1 Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації. Метрологічне забезпечення системи ТЗІ. Стандартизація, сертифікація та випробовування засобів ТЗІ

УДК 621.3.06

МОДЕЛЬ МІКРОСТРУКТУРИ ДІЯЛЬНОСТІ З ЗАХИСТУ ІНФОРМАЦІЇ

Олександр Потій
ЗАТ „Інститут інформаційних технологій”

Анотація: **Розглядається процедура розробки мікроструктури діяльності. На прикладі процесів аналізу ризиків розроблена нормативна модель структури діяльності із захисту інформації на мікрорівні у складі моделей типу «ціль-результат», «ціль-процес», функціональних моделей та моделей предметної області аналізу ризиків.**
Summary: **Procedure of activity microstructure development is considered. Examples of normative models for security activity structure (as an integral part of aim-result, aim-process and functional models) on micro level for risk analyses processes are developed.**
Ключові слова: **Процесний підхід, діяльність із захисту інформації, модель діяльності, процес захисту інформації.**

Вступ

Застосування процесного підходу до захисту інформації висуває вимогу щодо розроблення формальних моделей діяльності із захисту інформації. У роботах [1, 2] запропоновано здійснювати моделювання структури діяльності на макро- та мікрорівні. Макроструктура діяльності представляє собою структуру верхнього рівня та визначається множиною процесів захисту інформації і встановленими на цій множині відношеннями. Макроструктура – це по суті метамодель, яка описує діяльність із захисту інформації (ДЗІ) в цілому та характеризує взаємовідношення процесів захисту інформації (ПЗІ). Мікроструктура діяльності розкриває внутрішню будову ДЗІ, встановлює призначення та містить функціональну модель кожного ПЗІ. На сьогодні в існуючих нормативних документах та стандартах [3 – 9] визначається тільки множина заходів захисту інформації. Для впровадження цих заходів у практику захисту інформації необхідно визначити структуру діяльності із захисту інформації, що є актуальною науково-технічною задачею. На жаль на цей час не визначені процедури моделювання діяльності із захисту інформації і, як наслідок, не визначена структура такої діяльності. У даній роботі автор пропонує процедуру розробки мікрострукри діяльності, а також структуру процесів захисту інформації.

Стаття присвячена вирішенню задачі синтезу нормативної моделі діяльності із захисту інформації та визначення складу і структури (на мікрорівні уявлення) діяльності із захисту інформації. Результати, що викладені у статті, формують теоретичні основи процесного підходу до захисту інформації.

І Процедура розробки мікроструктури діяльності із захисту інформації

Формалізована модель мікроструктури діяльності із захисту інформації являє собою формальну конструкцію виду

$$\grave{I}_{SI}^{micro} = \left\langle \grave{I}_{\ddot{I}\ddot{I}}, \grave{I}_{\ddot{O}\ddot{I}}, \mathrm{G}_{\ddot{I}}, \grave{I}_{\ddot{O}\eth}, \grave{I}_{\hat{O}} \right\rangle, \qquad (1)$$

де $\grave{I}_{\ddot{I}\ddot{I}}$ – модель предметної області родини процесів захисту інформації;

$\grave{I}_{\ddot{O}\ddot{I}}$ – модель типу «ціль – процес» (ЦП-модель), що відображає взаємозв’язок між цілями та процесами;

$G_{\ddot{I}}$ – ієрархічна модель процесів (операцій, дій) захисту інформації;

$\grave{I}_{\ddot{O}\eth}$ – модель типу «ціль – результат» (ЦР-модель), що відображає взаємозв’язок між цілями та

результатами захисту інформації;

$\grave{I}_{\hat{O}}$ – функціональна модель процесів захисту інформації.

Призначення моделей та їх детальний опис, що входять до складу (1), розглядаються у роботі [1]. Для розробки мікроструктури діяльності із захисту інформації пропонується використовувати процедуру, що складається з чотирьох етапів (рис. 1).

Етап 1. На цьому етапі розробляється модель предметної області процесу ЗІ, що є сукупністю інформаційно-понятійних діаграм. Під час моделювання з'ясовують сутність концептів, що входять до предметної області, уточнюються визначення та встановлюються логічні відношення між концептами. Моделювання дозволяє дослідникові точніше уявити предметну область діяльності із ЗІ, що знижує помилки під час визначення цілей, результатів та змісту процесів захисту інформації.

Етап 2. На другому етапі рекомендується розробити модель типу «ціль-процес» та ієрархію процесів захисту інформації. Під час моделювання формулюються основні цілі діяльності та визначаються процеси ЗІ, що мають бути здійснені для досягнення цих цілей. Для формування цілей рекомендується застосовувати нормативні документи [2 – 9]. Паралельно розробляється ієрархічна модель ПЗІ (дерево процесів), тобто здійснюється декомпозиція процесів на складові елементи.

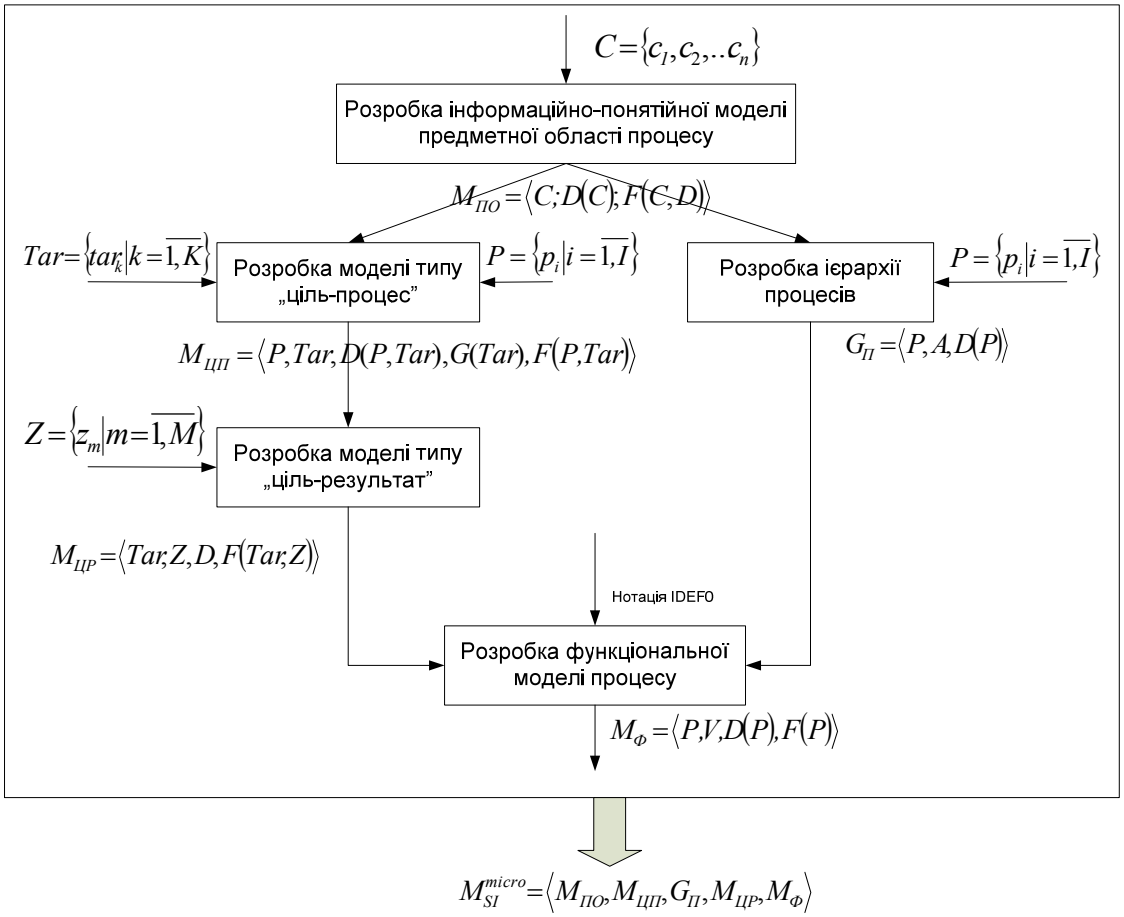


Рисунок 1 – Процедура розробки мікроструктури діяльності із захисту інформації

Етап 3. На третьому етапі розробляється модель типу «ціль-результат». Розробник по суті має здійснити декомпозицію цілей, що визначені на попередньому етапі, та встановити бажані вимірювальні результати діяльності.

Етап 4. На четвертому етапі, використовуючи результати попереднього моделювання, формується структура процесу ЗІ, тобто розробляється його функціональна модель. Під час розробки функціональної моделі здійснюється уточнення цілей та результатів діяльності, а також декомпозиція процесів ЗІ. Розробкою функціональної моделі закінчується формування мікроструктури діяльності із захисту інформації.

II Модель класу основних процесів захисту інформації

Всі процеси захисту інформації на макрорівні пропонується розділити на п’ять класів:

- клас процесів управління безпекою (**M**-процеси);
- клас основних процесів захисту інформації (**S**-процеси);
- клас організаційних процесів (**O**-процеси);
- клас процесів удосконалення (**I**-процеси);
- клас допоміжних процесів (**A**-процеси).

