УДК 004.056
DOI: 10.15587/2312-8372.2016.66462

Жора В. В.

ДОСЛІДЖЕННЯ ЗАСТОСОВНОСТІ ОНТОЛОГІЧНОГО ПІДХОДУ ДО ПОБУДОВИ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Визначено основні етапи побудови комплексних систем захисту інформації, здійснений їх аналіз на предмет застосовності методів формального моделювання. Запропоновано використовувати онтологічні моделі на окремих етапах побудови комплексних систем захисту інформації. Наведено приклад таксономії та онтологічної моделі порушника.

Ключові слова: *захист інформації, інформаційно-телекомунікаційна система, онтологія, порушник.*

1. Вступ

Суспільний розвиток у XXI столітті супроводжується проникненням інформаційних технологій в усі сфери людського життя. Окрім набуття нових можливостей з передачі і обробки даних, використання інформаційних технологій може містити потенційні загрози цим даним, а відтак — інтересам, в тому числі життєво важливим, людини та навіть держави.

Актуальність задач захисту інформації підвищується з кожним роком, незважаючи на постійний розвиток і вдосконалення технологій забезпечення безпеки інформації. Кібернетичний простір, утворений за допомогою пов'язаних у локальному масштабі інформаційних систем, перетворюється на сферу ведення бойових дій та джерелом збагачення високотехнологічної злочинності.

Окрім винайдення якісно нових методів і засобів захисту інформації, суспільство потребує узагальнення та систематизації знань в сфері інформаційної безпеки, а також нових ідеологічних, архітектурних та методологічних принципів забезпечення безпеки інформації.

2. Аналіз літературних даних та постановка проблеми

Одним із загальновизнаних підходів до захисту інформаційно-телекомунікаційних систем (далі — ІТС) є побудова систем управління інформаційною безпекою, що поєднують в собі процеси з розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки [1]. Відповідно до нормативно-правової бази України, сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС визначається як комплексна система захисту інформації (далі — КСЗІ) [2], порядок побудови якої наведено в [3].

Однією з ключових в сфері захисту інформації є проблема побудови повної несуперечливої моделі захищеної ІТС та узагальнення підходів до моделювання подібних систем [4]. Загалом, задача побудови КСЗІ є слабо формалізованою, а питання повноти і несуперечливості виникають на різних етапах її створення, зокрема в частині моделювання загроз інформації, порушника, розробки політики безпеки інформації тощо.

Через низький рівень формалізації сфері захисту інформації бракує стійкого теоретичного підґрунтя та структурованої бази знань, що обмежує можливість застосування в ній ефективних математичних методів, зокрема аналітичного та імітаційного моделювання. Одним з можливих підходів до вирішення цієї проблеми є використання онтології, що передбачає концептуалізацію предметної галузі та визначає поняття, їх атрибути та відношення між ними [5].

Онтологічний підхід базується на формальному описі термінів і концепцій, фактично визначаючи загальний словник (таксономію, тезаурус і т. ін.) предметної галузі, що має використовуватися не тільки для уніфікації понять з точки зору людського розуміння, а й для створення інтерфейсів взаємодії й обміну даними в рамках цієї області знань, насамперед автоматизованих.

В світовій та вітчизняній науці онтології вже знаходять застосування у вирішенні задач моделювання систем захисту інформації. В якості прикладів базових онтологій високого рівня можна навести чинні в Україні стандарти ДСТУ 3396.2-97, НД ТЗІ 1.1-003-99, СОУ Н НБУ 65.1 СУІБ 1.0:2010, чимало міжнародних стандартів. Проте, аналіз багатьох з них свідчить про їхню неузгодженість, часткову застарілість. Отже, розробка високорівневої онтології в галузі інформаційної безпеки, а також низькорівневих предметно-орієнтованих онтологій, що можуть бути застосовані для окремих задач захисту інформації, є актуальною проблемою. Прикладами таких рішень можуть бути праці [6–8].

