Ontology-Based Risk Analysis System Concept

Grabusts P.
Rezekne Academy of Technologies,
Rezekne, Latvia
Email: peter@ru.lv

Uzhga-Rebrov O.
Rezekne Academy of Technologies,
Rezekne, Latvia
Email: rebrovs@tvnet.lv

***Abstract*—The work is dedicated to the development of an ontology concept for assessment risk of threats for information systems on the Microsoft approach – the model of identifying threats STRIDE and methodology DREAD for assessment risk of threats. The aim of the study is to describe the security implementation methodology of information systems offered by Microsoft. The basic concepts and techniques of this model are given and ontology concept of risk assessment is proposed, some of the classes and subclasses of the developed ontology are described.**

***Keywords*—information system, risk analysis, ontology, thread, DREAD, Protégé, STRIDE.**

I. Introduction

The relevance of information security is not in doubt today is characterized by continuous and increasing threats to information systems (IS) and networks. The data, processed in IS, are important to users, as a weak and unreliable system can cause dramatic consequences: the loss of intellectual property, simple system, performance degradation, detriment to business reputation, loss of customer trust, financial risks. The contingent problems originated during the implementation of security systems, is presented in Fig. 1 [1].

Figure 1. Problems of implementation of protection IS

To manage the information security of IS the risk analysis is needed. Risk is a comprehensive evaluation of the effectiveness of confrontation threats [2], [3]. Mainly two approaches to defining security risks are described in literature [7], [11].

The degree of risk is evaluated on the basis of specific requirements for information security:

- variously regulations;
- recommendation of software producers;
- international standards.

The second approach involves determining the probability of potential threats and the extent of the damage. The degree of risk is calculated separately for each threat using various techniques. Expert evaluation of the probability of threats and the empirical value of possible damage is taken into account.

This article discusses Microsoft's approach of risk management for IS and the possibility of applying the method of ontology to describe threats to IS.

II. Method of risk management based on Microsoft

Announced in 2002 Microsoft initiative called "Trustworthy Computing" was not just another marketing campaign, but a significant step for the protection of the software at various levels. The essence of the initiative lies in the fact that developing IS, it is necessary to pay special attention to the security from the earliest stages.

"Trustworthy Computing" is a serious initiative within Microsoft to improve the security and reliability of computers. Security means a system is resilient to attack, and the confidentiality, integrity, and availability of both the system and its data are protected [16].

The first and most important criterion for the introduction of reliable protection is the confidence in the fact that protection of IS should be part of the development of the IS project. Microsoft has offered the security strategy SD3+C (Secure by Design, by Default, in Deployment, by Communication).

Structure SD3+C contains 4 principal components [1] (see. Tab. I). Stages of simulation IS threats are shown in Fig. 2 [1]. In the process of designing IS the threat modeling has great importance:

- an important part of IS design;
- reduces the costs on the developing IS security;
- helps the developers identify threats to the system.

It is necessary to generalize information about potential threats and identify the them. STRIDE model (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) defines the types of potential threats (see. Tab. II) [17].

To evaluate the risk of threats to IS Microsoft offers methodology DREAD (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability) [18]:

Table I. SD3+C SECURITY FRAMEWORK

Component	Characteristics
Secure by Design	Secure architecture and code
	Threat analysis
	Reduce vulnerabilities
Secure by Default	Reduce attack surface area
	Unused features off by default
Secure in Deployment	Protect, detect, defend, recover, manage
	Process: How to architecture guides
	People: Training
Secure by Communication	Clear security commitment
	Full member of the security community
	Microsoft Security Response Center

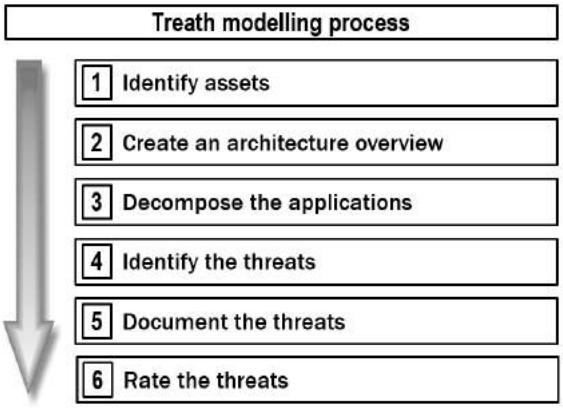

Figure 2. Treath modelling process

Table II. IDENTIFY SECURITY RISKS AND THREADS - STRIDE

Types of threats	Characteristics
Spoofing	Forge e-mail messages
	Replay authentication packets
Tampering	Alter data during transmission
	Change data in files
Repudiation	Delete a critical file and deny it
	Purchase a product and later deny it
Information disclosure	Expose information in error messages
	Expose code on Web sites
Denial of service	Flood a network with SYN packets
	Flood a network with forged ICMP packets
Elevation of privilegies	Exploit buffer overruns to gain system
	Obtain administrator privileges