Основні процеси захисту інформації об’єднуються у три родини: родина процесів аналізу ризиків – SAR, родина процесів інжинірінга безпеки – SEN та родина процесів надання гарантій безпеки – SAS.

Процеси аналізу ризиків безпеки спрямовані на виявлення, ідентифікацію та оцінювання загроз безпеки, вразливостей будь-якого типу (операційних або технічних), які існують в організації або в ІТС, оцінювання можливих втарт від порушення безпеки інформації. Процеси цієї родини формують основні цільові чинники діяльності із захисту інформації.

Процеси інжинірингу безпеки разом з іншими інженерними дисциплінами (інжиніринг програмного забезпечення, інжиніринг бізнес-процесів, проектування ІТС тощо) визначають зміст практичної діяльності із захисту інформації та впроваджують заходи захисту інформації, що запобігають реалізації загроз безпеки, спрямовані на відновлення функціонування систем та усунення негативних наслідків порушення безпеки тощо.

Нарешті процеси надання гарантій безпеки спрямовані на формування доказів або свідчень щодо повноти, коректності та якості запроваджених заходів захисту інформації та реалізованих систем (засобів) захисту інформації. Результати виконання цих процесів формують основу довіри суб’єктів захисту інформації до надійності захисту інформації.

Всі разом ці родини процесів спрямовані на досягнення головної мети – зниження ризиків безпеки та забезпечення бажаного рівня безпеки інформації. Базові концепти та відношення предметної області S-процесів представлені у вигляді інформаційно-понятійної (концептуальної) моделі на рис. 2.

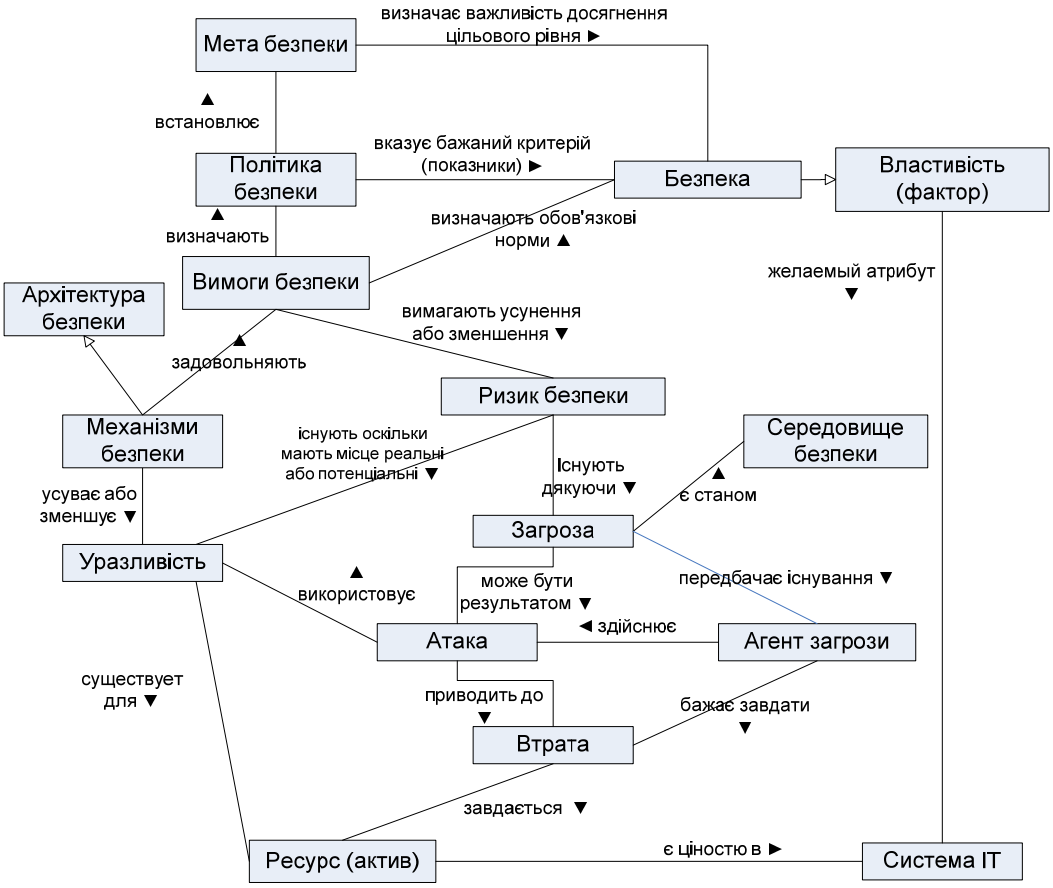


Рисунок 2 – Концептуальна модель предметної області S-процесів

Цілі безпеки визначають важливість досягнення цільового рівня безпеки. Політика безпеки інституціоналізує головну мету та відповідні задачі захисту інформації шляхом закріплення бажаних критеріїв безпеки. Вимоги безпеки специфікують політику безпеки шляхом встановлення конкретного рівня захищеності в термінах критеріїв та показників захищеності (безпеки). Вимоги безпеки вимагають усунення або зниження рівня ризиків захищеності. Ці ризики безпеки є наслідком реалізації загроз шляхом здійснення агентами загроз конкретних атак на активи, що захищаються. Вимоги безпеки задовольняються шляхом запровадження відповідних механізмів захисту, які усувають вразливості.

Використовуючи нотацію стандарту IDEF0 [10] була розроблена функціональна модель основних процесів захисту інформації, що надана на рис. 3. Розглянемо більш детальніше структуру основних процесів захисту інформації.

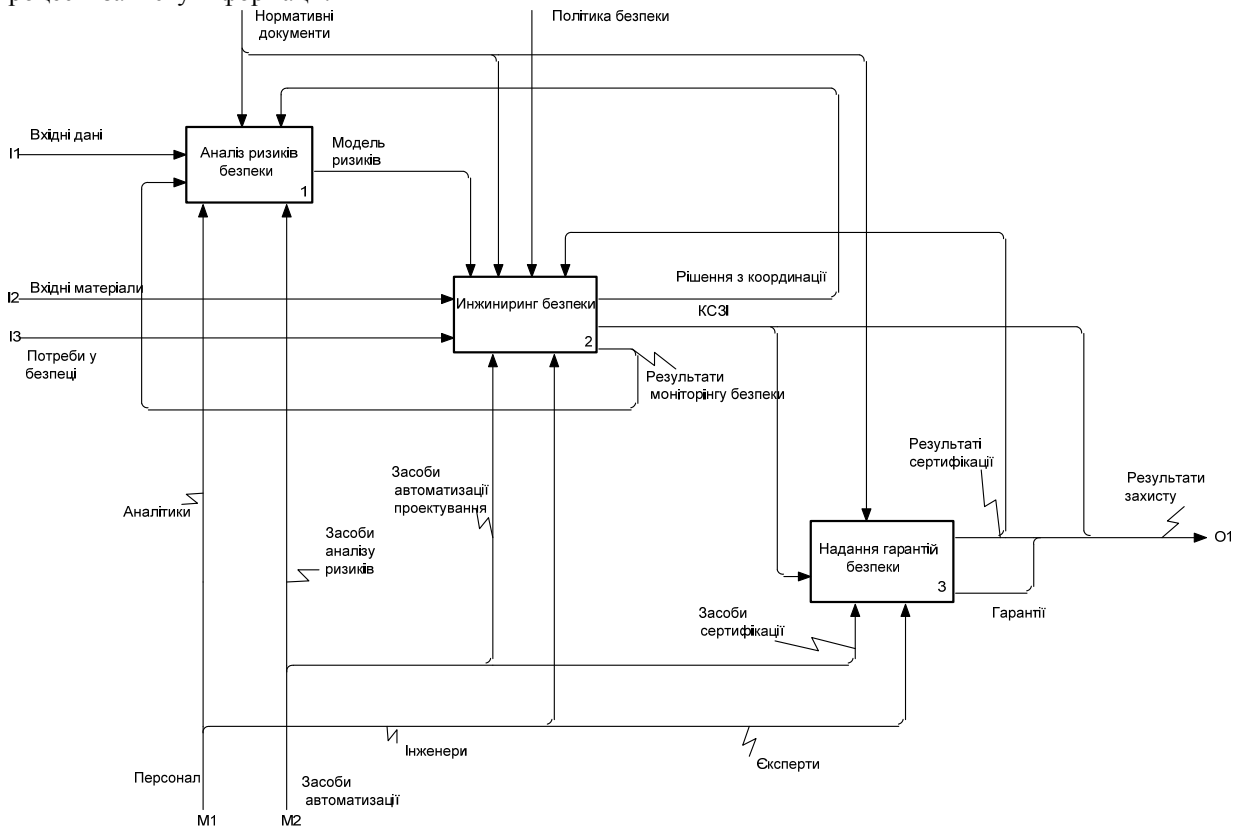


Рисунок 3 – Структура класу основних процесів захисту інформації

III Модель родини процесів SAR «Аналіз ризиків»

Модель предметної області родини процесів SAR. Родина процесів аналізу ризиків складається з процесів ЗІ, які спрямовані на оцінювання рівня загроз безпеки, вразливостей та можливих втрат від порушення безпеки інформації. Модель предметної області родини SAR наведена на рис. 4. Фокус ІП-діаграми складають концепти «ризик-актив-втрата-інцидент безпеки».