3. Об'єкт, мета та задачі дослідження

Об'єктом дослідження в цій роботі є комплексна система захисту інформації, яка створюється в інформаційно-телекомунікаційній системі з метою забезпечення безпеки інформації, необхідність захисту якої визначено законодавством.

Метою роботи є дослідження застосовності онтологій до вирішення задач захисту інформації, зокрема, до різноманітних етапів створення КСЗІ.

Для досягнення поставленої мети були сформульовані такі завдання:

— проаналізувати можливість використання предметно-орієнтованих онтологій для опису окремих етапів побудови КСЗІ, визначених в [3];

— розробити приклад низькорівневої онтології для окремого етапу побудови КСЗІ.

4. Онтологічні моделі окремих етапів побудови КСЗІ

Практична діяльність із створення КСЗІ як основного механізму забезпечення безпеки інформації, вимога щодо захисту якої встановлена законом, переважним чином спирається на викладені в нормативно-правовій базі з технічного захисту інформації теоретичних положень. Останні, в свою чергу, є похідними від «Оранжевої книги» Міністерства оборони США [9] та Канадських критеріїв безпеки комп'ютерних систем [10], тобто є статичними і застарілими. Більшість розробників КСЗІ, на жаль, не використовують сучасні напрацювання в теорії захисту інформації, що суттєво звужує можливість тиражування ефективних рішень, верифікації їх сторонніми дослідниками та повторюваність результатів. Формалізація основних етапів створення КСЗІ має на меті усунення протиріч та охоплення усіх основних аспектів, що необхідно враховувати в процесі проектування систем захисту інформації.

В процесі побудови КСЗІ прийнято виділяти такі основні етапи [3]:

— формування загальних вимог до КСЗІ в ІТС;

— розробка політики безпеки інформації в ІТС;

— розробка технічного завдання на створення КСЗІ;

— розробка проекту КСЗІ;

— введення КСЗІ в дію та оцінка захищеності інформації в ІТС;

— супроводження КСЗІ.

Важливим етапом робіт з формування загальних вимог до КСЗІ в ІТС є обстеження середовищ функціонування ІТС. Остання при цьому розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки. На підставі обстеження визначається перелік об'єктів захисту, тобто, фактично формується суб'єктно-об'єктна модель ІТС, визначаються доступи і відношення між об'єктами. Окремі результати щодо формалізації цього етапу викладені у [4].

На наступному за обстеженням середовищ функціонування ІТС етапі зазвичай розробляються моделі загроз і порушника, на підставі чого згодом здійснюється оцінка ризиків і формується перелік суттєвих для конкретної ІТС загроз. Важливі результати в сфері застосування онтологій на цьому етапі отримані в роботах [11–14].

Розробці детальних вимог до КСЗІ передує етап розробки політики безпеки, тобто формування загальних вимог, правил, обмежень, рекомендацій і т. п., які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій. До цього етапу також є приклади застосування онтологій в частині визначення правил розмежування доступу [14].

Отже, на етапах розробки технічного завдання та проектування можуть бути використані результати, отримані на попередніх етапах за допомогою формалізованих методів та моделей.

Схематично застосовність онтологій на різних етапах побудови КСЗІ зображено на рис. 1.

В якості прикладу розглянемо використання онтологічного методу при побудові моделі порушника.

