$$= \int_{\substack{0 \\ (\alpha=1,3)}}^{1} M(КВК(M_{\alpha}^{e_A}))\,d\alpha = \int_{0}^{0,8} 0{,}335\,d\alpha + \int_{0,8}^{0,9} 0{,}049\,d\alpha + \int_{0,9}^{1} 0{,}055\,d\alpha = 0{,}439.$$

З розрахунків ФУП видно, що $F(\underset{\sim}{B}^{eA}) < F(КВК(\underset{\sim}{M}^{A})) < F(\underset{\sim}{ДВ}^{eA})$. Отже поточне КВК ($\underset{\sim}{M}^{A}$) знаходиться між $\underset{\sim}{B}^{eA}$ і $\underset{\sim}{ДВ}^{eA}$, але, відповідно до розрахунків, ближче до $\underset{\sim}{B}^{eA}$. Отже, результат застосування побудованих нечітких евристичних правил показує, що можливість сканування портів на заданий момент часу – висока.

V Висновки

Описані моделі можуть використовуватися в загальній концепції побудови моделей і технологій систем ідентифікації атак як додатковий засіб, що дозволяє виявляти аномалії у відповідному середовищі, які створюються, наприклад, в результаті дії різних складних механізмів, закладених у сучасних скануючих утилітах.

Література: ***1.*** *Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа . – СПб: Наука и техника, 2004. – 384 с.* ***2.*** *Коул Э. Руководство по защите от хакеров: Пер. с англ. – М.: Издательский дом "Вильямс", 2002. – 640 с.* ***3.*** *Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. – 2-е изд. – СПб.: БХВ-Петербург, 2003. – 368 с.* ***4.*** *Лукацкий А. В. Обнаружение атак. – СПб.: БВХ–Петербург, 2001. – 624 с.* ***5.*** *Бэнкс М. Психи и маньяки в Интернете. – Пер. с англ. – СПб: Символ-Плюс, 1998. – 320 с.* ***6.*** *Модели принятия решений на основе лингвистической переменной / А. Н. Борисов, А. В. Алексеев, О. А. Крумберг и др. – Рига: Зинатне, 1982. – 256 с.* ***7.*** *Обработка нечеткой информации в системах принятия решений / А. Н. Борисов, А. В. Алексеев, Г. В. Меркурьева и др. – М.: Радио и связь, 1989. – 304 с.* ***8.*** *Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.: Мир, 1976. – 166 с.* ***9.*** *Вероятность и математическая статистика. Энциклопедия / Под ред. Прохорова Ю. В. - М.: БРЭ, 1999. – 910 с.* ***10.*** *Кофман А. Введение в теорию нечетких множеств.- М.: Радио и связь, 1982. – 432 с.* ***11.*** *Корченко О. Г. Системи захисту інформації: Монографія – К.: НАУ, 2004. – 264 с.*

УДК 681.3.06

МЕТОДИКА ВИЗНАЧЕННЯ ЦІЛЬОВОГО ПРОФІЛЮ ЗРІЛОСТІ ПРОЦЕСІВ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ МЕТОДУ ВИРІШУЮЧИХ МАТРИЦЬ

Олександр Потій, Анатолій Лєншин
Харківський національний університет радіоелектроніки

Анотація: **Пропонується методика визначення цільового профілю зрілості з урахуванням вимог до конфіденційності, цілісності та доступності критичних інформаційних ресурсів.**
Summary: **The approach to designate purpose maturity profile according with integrity, confidentiality and availability requirements to critical informational assets are proposed.**
Ключові слова: **Модель зрілості процесів захисту інформації, безпека інформації, попарні порівняння.**

Вступ

Сучасні підходи до захисту інформації потребують застосування комплексних рішень завдань захисту інформації. Одним із елементів таких рішень є управління зрілістю процесів захисту інформації. Завдання управління потребує прийняття рішень та здійснення коректуючих впливів. Прийняття рішень (наприклад, начальником служби захисту інформації) можливо за таких умов:

- наявні альтернативи;
- визначені цілі;
- визначені обмеження на реалізацію поставлених цілей.

Тобто якщо немає альтернатив – немає об’єкту відносно якого потрібно приймати рішення, якщо

немає цілей – рішення взагалі не потрібно приймати, якщо немає обмежень, то будь-яке рішення буде оптимальним, точніше – саме поняття „оптимальності" втрачає сенс. При прийнятті рішень щодо захисту інформації об'єктивно існують альтернативи, тобто різні шляхи реалізації захисту в різних сферах практичної діяльності (процедурній, адміністративній, програмно-технічній тощо). Як обмеження виступають кошти, виділені на організацію захисту, кількість особового складу та час, протягом якого необхідно нейтралізувати викриті загрози. Задача визначення цілей трактується при здійсненні управління зрілістю процесів як визначення цільового профілю зрілості, тобто необхідного підрівня зрілості для кожного напрямку практичної діяльності щодо захисту інформації. Дана стаття присвячена розробці методики визначення цільового профілю зрілості.

I Основи оцінки зрілості процесів захисту інформації. Постановка задачі та загальний підхід до визначення цільової зрілості

У даній роботі автори дотримуються погляду на захист інформації як на особливу форму діяльності (соціальної, організаційної, технічної, управлінської та інформаційної) [1]. У такому контексті управління безпекою інформації є не що інше, як організація та здійснення управління діяльністю із захисту інформації. Одним з принципів управління безпекою інформації є принцип використання процесного підходу [2]. Суть принципу полягає у тому, що бажаний результат захисту інформації досягається ефективніше, коли пов'язані ресурси та діяльність (дії, роботи, заходи) управляються як процес. Застосування принципу приводить до того, що захист інформації, як діяльність, представляється як взаємопов'язана сукупність процесів захисту інформації, а у найвищому еволюційному розвитку – як система процесів захисту інформації.

У загальному сенсі пропонується таке визначення процесу захисту інформації (ПЗІ) – це сукупність дій, спрямованих на реалізацію заходів захисту (безпеки), розробку та/або практичне застосування способів (механізмів) та засобів захисту інформації.