Актив – інформація та ресурси системи, які мають певну цінність для власника активу та підлягають захисту (рис 5). Актив потребує захисту, тому що він є потенційним об'єктом атаки або існує ймовірність настання небезпечної події, в результаті якої може бути нанесена шкода активу. Необхідно розрізнювати таки типи активів: інформаційні ресурси; компоненти програмного забезпечення; компоненти апаратного забезпечення; програмно-апаратні компоненти; людські ресурси; організаційні активи тощо.

Загроза – це ситуація (стан), яка підвищує ймовірність реалізації однієї або декількох атак (рис. 6). У системі та середовищі безпеки потенційно існують загрози та інші небезпечні події. Під загрозою ми розуміємо події, джерелом яких є людина (агент загроз). Настання небезпечної події може призвести до нещасного випадку, а реалізація загрози – є атакою агента загроз. Загроза передбачає існування одного або декількох агентів загроз – тобто осіб або програм (процесів), яки реалізують конкретну атаку, а також наявність спеціальних умов або станів системи, що впливають на мотивацію та можливості агента загроз щодо зловживання активами або нанесення їм шкоди. Таким чином, загроза – це умова реалізації атаки. Небезпечна подія може привести до настання нещасного випадку. Небезпечна подія пов'язана з

факторами, що не залежать від зловмисних дій людини (рис. 7).

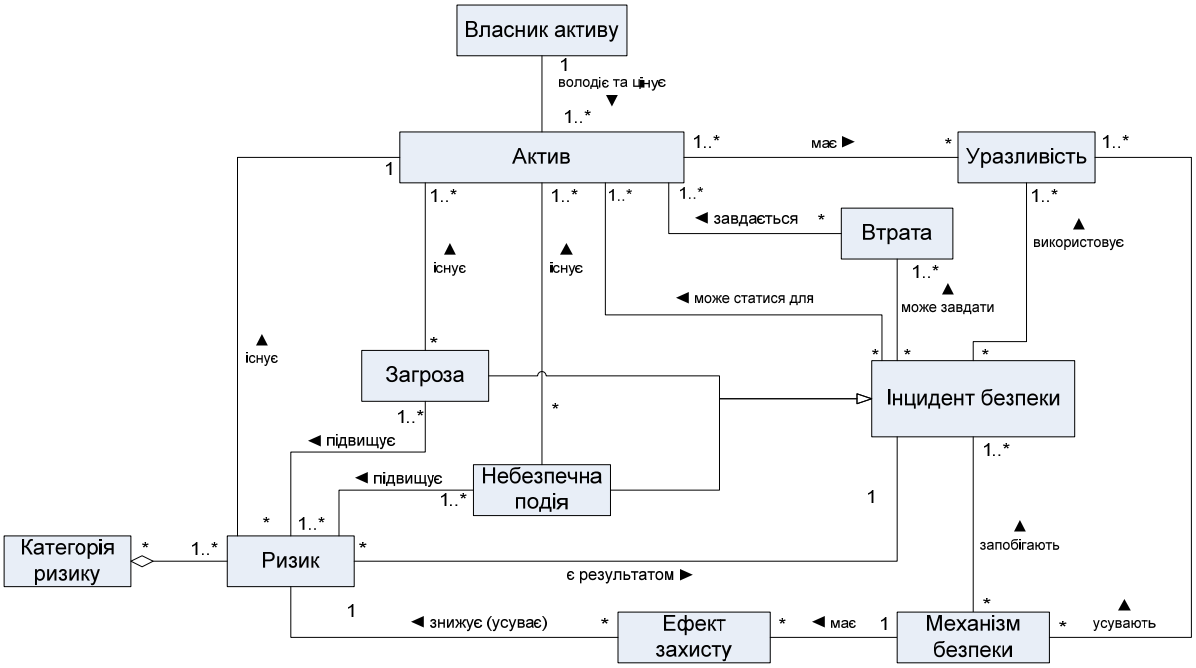


Рисунок 4 – Концептуальна модель предметної області родини SAR

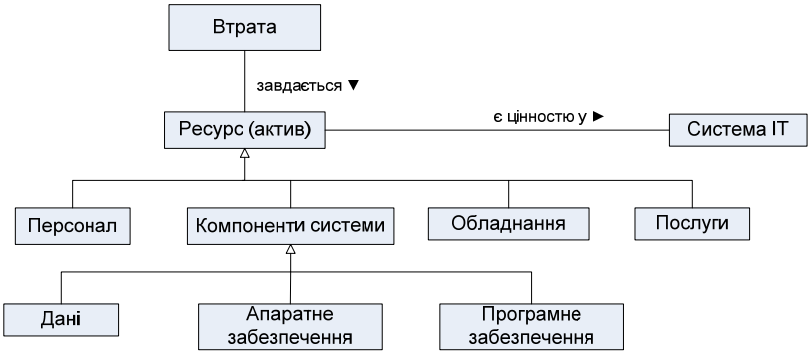


Рисунок 5 – IP-діаграма поняття ресурс (актив)

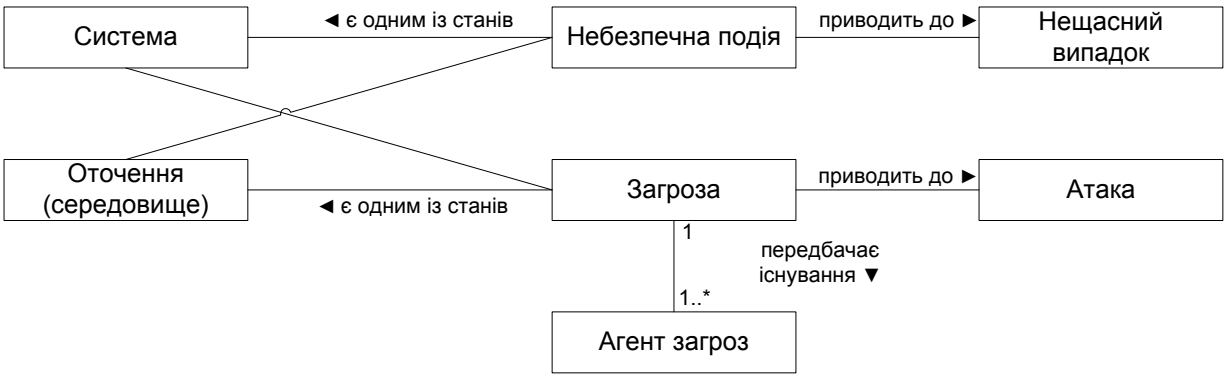


Рисунок 6 – IP-діаграма понять «небезпечна подія – загроза»

Втрата – це негативний вплив на актив, що є наслідком настання інциденту безпеки.

Інцидент безпеки – небажана подія або сукупність подій, настання яких, як наслідок, приводить до зниження цінності (пошкодження) активу (рис. 8). Інцидент безпеки – це комплексна подія, яка міститься в настанні нещасного випадку та здісненні атаки, супроводжується втратами та використанням вразливостей безпеки.

Вразливість – це властивість деякого об'єкту (системи, засобу, процесу), яка може бути використана агентом загрози (зловмисником) для здійснення цілеспрямованої атаки, або яка є фактором нанесення втрат у разі нещасного випадку. Тобто, це слабкість системи, яка підвищує ймовірність успіху атаки або імовірність настання нещасного випадку. Вразливості не обмежуються лише недоліками у програмному або апаратному забезпеченні (тобто технічні вразливості). Вони включають недоліки, що мали місце під час проектування системи, інсталяції та конфігурації системі, її експлуатації, а також недоліки роботи персоналу тощо (операціональні вразливості).

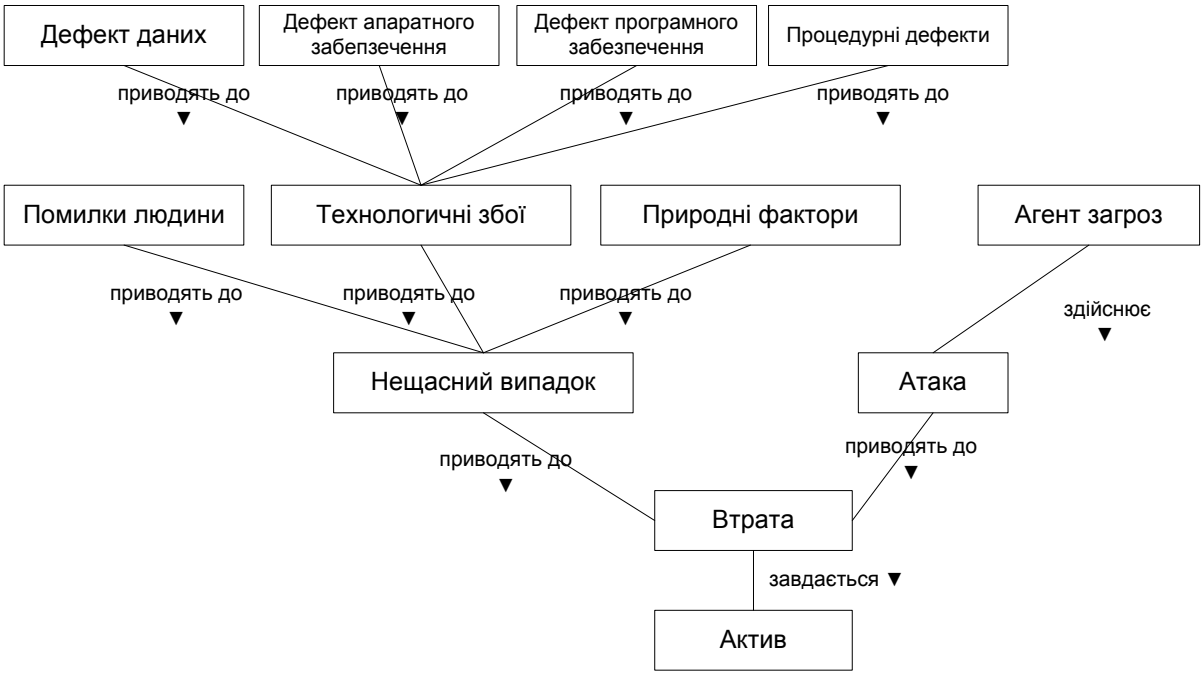


Рисунок 7 – ІП-діаграма, що характеризує невизначеність оцінювання загроз та нещасного випадку

