Онтологічний підхід до розробки національних стандартів України з оцінювання безпеки інформаційних технологій

© Рогушина Ю.В.
Інститут програмних систем НАН України, Київ, Україна
ladamandraka2010@gmail.com
© Гладун А.Я
Міжнародний науково-навчальний центр інформаційних технологій та систем НАН України та МОН України, Київ, Україна
glanat@yahoo.com
© Снігир Г.В.
ПрАТ "Міжнародні Авіалінії України", Київ, Україна
mandraka1966@gmail.com

Анотація

Розробка нормативно-правової бази України для підтримки інформаційної безпеки, яка повинна відповідати міжнародним стандартам та кращим зарубіжним практикам, потребує створення методів та засобів обробки і аналізу відповідної інформації на семантичному рівні. Аналіз публікацій вказує на велику кількість національних стандартів, безпосередньо пов'язаних з інформаційною безпекою, які вже розроблені або знаходяться на стадії узгодження. Між цими стандартами та їх елементами існує складна система ієрархічних відношень, взаємозв'язків, посилань та відповідностей. Через недостатньо глибоко стандартизовану та усталену україномовну термінологію виникають різні варіанти перекладу основних понять та назв. Тому виникає потреба в узгодженні термінологічної бази стандартів на семантичному рівні на основі сучасних засобів подання та обробки знань, які уможливлюють автоматизоване знаходження протиріч та розбіжностей. В роботі проаналізовано вимоги, що застосовуються до терміносистем та визначень термінів, що використовуються в галузевих терміносистемах, та пропонуються шляхи для задоволення цих вимог.

Для формалізації терміносистем стандартів пропонується використовувати онтологічний аналіз, який дозволить інтегрувати наявні знання із сфери інформаційної безпеки у відкритих ресурсах Web з досвідом експертів із стандартизації. Наявність онтологічних метаописів стандартів має забезпечити швидкий та ефективний доступ до релевантних відомостей та коректну однозначну інтерпретацію контенту стандартів. Розроблено базові принципи побудови онтологічного опису стандарту.

Запропонований підхід детально розглянуто на прикладі стандарту "Інформаційні технології. Методи захисту. Оцінювання безпеки операційних систем", побудовано онтологію термінів цього стандарту, визначено їх властивості та відношення. Розглянуто перспективи та доцільність створення глобальної семантичної мережі стандартів, яка пов'язує окремі національні та міжнародні стандарти, сферу її застосування для семантичної обробки інформації. Така мережа має стати основою для еталонної семантичної розмітки різноманітних інформаційних ресурсів (як природномовних, так і мультимедійних), дозволить вдосконалювати онтології предметних областей та зробити більш ефективним доступ до інформації.

1 Вступ

Сьогодні в Україні велике значення надається розробці нормативно-правової бази для підтримки інформаційної безпеки. Значна увага приділяється гармонізації нормативно-правового забезпечення України щодо оцінки відповідності систем управління інформаційною безпекою правилам та процедурам, які відповідають міжнародним стандартам та кращим міжнародним практикам. Це створює передумови для усунення технічних бар'єрів між країнами в сфері технічного регулювання, в тому числі з питань безпеки.

Практично усі сфери діяльності людини важко уявити без використання стандартів, які акумулюють передовий науково-технічний досвід багатьох країн, забезпечуючи єдність вимог до продукції, яка є предметом міжнародного товарообміну (взаємозамінність комплектуючих виробів, єдині методи випробувань і оцінювання якості виробів). Якість стандартів, що розробляються, залежить від багатьох чинників, включаючи компетентність розробників та узгодженість термінологічної бази, що безпосередньо впливає на ефективність їх використання.

Міжнародні організації доклали великих зусиль для забезпечення уніфікації засобів та систем інформаційної безпеки. Це відображено у великій кількості міжнародних стандартів ISO, зі значною частиноюяких вже гармонізовано. національні стандарти України – ДСТУ. В Україні діяльність зі стандартизації ґрунтується на

правових нормах Закону України «Про стандартизацію» [1], Декрету КМУ «Про стандартизацію та сертифікацію», інших нормативних актах у цій сфері, з урахуванням принципів і положень міжнародних організацій зі стандартизації [2,3]. Стандартизація – це складна, міжгалузева, комплексна й багатоаспектна задача, рішення якої пов'язане із розробкою сучасних нових методів та технологій. Приміром, в [4] проаналізовано ієрархічну структуру більш ніж 100 стандартів, пов'язаних з методами і засобами забезпечення безпеки інформаційних технологій.