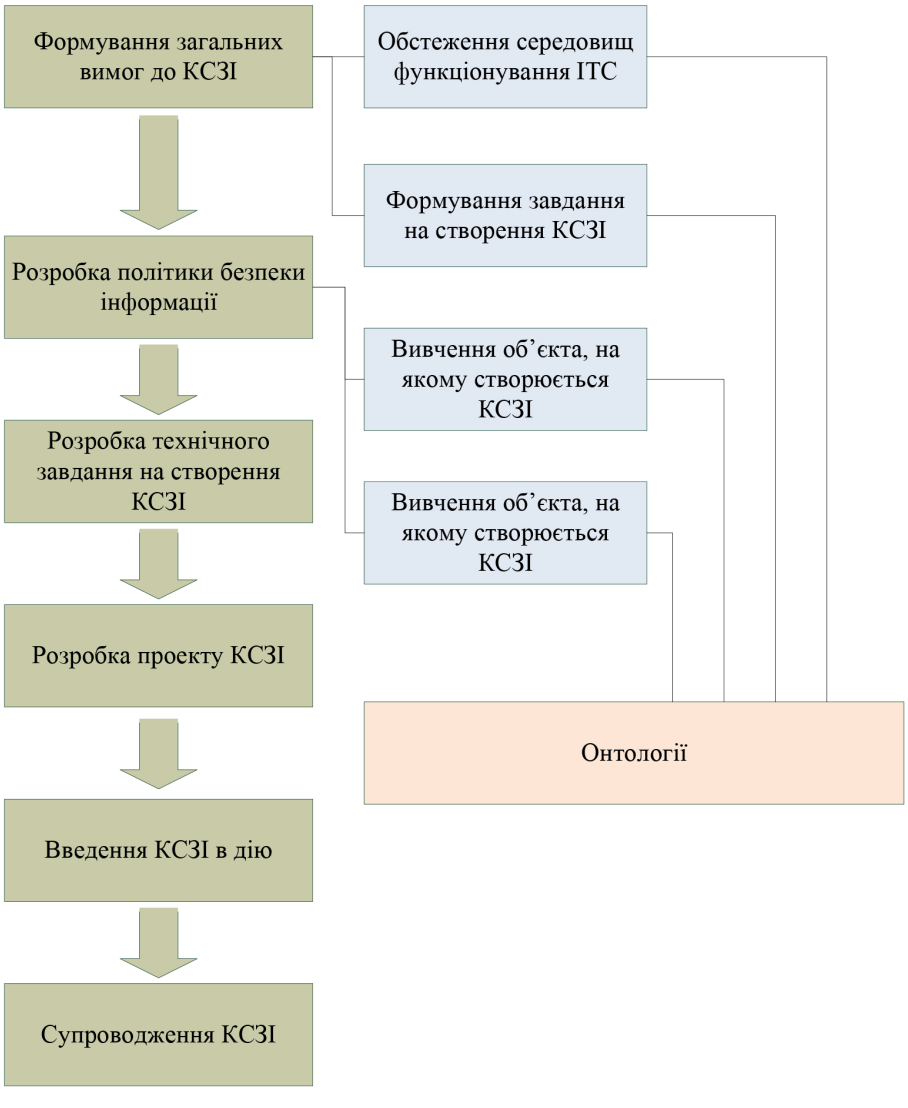

Рис. 1. Застосовність онтологічних моделей під час побудови КСЗІ

Під порушником будемо розуміти особу, яка навмисно чи помилково, використовуючи наявні можливості, методи і засоби, здійснила спробу виконати дії (операції), які призвели або можуть призвести до порушення конфіденційності, цілісності та доступності інформації.

Стосовно ІТС порушники можуть бути внутрішніми (з числа користувачів, адміністраторів чи персоналу ІТС) та зовнішніми (сторонні особи). Таксономію порушників зображено на рис. 2.

Подібні таксономії також можна визначити для інших специфікацій порушників, що класифікуються за:

— мотивами здійснення порушень;
— метою здійснення порушень;
— за рівнем кваліфікації та обізнаності щодо ІТС;
— за можливостями використання засобів і методів подолання систем захисту;
— за часом дії;
— за місцем дії.

За наведеними специфікаціями можна сформулювати загальну онтологічну модель порушника (рис. 3).

Таким чином, в онтології порушника визначені споріднені класи (поняття), такі як порушник, загроза, атака, та запроваджено відношення між ними.

