

ОНТОЛОГІЧНІ МОДЕЛІ ВЛАСТИВОСТЕЙ ЗРІЛОСТІ ПРОЦЕСІВ ЗАХИСТУ ІНФОРМАЦІЇ

О.В. ПОТІЙ

Розглядаються проблемні питання аналізу властивостей зрілості процесів захисту інформації. На основі використання онтологічного підходу до аналізу, розроблені та пропонуються онтологічні моделі властивостей зрілості. Надані визначення основних властивостей зрілості.

The paper considers problems of analyzing properties of maturity of information security processes. Some ontological models of maturity properties are developed and proposed on the basis of using the ontological approach to analysis. Determining the basic properties of maturity is given.

ВСТУП

Концепція зрілості процесу вперше запропонована в галузі виробництва програмного забезпечення та управління проектами, але в сфері захисту інформації вона на сьогодні не знайшла широкого використання. Під *зрілістю процесу захисту інформації* ми розумітимемо сукупність спеціальних властивостей процесу захисту інформації, які обумовлюють та характеризують його здатність досягати запланованої мети та результатів у відповідності до його призначення [1].

У рамках системодіяльної методології захисту інформації та процесного підходу до захисту інформації, використання концепції зрілості є дуже плідною [2]. Водночас зазначимо, що дослідники не приділяють достатньої уваги вивченню самої суті такої категорії як зрілість. До теперішнього часу немає єдиного тлумачення поняття «зрілість» стосовно таких об'єктів, як процес, діяльність, організація і це є однією з основних передумов формування проблеми розуміння категорії зрілості. В існуючих роботах та стандартах [5, 6, 7, 8, 9] немає чіткого розмежування таких понять, як зрілість процесу, зрілість діяльності, зрілість організації, хоча в обігу ці терміни використовуються. Така термінологічна невизначеність призвела до існування чисельних моделей зрілості, що використовуються у сферах програмної інженерії, управління високотехнологічними проектами, стратегічного планування діяльності, управління інформаційними технологіями. Як зазначено в [5], сьогодні на практиці використовується більш, ніж 30 моделей зрілості. Але наявні моделі зрілості є вербальними (описовими), не мають достатнього наукового обґрунтування та будуються на інтуїції дослідників. Зазначимо, що в сфері захисту інформації на сьогодні не визначено жодної моделі.

Тому, з точки зору розвитку системодіяльної методології захисту інформації та створення теоретичних основ та науково-методичного апарату процесного підходу до захисту інформації, надання логічного пояснення суті категорії „зрілість”, обґрунтування можливості її застосування в галузі захисту інформації, розроблення онтологічних моделей зрілості процесів захисту

інформації, які визначають сутність основних понять, що стосуються зрілості та встановлює відношення між цими поняттями, є достатньо актуальними науковими завданнями. Автором у роботах [1-4] здійснена спроба вирішення цих завдань. Важливою задачею з точки зору вивчення категорії зрілості є розкриття ролі та проявлення загальносистемних закономірностей цієї категорії, розроблення сукупності моделей зрілості, що дозволяють вивчити та охарактеризувати зрілість як системну властивість процесів та діяльності захисту інформації. У рамках системодіяльної методології цей контекст безпеки розширюється. Зрілість пропонується розглядати як основу для формування впевненості у тому, що діяльність із захисту інформації, процеси, адміністративні і процедурні заходи безпеки дійсно відповідають й адекватні цілям захисту інформації та спрямовані на вирішення задач захисту. На рис. 1 ілюструється ця позиція.

Такий погляд на зрілість у контексті безпеки інформації логічно пов'язується із сучасною концепцією безпеки інформаційних технологій, а саме з її складовим елементом – концепцією гарантій безпеки [10, 11]. У відповідності до цієї концепції впевненість власника критичних активів у їх захищеності має ґрунтуватися на доказах (свідченнях) відносно рівня гарантій безпеки систем (продуктів) інформаційних технологій, які надав виробник. *Гарантія* – це виконання відповідних дій або процесів для поступового формування (забезпечення) впевненості у тому, що об'єкт досягає (задовольняє вимоги) поставлених задач захисту. На рівні управління та організації захисту інформації впевненість власника критичних активів має також ґрунтуватися на свідченнях відносно рівня зрілості процесів захисту інформації, що здійснюються в організації.

