PERSONALITY & SOCIETY

PERSONALITY&SOCIETY | ISSN: 2712-8024
Volume 2, Issue 3 – January – June, 2021 / pp 11-17
Doi: https://doi.org/10.46502/issn.2712-8024/2021.3.2

Received:12.04.2021 | Accepted: 05.06.2021

Psychological readiness and ontologies in security of digital multilevel distributed systems

Психологическая готовность и онтологии в обеспечении безопасности цифровых многоуровневых распределенных систем

Preparación psicológica y ontologías en seguridad de sistemas distribuidos digitales multinivel

……

Kosolapova Olga Aleksandrovna[2]

Abstract

Information, computer environments and systems require not only technological, but also psychological, neuro-linguistic support. The evolution of a digital, competency-based society requires the active introduction of information and communication technologies in all key areas (e-government, e-learning, e-business, etc.). There is also a negative impact of such an evolutionary process, for example, the emergence of IT risks and threats to the individual, society and society. It is also possible to strengthen the information confrontation, hybrid war, "Trojan training", etc. It is very important to ensure the security of multilevel distributed information structures of the digital economy. The article discusses the systemic analysis of this problem, explores some specific aspects and tasks, in particular the use of ontologies and formalization. System-synergistic analysis of psychological readiness and its support by ontological approach was carried out. System objectives of network attacks and psychological influences in conditions of evolution of distributed infological system are revealed. A general model of system security ontology in a formal-semantic and infological form is proposed. Everything is implemented based on the semantics of controlled process metadata (Resource Description Framework), metadata prediction languages (Ontology Language), ontology standards, analytics, "parallelization" of knowledge and updating of knowledge bases, Big Data, Data Mining, Social Mining, Data Centers, multi-agent and other systems.

Key words: psychology, ontology, security, distributed systems, networks, digital economy, infological.

Аннотация

Информационные, компьютерные среды и системы требуют не только технологической, но и психологической, нейролингвистической поддержки. Эволюция цифрового общества, основанного на компетенциях, требует активного внедрения информационно-коммуникационных технологий во всех ключевых областях (электронное правительство, электронное обучение, электронный бизнес и т.д.). Существует также негативное влияние такого эволюционного процесса, например, возникновение ИТ-рисков и угроз для личности, общества и общества. Также возможно усиление информационного противостояния, гибридной войны, "троянской подготовки" и т.д. Очень важно обеспечить безопасность многоуровневых распределенных информационных структур цифровой экономики. В статье рассматривается системный анализ данной проблемы, исследуются некоторые специфические аспекты и задачи, в частности использование онтологий и формализация.

[2] Master degree student Linguistic University of Nizhny Novgorod, Russia, https://orcid.org/0000-0001-5195-2333

Проведен системно-синергетический анализ психологической готовности и ее поддержки с помощью онтологического подхода. Выявлены системные цели сетевых атак и психологических воздействий в условиях эволюции распределенной инфологической системы. Предложена общая модель онтологии системной безопасности в формально-семантической и инфологической форме. Все реализовано на основе семантики метаданных управляемых процессов (Структура описания ресурсов), языков прогнозирования метаданных (Язык онтологий), стандартов онтологий, аналитики, "распараллеливания" знаний и обновления баз знаний, Больших данных, интеллектуального анализа данных, Социального анализа, Центров обработки данных, мультиагентных и других систем.

Ключевые слова: психология, онтология, безопасность, распределенные системы, сети, цифровая экономика, инфология.

