p-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2023. № 4
e-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2023. № 4

UDC 004.82:343.9

DEVELOPMENT OF APPLIED ONTOLOGY FOR THE ANALYSIS OF DIGITAL CRIMINAL CRIME

Vlasenko L. O. – PhD, Associate Professor of the Department of Software Engineering and Cyber Security, State University of Trade and Economics, Kyiv, Ukraine.

Lutska N. M. – Dr. Sc., Professor of the Department of Automation and Computer Technologies of Control Systems, National University of Food Technologies, Kyiv, Ukraine.

Zaiets N. A. – Dr. Sc., Professor of the Department of Department of Automation and Robotic Systems, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine.

Savchenko T. V. – PhD, Associate Professor of the Department of Software Engineering and Cyber Security, State University of Trade and Economics, Kyiv, Ukraine.

Rudenskiy A. A. – Senior lecturer of the Department of Automation and Robotic Systems, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine.

ABSTRACT

Context. A feature of the modern digital world is that crime is often committed thanks to the latest computer technologies, and the work of law enforcement agencies faces a number of complex challenges in the digital environment. The development of information technology and Internet communications creates new opportunities for criminals who use digital traces and evidence to commit crimes, which complicates the process of identifying and tracking them.

Objective. Development of an applied ontology for a system for analyzing a digital criminal offense, which will effectively analyze, process and interpret a large amount of digital data. It will help to cope with the complex task of processing digital data, and will also help automate the process of discovering new knowledge.

Methods. To build an ontological model as a means of reflecting knowledge about digital crime, information was collected on existing international and domestic classifications. The needs and requirements that must be satisfied by the developed ontology were also analyzed. The creation of an ontological model that reflects the basic concepts, relationships in the field of digital criminal offense was carried out in accordance with a recognized ontological analysis of a specialized subject area.

Results. An applied ontology contains the definition of entities, properties, classes, subclasses, etc., as well as the creation of semantic relationships between them. At the center of the semantics is the Digital Crime class, the problem area of which is complemented by the interrelated classes Intruder, Digital evidence, Types of Crime, and Criminal liability. Such characteristics as motive, type of crime, method of commission, classification signs of digital traces and types of crime, as well as other individual information were assigned to the attributes of the corresponding classes. An ontological model was implemented in OWL using the Protégé software tool. A feature of the implementation of the applied ontology was the creation of SWRL rules for automatically filling in additional links between a class instance. Manual and automatic verification of the ontology showed the integrity, consistency, a high degree of correctness and adequacy of the model. The bugs found were usually related to technical aspects and semantic inconsistencies, which were corrected during further development iterations.

Conclusions. The research confirmed the effectiveness of the developed applied ontology for the analysis of digital criminality, providing more accurate and faster results compared to traditional approaches.

KEYWORDS: ontology, digital forensic, digital crime, digital evidence.

ABBREVIATIONS

CCU is a Criminal Code of Ukraine;
CS is a Computer System;
DSS is Decision Support Subsystem.

NOMENCLATURE

O^{ao} is an extended Applied ontology;
C is a set of domain classes;
A is a set of attributes that describe class objects;
R is a set of relationships between concepts;
T is a set of standard attribute value types;
F is a set of restrictions for the values of concepts and attribute relations (rules and axioms);
D is a set of instances of classes;
R^a is the associative relation (Object Property);
R^h is the heredity relation “SubDataPropertyOf”;
R^{ca} is the relation class-data (Data Property);
R^{cd} is the relation class-individual “has individual”.

INTRODUCTION

With the advent of computer, microprocessor technology, the Internet, etc. A new sphere and new tools for committing crimes have appeared in the world – digital crimes. Modern digital crimes are so diverse that they are committed against both private individuals and government agencies. Their negative consequences for the lives of people, the functioning of organizations, governments are often quite strong. Until recently, such offenses were not regulated by law and therefore active work was carried out in this direction. Now most states of the world have in their criminal code a section dedicated to liability in the event of a certain type of digital offense. But the legal and policy aspects of responding to digital crime cannot be permanent and must constantly change and improve.

Experts note that in the past few years there has been an increase in the number of digital offenses. Digital criminals are learning, using new approaches and tech-

DOI 10.15588/1607-3274-2023-4-17

nologies, and therefore the methods of identifying and disclosing them are becoming more complicated. According to the official statistics of the Office of the Prosecutor General of Ukraine [1] (Fig. 1), the number of digital crimes in Ukraine in 2022 increased by almost 64% compared to 2019. As for the current 2023, the number of crimes committed in the first half of the year exceeds the number for the entire 2019. Therefore, it can be assumed that in 2023 the total number will be the highest over the past 5 years. This can be explained by several additional factors.

First of all, there was a significant intensification of cybercrimes in the framework of the Russian-Ukrainian war, such as unauthorized interference in the operation of information, electronic communication, information and communication systems, electronic communication networks, etc. The emergence, development and active implementation of artificial intelligence in various areas of human activity and life can become the next challenge for protection against digital crimes. That is why it is necessary to stimulate the development of modern tools that could help and facilitate the work of cyber police, information security specialists [2–4].

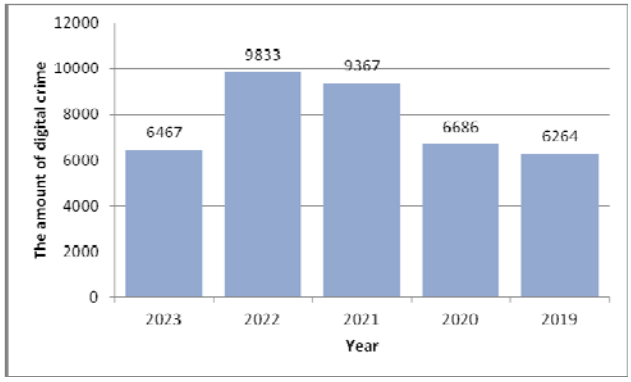


Figure 1 – Statistics of digital crimes in Ukraine for the period 2019–2023

The use of a generally acceptable classification scheme in this area would contribute to the improvement of legislation, the development of various quick countermeasures, deepening cooperation, etc. A number of problems in creating a subsystem for supporting the analysis of a digital criminal offense is due to the fact that the existing classifications of types and kinds of digital crimes, motives and threats to commit them, as a rule, are incomplete, fragmentary, use different terminology to define the same object, are developed to solve specific task. This makes them incompatible with each other.

Automating the process of digital crime analysis is very important, but complicated by working with unstructured forensic data, as it comes from different sources. Another problem is the lack of semantics for the concept of investigating a digital crime and determining punishment for it.

The authors propose a variant of the ontology, which includes, in addition to the type and kind of crime, accounting for digital traces, methods for committing a crime, and also determining the type of punishment in accordance with the current legislation of Ukraine. This work may be of interest to those involved in digital forensics, cybercrime, information security.

The object of study is the process of combining knowledge and data of digital forensics, cyber defense, Ukrainian legislation, aimed at identifying the commission of a digital crime and the type of criminal punishment for it.

The subject of study is an applied domain ontology for a digital crime analysis system.

The purpose of the work is to build an applied ontology to combine heterogeneous digital crime data obtained from different sources and systems, automate data processing, analyze large data sets and develop decision options for the decision support subsystem.

1 PROBLEM STATEMENT

The purpose of a decision support system (DSS) for digital crime analysis based on applied ontology is the ability to provide information to investigators, cyberpoliticians and other users about possible digital crimes and criminal liability options for committing them. This can significantly improve the organization of work on the analysis of criminal digital crime, reduce the time to make more informed decisions based on the array of available data. The developed subsystem can be used as an auxiliary tool in the work of professional workers and as a tool to increase the awareness of citizens.

The applied ontology is described by a tuple (1):

$$O^{ao}=< C, A, R, T, F, D >. \quad (1)$$

The ontology (1) for the analysis of criminal digital crime should include only those elements that will be used.