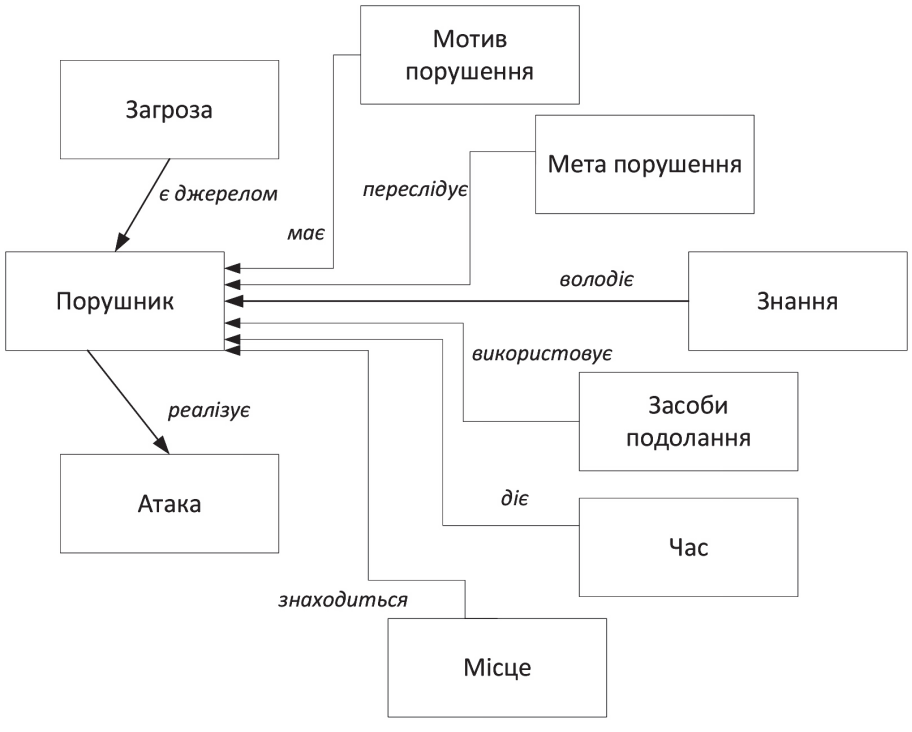

Рис. 3. Онтологічна модель порушника

Так, порушник реалізує навмисні чи ненавмисні дії (атаку), спрямовані на порушення фундаментальних властивостей захищеності інформації, виступаючи при цьому джерелом загрози інформації. Поняття місця, часу дії, засобів подолання механізмів захисту, наявні знання, мета та мотив порушення характеризують можливості порушника щодо реалізації тієї чи іншої загрози.

