УДК 004.056.5

Архипов О.Є., Петренко М.А.

ЗАСТОСУВАННЯ ОНТОЛОГІЧНИХ ІЄРАРХІЙ У ЗАДАЧАХ ВИЗНАЧЕННЯ ЦІННОСТІ ІНФОРМАЦІЇ

В статті розглянуто проблему експертно-аналітичного визначення цінності інформації (інформаційних ресурсів), яка через суб'єктивізм експертів та можливі спрощення процедури оцінювання призводить до збільшення імовірності помилок в результатах експертизи. Щоб запобігти цьому, доцільно певним чином регламентувати проведення процедури прямого експертного оцінювання, обмеживши в ній передумови виникнення суттєвих суб'єктивних похибок. Зокрема цим вимогам задовольняє застосування так званого ноніусного підходу до визначення цінності інформаційних ресурсів, що, однак потребує попередньої структуризації інформації у відповідній предметній сфері (галузі діяльності). Вдалою формою такої структуризації є онтологічна ієрархія інформаційних елементів сфери (галузі) діяльності. На прикладах існуючих застосувань інформаційних онтологічних ієрархій проаналізовано їхні основні властивості. Запропонований підхід до формування інформаційної онтологічної ієрархії, що спирається на структуру існуючих в організації функціонально-виробничих зв'язків. Крім того, дослідження цих зв'язків з позицій забезпечення сталості виробничих процесів та якості кінцевої продукції дозволяє отримати достатньо прозорі оцінки цінності інформаційних елементів, що утворюють різні рівні інформаційної онтології.

Ключові слова: ноніусний підхід, онтологія, цінність інформації, експертно-аналітичний метод, інформаційні ресурси, ієрархія.

Вступ. Одним із базових положень побудови систем захисту інформації (СЗІ) є принцип розумної достатності, відповідно до якого витрати на побудову та супровід СЗІ мають співставлятися з можливими втратами, обумовленими реалізаціями загроз щодо інформації, яка підлягає захисту. Це дозволяє оптимізувати витрати на створення СЗІ, забезпечивши адекватність рівня захисту рівню цінності інформації. Тому визначення кількісного значення цінності інформації, яку треба захищати, є провідним моментом процедури оптимізації витрат на СЗІ. На методологічному рівні принцип розумної достатності реалізується в концепціях аналізу та керування інформаційними ризиками. Однак практичне втілення цих концепцій в процесі створення СЗІ вимагає вирішення ряду проблемних питань, одне з яких – оцінювання цінності інформації, зокрема інформаційних ресурсів (ІР), які захищаються. Актуальність цього питання наглядно підтверджується тією увагою, що приділяється йому в численних нормативних та настановчих документах [1,2,3,4], причому фактично всі означені документи у якості основного механізму оцінювання цінності ІР визначають метод експертно-аналітичних оцінок. Як приклад, можна взяти стандарт ДСТУ ISO/IEC TR 13335-3 [1], в якому даний метод експертизи цінності ІР використовується в рамках так званого «детального аналізу ризиків», що являє собою один з варіантів корпоративної стратегії аналізування ризиків. Процедура експертно-аналітичного оцінювання кожного ІР базується на системі критеріїв, за якими сукупна оцінка цінності ІР формується з витрат на його створення (придбання, обслуговування, відновлення) та можливих збитків організації, яка володіє ІР, обумовлених реалізацією загроз щодо конфіденційності, цілісності та доступності відповідного ІР.

Взагалі ефективне застосування методики «детального аналізу ризиків» вимагає від експерта глибоких знань (як в сфері інформаційних технологій, так і в сфері ділової активності організації), значного часу та зусиль. Тому експерти в своїй практичній діяльності часто віддають перевагу так званому «неформальному підходу» до аналізу ризиків [1], в якому експертиза цінності ІР спирається не на структурно-аналітичні методи аналізу витрат та прогнозування можливих збитків, а виключно на персональний досвід та рівень поінформованості експерта у відповідній предметній галузі. Тобто експерт, минаючи багатоетапну аналітичну процедуру, відразу визначає цінність ІР в цілому, не переймаючись її формуванням шляхом інтеграції певної кількості попередньо визначених фрагментарних (часткових) оцінок. Подібне пряме експертне оцінювання дає суттєву економію зусиль і часу, однак разом з тим істотно збільшує ймовірність суб'єктивних помилок в результатах експертизи. Через це було б доцільно певним чином регламентувати проведення процедури прямого експертного оцінювання. На жаль в означених вище документах подібна інформація відсутня, зокрема, в [1] визначено лише суть «неформального підходу».

