КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.21.211222
УДК 004.82:343.9

Власенко Лідія Олександрівна
к.т.н., доц., доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID ID: 0000-0002-2003-6313
vlasenko.lidia1@gmail.com

Луцька Наталія Миколаївна
д.т.н., проф., професор кафедри автоматизації та комп'ютерних технологій систем управління
Національний університет харчових технологій, Київ, Україна
ORCID ID: 0000-0001-8593-0431
lutskanm2017@gmail.com

Савченко Тетяна Віталіївна
к.т.н., доц., доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID ID: 0000-0002-8884-5360
sv_t@ukr.net

Богданов Олександр Михайлович
д.т.н., проф.
професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0009-0005-2605-6189
o.bohdanov@kubg.edu.ua

ОНТОЛОГІЧНЕ МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ ДАНИХ ЦИФРОВОГО КРИМІНАЛЬНОГО ЗЛОЧИНУ

Анотація. У статті сформовано та досліджено онтологічну модель інформаційних даних цифрового кримінального злочину. Онтологічне моделювання дозволило концептуалізувати знання та ефективно подолати проблеми недостатньої структурованості, неоднозначності та неузгодженості даних та знань в сфері цифрової криміналістики. На основі проведеної класифікації виділено п’ять основних класів (Цифровий злочин, Цифрові сліди, Типи злочинів, Злочинець та Кримінальна відповідальність), до яких відносяться множини користувацьких і некористувацьких екземплярів, в тому числі відповідні статті Кримінального кодексу України та міжнародного права. Користувач формує екземпляри трьох класів: Цифровий злочин, Цифрові сліди та Злочинець. Вони містять персональну інформацію про цифровий злочин та є основними даними користувацької частини онтологічної моделі як бази знань. Класи Типи злочинів та Кримінальна відповідальність є некористувацькими та зміни до них можуть вносити лише фахівці зі служби супроводження моделі. Онтологічна модель реалізована в Protege мовою OWL, що є неформальним стандартом для створення та обміну онтологіями. Із виділених семи зв’язків між сутностями лише три заносяться до онтології користувачем, інші – на основі розроблених правил SWRL, формуються автоматично. Використовуючи мову запитів SPARQL, наведено шаблони пошуку, фільтрації та аналізу інформації в реальному часі, що допомагають виявити складні взаємозв'язки між об'єктами та згенерувати нові онтологічні знання. Результати дослідження підкреслюють важливість онтологічного моделювання в сфері цифрової криміналістики та способів використання SPARQL-запитів для покращення обробки даних, аналізу та розуміння знань у цій галузі.

Ключові слова: цифровий кримінальний злочин; прикладна онтологія; цифрова криміналістика.

ВСТУП

За даними Федерального Бюро Розслідувань (ФБР) [1] було зареєстровано 800944 скарги на злочини, скоєні в Інтернеті, на щонайменше 422 мільйони людей (рис. 1). Також ФБР прогнозує, що в 2023 році буде зламано майже 33 мільярди облікових записів, а витрати на ці зломи оцінюються у 8 трильйонів доларів. За даними ФБР до найпоширеніших цифрових злочинів відносяться: фішинг, порушення персональних даних, вимагання, втручання в роботу технічної підтримки, шахрайства, пов'язані з неоплатою/недоставкою послуг.

За офіційною статистикою Офісу Генерального прокурора України [2] кількість цифрових злочинів в Україні за останні 5 років зросла майже на 64% і в 2022 році становила майже 9900 зареєстрованих правопорушень. І за прогнозами на 2023 рік Офіс Генерального прокурора України очікує її зростання. Найбільша кількість правопорушень у 2022 році була порушена за статтею 362 Кримінального Кодексу України (ККУ) [3] «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї».