Застосування процесного підходу в управлінні безпекою інформації забезпечує:

- ✓ строге визначення процесу досягнення бажаного результату захисту інформації;
- ✓ виявлення та вимірювання результатів ПЗІ;
- ✓ виявлення інтерфейсу ПЗІ з іншими функціями організації;
- ✓ оцінку можливого ризику, його наслідків та впливу ПЗІ на інтереси суб'єктів захисту інформації;
- ✓ чіткий розподіл відповідальності, повноважень та підзвітності під час управління процесом;
- ✓ виявлення суб'єктів та об'єктів, що приймають участь у реалізації ПЗІ, а також сторін, зацікавлених у результатах ПЗІ;
- ✓ більшу конкретизацію під час проектування діяльності; при проектуванні процесу більша увага приділяється діям (операціям, роботам), потокам, в основному інформаційним потокам, контрольним показникам, потребам у підготовці персоналу, обладнанні (інструментарії), методах, матеріалах та інших ресурсах, потрібних для досягнення бажаного результату.

Таким чином, діяльностний та процесний підходи формують основу для структуризації діяльності із захисту інформації, представлення її як сукупності процесів, що надає певні переваги, а саме:

- ✓ під час формування стратегії та політики безпеки інформації використання визначених ПЗІ в усій організації призведе до більш передбачених результатів, більш ефективного використання ресурсів, скорочення часу циклу та зниження витрат;
- ✓ для встановлення цілей захисту та показників захисту; розуміння зрілості ПЗІ сприяє виробленню конкретних цілей та планових показників захисту;
- ✓ у контексті управління безпекою інформації прийняття процесного підходу до всіх заходів безпеки призводить до зниження витрат, запобігання помилкам, поліпшення контролю за відхиленням, скорочення часу виконання завдань та більш передбаченим результатам;
- ✓ у контексті управління персоналом встановлення ефективних за витратами процесів з управління персоналом, що сприяє проведенню цих процесів відповідно до потреб організації та забезпечує підвищення компетентності персоналу.

Такий підхід до захисту інформації дозволить більш ґрунтовно підійти до проблеми атестації комплексної системи захисту інформації та сформулювати методичний апарат атестації процесів захисту інформації, основою якого є оцінка ПЗІ з метою визначення або вдосконалення рівня зрілості ПЗІ. Під зрілістю процесу будемо розуміти здатність процесу досягати своєї мети та відповідати своєму призначенню. Зрілість процесу проявляється через набуття ним певних властивостей або характеристик. До базових характеристик будемо відносити такі:

- ✓ неповнота процесу;
- ✓ здійснюваність процесу;

- ✓ керованість процесу;
- ✓ усталеність процесу;
- ✓ прогнозованість процесу;
- ✓ удосконаленість процесу.

З точки зору управління безпекою інформації перед суб'єктом управління стоїть завдання щодо визначення поточного рівня зрілості ПЗІ, визначення бажаного рівня зрілості процесу (або цільової зрілості), визначення та реалізація сукупності дій для досягнення цільової зрілості. У загальному випадку цільова зрілість (*ЦЗ*), поточна зрілість (*ПЗ*) та сукупність дій пов'язані між собою таким виразом:

$$ЦЗ(t) = f\left(ПЗ(t_0), \overline{U_{t_0,t}}\right) \quad (1)$$

де $ЦЗ(t)$ – цільова зрілість, яка планується до досягнення на момент часу *t*, $ПЗ(t_0)$ – поточна зрілість, що досягнута процесом на момент часу t_0, $U_{t_0,t}$ – сукупність заходів для досягнення *ЦЗ*, f – функція переходу.

Визначення зрілості ПЗІ ґрунтується на оцінюванні процесів. Процеси оцінюються на відповідність одній або декільком оціночним моделям. Результати оцінки відбиваються з використанням встановленої системи мір та рейтингів, що входять до нормативної (еталонної) моделі. На рис. 1 наведена контекстна діаграма процесу визначення зрілості процесу.

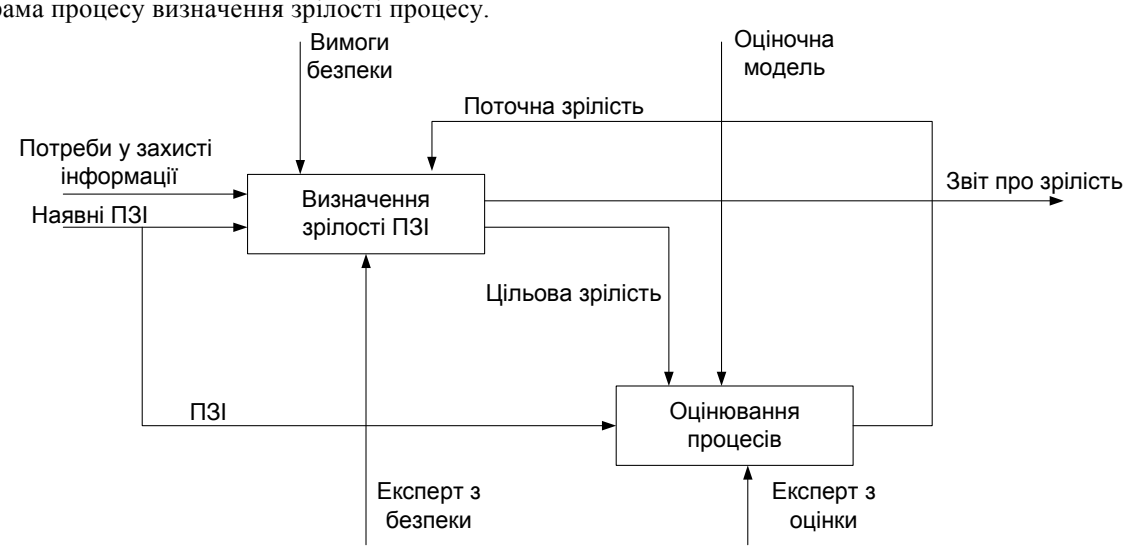


Рисунок 1 – Процес визначення зрілості процесу

Потреби та сподівання суб'єктів захисту інформації відбиваються у специфікації вимог безпеки. Вимоги для визначення рівня зрілості процесу мають документуватися у специфікації вимог безпеки (за аналогією зі специфікацією вимог гарантій у Єдиних критеріях [3]). Із аналізу специфікації вимог визначається цільова зрілість, яка представляє бажаний рівень зрілості ПЗІ, а також об'єм оцінювання. Під цільовою зрілістю будемо розуміти зрілість ПЗІ, яка за думками суб'єкту захисту інформації та замовника оцінки зрілості забезпечить прийнятну ступінь ризику для успішної реалізації визначеної вимоги безпеки.