Постановка задачі. Можна припустити, що експерт, формулюючи свої висновки в ході прямої експертизи, свідомо чи підсвідомо спирається на систему певних уявлень про цінність групи добре відомих йому ІР, які він вважає базовими в сфері даної фахової діяльності. Тому, складаючи свою експертну оцінку щодо цінності представленого на експертизу нового ІР, експерт «вмонтовує» цей новий ІР до існуючої системи базових ресурсів і інтерполює його ціннісний показник за вже відомими значеннями цінності як «близьких» так і «віддалених» базових ресурсів.

На жаль отримана інтерполяційна оцінка є результатом, який формується у спосіб, що звичайно лишається поза можливістю його свідомої фіксації експертом [5].Тим не менш з літератури відомі спроби побудови евристико-емпіричних процедур, мета яких – заміщення експерта у процесі формування експертного висновку або суттєве спрощення його продукування. Зокрема в [6,7] запропоновано так званий ноніусний підхід до визначення цінності ІР, який дозволяє поступово конкретизувати клас, групу, підгрупу ресурсів, близьких за певними характеристиками об'єкту експертизи, послідовно звужуючи до прийнятного обсягу множину базових ресурсів, призначених до порівняльного зіставлення з новим ІР.

Проілюструємо роботу ноніусної схеми. Припустимо, що оцінюється важливість інформаційного ресурсу IR, зміст якого – дані контракту про постачання певного виду військової техніки до деякої країни (рис.1).

Загальний обсяг документів у сфері зовнішніх відносин становить:

$$N = \sum_i n_i = \sum_i \sum_k m_{ik} = \sum_i \sum_k \ldots \sum_r L_{ikr} \qquad (1)$$

Відповідно до суті ноніусного підходу, деталізуючи характер та особливості ресурсу IR, поступово спускаємося щаблями ієрархії рис.1, редукуючи початкову множину з N аналізуємих документів до вмісту певної «атомарної» комірки з обмеженою кількістю базових інформаційних ресурсів $\{IR_l\}, l = \overline{1, L}$. Вважаємо, що цінність c_l кожного з цих ресурсів вже відома і разом вони утворюють скінчену лінійно впорядковану множину $\{c_1, c_2, ..., c_L\}$. Для вироблення рішення щодо цінності c_{IR} ресурсу IR експерту потрібно «втиснути» цей ресурс у множину $\{IR_l\}$, та, орієнтуючись за ціновими показниками елементів цієї множини, визначити цінність c_{IR}. Можливою формою оцінки може бути зважена сума:

$$c_{IR} = \sum_l w_l c_l, \qquad (2)$$

де w_l - система ваг, що задаються експертом за результатами співставлення ресурсу IR з іншими елементами множини $\{IR_l\}$ із застосуванням методу попарних порівнянь Сааті чи у інший спосіб. Надалі оцінений ресурс IR можна ввести до множини базових ресурсів.

Слід зазначити, що умовою реалізації ноніусного підходу є існування ієрархії взаємопов'язаних понять, які охоплюють певну предметну (фахову) галузь. Саме наявність такої ієрархії дозволяє здійснити віднесення об'єкту експертизи до певної підгрупи базових ресурсів.

Ще одним прикладом прямого експертного оцінювання, близьким за своєю суттю до ноніусного підходу, є процедура надання грифа секретності матеріальним носіям секретної інформації (МНСІ). Гриф секретності має відповідати ступеню секретності інформації, розміщеної на МНСІ, який визначається шляхом зіставлення змісту цієї інформації зі змістом статей Зводу відомостей, що становлять державну таємницю (ЗВДТ) [8] та виявленням конкретної статті, під зміст якої підпадає інформація, розміщена на МНСІ. Реалізація цієї пошукової процедури забезпечується ієрархічною структурою ЗВДТ [8], яка дозволяє достатньо просто віднайти відповідну статтю.