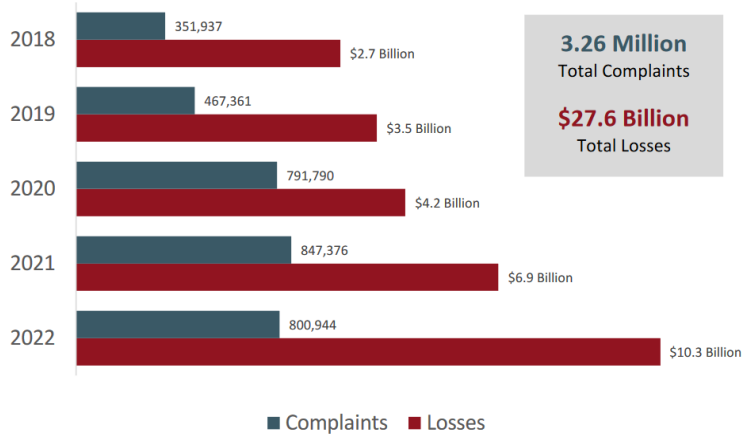


Рис. 1. Статистика злочині в Інтернеті за період 2018 – 2022 роки за даними ФБР

В зв'язку із тенденціями, які прослідковуються останнім часом, а саме, збільшення цифрових кримінальних злочинів, підвищення вмінь і навичок злочинців в IT-сфері, розвитку цифрових, інформаційних технологій, пристроїв, цифровізації всіх сфер життя, впроваджені елементів штучного інтелекту в різні пристрої користування, спеціалістам необхідно збирати, аналізувати, обробляти великі масиви різнорідної часто неповної інформації. Отже, з'являється об'єктивна необхідність побудови онтології для сфери цифрової криміналістики, яка б дозволила відстежувати зміни та появу нових трендів в галузі цифрових кримінальних злочинів, а також аналізувати нові методи та технології, які використовуються злочинцями.

Постановка проблеми. Незважаючи на широку дослідницьку діяльність в цій сфері більшість розроблених онтологічних моделей для цифрової криміналістики не є універсальними, здебільшого спрямовані на підтримку процесу розслідування цифрового кримінального злочину, пошуку нових знань, пов'язаних з можливими мотивами і способами його скоєння. У переважній більшості онтологічних моделей враховані лише вузькоспеціалізовані аспекти, що суттєво звужує сферу їх застосування

[4]. Онтологічна модель, запропонована в даній статті, орієнтована на поглиблення та кращу організацію знань предметної області цифрової криміналістики України з урахуванням аспектів міжнародного законодавства.

Аналіз останніх досліджень і публікацій. Онтології широко використовуються в різних дисциплінах як підхід для представлення та міркування знань предметної області. Однак, незважаючи на широку дослідницьку діяльність, пов'язану з онтологіями, і застосування в різних галузях, розвиток онтологій і дослідницька діяльність все ще є недостатньою для цифрової криміналістики. Зокрема, в роботах [5], [6] обґрунтовується доцільність створення онтології для цифрових кримінальних злочинів. Така онтологія дозволяє краще класифікувати концепти цифрової криміналістики, а також включає в себе такі сфери, як професійна спеціалізація, сертифікація, розробка цифрових криміналістичних інструментів, навчальні програми та навчальні матеріали. Однак, вона містить кримінальну відповідальність країн авторів та не враховує законодавство України.

Останні роки знаменуються активним впровадженням онтологій в різних сферах, для різноманітних предметних областей, як методологія для представлення існуючих та нових знань, а також метазнань. Існують кардинально різні підходи до побудови онтологічних моделей, що пов'язано з різноманітністю і особливостями предметних областей, поставлених задач, цілей та області застосування, масштабів та складності архітектури онтології, джерел даних, рівня деталізації, варіанту формалізму (OWL чи RDF), інструментами реалізації, співпраці з експертами проблемної області, відповідності існуючим стандартам предметної області, можливості адаптації до змін і розширення, кінцевих користувачів. Одним з вітчизняних підходів є побудова онтологічної моделі на поєднанні предметної і проблемної областей за рахунок взаємодії онтологій процесів, задач та предметної області [7], [8]. Інший, міжнародний, підхід ґрунтується на використанні ієрархії під час створення онтологічної моделі. В залежності від обраного підходу може бути використана три- або чотирьохрівнева онтологія [9], для якої спочатку розробляється онтологія верхнього рівня. На сьогодні продовжується процес стандартизації однієї з таких онтологій – BFO [10]. Далі розробляються онтологія додатку, і прикладна онтологія процесів, задач тощо.

Метою статті є розробка моделі, на основі онтологічного підходу, яка описує основні концепти цифрових кримінальних злочинів. Онтологічна модель включає класи, властивості, відношення між ними, аксіоми, правила, а також специфічну інформацію для кожного класу, яка допоможе краще розуміти предметну область цифрової криміналістики шляхом концептуалізації даних та знань.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

В даній роботі представлено прикладну онтологію інформаційних даних цифрового кримінального злочину, як інструмент, що допоможе узгодити та формалізувати існуючі поняття та відношення. Особливістю цифрової криміналістики є робота з великими масивами неоднорідної інформації, отриманої з різних джерел даних. Часто складністю є їх поєднання між собою і виявлення взаємозв'язків і взаємовпливів. Прикладна онтологія в цьому випадку може забезпечити інтеграцію даних, спільне використання та виявити приховані взаємозв'язки та створити нові знання.

В розробленій прикладній онтології були враховані основні елементи сучасного цифрового злочину, такі як: особа злочинця, мотив та спосіб скоєння правопорушення,

вид та тип злочину, цифрові сліди (докази) його скоєння, а також кримінальна відповідальність, передбачена Кримінальним кодексом України та міжнародним правом.