- Damage potential (How much are the assets affected?)
- Reproducibility (How easily the attack can be reproduced?)
- Exploitability (How easily the attack can be launched?)
- Affected users (What's the number of affected users?)
- Discoverability (How easily the vulnerability can be found?)

For each of the identified vulnerabilities, for listed factors, the assessment from 0 to 10 is given and the total risk is calculated based on the formula (1):

$$Risk{-}DREAD = \frac{DMG + R + E + AU + D}{5} \quad (1)$$

Where: DMG - Damage, R - Reproducibility, E - Exploitability, AU - Affected users and D - Discoverability.

The question is, what vulnerabilities must be considered primarily, i.e., to determine priorities. For a more detailed assessment the scale CVSS is used (Common Vulnerability Score System) [19].

Currently, IT management has to identify and evaluate vulnerabilities in various software and hardware platforms. They need some way to rank them according to the risk and choose those which must be closed first. However, there are a lot of vulnerabilities and the counting is carried out by their own rules on all platforms. CVSS - is an open platform that helps to solve this problem:

- Standardized range of vulnerabilities. When an organization introduces a common scale of vulnerabilities for all software and hardware platforms, it can develop a common management policy by closing vulnerabilities. This policy may be similar to an agreement on the level of service that sets how quickly a particular vulnerability must be identified and eliminated.
- Open platform. Using CVSS everyone can see the individual characteristics used in the obtaining of total value.
- Ranging from risk. When infrastructure component is designed, the vulnerability gets the particular case. Thus, the calculated vulnerability index is the actual risk for a particular company. This gives users a basis for comparison of vulnerabilities.

CVSS standard was developed by a group of security experts of National Infrastructure Advisory Council. This group included experts from various organizations such as CERT / CC, Cisco, DHS / MITRE, eBay, IBM Internet Security Systems, Microsoft, Symantec.

CVSS provides tools to calculate a numerical indicator on a ten-point scale that allows security professionals operatively make a decision about how to respond to a particular vulnerability. The higher the value of the metric, the more rapid response is required.

The standard includes three groups of metrics:

- Basic metrics describe the characteristics of vulnerabilities that do not change over time and do not depend on the runtime environment. These metrics describe the complexity of exploitation of vulnerability and potential damage to the confidentiality, integrity and availability of information.
- Temporary metrics, as the name implies, introduce in the overall assessment the amendment on the completeness of available information about vulnerabilities, the maturity of the exploiting code (if any) and the availability of correction.
- Using the contextual metrics, security experts can make amendments to the resulting score, taking into account the characteristics of the information environment.

Risk assessment is in fact the main objective in the IS management process: analyzing the information security risks and to take decisions to minimize the risk level. To minimize risks, the following steps are possible [16]:

- do nothing;
- warn the user;
- remove the problem;
- fix problem.

III. Possibilities of using ontologies

In recent years the development of ontologies is formal description of the terms in the domain and the relationships between them that moves from the world of artificial intelligence laboratories to desktops of domain experts [4]. In the World Wide Web ontologies have become common things. Ontologies on the net range from large taxonomies, categorizing Web sites, to categorizations of products sold and their characteristics. In many disciplines nowadays standardized ontologies are being developed that can be used by domain experts to share and annotate information in their fields.

The philosophical term "ontology" is known for a long time, but at the end of the last century, this concept was rethought with regard to knowledge engineering. The classic definition of an ontology in modern information technologies: "An ontology - a formal specification of a conceptualization that takes place in a context of the subject area" [13].

Informally, an ontology is a description of the view of the world in relation to a particular area of interest. This description consists of the terms and rules for the use of these terms, limiting their roles within a specific area. Formally, ontology is a system consisting of a set of concepts and a set of statements about the concepts on the base of which you can build up classes, objects, relations, functions, and theories.

Formally, an ontology is defined as $O =< X, R, F >$, where:

- X - a finite set of concepts of subject area;
- R - a finite set of relationships between concepts;
- F - a finite set of functions of the interpretation given on the concepts and / or relationships.