Онтологічна ієрархія. В обох наведених вище прикладах прийняття рішень базується на використанні специфічних ієрархічних структур – онтологій, вивченню, розробленню та застосуванню яких останнім часом приділяється значна увага [9,10].

Онтологія – це спроба всеосяжної та детальної формалізації деякої області знань за допомогою концептуальної схеми. Зазвичай така схема складається зі структури даних, які містить усі релевантні класи об'єктів, їх точні специфікації для певної предметної області, зв'язки і правила (теореми, обмеження), прийняті в цій області.

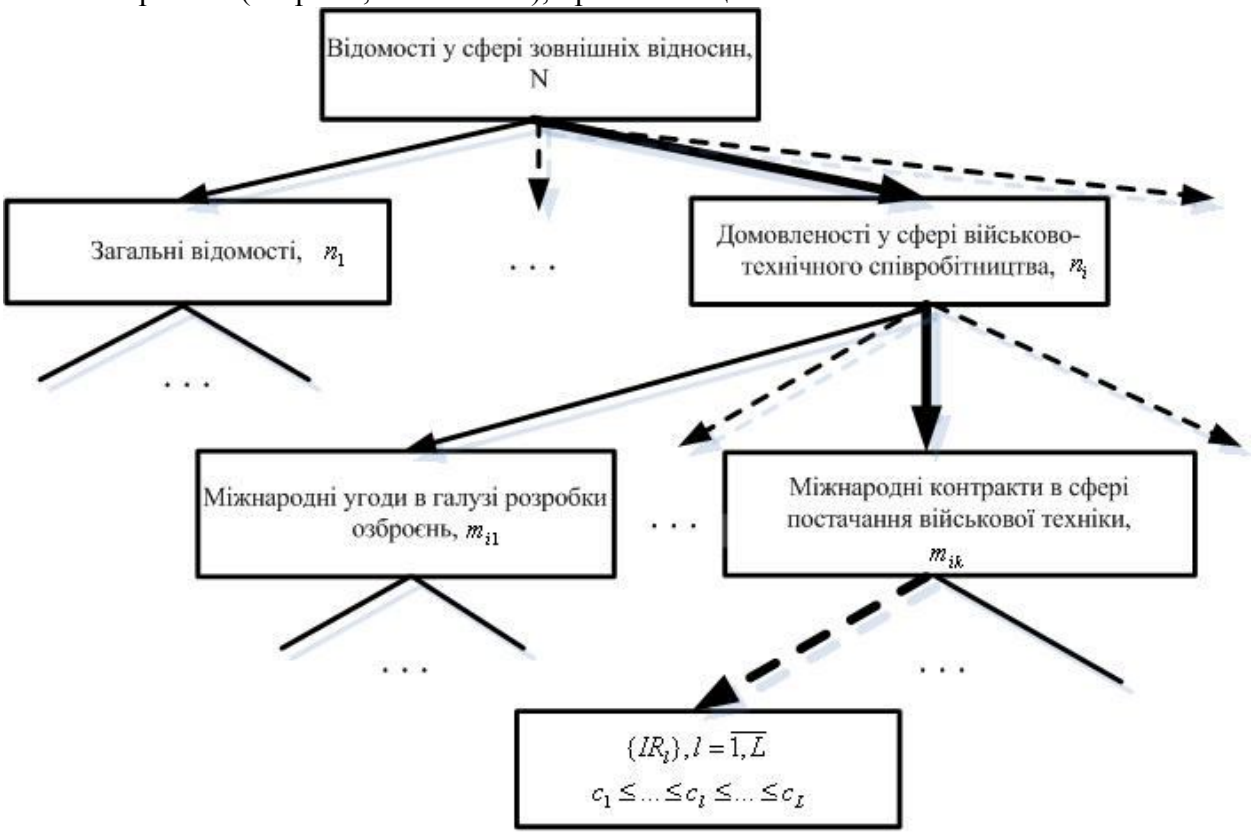

Рис.1. Приклад схеми класифікації інформаційних ресурсів у певній предметній сфері

Вперше поняття онтології, як формального опису термінів, зустрічається в області вивчення штучного інтелекту. Проте, останнього часу дане поняття поширюється і на інші предметні області.