Таким чином, впевненість у виконанні вимог безпеки інформації складається з *технологічної впевненості* та *операційної впевненості*. Технологічна впевненість формується на основі надання гарантій з боку виробника системи (продукту) інформаційних технологій, тобто на технічному рівні. Операційна впевненість формується на основі надання свідчень відносно рівня зрілості процесів

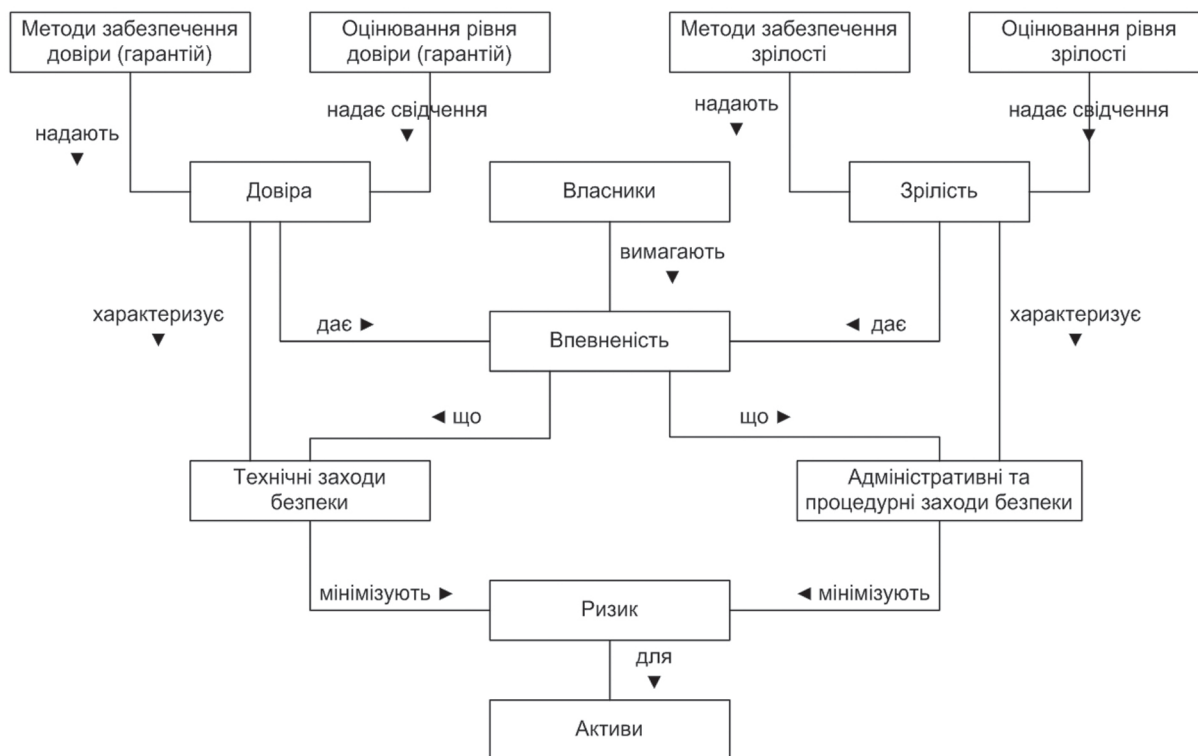


Рис. 1. Онтологічна модель впевненості у безпеці інформації

захисту інформації, що реалізуються в рамках системи захисту інформації на адміністративному (управлінському) та організаційному рівнях. Саме у такому контексті у роботі розглядається зрілість та вирішуються відповідні наукові задачі щодо моделювання властивостей зрілості, досліджуються загальносистемні закономірності зрілості, розробляються моделі та методи її оцінювання.