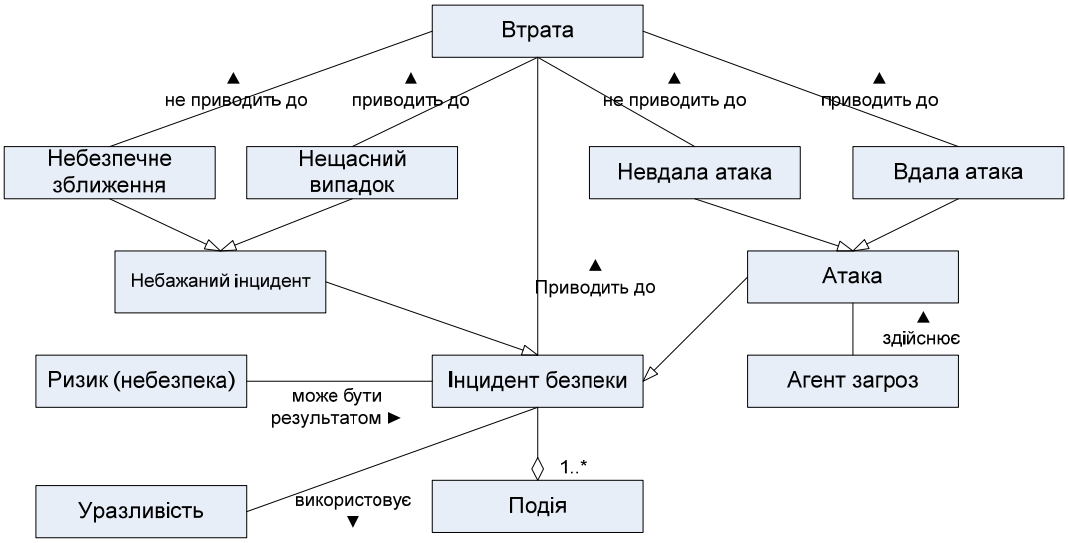


Рисунок 8 – ІП-діагарама поняття «інцидент безпеки»

Механізми безпеки - механізми, що спрямовані на задоволення вимог безпеки, запобігають реалізації загроз безпеки та небезпечних подій та усувають вразливості безпеки. Механізм безпеки може бути реалізований як комбінація апаратних та програмних компонент, як деякі процедури, що виконуються персоналом (заходи захисту) тощо. Механізм безпеки реалізується заради *ефекту захисту*, який полягає у зниженні рівня ризику безпеки.

Ризик – це небажаний інцидент безпеки, для якого були визначені певні характеристики – величина наслідків (втрат), частотні характеристики, рівень тощо.

Категорія ризику – це угрупування ризиків за ознакою схожості з призначенням власного рівня.

Оцінка ризику в загальному випадку залежить від рівня загрози безпеці інформації, ймовірності настання нещасного випадку, наявності та рівня небезпечності уразливостей та рівня потенційних втрат, які можуть бути нанесені в результаті порушення безпеки інформації. Оцінка ймовірності атаки та нещасного випадку пов'язана з певними факторами невизначеності, які залежать від конкретної ситуації. Тому оцінка ймовірності атаки та нещасного випадку не може бути визначена точно, а може визначатися у деякому інтервалі або на якісному рівні. На оцінку рівня втрат також впливають фактори невизначеності, що пов'язані з природою активів. Оскільки фактори мають досить велику невизначеність, то точні оцінки, що пов'язані з ними, здійснення планування та обґрунтування захисту інформації значно ускладнюється.

ЦП-модель родини процесів SAR. Надана інформаційно-понятійна модель дозволила сформувати модель «ціль-процес» виду:

$$M_{ÖÏ}^{SAR} = \langle P_{SAR}, Tar_{\mathrm{SAR}}, D(P_{SAR}, Tar_{SAR}), G(Tar_{SAR}), F(P_{SAR}, Tar_{SAR}) \rangle . \quad (2)$$

Множина цілей Tar_{SAR} складається з таких цілей:

tar_1^0 – здійснювати оцінювання ризиків;

tar_1^1 – визначати властивості загроз безпеки;

tar_2^1 – розуміти уразливості безпеки в конкретному середовищі;

tar_3^1 – визначати характеристики втрат;

tar_4^1 – розуміти ризики безпеки;

tar_5^1 – ранжирувати ризики безпеки.

Ці цілі складають деревоподібну ієрархію $G(Tar_{SAR})$, що наведена на рис. 9.

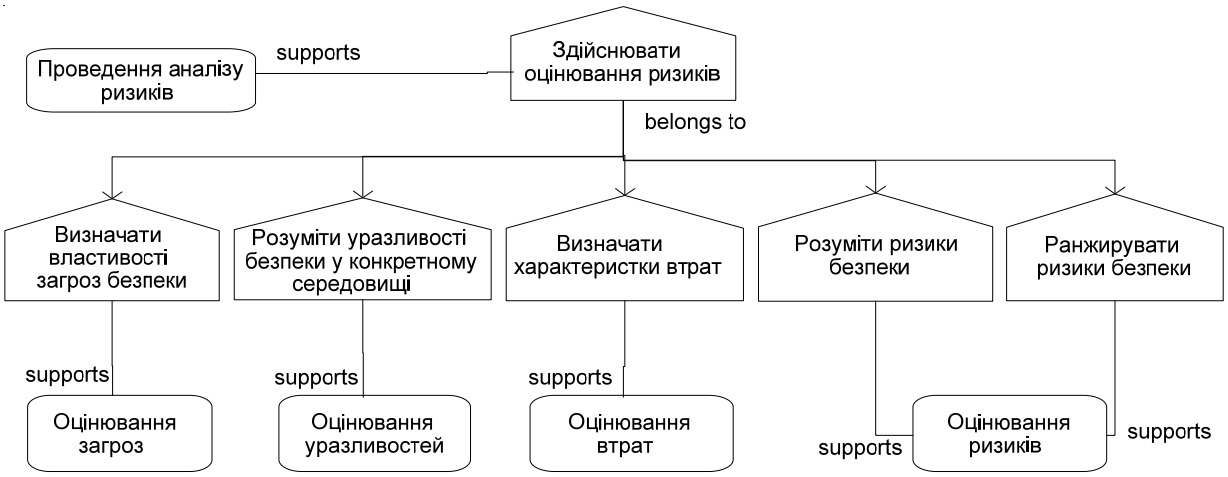


Рисунок 9 – Модель $M_{ÖÏ}^{\mathrm{SAR}}$ родини SAR

Множина процесів P_{SAR}, що спрямовані на досягнення цих цілей, складається з таких процесів: SAR_THR – процес оцінювання загроз безпеки; SAR_VUL – процес оцінювання уразливостей безпеки; SAR_IMP – процес оцінювання втрат; SAR_RSK – процес оцінювання ризиків безпеки. Відношення

$D(P_{SAR}, Tar_{SAR})$ представлені у вигляді відповідного відображення $F(P_{SAR}, Tar_{SAR})$ на деревоподібної ієрархії $G(Tar_{SAR})$ (рис. 9).

Дерево процесів SAR. У моделі (2) кожній цілі на діаграмі поставлено у відповідність конкретний процес. Спираючись на модель (2), а також на вимоги нормативних документів [3 – 10] побудуємо ієрархічну модель процесів родини SAR виду

$$G_I^{SAR} = \langle P_{SAR}, A, D(P_{SAR}) \rangle \quad (3)$$

На рис. 10 надана ієрархія процесів G_I^{SAR} у родині процесів SAR. Для побудови моделі обрано відношення типу $d_{POS}(p_i, p_j)$ – відношення підпорядкованості за процесом, що відображає процесно-орієнтований критерій об'єднання процесів (приналежність одному і тому ж процесу).