Потреба в розробці онтологій виникає в разі необхідності виконання структуризації знань у певній предметній області для багаторазового повторного використати цих знань або для спільного розуміння широким загалом користувачів структури інформації у різних сферах діяльності.

В найпростішому випадку побудова онтології зводиться до виділення базових понять предметної області та встановлення співвідношень між ними. Однією з проблем розробника онтології є необхідність виявлення усіх елементів, які входять до складу предметних областей. Проте онтологічна структура має бути динамічною щодо змін. Онтології зазвичай будуються на аналізі функціональних властивостей та зв'язків елементів певної предметної області або на аналізі змісту термінів відповідної сфери, їх співпідрядності.

Одним з прикладів вдалого застосування та використання онтологічного аналізу можна вважати ЗВДТ. В ЗВДТ всі сфери діяльності розподілено на чотири: сфера оборони, сфера економіки, науки і техніки, сфера зовнішніх відносин та сфера державної безпеки і охорони правопорядку [11]. Відповідно, сфера оборони містить основні специфікації понять щодо даних про вид збройних сил, округ, полки, окремі військові частини, тощо. Сфера економіки охоплює специфікації питань мобілізаційної потужності, створення державних матеріальних резервів, формування, фінансування та виконання оборонного замовлення й т.п. Те саме стосується і інших сфер діяльності. Всі вони містять в собі певні специфіковані поняття, які в свою чергу розкриваються через ще більш деталізовані та конкретизовані

категорії. Фактично кожна із зазначених сфер являє собою часткову онтологічну ієрархію, що поглинається ще більш загальною онтологічною ієрархією, кореневим поняттям якої є вся множина відомостей, які становлять державну таємницю. З іншого боку будь який елемент цієї онтологічної ієрархії припускає своє розвинення у відповідну часткову ієрархічну структуру. Зразком такого розвинення є онтологічна ієрархія, що утворилася з поняття **Відомості у сфері зовнішніх відносин** (розділ ЗВДТ) (рис.1) і являє собою часткову онтологію загальної ієрархічної онтології ЗВДТ. Менша за обсягом часткова ієрархічна структура підпорядкована інформаційному ресурсу **Домовленості у сфері військово-технічного співробітництва**, ще більш обмежена – ресурсу **Міжнародні контракти в сфері постачання військової техніки**. Підлеглі ієрархічні структури відсутні лише для елементів найнижчого "атомарного" рівня онтології ресурсів секретної інформації сфери зовнішніх відносин.

Такий же підхід можна використовувати при побудові онтологій і в інших випадках, зокрема для організацій, в тому числі і комерційних: всю сукупність даних, понять, термінів чи об'єктів, які утворюють предметну область у сфері функціонування відповідної організації, треба категоріювати, дати докладні специфікації цих категорій та вказати їх зв'язки, можливі підпорядкованості, залежності. Для ЗВДТ ці категорії розроблено державними експертами в процесі багаторічної роботи, а ефективність отриманої структуризації секретної інформації підтверджена часом. Однак чи можна забезпечити належну якість проведення онтологічного аналізу у більш стислий час, при залученні до цієї справи спеціалістів різних рівнів компетентності, які не є фаховими експертами або навіть зовсім не мають досвіду проведення експертиз? Як формалізувати цей процес?

Методика побудови онтологічної ієрархії визначення цінності інформації. Припустимо, що об'єктом онтологічного аналізу є представлена у різних формах (в тому числі і у вигляді сукупності ІР) інформація, існування якої є необхідною умовою сталого та якісного функціонування деякої виробничої організації, мета діяльності якої – створення (виготовлення) певного матеріального продукту (товарів).

