементами $(1 - k_h)$ для кожного підграфа G_i.

Після цього обчислюється вектор $\| RTMS_i \|^1_{Q_i}$ відносних оцінок ризиків по кожному об'єкту підграфа G_i з урахуванням механізмів захисту:

$$\| RTMS_i \|^1_{Q_i} = \| RTS_i \|^1_{Q_i} \circ \| MS_i \|^1_{Q_i}. \quad (4)$$

Сума елементів вектора $\| RTMS_i \|^1_{Q_i}$, нормована по всіх таких векторах, дозволяє обчислити відносний ризик RM_i підграфів G_i з урахуванням застосування механізмів захисту:

$$RM_i = \frac{\oplus \| RTMS_i \|^1_{Q_i}}{\sum_i \oplus \| RTMS_i \|^1_{Q_i}}. \quad (5)$$

Для повноти картини щодо оцінок ризиків по кожному об'єкту доцільно провести уточнення цих оцінок на основі коефіцієнтів підвищення стійкості об'єктів захисту, отриманих у результаті прогностичного моделювання, а саме:

$$\| PRTMS_i \|^1_{Q_i} = \| RTMS_i \|^1_{Q_i} \circ \| IPS_i \|^1_{Q_i}. \quad (6)$$

Такий підхід можна застосувати й для уточнення RM_i.

Отримані результати за виразами (3), (5), (6) порівнюються між всіма підграфами. Таке порівняння дозволяє визначити пріоритетність застосування (закупівель) окремих механізмів і поступового формування системи захисту.

Результати розрахунків можуть бути представлені у вигляді таблиць, а також різного виду діаграм, що є зручним для аналізу особами, що приймають рішення.

5. Можливі варіанти створення технологічного інструментарію проведення обчислень

Відомо, що здатність виконувати експертний аналіз – це не тільки питання наявності певних знань і рівня кваліфікації. Для цього потрібно мати й дуже специфічні навички й уміння розібратися в конкретній ситуації в даній предметній області. Але в сьогоднішніх умовах і цього може бути недостатнім для вироблення ефективного рішення. Тому вже стало

звичайною практикою застосування експертами для підтримки діяльності засобів інформаційних технологій.

На сьогодні визначено декілька типів систем, що можуть використовуватись для підтримки підготовки рішень експертами, починаючи від експертних систем і до використання програмних інструментів, які в основному спираються на вичерпну інформаційну підтримку розгляду проблем, візуалізацію процесу пошуку рішення та результатів, а також на застосування певних математичних моделей.

У цьому сенсі інструментарій реалізації підходу, що пропонується, доцільно віднести до розрахункових інформаційно-аналітичних систем (ІАС), в яких забезпечується аналіз інформації шляхом проведення функціональних розрахунків і подання результатів в аналітичній формі (графіки, діаграми, тощо) з метою підтримки прийняття рішень. Основним завданням ІАС є ефективне зберігання, обробка та аналіз даних (інформації).

Масштаби реалізації ІАС залежать від розмірів інфраструктури ПдО, аналіз захищеності якої проводиться, та відповідно до обсягів необхідних даних. Для задач підтримки прийняття рішень у ПдО з незначними характеристиками для інформаційної системи цілком достатнім може бути використання комплексу готових програмних застосунків, наприклад, офісних програм пакета Ms Office – Word, Excel, Visio, PowerPoint (рис. 6), або засобів матричної системи MATLAB, яка є зручним інструментом для проведення числових науково-технічних обчислень та їх графічної візуалізації. Наявність у MATLAB мови програмування та можливість під'єднувати різні пакети розширення дозволяють створювати у цьому середовищі завершені програмні засоби.