On a formal level, an ontology is a system consisting of a set of concepts and a set of statements about these concepts, on the base of which we can build classes, objects, relations, functions and theory. The main components of the ontology are classes or concepts, relations, functions, axioms, examples.

It is accepted that an ontology is a system of concepts of a subject area, which is represented as a set of concepts linked by different relations to determine the field of knowledge. The formal structure of the ontology is an advantage for the quality of the method of knowledge representation.

There are many ways to classify types of ontologies. One of the popular ways in the ontology classifies the ontologies according to the level of dependence on the specific task or the viewpoint of the problem [8]:

- Top-level ontologies - describe the most general concepts that do not depend on the subject areas;
- Domain-ontologies - formal description of the subject area, used to clarify the concepts defined in the meta-ontology and defines a common terminology base of subject area;
- Task ontologies - an ontology that defines a common terminology base, related to a specific task;
- Application ontologies - are often used to describe the outcome of actions performed by the objects of subject area or the problem.

The simplest model of ontology with relations is usually based on a class-subclass relationships. Such models are often called taxonomies - hierarchies of concepts towards investments.

Thus, the aim of building an ontology is a representation of knowledge in a particular subject area. A conditional concept of structure based on the use of ontologies can be represented for systems of risk analysis [5], [6], [9], [10], [12], [14], [15] (see. Fig. 3).

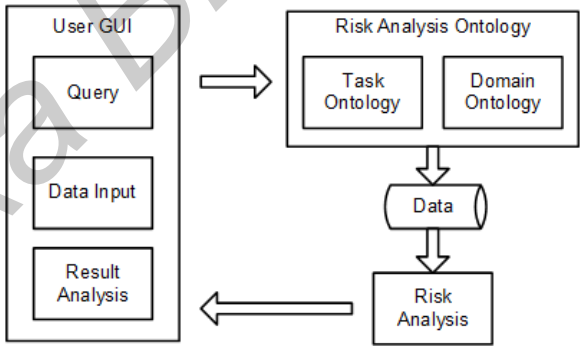

Figure 3. Conditional structure of risk analysis system based on ontologies

IV. The ontology concept of risk assessment

To create the ontology we use the Protégé program [20]. Protégé is a special tool for creating and editing the ontology. Protégé is an ontology and knowledge base editor. Protégé is a tool that enables the construction of domain ontologies, customized data entry forms to enter data. Protégé allows the definition of classes, class hierarchies, variables and the relationships between classes and the properties of these relationships.

Protégé is an initial, free - open source of the platform, which includes a special set of tools and allows to build knowledge-based models of a subject area and applications. Protégé is an extensible knowledge model. Development of ontologies using Protégé begins with identifying and describing of class hierarchy, and then copies of these classes and different types of relationships (properties).

The OWL Web Ontology Language is designed for use by applications that need to process the content of information instead of just presenting information to humans. OWL facilitates greater machine interpretability of Web content than that supported by XML, RDF. OWL ontology may include descriptions of classes, their characteristics and relationships.

The ontology concept for assessment risk of threats for information systems based on the concepts of STRIDE and DREAD methodology is proposed (see. Fig. 4).

Figure 4. Hierarchy of classes in risk assessment

The upper level of ontology is the class Threat. This is an abstract class, which includes all the main classes of the subject area and risk analysis tasks (see Fig. 5). Class Security requirements is a list of security requirements to IS. It is understood that this class will contain the attributes of the confidentiality, integrity and availability, as well as the priorities of these attributes.

Status of class Security problems has not been determined.

Class Threat type is a list of subclasses of identify threats model STRIDE from Table II. STRIDE example is shown in Fig. 6 and their number can be complemented.

Class Risk analysis represents a list of subclasses of DREAD method. DREAD example is shown in Fig. 7.

Class Scale CVSS is used for the problem to calculate the risk with the method DREAD using the accumulated knowledge of the STRIDE.

It should be noted that this concept is under development and will be complemented.

V. Conclusions

Creating ontologies is a perspective direction of modern research on the processing of information, including risk analysis topics in a variety of applications. This article discussed the Microsoft approach to the identification of IS threats and a method of risk assessment. The ontology concept was proposed to assess the risks of IS threats, some of the classes and subclasses of the developed ontology were described. Thus, ontology becomes the storage and knowledge management system.

References

[1] Microsoft Official Course 2840A - Implementing Security for Applications. Microsoft, 2004.