Resumen

La información, los entornos y los sistemas informáticos requieren no solo apoyo tecnológico, sino también psicológico y neurolingüístico. La evolución de una sociedad digital basada en competencias requiere la introducción activa de tecnologías de la información y la comunicación en todas las áreas clave (gobierno electrónico, aprendizaje electrónico, comercio electrónico, etc.). También hay un impacto negativo de tal proceso evolutivo, por ejemplo, la aparición de riesgos y amenazas de TI para el individuo, la sociedad y la sociedad. También es posible fortalecer la confrontación de información, la guerra híbrida, el "entrenamiento troyano", etc. Es muy importante garantizar la seguridad de las estructuras de información distribuidas multinivel de la economía digital. El artículo analiza el análisis sistémico de este problema, explora algunos aspectos y tareas específicas, en particular el uso de ontologías y la formalización. Se llevó a cabo un análisis sinérgico del sistema de la preparación psicológica y su apoyo mediante un enfoque ontológico. Son revelados los objetivos del sistema de los ataques de red y las influencias psicológicas en las condiciones de la evolución del sistema infológico distribuido. Se propone un modelo general de ontología de seguridad de sistemas en forma formal-semántica e infológica. Todo se implementa en base a la semántica de metadatos de procesos controlados (Resource Description Framework), lenguajes de predicción de metadatos (Ontology Language), estándares de ontología, analítica, "paralelización" de conocimiento y actualización de bases de conocimiento, Big Data, Data Mining, Social Mining, Centros de datos, multiagente y otros sistemas.

Palabras clave: psicología, ontología, seguridad, sistemas distribuidos, redes, economía digital, infológica.

Introduction

The evolution of a competency-based and knowledge-based society requires the active introduction of information and communication technologies. Changes in the IT infrastructure of key areas and structures (e-government, e-learning, e-business, etc.) will also be required. Risks and threats to the individual, society and society are increasing.

Without a relevant system of psychological training and security in the context of multilevel distributed information attacks, it's impossible to solve other pressing problems of the digital economy. Therefore, a system analysis of this problem has been carried out, and the composite problems for making practically oriented decisions have been studied.

Theoretical bases

Complexity of modeling – in insufficient identification of dependences of indicators, parameters. It's necessary to apply situational modeling, linguistic programming and ontologies (Gruber, 1995). Ontologies became more active in development of managing actions and in information and legal communities. It's model of representation of knowledge, for example, in the form of semantic interrelations – concepts, properties and the relations between them and processes.

The ontology will provide integration of concepts and platforms of a solution of tasks to the companies nominating safety to the first positions, ensuring information security of the website, its audit. It's useful to the companies using many platforms, diverse programs.

The scheme of creation of ontology consists of stages:

1) studying of a system (formalization, conceptualization and computerization);
2) classification of objects by properties of classes (the coordinated understanding by research group);
3) identification of communications in an explicit form;
4) identification of "class" abilities.

Identification of systems in ontologies – on the basis of knowledge (experts), semantic models.

The ontology is the conceptual and formalized classification form in a certain data domain reflecting its entities, data, classes and interrelations of classes and also their quality. Everything is implemented on the basis of metadata semantics of controlled processes (Resource Description Framework), languages of forecasting of metadata (Ontology Language), standards of ontologies, analytics, "parallelization" of knowledge and updating of knowledge bases, Big Data, DPC, multi-agents, neuro-systems and other not-classical systems.

Object-oriented models are developed by different methods, for example, use:

1) the knowledge base, "builds in" it the tasks by means of inference rules and creates models of knowledge so that the solution method "almost" forms in the base;
2) ontologies (meta-ontology) taking into account metastructures of the processed data.

There's a "golden rule": ontologies define the hierarchy of classes, properties, relations and instances. First, upper-level ontologies (metaponition) are formed, then lower-level ontologies are formed, etc.

Ontologies such as Enterprise Project (Uschold M.,1997), Process Specification Language (Bock & Gruninger, 2005), Virtual Enterprise (Fox, Barbuceanu, Gruninger & Lin, 1997), Super Project (Hepp M., 2005), OntoGov (Abecker, 2004) and others (Kudryavtsev, 2021).

They help resolve situations where adaptability, automation, reduced communication resources; technology chains and decision-making are needed.