Як відомо, виробництво – це сукупність взаємопов'язаних процесів: основних, допоміжних і обслуговуючих [12]. Основними процесами є технологічні процеси (ТП) виробництва, завдяки яким саме і утворюється матеріальний продукт – основний результат виробництва. В зв'язку з цим процес формування онтологічної інформаційної ієрархії виробничої організації треба починати з аналізу найнижчих щаблів виробництва, тобто з визначення інформації, задіяної у основних виробничих процесах (або бізнес – процесах, якщо виробництво не є матеріальним, наприклад, якщо мета діяльності організації – надання послуг). Зокрема, якщо мова йде про певне матеріальне виробництво, починати треба з аналізу його основних ТП.

На Рис.2 наведено фрагмент схеми ТП, представленого на рівні виконання окремих операцій (кружечки на схемі –виконання відповідних операцій). Потовщені стрілки на схемі вказують на потоки інформації (I_1, I_2, I_3, I_6), відбір якої забезпечує контроль параметрів вихідної сировини і матеріалів, задіяних у процесі виробництва, та характеристик стану ТП. Ця так звана параметрична інформація (дані зворотнього зв'язку), яка передається від об'єкта управління (ТП) до системи управління ТП. За результатами оброблення отриманих даних система управління видає інформацію, яка передається каналом прямого зв'язку (інформаційні потоки I_4, I_5) до об'єкту управління.

Ця інформація, змінюючи режими роботи сервісних пристроїв та устаткування, безпосередньо пов'язаних з регулюванням стану ТП, забезпечує оптимізацію виконання окремих операцій ТП та технологічного циклу виробництва в цілому. Загалом усю перелічену вище інформацію можна узагальнити єдиним поняттям «технологічна інформація».

Аналогічним чином можна проаналізувати інші ТП, що входять до виробничого циклу організації. Крім різних фрагментів технологічної інформації основне виробництво буде характеризуватися інформацією про випуск кінцевого продукту, постачання та

споживання сировини, енергоресурсів, кількісними та якісними показниками виробництв в цілому і т.ін. Слід також зазначити, що в межах управління даним ТП реалізуються зв'язки із суміжними ТП, забезпечується ремонт устаткування та обладнання, постачання інструментів.

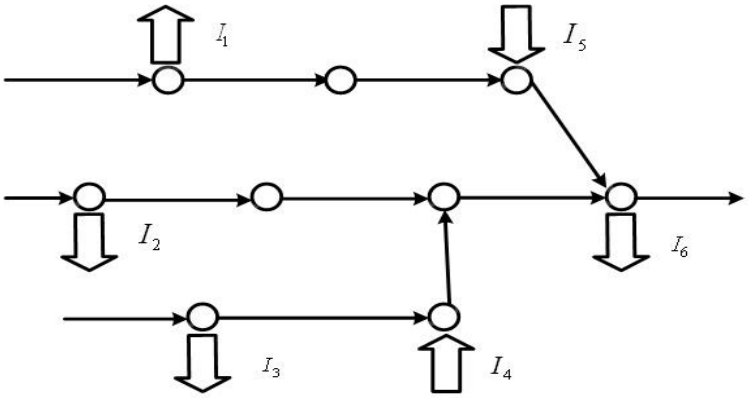

Рис.2. Фрагмент схеми технологічного процесу

Крім того, до складу організації мають входити забезпечуючи підрозділи, в яких циркулює фінансово-економічна інформація, статистично-звітна інформація, відомості кадрової служби (включно з відповідними персональними даними), інформація, пов'язана з розробкою, проектуванням, технологічною підготовкою та плануванням випуску нових видів продукції тощо. Представлена у документованому вигляді, уся ця інформація становить внутрішні інформаційні ресурси організації. Циркуляцію цих документів в організації забезпечує система документообігу та архівний підрозділ.

Окремий ІР формується з інформаційних потоків, орієнтованих назовні організації (зовнішня інформація). Це відомості про продаж та маркетинг, логістику та постачання, податковий облік та виплату податків, зовнішнє інвестування, портфель замовлень, інше.

Загалом уся інформація, перелічена вище, являє собою **Сукупну інформацію організації**, яку можна представити у вигляді багаторівневої ієрархії. На першому рівні виокремлемо:

1.Внутрішня інформація / 2.Зовнішня інформація.