[2] Y. Y. Haimes, Risk Modelling, Assessment, and Management. USA: John Wiley & Sons, Inc., 2009.

[3] J. Mun, Modelling Risk. USA: John Wiley & Sons, Inc., 2006.

[4] D. Gašević, D. Djurić and V. Devedžić, Model driven architecture and ontology development. Springer-Verlag, 2006.

[5] C. Blanco, J. Lasheras, R. Valencia-Garcia, E. F. Medina, A. Toval and M. Piattini, A systematic review and comparison of security ontologies. International Conference on Availability, Reliability and Security (ARES). Barcelona, IEEE Computer Society 813-820, 2008.

[6] A. Ekelhart, S. Fenz, M. Klemen and E. Weippl, Security Ontologies: Improving Quantitative Risk Analysis. 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 2007.

[7] S. Fenz and A. Ekelhart, Formalizing information security knowledge. In 4th International Symposium on Information, Computer, and Communications Security (ASIACCS '09), pp. 183-194, 2009.

[8] N. Guarino, Formal Ontology in Information Systems. 1st International Conference on Formal Ontology in Information Systems, FOIS, Trento, Italy, IOS Press, 3-15, 1998.

[9] B. Tsoumas and D. Gritzalis, Towards an ontology-based security management. In 20th International Conference on Advanced Information Networking and Applications, pp. 985- 992, 2006.

[10] A. Vorobiev and J. Han, Security Attack Ontology for Web Services. Proceedings of the Second International Conference on Semantics, Knowledge, and Grid SKG '06. IEEE Computer Society, p. 42., 2006.

[11] A. Avizienis, J.-C. Laprie, B. Randell and C. E. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," EEE Trans. Dependable Sec. Comput., vol. 1, no. 1, pp. 11–33, 2004.

[12] M. Donner, "Toward a Security Ontology, " IEEE Security and Privacy, 2003.

[13] T. R. Gruber, "A translation approach to portable ontologies," Knowledge Acquisition, 5(2), 199-220, 1993.

[14] A. Herzog, N. Shahmehri and C. Duma, "An Ontology of Information Security," International Journal of Information Security 1.4: 1-23, 2007.

[15] J. Undercoffer, A. Joshi and A. Pinkston, "Modeling computer attacks: an ontology for intrusion detection," Lecture Notes in Computer Science, pp. 113–135.2820, 2003.

[16] "Trustworthy Computing, Microsoft White Paper," (revised October 2002 version). [Online].

[17] "STRIDE model," [Online]. Available: https://msdn.microsoft.com/en-us/library/ff648641.aspx [Accessed: Dec. 15, 2016].

[18] "DREADful the DREAD system," Microsoft Corporation, 2005. [Accessed: Dec. 15, 2016].

[19] "Common Vulnerability Scoring System (CVSS)," [Online]. Available: https://nvd.nist.gov/cvss.cfm [Accessed: Dec. 01, 2016].

[20] "Protégé project homepage," [Online]. Available: http://protege.stanford.edu/ [Accessed: Dec. 01, 2016].

КОНЦЕПЦИЯ ИСПОЛЬЗОВАНИЯ ОНТОЛОГИЙ В СИСТЕМАХ АНАЛИЗА РИСКОВ

Грабуст П.С., Ужга-Ребров О.И.

Работа посвящена разработке концепции онтологии для оценки рисков угроз информационным системам по подходу Microsoft - модели идентификации угроз STRIDE и методики DREAD для оценки рисков угроз. Даны основные понятия и методики этой модели и предложена концепция онтологии по оценке рисков, описаны некоторые классы и подклассы разрабатываемой онтологии.

