UDC 004
DOI https://doi.org/10.32838/2663-5941/2019.4-1/14

Kozlenko O.V.
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

INFORMATION SECURITY ONTOLOGY WITH LEAKS SCENARIOS AND INFORMATION SECURITY CULTURE

Analysis of CISS bases on many factors (attack scenarios on the system, etc.), many of which also depends not on hardware elements. Common errors and misunderstanding of the security incidents and how to react also plays an important role. So, for basic security system assessment evaluation, structure, that has determined factors and scenarios of CISS analysis for further use will greatly simplify understanding and automating processes of these evaluations. Attack's results can affect information both directly and indirectly. Usually information threats in the information system depend on the characteristics of the internal system, physical environment, staff and processed information. Threats can have as an objective component (changing the conditions of the physical environment, refusal of elements interactions) and a subjective (human errors or malicious actions), which can be accidental or intentional. Human factor crucially plays important role, because it's usually associated with the lack of or imperfect security measures, but always connected to non-compliance with security policy. In terms of information security, information has three main properties: confidentiality, integrity and availability, and threats, that lead to violation of information and/or its loss for any of the aforementioned properties, respectively are called – threats to confidentiality, integrity and availability of information. Information system analysis is a complex procedure and requires a lot of different, smaller ones. One of components of that analysis is the determination of the CISS elements. To determine these elements for information leaks scenarios in system, security staff should know possible threats to the target system and appropriate way to secure it. Proposed ontological structure can be used to determine average risk of information leakage scenarios and to determine information security culture level to specify overall formal security assessment of organization and, as such, to automate the process of determining risk evaluation.

Key words: *ontology, risk assessment, information leaks scenarios, information security culture, information threat, information attack, human factor.*

Introduction. Providing reliable information security requires significant funds. Therefore, before the security measures implementation we need to ensure in its appropriateness. In particular, preservation of sensitive data for many companies is a top priority in the conduct of business success, and information about the competitor can help to build your business plan so as to outrun them. In general, data leaks can lead not only to substantial financial losses, but also to the complete collapse of the company. To implement necessary security measures to information security leaks and other threats needs to be analyzed for a complete analysis of appointed systems to determine its measures.

Task description. System analysis bases on many factors, such as information leaks scenarios and more. At the same time you must also consider the administrative aspects of data security, such as staff awareness about information systems threats. To evaluate, for example, the average value of information leakage risk we need to determine many factors and predefined structure, which has these factors and scenarios for further use will greatly simplify understanding and automating process of this evaluation. But information security depends not only on the technical aspects of security. Common errors and misunderstandings of the definition of security incidents and how to react also plays an important role. This article focuses on the demonstration of structure that can be used to CISS system analysis for further overall formal security assessment determination and, as such, to automate the process of estimation of this assessment using this structure.

Research evaluations. Common way of using ontology in information security field is to use it in specific way to determine more abstract events (like ontology for virus attacks [10; 11] and so on), or taxonomy for information security field and architecture, based on work at the intersection of knowledge representation [2; 10] and machine learning, includes machine learning modules for automatic file format identification, tokenization, and entity identification [11]. In outline ontology of secure operations in cyberspace, describing its primary characteristics through some basic modeling examples. Such phenomena as information security culture on the other

hand is very unclear in terms of its structure and definition [8; 12].

Main research. Structure for complex information security systems (further – CISS) analysis should have a high level of detail using formalized conceptual framework because there can be large amount of definitions and relationships between this definitions. Aforementioned features presented in such structures as "ontologies". Among computational linguistics professionals the most established (classic) definition of ontology is the definition that was given by Hubert: "Ontology is a specification of conceptualization" [1, p. 199]. Similarly, there are a number of extended Hubert's definitions, among which there are:

– ontology – a specification of conceptualization, where the conceptualization sets of domain objects and relationships between them [2, p. 208];

– ontology – a knowledge which is formally presented on the conceptualization basis.

Formally, ontology consists of terms organized in taxonomy of definitions and attributes, and related axioms and rules [2, p. 209].

There are also difficulties with the formal definition of "ontology". According to [3, p. 19], computer domain ontology (CDO) is a set: $O = X, R, F$, where $X = \{x_1, x_2, \ldots, x_i, \ldots, x_n\}, i = \overline{1, n}, n = CardX$ – set of definitions of the appointed CDO; $R = \{r_1, r_2, \ldots, r_k, \ldots, r_m\}, R = x_1 * x_2 * \ldots * x_n, k = \overline{1, m}, n = CardR$ – set of relations of definitions of the appointed CDO. In general, relations are divided into common (of which there are usually partial order relations) and specific relationship in the given CDO. $F = X * R$ – set of the interpretation functions of the given concepts and relationships. A special case of interpretation functions F set is a compiled glossary for set of multiple concepts X. X_i definition determination generally includes a subset of concepts $\{x_{i-1}\}$, which are determined by X_i; relation R_k, that linking X_i with $\{x_{i-1}\}$; and set of particular to X_i attributes (values).