In particular, the set of relations (1) consists of relations: associative, subordinate, “is – a”, “class – data”, and is represented by a tuple (2):

$$R = < R^a, R^h, R^{ca}, R^{cd} >. \quad (2)$$

The applied ontology, which is part of the DSS, is used to solve the following tasks:

– structured representation of the subject area;

– introduction of a clear classification of terminology specific to the subject area;

– creation of a knowledge base for decision support for the industry;

– improvement of processing, search and filtering of heterogeneous information;

– identification of additional (implicit) links between concepts based on data semantics;

– analysis of the trend of changes taking place in the field of digital crime.

2 REVIEW OF THE LITERATURE

The creation of ontologies for digital crimes is overwhelmingly reduced to cybercrime ontologies. Ontologies of criminal offenses are also often created, where cyber-

DOI 10.15588/1607-3274-2023-4-17

crime is one of the subtypes. In particular, the classification of cybercrime may have a semi-formal approach to the development of a taxonomy of cybercrime [2]. The use of design science (DS) as a paradigm for solving organizational problems makes it possible to take into account the emergence and evaluation of innovative artifacts in the ontology of cybercrime classification [5].

The active development of artificial intelligence in recent years has brought the creation of ontological systems of digital forensics to a new technical and philosophical level. This type of ontologies [6] makes it possible to trace the entire chain of a digital crime, identify anomalies in the investigation process, and automate the processing of digital evidence traces [7]. The semantic ontology of digital evidence allows an investigator to quickly discover what artifacts may be available on a device before the time-consuming process of investigating digital devices begins, preventing the creation of data that has no practical value for the investigation.

A separate capacitive process in digital forensics is the analysis of the results of a forensic medical examination [8]. The use of semantic web technologies, in particular, ontologies, can greatly facilitate the work with them for the investigator when analyzing digital evidence [9] using RDF [10]. Modern ontologies support the specification of a web service. Creating a convenient and friendly graphical interface allows the investigator to receive a forensic examination report online based on requests, ready to submit it to the court [11].

Separately, it should be noted the development of ontologies in order to analyze the content received from Android smartphones [10]. The ontology may provide for the organization of evidence retrieved from mobile devices. Thus, a network of interconnected material is formed, in which it improves the process of data analysis and search for relevant evidence for the investigation [12].

In [13], an ontology of the subject area of cyberforensics for criminal investigation was built in accordance with the categories of cybercrime, laws, evidence, and information criminals. This ontology does not contain an application layer.

It should be noted that in the Ukrainian conceptual environment digital crime is a broader concept and cybercrime is its subspecies. While in the vast majority of foreign sources they are used by the authors as identical concepts. Also, most of the developed ontologies are of a general nature and do not take into account the specifics of the legislation of a particular country.

3 MATERIALS AND METHODS

According to Ukrainian legislation, criminal liability for digital crimes depends on several factors. Important among the factors are the type of digital offense committed, the extent of damage and harm caused, or the specific type of crime, motivation, as well as the personal characteristics of the person who committed this crime (for example, the circumstances of the commission, preliminary criminal actions and cooperation with law enforcement, special features, etc.). Thus, it is possible to identify a set of basic concepts that are connected by different types of connections (Fig. 2). Five concepts of which are non-empty classes: Digital Crime, Types of Crime, Criminal liability, Digital evidence, Intruder.

The developed applied ontology of the decision support subsystem for the analysis of a digital criminal offense is based on the processing and generalization of the analysis of research works of Ukrainian and foreign scientists [14–20].

Any crime starts with motive and intruder. Digital crime is no exception. The most common **Motives**, as a property of a certain crime, include the following: enrichment, terrorism, espionage, military and economic espionage, targeting national information infrastructure, revenge, hate (national origin, gender, race), greed. **Intruders**, in turn, were divided according to the type of crime they commit into: spy, terrorist, corporate raiders, professional criminals, hacker and others.

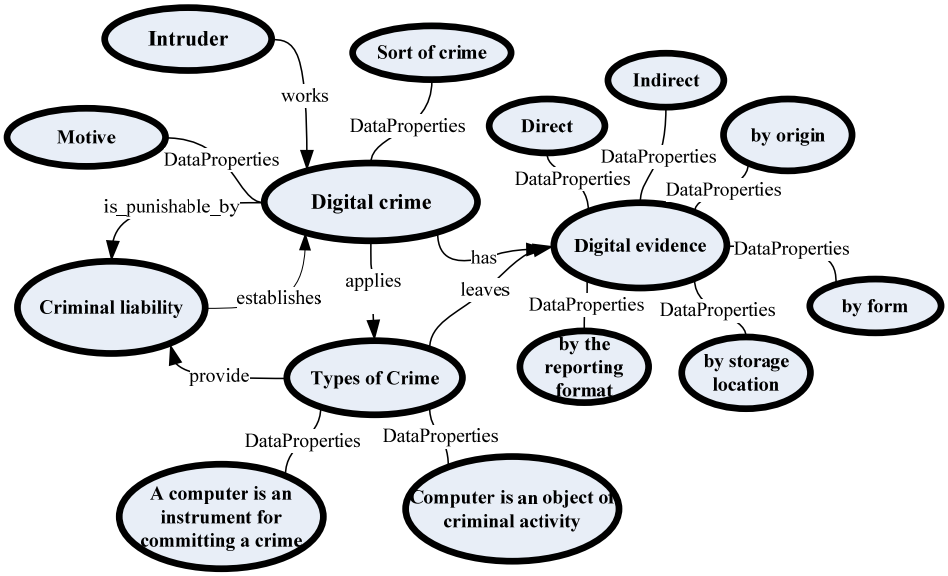


Figure 2 – Conceptual Model of Applied Ontology for Digital Crime Analysis System

DOI 10.15588/1607-3274-2023-4-17

Each individual digital crime belongs to a specific **Sort of Crimes**. There are various Sort of Crimes: Against Individuals – the most common are spamming and related threats, e-mail spoofing, cyber defamation, cyber stalking, cyber harassments, libel and false information, phishing; Against Property – internet time theft, credit card frauds, intellectual property crimes, identity theft, misuse of devices; Against Organizations – different types of attacks, computer-related offences, unauthorized accessing of computer, economic espionage, denial of service, Industrial espionage, computer contamination, e-mail bombing, copyright-related offences; Against Society – pornography, illegal gambling and online games, glorification of violence, hate speech, forgery, religious offence, racism, Web Jacking; Against Government – cyber terrorism, hacking, military espionage, accessing confidential information, cyber warfare (crimes are considered an attack on that national sovereignty).

In the world and in Ukraine, digital crimes have a certain typification. **Types of Crime** were divided into two groups for convenience: A computer is an instrument for committing a crime – Content violations, Unauthorized modification of data, software, Improper use of Communications; Computer is an object of criminal activity – unauthorised access, malicious code, interruption of services, Theft or misuse of services.

Each crime has **Digital evidence**, which are carriers of a certain set of information and provide an evidence base in identifying the offender, proving his guilt and issuing an appropriate sentence. The peculiarities of digital evidences are their heterogeneity, for the frequent short period of their existence, they can be forged or destroyed. Also, digital evidences can be located in various hardware and software, in particular, on a computer hard drive, flash drive, local network devices, websites, social networks, emails, etc. In order to take into account, the existing diversity as a basis for the Digital evidence class [14], the chosen classification was developed in (Fig. 2).

In Ukraine, **Criminal liability** for committing a digital crime is regulated by the following legal documents: the Constitution of Ukraine, the Criminal Code of Ukraine (CCU) [21], the laws of Ukraine: "On Information", "On the Protection of Information in Information and Telecommunication Systems", "On the Basics National Security" "On the Basic Principles of Ensuring Cybersecurity of Ukraine", "On Amendments to the Criminal Code of Ukraine to Improve the Efficiency of Combating Cybercrime in Martial Law". The article presents fragments of this class, containing separate articles corresponding to the crimes considered in the examples as a possible form of punishment (Fig. 3).