У сучасному міжнародному праві існує чотири чинні регіональні угоди у сфері боротьби з кіберзлочинністю. В розробленій прикладній онтології, як основний документ міжнародного регулювання кіберзлочинності, враховано Конвенцію про кіберзлочинність Ради Європи, прийнята 21.11.2001 року та Додатковий протокол від 28.01.2003 р. (часто її називають Будапештська конвенція) [11]. Це пояснюється вектором державної політики України, орієнтацію на членство в Європейському Союзі. Але при необхідності прикладна онтологія може бути доповнена та розширена необхідними новими даними.

МЕТОДИКА ДОСЛІДЖЕННЯ

Онтологічне моделювання на основі інформаційних даних цифрового кримінального злочину проводилось в середовищі Protege 5.5, оскільки воно має ряд суттєвих переваг. Зокрема, підтримує формалізовану мову опису онтологій Web Ontology Language (OWL), яка на сьогодні є негласним стандартом; надає різні засоби для візуалізації онтології; різні інструменти для перевірки логічності і незаперечності в її побудові; можливість інтеграції та взаємодії з іншими онтологіями.

При розробці онтологічної моделі інформаційних даних цифрового кримінального злочину було створено класи, підкласи, екземпляри, атрибути, відношення, аксіоми, правила. Загальна метрика наведена на рис. 2.

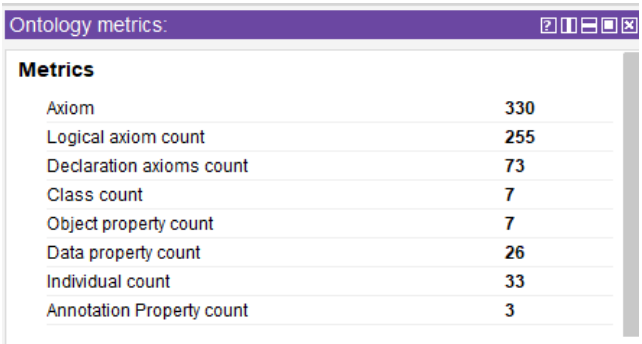
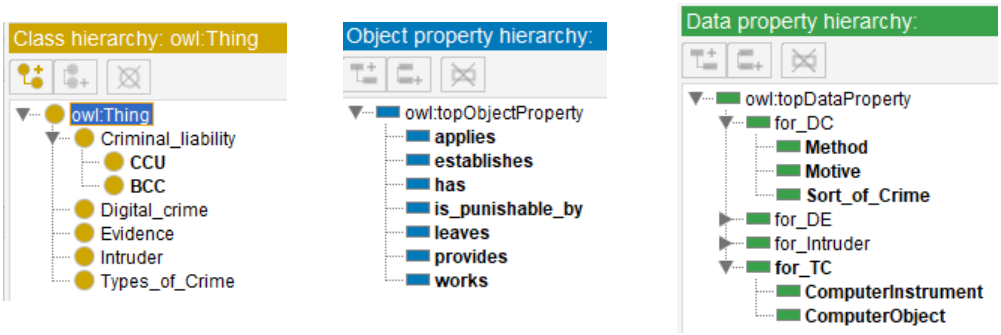


Рис. 2. Онтологічна метрика

Прикладна онтологія містить 5 класів: Цифровий злочин, Цифрові сліди, Типи злочинів, Злочинець та Кримінальна відповідальність. Останній клас містить два підкласи: перший стосується відповідальності згідно законодавства України, а другий – за міжнародним законодавством. Ієрархія класів наведена на рис. 3а. Між класами були встановлені відношення, наведені на рис. 3б. Слід зазначити, що за логікою побудови всі відношення є транзитивними, окрім відношення *establishes*, яке являється інверсним. Також для класів були виділені властивості даних. Їх ієрархія наведена на рис. 3 в.

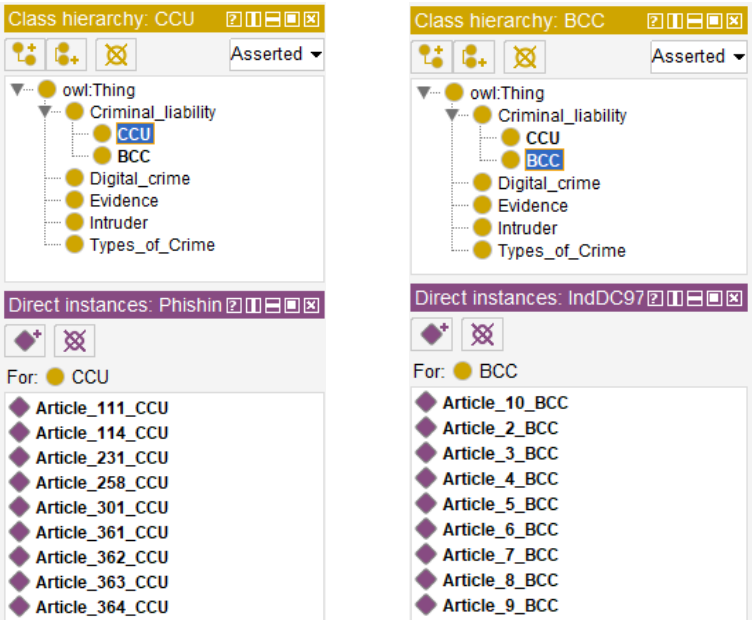
ISSN 2663 - 4023



а) б) в)