1. ЗАДАЧА РОЗРОБКИ ОНТОЛОГІЧНИХ МОДЕЛЕЙ ВЛАСТИВОСТЕЙ ЗРІЛОСТІ

Зрілість – це комплексна властивість процесу, яка характеризує процес, діяльність та навіть організаційну систему у цілому. У ряді робіт [5, 6] та нормативних документах [8, 12, 13] наводяться підходи, та робляться спроби запропонувати методи оцінювання зрілості. Але в інтересах розв'язання практичних задач оцінювання зрілості важливо чітко ідентифікувати властивості зрілості, що притаманні довільному процесу. Для кожної ідентифікованої властивості важливо встановити ознаки та показники оцінювання, а також запропонувати метод оцінювання.

Доступні джерела, у своїй більшості, надають лише загальний «орієнтир» у питанні визначення та оцінювання властивостей зрілості (такий висновок можна зробити й відносно існуючих стандартів, що висувають вимоги щодо зрілості процесів). Але відомі роботи не надають практичних та методичних рекомендацій стосовно оцінювання важливих для проектування, впровадження та удосконалення процесів захисту інформації властивостей зрілості. Надають несурові, суперечливі визначення бажаних властивостей ПЗІ, зустрічаються описи та характеристики зрілості конкретних процесів

[14, 12, 9] або характеристики рівнів зрілості [15, 7, 8, 9] які є точно не визначеними. Це ускладнює як розробку методів оцінки зрілості, так і порівняння різних процесів у просторі зрілості.

У зв'язку з наведеним дуже корисним виглядає виділення із всієї множини властивостей зрілості тих, які можуть бути описані та оцінені об'єктивно, що створює сприятливі умови та можливості для своєчасного виявлення недоліків та операційних уразливостей у діяльності із захисту інформації та усунути їх, для створення автоматизованих засобів оцінювання властивостей. Властивості, що виявлені, корисно класифікувати, об'єднати в аналітичний вимір, тобто у множину об'єктів одного або декількох типів, що організовані у вигляді онтологічних структур та забезпечують загальний інформаційний контекст для розв'язання деяких практичних задач (наприклад, оцінювання, аналіз, вимірювання, ідентифікація тощо). У зв'язку з цим актуальною є задача ідентифікації, формування та класифікації множини властивостей зрілості, що придатні для об'єктивного оцінювання зрілості процесів захисту інформації.

Як методологічну та методичну основу розв'язання цієї задачі пропонується обрати онтологічний підхід, використати методи онтологічного аналізу та інжинірингу властивостей зрілості. Використання декількох ракурсів бачення та уявлення онтології властивостей зрілості (тобто побудова та аналіз різних онтологічних структур на множині властивостей зрілості) забезпечує більш глибокий аналіз властивостей, виявлення класифікаційних ознак, визначення складу властивостей, функціональних відношень між ними тощо.

Формування набору властивостей зрілості, який придатний для оцінювання процесів захисту інформації, що проектується та впроваджуються, означає необхідність ідентифікації цих властивостей та надання їх чіткого, ясного та, за можливістю, формального визначення, встановлення певних типів відношень на множині властивостей зрілості та формуванні *аналітичного виміру зрілості*. Можливість дослідження властивостей зрілості означає перш за все можливість *систематичного оцінювання* зрілості, що є актуальним, оскільки:

– оцінювання властивостей зрілості дозволяє виявляти недоліки в організації діяльності із захисту інформації, важливі процеси захисту інформації;

– якщо встановити залежність між властивостями зрілості процесів і результативністю та ефективністю процесів, то оцінювання перших дозволить своєчасно (ще на етапі проектування організаційної системи захисту інформації) прогнозувати результати діяльності із захисту інформації, і, відповідно, рівень захищеності критичних активів.