2 Постановка задачі

У зв'язку з важливістю розробки національного нормативно-правового забезпечення інформаційної безпеки, великим обсягом міжнародних стандартів в цій сфері та термінологічними проблемами гармонізації національних стандартів України виникає потреба у розробці методів та засобів узгодження термінологічної бази на семантичному рівні, з використанням сучасних засобів подання та обробки знань. Пропонується використовувати для цього онтологічний аналіз, щоб інтегрувати наявні знання в цій сфері, які містяться у відкритих ресурсах Web, із досвідом експертів зі стандартизації. Онтологічні метаописи стандартів, що характеризують їх семантику, забезпечать коректну однозначну інтерпретацію вмісту стандартів та їх автоматизовану обробку.

3 Вимоги до термінології, що застосовується в національних стандартах України

Термін – це слово або словосполучення, яке зіставляється з чітко окресленим поняттям предметної області (ПрО) і вступає в системні відношення з іншими одиницями мови, утворюючи разом з ними особливу систему – *термінологію*. Виділяють такі ознаки терміну: 1) чітку визначенність, зафіксовану в словнику; 2) однозначність в межах певної термінологічної системи; 3) точність, яка не залежить від контексту; 4) стилістичну нейтральність; 5) відсутність синонімів в межах обраної терміносистеми; 6) системність; 7) стисліcть. Принциповим у відборі термінів є цілісність системи понять та термінів, які змістовно підпорядковуються певній теорії або концепції.

Галузеві термінології (тобто сукупності термінів конкретних галузей) називають *терміносистемами*, або термінологічними системами. Характеризуючи сучасну україномовну термінологію в ІТ-сфері в цілому та окремо – пов'язану з інформаційною безпекою, необхідно відмітити як динаміку її розвитку та інтенсивність збагачення новими лексичними одиницями, так і неоднозначні визначення багатьох ключових понять.

Для формалізації терміносистем певної ПрО широко використовують моделі знань щодо ПрО: тезауруси, таксономії, онтології. Визначення термінів створюються вручну експертом ПрО, будуються автоматично на основі обробки інформаційних джерел або здобуватися з інших баз знань (тезаурусів, онтологій тощо). В усіх випадках доцільно дотримуватися певних правил та удосконалювати отримані визначення відповідно до наведених нижче принципів [5].

Потрібно, щоб кожне визначення терміну: - викладалося в однині (виключення складають поняття, які самі є множинними); - визначало, чим саме є наведене поняття, а не тільки чим воно не є; - мало вигляд описової фрази або речення; - містило лише поширені скорочення; - викладалося без використання визначень інших даних або базових понять; - відображало суттєвий зміст поняття; - було точним та однозначним; було стислим; - припускало окреме використання; - подавалося без пояснювальної інформації, функціонального використання або процедурної інформації; - не містило циклічних посилань; - використовувало однакову термінологію та логічну структуру для пов'язаних визначень. Для близьких або пов'язаних визначень повинні використовуватись одна й таж сама термінологія та синтаксис.

4 Терміносистема стандарту з оцінювання безпеки операційних систем

Розглянемо створення терміносистеми в ПрО інформаційної безпеки на прикладі стандарту "Інформаційні технології. Методи захисту. Оцінювання безпеки операційних систем" (ISO/IEC TR 19791:2010 (E), IDT), що бузується на міжнародному стандарті "Information technology – Security techniques – Security assessment of operational systems" [6]. Цей стандарт надає настанови і розширені критерії оцінювання *операційних систем* – поєднання персоналу, процедур і процесів, інтегрованих за допомогою функцій і механізмів на основі технічних засобів, які використовуються для обгрунтування застосовного рівня залишкового ризику у певній операційній системі. Для багатьох організацій інформація є основним ресурсом і вимагає захисту від загроз несанкціонованого розголошення, зміни або знищення.

Ці ресурси захищаються за допомогою поєднання технічних засобів керування та підтримки інфраструктур операційного контролю персоналу, політики, процедур і заходів фізичного захисту. При оцінюванні продукту послуги, пов'язані з безпекою, – це такі ІТ-функції, які впроваджені для досягнення цілей інформаційної безпеки технології. У контексті ОС можуть бути оцінені також процедурні та фізичні вклади у безпеку. Вони ідентичні

функціям ІТ, оскільки вони являють собою такі засоби безпеки ОС, які разом сприяють досягненню цілей безпеки. Однак вони, як правило, не залежать від технології і більш пристосовані до оцінювання на стадії контролю життєвого циклу операційної системи і таким чином розглядаються окремо від функціональних вимог. Стандарт орієнтований на тих, хто бере участь в розробці, інтеграції, впровадженні і керуванні безпекою операційних систем, а також експертів, які бажають застосувати ISO/IEC 15408 в операційних системах.

