DOI: 10.59647/978-617-520-936-3/1

Онтологічний підхід до задач захисту інформації

Осокін Арсен, бакалавр, студент [1] [i] (ORCID: 0009-0000-5388-6966)

[1] *Київський національний університет будівництва і архітектури, 03037, м. Київ, проспект Повітряних Сил, 31, Україна*

АНОТАЦІЯ

Онтологічний підхід до захисту інформації надає нові можливості для побудови концептуальних моделей, що систематизують управління безпекою інформаційних систем. Він дозволяє більш гнучко підходити до виявлення загроз та управління ризиками завдяки опису взаємозв'язків між компонентами системи. Однак складність його впровадження пов'язана з необхідністю ретельної розробки онтологічних моделей та інтеграції з існуючими інструментами кібербезпеки. Такий підхід є особливо актуальним в умовах зростання кіберзагроз та складних архітектур інформаційних систем.

Ключові слова: онтологія, захист інформації, кібербезпека, управління ризиками, інформаційна безпека.

1. ВСТУП

Інформаційна безпека стає дедалі важливішою через швидке зростання обсягів цифрових даних та кількості кіберзагроз. Традиційні методи, такі як системи управління доступом і фаєрволи, не завжди відповідають вимогам нових динамічних середовищ, адже вони часто базуються на статичних правилах, що обмежують їх здатність до адаптації. В умовах постійно змінюваних кіберзагроз необхідно використовувати більш гнучкі підходи, які можуть автоматично реагувати на нові виклики.

Одним із таких перспективних підходів є онтологічний підхід до захисту інформації, що дозволяє не лише враховувати взаємозв'язки між елементами системи, але й будувати динамічні моделі її поведінки. Однак реалізація цього підходу є складним завданням, що вимагає значних зусиль з розробки онтологій та інтеграції їх у наявні системи безпеки.

2. МЕТА РОБОТИ

Метою роботи є дослідження онтологічного підходу до задач захисту інформації, порівняння його з існуючими методами та аналіз труднощів його реалізації в інформаційних системах.

3. ПРИНЦИПИ ОНТОЛОГІЧНОГО ПІДХОДУ

Онтологічний підхід до захисту інформації передбачає створення моделі, яка описує всі сутності системи, їх властивості та взаємодії між ними. Це дозволяє будувати систему, що не просто застосовує заздалегідь визначені правила для захисту, а розуміє зв'язки між її компонентами, ідентифікуючи вразливі місця та потенційні загрози. Наприклад, замість того, щоб просто блокувати певні типи трафіку, як це робить фаєрвол, онтологія може враховувати, як цей трафік пов'язаний з іншими елементами системи і який вплив він може мати на різні компоненти. Це підвищує здатність до виявлення складних і багатогранних загроз, які можуть бути непомітними для традиційних систем.

Однією з основних переваг онтологічного підходу є його здатність автоматизувати процес управління загрозами. Завдяки моделюванню взаємодій між компонентами, онтологія може в реальному часі оцінювати можливі ризики та адаптувати політику захисту залежно від змін у системі. Це стає особливо важливим у динамічних середовищах, таких як хмарні обчислення або розподілені системи, де конфігурації можуть змінюватися буквально кожну секунду.

4. ПЕРЕВАГИ ОНТОЛОГІЧНОГО ПІДХОДУ

Онтологічний підхід до захисту інформації має кілька ключових переваг. По-перше, він забезпечує систематизований і формалізований підхід до організації знань про систему, що дозволяє точно описати її компоненти та їхні взаємозв'язки. По-друге, цей підхід сприяє кращому розумінню загроз і ризиків, пов'язаних із кожним компонентом системи, оскільки зв'язки між елементами стають прозорішими. Це дає можливість побудувати ефективнішу стратегію захисту, що враховує майже всі аспекти функціонування інформаційної системи.

Крім того, онтології забезпечують масштабованість і гнучкість систем захисту, що є важливим у контексті сучасних гетерогенних мереж і динамічних середовищ. Використовуючи онтологічну модель, можна легко адаптувати систему до нових вимог, додати нові компоненти або змінити існуючі, не порушуючи загальної структури захисту.

Онтологічний підхід також відкриває можливість для автоматизації процесів управління ризиками та виявлення загроз, що значно підвищує ефективність захисту. За допомогою алгоритмів, що працюють на основі онтологій, можна аналізувати величезні обсяги даних, ідентифікувати загрози в режимі реального часу та оперативно вживати необхідних заходів для їх нейтралізації.

5. СКЛАДНОСТІ РЕАЛІЗАЦІЇ

Попри значні переваги, реалізація онтологічного підходу стикається з низкою серйозних викликів. Одним із головних бар'єрів є складність розробки самих онтологій. Створення моделі, яка адекватно описує всі елементи системи та їхні взаємозв'язки, вимагає глибоких знань про структуру системи та її поведінку. Крім того, кожен компонент має бути точно охарактеризований, а це може бути дуже трудомістким процесом, особливо для великих або складних систем. Також важливо, щоб ці моделі залишалися актуальними, оскільки інформаційні системи постійно змінюються. Це означає, що онтології потребують регулярного оновлення, що вимагає додаткових ресурсів.

Іншою складністю є інтеграція онтологічного підходу з існуючими системами безпеки. Більшість сучасних систем захисту інформації використовують традиційні методи, тому

перехід на онтологічну модель може вимагати серйозних змін у інфраструктурі безпеки. Це може включати оновлення інструментів моніторингу, перепроектування систем виявлення загроз або зміни в управлінні доступом.