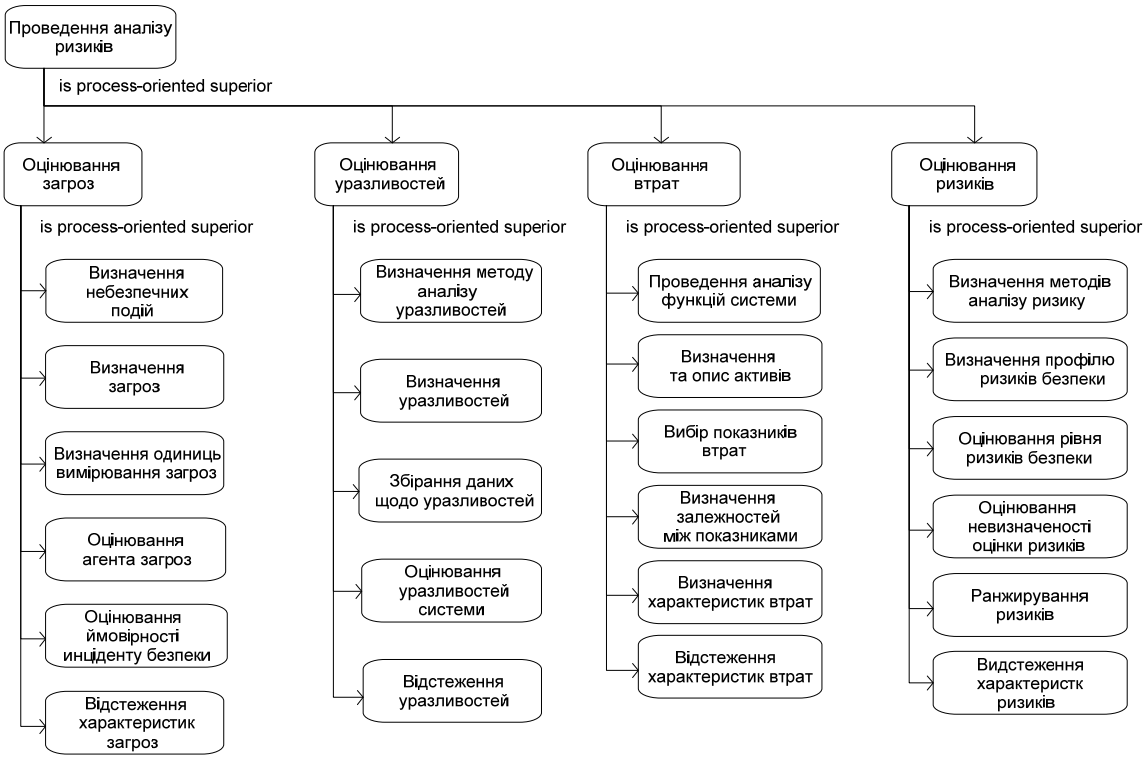


Рисунок 10 – Дерево процесів G_I^{SAR}

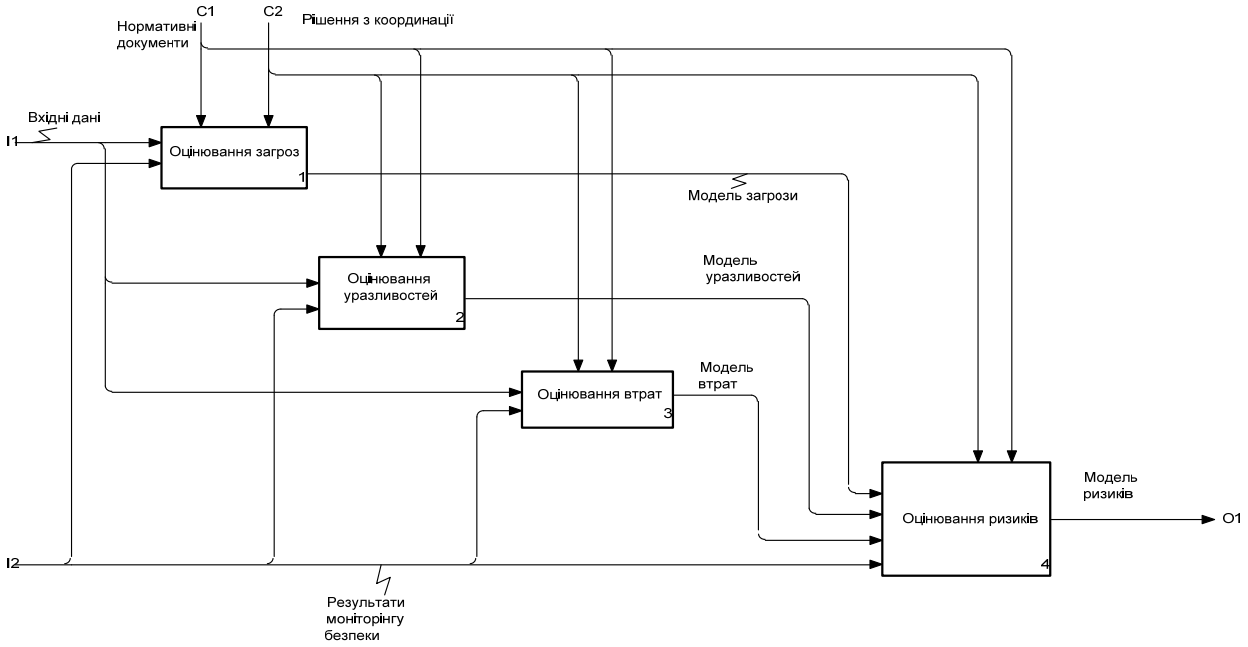
Функціональна модель родини процесів SAR. Функціональна модель родини процесів будується за правилами та нотацією стандарту функціонального моделювання IDEF0 [11]. Функціональна модель родин $M_{FO}^{SAR} = \langle P_{SAR}, V_{SAR}, D(P_{SAR}), F(P_{SAR}) \rangle$ визначає відношення між процесами, що входять до складу родини відповідно до (3), та визначає важливі на даному рівні моделювання результати процесів. Результатом моделювання є структура родини процесів та встановлені інформаційні зв'язки та зв'язки управління між процесами родини. На рис. 11 надано структура родини процесів SAR.

IV Модель процесу SAR_THR – «Оцінювання загроз безпеки»

Призначення процесу SAR_THR. Відповідно до формальної моделі процесу [12] призначення процесу складають його мета та результати. Моделювання призначення процесу є важливим елементом, тому що саме призначення процесу орієнтує нас на результати діяльності. Для побудови моделі $M_{FD}^{SAR\_THR}$ нам необхідно визначити мету процесу $Tar_{SAR\_THR} = \{tar_k | k = \overline{1, K}\}$, множину результатів процесу $Z_{SAR\_THR} = \{z_m | m = \overline{1, M}\}$ та встановити на цих множинах відповідні відношення.

Аналіз моделі $M_{ÖÏ}^{\mathrm{SAR}}$ показує, що процесу SAR_THR відповідає мета tar_1^1, що полягає у ідентифікації загроз безпеки та визначенні їх властивостей і характеристик.

Основним результатом виконання процесу є модель загрози. *Модель загрози* – це формальний, полуформальний або неформальний опис загрози безпеки, її складових частин та характеристик. Модель загрози може бути представлена в різні способи. Для нас важливо описати модель загрози в конкретних результатах, що можуть бути отримані як вихід реалізації процесу SAR_THR. Пропонується така множина результатів, що надана у вигляді графу $F_{SAR\_THR}\left(Tar_{SAR\_THR}, Z_{SAR\_THR}\right)$ (рис. 12). На графі вказані типи відношень між елементами моделі. На рис. 13 надана функціональна модель процесу SAR_THR .



Ри

сунок 11 – Модель процесу аналізу ризиків SAR в нотації IDEF0

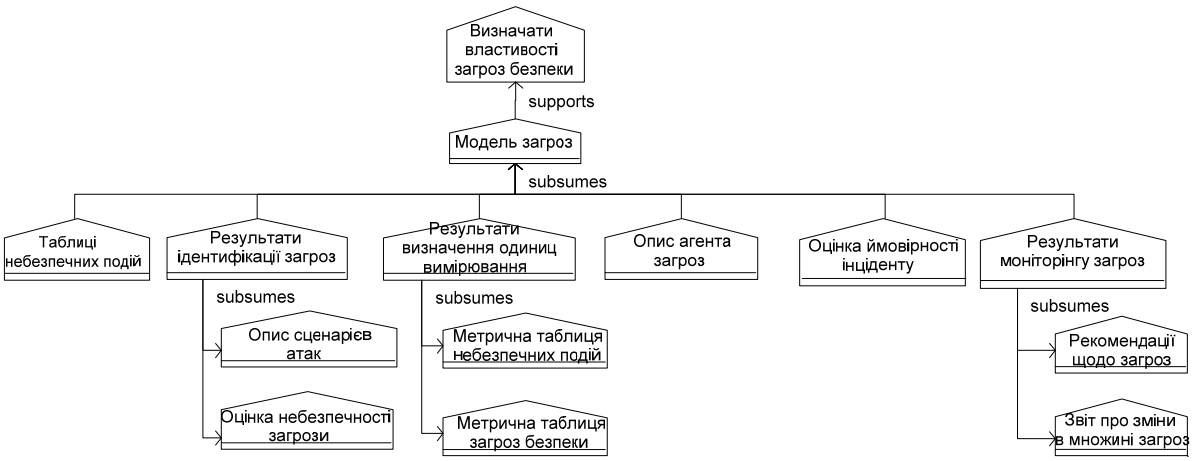


Рисунок 12 – ЦР-модель $M_{ÖÐ}^{SAR\_THR}$ процесу SAR_THR

V Модель процесу SAR_VUL "Оцінювання вразливостей безпеки"