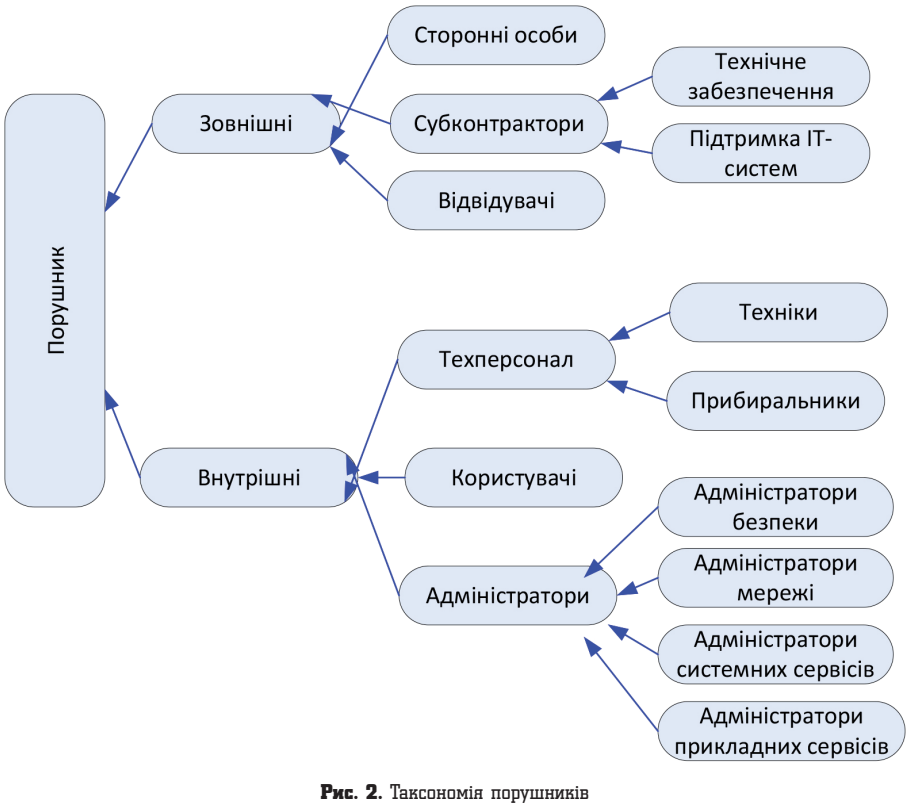

Рис. 2. Таксономія порушників

5. Обговорення результатів дослідження застосовності онтологічного підходу до побудови КСЗІ

Наведена у розділі 4 базова онтологія може бути закодована на мові OWL (Web Ontology Language) і представлена за допомогою поширених інструментальних засобів (Protégé, NeOn Toolkit тощо). Також очевидно, що ця онтологічна модель може бути в подальшому деталізована для кожного з понять. База знань, отримана в цьому випадку, може в подальшому бути використана розробниками КСЗІ для створення моделей порушника в конкретних умовах функціонування ІТС.

Аналогічні приклади можуть бути наведені для інших етапів побудови КСЗІ, визначених на рис. 1.

6. Висновки

У результаті проведених досліджень:

1. З'ясовано, що онтологічний підхід є застосовним для створення формальних моделей окремих етапів робіт з побудови КСЗІ, таких як обстеження середовищ функціонування ІТС, розробка моделей загроз і порушника, оцінка ризиків, розробка політики безпеки інформації.

2. Розроблено таксономію та онтологічну модель порушника як окремого етапу побудови КСЗІ.

У світовій базі знань є чимало прикладів сформованих онтологій, які, на жаль, використовують інші класи та поняття, які визначені в нормативно-правовій та термінологічній базі України, тож завдання створення високорівневої онтології галузі захисту інформації та низькорівневих предметно-орієнтованих онтологій, що базуються на понятійній базі як [2], так і сучасних міжнародних стандартів, є надзвичайно актуальним.

Наведений в роботі приклад онтології може бути деталізований та слугувати основою для розробки інших онтологій за етапами робіт з побудови КСЗІ.