Важливою задачею є визначення рівня цільової зрілості, яка потім зіставляється з поточною зрілістю. Її вирішення пропонується здійснювати на основі аналізу значущості різних напрямків практичної діяльності щодо захисту інформації за допомогою залучення експертної групи із урахуванням рівнів критичності інформації, що циркулює в інформаційно-телекомунікаційній системі (ІТС) організації. Пропонується така загальна методика визначення рівня цільової зрілості ПЗІ.

1. На основі аналізу захищеності об'єктів, що підлягають захисту, існуючих загроз та вразливостей ІТС, рівня критичності інформації, яка циркулює в ІТС, визначається найвищий рівень вимог, що висуваються до конфіденційності, цілісності та доступності інформації, а отже і до ІТС в цілому.

2. Із врахуванням задач забезпечення конфіденційності, цілісності та доступності інформації проводиться декомпозиція загальної задачі захисту. По результатам декомпозиції будується дерево ієрархій діяльності з забезпечення безпеки інформації.

3. Експертна група здійснює експертне оцінювання відносної значущості складових побудованої ієрархії та вагомості напрямків практичної діяльності для задоволення вимог безпеки. Проводиться обчислення коефіцієнтів відносної значущості напрямків практичної діяльності щодо захисту інформації із застосуванням методу вирішуючих матриць.

4. На основі одержаних на попередньому кроці коефіцієнтів відносної значущості розраховується цільова зрілість процесів захисту інформації.

II Визначення найвищого рівня зрілості, що потребується

Класифікацію інформації пропонується здійснювати за методикою, розробленою відповідно до вимог НД ТЗІ 1.4-001-2000 [4] на основі Федерального стандарту США FIPS 199 [5] та німецького стандарту BSI [6].

Згідно з положеннями НДТЗІ 2.5-004-99 [7] до інформації висуваються вимоги щодо конфіденційності, цілісності, доступності. Відповідно до НДТЗІ 1.1-003-99 [8] властивості інформації визначаються таким чином:

- **конфіденційність інформації** (information confidentiality) – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем та/або процесом;
- **цілісність інформації** (information confidentiality) – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем та/або процесом;
- **доступність інформації** (information availability) – властивість інформації, яка полягає в тому, що користувач або процес, який наділений відповідними повноваженнями, може використовувати її відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (невеликого) проміжку часу, тобто, вона знаходиться у тому вигляді, у тому місці та часі, що необхідні користувачу.

У табл. 1 наведено характеристику потенційно можливих збитків для кожної вимоги безпеки [5].

Таблиця 1 – Рівні збитків внаслідок порушення вимог безпеки

Вимога безпеки	Потенційно можливий рівень збитків		
	Низький	Середній	Високий
Конфіден-ційність	Неавторизоване розкриття або ознайомлення із інформацією може призвести до обмеженого впливу на діяльність, ресурси та співробітників організації	Неавторизоване розкриття або ознайомлення із інформацією може призвести до серйозного (відчутного) впливу на діяльність, ресурси та співробітників організації	Неавторизоване розкриття чи ознайомлення із інформацією може викликати тяжкий або навіть катастрофічний вплив на діяльність, ресурси та співробітників організації
Цілісність	Неавторизована модифікація або знищення інформації може призвести до обмеженого впливу на діяльність, ресурси та співробітників організації	Неавторизована модифікація або знищення інформації може призвести до серйозного (відчутного) впливу на діяльність, ресурси та співробітників організації	Неавторизована модифікація чи знищення інформації може викликати тяжкий або навіть катастрофічний вплив на діяльність, ресурси та співробітників організації
Доступність	Припинення доступу або використання інформації, що обробляється, чи інформаційних систем може призвести до обмеженого впливу на діяльність, ресурси та співробітників організації	Припинення доступу або використання інформації, що обробляється, чи інформаційних систем може призвести до серйозного (відчутного) впливу на діяльність, ресурси та співробітників організації	Припинення доступу або використання інформації, що обробляється, чи інформаційних систем може викликати тяжкий або навіть катастрофічний вплив на діяльність, ресурси та співробітників організації

Для визначення розміру впливу на діяльність, ресурси та співробітників організації застосовують критерії, наведені в абл.. 2 [5].

Таблиця 2 – Критерії визначення рівня збитків

Обмежені збитки (низький рівень)		
№	Категорії збитків	Критерії
1.	Ефективність виконання завдань та робіт організації	✓ існує вплив на виконання окремих завдань та робіт, але ефективність виконання цих завдань організації знижується не суттєво;