В оцінюванні безпеки ОС можна виокремити наступні етапи:

- Проблема безпеки формулюється як множина ризиків, які слід усунути або пом'якшити, і група політик безпеки, які слід застосувати. Для цього слід провести попередній аналіз і визначити завдання ОС і провести оцінку ризиків для визначення таких ризиків, яким слід протидіяти за допомогою технічних та операційних засобів керування. Результати аналізу записуються в системний об'єкт безпеки
- Проблема безпеки ділиться на рішення по забезпеченню безпеки високого рівня і групу організаційних політик захисту, які слід застосувати. Ці цілі записуються в системний об'єкт безпеки.
- Цілі безпеки в подальшому уточнюються у вимогах щодо безпеки, які можуть оцінюватися незалежним експертом. Деякі цілі безпеки будуть віднесені до технічних, інші до операційних засобів керування. Деякі можуть вимагати як технічних, так і операційних засобів керування. Наприклад, контроль несанкціонованого доступу до інформаційних ресурсів часто доповнюється як через забезпечення фізичної безпеки об'єкта, в якому містяться ресурси (наприклад, замки, захисні пристрої), так і за допомогою функцій ІТ. Вимоги до безпеки записуються в системний об'єкт безпеки.
- Сукупність дій експерта, яких слід додержуватись при оцінюванні, визначається на підставі загальних цілей і загального забезпечення гарантії захисних заходів. Ці вимоги забезпечення гарантії записуються в системний об'єкт безпеки.
- Незалежний експерт визначає факт того, що ОС відповідає вимогам безпеки, на основі вимог, зазначених у системному об'єкті безпеки.
- Продовження оцінювання також є можливим з метою отримання гарантії того, що ОС відповідає власним вимогам при експлуатації. Вони фокусуються на операційних засобах керування ОС, оскільки вони залежать від поводжень людини, що менш керовані, ніж поведінка ІТ.
- Періодична повторне оцінювання ОС може визначити, що ОС продовжує відповідати своїм вимогам, незважаючи на зміни в ОС або її середовищі. Це визначається тим, які зміни мали місце, шляхом оцінювання впливу цих змін, оновлення системного об'єкту безпеки, і визначення того, що безпека все ще зберігається.

Першочерговою метою оцінювання ОС є гарантування того, що цілі безпеки ОС впроваджені правильно та ефективно. Однак, оцінювання як операційних, так і технічних засобів керування безпекою, не може абсолютно гарантувати, що ці засоби керування завжди будуть функціонувати належним чином. Процедура оцінювання виносить недиференційований висновок. Навіть коли оцінка не виявляє неприйнятних вразливостей, завжди залишається залишковий ризик неналежного функціонування засобів керування. Цей ризик можна зменшити за допомогою додаткових засобів керування, або використовуючи інші заходи забезпечення гарантії, які дають більшу впевненість. Залишковий ризик невірної або неефективної роботи можна визначити тільки шляхом безперервного моніторингу і оцінювання.

Концепція ISO/IEC 15408 з безпеки приділяє особливу увагу підтвердженню наявності існування функцій захисту і їх правильної і ефективної роботи. Високі рівні гарантії висувають більш докладні вимоги до змісту і стилю подання таких підтверджень. Крім того, більш високий ступінь забезпечення гарантії іноді вимагає більш строгого аналізу підтверджень як з боку розробника, так і експерта з оцінювання.

Оцінювання продукту ISO/IEC 15408 проводиться у порядку, що передбачає типове операційне середовище, в якому цей продукт може застосовуватись. При оцінюванні продукту головна увага зосереджується на контрольній перевірці таких функцій захищеності, які цей продукт забезпечує незалежно від конкретних умов експлуатації. При оцінюванні продукту застосовуються різноманітні технічні характеристики, проектна документація та документація з тестування для обґрунтування висновку про коректність. При цьому вимоги щодо забезпечення гарантії, як правило, не випливають з проблеми безпеки. Натомість, вони вибираються аксіоматично або стратегічним рішенням. Основною метою оцінювання продукту є отримання гарантії того, що функції безпеки реалізовані правильно.

Базисна інформація для визначення коректності визначається вимогами безпеки, які містяться в цілях безпеки продукту, що включає в себе простежуваність проблеми безпеки. Проблема, зазначена в ST, ґрунтується на оцінці загрози для всіх видів оточення. Область застосування оцінювання продукту обмежується вимогами безпеки ІТ.

Термінологічна база цього стандарту включає терміни з ISO/IEC 15408-1, ISO/IEC 18045, а також наступні терміни з відповідними визначеннями:

- *Адміністративний контроль* (management controls): Контроль безпеки (тобто засоби захисту і заходи протидії) інформаційної системи, що зосереджується на керуванні ризиком і керуванні безпекою інформаційної системи.

