УДК 004.056+004.942

ОНТОЛОГІЧНИЙ АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДАНИХ

А. В. Кудряшова

Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

Розглянуто проблему класифікації загроз інформаційної безпеки в умовах стрімкого розвитку інформаційних технологій, що супроводжується зростанням залежності організацій від інформаційних систем та значним збільшенням обсягів даних. Проаналізовано недоліки існуючих підходів до оцінки та попередження ризиків, які часто зосереджуються на вузьких аспектах безпеки, не враховуючи взаємозв'язки між різними типами загроз та елементами інформаційної інфраструктури. Запропоновано універсальну онтологічну модель, що дозволяє систематизувати знання про загрози інформаційної безпеки та надає інструменти для їх ідентифікації, аналізу, прогнозування та попередження. Модель базується на багаторівневій ієрархічній структурі, яка охоплює як загальні категорії загроз, так і конкретні прояви, зокрема: класифікацію загроз за аспектами інформаційної безпеки (конфіденційність, цілісність, доступність); ймовірністю виникнення (ймовірні, малоймовірні загрози); компонентами інформаційних систем, на які спрямовані загрози (інфраструктура, апаратне та програмне забезпечення, дані); обсягом збитків (граничні, значні, незначні); розташуванням джерел загрози (внутрішні, зовнішні); способом реалізації (випадкові дії, навмисні дії, природні явища, техногенні фактори); характером завданого збитку (матеріальні, моральні). Сформовано екземпляри, що деталізують класифікацію через реальні сценарії загроз. Основним інструментом моделі є онтологічний граф, який відображає ієрархію, взаємозв'язки між класами та екземплярами.

Запропонований підхід забезпечує комплексний аналіз загроз та дозволяє ідентифікувати потенційні ризики на основі їх класифікаційних ознак. Використання онтологічного графа сприяє візуалізації та аналітичній обробці загроз, що підвищує ефективність прийняття рішень у сфері управління інформаційною безпекою. Модель може бути інтегрована в програмні інструменти моніторингу та прогнозування загроз, а також адаптована для практичного застосування в корпоративних системах безпеки.

Ключові слова: *онтологія, інформаційна безпека, загроза, клас, екземпляр, граф.*

Постановка проблеми. У сучасних умовах стрімкого розвитку інформаційних технологій інформаційна безпека стає одним із ключових аспектів забезпечення стабільної роботи організацій. Зростання залежності від інформаційних систем,

розширення кількості підключених пристроїв, а також збільшення обсягів даних створюють нові ризики, пов'язані з порушеннями конфіденційності, цілісності та доступності інформації. При цьому різноманітність загроз, які можуть виникати як через випадкові технічні збої, так і через навмисні дії зловмисників, ускладнює їхню класифікацію, оцінку та попередження.

Існуючі підходи до аналізу загроз інформаційної безпеки часто зосереджуються на вузькоспеціалізованих аспектах, не враховуючи складних взаємозв'язків між різними типами загроз та компонентами інформаційних систем. Це призводить до фрагментованості підходів до забезпечення безпеки, що ускладнює своєчасне виявлення ризиків, прогнозування потенційних інцидентів та розроблення ефективних заходів реагування.

Побудова онтологій для класифікації загроз є перспективним підходом, що дозволяє систематизувати знання в цій сфері. Онтології забезпечують багаторівневу ієрархічну структуру, яка дає змогу врахувати як загальні категорії загроз, так і їхні конкретні прояви. Проте побудова таких моделей вимагає не лише створення чіткої класифікації загроз, а й формування екземплярів, що відображають реальні сценарії їхнього виникнення, а також побудови онтологічного графу для візуалізації та аналізу взаємозв'язків між класами та екземплярами.

Отже, проблема полягає у необхідності розроблення універсальної онтологічної моделі загроз інформаційної безпеки, яка враховувала б різні аспекти загроз, їхню природу, джерела виникнення, ймовірність реалізації, а також наслідки. Така модель повинна стати основою для аналізу, прогнозування та попередження загроз, а також для підтримки прийняття рішень у сфері управління інформаційною безпекою.

Аналіз останніх досліджень та публікацій. Публікації присвячені побудові онтології альтернатив прототипування інтерактивних віртуальних систем [1], оцінюванню компетентності експертної групи на основі онтологічного аналізу [2], розробленню онтологічної моделі для моніторингу та оцінки діяльності наукових установ [3], використанню онтологічного підходу для підвищення якості розроблення національних стандартів України [4], розробленню методу оцінювання достатності інформації для визначення якості програмного забезпечення на основі онтології [5, 6], розробленню онтологічної моделі бази даних [7] тощо. Однак, недостатньо розкрите питання використання методів онтологічного аналізу для класифікації загроз інформаційної безпеки.