Рис. 3. Ієрархія концептів: а – класів; б – об'єктних властивостей; в – властивостей даних

Розробниками було передбачено два типи класів: користувацькі, які дозволяють створення, занесення і заповнення екземплярів користувачами онтології і некористувацькі – створені і заповнені інженерами з онтології в співпраці з експертами і фахівцями у сфері цифрової криміналістики і права. На рис. 4. наведено фрагменти підкласів ККУ та Будапештської конвенції про кіберзлочинність некористувацького класу Кримінальної відповідальності, заповнені екземплярами, що відповідають відповідним кримінальним статтям.



а) б)

Рис. 4. Фрагменти екземплярів некористувацького класу кримінальної відповідальності: а – підклас ККУ; б – підклас Будапештська конвенція про кіберзлочинність

Для встановлення більш складних відношень між об'єктами онтології, автоматичного виводу нових знань на основі існуючих даних та властивостей в онтології, для виведення логічних висновків були розроблені та прописані SWRL-правила (рис. 5).

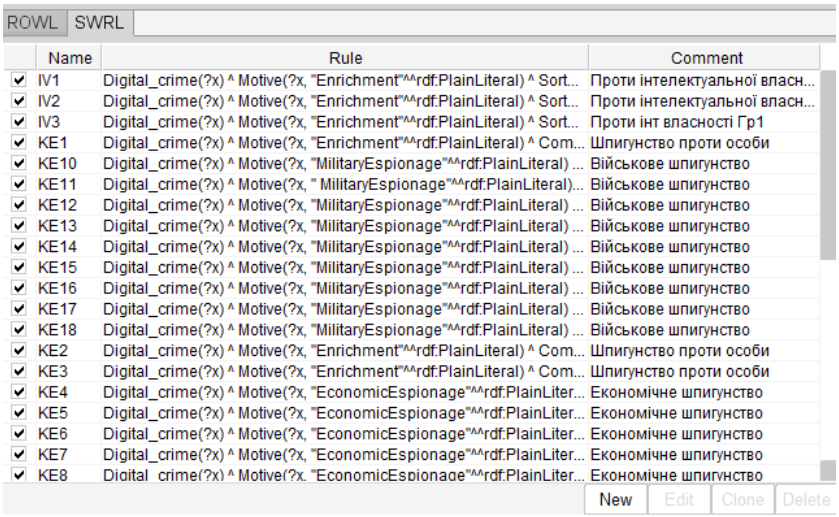


Рис. 5. Фрагмент SWRL-правил

На рис. 6 наведено результат роботи вбудованого Резонера на прикладі екземпляру Фішинг для класу Тип_злочину. Таким чином, забезпечується перевірка онтології на ясність, зрозумілість і відсутність логічних непослідовностей. Також тестування правильності роботи онтології проводилось на визначеній кількості екземплярів користувацького класу Цифровий_злочин. В ході роботи з ними були виявлені незначні лінгвістичні неточності, які були виправлені. Логічні невідповідності були відсутні.