- *Аналіз ризику* (risk analysis): Систематичне використання інформації для визначення джерела й оцінювання ризику.
- *Залишковий ризик* (residual risk): Ризик, що залишається після обробки ризику.
- *Захищена зона* (security domain): Частина операційної системи яка виконує функції політики забезпечення захисту.
- *Зовнішня операційна система* (external operational system): Окрема операційна система, яка взаємодіє з оцінюваною операційною системою.
- *Керування ризиком* (risk management): Скоординовані дії з керування й контролю структурою стосовно ризику.
- *Компонент* (component): Розпізнавана та окрема частина операційної системи, яка виконує частину функцій системи.
- *Контроль безпеки* (security controls): Керування, операційний і технічний контроль (тобто засоби захисту і заходи протидії), заздалегідь описані для інформаційної системи з метою захисту конфіденційності, цілісності й доступності системи та її інформації.
- *Контрольна перевірка* (verification): Процедура оцінювання, яка використовується для підтвердження того, що контроль безпеки операційної системи запроваджений і виконаний правильно і є ефективним при застосуванні.
- *Мета оцінювання системи* (system target of evaluation): Операційна система, якою керують у відповідності з її експлуатаційною настановою, включаючи як технічні, так і операційні засоби керування.
- *Обробка ризику* (risk treatment): Процедура вибору й застосування варіантів коригування ризику.
- *Операційна система* (operational system): Інформаційна система, яка виступає як інтерфейс між пристроями обчислювальної системи і прикладними програмами.
- *Операційний контроль* (operational controls): Контроль безпеки (тобто засоби захисту і заходи протидії, які переважно запроваджуються і виконуються людьми (на відміну від систем).
- *Оцінка ризику* (risk assessment): Уся процедура аналізу й оцінювання ризику.
- *Підсистема* (subsystem): Один чи більше ніж один компонент ОС, що можуть діяти окремо від решти системи.
- *Ризик* (risk): Поєднання ймовірності виникнення певної комбінації обставин та її наслідків.
- *Технічні засоби керування* (technical controls): Керування безпекою (тобто засоби захисту і заходи протидії), які переважно запроваджуються і виконуються інформаційною системою за допомогою механізмів, що містяться в апаратних, програмних або мікропрограмних компонентах забезпечення системи.

Однак ці конфігурації не приймають до уваги будь-які специфічні оточення. По завершенні оцінювання продукту все ще залишається необхідність інтегрувати оцінений продукт з іншими продуктами для створення ST, і в кінцевому рахунку, для звірки того, що ОС надає параметри безпечності та поведінки у своєму середовищі і операційних конфігурацій. При оцінюванні продукту, як правило, застосовуються ті ж самі заходи забезпечення гарантії по всіх визначених функціях безпеки. Хоча технічно можливо отримати різні домени безпеки в продуктах, але зазвичай такий метод для оцінювання типового продукту не застосовується.

Свідоцтво і звіти оцінювання можуть використовуватися для підтримки інтеграції ОС і контрольної верифікації. Хоча різниця між властивостями продукту ІТ і ОС для цілей оцінювання безпеки невелика, але оцінювання ОС ускладнюють наступні причини:

- ОС може включати в себе багато комплектуючих та розроблених на замовлення ІТ-компонент, згрупованих в захищених доменах. Склад кожної системи захищеного домену може базуватися на декількох факторах, таких як технологія, функціональність і критичність захищених ресурсів;
- ОС може містити кілька конкретних зразків однакового продукту (приміром, кілька копій ОС від одного і того ж постачальника) або кілька різних зразків продуктів одного виду (приміром, кілька систем мережного захисту від різних постачальників);
- ОС може мати політики безпеки, які застосовуються лише на деяких захищених доменах, а на інших можуть не застосовуватися;
- Залишкові ризики можуть бути прийнятними в межах різних доменів ОС, тоді як сам продукт протидіє конкретним загрозам для конкретних типів активів без врахування ризику.

Всі ці фактори впливають на вимоги до безпеки ОС. Зокрема потрібні різні форми гарантії в різних зонах, залежно від інформації, або від видів обраних функціональних засобів керування. Це означає, що цілі забезпечення визначаються і пояснюються як частина вирішення проблеми.

Більш того, оцінювання ОС повинне включати усі засоби керування, які розглядаються як припущення при оцінюванні продуктів. Загалом види вимог до безпеки технічних засобів керування в ISO/IEC 15408-3 можуть бути розширені і на операційні засоби керування. Наприклад, концепція оцінювання проектної документації для технічних засобів керування перетворюється на оцінювання опису операційних засобів керування. Дії людей, які

впроваджують операційні засоби керування, можна випробувати тим же шляхом, що і дії програми тестування технічних засобів керування.

Деякі вимоги ISO/IEC 15408-3, що стосуються розробки системи, можуть не застосовуватися в ОС, або їх оцінювання повинне відстрочуватися до настання фази інсталяції системи. Аналогічно, забезпечення безпеки в операційних засобах керування можна досягти у фактичному операційному середовищі, тоді як технічні засоби керування аналізуються і випробовуються у своєму середовищі розробки.

Для оцінювання засобів керування в ОС необхідно узагальнити і змінити класи безпеки для технічної функціональності в ISO/IEC 15408-3. Області, в яких потрібні додаткові компоненти безпеки для роботи з ОС: - Вся архітектура безпеки та її компоненти; - Конфігурація складових компонентів ОС; - Політики керування, правила і процедури ОС; - Вимоги та правила для взаємодії з іншими довіреними і ненадійними ОС; - Моніторинг нетехнічних засобів керування на фазі експлуатації.