Мета статті. Метою дослідження є розроблення онтології для класифікації загроз інформаційної безпеки.

Виклад основного матеріалу дослідження. Онтологія загроз інформаційної безпеки є структурованою моделлю, що забезпечує систематизацію загроз відповідно до їх характеристик, аспектів впливу та способів реалізації. На рис. 1. представлено фрагмент таксономії понять онтології для класифікації загроз інформаційної безпеки.

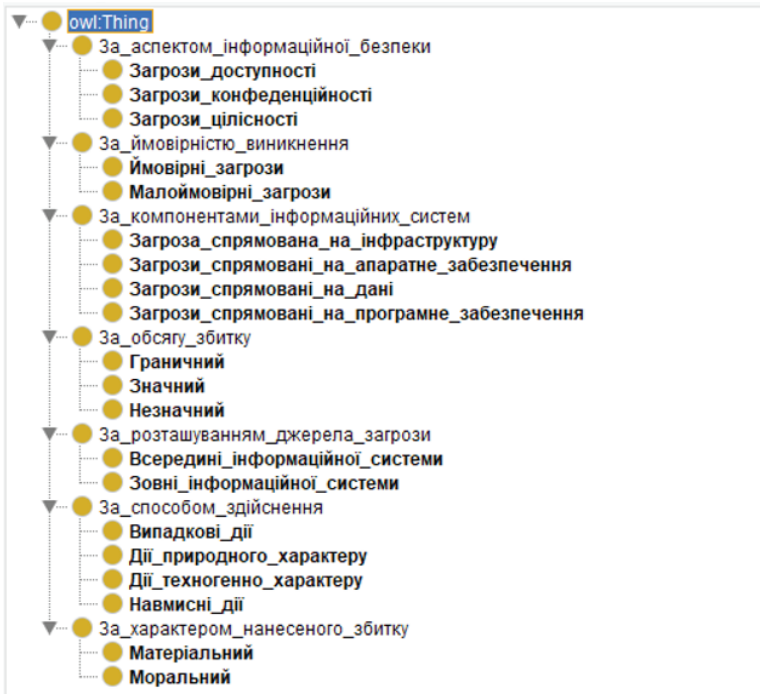

Рис. 1. Фрагмент таксономії понять онтології для класифікації загроз інформаційної безпеки

За аспектом інформаційної безпеки загрози класифікуються на три основні категорії: загрози доступності, загрози конфіденційності, загрози цілісності. Загрози доступності стосуються порушення безперервного доступу до інформаційних ресурсів, що може унеможливити їх використання в критичний момент. Загрози конфіденційності зосереджені на ризиках розголошення або несанкціонованого доступу до даних, що порушує принцип збереження секретності інформації. Загрози цілісності спрямовані на порушення правильності, повноти або актуальності даних, що може вплинути на прийняття рішень або функціонування системи загалом.

За ймовірністю виникнення загрози поділяються на ймовірні та малоймовірні. Ймовірні загрози характеризуються високою вірогідністю реалізації через існуючі умови або вразливості, тоді як малоймовірні загрози можуть виникнути лише за специфічних обставин, що мають низьку ймовірність реалізації.

У розрізі компонентів інформаційних систем загрози класифікуються залежно від того, на який елемент системи вони спрямовані. Загрози, спрямовані на інфраструктуру, пов’язані з пошкодженням або виведенням з ладу фізичних елементів, таких як сервери, мережеве обладнання чи комунікаційні канали. Загрози, що стосуються апаратного забезпечення, охоплюють атаки на пристрої або окремі компоненти обладнання. Загрози, спрямовані на дані, передбачають несанкціоноване видалення, зміну або викрадення інформації. Загрози програмного забезпечення включають атаки на додатки, операційні системи чи інші програмні елементи.

За обсягом збитку загрози поділяються на граничні, значні та незначні. Граничні загрози характеризуються катастрофічними наслідками для функціонування інформаційної системи або організації загалом. Значні загрози можуть суттєво порушити функціонування окремих компонентів системи, проте не призводять до повного колапсу. Незначні загрози мають обмежений вплив, що не є критичним для системи.

Критерій розташування джерела загрози дає змогу розрізняти загрози, що виникають усередині або поза межами інформаційної системи. Внутрішні загрози походять від користувачів, співробітників або внутрішніх процесів системи, тоді як зовнішні загрози викликані впливом зовнішніх суб'єктів або подій.