Продовження Таблиці 2

		✓ максимальний час недоступності ресурсу більше 24 годин
2.	Шкода ресурсам організації	✓ мінімальна шкода ресурсам організації ✓
3.	Порушення законів, інструкцій та контрактів	✓ порушення правил та законів може викликати лише незначні наслідки; ✓ невеликі порушення умов контракту, які призводять до незначних штрафних санкцій;
4.	Фінансові втрати	✓ Фінансові втрати прийнятні для організації
5.	Негативний вплив на імідж організації	✓ мінімальний підрив репутації/довіри
6.	Шкода, заподіяна співробітникам організації	✓ мінімальний вплив на соціальний та фінансовий стан співробітників; ✓ імовірність травматизму дуже низька
Серйозні (відчутні) збитки (середній рівень)		
№	Категорії збитків	Критерії
1.	Ефективність виконання завдань та робіт організації	✓ існує вплив на виконання окремих завдань та робіт, який значно знижує їх ефективність та може призвести до суттєвого порушення організацією своїх окремих зобов'язань та планових задач; ✓ максимальний час недоступності від 1 до 24 годин
2.	Шкода ресурсам організації	✓ заподіяна значна шкода ресурсам організації
3.	Порушення законів, інструкцій та контрактів	✓ порушення правил та законів із значними наслідками; ✓ крупні порушення умов контракту, які призводять до накладання великих штрафних санкцій
4.	Фінансові втрати	✓ фінансові втрати значні для організації, але вона може їх витримати
5.	Негативний вплив на імідж організації	✓ очікується значний підрив репутації/довіри
6.	Шкода, заподіяна співробітникам організації	✓ значний вплив на соціальний та фінансовий стан співробітників; ✓ існує імовірність травматизму співробітників
Катастрофічні збитки (високий рівень)		
№	Категорії збитків	Критерії
1.	Ефективність виконання завдань та робіт організації	✓ існує вплив на виконання завдань та робіт, який призводить до неможливості виконання організацією своїх зобов'язань; ✓ максимальний час недоступності менше 1 години
2.	Шкода ресурсам організації	✓ руйнування ресурсів організації
3.	Порушення законів, інструкцій та контрактів	✓ фундаментальне порушення правил та законів; ✓ крупні порушення умов контракту із деструктивними наслідками
4.	Фінансові втрати	✓ фінансові втрати, які організація може не витримати
5.	Негативний вплив на імідж організації	✓ Підрив репутації/довіри в державному /національном масштабі; ✓ виникнення загрози існуванню організації
6.	Шкода, заподіяна співробітникам організації	✓ може призвести до соціального та фінансового краху співробітників; ✓ небезпека життю та здоров'ю співробітників організації

Вимоги безпеки (ВБ) можуть бути висунені як до інформації користувачів, так і до системної інформації, що може зберігатися в електронному або у паперовому вигляді.

Важливість інформаційного ресурсу визначається через трійку пар типу (**вимога безпеки**, *величина збитку*), тобто [5]

ВБ (тип інформації) = {(**конфіденційність**, *рівень збитку*),
(**цілісність**, *рівень збитку*),
(**доступність**, *рівень збитку*)}.

Наприклад:

ВБ (особові дані про працівників) = {(**конфіденційність**, *середній*),
(**цілісність**, *низький*),
(**доступність**, *низький*)}.

Позначимо інформаційний ресурс як i. Тоді сукупність інформаційних ресурсів організації буде представлено множиною $I = \{i_1, \text{K}, i_n\}$, де n – кількість інформаційних ресурсів організації. Множину вимог до конфіденційності позначимо як $K = \{k_1, \text{K}, k_n\}$, до цілісності $Ц = \{ц_1, \text{K}, ц_n\}$, доступності $Д = \{д_1, \text{K}, д_n\}$. Визначимо вимоги безпеки до кожного інформаційного ресурсу, згідно з наведеними критеріями (табл. 2).

Визначення загальних вимог безпеки до інформації здійснюється за принципом максимуму. Тобто розглядаються питання про потенційні збитки, які можуть бути нанесені при порушенні конфіденційності, цілісності та доступності інформаційним ресурсам. Суворість вимоги визначається збитком або сумою збитків, які мають місце у найсерйозніших випадках порушень безпеки. Таким чином:

$$K_{\max} = \max_{j=\overline{1,n}} k_j \qquad Ц_{\max} = \max_{j=\overline{1,n}} ц_j \qquad Д_{\max} = \max_{j=\overline{1,n}} д_j \tag{2}$$

Використовуючи (2) визначимо вимоги безпеки до інформації ІТС організації в цілому.

Будемо вважати, що для деякої гіпотетичної організації були одержанні такі вимоги безпеки $K_{\max} = "високий"$, $Ц_{\max} = "високий"$, $Д_{\max} = "середній"$.

III Декомпозиція загальної задачі захисту

Декомпозиція загальної задачі захисту має проводитися відповідно до сучасних поглядів на захист інформації, які викладено у стандартах галузі захисту інформації ISO/IEC 17799 [9], ISO/IEC 28147 [10], NIST SP 800-26 [11], NIST SP 800-53 [12].

Загальної задачею захисту є забезпечення такого стану ІТС, в якому за допомогою визначених процесів захисту інформації, технічних, криптографічних та організаційних заходів забезпечується конфіденційність, цілісність та доступність інформації, що обробляється в ІТС. Таким чином, цілями першого рівня є задачі забезпечення конфіденційності, цілісності та доступності інформації. Оскільки вимоги безпеки мають забезпечуватися шляхом проведення заходів безпеки, що належать до різних сфер практичної діяльності із забезпечення захисту інформації, цілями другого рівня є проведення заходів безпеки відповідних сфер практичної діяльності. Цілями третього рівня є виконання процесів захисту інформації, що визначені у напрямках практичної діяльності із забезпечення безпеки інформації (рис. 2).