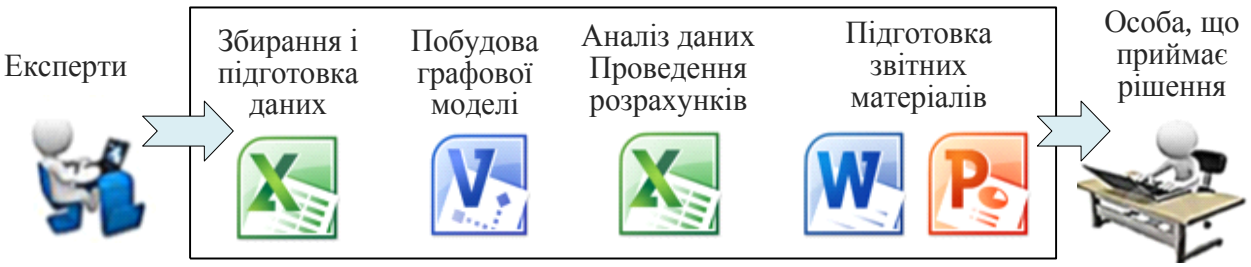


Рисунок 6 – Реалізація інформаційної системи підтримки прийняття рішень за допомогою офісних застосунків

Для великих розгалужених структур необхідним є створення спеціальної ІАС. Структура комплексу програмного забезпечення подібної ІАС показана на рис. 7. Поділ структури на зазначені підсистеми обумовлений об'єднанням у них програмних модулів схожої функціональності.

Як правило, системи створюються на базі ПЗ, що вільно розповсюджується. Клієнтське ПЗ ІАС має відповідати таким основним вимогам:

- функціонування в середовищі операційної системи Windows або сімейства Linux;
- зручний користувацький інтерфейс;
- реалізація експорту даних у текстовому форматі та в форматі електронної таблиці;
- реалізація формування і виведення друкованих звітних форм;
- реалізація всіх функцій щодо оцінювання ризиків ураження середовища.

Центральною частиною ІАС є розрахунково-аналітична підсистема, яка виконує інформаційно-довідкову, розрахункову та аналітичну підтримку прийняття рішень, формування аналітичної та статистичної звітності. Інші підсистеми комплексу взаємодіють із нею під керуванням підсистеми координації і взаємодії експертів, у завдання якої входять управління доступом до інформаційних ресурсів системи, забезпечення безпеки при взаємодії, реєстрація та облік роботи експертів та інших користувачів, формування експертних груп, забезпечення електронного документообігу між експертами.