Існує п'ять основних способів досягнення гарантії в ОС: - Аналіз проекту ОС; - Тестування ОС; - Перевірка того, що ОС була встановлена і налаштована правильно; - Перевірка того, що ОС працює надійно; - Повторне використання результатів оцінювання .

Цей стандарт базується на триступеневому підході до встановлення необхідного рівня безпеки для операційної системи:

1. Оцінювання ризику, для визначення ризиків безпеки системи;
2. Зниження ризику, для вжиття заходів протидії або усунення ризиків безпеки шляхом вибору, застосування і оцінювання заходів безпеки;
3. Сертифікація, для підтвердження того, що залишкові ризики, які залишаються у рамках системи, після застосовування засобів керування, підходять для системи, яка буде використовуватися в живій роботі.

Модель оцінювання безпеки ISO/IEC 15408 виключає аналіз операційного середовища, яке оточує ІТ частину інформаційної системи. Як правило, безпека операційних систем залежить також від заходів безпеки ІТ, адміністративного або фізичного характеру. Тому потрібно визначити способи представлення та оцінювання таких вимог та засобів керування.

5 Використання онтологічного аналізу в стандартизації

Онтології ПрО, що характеризують певні стандарти, є потужним інструментом для обробки, аналізу та застосування знань, що містяться в цих стандартах, забезпечують їх автоматизовану обробку та інтеграцію [7].

Важливим питанням, пов’язаним з розробкою стандартів, є їх інтероперабельність та забезпечення їх автоматизованого пошуку та порівняння. Тому в процесі розробки стандартів виникає необхідність в побудові їх семантичних метаописів. Такими метаописами можуть стати онтології ПрО стандарту, в яких формалізуються основні поняття ПрО, що відображаються в стандарті, та зв’язки між ними. Онтологічний підхід полегшує коректний переклад стандартів та дозволяє визначити, які саме близькі за значенням терміни потрібно використовувати у кожному окремому випадку [8].

Щоб виявити семантичну близькість між стандартами, потрібно співставити їх онтології, знайти близькі за значенням поняття та на основі цього обчислити семантичну відстань між стандартами [9].

Саме онтології ПрО можуть стати джерелом знань для пошуку компетентних фахівців для розробки національних стандартів: за існуючим стандартом треба побудувати онтологію та порівняти її з онтологіями фахівців, які можна отримати з аналізу результатів їх науково-технічної та навчально-методичної діяльності, що відображається в їх публікаціях. Крім того, наявність онтології стандарту дозволяє надалі знаходити потрібні стандарти, здобувати з них необхідні користувачам знання та аналізувати їх вміст на семантичному рівні.

Ще одна сфера застосування онтологій стандартів – автоматизована побудова сфер компетенцій підкомітетів зі стандартизації, формалізованих через поєднання онтологій вже розроблених стандартів та наявність об’єктивних автоматизованих методів для класифікації нових стандартів до найбільш релевантного підкомітету. Аналіз відношень між онтологіям стандартів дозволить також визначити порядок розробки стандартів та визначення не тільки формальних, але й семантичних зв’язків між ними: приміром, стандарт, в якому визначаються певні терміни, потрібно розробляти раніше, ніж той, в якому ці терміни вже використовуються.

6 Розробка онтології стандарту

Розглянемо це на прикладі побудови онтології для стандарту “Інформаційні технології. Методи захисту. Оцінювання безпеки операційних систем”. Усім визначеним у стандарті термінам мають відповідати класи онтології відповідної ПрО, яка описує цей стандарт та є підкласами класу “Термін стандарту”. Спочатку в онтології створюється клас “Стандарт”, який описує основні характеристики стандарту, такі як назва, код, тематика, рік прийняття, розробники, обсяг тощо.

Для відображення окремих термінів стандарту доцільно використовувати саме екземпляри онтології класу “термін стандарту”, до яких можна застосовувати такі відношення, які реалізуються для екземплярів класів онтології (рис.1). Для інтероперабельного використання знань, які відображаються у стандартах, доцільно додати до опису класу “Стандарт” зв’язки даного стандарту з іншими. Крім того, можна вказати, які саме терміни відносяться до цього стандарту за допомогою властивості об’єктів “Стандарт використовує термін”. Якщо онтологія створюється не для окремого стандарту, а для групи стандартів, то можна вказувати, що стандарт використовує термін, визначений в іншому стандарті, що описано даною онтологією. Це забезпечує однаковість термінів, що застосовуються, та спрощує розуміння вмісту стандартів. Щоб автоматизувати цей процес, доцільно використовувати спеціалізовані програмні засоби, орієнтовані на це [10].