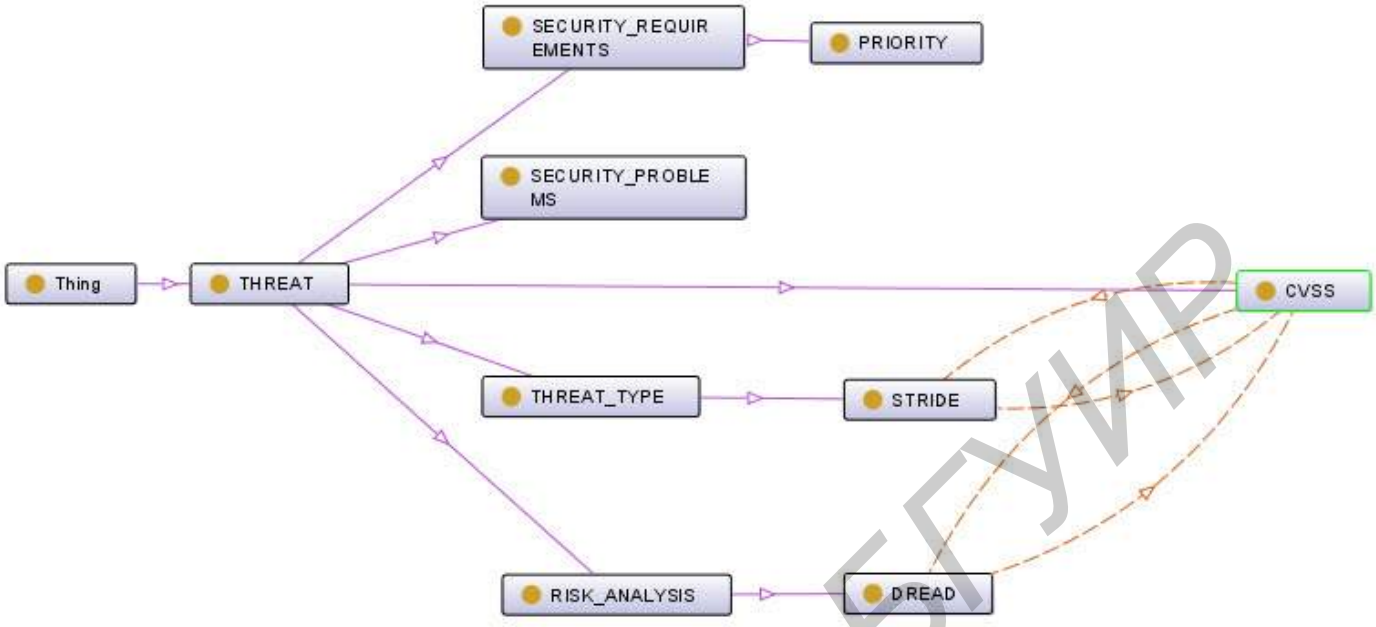

Figure 5. Ontology of IS risk assessment system

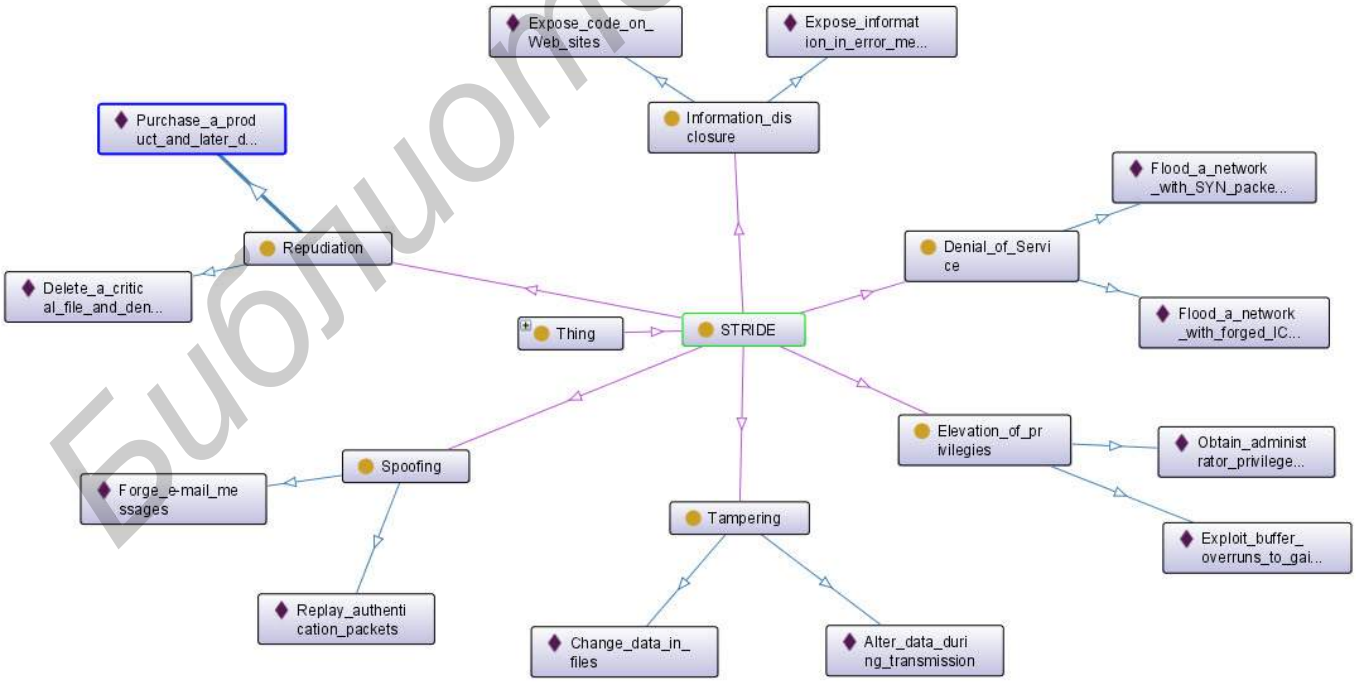