Література

1. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements [Electronic resource]. — The British Standards Institution, 01.10.2013. — Available at: \www/URL: http://dx.doi.org/10.3403/30126472u
2. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]: Наказ ДСТСЗІ СБУ від 28 квітня 1999 року № 22. — Режим доступу: \www/URL: http://www.dut.edu.ua/uploads/l_1021_47029323.pdf. — 14.03.2016.
3. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Електронний ресурс]: Наказ ДСТСЗІ СБУ від 08 листопада 2005 року № 125. — Режим доступу: \www/URL: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=102106&cat_id=46556&ctime=1344502446343. — 14.03.2016.
4. Антонюк, А. О. Теоретичні основи моделювання та аналізу систем захисту інформації [Текст]: монографія / А. О. Антонюк, В. В. Жора. — Ірпінь: Національний університет ДПС України, 2010. — 310 с.
5. Антонюк, А. О. Онтологічний підхід до вирішення задач захисту інформації [Текст] / А. О. Антонюк, В. В. Жора // Шестнадцатая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». — Киев, 2013. — С. 73–74.
6. Потій, О. В. Онтологічні моделі властивостей зрілості процесів захисту інформації [Текст] / О. В. Потій // Прикладная радиоэлектроника. — 2009. — Т. 8, № 3. — С. 388–395.
7. Потий, А. В. Системно-онтологический анализ предметной области оценивания гарантий информационной безопасности [Текст] / А. В. Потий, Д. С. Комин // Радіоелектронні і комп'ютерні системи. — 2010. — № 5. — С. 50–56.
8. Антонюк, А. О. Використання онтологічного підходу при побудові моделі загроз інформації [Текст] / А. О. Антонюк, В. В. Жора, І. Г. Кожевников // Всеукраїнська науково-практична конференція «В. М. Глушков — піонер кібернетики». — Київ, 2014. — С. 187–188.
9. DoD 5200.28-STD. Department of Defense Trusted Computer System Evaluation Criteria [Electronic resource]. — December 1985. — Available at: \www/URL: http://fas.org/irp/nsa/rainbow/std001.htm. — 15.03.2016.
10. Mate Bacic, E. The Canadian trusted computer product evaluation criteria [Text] / E. Mate Bacic // Proceedings of the Sixth Annual Computer Security Applications Conference. — Institute of Electrical & Electronics Engineers (IEEE), 1990. — P. 188–196. doi:10.1109/csac.1990.143768
11. Ekelhart, A. Security Ontology: Simulating Threats to Corporate Assets [Text] / A. Ekelhart, S. Fenz, M. D. Klemen, E. R. Weippl // Lecture Notes in Computer Science. — 2006. — Vol. 4332. — P. 249–259. doi:10.1007/11961635_17
12. Ekelhart, A. Security Ontologies: Improving Quantitative Risk Analysis [Text] / A. Ekelhart, S. Fenz, M. Klemen, E. Weippl // Proceedings of the 40th Annual Hawaii International Conference on System Sciences. — Institute of Electrical & Electronics Engineers, 2007. — P. 156a. doi:10.1109/HICSS.2007.478
13. Fenz, S. Ontology based IT-security planning [Text] / S. Fenz, E. Weippl // Proceedings of the 12th Pacific Rim International Symposium on Dependable Computing (PRDC'06). — Institute of Electrical & Electronics Engineers (IEEE), 2006. — P. 389–390. doi:10.1109/prdc.2006.49
14. Choi, C. A Design of Onto-ACM (Ontology based Access Control Model) in Cloud Computing Environments [Text] / C. Choi, J. Choi, B. Ko, K. Oh, P. Kim // Information Leakage Prevention in Emerging Technologies. — 2012. — Vol. 2, № 3/4. — P. 54–64.

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ ОНТОЛОГИЧЕСКОГО ПОДХОДА К ПОСТРОЕНИЮ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Исследованы основные этапы построения комплексных систем защиты информации, проведен их анализ та предмет применимости методов формального моделирования. Предложено использовать онтологические модели на отдельных этапах построения комплексных систем защиты информации. Приведен пример таксономии и онтологической модели нарушителя.

Ключевые слова: защита информации, информационно-телекоммуникационная система, онтология, нарушитель.

Жора Віктор Володимирович, *молодший науковий співробітник, науково-дослідний відділ № 11 «Автоматизованих інформаційних систем», Інститут програмних систем НАН України, Київ, Україна,* ***e-mail: victor.zhora@gmail.com****.*

Жора Виктор Владимирович, *младший научный сотрудник, научно-исследовательский отдел № 11 «Автоматизированных информационных систем», Институт программных систем НАН Украины, Киев, Украина.*

Zhora Victor, *Institute of Software Systems, National Academy of Science of Ukraine, Kyiv, Ukraine,* ***e-mail: victor.zhora@gmail.com***