Thus, we get a set of classes:

$$C = \{\text{Digital\_Crime, Intruder, Digital\_evidence, Types\_of\_Crime, Criminal\_liability}\} \quad (3)$$

and a set of connections between the individuals of these classes:

$$R^a = \{\text{has, works, applies, is\_punishable\_by, establishes, leaves, provides}\} \quad (4)$$

Figure 3 shows an extended fragment of the conceptual model, which includes a part that describes the classification of crimes based on their motive with reference to the punishment provided for by the current legislation of Ukraine. The model also shows relationships between concepts such as Data Properties Rcd, Object Properties Ra, and class-individual Rcd, as well as the values of these attributes (set T).

Taking into account the peculiarities of the subject area, when creating the ontology, it was taken into account that some of the selected classes should be defined and the filling process is provided by a group of specialists. It includes developers, industry experts, future users (selectively if necessary). In the future, users cannot independently make changes and additions to the classes: Types of Crime and Criminal liability. For instances of the Digital Crime, Intruder and Evidence classes, individual positions are filled in by users. in the Table. 1 shows the corresponding characteristics of the classes.

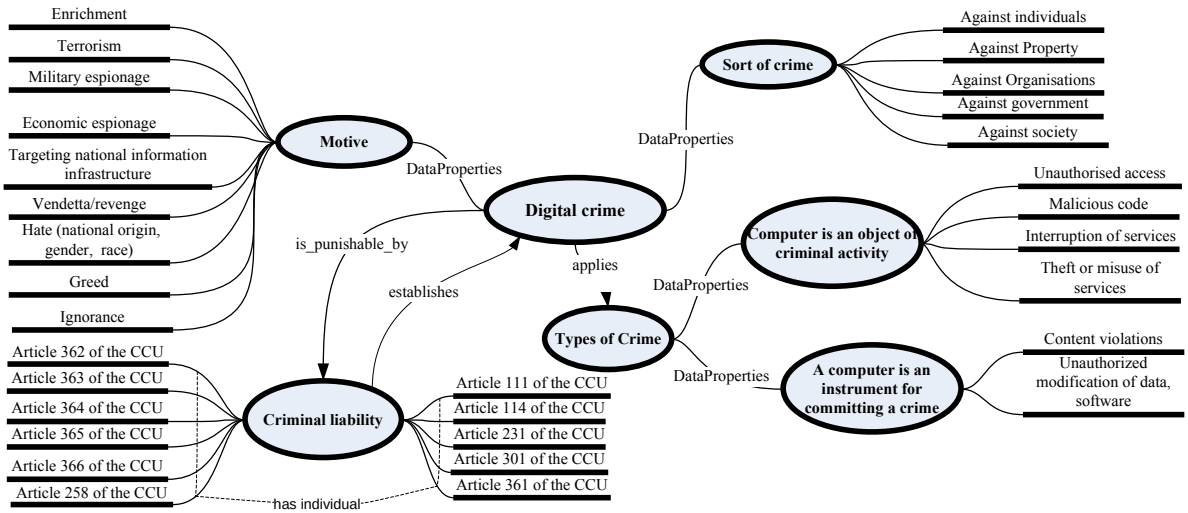


Figure 3 – Extended fragment of the conceptual model with attributes for the Digital Crime and Type of Crime classes and instances of the Criminal liability class

DOI 10.15588/1607-3274-2023-4-

Table 1 – Class characteristics

Class	Individuals	User changes	Data Property	Object Property
Digital Crime	+	+	+	+
Criminal liability	+	–	–	–
Evidence	+	+	+	+
Intruder	+	+	+	+
Types of Crime	+	–	+	+

In order to conduct a deeper and more automated data analysis, a formalized expression of logical conditions and relationships based on SWRL rules was used. Their advantage is the ability to define complex logical connections and relationships between objects, finding new knowledge based on existing ones and establishing new relationships between elements, improving the quality of search in the ontology. Also, SWRL rules can be used to passively check the consistency of data in the ontology, identify contradictions and inconsistencies.

The developed rules are divided into the corresponding categories of Types of Crime for structure. The ontology contains 206 rules developed by SWRL. Table 2 shows some of them. The rules presented relate to the section on cyberterrorism. Thus, new links are formed between user and non-user class instances: applies, is_punishable_by, establishes, leaves.

The developed system is designed in such a way that, if necessary, it can be expanded and supplemented with additional concepts, attributes, relationships, etc.

Table 2 – Example of rules developed for applied ontology (*F*)

Rule Number	SWRL Rule	Rule category
KT1	Evidence(?x) ^byForm(?x,?y) –> leaves(Ciberterorrism,?x)	Ciberterorrism
KT2	Evidence(?x) ^ UnauthorizedAccessDevices(?x,?y) –> leaves(Ciberterorrism,?x)	Ciberterorrism
KT3	Evidence(?x) ^ byOrigin(?x, "InformationGeneratedByCSBasedOnDataInput") –> leaves(Ciberterorrism,?x)	Ciberterorrism
KT4	Evidence(?x) ^ ByTheReportingFormat(?x, "HumanReadableInformation") –> leaves(Ciberterorrism,?x)	Ciberterorrism
KT5	Evidence(?x) ^ ByStorageLocation (?x, "InformationStoredInCS") –> leaves(Ciberterorrism,?x)	Ciberterorrism
KT6	Digital_crime(?x) ^Motive(?x, "Terrorism") ^ Sort_of_Crime(?x, "AgainstSociety") ^ has(?x,?y) ^ leaves (Ciberterorrism,?y) -> applies(?x, Ciberterorrism)	Ciberterorrism
KT7	Digital_crime(?x) ^Motive(?x, "Terrorism") ^ Sort_of_Crime(?x, "AgainstGoverment") ^ has(?x,?y) ^ leaves(Ciberterorrism,?y) -> applies(?x, Ciberterorrism)	Ciberterorrism
KT8	Digital_crime(?x) ^Motive(?x, "Enrichment") ^ Sort_of_Crime(?x, "AgainstSociety") ^ has(?x,?y) ^ leaves (Ciberterorrism,?y) -> applies(?x, Ciberterorrism)	Ciberterorrism
KT9	Digital_crime(?x) ^Motive(?x, "Enrichment") ^ Sort_of_Crime(?x, "AgainstGoverment") ^ has(?x,?y) ^ leaves (Ciberterorrism,?y) -> applies(?x, Ciberterorrism)	Ciberterorrism
KT10	Intruder(?x) ^ byType(?x, "Terrorist") ^ works(?x,?y) ^ applies(?y, Ciberterorrism) -> is_punishable_by(?y, Article_258_CCU)	Ciberterorrism
KT11	Intruder(?x) ^ byType(?x, "Terrorist") ^ works(?x,?y) ^ applies(?y, Ciberterorrism) -> is_punishable_by(?y Article_361_CCU)	Ciberterorrism
KT12	Intruder(?x) ^ byType(?x, "Hackers") ^ works(?x,?y) ^ applies(?y, Ciberterorrism) -> is_punishable_by(?y, Article_258_CCU)	Ciberterorrism
KT13	Intruder(?x) ^ byType(?x, "Hackers") ^ works(?x,?y) ^ applies(?y, Ciberterorrism) -> is_punishable_by(?y, Article_361_CCU)	Ciberterorrism

4 EXPERIMENTS

To implement the developed ontological model, the semantic language OWL and the free Protege software were chosen. These tools were favored due to OWL's powerful expressiveness, its versatility and integration with other tools (such as search and visualization), its large developer community, and ease of development and deployment.

Figure 4 shows the VOWL-graph of the developed ontology. You can see the set of standard types of attribute values *T* from (1), as well as the Data Property hierarchy introduced for convenience – the set R^h. Figure 5 shows the set of Object Property Ra associations and an example of the constraints imposed on the is_punishable_by relation.

Figure 6, a shows a fragment of individuals of the Type of Crime class and their attributes. Note that these classes are filled with knowledge engineers. In Figure 6, b is presented respectively in the Data Property.

Figure 7 shows an example of the SWRL rules that were coded in the SWRL Protégé5.0 tab and the results and their explanations obtained after putting these rules into the ontology. In particular, in the Edit window that opens, you can see a rule that forms a new is_punishable_by relationship between objects of the Digital Crime and Criminal liability class through works applies custom relationships. Note that the last link is also formed based on the SWRL rules.