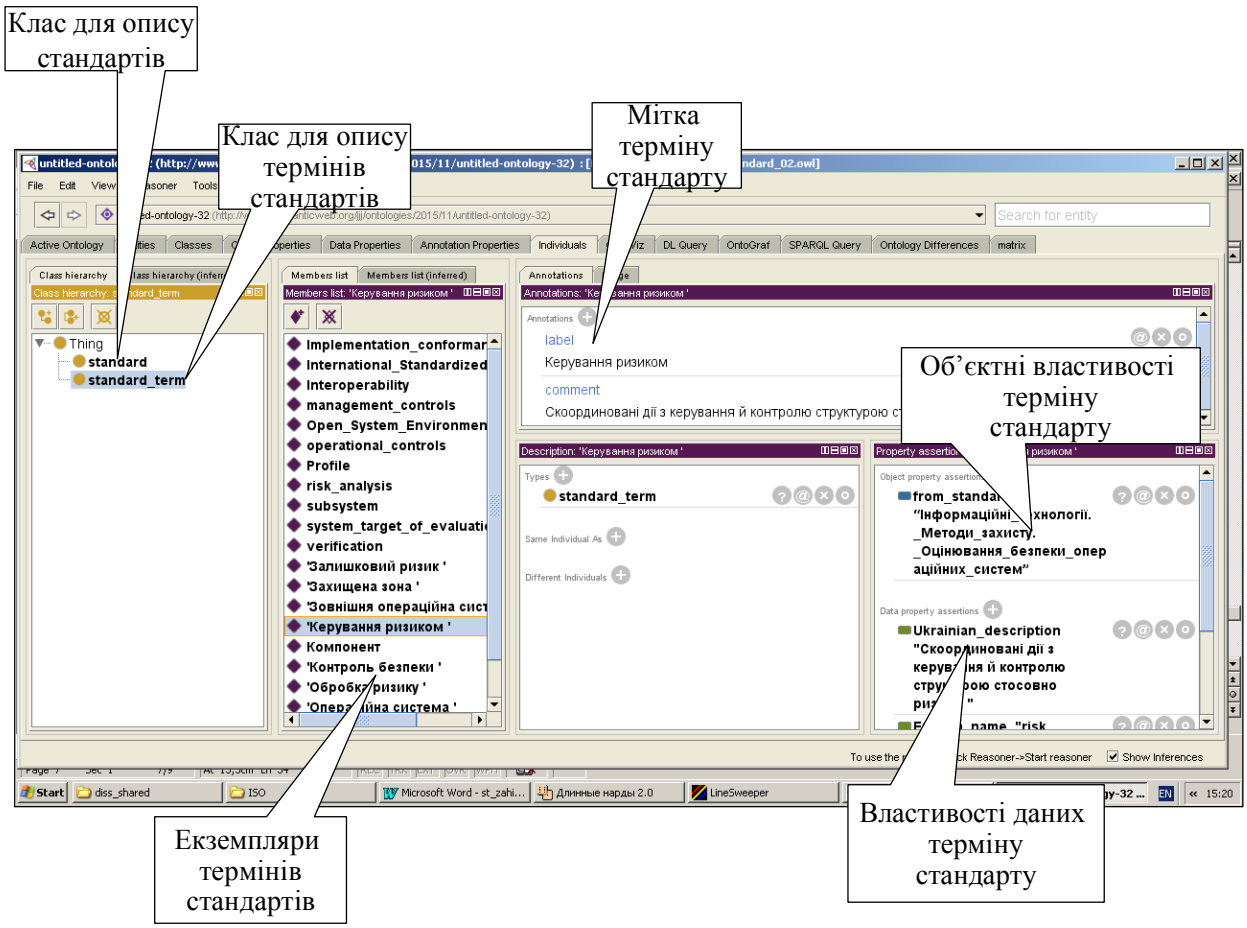

Рис. 1. Онтологія опису стандарту

Клас “Термін стандарту” має властивості даних (Data Properties) “Назва стандарту”, “Назва терміну українською”, “Назва терміну англійською”, “Опис терміну українською”, “Опис терміну англійською” та “Примітка” типу “рядок символів” та властивості об’єктів (Object Properties) “Є підкласом” та “Є синонімом”, які дозволяють встановлювати семантичні зв’язки між елементами термінами стандарту. Крім того, в таку онтологію можна додати семантичні зв’язки між термінами ПрО: приміром, якщо один термін є підкласом іншого або між ними існують специфічні для ПрО взаємини (бути компонентом, бути умовою тощо), які можна відобразити через об’єктні властивості відповідних класів та їх елементів. Щоб встановити однозначний зв’язок терміну з оригінальним англомовним терміном, доцільно використовувати англомовну назву в якості його імені, а для того, щоб забезпечити коректне розуміння україномовного контенту, рекомендується використовувати переклад терміну українською в якості його мітки. Це дозволить запобігти синонімічного дублювання термінів різними варіантами перекладу (в онтології неможливо створити два класи з одним ім’ям), але надати можливість використовувати кілька варіантів перекладу (в процесі вибору найбільш вдалого).