Methodology

Today's view of information security challenges requires an evolutionary approach. It's necessary to take into account not only the composite tasks, but also their connections, technological and infrastructure capabilities of society. In particular, the genesis of the problem for the evolutionary purposes of the information society (Polyakov, 2016) will require solving the following tasks:

1) technological support of all socially and economically important spheres of life, critical for social and personal development;
2) taking emergence (Kotenko, et al., 2018) properties of impacts and counteractions;
3) reducing risks of vulnerability from IT impact, turning information confrontation into information war and terrorism;
4) providing information advantages into competitive, market advantages;
5) creation of self-improving in the legal field of IT-infrastructure key structures of society, as well as training of specialists able to effectively and quickly solve the above-mentioned tasks.

Two legal categories should be distinguished between "information protection" and "information security". Especially in relation to psychological readiness for attacks and possible damage.

The targets of network attacks and attacks are:

1) discrediting, justifying psycho-informational influence, attracting allies, sympathizers;
2) reducing the measure of psychological readiness to repel vulnerabilities, the main part of a large-scale attack;
3) psychological effect of influence due to involvement of third parties, their psychological processing.

There's a need for coordination to prevent attacks that have not yet begun:

1) monitoring critical parts of national cyberspace for the presence of destruction, vulnerabilities, assessment of real and projected damage;
2) comparison of current estimates, potentially possible damage from successful realization and destructive actions against state structures, objects and adoption of adaptive key measures;
3) verification of information, implementation of measures and actions to increase public confidence in state structures;
4) practical measures directed against the initiator of the information conflict.

The psychological and political impacts of conflict, as confirmed by world practice, should be taken into account. It's necessary to develop protective psychological actions of the attacked side. It's necessary to apply considerations on actions of a psycho-informational nature, which are well studied, described well in the traditional policy of IT-security.

New challenges require a review of previous approaches, including psychological impact. It's advisable to focus on the formation of their information and psychological component.

Ontologies can be considered as a formal and practical tool. Ontologies help to create a system representation of subject-oriented knowledge, help to describe system models, processes and structures, semantic connections for their subsequent mapping to the subject area.

Results

The model is formalized by the form: M=<A, B, C, D, E>, where, for example, A – characteristics of infrastructure, B – characteristics of software, C – a vector of parameters of technical support, D – a vector of costs, E – a vector of criteria (standards) of security.

We offer a general ontologies models of safety strategy in the system can be considered (Table 1).

Table 1.
General system security ontology model.

Processes and their activities	System (company, organization, influence)	Strategy and its target orientatio
Activity	System	Purpose
Activity specification	Client (Network element)	Have purpose
Execute	Corporation	Planned purpose
Start time	Partner	Strategic objective
End time	Legal Entity	Job, workflow
Condition	Segment, structure	Scope
Effect	Manage	Adaptivity
Functionality	Make, delegate	Result
Activated Communications	Management	Ensure achievement
Authority	Ownership	Strategy
Activity owner	Provider, owner	Strategy planning
Vulnerability event	Vulnerability	Strategic action
Plan	Owner	Solution
Planning	Stakeholder	Critical (risk) status
Process Specification	Employment Contract	Non-Critical Assumption
Ability	Protect	Vulnerability
Skills Impact	Customer/Provider	Risk Factor

Factor of model efficiency of ontologies in definition of a system security policy is fixing of structures and all of them connections with the help of formal, their consistent representation which will provide logicality, laconicism and visibility of the made decision. Taking into account the system of ontologies which is based on conceptual basis.

Most often the requirement of visualization is provided with means of the graph theory (Omelchenko, 2018). It's adequate to ontologic model approach and semantics of the modelled data domain and various applications (Maksimov, Dautova, Salyamova, 2017). For example, to safety and configuring of services of e-Government (Kaziev, Kaziev, & Kazieva, 2017) on the basis of ontologies (Ontology-enabled e-Gov Service Configuration, OntoGov – the project of the European Union).

Virtualization and visualization change educational approaches and technologies intensively. These are powerful tools of demonstration macro - and micro-processes in the nature, society and knowledge. In addition to ontologies special means of virtualization and new tools of visualization appeared. For example, the multimedia approach for interactive specifications of applied algorithms and data view called VM technology or VIM technology. The name VM is formed from reduction of a phrase "Visualization of Methods". The method is applied in data visualization (Peng, Downs, Lacagnina, Ramapriyan, Ivanova, et.al., 2021), as the action plan (more precisely as the procedure, an algorithm) solutions.