DOI 10.15588/1607-3274-2023-4-

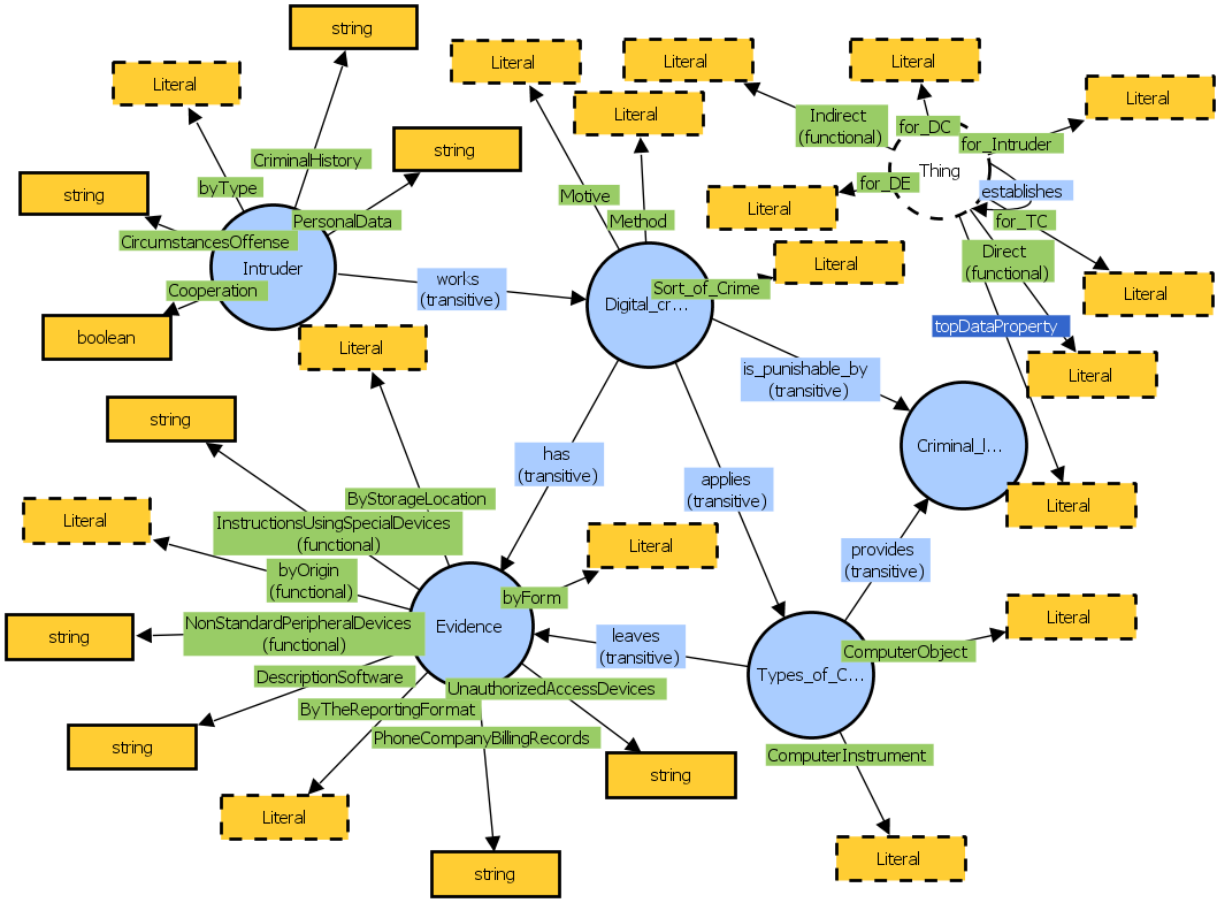


Figure 4 – VOWL-graph of the developed ontology

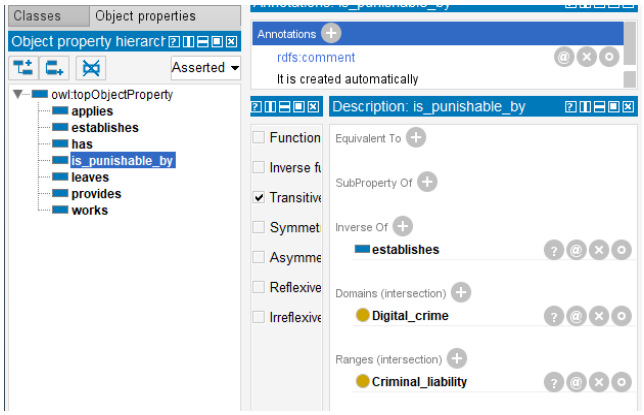


Figure 5 – Object Property

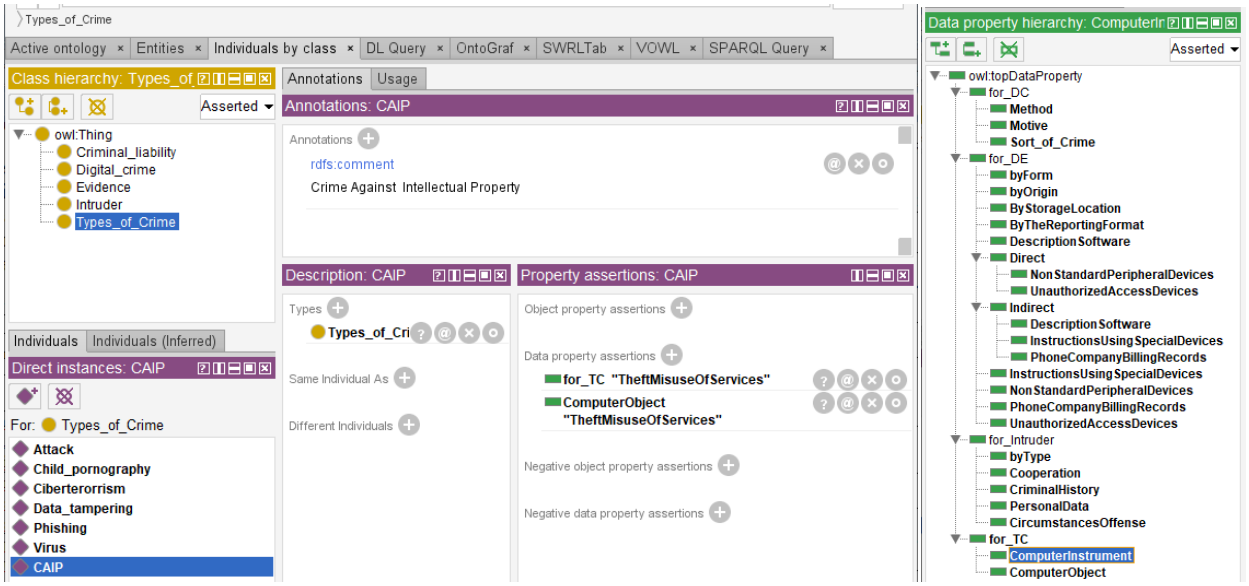
5 RESULTS

To check the correctness of the developed ontology, Reasoner machines were used. The purpose of Reasoner is to classify, reproduce the class hierarchy embedded in the ontological model, work with instances, determine their belonging to classes in accordance with logical rules and axioms, check consistency, and show inconsistencies. Reasoner is based on the concept of Open World Reasoning.

Protégé 5.5.0 has the ability to work with three Reasoners: Fact++, HermiT 1.4.3.456 and Pellet. The main difference between them is the algorithms for building links, data formats and the ontological modeling language that Reasoner supports.

To check the correctness of the ontology, a series of experiments were carried out. Each series of experiments corresponded to a certain type of digital crime. Individuals were created for the corresponding classes, for each of them a unique set of attributes was set.