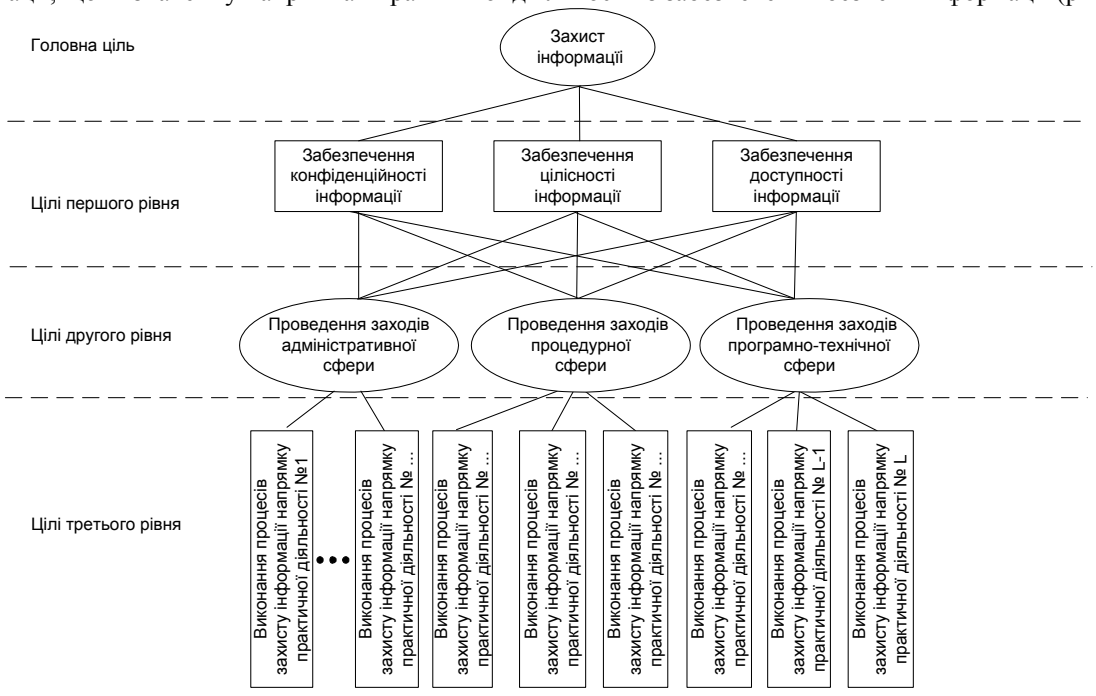


Рисунок 2 – Ієрархія вимог згідно з NIST SP 800-26

Вибір того чи іншого способу декомпозиції вихідної задачі залишається за експертною групою та особою, що приймає рішення. Для подальшого розгляду методики використаємо декомпозицію запропоновану в NIST SP 800-26 – як найбільш складну для проведення обчислень.

IV Проведення експертного оцінювання відносної значущості складових побудованої ієрархії

Загальна задача захисту інформації є ціллю вищого рівня, що позначається як X_1^0. Індекси умовних позначень мають таке змістовне навантаження: X_l^k ціль k-го рівня з порядковим номером на рівні, що дорівнює l.

Цілі другого рівня: забезпечення конфіденційності інформації – позначається як X_1^1, забезпечення цілісності інформації – X_2^1, забезпечення доступності інформації – X_3^1.

В табл. 3, 4 наведено позначення для сфер захисту та напрямків практичної діяльності щодо захисту інформації відповідно.

Оцінки значущості вкладу підцілей у досягнення цілі вищого рівня здійснюються зверху вниз попарним порівнянням [13]. Сутність попарного порівняння, наприклад X_i^1 та X_j^1 відносно до цілі X^0 полягає у оцінці суджень про те, у якій мірі X_i^1 більш важлива (більш вагома) для досягнення цілі X^0 ніж підціль X_j^1. Позначимо цю оцінку через α_{ij}. Подібні оцінки надаються експертами. На практиці рекомендовано вживати шкалу оцінок, що надана в табл. 5.

Таблиця 3 – Умовні позначення для сфер практичної діяльності

	Назва сфери практичної діяльності	Умовне позначення
1	Адміністративна	X_1^2
2	Процедурна	X_2^2
3	Програмно-технічна	X_3^2

Таблиця 4– Умовні позначення для напрямків практичної діяльності

	Назва напрямку практичної діяльності	Умовне позначення
1	Управління ризиками	X_1^3
2	Аналіз заходів з забезпечення безпеки інформації	X_2^3
3	Життєвий цикл	X_3^3
4	Сертифікація та акредитація	X_4^3
5	План захисту системи	X_5^3
6	Кадрова безпека	X_6^3
7	Фізична безпека та захист обладнання	X_7^3
8	Управління виробництвом, вхідний/вихідний контроль	X_8^3
9	Планування безперервної роботи	X_9^3
10	Експлуатація апаратного та програмного забезпечення	X_{10}^3
11	Цілісність даних	X_{11}^3

12	Документація	X_{12}^3
13	Інформування, тренування та навчання	X_{13}^3
14	Реагування на інциденти	X_{14}^3
15	Ідентифікація та автентифікація	X_{15}^3
16	Логічні засоби управління доступом	X_{16}^3
17	Журнали аудиту	X_{17}^3

Таблиця 5 – Шкала оцінок

Перевага X_i над X_j	Відсутня	Помірна	Значна	Велика	Дуже велика	Проміжні оцінки
α_{ij}	1	3	5	7	9	2, 4, 6, 8

Результати оцінок заносяться у таблиці (матриці) для підцілей r-ого рівня, матриця парних порівнянь буде мати вигляд, наведений в табл. 6.

У лівому стовпці та першому (верхньому) рядку записуються цілі, що порівнюються. У верхній лівій клітинці записується ціль, відносно якої оцінюються підцілі нижчого рівня.

Таблиця 6 – Заповнення таблиці попарних порівнянь

X^{r-1}	X_1^r	X_2^r	...	X_t^r	$q_j^{(r-1)}$	$\gamma_j^{(r-1)}$
X_1^r	1	$\alpha_{12}^{(r)}$	...	$\alpha_{1t}^{(r)}$	$q_1^{(r-1)}$	$\gamma_1^{(r-1)}$
X_2^r	$\alpha_{21}^{(r)}$	1	...	$\alpha_{2t}^{(r)}$	$q_2^{(r-1)}$	$\gamma_2^{(r-1)}$
M	M	M	1	M	M	M
X_t^r	$\alpha_{t1}^{(r)}$	$\alpha_{t2}^{(r)}$	...	1	$q_t^{(r-1)}$	$\gamma_t^{(r-1)}$

У результаті попарного порівняння заповнюється матриця оцінок, що являє собою зворотно симетричну матрицю відносно головної діагоналі. Зрозуміло, що порівняння підцілі з собою дорівнює одиниці, тобто матриця буде заповнена по головній діагоналі одиницями.