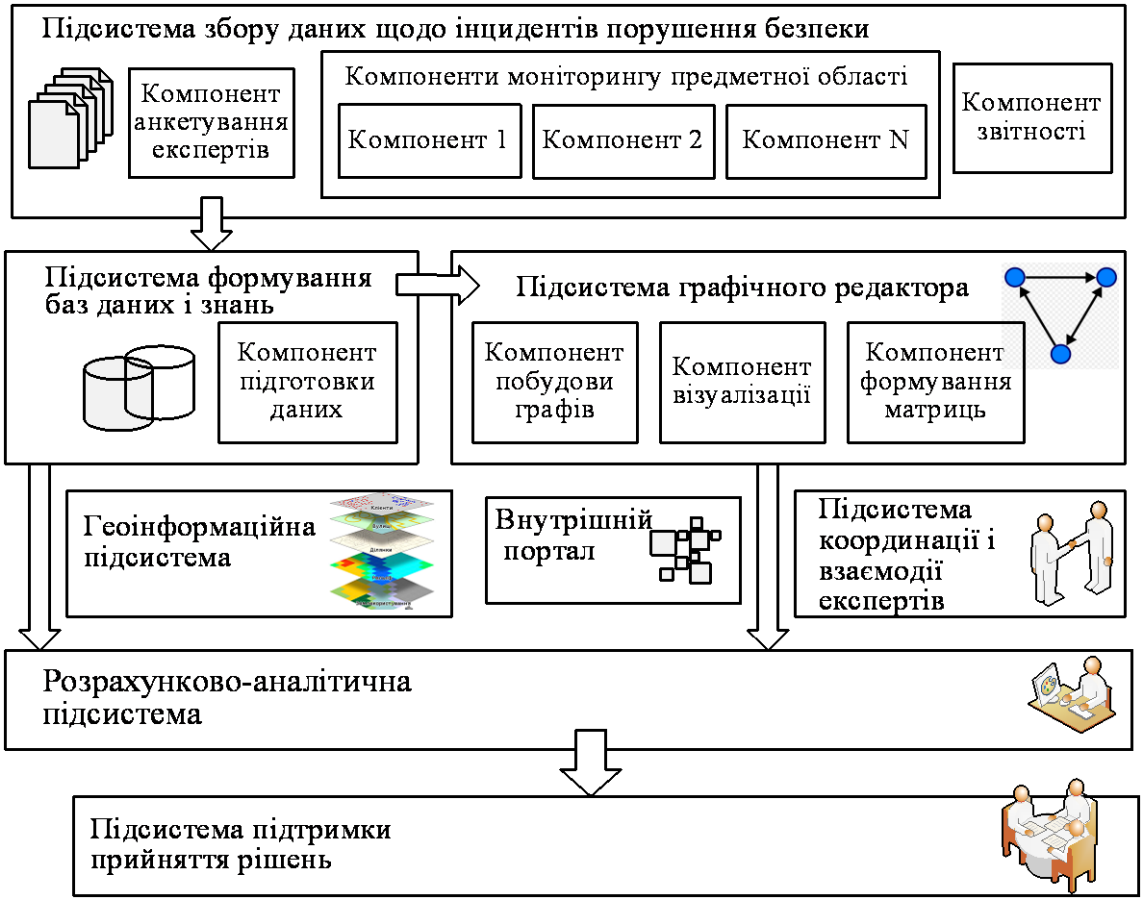


Рисунок 7 – Структура комплексу програмного забезпечення ІАС

Розрахунково-аналітична підсистема реалізується за принципами експертних систем, що передбачають використання бази знань, яка визначає судження експертів за наборами фактів через модуль зіставлення. Розрахункові операції можуть виконуватися як в автоматичному, так і в покроковому напівавтоматичному режимі (з підтвердженням користувача).

Внутрішній портал підтримує довідково-інформаційне обслуговування експертів та зацікавлених осіб, а також оперативний інформаційний обмін між експертами під час групової роботи. Також для забезпечення вичерпного інформування експертів щодо просторового розміщення об’єктів та можливих джерел загроз доцільно використовувати геоінформаційну підсистему.

Сучасним засобом подолання проблем, пов’язаних із використанням стандартного ПЗ, апаратних ресурсів та забезпеченням безпеки, є використання дата-центрів та архітектур хмарних обчислень, в яких реалізується сервіс-орієнтована організація підтримки ресурсів та застосовуються високопродуктивні платформи обчислювальної та комунікаційної техніки з резервуванням критично важливих елементів. Це забезпечує надійність зберігання інформації, високий рівень доступності, захищеності інформації, простоту нарощування нових ресурсів, нижчу сукупну вартість володіння інформаційною системою [17].

6. Висновки

У дослідженні показано, що в умовах збільшення агресивних проявів завдання створення методик підтримки прийняття рішень щодо упередження атак в автоматизованому режимі і визначення пріоритетності побудови системи захисту є актуальним. Метод, що пропонується, базується на графовій моделі бінарної протидії «загроза» → «об’єкт» та відомій мо-

делі безпеки з повним перекриттям, що дозволяє забезпечити процес вибору відповідних механізмів захисту. Одночасне застосування елементів онтологічних описів підвищує рівень конкретності методу та більш чіткого уявлення щодо стану середовища.

Запропоновано підхід щодо матричного подання даних і зв'язків, який, як і онтологічні моделі, є достатньо зручним і наочним для комп'ютерного програмування. Методологія використання матриць дозволяє увесь процес розв'язання задач прогностичного моделювання, оцінювання ризиків та прийняття рішень щодо вибору механізмів захисту представити як послідовність трансформацій пов'язаних між собою матриць, що містять дані щодо характеристик основних понять і відношень між ними.

Запропоновано можливі варіанти створення ІТ-інструментарію для реалізації процесів підтримки прийняття рішень.