Крім цього, додатковий загальнонауковий інтерес до онтологічного дослідження властивостей зрілості полягає в тому, що це дозволить розширити рамки загальнонаукового уявлення про властивості процесів взагалі, як системних утворень, незалежно від виду діяльності (бізнес-процесів, процесів інжинірингу, процесів управління тощо).

Нехай універсальна множина властивостей зрілості позначається як $M^{\Sigma} = \{\mu_1, \mu_2, \dots, \mu_{\infty}\}$. Необхідно побудувати формальну модель онтології властивостей зрілості виду

$$O_{\mu} = \langle M^B, R, A \rangle, \quad (1)$$

де $M^B = \{\mu_1, \mu_2, \dots, \mu_m\}$ – базова множина властивостей зрілості, що подано в онтології відповідним набором термінів; $R = \{r_1, r_2, \dots, r_n\}$ – множина типів відношень, що можуть бути встановлені між властивостями зрілості; $A = \{a_1, a_2, \dots, a_k\}$ – множина аксіом (правил та тверджень), у відповідності до яких визначаються типи відношення та формулюються достовірні твердження відносно властивостей зрілості.

Формальна модель онтології (1) має являти собою цілісну структурну специфікацію властивостей зрілості, формалізоване уявлення аналітичного простору (виміру) зрілості.

Розв'язання цієї задачі передбачає розв'язання таких складових задач.

1. У загальному випадку множина властивостей зрілості M^{Σ} нескінченна, тобто аналітичний простір зрілості є невичерпним. З цього випливає таке: 1) не існує можливості задати (описати) повну (вичерпну) множину властивостей зрілості; 2) завжди існує можливість сформулювати нову властивість зрілості. Тому на практиці актуальною є задача формування скінченної множини властивостей зрілості, які на цей час мають опис,

є зрозумілими, можуть бути пояснені, та відносно яких можна застосувати формальний або неформальний апарат моделювання та оцінювання (або вимірювання). Таку множину властивостей називатимемо базовою множиною властивостей зрілості, та позначати як $M^B = \{\mu_1, \mu_2, \dots, \mu_m\}$. Таким чином, під час побудови онтології (1) необхідно здійснити перехід від універсальної множини властивостей зрілості до базової множини $M^{\Sigma} \xrightarrow{F} M^B$.

2. На базовій множині властивостей зрілості необхідно встановити певні типи відношень R та подати результати аналізу у вигляді сукупності графових моделей, що складають аналітичний вимір зрілості. Аналітичний вимір зрілості – це сукупність пов'язаних орієнтованих графів $G_{\mu}(M^B, R)$, які є сукупністю пар елементів вигляду $r(\mu_i, \mu_j)$, де $\mu_i, \mu_j \in M^B$; $r(\mu_i, \mu_j) \in R$; $i, j = \overline{1, n}$, що вказують, які елементи з множини M^B пов'язані між собою конкретним типом відношень. При цьому елементи $\mu_i, \mu_j \in M^B$ утворюють вершини графа, а відношення $r(\mu_i, \mu_j) \in R$ – ребра графу. Для опису та обґрунтування графів необхідно обрати та застосувати відповідну аксіоматику $A = \{a_1, a_2, \dots, a_k\}$.

3. На основі дослідження та аналізу формальної моделі онтології властивостей зрілості необхідно сформулювати однозначні, з точки зору тлумачення, визначення властивостей зрілості.

Для моделювання системи властивостей скористаємося методологією родини IDEF (Integrated DEfinition), а саме державним стандартом США IDEF5, що розроблений для підтримки онтологічного аналізу [16].

Основними групами графових моделей онтології є [17, 18]: графи синтаксичних відношень; графи стандартних відношень; графи концептуальних відношень; графи проблемно-орієнтованих відношень.

Моделювання властивостей зрілості здійснюватимемо за допомогою графів стандартних відношень. Графи стандартних відношень дозволяють подати такі структурні моделі предметної галузі, як структуру таксономії понять, структуру теоретико-множинних відношень, структуру стандартної партономії тощо.