DOI 10.15588/1607-3274-2023-4-17



a) b)

Figure 6 – Hierarchies of classes and individuals of the class Type of Crime (a) and Data Property (b) in Protégé

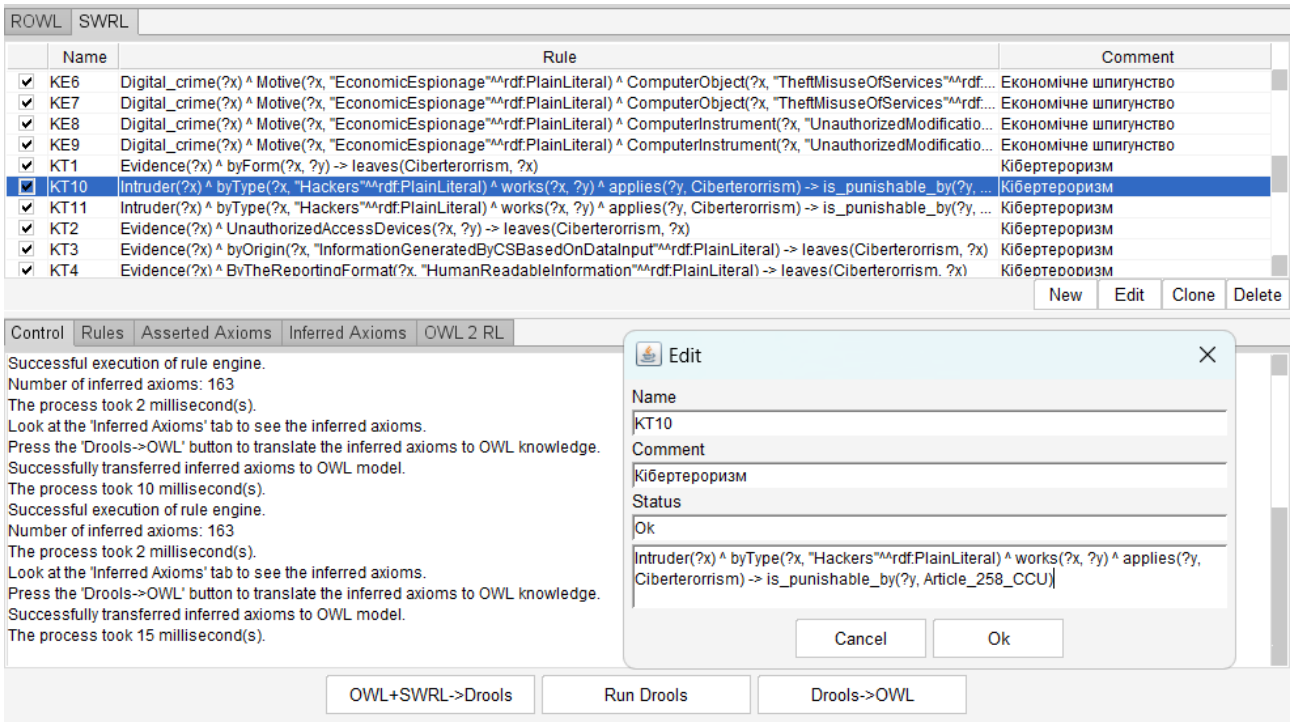


Figure 7 – Example SWRL rules encoded into an ontology

Figure 8 shows the result of Reasoner's work on a series of experiments on the digital crime of cyberterrorism for an individual IndDC97 of the Digital Crime class. For this digital crime, the corresponding instances of the Data Properties set were set, digital traces were created – individuals DE97, DE97a. The digital crime IndDC97 is related to the Types of Crime of the Ciberterorrism individual through logical rules (Table 2) and the relation applies. Criminal liability is also defined in accordance with Articles 361 and 258 of the Criminal Code of Ukraine by the connection is punishable by.

Figure 9 illustrates the result of the Reasoner check for digital crime IndDC97. For the Ciberterorrism individual of the Types of Crime class, its digital traces DE97, DE97a were matched by logical rules and the relation leaves.

The digital crime ontograph IndDC97 demonstrates connections between class individuals (Fig. 10), which are formed automatically based on the introduced SWRL rules (Table 2). The new connections can be seen on the left in Figure 10.

DOI 10.15588/1607-3274-2023-4-17

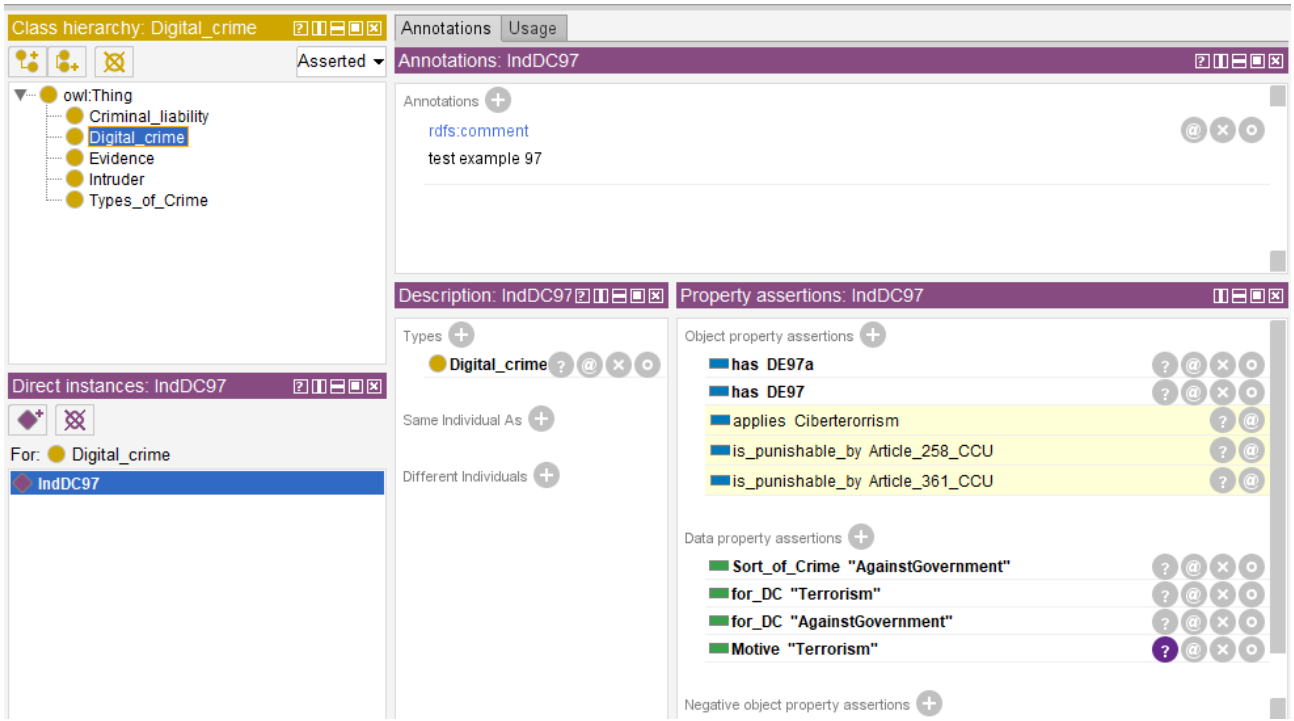


Figure 8 – Reasoner example for the Ciberterorrism individual of the Types of Crime class