Практична цінність полягає у розробці методу, який може стати базовим при проєктуванні захищеного середовища з системами захисту від найбільш непередбачуваних атак «нульового дня». Метод може бути використаним у будь-яких галузях діяльності, зокрема, у сферах оборонного планування, надзвичайних ситуацій і у відповідних ситуаційних центрах.

СПИСОК ДЖЕРЕЛ

1. Качмар О.В. Агресія як соціальний феномен. *Нова парадигма.* 2014. Вип. 125. С. 197–205.
2. Шевченко В.Л., Нестеренко О.В., Нетесін І.Є., Шевченко А.В. Прогностичне моделювання комп'ютерних вірусних епідемій: монографія / за ред. В.Б. Поліщука. Київ: УкрНЦ РІТ, 2019. 152 с.
3. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / Інститут проблем національної безпеки; Національна академія Служби безпеки України. Київ, 2004. 472 с.
4. Нестеренко О.В. Безпека інформаційного простору державної влади. Технологічні основи. Київ: Наукова думка, 2009. 352 с.
5. Хоффман Л.Дж. Современные методы защиты информации / пер. с англ. Москва: Советское радио, 1980. 264 с.
6. Палагин А.В., Петренко Н.Г. К вопросу системно-онтологической интеграции знаний предметной области. *Математичні машини і системи.* 2007. № 3, 4. С. 63–75.
7. Хнигічева А.М., Новіков О.М., Тимошенко А.О. Моделювання безпеки складних інформаційно-комунікаційних систем із використанням логіко-ймовірнісного методу. *Наукові вісті Національного технічного університету України Київський політехнічний інститут*. 2010. Вип. 6. С. 70–77.
8. Нестеренко А.В., Нетесин И.Е. Графовая модель кибербезопасности информационных ресурсов. *Проблемы управления и информатики*. 2020. № 4. С. 91–108.
9. Nesterenko A.V., Netesin I.E. Cybersecurity graph model of information resources**.** *Journal of automation and information sciences.* 2020. N 52 (8). P. 14–31. DOI: 10.1615/ JAutomatInfScien.v52.i8.20.
10. Böhm F., Menges F., Pernul G. Graph-based visual analytics for cyber threat intelligence. *Cybersecurity*. 2018. Vol. 1. Article number 16. SpringerOpen. URL: https://cybersecurity.springeropen.com/articles/10.1186/s42400-018-0017-4.
11. Nesterenko O., Netesin I., Polischuk V., Trofymchuk O. Development of a procedure for expert estimation of capabilities in defense planning under multicriterial conditions. *Eastern-European Journal of Enterprise Technologies.* 2020. N 4/2 (106). P. 33–43. DOI: 10.15587/1729-4061.2020.208603.
12. Wang X., Meng Y. and etc. A Simple Three-Dimensional Matrix Method for Global Constellation Intrasatellite Link Topological Design. *International Journal of Navigation and Observation*. 2014. Article ID 502158. 17 p. DOI:10.1155/2014/502158.
13. Штангрет А.М. Теоретико-методологічні аспекти забезпечення економічної безпеки підприємств авіаційної галузі. *Ефективна економіка.* 2011. № 6. URL: http://www.economy.nayka.com.ua/?op=1&z=581.
14. Рейнгольд Э., Нивергельт Ю., Део Н. Комбинаторные алгоритмы. Теория и практика / пер. с англ. М.: Мир, 1980. 478 с.
15. Харари Ф. Теория графов / пер. с англ. М.: Мир. 1973. 302 с.

16. Гантмахер Ф.Р. Теория матриц. 5-е изд. М.: Физматлит, 2004. 560 с.
17. Поліщук В.Б., Нетесін І.Є., Нестеренко О.В. Інформаційні технології в управлінні оборонними ресурсами: методологічний контекст та приклади практичної реалізації. Ч. 1: монографія / за ред. В.Б. Поліщука. Київ: УкрНЦ РІТ, 2019. 120 с.

Стаття надійшла до редакції 12.08.2021