Важливим фактором є й потреба у значних обчислювальних ресурсах для ефективної роботи онтологічної системи. Обробка великих обсягів даних у реальному часі, побудова і підтримка взаємозв'язків між компонентами системи вимагає високих обчислювальних потужностей, що може стати додатковою проблемою для організацій із обмеженими ресурсами.

6. ПОРІВНЯННЯ З ІСНУЮЧИМИ АНАЛОГАМИ

Онтологічний підхід має кілька суттєвих переваг над існуючими методами захисту інформації. На відміну від традиційних систем управління доступом, які покладаються на жорсткі політики та ролі, онтології дозволяють описати складні взаємодії між компонентами системи і гнучко налаштовувати доступ на основі цих взаємозв'язків. Це робить онтологічний підхід більш ефективним для динамічних середовищ, де традиційні методи можуть виявитися занадто жорсткими і не в змозі швидко реагувати на зміни.

Також, на відміну від систем, які базуються на фіксованих правилах (наприклад, фаєрволи або IDS/IPS), онтології не обмежуються заздалегідь визначеними сценаріями. Вони дозволяють гнучко адаптувати поведінку системи на основі поточних даних та взаємозв'язків, що значно підвищує їх здатність до виявлення нових і складних загроз. Однак, порівняно з методами машинного навчання, онтологічні системи мають ту перевагу, що не потребують великих обсягів навчальних даних для ефективної роботи. З іншого боку, машинне навчання дозволяє швидко адаптувати систему до нових умов, тоді як онтології вимагають детального і часто тривалого процесу моделювання.

7. ПРИКЛАДИ УСПІШНОЇ РЕАЛІЗАЦІЇ

Одним із найбільш відомих прикладів успішної реалізації онтологічного підходу є система MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge). MITRE ATT&CK – це глобальна база знань про тактики, техніки та процедури атак, яку використовують як основу для моделювання поведінки зловмисників. Вона базується на онтологічному підході, де кожна техніка або тактика описується як сутність з певними властивостями та взаємозв'язками.

MITRE ATT&CK дозволяє побудувати модель загроз, яка показує, як різні техніки атак можуть використовуватися для компрометації системи. Ця модель не лише описує загрози, але й допомагає організаціям відстежувати ймовірність різних атак у своїх системах, а також визначати, де найвищий ризик виникнення інцидентів безпеки. Використання MITRE ATT&CK у системах моніторингу дозволяє інтегрувати цю модель із засобами виявлення загроз, що значно підвищує точність і швидкість реагування на атаки.

Одним із прикладів практичного використання MITRE ATT&CK є його інтеграція з системами виявлення загроз і реагування на них, такими як SIEM (Security Information and Event Management). У таких системах онтологічна база знань MITRE ATT&CK використовується для аналізу поведінкових шаблонів і виявлення відхилень, що дозволяє краще відстежувати складні атаки, які могли б залишитися непоміченими при використанні лише традиційних методів захисту.

Успіх MITRE ATT&CK підкреслює важливість онтологічного підходу до захисту інформації, оскільки цей підхід дозволяє створювати більш точні й адаптивні системи захисту. Завдяки своїй гнучкості, онтологічні моделі можуть бути постійно оновлювані й доповнювані новими даними про загрози, що робить їх дуже ефективним інструментом у сучасних системах кібербезпеки.

8. ВИСНОВКИ

Онтологічний підхід до захисту інформації є перспективним напрямком, що дозволяє забезпечити більш точний та гнучкий захист сучасних інформаційних систем. Однак його реалізація вимагає значних ресурсів, як людських, так і технічних. Попри складності, цей підхід відкриває нові можливості для моделювання загроз та управління ризиками завдяки своїй здатності враховувати взаємозв'язки між компонентами системи. З огляду на швидке зростання складності кіберзагроз, онтології можуть стати важливим елементом майбутніх систем безпеки, забезпечуючи більш гнучке і динамічне реагування на нові виклики.

Список літератури

[1] Lewis, P. R., Yakovlev, N. (2020). Ontologies for cybersecurity: Threat intelligence and mitigation. *Proceedings of the 2020 International Conference on Cybersecurity*.

[2] Undercoffer, J., Joshi, A., Finin, T., Pinkston, J. (2002). Modeling computer attacks: An ontology for intrusion detection. *Proceedings of the 25th Annual IFIP WG 11.3 Conference on Data and Applications Security*.

[3] Bertino, E., Sandhu, M. (2005). Database security—Concepts, approaches, and challenges. *IEEE Transactions on Dependable and Secure Computing*.

[4] Schoultz, R. D., Snyder, B. (2019). Ontology-based approach for dynamic cybersecurity threat detection. *Cybersecurity and Network Security Journal*.

[5] Stewart, J. N. (2020). Cybersecurity ontologies: Structuring knowledge in an interconnected world. *Information Security Journal: A Global Perspective*.

[6] Parsons, D. P. (2021). Security event correlation using MITRE ATT&CK framework: A case study. *Journal of Information Security Technology*.

[7] «ДСТУ ГОСТ 7.1: 2006»

[8] «ДСТУ 8302:2015»

[i] *Робота виконана під керівництвом к. т. н., доц. Олени Гордої*