Отримані експертні оцінки підлягають обробці таким чином:

- обчислюється середнє геометричне для кожного рядка:

$$q_j^{(r-1)} = \sqrt[t_r]{\alpha_{j1}^{(r)} \text{K} \times \alpha_{jj}^{(r)} \times \alpha_{jt_r}^{(r)}} \tag{3}$$

- обчислюються нормовані значення:

$$\gamma_j^{(r-1)} = \frac{q_j^{(r-1)}}{\sum_{i=1}^{t_r} q_i^{(r-1)}}. \tag{4}$$

Величина γ_j^{r-1} характеризує значущість підцілі $X_j^{(r)}$ для цілі $X^{(r-1)}$.

Сукупність усіх γ_j^{r-1} складає вектор-стовпчик значень вкладу цілі r-ого рівня в досягнення цілі $r-1$ рівня.

Необхідною умовою при використанні експертних оцінок є перевірка їх узгодженості за таким алгоритмом [13].

1) Розрахувати власне число матриці $L_{\max}$:

$$L_{\max} = \sum_{i=1}^{n} \gamma_i^{(r-1)} \sum_{j=1}^{n} \alpha_{ji}^{(r)}, \tag{5}$$

де $\gamma_i^{(r-1)}$ – i -та компонента вектору вкладу в досягнення цілі $r-1$ рівня, $\alpha_{ji}^{(r)}$ – експертна оцінка відносної значущості підцілей r -го рівня з номерами j та i.

2) Обчислити індекс узгодженості $IУ$:

$$IУ = \frac{(L_{\max} - n)}{(n-1)}, \tag{6}$$

де n – порядок матриці.

3) Взяти значення випадкової узгодженості $ВипУ$ для визначеного розміру таблиці попарних порівнянь (табл. 7)

Таблиця 7 – Значення випадкової узгодженості для матриць різного порядку

Порядок матриці	1	2	3	4	5	6	7	8	9	10
Випадкова узгодженість	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49

4) Розрахувати відношення узгодженості $Відн У$:

$$Відн У = \frac{IУ}{ВипУ}. \tag{7}$$

5) Порівняти одержаний на кроці (4) результат з граничним значенням: якщо: $Відн У >= 0{,}2$ експертні оцінки не узгоджені, якщо $Відн У < 0{,}2$ то експертні оцінки є узгодженими.

Проведемо експертне оцінювання відносної значущості елементів дерева цілей, що одержано в результаті проведення декомпозиції (рис. 1)

Для табл. 8 – 10 при наданні експертних оцінок відносна значущість цілей другого підрівня оцінюється виходячи з того, проведенню заходів якої сфери практичної діяльності надається перевага при вирішенні задачі забезпечення визначеної вимоги безпеки інформації. Оцінки надаються відповідно до реальних можливостей організації з проведення заходів та з урахуванням середовища експлуатації ІТ системи.

Таблиця 8 – Таблиця попарних порівнянь значущості сфер практичної іяльності для забезпечення вимоги конфіденційності інформації

X_1^1	X_1^2	X_2^2	X_3^2	$q_j^{(1)}$	$\gamma_j^{(1)}$
X_1^2	1	5	1	1,7008	0,455
X_2^2	1/5	1	1/5	0,345	0,09
X_3^2	1	5	1	1,7008	0,455
$Відн У = 0$					

Таблиця 9 – Таблиця попарних порівнянь значущості сфер практичної діяльності для забезпечення цілісності інформації

X_2^1	X_1^2	X_2^2	X_3^2	$q_j^{(1)}$	$\gamma_j^{(1)}$
X_1^2	1	5	1/5	1	0,212
X_2^2	1/5	1	1/8	0,292402	0,062
X_3^2	5	8	1	3,419952	0,726
$Відн У = 0{,}1482$					

Таблиця 10 – Таблиця попарних порівнянь значущості сфер практичної діяльності для забезпечення доступності інформації

X_3^1	X_1^2	X_2^2	X_3^2	$q_j^{(1)}$	$\gamma_j^{(1)}$
X_1^2	1	1/6	3	0,793	0,184
X_2^2	6	1	5	3,107	0,721
X_3^2	1/3	1/5	1	0,405	0,095
$ВідхУ = 0{,}1878$					

Заповнюючи таблиці попарних порівнянь експертна група порівнює відносну значущість виконання процесів захисту інформації напрямку практичної діяльності із забезпечення захисту інформації в межах сфери практичної діяльності із забезпечення захисту інформації до якої вони відносяться. Оцінки надаються відповідно до реальних можливостей організації з виконання процесів, з урахуванням середовища експлуатації ІТС та результатів аналізу загроз. Результати оцінки наведені в табл. 11, 12 та 13

.

Таблиця 11 – Таблиця попарних порівнянь значущості напрямків практичної діяльності

X_1^2	X_1^3	X_2^3	X_3^3	X_4^3	X_5^3	q_j^2	$\gamma_j^{(2)}$
X_1^3	1	3	4	7	1	2,425805	0,362
X_2^3	1/3	1	2	3	1/3	0,922108	0,138
X_3^3	1/4	1/2	1	3	1/4	0,622865	0,094
X_4^3	1/7	1/3	1/3	1	1/7	0,295878	0,044
X_5^3	1	3	4	7	1	2,425805	0,362
$ВідхУ = 0{,}014$							

Для одержаних нами експертних оцінок виконується нерівність $ВідхУ < 0{,}2$. Таким чином, оцінки є узгодженими, а їх якість залежить від кваліфікації підібраної групи експертів.