The VM technology is based on set of the computing circuits presented in so-called "movie". Each of these schemes reflects some knowledge of a specific method of ontologies processing. For example, about a set (structure) of tops and moving objects in coordinates "space time" and also defines an order of scanning of these tops and objects. The user displays the algorithmic ideas in the form of the computing circuit, specifying its specific filling in the course of the program forming.

The purpose of such approach is obvious and relevant - it's increase in productivity of application programmers, support of visualization of work of parallel programs, ensuring availability to a wide range of users enough difficult parallel computings. Without "parallelization" it's impossible to increase already productivity. As well as without cloud computing.

The main idea of VIM technology – complex use of visualization, animation and scoring at a solution of applied tasks, representation of applied methods (algorithms). VIM technologies, ontologies and neurolinguistic analytics (NLP) are "three whales" of risk reduction and damage of a digital security.

Risk classification is based on the achievement of flexibility, taking into account the individual risk influences of business processes in the environment, management. If, for example, a company's intranet resources have a potential risk of class N={n}, each of which has implementations n={x}, the effectiveness of a separate security appliance for a particular threat implementation is p and depends on the security appliance and the way the threat is implemented.

The effectiveness of E protection measures depends dynamically on how the threat is implemented by a specific security tool E=f (p,m), where m is the number of security tools used by the company's infrastructure security subsystem.

At the same time, pseudosecurity leads to an increase in risks, an adaptation mechanism for the development of the system is needed, adjusted by the degree of risk (Kuklin, Krivenko & Kriventsova, 2019).

Risk identification is assessed by system tension, for example, by:

$$F(x) = \sum_{i=1}^{N(x)} q_i^x,$$

$$F(N_j) = \frac{N_j}{[N_j]}\, F(N_j),$$

$F(x)$ is the frequency of stress effects, N is the number of objects, subsystems, q_i^x is the frequency of a risk situation causing damage to x or more objects, $N(x)$ is the number of different scenarios of risks, threats, $F(N_j)$ is the total frequency of scenarios N_j.

The logical process control model is recorded, for example, by a disjunctive normal form.

Discussion

Technologically, models of cyber threats, especially of a military-political nature, correspond to the main classes of goals (violations) that these threats pursue. For example, loss of potential users trust. Methods of implementing destructive effects can involve both threats of the listed classes and various combinations thereof. In the context of targets, threat features are related to the complexity of potential attack objects, as well as the requirements for these objects. At the same time, NLP-analytics can be effective in analyzing such threats, countering such threats.

NLP analysis of possible cyber threat scenarios suggests that:

1) the technical component of scenarios often coincides with models well studied and adequate in traditional IT security, and the difference is related only to the feature of attack objects, complexity of the organization and requirements for them;
2) the political component does not differ from the model corresponding to scenarios using other types of attacking weapons, and such scenarios themselves are adequately described by various means, for example, neuro-linguistic;
3) technical and political component of conflict scenarios are poorly connected, can be analyzed independently (this fact greatly facilitates formal description of such scenarios using neuro-systems).

Effective measures such as password access to computers and networks, password control, filtering, administrator priority access, careful staff selection, training and training, security monitoring, use of licensed antivirus packages, backup and archiving will help ensure practical security. It's important to familiarize personnel with laws, technologies on information security, for example, the law on insider information. representatives of different ethnic commonalities.

Conclusion

Models of the enemy (aggressor) in cyber conflicts of a military-political nature should always be developed on the basis of the fact that the attacking side has the following capabilities:

1) technical, technological, organizational and space-time resources capable of effectively using them;
2) act on behalf of the state, with economic and political powers (but often it's a simulation of such a situation);
3) access to confidential information about the critical sector of cyberspace, their relationships, including vulnerabilities of destructive cyber actions, as well as information about potential damage in such actions.