На рис.2 представлена онтологія ПрО, до якої відноситься терміносистема стандарту “Інформаційні технології. Методи захисту. Оцінювання безпеки операційних систем”. Зв’язки між класами, екземплярами класів та їх властивостями в онтології стандарту відображаються візуально наступним чином.

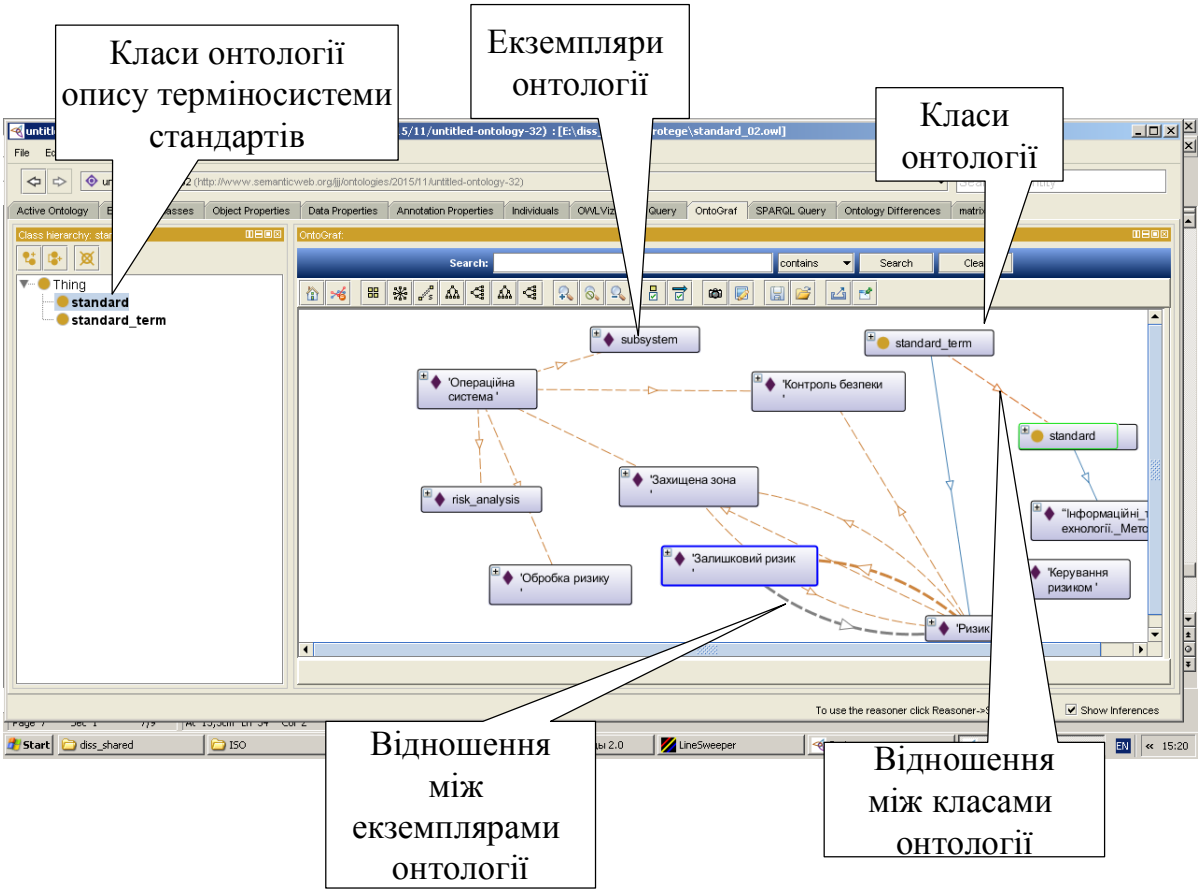

Рис. 2. Візуалізація зв’язків між класами, екземплярами класів та їх властивостями в онтології стандарту

7 Висновки та перспективи досліджень

В майбутньому результатом цієї роботи має стати створення *глобальної семантичної мережі стандартів*, яка пов’яже окремі національні та міжнародні стандарти; об’єкти, що використовують ці стандарти та посилаються на них (як матеріальні, так і інформаційні об’єкти); фахівців, що є експертами в сфері розробки стандартів, та організації різного рівня, що підтримують різні види діяльності, пов’язаної із розробкою та використанням стандартів. Інтероперабельне представлення знань та застосування відповідних технологій та форматів дозволить інтегрувати цю мережу знань із знаннями, представленими в Semantic Web.