За способом здійснення загрози поділяються на випадкові дії, природні явища, техногенні фактори та навмисні дії. Випадкові дії виникають через помилки користувачів або несправність обладнання. Природні явища включають стихійні лиха, що впливають на інфраструктуру системи. Техногенні фактори пов'язані з аваріями або технічними збоями. Навмисні дії охоплюють цілеспрямовані атаки з боку зловмисників.

Ще одним критерієм є характер завданого збитку, за яким загрози поділяються на матеріальні та моральні. Матеріальні загрози пов'язані зі збитками, які можна оцінити в грошовому еквіваленті, наприклад, витрати на відновлення системи чи втрату даних. Моральні загрози спричиняють шкоду репутації, довірі або нематеріальним активам організації [8, 9].

Для представлених класів також сформовано екземпляри (рис. 2), що дозволяє уточнити та конкретизувати кожну категорію загроз за допомогою реальних прикладів. Формування екземплярів є важливим етапом розроблення онтологій, оскільки вони забезпечують практичну реалізацію теоретичних конструкцій та полегшують застосування моделі в реальних сценаріях.

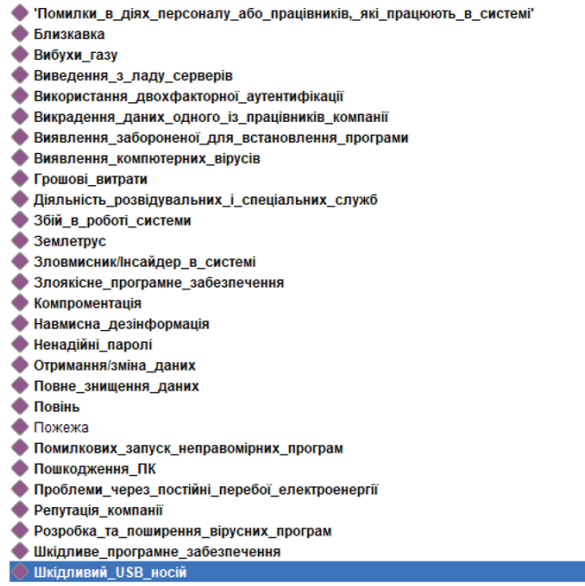

Рис. 2. Екземпляри класів

На основі сформованих класів та відповідних екземплярів побудовано онтологічний граф (рис. 3.), який відображає структуру взаємозв'язків між різними категоріями загроз інформаційної безпеки. Онтологічний граф дозволяє комплексно представити ієрархію загроз, їхню класифікацію, а також взаємозв'язки між окремими елементами. Структура онтологічного графу відображає різні рівні деталізації. Верхній рівень охоплює загальні класифікації загроз, такі як «За аспектом інформаційної безпеки», «За ймовірністю виникнення» тощо. Ці класи деталізуються підкласами, що уточнюють тип загроз, наприклад, «Загрози доступності», «Загрози конфіденційності», «Загрози цілісності» та ін. Екземпляри, які прив'язані до кожного класу, формують найнижчий рівень онтології. Завдяки графу спрощується процес аналізу загроз, їхньої ідентифікації та оцінки ризиків. Він може використовуватись як основа для розроблення систем підтримки прийняття рішень у сфері інформаційної безпеки. Крім того, граф забезпечує інтеграцію онтології в програмні інструменти моніторингу та прогнозування загроз, підвищуючи ефективність реагування на потенційні інциденти [2, 8, 9].