Онтологічна модель стандартних відношень – це граф $G(S, R)$, де вершини графа $\{S_i\}$ відповідають поняттю та характеризують позначкою – ім'ям поняття (термін), ребра $\{R_i\}$ відображують однорідне семантичне відношення між поняттями. У моделі подається декілька однорідних видів відношень, повний перелік яких встановлюється заздалегідь.

2. ПРОБЛЕМНО-ОРІЄНТОВНА ОНТОЛОГІЯ ЗРІЛОСТІ ПРОЦЕСІВ ЗАХИСТУ ІНФОРМАЦІЇ

Проблемно-орієнтовна онтологія зрілості об'єднує всі найбільш важливі поняття відносно категорії «зрілість» та по суті розкриває зміст цієї категорії. Основна мета онтологічного моде-

Виходячи з цих міркувань, наведемо таке визначення.

Показник зрілості – це 1) спеціальні кількісні або якісні характеристики, що вводяться для оцінки окремої властивості зрілості (тобто формують свідчення про ступінь володіння процесом конкретною властивістю зрілості або 2) кількісні або якісні характеристики оцінки рівня зрілості процесу або 3) бінарний індикатор наявності або відсутності властивості зрілості процесу

Вимога зрілості – це спеціальна вербальна або формальна конструкція, яка визначає властивості зрілості (ознаки та показники), які є бажаним для конкретного процесу, що моделюється або реалізується.

Зрілість процесу захисту інформації специфікується у термінах вимог зрілості. У залежності від ступеня абстракції вимоги зрілості можуть бути виражені або неформально (наприклад, висування вимоги досягнення властивості зрілості) або формально (наприклад, висування вимог щодо досягнення конкретних значень показників зрілості).

3. ТАКСОНОМІЯ ВЛАСТИВОСТЕЙ ЗРІЛОСТІ

Таксономія властивостей зрілості побудована на основі аналізу доступних джерел, що містять описи характеристик зрілості процесів у різних сферах діяльності [5-9], а також використовуючи стандартну процедуру проведення онтологічного аналізу [16].

Формально таксономія властивостей зрілості це онтологічна модель виду

$$O = \langle M, R_{tax}, A_{tax} \rangle, \quad (2)$$

де $M^B = \{\mu_1, \mu_2, \dots, \mu_m\}$ базова множина властивостей зрілості; R_{tax} – стандартне відношення типу «є представником», «є класом (підкласом)» (kind-of, subkind-of); A_{tax} – стандартні аксіоми класифікаційних відношень.

Таксономія властивостей подається у вигляді графа стандартних відношень $G_T(M, R_{tax})$.

3.1. Загальна таксономія властивостей зрілості

У роботі [4] наведено результати аналізу різних джерел, що дозволило виявити сукупність властивостей, які на цей час мають пояснення та відрізняються тими або іншими дослідниками. На основі цього аналізу розроблено загальну таксономію властивостей зрілості, яка зображена на рис. 3.

Зрілість, як елемент таксономії, являє собою клас властивостей процесу (наряду з іншими властивостями процесу такими як ефективність, результативність тощо). У свою чергу цей клас має відповідні підкласи властивостей. Клас та підкласи властивостей пов'язані відношенням типу «є підкласом» (subkind-of), «є представником», що є стандартними класифікаційними (таксономічними) відношеннями.

Загальна таксономія властивостей зрілості є трирівневою ієрархією, де властивість «зрілість» є кореневою вершиною графа. Властивості «здійснюваність», «керованість», «усталеність», «прогнозованість», «оптимальність» складають перший рівень ієрархії. Атомарний рівень ієрархії складають 12 властивостей.

Властивостям першого рівня ієрархії пропонується надати такі визначення:

Здійснюваність – властивість, яка характеризує здатність виконання процесу, тобто виконання деякої множини дій (операції), що дозволяє отримати результати процесу відповідно до його призначення.

Керованість – властивість, яка характеризує рівень виконання функцій управління процесу.

Усталеність – властивість, яка характеризує рівень впровадження процесів захисту інформації у повсякденну діяльність організації.