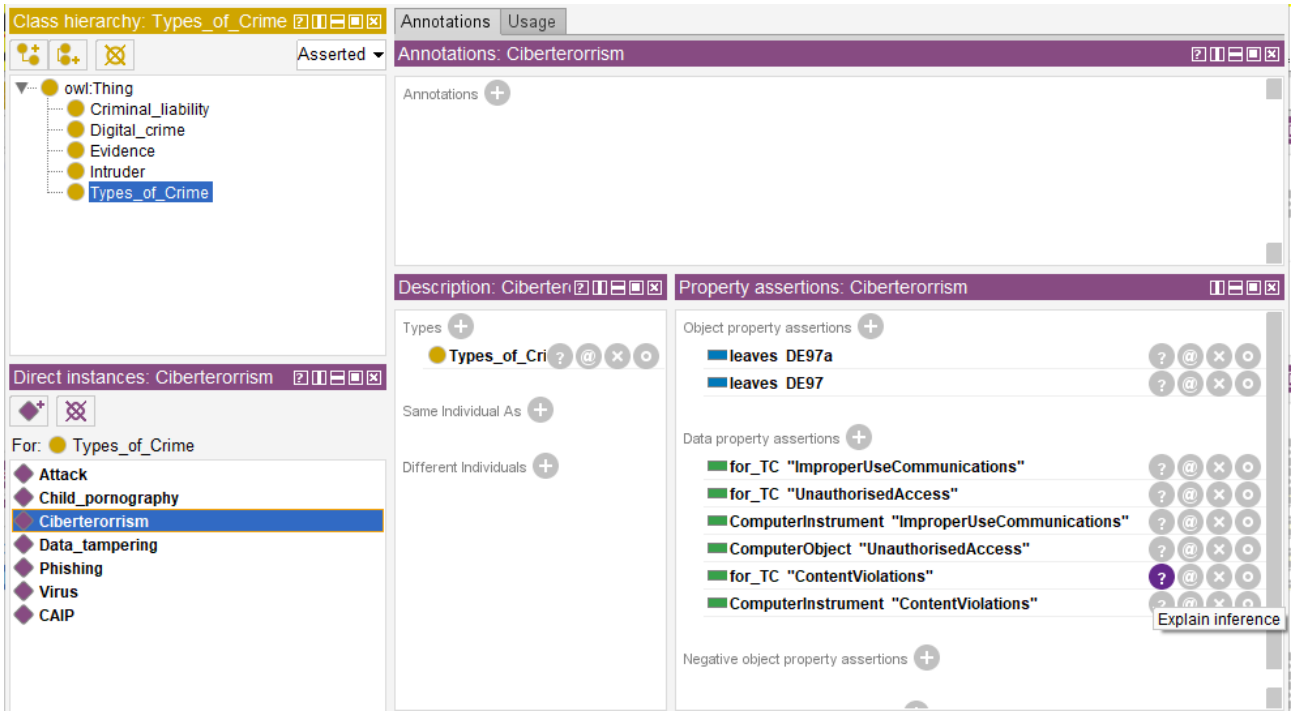


Figure 9 – Reasoner example for the Ciberterorrism individual of the Types of Crime class

6 DISCUSSION

Validation of an applied ontology depends on specific needs and requirements. For small ontologies, manual verification may be sufficient. For large ontologies, semi-automated or automatic approaches are usually produced – in particular, testing. The developed ontology was checked manually and automatically.

98 test instances of the Digital Crime class and the corresponding objects of the Intruder and Evidence classes were developed. Syntax errors were found during a manual check. No semantic errors were found.

The developed ontology was tested using the online resource Ontology testing Themis [22]. The test results (Table 3) showed that the developed ontology was successfully tested, is adequate, accurate, valid and does not contain contradictions.

DOI 10.15588/1607-3274-2023-4-17

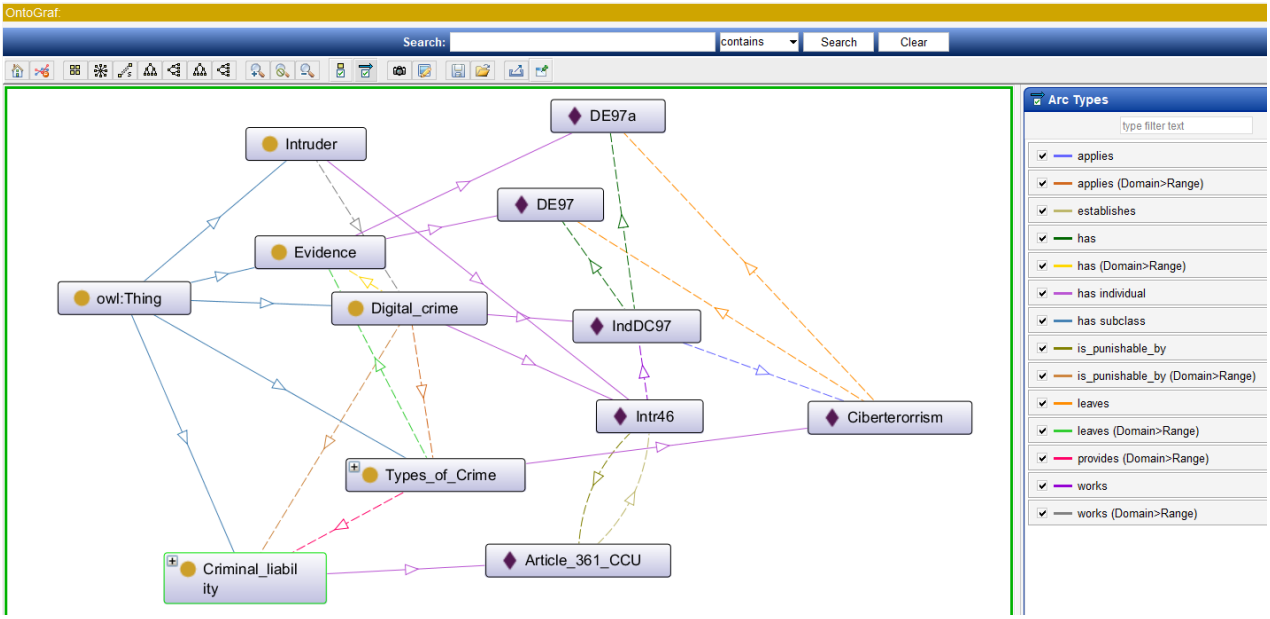


Figure 10 – Ontograph for Digital Crime IndDC97

Table 3 – Test results by Ontology testing Themis

Metric	Result
Percentage of covered requirement	97.83%
Percentage of requirements with terms that are undefined in the ontology	2.17%
Percentage of requirements that lead to conflict	0
Percentage of tested terms	83.06%

The practical value of an ontology lies in its use as a basis for a decision support system. Due to the use of the OWL language, such an application can be WEB-oriented [23]. At the same time, in addition to the semantic database and knowledge, the user can form different queries to the ontology. For example, in Fig. Figure 11 shows the DL-query of the following template: "Find instances of the Evidence class that have feedback from has with an instance of the Digital crime class, which in turn has feedback from works with an instance of the Intruder class, and also has a corresponding byForm attribute value".

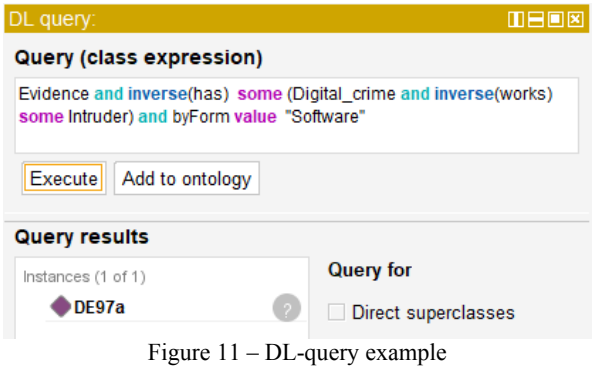


Figure 11 – DL-query example

The proposed ontological model does not accompany the process of solving a crime, since such models already exist in sufficient numbers. It aims to collect and analyze already solved crimes and obtain information on automatically classified crimes, as well as to analyze their common features, patterns and trends.

CONCLUSIONS

The proposed model can be used to improve the analysis, organization and interpretation of data related to digital criminal activity. The developed ontology helps to understand and classify crimes, make connections between different aspects of digital crimes and promote effective interaction between users.

The scientific novelty. The paper presents a modern approach to modeling digital crime. The developed ontology allows obtaining new knowledge, approaches or tools in the field of digital crime analysis, improves cooperation between various organizations, exchanges information and jointly analyzes data.

The practical significance. The developed ontology can be used for intelligent data analysis of digital crimes, collecting this data, classifying, grouping, combining digital traces, types of crimes and criminals, as well as determining the possible punishment. The ontology does not contain closed and confidential information, therefore it is publicly available. The use of the OWL language makes it compatible and integrated with the vast majority of modern applications. It can also be used in the educational process in the relevant specialties, in particular 125 "Cybersecurity and Information Protection".