Although the aforementioned sets is the ontology definition, but most convenient way to represent it is in the form of ontograph. Ontograph is a one directional graph in which in the one peak can go in and out few curves, where peaks are the concepts of domain and curves – relationships between them.

In the simplest case, an ontology design methodology includes three stages of the design:

1. preliminary analysis of the subject area;
2. manual ontograph construction;
3. visual representation.

As you can see, the first stage in developing ontology ("preliminary analysis of the subject area") is the most important because this stage consists of the determination of the basic terms and relations between them. To build ontology for (CISS) analysis, information leakage scenarios and analysis of the administrative aspects of data security is required to understand the possible security problems.

Information systems analysis is a complex procedure and requires a lot of different, smaller procedures. One of the components of that analysis is the determination of the CISS elements. To determine these elements for information leaks in system security staff should know possible threats to the target system and appropriate way to secure it. According to [4, p. 22], realization of potential insecure actions that lead to lowering information resources' value with the potential adverse effects on the system and information are called threats and realization of threat is called an attack.

To build ontology for CISS analysis we need to analyze each of these scenarios separately [5; 6; 7]:

– "Point-of-Sale intrusion" scenario includes attacks on the retail trading environment;

– "Web-App Attacks" scenario includes instances of malicious code aimed at the machine instructions vulnerabilities in applications or disruption of authentication mechanisms;

– "Crimeware" scenario includes all cases of obtaining classified information with help of malicious software except for aforementioned attacks;

– "Cyber-espionage" scenario have incidents in which occurred unauthorized access to systems and networks associated with motive of someone else's information disclosure and/or motive for espionage;

– "Payment card skimmers" scenario includes devices that are physically installed in places of payment cards data reading from magnetic tapes and aimed at data gathering and illegal interference in payment transactions;

– "Physical theft/loss" scenario includes cases of theft or loss of physical data sources due to carelessness of its owner;

– "Miscellaneous Errors" scenario includes incidents of accidental compromising of security attributes of information assets that do not fit under other scenarios mentioned;

– any attack aimed at network availability violation or its corresponding system belongs to "Denial-of-Service" scenario. Typically, results of such incidents do not violate confidentiality;

– "Privilege misuse' scenario is covering all incidents that have occurred because of employees or trust persons abused their rights consciously or negligently performed their duties.

Also in that statement for 2016 Verizon [5] correspond threats to each of the above scenarios and,

based on this, we define the set of necessary security measures, which consists of:

– "Software check-out" – a thorough check of types, versions of all software patches;

– no unnecessary software, accounts, and other ports – constant check that there are no system software, accounts, ports etc. that are not used;

– updates and patches – constant patch updates and installs for software and OS;

– system files integrity – constant check of suspicious changes to system files, emergence of new suspicious files in the system areas and reporting in case of such activity;

– antivirus software – use of effective antivirus products, anti-spyware and personal firewalls;

– security software upgrade – constant check for updates to the security software and their installation;

– DEP, ASLR, EMET – use of Data Execution Prevention (DEP), Address space layout randomization (ASLR) and Enhanced Mitigation Experience Toolkit (EMET) technologies;

– web-applications testing - web applications check for potential security vulnerabilities, bugs in the code, etc;

– confidentiality of developed software materials – constant check that unauthorized persons do not have access to development (scripts, unused libraries, etc.);

– backups - automatic procedure for backing up data on a regular basis;

– information security training for employees – mandatory training for employees in information security;

– employees knowledge verification in IS – periodic IS testing for employees;

– traffic filtering – traffic filtering from authorized services and ports;

– services distribution – distribution of critical system services from all other services (physically located on another machine, etc.);

– administrator's control – monitoring of administrators by senior management;

– complex passwords – use of complex passwords;

– default Passwords – procedure for changing all default passwords;

– IP blacklist/ whitelist – use of blacklists for known malicious IP addresses or whitelist for trusted IP addresses;

– TFA – use of two-factor authentication;

– netflow protocol – use of network traffic record;

– event logging – constant check and documentation of suspicious activity in the event logs;

– account Management – process of system accounts review and remove procedures for those that are not associated with any business process and owner;