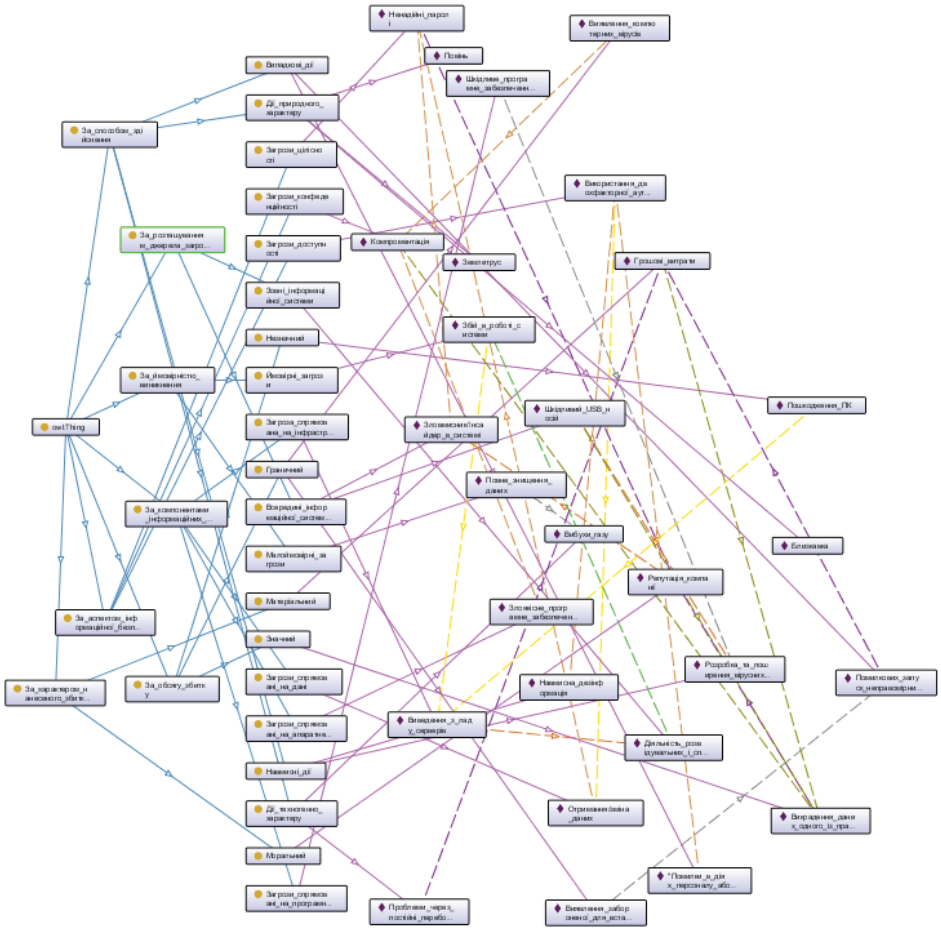

Рис. 3. Загальний онтологічний граф класів та екземплярів

Таким чином, представлена онтологія забезпечує всебічний підхід до аналізу та класифікації загроз, що дозволяє не лише ідентифікувати потенційні ризики, але й розробляти ефективні механізми їхнього попередження та мінімізації.

Висновки. Внаслідок онтологічного аналізу розроблено загальний онтологічний граф, який виступає не лише як модель, що систематизує знання про загрози інформаційної безпеки, але й як практичний інструмент для вдосконалення систем управління безпекою у сучасних інформаційних середовищах. Крім того, формування екземплярів для кожного класу онтології сприяє інтеграції онтології в практичні системи управління інформаційною безпекою та підвищує її прикладну цінність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kudriashova, A., Pikh, I., Senkivskyy, V., Merenych, Y. Evaluation of prototyping methods for interactive virtual systems based on fuzzy preference relation. *Eastern-European Journal of Enterprise Technologies*. 2024. № 5(4 (131). Pp. 71–81.
2. Кудряшова А. В., Сельменський Р. А. Роль онтології в оцінюванні компетентності експертів. Методика опрацювання експертних висновків щодо факторів впливу на якість післядрукарського опрацювання книжкових видань. *Поліграфія і видавнича справа*. 2022. № 2 (84). С. 36–43.
3. Глоба Л. С., Новогрудська Р. Л., Задоєнко Б. О. Онтологічна модель оцінки ефективності функціонування наукових установ. *Вісник Харківського національного університету імені В.Н. Каразіна, серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління»*, 2020. № 45. С. 21–34.
4. Гладун А. Я., Рогушина Ю. В. Онтологічний підхід до проблем підвищення якості розроблення національних стандартів України. *Стандартизація. Сертифікація. Якість*. 2016. № 2. С. 19–28.
5. Говорущенко Т.О., Іванов О. В., Павлова О. О. Метод оцінювання достатності інформації для визначення якості програмного забезпечення на основі зваженої онтології. *Вісник Хмельницького національного університету. Технічні науки*. 2016. № 5. С. 146–155.
6. Говорущенко Т. О., Поморова О. В. Метод оцінки достатності інформації для визначення складності та якості програмного забезпечення на основі порівняльного аналізу онтологій. *Радіоелектронні і комп'ютерні системи*. 2016. № 6. С. 59–68.
7. Сілагін О., Сілагін Є., Денисюк В., Денисюк А. Розробка онтологічної моделі бази знань «Бібліотека» на базі середовища Protégé. *Інформаційні технології та комп'ютерна інженерія.* 2023. № 3. С. 12–21.
8. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посіб. К.: Кондор, 2008. 382 с.
9. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с.