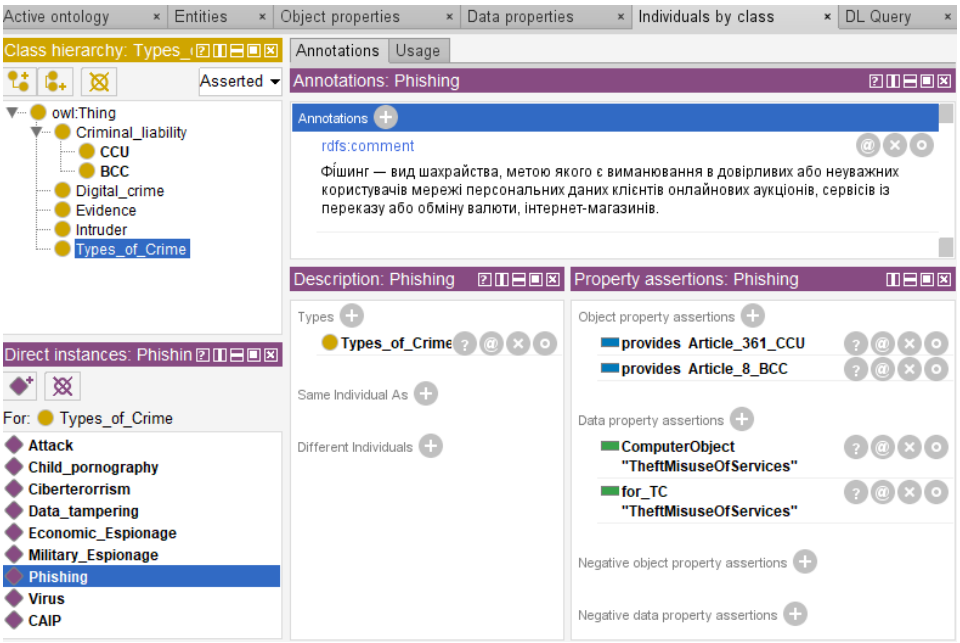


Рис. 6. Екземпляр Фішинг класу Тип_злочину та його атрибути

Візуалізація онтологічної моделі (рис. 7) у вигляді графа, дозволяє прослідкувати структуру онтології і появу нових відношень між її компонентами.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023

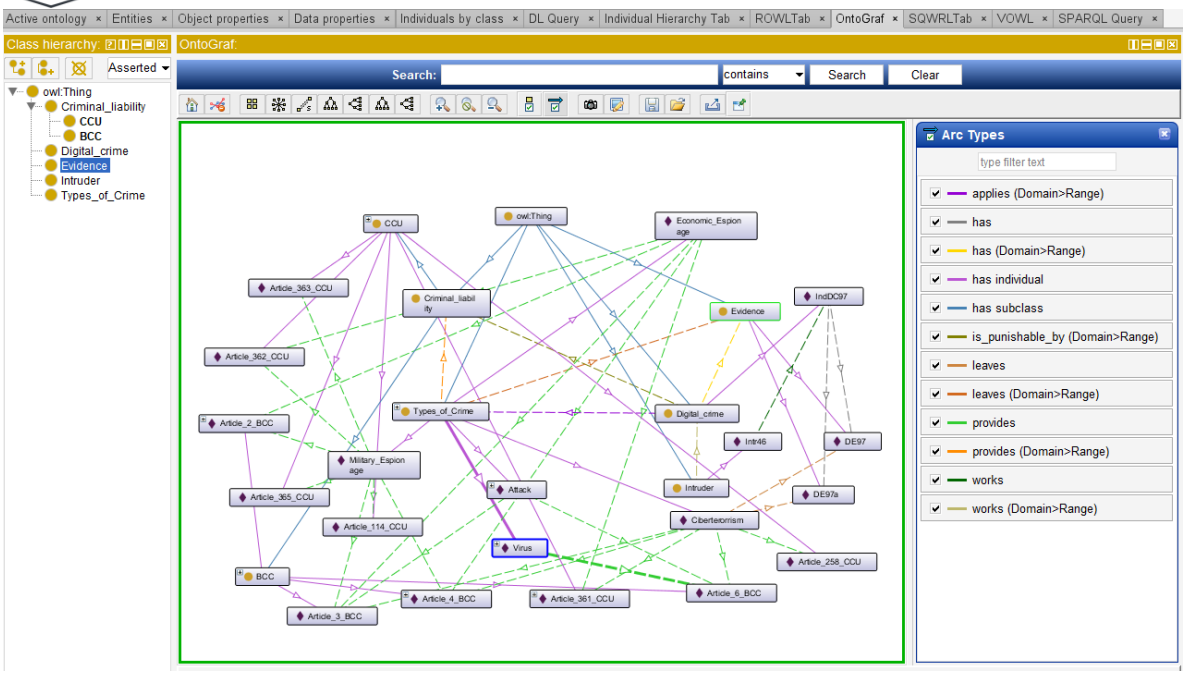


Рис. 7. Онтограф розробленої онтології

Перевірити онтологію на правильність, наявність логічних помилок в Protege, а також змоделювати її можна за рахунок SPARQL-запитів [12]. При проектуванні прикладної онтології передбачено можливість її розширення.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Запити до онтології є центральною складовою процесу роботи з онтологічними моделями. Вони дозволяють отримувати конкретні дані, взаємозв'язки та іншу інформацію зі структурованих знань, представлених у форматі RDF. Запити до онтології розкривають можливості аналізу, пошуку та отримання нових знань з областей, які підтримуються цією онтологією. Protégé 5.5 підтримує запити мовою SPARQL. Це є мова запитів та протокол для роботи з даними в форматі RDF.

Основними аспектами на використання SPARQL-запитів є можливість: отримувати результат запиту у зручному форматі на основі складних запитів для пошуку інформації за різними умовами, взаємозв’язками між даними; проводити арифметичних підрахунків і працювати зі статистичним аналізом; застосовувати основні види реляційних операцій при роботі з семантичними даними; об’єднувати дані з різних джерел – інших онтологій та семантичних баз даних; для уникнення і виправлення можливих помилок і невідповідностей перевіряти консистентність та валідність даних.