Figure 6. An ontology fragment of threat identification model STRIDE

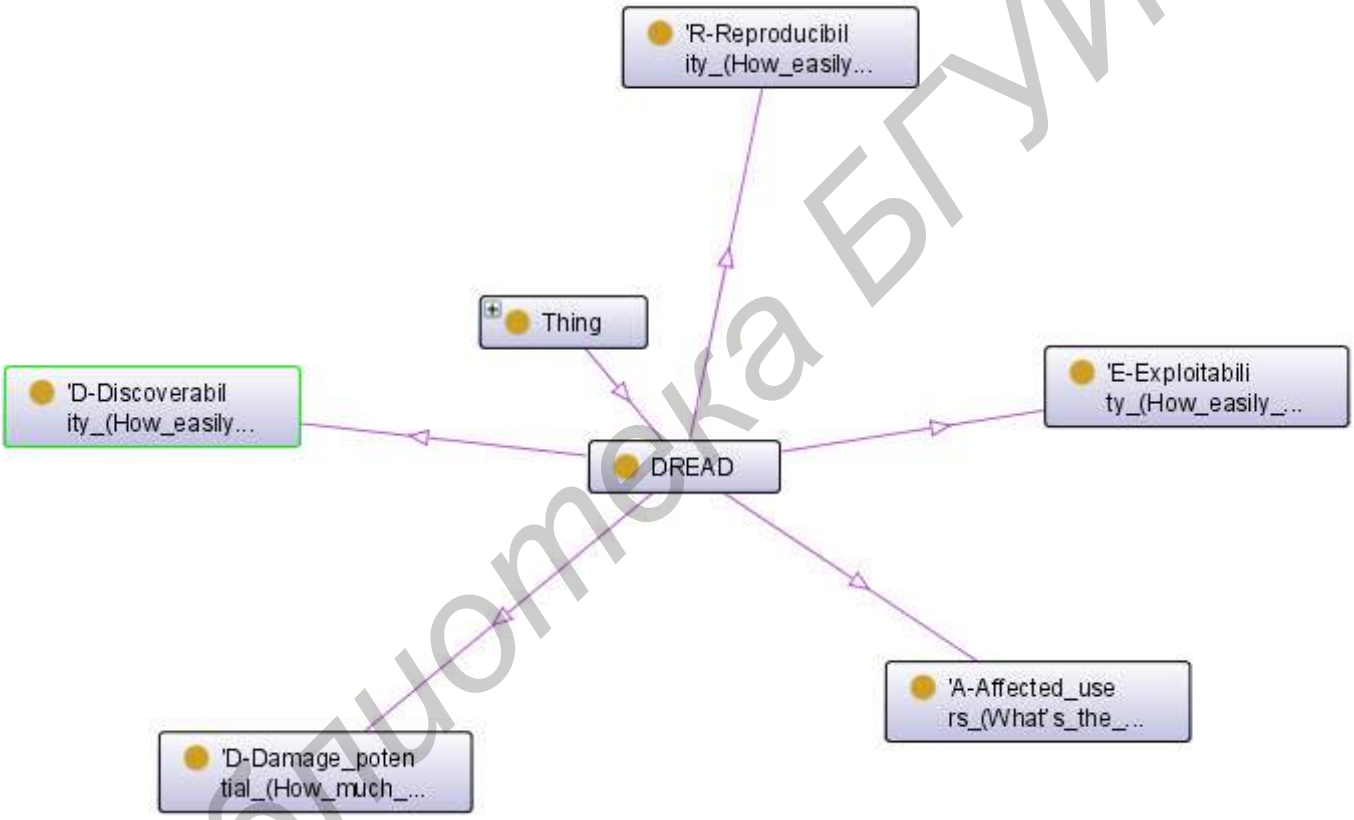

Figure 7. An ontology fragment of risk assessment method DREAD