Призначення процесу SAR_VUL. З моделі $M_{ÖÏ}^{\mathrm{SAR}}$ видно, що процесу SAR_VUL відповідає мета tar_2^1 – розуміти уразливості безпеки в конкретному середовищі. Оцінювання вразливостей (слабких місць)

полягає у визначенні та наданні характеристик слабких місць у безпеці системи. Предметна область процесу включає аналіз активів системи, визначення конкретних слабких місць та надання комплексної оцінки вразливості усієї системи. В цілях комплексної оцінки вразливості усієї системи. В цілях розробки даної моделі «слабке місце» відноситься до аспектів системи, які можуть використовуватися для інших цілей, ніж ті, що визначені у проектній документації, а також слабкості, помилки в безпеці або дефекти в реалізації системи, котрі ймовірно можуть бути використані для здійснення атаки. Сукупність операцій процесу виконується в будь-який час життєвого циклу системи для підтримки рішення щодо розробки, підтримки або функціонування системи в конкретному оточенні. Результати, що підтримують мету процесу, надані на графі $F_{SAR\_VUL}\left(Tar_{SAR\_VUL}, Z_{SAR\_VUL}\right)$ (рис. 14). Граф, сукупність цілей, результатів та відношення на них складають модель $M_{ÖÐ}^{SAR\_VUL}$.

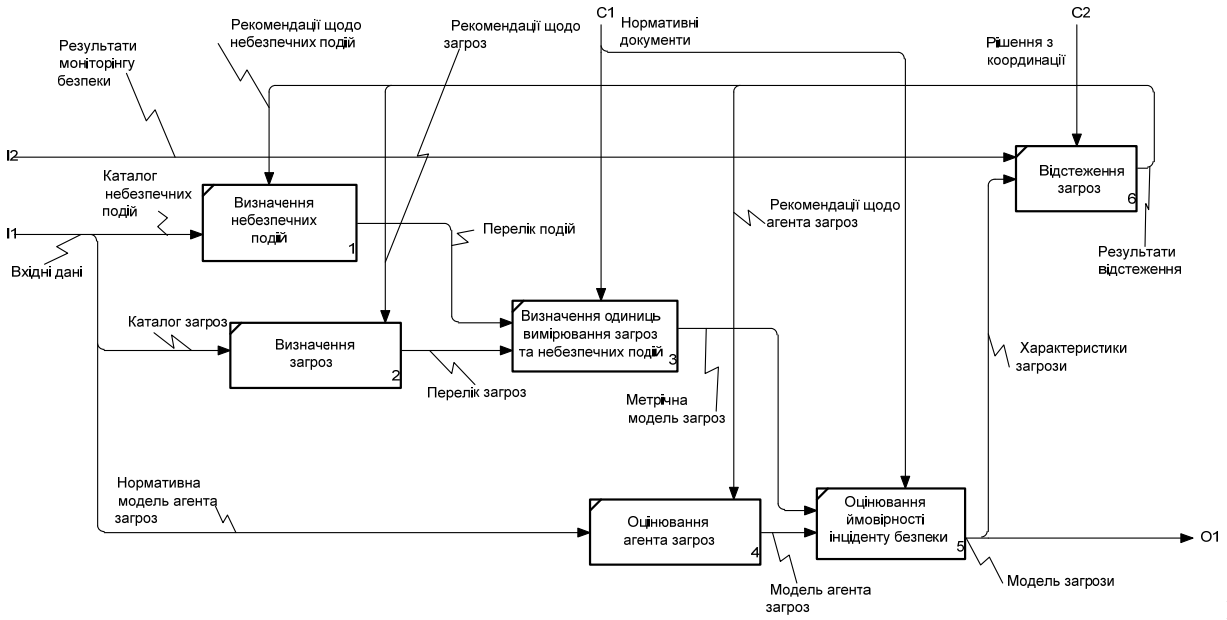


Рисунок 13 – Функціональна модель процесу SAR_THR

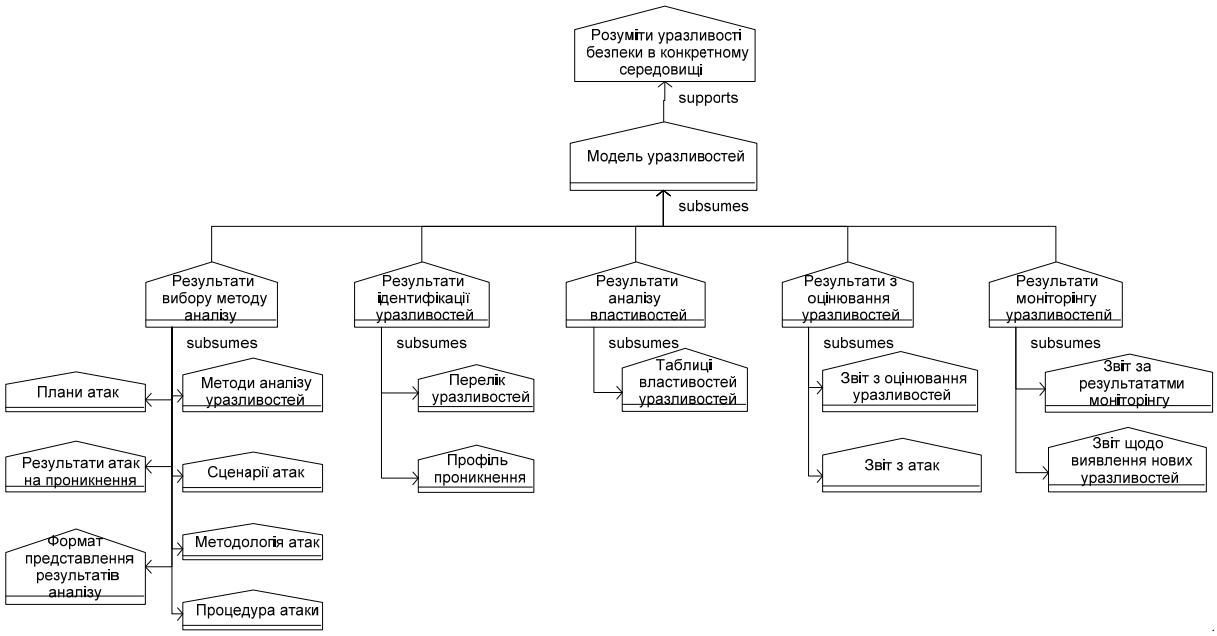


Рисунок 14 – Модель $M_{ÖÐ}^{SAR\_VUL}$ процесу SAR_VUL

На рис. 15 наведена функціональна модель процесу оцінювання вразливостей безпеки.

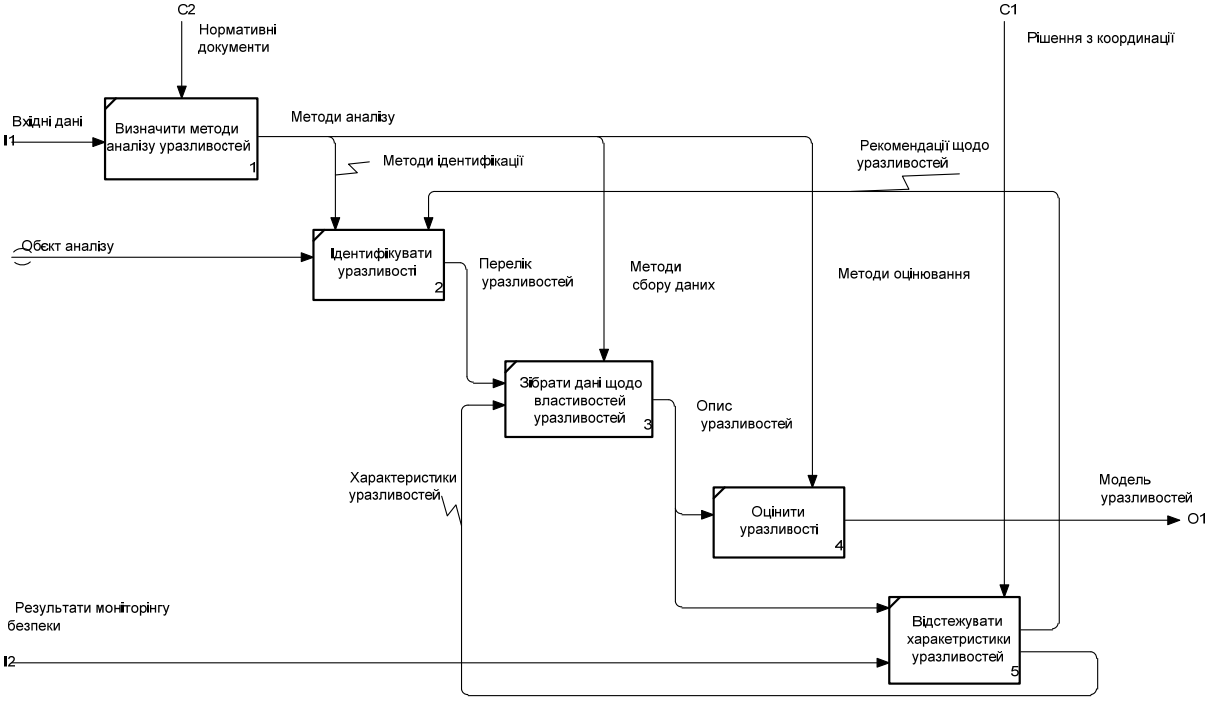


Рисунок 15 – IDEF0-модель процесу *SAR_VUL*

VI Модель процесу SAR_IMP «Оцінювання втрат»