Таблиця 12 – Таблиця попарних порівнянь значущості напрямків практичної діяльності

X_2^2	X_6^3	X_7^3	X_8^3	X_9^3	X_{10}^3	X_{11}^3	X_{12}^3	X_{13}^3	X_{14}^3	q_j^2	$\gamma_j^{(2)}$
X_6^3	1	0,5	1/5	1/4	1/4	1/6	1/3	0,5	1/3	0,338	0,030
X_7^3	2	1	1/4	1/3	1/3	1/5	1/2	1	1/2	0,520	0,045
X_8^3	5	4	1	2	2	1/2	3	4	3	2,244	0,196
X_9^3	4	3	1/2	1	1	1/3	2	3	2	1,423	0,124
X_{10}^3	4	3	1/2	1	1	1/3	2	3	2	1,423	0,124
X_{11}^3	6	5	2	3	3	1	4	5	4	3,274	0,286
X_{12}^3	3	2	1/3	1/2	1/2	1/4	1	2	1	0,857	0,075
X_{13}^3	2	1	1/4	1/3	1/3	1/5	1/2	1	1/2	0,520	0,045
X_{14}^3	3	2	1/3	1/2	1/2	1/4	1	2	1	0,857	0,075
$ВідхУ = 0{,}0137$											

Таблиця 13 – Таблиця попарних порівнянь значущості напрямків практичної діяльності

X_3^2	X_{15}^3	X_{16}^3	X_{17}^3	q_j^2	$\gamma_j^{(2)}$
X_{15}^3	1	7	2	2,410	0,592
X_{16}^3	1/7	1	1/5	0,305	0,075
X_{17}^3	1/2	5	1	1,357	0,333
$Відн У = 0{,}0143$					

V Розрахунок цільової зрілості процесів захисту інформації

Обчислимо значущість напрямків практичної діяльності захисту інформації, використавши метод вирішуючих матриць. Для обчислення коефіцієнта значущості напрямків практичної діяльності, необхідно помножити коефіцієнт значущості виконання процесів захисту інформації відповідного напрямку на коефіцієнт значущості проведення заходів відповідної сфери із захисту інформації для забезпечення вимоги безпеки.

Розрахунок окремого коефіцієнта вектора значущості для забезпечення конкретної вимоги безпеки $V(ВБ) = \{v_1(вб), \text{К}, v_n(вб)\}$ здійснюється за формулою:

$$v_i(вб) = \gamma_j^{21}(вб) \cdot \gamma_i^{32},\ i = \overline{1,n},\ j = f(i),\ j \in \overline{1,t}\ , \tag{8}$$

де n – кількість напрямків практичної діяльності, t – кількість сфер практичної діяльності, $f(i)$ – функція, що повертає порядковий номер сфери до якої відноситься i-ий напрямок практичної діяльності, γ_m^{sp} – коефіцієнт значущості цілі рівня s з порядковим номером m для цілі рівня p.

Як вимоги безпеки виступають конфіденційність, цілісність та доступність інформації. Таким чином розрахована матриця коефіцієнтів вагомості впливу напрямків практичної діяльності на забезпечення вимог безпеки, що висуваються для інформації буде ($V(КЦД)$) мати розмір $3 \times n$, де n – кількість напрямків практичної діяльності.

Коефіцієнти значущості для конфіденційності – це вектор $V(К) = \{v(К)_1, \text{К}, v(К)_n\}$ розмірністю n, елементи якого дорівнюють елементам першого рядка матриці $V(КЦД)$.

Коефіцієнти значущості для цілісності – це вектор $V(Ц) = \{v(Ц)_1, \text{К}, v(Ц)_n\}$ розмірністю n, елементи якого дорівнюють елементам другого рядка матриці $V(КЦД)$.

Коефіцієнти значущості для доступності – це вектор $V(Д) = \{v(Д)_1, \text{К}, v(Д)_n\}$ розмірністю n, елементи якого дорівнюють елементам третього рядка матриці $V(КЦД)$.

Використовуючи (8), розрахуємо чисельні значення матриці коефіцієнтів вагомості впливу напрямків практичної діяльності з забезпечення вимог безпеки для наданих у пункті 3 експертних оцінок.

$$V(КЦД) = \begin{Vmatrix} 0.165 & 0.063 & 0.043 & 0.020 & 0.165 & 0.003 & 0.004 & 0.018 & 0.011 & 0.011 & 0.026 & 0.007 & 0.004 & 0.007 & 0.269 & 0.034 & 0.152 \\ 0.077 & 0.029 & 0.020 & 0.009 & 0.077 & 0.002 & 0.003 & 0.012 & 0.008 & 0.008 & 0.018 & 0.005 & 0.003 & 0.005 & 0.430 & 0.054 & 0.242 \\ 0.067 & 0.025 & 0.017 & 0.008 & 0.067 & 0.022 & 0.032 & 0.141 & 0.089 & 0.089 & 0.206 & 0.054 & 0.032 & 0.054 & 0.056 & 0.007 & 0.032 \end{Vmatrix}$$

Для побудови цільового профілю зрілості використаємо модель зрілості процесів захисту інформації, апропоновану в міжнародному стандарті ISO/IEC 28147. Визначена модель нараховує 5 рівнів зрілості. Враховуючи те, що етапом розвитку зрілості процесів, які виконуються в організації, вважається атестація на відповідність підрівню зрілості, а також з метою підвищення точності визначення цільового профілю як шкалу будемо використовувати підрівні моделі зрілості. В ISO/IEC 28147 нараховується 12 підрівнів моделі зрілості (табл. 14)

Цільовий профіль – це множина номерів підрівнів моделі зрілості, визначених для кожного напрямку практичної діяльності. Цільовий профіль позначається як $ЦП = \{цп_1, \text{К}, цп_n\}$.

Проведемо розрахунок елементів цільового профілю зрілості для напрямків практичної діяльності. При обчисленні будемо виходити з таких міркувань:

1) якщо найвищий рівень вимоги до інформації, що обробляється в ІТС організації, визначений як високий, то напрямок практичної діяльності, що відповідає за його задоволення, має відповідати критеріям

найвищого рівня зрілості, тобто має бути атестованим на відповідність дванадцятому підрівню зрілості для визначеної моделі;

Таблиця 14 – Підрівні моделі зрілості згідно з ISO/IEC 28147

№	Назва підрівня зрілості
1	1.1 Виконання базових практик
2	2.1 Планування виконання
3	2.2 Дисципліна виконання
4	2.3 Оцінка/перевірка виконання
5	2.4 Контроль (відстеження) виконання
6	3.1 Визначення стандартних процесів (робіт)
7	3.2 Виконання визначених процесів (робіт)
8	3.3 Координація робіт
9	4.1 Введення показників якості досягнення цілей
10	4.2 Об'єктивне управління виконанням робіт
11	5.1 Підвищення якості управління
12	5.2 Підвищення ефективності процесів (робіт)