Перед тим як переходити безпосередньо до запитів, спочатку необхідно сформулювати префікси до онтології:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
```

ISSN 2663 - 4023

```
PREFIX onto:
<http://www.semanticweb.org/lidiia/ontologies/2023/6/untitled-ontology-
16#>
```

Запит 1. Отримати типи злочинів та віднесені до них статті кримінального відповідальності. Мовою SPARQL цей запит перепишеться: вивести екземпляри класу Criminal_liability (instA) та підкласи (CCU та BCC – subcl), до яких вони належать, та пов'язані залежністю provides з екземплярами класу Types_of_Crime (instB). Результат упорядкувати за типами злочину.

```
SELECT ?instB ?subcl ?instA
   WHERE {
          ?instA rdf:type ?subcl.
          ?subcl rdfs:subClassOf* onto:Criminal_liability.
           ?instB rdf:type onto:Types_of_Crime.
          ?instB onto:provides ?instA
}
ORDER BY ?instB
```

Результат запиту 1 зображений на рис. 7, на якому можна побачити, що в онтології з типом злочину Фішинг пов'язані зв'язком provides два екземпляри класу кримінальної відповідальності – один з підкласу ККУ і один – з Будапештської конвенції про кіберзлочинність.

instB	subcl	instA
Attack	BCC	Article_3_BCC
Attack	BCC	Article_5_BCC
Attack	CCU	Article_361_CCU
Attack	BCC	Article_4_BCC
Attack	BCC	Article_2_BCC
Attack	BCC	Article_6_BCC
Child_pornography	CCU	Article_301_CCU
Child_pornography	BCC	Article_9_BCC
Ciberterorrism	CCU	Article_258_CCU
Ciberterorrism	CCU	Article_361_CCU
Ciberterorrism	BCC	Article_4_BCC
Ciberterorrism	BCC	Article_3_BCC
Ciberterorrism	BCC	Article_6_BCC
Data_tampering	CCU	Article_366_CCU
Data_tampering	BCC	Article_7_BCC
Economic_Espionage	BCC	Article_4_BCC
Economic_Espionage	CCU	Article_362_CCU
Economic_Espionage	BCC	Article_2_BCC

Execute

instB	subcl	instA
Economic_Espionage	CCU	Article_361_CCU
Economic_Espionage	BCC	Article_3_BCC
Military_Espionage	CCU	Article_363_CCU
Military_Espionage	BCC	Article_3_BCC
Military_Espionage	CCU	Article_365_CCU
Military_Espionage	BCC	Article_4_BCC
Military_Espionage	CCU	Article_362_CCU
Military_Espionage	CCU	Article_114_CCU
Military_Espionage	BCC	Article_2_BCC
Phishing	BCC	Article_8_BCC
Phishing	CCU	Article_361_CCU
Virus	BCC	Article_6_BCC
Virus	BCC	Article_4_BCC
Virus	CCU	Article_361_CCU
Virus	BCC	Article_2_BCC
CAIP	CCU	Article_364_CCU
CAIP	CCU	Article_231_CCU
CAIP	BCC	Article_10_BCC

Execute

Рис. 7. Результат запиту 1

Запит 2, 3. Отримати статті кримінальної відповідальності, в яких передбачається відповідальність за несанкціонований доступ. Аналогічний сформувати запит за статями ККУ. Мовою SPARQL цей запит перепишеться: вивести екземпляри класу Criminal_liability, підклас BCC – для запиту 2 або CCU – для запиту 3 (instA), які пов'язані з екземплярами класу Types_of_Crime (instB) зв'язком provides, що мають атрибут ComputerObject=UnauthorisedAccess. Результат упорядкувати за статтями.