Прогнозованість – властивість, яка характеризує рівень застосування кількісного аналізу результативності та ефективності процесів захисту інформації та обумовлює можливості прогнозувати результати виконання процесу.

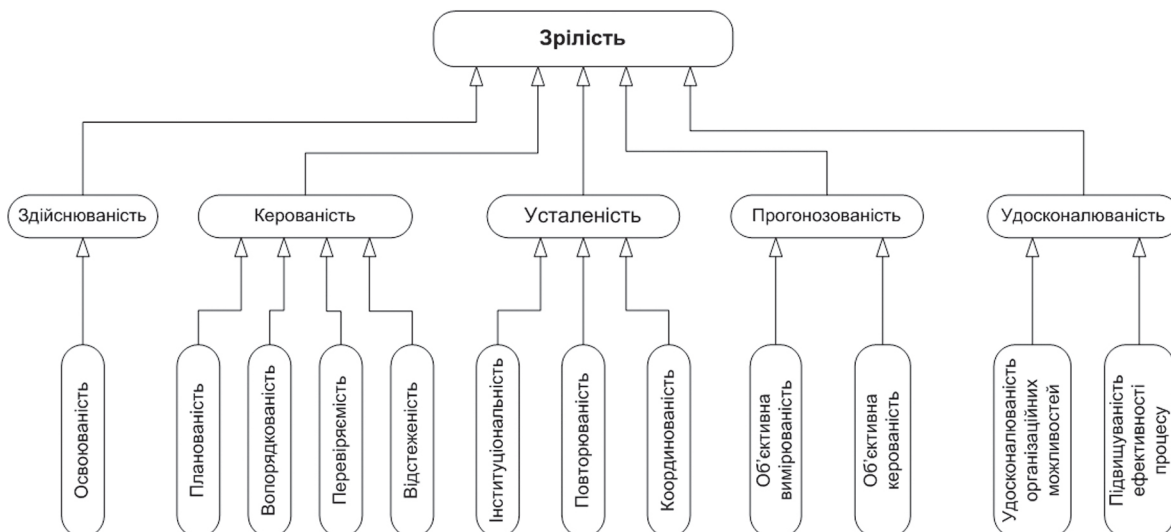


Рис. 3. Загальна таксономія властивостей зрілості

Удосконалюваність – властивість, яка характеризує якість виявлення джерел існуючих та потенційних проблем ефективності та результативності, аналізу причин виникнення проблем, рівень зусиль, спрямованих на усунення недоліків виконання процесів, визначення та впровадження змін у процес, рівень впровадження інноваційних технологій та динаміку поліпшення характеристик процесу.

3.2. Таксономія властивостей керованості

На рис. 4 зображено граф таксономії властивості керованості.

Властивостям керованості пропонується надати такі визначення:

Спланованість – властивість, яка характеризує рівень планування виконання процесів захисту інформації.

Впорядкованість – властивість, яка характеризує рівень дисципліни виконання процесів захисту інформації та рівень відповідності виконання процесу захисту інформації плану виконання.

Перевіряємість – властивість, що характеризується зусиллями, необхідними для підтвердження правильності виконання процесу та аналізу його результатів.

Відстеженість – властивість, яка характеризує якість контролю (моніторингу) під час виконання процесу у відповідності до запланованих показників, вимірювання та запровадження коригуючих дій.

Атестованість – властивість, яка характеризує здійснення атестації процесу на відповідність нормативним документам відповідно до встановлених процедур атестації.

Верифікованість – властивість, яка характеризує перевіреність на відповідність результатів виконання процесу

Вимірюваність – властивість, що характеризує можливість кількісної (якісної) оцінки ре-

зультатів виконання процесу та ефективності досягнення результатів.

Корегованість – властивість, що характеризує можливість виконання корегуючих дій на основі отриманих результатів оцінювання результатів виконання процесу.