Along with the need for professional experience, competences in safety, it's necessary to turn to psychology, ontology, opinions of experts and heuristics. Intellectual, for example, expert systems provide invaluable assistance. They make it possible to structure information, analyze situations, solutions, organize them and choose the optimal ones.

Decision methods and mathematical optimization methods are used to find estimates, model alternative solutions, and best choices. However, a whole set of auxiliary tasks is solved approximately, using intuition and heuristic procedures.

The difficulty of modeling is in the difficulty of identifying, describing the dependencies between different indicators and parameters. Here SII, situational modeling are useful.

References

Abecker, A., Apostolou, D., Hinkelmann, K., Probst, F., Stojanovic, L. & Tambouris, T. (2004) Ontology-enabled e-Government Service Configuration / The OntoGov Approach. M.A. Wimmer (Ed.): e-Gov Days: state-of-the-art 2004. Tagungsband zu den dritten e-Gov Days des Forums eGovernment, Wien: OCG.

Bock, C., & Gruninger, M. (2005) PSL: A Semantic Domain for Flow Models. Software & Systems Modeling, 4(2), pp.209-231.

Fox, M., Barbuceanu, M., Gruninger, M. & Lin, J. (1997) An Organization Ontology for Enterprise Modelling. Simulating Organizations: Computational Models of Institutions and Groups. M. Prietula, K. Carley, L. Gasser (Eds). Menlo Park CA: AAAI/MIT Press, pp. 131-152. URL: https://www.researchgate.net/publication/2549524_An_Organization_Ontology_for_Enterprise_Modelling

Gruber, T. (1995) Toward Principles for the Design of Ontologies Used for Knowledge Sharing. Journal of Human-Computer Studies, No. 43(5-6), pp. 907–928.

Hepp, M., et al. (2005). Process Management: A Vision Towards Using Semantic Web Services for Business Process Management / IEEE International Conference on e-Business Engineering. -Beijing, China, Oct.18-20, pp. 535-540.

Kaziev, V., Kaziev, K., & Kazieva, B. (2017) Fundamentals of legal informatics and informatization of legal systems: a textbook. -2nd ed. -M.: University textbook: INFRA-M. –336p. ISBN 978-5-16-104376-9 (INFRA-M, online).

Kudryavtsev, D. (2021) Overview of application of ontologies in modeling and management, Business Engineering Groups URL: http://bigc.ru/theory/experience/ontologies_for_modelling.php (date of appeal: 15.04.2021).

Kuklin, A., Krivenko, N., & Kriventsova, L. (2019) Economic security and pseudo-security as elements of the development of the socio-economic system. Intern. Research J., No.11(89-1). DOI: https://doi.org/10.23670/IRJ.2019.89.11.031.

Kotenko, I., Fedorchenko, A., Doynikova, E. & Chechulin, A. (2018) An Ontology-based Hybrid Storage of Security Information. Information Technology & Control, No.4, pp. 655-667.

Maksimov, S., Dautova, R., & Salyamova, G. (2017) Use of ontological approach in development of web applications. Information technologies, problems and solutions, UGNTU, No. 1, pp. 262-265. URL: https://www.elibrary.ru/download/elibrary_29300227_68271157.pdf (date of appeal: 15.04.2021).

Omelchenko, A. (2018) Theory of Graphs. Moscow: ICNMO, 416 p. ISBN 978-5-4439-1247-9. URL: https://www.ozon.ru/context/detail/id/143996010/ (date of appeal: 19.04.2021).

Peng, G, Downs, R, Lacagnina, C, Ramapriyan, H, Ivanova, I, et.al. (2021) Call to Action for Global Access to and Harmonization of Quality Information of Individual Earth Science Datasets, Data Science Journal, 20(1), p. 19. DOI: http://doi.org/10.5334/dsj-2021-019

Polyakov, V. (2016) Aspects of information security in information training. M.: FSBNU "IUO RAO". -135p.

Uschold, M., King, M., Moralee, S. & Zorgios, Y. (1997) The Enterprise Ontology AIAI. The University of Edinburgh, 208p.