Prospects for further research. It is planned to expand the developed ontology with additional classes and attributes, in particular, classes that will contain data about the injured party and the result of the harm caused to them.

REFERENCES

1. Pro zareyestrovani kryminalni pravoporushennya ta rezultaty yikh dosudovoho rozsliduvannya (2023) In: ofis holovnoho prokurora. https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2. Accessed 20 Aug 2023
2. Barn R., Barn B. An ontological representation of a taxonomy for cybercrime, *Twenty-Fourth European Conference on Information Systems (ECIS)*. İstanbul, Turkey, 2016. Access mode: https://core.ac.uk/download/pdf/42490758.pdf

DOI 10.15588/1607-3274-2023-4-17

3. Vlasenko L., Lutska N., Zaiets N., Korobiichuk I., Hrybkov S. Core Ontology for Describing Production Equipment According to Intelligent Production, *Applied System Innovation*, 2022, Vol. 5, Issue 5, pp. 98–111. DOI: 10.3390/asi5050098
4. Vlasenko L. O., Lutska N. M., Zaiets N. A., Shyshak A. V., Savchuk O. V. Domain ontology development for condition monitoring system of industrial control equipment and devices, *Radio Electronics, Computer Science, Control*, 2022, Vol. 1, pp. 157–166. DOI: 10.15588/1607-3274-2022-1-16
5. Donalds C., Osei-Bryson K. M. Toward a cybercrime classification ontology: A knowledge-based approach, *Computers in Human Behavior*, 2019, Vol. 92, pp. 403–418. DOI: 10.1016/j.chb.2018.11.039
6. Sikos L. F. AI in digital forensics: Ontology engineering for cybercrime investigations. *Wiley Interdisciplinary Reviews: Forensic Science*, 2020, Vol. 3, Issue 3, pp. 1–11. DOI: 10.1002/wfs2.1394
7. Karanasios S., Thakker D., Lau L., Allen D., Dimitrova V., Norman A. Making sense of digital traces: An activity theory driven ontological approach, *Journal of the American Society for Information Science and Technology*, 2013, Vol. 64, Issue 12, pp. 2452–2467. DOI: 10.1002/asi.22935
8. Brady O., Overill R., Keppens J. Addressing the increasing volume and variety of digital evidence using an ontology. *2014 IEEE joint intelligence and security informatics conference*. IEEE, 2014. pp. 176–183. DOI: 10.1109/JISIC.2014.34
9. Michel M. C., Carvalho M., Crawford H., Esterline A. C. Cyber identity: Salient trait ontology and computational framework to aid in solving cybercrime, *2018 17th IEEE International Conference on Trust, Security and Privacy In Computing and Communications/12th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE)*, IEEE, 2018, pp. 1242–1249. DOI: 10.1109/TrustCom/BigDataSE.2018.00171
10. Alzaabi M., Jones A., Martin T. A. An Ontology-Based Forensic Analysis Tool. *Proceedings of the 2013 Annual ADFSL Conference on Digital Forensics, Security and Law*, 2013, pp. 121–136. Access mode: https://commons.erau.edu/adfsl/2013/wednesday/5
11. Akremi A., Sriti M.-F., Sallay H., Rouached M., Ontology-based smart sound digital forensics analysis for web services, *International Journal of Web Services Research*, 2019, Vol. 16, № 1, 70–92. DOI: 10.4018/IJWSR.2019010104
12. Alzaabi M., Ontology-Based Forensic Analysis of Mobile Devices, *Proceedings of the 20th IEEE International Conference on Electronics, Circuits and Systems*, IEEE, 2013, pp. 64–68. DOI: 10.1109/ICECS.2013.6815346
13. Park H., Cho S., Kwon H. Cyber Forensics Ontology for Cyber Criminal Investigation. *Forensics in Telecommunications, Information and Multimedia, LNICST*, 2009, Vol. 8, pp. 160–165. DOI: 10.1007/978-3-642-02312-5_18
14. Naidyon Ya. Ponyattya ta klasyfikatsiya virtualnykh slidiv kiberzlochyniv, *Pidpryyemnytstvo, hospodarstvo i pravo*, 2019, 5, pp. 304–307. DOI: 10.32849/2663-5313/2019.5.56
15. Lysenko S. M., et al. Rezilientnist kompiuternykh system v umovakh kiberzahroz: Ontolohiia ta taksonomiia, Radioelektronni i kompiuterni systemy, 2020, No. 1, pp. 17–28. DOI: 10.32620/reks.2020.1.02
16. Maskun M., Achmad A., Naswar N., Assidiq H., Syafira A., Napang M., Hendrapati M. Qualifying Cyber Crime as a Crime of Aggression in International Law, *Cybercrime under International Law*, 2020, – Vol. 13, № 2, pp. 397–418. DOI: 10.14330/jeail.2020.13.2.08
17. Uma M., Padmavathi G. A survey on various cyber attacks and their classification, *Int. J. Netw. Secur.*, 2013, Vol. 15, №5, pp. 390–396. DOI:10.6633/IJNS.201309.15(5).09
18. Chandra A., Snowe M. J. A taxonomy of cybercrime: Theory and design, *International Journal of Accounting Information Systems*, 2020, Vol. 38, pp. 100467. DOI: 10.1016/j.accinf.2020.100467
19. Harmandeep S. B., Kumar G. Cybercrimes: A proposed taxonomy and challenges, *Journal of Computer Networks and Communications*, 2018, Vol. 11. DOI: 10.1155/2018/1798659
20. Goni O. Cyber Crime and Its Classification, *Int. J. of Electronics Engineering and Applications*, 2022, Vol. 10, № 1, pp. 1–17, DOI: 10.30696/IJEEA.X.I.2021.01-17In
21. Kryminalnyi kodeks Ukrainy (2001) In: Verkhovna Rada Ukrainy. Zakonodavstvo Ukrainy. https://zakon.rada.gov.ua/laws/show/2341-14. Accessed 20 Aug 2023
22. Themis. Ontology testing. https://themis.linkeddata.es/index.html. Accessed 20 Aug 2023
23. Lutska N., Vlasenko L., Ladanyuk A., Zaiets N., Korobiichuk I. Ontological Support System of Managerial Decision-Making of Production Tasks for a Food Enterprise, *Machinery & Energetics*, 2022, Vol. 13, № 3, pp. 53–61. DOI: 10.31548/machenergy.13(3).2022.53-61

Received 30.08.2023.
Accepted 15.11.2023.

УДК 004.82:343.9

РОЗРОБКА ПРИКЛАДНОЇ ОНТОЛОГІЇ ДЛЯ АНАЛІЗУ ЦИФРОВОГО КРИМІНАЛЬНОГО ЗЛОЧИНУ

Власенко Л. О. – канд. техн. наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет, Київ, Україна.

Луцька Н. М. – д-р техн. наук, професор, професор кафедри автоматизації та комп'ютерних технологій систем управління, Національний університет харчових технологій, Київ, Україна.

Заєць Н. А. – д-р техн. наук, професор, професор кафедри автоматики и робототехнічних систем ім. академіка І. І. Мартиненка, Національний університет біоресурсів и природокористування України, Київ, Україна.

Савченко Т. В. – канд. техн. наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет, Київ, Україна.

Руденський А. А. – ст. викл кафедри автоматики и робототехнічних систем ім. академіка І. І. Мартиненка, Національний університет біоресурсів и природокористування України, Київ, Україна.

АНОТАЦІЯ

Актуальність. Особливістю сучасного цифрового світу є те, що злочинність вже нерідко вчиняється завдяки новітнім комп'ютерним технологіям, а робота правоохоронних органів стикається з низкою складних викликів у цифровому середовищі.. Розвиток інформаційних технологій та інтернет-комунікацій створює нові можливості для злочинців, які використовують цифрові сліди та докази для здійснення злочинів, що ускладнює процес їх виявлення та відслідковування.