3.3. Таксономія властивості усталеності

На рис. 5 наведено таксономію властивості усталеності. Властивостям усталеності пропонується надати такі визначення:

Інституціональність – властивість, що характеризує рівень інституціонального закріплення процесів захисту інформації в організації та рівень сформованості інституту інформаційної безпеки в організації.

Повторюваність – властивість, що характеризує систематичність виконання процесів захисту інформації в організації та стабільність результатів виконання процесів.

Координованість – властивість, що характеризує рівень координації дій суб'єктів під час виконання процесів захисту інформації на рівні окремого процесу, групи процесів або організації у цілому.

3.4. Таксономія властивості прогнозованості

На рис. 6 наведено таксономію властивості прогнозованості.

Властивостям усталеності пропонується надати такі визначення:

Об'єктивна вимірюваність – властивість, що характеризує рівень застосування об'єктивних показників, критеріїв та методик вимірювання (оцінювання) властивостей та характеристик процесів захисту інформації та їх результатів.

Об'єктивна керованість – властивість, що характеризує ефективність системи управління процесом на основі кількісного зворотного зв'язку.



Рис. 4. Таксономія властивості «Керованість»



Рис. 5. Таксономія властивості «Усталеності».

3.5. Таксономія властивості удосконалюваності

На рис. 7 наведено таксономію властивості удосконалюваності.

Властивостям усталеності пропонується надати такі визначення:

Удосконалюваність організаційних можливостей – властивість, що характеризує рівень впровадження процесів постійного удосконалення ПЗІ.

Підвищуваність ефективності ПЗІ – властивість, що характеризує виконання специфічних завдань, що спрямовані на забезпечення постійного контролю виконання ПЗІ та підвищення його ефективності.

Аналіз розробленої таксономії дозволяє зробити такі висновки:

1. Загальна таксономія зрілості (рис. 4.5) є повною таксономією, що відповідає всім висунутим вимогам.

2. Таксономії властивостей керованості та прогнозованості не відповідають вимозі 4.2, тому

що відсутній єдиний атомарний рівень. Це вказує на те, що актуальними є дослідження, які дозволять виявити властивості, що є підкласами властивостей спланованості, впорядкованості та повторюваності.

3. Таксономії властивостей прогнозованості та оптимальності є дворівневими ієрархіями. Тому доцільно проведення подальших досліджень, з метою визначення атомарних властивостей зрілості для цих таксономій. Виявлення атомарних властивостей значно полегшить розробку системи показників та критеріїв оцінки властивостей прогнозованості та оптимальності.

ВИСНОВКИ

Впорядкування властивостей зрілості на основі таксономічних відношень є проявлення загальносистемної закономірності ієрархічності властивості зрілості. У відповідності до цієї закономірності будь-яка система складається з підсистем (елементів) і водночас є підсистемою (елемен-

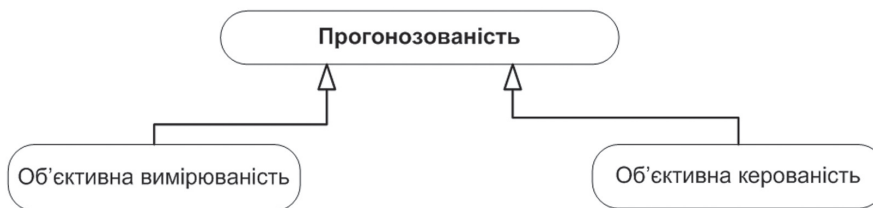


Рис. 6. Таксономія властивості «прогнозованості»

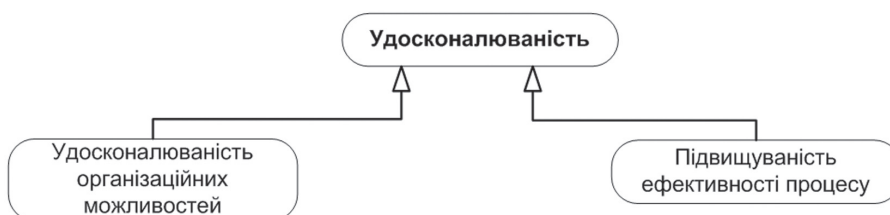


Рис. 7. Таксономія властивості «удосконалюваності»