```
SELECT ?instA ?instB
   WHERE {
```

ISSN 2663 - 4023

```
            ?instA rdf:type onto:BCC. # CCU
            ?instB onto:provides ?instA.
            ?instB onto:ComputerObject "UnauthorisedAccess"
}
ORDER BY ?instA
```

Результат запитів 2 та 3 зображений на рис. 8. Можна побачити, що до одного екземпляру статті ККУ чи Будапештської конвенції про кіберзлочинність може відноситися не тільки один тип злочинності.

Це лише деякі запити, які можна робити на розробленій онтології.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

На основі проведеного аналізу предметної області цифрової криміналістики було побудовано прикладну онтологію по роботі з інформаційними даними цифрового кримінального злочину, яка відіграє ключову роль при вирішенні проблем складності, недостатньої структурованості та неоднозначності даних, які супроводжують злочин.

При створені онтологічної моделі були враховані основні складові цифрового злочину, починаючи від мотиву злочинця і закінчуючи передбаченими варіантами кримінальної відповідальності. Розроблена онтологія являється структурованою, логічною, не має перехресних зв'язків, що доводиться результатами роботи резонера на визначеній кількості тестових екземплярів класу Кримінальний злочин та тестуванням онтології за допомогою різноманітних SPARQL-запитів.

instA	instB
Article_2_BCC	Economic_Espionage
Article_2_BCC	Attack
Article_2_BCC	Military_Espionage
Article_3_BCC	Military_Espionage
Article_3_BCC	Attack
Article_3_BCC	Ciberterorrism
Article_3_BCC	Economic_Espionage
Article_4_BCC	Economic_Espionage
Article_4_BCC	Ciberterorrism
Article_4_BCC	Attack
Article_4_BCC	Military_Espionage
Article_5_BCC	Attack
Article_6_BCC	Ciberterorrism
Article_6_BCC	Attack
Article_7_BCC	Data_tampering
Article_9_BCC	Child_pornography

Execute

а)

instA	instB
Article_114_CCU	Military_Espionage
Article_258_CCU	Ciberterorrism
Article_301_CCU	Child_pornography
Article_361_CCU	Ciberterorrism
Article_361_CCU	Economic_Espionage
Article_361_CCU	Attack
Article_362_CCU	Economic_Espionage
Article_362_CCU	Military_Espionage
Article_363_CCU	Military_Espionage
Article_365_CCU	Military_Espionage
Article_366_CCU	Data_tampering

Execute

б)

Рис. 8. Результати запиту: а – запит 2; б – запит 3

Запропонована онтологічна модель дозволяє ефективно використовувати концепції семантичного WEB та графових без знань для відображення нових знань і відношень, що є основою для автоматичного виведення логічних висновків. Також допоможе майбутнім фахівцям з кібербезпеки зрозуміти основні аспекти цифрової криміналістики.

В подальшому планується проводити дослідження щодо підвищення ефективності побудованої онтології, розширення її архітектури і наповнення, інтегрування з іншими

існуючими онтологіями суміжних предметних областей і дослідження можливостей використання штучного інтелекту для автоматизації процесу розробки та застосування онтологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Federal Bureau of Investigation. (2022). Internet Crime Report 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
2 Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2
3 Кримінальний кодекс України. https://zakon.rada.gov.ua/laws/show/2341-14
4 Brady, O., Overill, R., & Keppens, J. (2014). Addressing the increasing volume and variety of digital evidence using an ontology. In 2014 IEEE Joint Intelligence and Security Informatics Conference (pp. 176-183). IEEE. DOI: 10.1109/JISIC.2014.34
5 Kapi, H. M., & Вентер, X. C. (2014). Toward a general ontology for digital forensic disciplines. Journal of Forensic Sciences, 59(5), 1231-1241.
6 Ellison, D., Ikuesan, R. A., & Venter, H. S. (2019, November). Ontology for reactive techniques in digital forensics. In 2019 IEEE Conference on Application, Information and Network Security (AINS) (pp. 83-88). IEEE.
7 Palagin, A., & Petrenko, N. (2009). System-ontological analysis of the subject area, Control systems and machines, 4, 3-14.
8 Lutskaya, N., Vlasenko, L., Zaiets, N., & Shtepa, V. (2021). Ontological Aspects of Developing Robust Control Systems for Technological Objects. In ICO 2020: Intelligent Computing and Optimization (Vol. 1324, pp. 1252-1261). Advances in Intelligent Systems and Computing book series. DOI: 10.1007/978-3-030-68154-8_107
9 Власенко, Л. О., Савченко, Т. В., & Луцька, Н. М. (2021). Вибір ієрархії та онтології верхнього рівня для розробки інтелектуальних автоматизованих систем управління промисловим підприємством. Наукові праці Національного університету харчових технологій, 27(4), 16-27. http://sw.nuft.edu.ua/Archiv/2021/swnuft_27_4.pdf.pdf
10 Smith, B. (2003). Blackwell guide to the philosophy of computing and information: Chapter ontology. Blackwell, 39, 61-64.
11 Конвенція про кіберзлочинність, ухвалена Радою Європи 23 листопада 2001 р. https://zakon.rada.gov.ua/laws/show/994_575
12 Луцька, Н. М., Власенко, Л. О., & Пупена, О. М. (2021). Технічні аспекти інтеграції відкритих онтологічних баз знань із сучасними автоматизованими системами управління. Наукові праці Національного університету харчових технологій, 27(1), 8-21. http://dspace.nuft.edu.ua/jspui/handle/123456789/32860

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023

Lidiia Vlasenko
PhD, Associate Professor of the Department of Software Engineering and Cyber Security