Мета. Розробка прикладної онтології для системи аналізу цифрового кримінального злочину, яка дозволить ефективно аналізувати, обробляти та інтерпретувати велику кількість цифрових даних. Вона допоможе впоратися зі складним завданням обробки цифрових даних, а також сприятиме автоматизації процесу виявлення нових знань.

DOI 10.15588/1607-3274-2023-4-17

Метод. Для побудови онтологічної моделі як засобу відображення знань про цифровий злочин було зібрано інформацію про існуючі міжнародну та вітчизняну класифікації, а також проаналізовані потреби та вимоги, які мають бути задоволені розробленою онтологією. Створення онтологічної моделі, яка відображає основні поняття, взаємозв'язки у сфері цифрового кримінального злочину, було здійснено відповідно з визнаним онтологічним аналізом спеціалізованої предметної області.

Результати. Прикладна онтологія містить означення сутностей, властивостей, класів, підкласів тощо, а також створення семантичних відношень між ними. В центрі семантики знаходиться клас цифровий злочин (Digital Crime), проблемну область якого доповнюють взаємозв'язані класи злочинець (Intruder), цифровий слід (Digital evidence), тип злочину (Types of Crime) та кримінальна відповідальність (Criminal liability). Такі характеристики, як мотив, вид злочину, метод скоєння, класифікаційні ознаки цифрових слідів та типів злочину, а також інша індивідуальна інформація були віднесені до атрибутів відповідних класів. Реалізована онтологічна модель на мові OWL програмним засобом Protégé. Особливістю реалізації прикладної онтології було створення SWRL-правил для автоматичного заповнення додаткових зв'язків між екземплярами класу. Ручна та автоматична перевірка онтології показала цілісність, узгодженість, високу ступінь коректності та адекватності моделі. Виявлені помилки були, як правило, пов'язані з технічними аспектами та семантичними неузгодженостями, які були виправлені під час подальших ітерацій розробки.

Висновки. Дослідження підтвердило ефективність розробленої прикладної онтології для аналізу цифрового кримінального злочину, забезпечуючи більш точні та швидкі результати порівняно з традиційними підходами.

КЛЮЧОВІ СЛОВА: онтологія, цифрова криміналістика, цифровий злочин, цифрові сліди.

ЛІТЕРАТУРА

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування 2023. Офіс генерального прокурора. – Режим доступу: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2
2. Barn R. An ontological representation of a taxonomy for cybercrime / R. Barn, B. Barn // Twenty-Fourth European Conference on Information Systems (ECIS): proceedings. – İstanbul, Turkey, 2016. – Access mode: https://core.ac.uk/download/pdf/42490758.pdf
3. Core Ontology for Describing Production Equipment According to Intelligent Production / [L. Vlasenko, N. Lutska, N. Zaiets et al.] // Applied System Innovation. – 2022. – Vol. 5, Issue 5. – P. 98–111. DOI: 10.3390/asi5050098
4. Domain ontology development for condition monitoring system of industrial control equipment and devices / [L. O. Vlasenko, N. M. Lutska, N. A. Zaiets et al.] // Radio Electronics, Computer Science, Control. – 2022. – Vol. 1. – P. 157–166. DOI: 10.15588/1607-3274-2022-1-16
5. Donalds C. Toward a cybercrime classification ontology: A knowledge-based approach / C. Donalds, K. M. Osei-Bryson // Computers in Human Behavior. – 2019. – Vol. 92. – P. 403–418. DOI: 10.1016/j.chb.2018.11.039
6. Sikos L. F. AI in digital forensics: Ontology engineering for cybercrime investigations / L. F. Sikos // Wiley Interdisciplinary Reviews: Forensic Science. 2020. – Vol. 3, Issue 3. – P. 1–11. DOI: 10.1002/wfs2.1394
7. Making sense of digital traces: An activity theory driven ontological approach / [S. Karanasios, D. Thakker, L. Lau et al.] // Journal of the American Society for Information Science and Technology. – 2013. – Vol. 64, Issue 12. – P. 2452–2467. DOI: 10.1002/asi.22935
8. Brady O. Addressing the increasing volume and variety of digital evidence using an ontology / O. Brady, R. Overill, J. Keppens // 2014 IEEE joint intelligence and security informatics conference. IEEE, 2014. – P. 176–183. DOI: 10.1109/JISIC.2014.34
9. Cyber identity: Salient trait ontology and computational framework to aid in solving cybercrime / [M. C. Michel, M. Carvalho, H. Crawford et al.] // 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. 12th IEEE International Conference on Big Data Science and Engineering. IEEE, 2018. – P. 1242–1249. DOI: 10.1109/TrustCom/BigDataSE.2018.00171
10. Alzaabi M. An Ontology-Based Forensic Analysis Tool / M. Alzaabi, A. Jones, T. A. Martin // Proceedings of the 2013 Annual ADFSL Conference on Digital Forensics, Security and Law, 2013. – P. 121–136. – Access mode: https://commons.erau.edu/adfsl/2013/wednesday/5
11. Ontology-based smart sound digital forensics analysis for web services / [A. Akremi, M.-F. Sriti, H. Sallay, M. Rouached] // International Journal of Web Services Research. – 2019. – Vol. 16, № 1. – P. 70–92. DOI: 10.4018/IJWSR.2019010104
12. Alzaabi M. Ontology-Based Forensic Analysis of Mobile Devices / M. Alzaabi // Proceedings of the 20th IEEE International Conference on Electronics, Circuits and Systems. IEEE, 2013. – P. 64–68. DOI: 10.1109/ICECS.2013.6815346
13. Park H. Cyber Forensics Ontology for Cyber Criminal Investigation / H. Park, S. Cho, H. Kwon // Forensics in Telecommunications, Information and Multimedia, LNICST, 2009. – Vol. 8. – P. 160–165. DOI: 10.1007/978-3-642-02312-5_18
14. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів / Я. Найдьон // Підприємництво, господарство і право. – 2019. – № 5. – С. 304–307. DOI: 10.32849/2663-5313/2019.5.56
15. Резильєнтність комп'ютерних систем в умовах кіберзагроз: Онтологія та таксономії / [С. М. Лисенко та ін.] // Радіоелектронні і комп'ютерні системи. – 2020. – № 1 – С. 17–28. DOI: 10.32620/reks.2020.1.02
16. Qualifying Cyber Crime as a Crime of Aggression in International Law / [M. Maskun, A. Achmad, N. Naswar et al.] // Cybercrime under International Law. – 2020. – Vol. 13, № 2. – P. 397–418. DOI: 10.14330/jeail.2020.13.2.08
17. Uma M. A survey on various cyber attacks and their classification / M. Uma, G. Padmavathi // Int. J. Netw. Secur. – 2013. – Vol. 15, № 5. – P. 390–396. DOI:10.6633/IJNS.201309.15(5).09
18. Chandra A. A taxonomy of cybercrime: Theory and design / A. Chandra, M. J. Snowe // International Journal of Accounting Information Systems. – 2020. – Vol. 38. – P. 100467. DOI: 10.1016/j.accinf.2020.100467
19. Harmandeep S. B. Cybercrimes: A proposed taxonomy and challenges / S. B. Harmandeep, G. Kumar // Journal of Computer Networks and Communications. – 2018. – Vol. 11. DOI: 10.1155/2018/1798659
20. Goni O. Cyber Crime and Its Classification / O. Goni // Int. J. of Electronics Engineering and Applications. – 2022. – Vol. 10, № 1. – P. 01–17, DOI: 10.30696/IJEEA.X.I.2021.01-17
21. Кримінальний кодекс України. Верховна Рада України. Законодавство України. – Access mode: https://zakon.rada.gov.ua/laws/show/2341-14
22. Themis. Ontology testing. – Access mode: https://themis.linkeddata.es/index.html
23. Ontological Support System of Managerial Decision-Making of Production Tasks for a Food Enterprise / [N. Lutska, L. Vlasenko, A. Ladanyuk et al.] // Machinery & Energetics. – 2022. – Vol. 13, №3. – P. 53–61. DOI: 10.31548/machenergy.13(3).2022.53-61

DOI 10.15588/1607-3274-2023-4-17