– centralized authentication – centralized point of authentication (such as LDAP, Active Directory, etc.);

– activity monitoring – check of the occurrences of user in the system in unusual time;

– encryption – use of encryption and special algorithms for classified information;

– no sensitive data in open text – scanning servers for the classified information in the plaintext format;

– DLP-system – use of Data Leak Prevention (DLP) system;

– incidents management – responding instructions for incidents to employees;

– roles in the incidents management – appointment of specific roles and responsibilities for staff in incidents management;

– network segmentation- network segmentation into several trusted zones;

– surveillance – use of surveillance for monitoring credit card terminals;

– terminal monitoring – constant check of terminal changes;

– user awareness – in-time warning information for users;

– effective design – use of new technologies and security measures in development for credit card terminals.

– As noted, not all threats are directly dependent on the technical characteristics of systems. Human factor is also crucially important, which is not always associated with the lack of or imperfect security measures, but always associated with issue in non-compliance with security policy (SP) [8, p. 72–75].

– The study of human factors in information security is increasingly attracting attention now because they have a significant impact on information security as a whole and on the insider side of its components. According to information given in [8, p. 79 9; p. 120], the majority of employees believe that the responsibility for the integrity of information assets rests on the information security division's shoulders, whose main task is to eliminate errors and incidents. But still, organizations suffer from accidental or intentional staff errors, despite the presence of security policies and necessary technologies. As noted in [8, p. 73] there are two possible solutions to address the issue of non-compliance:

– to implement a strict verification system that determines penalties and disciplinary measures in case of non-compliance. This solution provides quick

results, although negative perception of employees makes that effect short-lived;

– to develop a high level of information security culture (ISC). This solution is time-consuming, but has a lasting effect if succeeded.

It is important to note that there are many definitions of the term "information security culture". In short, most definitions agree that the ISC is a set of values, human beliefs, thoughts and behaviors that ensure a degree of compliance with information security police in the organization. ISC always has a positive or a negative impact on the company and always takes place in it. Also, as stated in [9, p. 102–105], there are factors that influence employee's behavior, such as regulations, established beliefs and behavior norms. New employees, who are in the process of adaptation to the collective norms, guided by the established norms of behavior with a gradual transition to a behavior standards, which are defined in the workplace [9, p . 47–61]. Thus, the organizational culture regulates the activity of workers. The employee takes the basics of correct behavior in the socialization process and it helps the employee to accept established patterns of behavior and standards in organizations (compliance). According to [8, p. 72] "ISC" is determined by terms "Staff" and "Management". The term "Staff" is defined by lower indicators 'Staff Security' and "SP compliance measure'; "Management" – by indicators "Management readiness rate" and 'Coordination'. The indicator "Coordination" is similarly defined by lower indicators like "Cooperation with IS division" and "Cooperation with management". These aforementioned indicators will be used for further analysis.

Now we have all needed information to develop ontology for CISS analysis based on the aforementioned information about leaks scenarios and IS culture. The first stage is the "Preliminary analysis of the subject area" and we need to define X and R sets. Thus concepts (X) set will look like: {Security control center, Confidential data, Security policy, ISC, information leaks security, staff, management, POS-intrusion, Web-App attacks, crimeware, cyber-espionage, payment card skimmers, physical theft/loss, Miscellaneous Errors, Privilege Misuse, Denial-of-Service, Staff Security, SP compliance measure, Management readiness rate, Coordination, Cooperation with IS division, Cooperation with management, "Software check-out", "Software check-out", No unnecessary software, accounts, and other ports, Updates and patches, System files integrity, Antivirus software, Security software upgrade, DEP, ASLR, EMET, Web-applications testing, Confidentiality of developed software materials, Backups, Information security trainings for employees, Employees knowledge verification in IS, Traffic filtering, Services distribution, Administrators control, Complex passwords, Default Passwords, IP blacklists/ whitelists, Two-factor authentication, Netflow protocol, Event logging, Account Management, Centralized authentication, Activity monitoring, Encryption, No sensitive data in open text, DLP-system, Incidents management, Roles in the incidents management, Network segmentation, Configuration, Malicious software security, Development materials security, Staff awareness, Passwords, Account control, Incidents control }.

Relations (R) set consists of following: {Whole-part, Specifies, Uses }.