Деталізуючи їх, отримуємо елементи другого рівня ієрархії:

1.1. Виробнича інформація / 1.2.Інформація забезпечуючих підрозділів

2.1. Відомості про продаж та маркетінг / 2.2. Статистично-звітна інформація / 2.3. Рекламно-довідкова інформація / 2.4. Розрахунки з постачальниками та отримувачами продукції / ...

Третій рівень ієрархії:

1.1.1. Технологічна інформація / 1.1.2. Документація з технологічної підготовки виробництва;

1.2.1. Дані про бухгалтерський облік / Відомості про облік та керування кадрами / Планово-фінансова інформація / Адміністративно-керівна інформація / Аналітико-маркетингова інформація / ...

. . . . . .

2.1.1. Відомості про постачальників, обсяги закупівель та специфікації сировини, матеріалів / 2.1.2. Договори з покупцями товарів, специфікації до них / 2.1.3. Ведення цінових структур, формування прайс-листів / ...

. . . . . .

В тих випадках коли це є необхідним або доцільним, можливо введення додаткових рівнів ієрархії. Наприклад:

1.1.1.1. Параметрична інформація: I_1, I_2, I_3, / 1.1.1.2. Інформація прямого каналу керування ТП: I_4, I_5.

Ступінь деталізації за напрямами онтологічної ієрархії індивідуальна для кожного з них і тісно пов'язана з можливістю підрахунку цінності інформації відповідного найнижчого рівня ієрархії. Так, якщо найнижчі "атомарні" комірки ієрархії за напрямом **1.1. Виробнича інформація** утворюють елементи параметричної інформації та інформації прямого каналу керування ТП, їх цінність обраховується за втратами від блокування чи перекручування (модифікації) цієї інформації, що призводить до погіршення якості продукту ТП, збільшенню відсотку браку або зупинці ТП.

Загалом цінність технологічної інформації будь-якого ТП (бізнес-процесу) визначається через оцінку впливу негативних наслідків реалізації загроз відносно цілісності чи доступності цієї інформації на характеристики стану ТП (бізнес-процесу) , його сталість. При такій оцінці враховується опосередкований вплив атак на інформаційні ресурси через зміни у вартості кінцевих продуктів ТП (на окремих стадіях бізнес-процесу) та продукції виробництва в цілому. Зокрема для "атомарних" елементів інформації I_1 - I_6 отримуємо часткові оцінки корисності (важливості) кожного типу цієї інформації для забезпечення виробничого процесу. Узагальнення (об'єднання) інформації I_1 - I_6 в категорію **1.1.1.Технологічна інформація** має супроводжуватися обрахуванням відповідної сукупної оцінки втрат від реалізації загроз щодо цієї категорії. Загалом мають бути отримані сукупні оцінки впливу кожної із загроз за кожним узагальненим ІР (типізованою інформаційною категорією) по всім підрозділам організації.

Доречно зауважити, що особливістю подібної процедури визначення цінності інформації або ІР є те, що вона відбувається на початковому етапі аналізу ризиків, коли ще відсутня деталізація можливих для даної організації інформаційних загроз та способів їх реалізації. Тому відповідно до вже сталого розуміння змісту поняття "цінність інформації" реальна цінність інформації (ІР) визначається винятково за впливом порушень доступності, цілісності та конфіденційності конкретної інформації (ІР) на діяльність (стан функціонування) організації, точніше за можливими втратами організації через ці порушення.

Для зовнішньої інформації організації (як і для деяких видів внутрішньої) часто характерні підвищені вимоги до її конфіденційності. Розрахунок можливих втрат в цьому випадку носить ймовірнісний характер й виконується із залучення ситуаційно-сценарних методів прогнозування [6,13].

Підкреслимо, що наведена вище методика побудови інформаційної онтології базована на виділенні основних інформаційних елементів онтології та встановленню співвідношень між ними шляхом аналізу функціонально-виробничої структури організації. Очевидно, що це є не єдино можливий підхід до формування онтології. Зокрема можна сподіватися на ефективне застосування для побудови онтології так званої інформаційної піраміди, яка характеризує особливості та властивості інформації, задіяної на різних рівнях управління організацією[14]: стратегічному, тактичному, оперативному. Цей підхід дозволяє ввести до структури онтології достатню кількість інформаційних елементів, що зможуть більш-менш повно представити предметну сферу, однак структура їх взаємозв'язків буде відрізнятися від відповідної структури, отриманої при побудові онтології за функціонально-виробничим принципом.