На основі такої онтології можна виконувати семантичну розмітку природномовних текстів – як контенту окремих стандартів, пов’язаних з інформаційною безпекою, так і інших документів – приміром, описів конкретних систем, в яких реалізовані ці стандарти. Це має значно спростити пошук та аналіз таких документів та забезпечити можливість їх автоматичної обробки. Прикладом такої обробки може бути пошук операційних систем, що задовольнять певним критеріям інформаційної безпеки відповідно до вказаного стандарту. При цьому користувачеві не потрібно буде самостійно відслідковувати зміни в останній редакції обраного стандарту або передивлятися опис кожної потенційно придатної системи – співставлення має виконуватися автоматизовано. Технологічною основою для такої семантичної розмітки та пошуку може стати середовище Wiki із семантичним розширенням [11].

Крім того, встановлення семантичної близькості між стандартами, що використовуються для розмітки, на основі онтологій дозволить визначити пріоритетні напрямки їх розвитку та забезпечити інформацію для подальшого їх вдосконалення.

Література

1. Закон України «Про стандартизацію». Верховна Рада України, Закон від 05.06.2014, № 13-15 –VII.
2. Державна система стандартизації. — К.: Держстандарт України, 1994.
3. ДСТУ 1.5:2003. Національна стандартизація правила побудови, викладання, оформлення та вимоги до змісту нормативних документів.
4. Цвілій О.О. Безпека інформаційних технологій: сучасний стан стандартів iso27k системи управління інформаційною безпекою // Телекомунікаційні та інформаційні технології. – No2, 2014. – С.73-79.
5. Грицик Н. Комп'ютерна термінологія та основні способи її перекладу/ Грицик Н. // XVIII-та Міжнародна науково-практична Інтернет-конференція «Проблеми та перспективи розвитку науки на початку третього тисячоліття», Переяслав-Хмельницький, 2013. – С.45-52.
6. ISO/IEC TR 19791:2010(en). – https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:19791:ed-2:v1:en
7. Gruber T., What is an Ontology? – http://www-ksl.stanford.edu/kst/what-is-an-ontology.html.
8. Гладун А.Я. Семантичні технології: принципи та практики (монографія)/ А.Я. Гладун, Ю.В. Рогушина.– К: Універсаріум, 2016. – 314с.
9. Гладун А.Я., Рогушина Ю.В. Онтологічний підхід до проблем підвищення якості розроблення національних стандартів України // Стандартизація, сертифікація, якість, №2 (99), 2016. – С.19-28.
10. Лесько О.В. Рогушина Ю.В. Анализ семантики естественно-языковых законодательных документов с использованием онтологии предметной области // Проблеми програмування, № 4, 2015. – С.58-71.
11. Rogushina J. Semantic Wiki resources and their use for the construction of personalized ontologies // CEUR Workshop Proceedings 1631, 2016. – P.188-195.

Ontological Approach to the Development of National Standards of Ukraine for Evaluation of Information Technology Security

© Julia V. Rogushina
Institute of Software Systems of National Academy of Sciences of Ukraine, Kyiv, Ukraine
ladamandraka2010@gmail.com
© Anatoly Y. Gladun
International Research and Training Center for Information Technologies and Systems NASU and MESU, Kyiv, Ukraine
glanat@yahoo.com
© Georgii V. Snigyr
Ukraine International Airlines, AVSEC department, Kyiv, Ukraine
mandraka1966@gmail.com

Abstract

The development of the normative legal framework of Ukraine oriented on support of the information security that has to comply with international standards and best international practices requires the creation of methods and means that provide processing and analyzing of the relevant informational resources on the semantic level. The solving of this complex task requires to harmonize the semantics of the terminology basis of standards by modern means of representation and processing of knowledge. Analysis of publications indicates a large number of national standards directly related to information security that were developed or are processed now.

There is a complex system of hierarchical relations, correlations, links and correspondences of these standards and their elements. Deep enough standardized and consolidated Ukrainian-language terminology causes different versions of the translation of the basic concepts and names deal with information security. Therefore we need to harmonize terminology base of standards on the semantic level by use of modern means of knowledge representation and processing that makes possible automated acquisition of contradictions and differences of different standards. The paper analyzes the requirements that apply to terminology and definitions of terms used in the industry terminological systems and suggests ways to meet these requirements.

We propose to use the ontological analysis for formalization of the terminological system of standards deal with information security because ontologies allow interoperable and explicit integration of existing knowledge from this subject domain (from the Web open resources) with the experience of experts from standardization sphere. The availability of ontological descriptions of the standards provides quick and efficient access to relevant information and correct

unambiguous interpretation of the standards` content. For this purpose the basic principles of the ontological description of standards are developed.

An approach proposed in this paper is described in details on example of the standard «Information technology - Security techniques - Security assessment of operational systems», an ontology that defines the terms of this standard, their properties and relations is built. We consider the prospects and feasibility of establishing a global semantic web of standards which connects the individual national and international standards and their scope for knowledge-based information processing. Such network can become the basis for the reference semantic markup of various heterogeneous information resources (as natural language and multimedia), allows improving and integrating the ontologies of subject domains and provides more efficient access to information.