The next step is "Manual ontograph construction". To perform this we will create a ranking list of terms based on generalized relation "above-below":

– security control center;

– confidential data, Security Policy, ISC;

– information leak security, Staff, Management;

– POS-intrusion, Web-App attacks, crimeware, cyber-espionage, payment card skimmers, physical theft/loss, Miscellaneous Errors, Privilege Misuse, Denial-of-Service, Management readiness rate, Coordination;

– staff Security, SP compliance measure, Cooperation with IS division, Cooperation with management, "Software check-out", Backups, Traffic filtering, Services distribution , Administrators control, IP blacklists/ whitelists, Two-factor authentication, Netflow protocol, Event logging, Encryption, No sensitive data in open text, DLP-system, Network segmentation, Configuration, Malicious software security, Development materials security, Staff awareness, Passwords, Account control, Incidents control.

Conclusions. Thus, in the article scenarios leaks that were obtained from leaks reports in 2015, 2016 and IS culture, which is related to the administrative threats was analyzed. During analysis sets of necessary terms and relations were defined for building ontological structure. Resulting structure for CISS systems analysis, which took into account possible leaks scenarios, studies of information security data identified incidents and specific IS culture level definition. This ontograph can be used as a base for CISS system analysis and, for example, to further determine overall formal assessment of security level and, as such, to automate the process of determining this estimation using that structure.

References:

1. Gruber T.R. A translation approach to portable ontologies Knowledge Acquisition. 1993. 289 p.
2. A. Nikonenko. The Ontological Knowledge Bases Review. 2009. 219 p.
3. A. Palagin, N. Petrenko, K. Malakhov. Technique for designing a domain ontology. УСиМ. 2009. 22 p.
4. Arkhypov O.E. On the methodology of identification and evaluation of assets of the information technology system . Information security .2011. 29 p.
5. 2016 Data Breach Investigation Report, Verizon Enterprise Solutions, 2016.
6. 2015 Data Breach Investigation Report, Verizon Enterprise Solutions, 2015.
7. 2013 Data Breach Investigation Report, Verizon Enterprise Solutions, 2013.
8. A.V. Potiy, D.Y. Pilipenko, I.N. Rebriy. The prerequisites of information security culture development and anapproach to complex evaluation of its level. 2012. 82 p.
9. Van Niekerk, J.F. Fostering Information Security Culture through Integrating Theory and Technology. 2010. 112 p.
10. Natascha Abrek. Attack Taxonomies and Ontologies. Network Architectures and Services . 2015. 20 p.
11. Stefan Fenz Andreas Ekelhart. Formalizing Information Security Knowledge. ASIACCS. 2009. 15 p.
12. Igor Kotenko and Andrey Chechulin. Attack Modeling and Security Evaluation in SIEM Systems. International Transactions on Systems Science and Applications. 2012. 27 p.

Козленко О.В. ОНТОЛОГІЯ АНАЛІЗУ КСЗІ З УРАХУВАННЯМ КІБ

Аналіз КСЗІ (комплексні системи захисту інформації) базується на багатьох факторах (сценарії атаки на систему тощо), багато з яких також не залежить від апаратних елементів. Помилки та нерозуміння виявлення інцидентів безпеки та способів їх реагування також відіграють важливу роль. Результати атаки можуть впливати на інформацію як прямо, так і побічно. Інформаційні загрози, зазвичай, в інформаційній системі залежать від особливостей внутрішніх компонентів, фізичного середовища, персоналу та оброблюваної інформації. Загрози можуть мати як об'єктивний компонент (зміна умов фізичного середовища, відмова взаємодії елементів), так і суб'єктивний (людські помилки чи зловмисні дії), які можуть бути випадковими або навмисними. Людський фактор відіграє важливу роль, оскільки він зазвичай пов'язаний з відсутністю або недосконалими заходами безпеки, але завжди пов'язаний з недотриманням політики безпеки. З точки зору інформаційної безпеки інформація має три основні властивості: конфіденційність, цілісність та доступність, а загрози, що призводять до порушення інформації, а її втрати для будь-якого з вищезгаданих властивостей, відповідно називаються – загрози конфіденційності, цілісності та доступності інформації. Аналіз інформаційних систем є складною процедурою і вимагає безлічі різних, менших. Однією з складових цього аналізу є визначення елементів КСЗІ. Щоб визначити ці елементи для сценаріїв витоку інформації в системі, працівники служби безпеки повинні знати можливі загрози цільовій системі та відповідний спосіб її захисту. Запропонована онтологічна структура може бути використана для визначення середнього ризику сценаріїв витоку інформації та для визначення рівня культури інформаційної безпеки для уточнення загальної формальної оцінки безпеки організації та, як такої, для автоматизації процесу визначення ризику.

Ключові слова: *онтологія, оцінка ризику, сценарії витоку інформації, культура інформаційної безпеки, інформаційна загроза, інформаційна атака, людський фактор.*