Висновки. Спрощення процедури експертного визначення цінності інформації (інформаційних ресурсів) за умов збереження достатньо високого рівня якості експертних оцінок можна отримати при використання так званого ноніусного підходу. Однак можливість його застосування вимагає попередньої структуризації інформації у певній предметній сфері (галузі діяльності). Вдалою формою такої структуризації є побудова онтологічної ієрархії інформаційних елементів відповідної сфери (галузі) діяльності. Аналіз існуючих застосувань інформаційних онтологічних ієрархій, їх основних властивостей та особливостей структури обумовлює доцільність використання у формування інформаційної онтологічної ієрархії підходу, який базується на вивчені та досліджені комплексу реалізованих в організації функціонально-виробничих процесів. Метою цих досліджень є

визначення складу, змісту та взаємозв'язків інформації, чия наявність забезпечує ефективне та стале функціонування організації. Саме на базі цієї інформації формується інформаційна онтологія.

Крім того, дослідження цих зв'язків з позицій забезпечення сталості виробничих процесів та якості кінцевої продукції дозволяє достатньо прозоро обчислити цінність певних інформаційних блоків, що утворюють різні рівні інформаційної онтології.

ЛІТЕРАТУРА

1. ДСТУ ISO/IEC TR 13335-3 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 3. Методи керування захистом IT.
2. ISO/IEC 27005, Information Technology – Security techniques – Information security risk management.
3. Еталонні архітектури MSA. – К. Майкрософт Україна; К.: Видавнича група BHV, 2005. – 352 с.
4. Руководство по управлению рисками безопасности. [Электронный ресурс / Группа разработки решений Майкрософт по безопасности и соответствию регулятивным нормам и Центр Microsoft Security Senter of Excellence. – : http://www.microsoft.com/rus/technet/security/guidance/complianceandpolicies/secrisk/
5. Архипов О.Є. Моделювання і прогнозування в соціальній сфері: Навч.-метод. посіб. / О.Є. Архипов, С.А.Архіпова. – К.: ІВЦ"Політехніка", 2001. – 60 с.
6. Архипов О.Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою: моногр. / О.Є.Архипов, О.Є.Муратов. – К.: Наук.-вид. відділ НА СБ України, 2011. – 195с.
7. Архипов О.Є. Щодо методики ідентифікації та оцінювання активів системи інформаційних технологій /О.Є. Архипов // Захист інформації. – №1(50), 2011. – С. 42-47.
8. Корченко О.Г. Модель складної орієнтованої мережі ЗВДТ / О.Г.Корченко, О.Є.Муратов, Ю.О.Дрейс, І.О.Козлюк // Захист інформації – №3, 2011. – С. 87-93.
9. Петренко Н. Компьютерные онтологии и онтолого-управляемая архитектура информационных систем / Krassimir Markov, Vitalii Velychko, Oleksy Voloshin // Information Models of Knowledge. - Kiev, Ukraine – Sofia, Bulgaria, 2010. – с.86-92
10. Рогушина Ю.В. Використання методу індуктивного виведення для вдосконалення онтології предметної області пошуку / Ю.В.Рогушина, І.Ю.Гришанова // Системні дослідження та інформаційні технології – №1, 2007. – . 62-70.
11. Звід відомостей, що становлять державну таємницю України. – К.: Друкарня Служби безпеки України, 2005. – 70 с.
12. Справочник проектировщика АСУ ТП / Г.Л.Смилянский, Л.З.Амлинский, В.Я.Баранов и др.; Под ред. Г.Л.Смилянского. – М.: Машиностроение, 1983. – 527 с.
13. Архипов О.Є. Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації / О.Є.Архипов, І.П.Касперський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип.2(15). – К. 2007. – С.13-19.
14. Информационные технологии управления / Под ред. Ю.М.Черкасова. –М.:ИНФРА-М, 2001. – 216 с.

Надійшла: 15.12.2011

Рецензент: д.т.н., проф. Корченко О.Г.