Призначення процесу SAR_IMP. Відповідно до моделі $M_{ÖÏ}^{\text{SAR}}$ процесу SAR_IMP відповідає мета tar_3^1 – визначати характеристики втрат. Головною метою оцінювання втрат є встановлення та надання характеристики впливу ризиків безпеки на IT-систему, визначення рівня втрат (шкоди) та надання оцінки імовірності виникнення конкретного виду втрат. Втрати можуть бути прямі, наприклад, втрата доходу або фінансові штрафи, або непрямі, наприклад, втрата репутації або нематеріальних активів. Основним результатом процесу є побудова моделі втрат, що можливі у конкретному середовищі, складовою якої є оцінка рівня втрат. Результати, що підтримують мету процесу, надані на графі $F_{SAR\_IMP}\left(Tar_{SAR\_IMP}, Z_{SAR\_IMP}\right)$ (рис. 16). Граф, сукупність цілей, результатів та відношення на них складають модель $M_{ÖÐ}^{SAR\_IMP}$. На рис. 17 надана функціональна модель процесу.

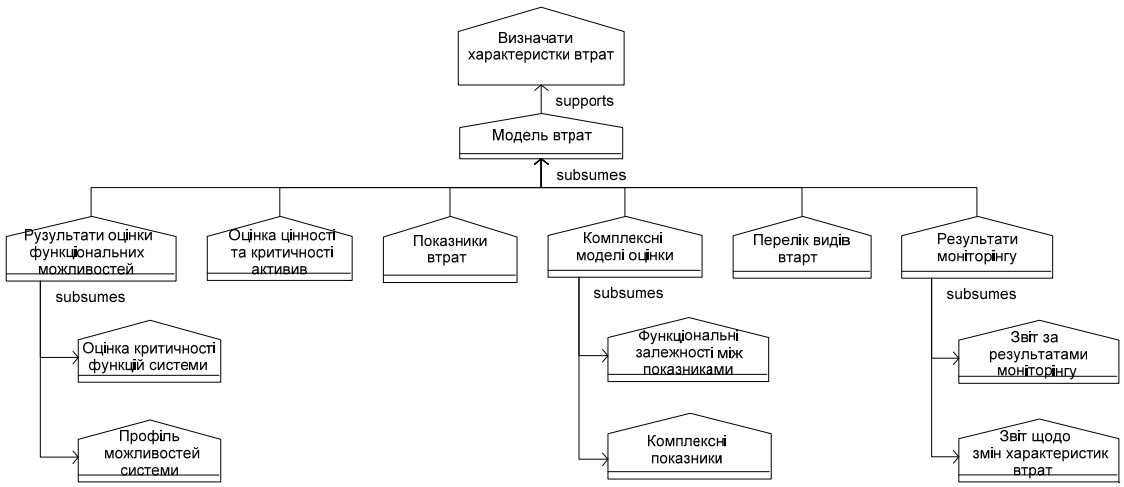


Рисунок 16 – Модель $M_{ÖÐ}^{SAR\_IMP}$ процесу SAR_IMP

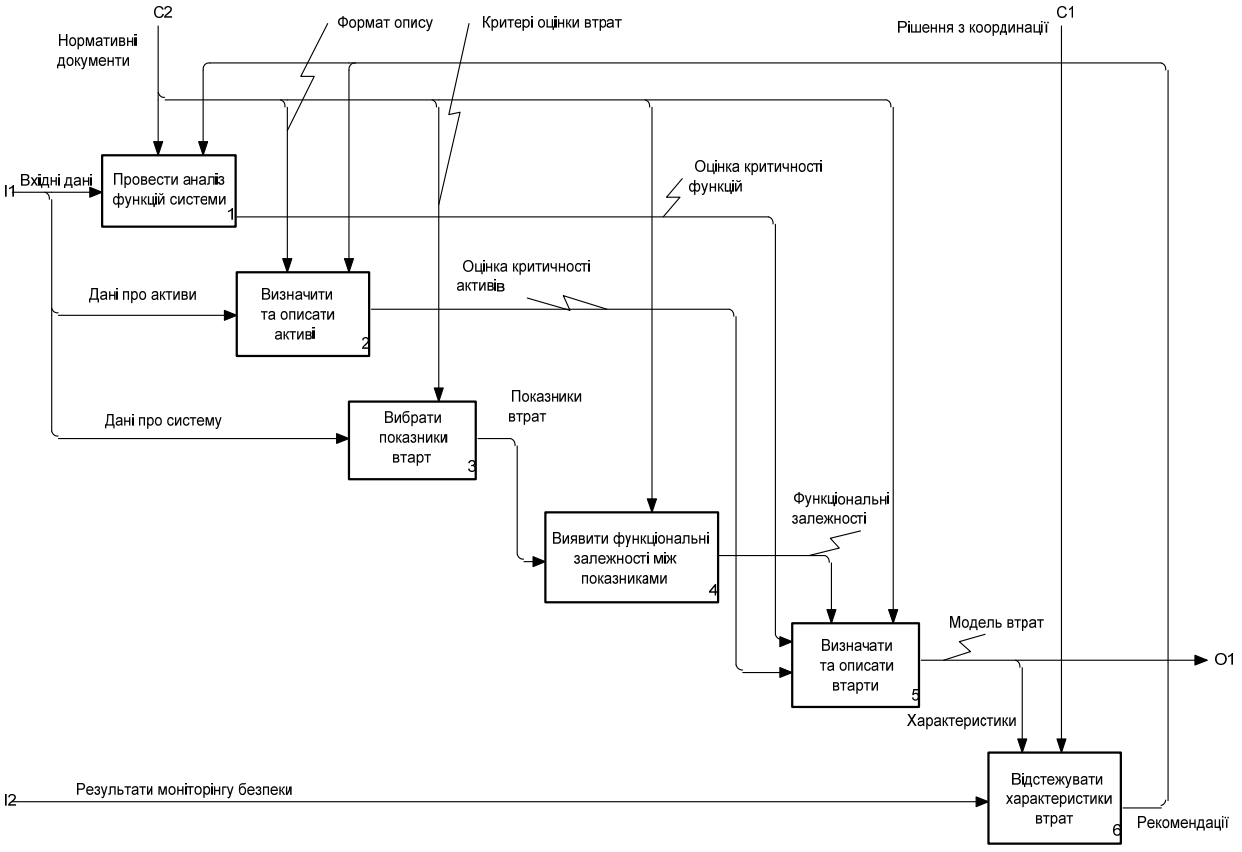


Рис унок 17 – IDEF0 модель процесу SAR_IMP

VII Модель процесу SAR_RSK «Оцінювання ризиків безпеки»

Призначення процесу SAR_RSK. Головною метою оцінювання ризику безпеки є визначення ризиків безпеки системи у визначеному оточенні. Предметною областю процесу є виявлення ризиків, що засновується на розумінні того, наскільки функціональні можливості та активи системи є вразливими до загроз. Результатом процесу є побудова профілю ризику. Під профілем ризику ми розуміємо поєднання загрози, слабкого місця та впливу, що можуть завдати шкоди активу. Операції оцінювання ризиків безпеки виконують в будь-який час життєвого циклу системи для підтвердження рішень, пов'язаних із розробкою, підтримкою та роботою системи у відомому оточенні. Відповідно до моделі $M_{ÖÏ}^{\mathrm{SAR}}$ процесу SAR_RSK відповідають: мета tar_4^1 – забезпечення розуміння ризику безпеки, пов'язаного із роботою системи у визначеному оточенні; мета tar_5^1 – призначення пріоритетів для ризиків згідно з встановленою методикою.

Результати, що підтримують мету процесу, надані на графі $F_{SAR\_RSK}\left(Tar_{SAR\_RSK}, Z_{SAR\_RSK}\right)$ (рис. 18). Граф, сукупність цілей, результатів та відношення на них складають модель $M_{ÖÐ}^{SAR\_RSK}$. На рис. 19 надана функціональна модель процесу.