REFERENCES

1. Kudriashova, A., Pikh, I., Senkivskyy, V., Merenych, Y. (2024). Evaluation of prototyping methods for interactive virtual systems based on fuzzy preference relation. Eastern-European Journal of Enterprise Technologies, 5(4 (131), 71–81 (in English).

2. Kudriashova A. V., Selmenskyi R. A. (2022). Rol ontolohii v otsiniuvanni kompetentnosti ekspertiv. Metodyka opratsiuvannia ekspertnykh vysnovkiv shchodo faktoriv vplyvu na yakist pisliadrukarskoho opratsiuvannia knyzhkovykh vydan. Polihrafiia i vydavnycha sprava, 2 (84), 36–43 (in Ukrainian).
3. Hloba L. S., Novogrudska R. L., Zadoienko B. O. (2020). Ontolohichna model otsinky efektyvnosti funktsionuvannia naukovykh ustanov. Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina, seriia «Matematychne modeliuvannia. Informatsiini tekhnolohii. Avtomatyzovani systemy upravlinnia», 45, 21–34 (in Ukrainian).
4. Hladun A. Ya., Rohushyna Yu. V. (2016). Ontolohichnyi pidkhid do problem pidvyshchennia yakosti rozroblennia natsionalnykh standartiv Ukrainy. Standartyzatsiia. Sertyfikatsiia. Yakist, 2, 19–28 (in Ukrainian).
5. Hovorushchenko T. O., Ivanov O. V., Pavlova O. O. (2016). Metod otsiniuvannia dostatnosti informatsii dlia vyznachennia yakosti prohramnoho zabezpechennia na osnovi zvaszhenoi ontolohii. Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky, 5, 146–155 (in Ukrainian).
6. Hovorushchenko T. O., Pomorova O. V. (2016). Metod otsinky dostatnosti informatsii dlia vyznachennia skladnosti ta yakosti prohramnoho zabezpechennia na osnovi porivnialnoho analizu ontolohii. Radioelektronni i kompiuterni systemy, 6, 59–68 (in Ukrainian).
7. Silahin O., Silahin Ye., Denysiuk V., Denysiuk A. (2023). Rozrobka ontolohichnoi modeli bazy znan «Biblioteka» na bazi seredovyshcha Protege. Informatsiini tekhnolohii ta kompiuterna inzheneriia, 3, 12–21 (in Ukrainian).
8. Kormych B. A. (2008). Informatsiina bezpeka: orhanizatsiino-pravovi osnovy: navch. posib. K.: Kondor, 382 (in Ukrainian).
9. Lipkan V. A., Maksymenko Yu. Ye., Zhelikhovskyi V. M. (2006). Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii: Navchalnyi posibnyk. K.: KNT, 280 (in Ukrainian).

doi: 10.32403/1998-6912-2024-2-69-21-28

ONTOLOGICAL ANALYSIS OF DATA INFORMATION SECURITY THREATS

A. V. Kudriashova

Ukrainian Academy of Printing,
19, Pid Holoskom, St., Lviv, 79020, Ukraine
alona.v.kudriashova@lpnu.ua

The problem of classifying information security threats in the context of the rapid development of information technologies is considered, which is accompanied by an increasing dependence of organizations on information systems and a significant growth in data volumes. The shortcomings of existing approaches to risk assessment and prevention are analyzed, as they often focus on narrow aspects of security without considering the interconnections between different types of threats and elements of the

information infrastructure. A universal ontological model is proposed, which allows systematizing knowledge about information security threats and provides tools for their identification, analysis, forecasting, and prevention.

The model is based on a multi-level hierarchical structure that includes both general categories of threats and specific manifestations, in particular: the classification of threats by aspects of information security (confidentiality, integrity, availability); the probability of occurrence (likely, unlikely threats); the components of information systems targeted by threats (infrastructure, hardware, software, data); the severity of losses (critical, significant, minor); the location of threat sources (internal, external); the method of realization (accidental actions, intentional actions, natural phenomena, technogenic factors); the nature of damage caused (material, moral). Instances have been created to detail the classification through real threat scenarios. The main tool of the model is an ontological graph that represents the hierarchy and interconnections between classes and instances.

The proposed approach ensures a comprehensive analysis of threats and allows identifying potential risks based on their classification characteristics. The use of the ontological graph facilitates the visualization and analytical processing of threats, enhancing decision-making efficiency in the field of information security management. The model can be integrated into software tools for threat monitoring and forecasting and adapted for practical application in corporate security systems.

Keywords: *ontology, information security, threat, class, instance, graph.*

Стаття надійшла до редакції 12.08.2024.
Received 12.08.2024.