том) системи більш високого порядку. Ієрархічна упорядкованість передбачає, що всі системи розташовуються по рівням ієрархії. Використання цієї закономірності у нашому випадку дозволяє нам розглядати зрілість як інтегративну, комплексну властивість та під час дослідження декомпозувати її на сукупність (множину) властивостей, які упорядковуються за відношенням ієрархічного підпорядкування. Таке уявлення спрощує у подальшому ідентифікацію ознак зрілості, проектування діяльності із забезпечення зрілості ПЗІ, здійснювати оцінювання зрілості тощо.

Література.

- [1] Потій О.В. Сутність категорії „зрілість” та змістовна модель зрілості процесів захисту інформації // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Т.5, 2006. - №1. – С. 139-147.
- [2] Потій О.В., В.Ф. Козак. Основні положення системодіяльної методології захисту інформації // Прикладная радиоэлектроника. – Т. 6, №3, 2007. – С. 407-418.
- [3] Потій О.В. Ентропійна модель зрілості процесів захисту інформації // Системи обробки інформації - № 7(65), 2007. – С. 74-77.
- [4] Потій О.В. Визначення функції зрілості процесів захисту інформації // Системи озброєння та військової техніки - № 2(16), 2007. – С. 101-104.
- [5] Арчибальд Р. Управление высокотехнологичными программами и проектами. – М.: Компания АйТи; ДМК Пресс, 2004. – 472 с.
- [6] Керцер Г. Стратегическое планирование для управления проектами с использованием модели зрелости. – М.: Компания АйТи, ДМКПресс, 2003 – 320 с.
- [7] ДСТУ ISO/IEC TR 15504-2002 Інформаційні технології. Оцінювання процесів життєвого циклу програмних засобів. (Частини 1-9).
- [8] ISO/IEC 21827: 2002. Information technology - Systems Security Engineering - Capability Maturity Model.
- [9] Control Objective for Information and related Technology (CobiT). IT Governance Institute, ISACA/ - 2000.
- [10] ISO/IEC 15408-3. Information technology - Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. 1999.
- [11] НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року №22.
- [12] ITIL IT Management Practices: Information Technology Infrastructure Library. Practices and guidelines developed by Central Computer and Telecommunications Agency (CCTA), London, 1995.
- [13] ДСТУ ISO/IEC TR 13335:2003. Інформаційні технології. Наставни з керування безпекою інформаційних технологій. Частина 1: Концепції та моделі безпеки інформаційних технологій. Частина 2: Керування та планування безпеки інформаційних технологій. Частина 3: Методи керування безпекою інформаційних технологій.
- [14] Cook-Davis, Terry Schlichter John, Bredillet Christophe, Beyond the PMBOK Guide / Proc. Of the PMI2001 Seminars&Symposium. – Nashville, TN, Network Square, PA: Project Management Institute, Nov. 1-10, 2001.
- [15] Schlichter John. The Project Management Maturity Model – An Update of the PMI's OPM3 Program. Режим доступу: <http://www.pmforum.org>
- [16] IDEF5 Method Report. – Armstrong Labarastory AL/HRGA. Wright-Patterson Air Force Base. – 1994.
- [17] Клещев А.С., Шалфеева Е.А. Каталог свойств онтологий. Принципы организации каталога. Препринт, 2007. Владивосток: ИАПУ ДВО РАН, 2007. – 24 с.
- [18] Шалфеева Е.А., Грибова В.В. Внутренние свойства онтологий. – Труды IV Международной конференции «Идентификация систем и задачи управления» SICPRO'05. Москва. – С. 1109-1128.

Надійшла до редколегії 24.09.2009



Потій Олександр Володимирович, доктор технічних наук, доцент, професор кафедри БІТ ХНУРЕ. Область наукових інтересів: проектування та розробка засобів КЗІ.