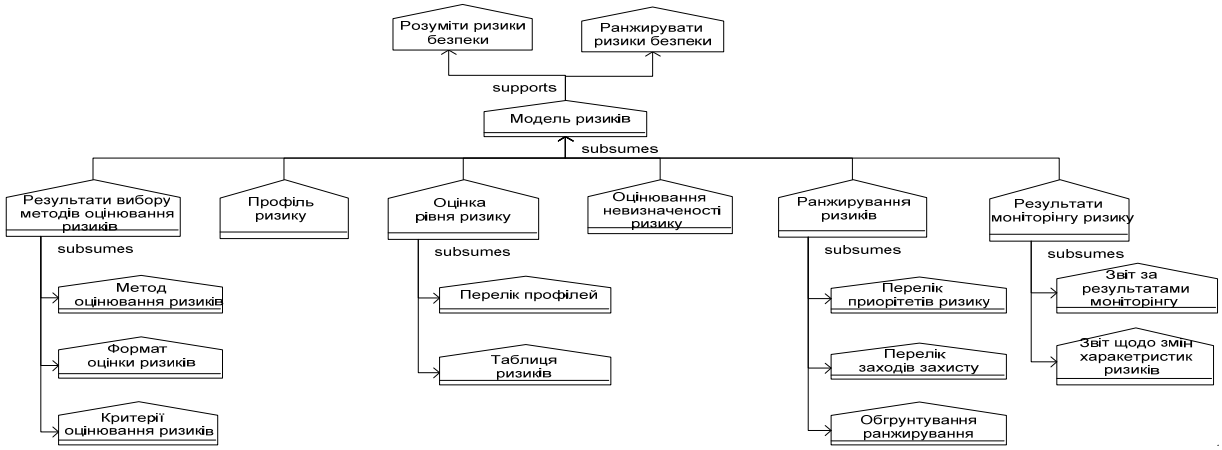


Рисунок 18 – Модель $M_{ÖÐ}^{SAR\_RSK}$ процесу SAR_RSK

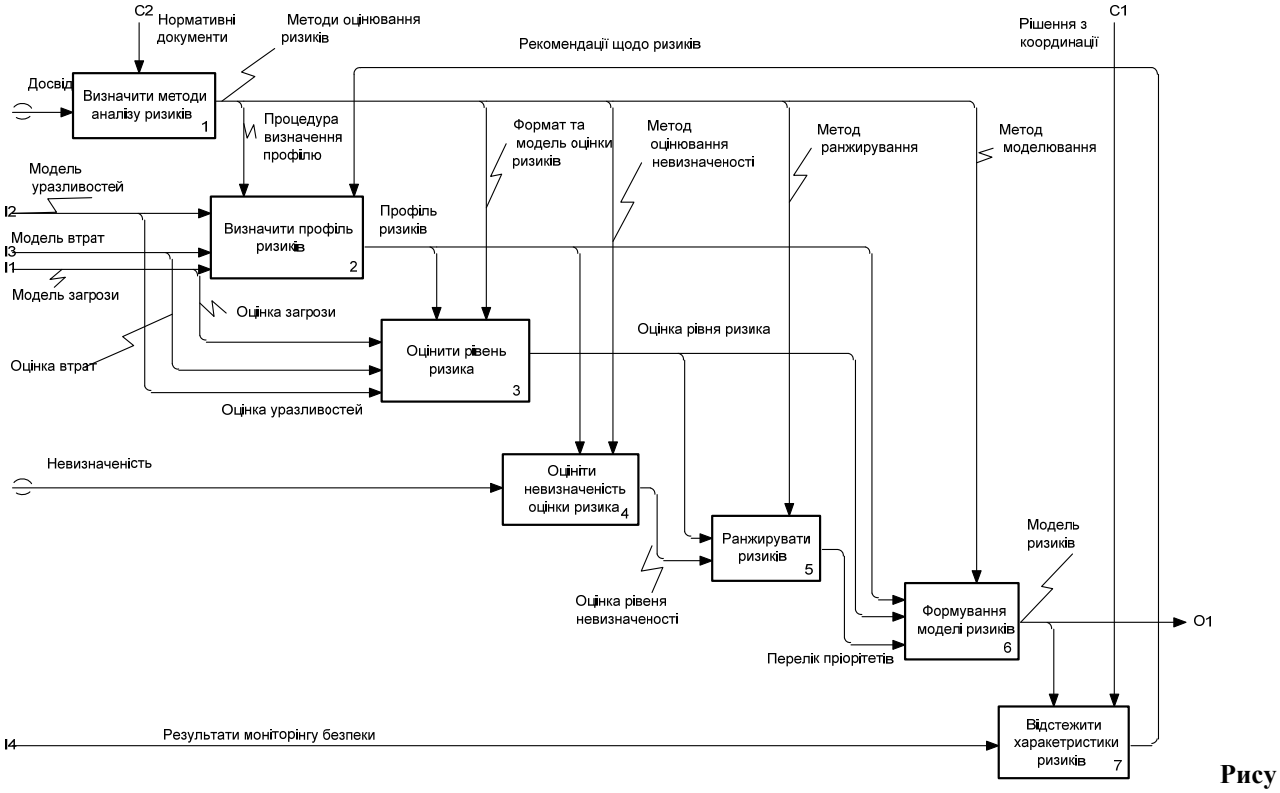


Рисунок 19 – Функціональна модель процесу SAR_RSK

Висновки

Розроблена сукупність моделей, які повністю визначають структуру діяльності з аналізу ризиків. Спираючись на ці моделі можна здійснювати уточнення результатів, адаптування моделей до конкретних умов здійснення діяльності із захисту інформації. Аналогічним чином розроблені моделі інших процесів захисту інформації. В цілому розроблені моделі подають погляд на діяльність із захисту інформації «як має бути». Ці моделі також можуть бути використані для порівняння з практикою, що склалася на конкретному об’єкті інформатизації з нормативною моделлю та сформувати відповідні напрямки удосконалення діяльності. Результати, викладені в статті, отримані в рамках проведення

досліджень, метою яких є синтез нових аналітичних моделей діяльності та процесів захисту інформації у рамках системодіяльнісної методології захисту інформації. Отримані результати мають важливе значення для удосконалення організаційно-технічних форм та методів захисту інформації. У роботах [2, 12 – 14] викладаються основні положення системодіяльнісної методології захисту інформації як складової частини системного підходу до вирішення проблем забезпечення безпеки інформації в складних організаційно-технічних системах.

У даній роботі по суті запропонована нормативна модель мікроструктури діяльності із захисту інформації на основі застосування методів морфологічного аналізу нормативних множин заходів безпеки, застосування методології SADT та методів функціонального моделювання IDEF0 і ARIS. Модель отримана вперше і являє собою нові знання відносно структури діяльності із захисту інформації. Результати носять методичний і теоретичний характер та можуть використовуватися на практиці для визначення організаційної системи захисту інформації. Отримані результати є елементами теоретичних та науково-методичних основ процесного підходу до захисту інформації.

*Література: **1.** Потій А. В. Формалізована модель діяльності // Радіоелектронні і комп'ютерні системи. Науково-технічний журнал. - № , 2007. – С.ХХ-ХХ **2.** Потий А. В. Эталонная модель системы процессов защиты информации. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник – Вип. 12 – Київ, 2006. – С. 17-31. **3.** ISO/IEC 21827: 2002 Information technology - Systems Security Engineering - Capability Maturity Model **4.** НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. **5.** ISO/IEC 17779:2000 Code of practice for information security management **6.** NIST SP 800-26. Security Self-Assessment Guide for Information Technology Systems **7.** Bundesamt fur Sicherheit in der Informationstechnik. IT Baseline Protection Manual, 1998. **8.** ДСТУ ISO/IEC TR 13335-2:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2: Керування та планування безпеки інформаційних технологій. **9.** ISO/IEC 27001:2005 (BS 7799-2:2005) Information technology Security techniques– Information Security Management Systems. **10.** NIST SP 800-53. Recommended Security Controls for Federal Information Systems. R. Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner, G. Rogers, A. Lee – 2005. **11.** РД IDEF 0. Методология функционального моделирования IDEF0. Руководящий документ. – Госстандарт России, Москва.- 2000. **12.** Потий А. В. Формальная модель процесса защиты информации // Радіоелектронні і комп'ютерні си стеми. Науково-технічний журнал. - №5, 2006. – С. 75-80 **13.** Бондаренко М. Ф., Потий О. В. Визначення та обґрунтування суті політики інформаційної безпеки // Радиотехника. Всеукраинский межвед. Научн.-техн. Сб. – 2003. – Вып. 134. – С. 9-25 **14.** Потій О. В. Процесний підхід до управління безпекою інформації//VIII Международная научно-практическая конференция"Безопасность информации в информационно-телекоммуникационных системах", 11-13 мая 2005. Тезисы докладов. – К.: НИЦ "Тезис", 2005. – С. 35-36.*

УДК 621.396

МЕТОДИКА ОТРИМАННЯ ОБРАЗУ МОВНОГО СИГНАЛУ ДЛЯ ВИРІШЕННЯ ЗАВДАННЯ ЩОДО ІДЕНТИФІКАЦІЇ ДИКТОРА

Максим Кузнецов
Національна академія СБ України

Анотація: **Розглянуто новітню методику спектральної обробки мовних сигналів, застосування якої дозволяє значно підвищити ефективність систем ідентифікації джерела сигналу.**
Summary: **This article is about the new speech-processing method, which allows to improving of the speech source identification systems efficiency greatly.**
Ключові слова: **Ідентифікація мови диктора, спектральна обробка, порядкові статистики, статистични критерії згоди, голосовий статистичний образ.**

Вступ

На сьогоднішній день повною мірою невирішеним та актуальним залишається загальнонаукове завдання щодо ідентифікації мови диктора. Розв'язанню цієї проблеми існуючими засобами заважає значна кількість перешкод, існування яких пов'язано із природою мовного сигналу, який є випадковим нестаціонарним процесом зі змінною дисперсією і складною формою поточної спектральної щільності потужності. Деякі з цих перешкод: неможливість встановлення точного переліку інваріантних ознак, які є характерними для