2) якщо найвищий рівень вимоги до інформації, що обробляється в ІТС організації, визначений як середній, то напрямок практичної діяльності, що відповідає за його задоволення має відповідати критеріям рівня зрілості, визнаним світовою спільнотою як базовий; на сучасному етапі таким рівнем визнано третій рівень, на якому мають бути визначені усі процеси захисту, тобто напрямок має бути атестованим на відповідність восьмому підрівню зрілості для визначеної моделі;

3) якщо найвищий рівень вимоги до інформації, що обробляється в ІТС організації, визначений як низький, то процеси захисту інформації мають відповідати першому рівню зрілості, тобто бути атестованими на відповідність першому підрівню „Виконання базових практик”;

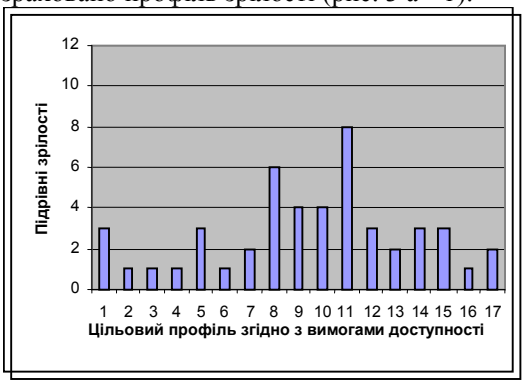
4) якщо в результаті обчислення профілю відносно вимог безпеки для одного напрямку практичної діяльності встановлюються різні підрівні зрілості процесів захисту інформації, то з метою задоволення усіх вимог має бути обраним підрівень з найбільшим порядковим номером; вибір підрівня здійснюється за виразом:

$$цn_i = \max_{j=\overline{1,g}} \left(\left\lceil L_j \cdot \left(v\left(КЦД\right)_{ji} / W_j \right) \right\rceil \right), \forall i = \overline{1,n} \qquad (9)$$

де $W_j = \max_{a=\overline{1,n}} (v\left(КЦД\right)_{ja}) \forall\ a = \overline{1,n}$, L_j – максимальний підрівень зрілості відповідно до значень $K_{\max}$, $Ц_{\max}$, $Д_{\max}$, g – кількість вимог безпеки (g=3), операція $\lceil\ \rceil$ – позначає округлення до найближчого цілого.

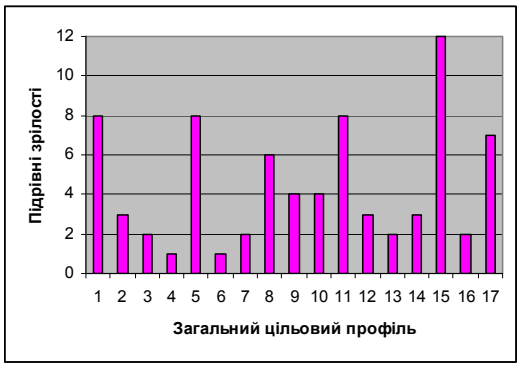
За результатами одержаних експертних оцінок було розраховано профіль зрілості (рис. 3 а – г).

а)



в)

б)



г)

Рисунок 3 – Цільові профілі зрілості

Висновки

В статті запропоновано методику визначення цільового профілю зрілості процесів захисту інформації. Як математична база прийняття рішення використовується метод вирішуючих матриць, для призначення коефіцієнтів значущості напрямків практичної діяльності – метод попарних порівнянь. Визначення необхідно рівня зрілості процесів захисту інформації ґрунтується на попередньому аналізі вимог безпеки до інформації, що циркулює в організації. Для вирішення задачі декомпозиції запропоновано використовувати стандарти в галузі захисту інформації. Методика може бути застосована на етапах первинного обстеження підприємства, що проводиться з метою визначення вимог безпеки під час аудиту безпеки та оцінки рівня зрілості процесів захисту інформації.

Застосування методики дозволяє визначити цільові орієнтири для роботи служби захисту інформації.

Література: ***1.*** *Потий А. В., Управление безопасностью информации: сущность и базовые принципы, // VIII Международная научно-практическая конференция"Безопасность информации в информационно-телекоммуникационных системах", Тезисы докладов. – К.: НИЦ "Тезис", 2005 г., 69-70 с.* ***2.*** *Потій О. В., Процесний підхід до управління безпекою інформації //VIII Международная научно-практическая конференция"Безопасность информации в информационно-телекоммуникационных системах", Тезисы докладов. – К.: НИЦ "Тезис", 2005 г., 35-36 с.* ***3****. ISO/IEC 15408, 1999: Information technology - Security techniques - Evaluation criteria for IT security.* ***4.*** *НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.* ***5.*** *FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems* ***6.*** *Bundesamt fur Sicherheit in der Informationstechnik. IT Baseline Protection Manual, 1998* ***7.*** *НД ТЗІ 2.5-004-99. Критерії захищеності інформації комп'ютерних системах від несанкціонованого доступу .* ***8.*** *НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.* ***9.*** *ISO/IEC 17779:2000 Code of practice for information securit management* ***10.*** *ISO/IEC 21827: 2002 Information technology - Systems Security Engineering - Capability Maturity Model* ***11.*** *NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems* ***12.*** *NIST SP 800-53, Recommended Security Controls for Federal Information Systems* ***13.*** *Саати Т. Принятие решений. Метод анализа иерархий. – М: Радио и связь, 1999. – 341с.*

УДК 681.3.06

ПОБУДОВА ФУНКЦІЙ НАЛЕЖНОСТІ ЕКСПЕРТНИХ ОЦІНОК ДО ЗОН БАЗОВИХ ДУМОК У ПРОСТОРІ СУБ'ЄКТИВНОЇ ЛОГІКИ

Анатолій Лєншин
ЗАТ „Інститут інформаційних технологій"

Анотація: **Пропонується підхід до побудови функцій належності експертних оцінок щодо зрілості процесів захисту інформації до зон базових думок у просторі суб'єктивної логіки.**
Summary: **The approach to create membership function for expert estimations of information security process maturity to opinion base regions in the space of subjective logic are proposed**