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0002-2003-6313
vlasenko.lidia1@gmail.com

Nataliia Lutska
Dr. Sc. (Tech.), Professor of the Department of Automation and Computer Technologies of Control Systems
National University of Food Technologies, Kyiv, Ukraine
ORCID ID: 0000-0001-8593-0431
lutskanm2017@gmail.com

Tetiana Savchenko
PhD, Associate Professor of the Department of Software Engineering and Cyber Security
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0002-8884-5360
sv_t@ukr.net

Oleksandr Bohdanov
Dr. Sc. (Tech.), Professor
Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0009-0005-2605-6189
o.bohdanov@kubg.edu.ua

ONTOLOGICAL MODELING OF INFORMATION DATA OF DIGITAL CRIMINAL CRIME

Abstract. In the article, an ontological model of information data of a digital criminal offense is formed and researched. Ontological modeling made it possible to conceptualize knowledge and effectively overcome the problems of insufficient structure, ambiguity and inconsistency of data and knowledge in the field of digital forensics. On the basis of the conducted classification, five main classes (Digital Crime, Digital Traces, Types of Crimes, Criminal and Criminal Liability) were identified, which include multiple user and non-user instances, including relevant articles of the Criminal Code of Ukraine and international law. The user creates instances of three classes: Digital Crime, Digital Traces, and Criminal. They contain personal information about digital crime and are the main data of the user part of the ontological model as a knowledge base. The Crime Types and Criminal Liability classes are non-user and can only be modified by model support specialists. The ontology model is implemented in Protege in the OWL language, which is an informal standard for creating and sharing ontologies. Of the selected seven relationships between entities, only three are entered into the ontology by the user, the others are formed automatically based on the developed SWRL rules. Using the SPARQL query language, real-time information search, filtering, and analysis patterns are provided to help discover complex relationships between objects and generate new ontological knowledge. The results of the study highlight the importance of ontology modeling in the field of digital forensics and how SPARQL queries can be used to improve data processing, analysis and understanding of knowledge in this field.

Keywords: digital crime; applied ontology; digital forensics.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Federal Bureau of Investigation. (2022). Internet Crime Report 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
2 Pro zareyestrovani kryminalni pravoporushennya ta rezultati yikh dosudovoho rozsliduvannya [About Registered Criminal Offenses and the Results of Their Preliminary Investigation].

https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

3 Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine]. https://zakon.rada.gov.ua/laws/show/2341-14

4 Brady, O., Overill, R., & Keppens, J. (2014). Addressing the increasing volume and variety of digital evidence using an ontology. In 2014 IEEE Joint Intelligence and Security Informatics Conference (pp. 176-183). IEEE. DOI: 10.1109/JISIC.2014.34

5 Kapi, H. M., & Вентер, Х. С. (2014). Toward a general ontology for digital forensic disciplines. Journal of Forensic Sciences, 59(5), 1231-1241.

6 Ellison, D., Ikuesan, R. A., & Venter, H. S. (2019, November). Ontology for reactive techniques in digital forensics. In 2019 IEEE Conference on Application, Information and Network Security (AINS) (pp. 83-88). IEEE.

7 Palagin, A., & Petrenko, N. (2009). System-ontological analysis of the subject area, Control systems and machines, 4, 3-14.

8 Lutskaya, N., Vlasenko, L., Zaiets, N., & Shtepa, V. (2021). Ontological Aspects of Developing Robust Control Systems for Technological Objects. In ICO 2020: Intelligent Computing and Optimization (Vol. 1324, pp. 1252-1261). Advances in Intelligent Systems and Computing book series. DOI: 10.1007/978-3-030-68154-8_107

9 Vlasenko L. O., Savchenko T. V., & Lutska N. M. (2021). Vybir ierarkhii ta ontolohii verkhnoho rivnia dlia rozrobky intelektualnykh avtomatyzovanykh system upravlinnia promyslovym pidpryiemstvom [Selection of Hierarchy and Top-Level Ontology for the Development of Intelligent Automated Control Systems for Industrial Enterprises]. Naukovi pratsi Natsionalnoho universytetu kharchovykh tekhnolohii, 27(4), 16-27. http://sw.nuft.edu.ua/Archiv/2021/swnuft_27_4.pdf.pdf

10 Smith, B. (2003). Blackwell guide to the philosophy of computing and information: Chapter ontology. Blackwell, 39, 61-64.

11 Konventsiya pro kiberzlochynnist, uhvalena Radoyu Yevropy 23 lystopada 2001 r. [Convention on Cybercrime, adopted by the Council of Europe on November 23, 2001]. https://zakon.rada.gov.ua/laws/show/994_575

12 Lutska N. M., Vlasenko L. O., & Pupena O. M. (2021). Tekhnichni aspekty intehratsii vidkrytykh ontolohichnykh baz znan iz suchasnymy avtomatyzovanymy systemamy upravlinnia [Technical Aspects of Integrating Open Ontological Knowledge Bases with Modern Automated Management Systems]. Naukovi pratsi Natsionalnoho universytetu kharchovykh tekhnolohii, 27(1), 8-21. http://dspace.nuft.edu.ua/jspui/handle/123456789/32860