Ontology of Cyber Security of Self-Recovering Smart GRID

Sergei A. Petrenko
Information Security Department
Saint Petersburg Electrotechnical University (LETI)
St. Petersburg, Russia
s.petrenko@rambler.ru

Krystina A. Makoveichuk
Department of Informatics and Information Technologies
Vernadsky Crimean Federal University
Yalta, Russia
christin2003@yandex.ru

***Abstract*—The article describes the modern Smart Grid from the standpoint of providing resistance to negative impacts, preventing them, and quickly restoring functions after accidents in accordance with the requirements of energy security. To implement this goal, the developed ontology of cyber-security of self-recovering Smart Grids has been proposed for implementation. A critical analysis of approaches and methods to ensure the sustainability of the functioning of power systems in the event of their destabilization. The ideology of sustainability of Smart Grid power systems on the basis of immunity was developed and a scheme for the formation of immunity for disturbances was proposed.**

Keywords—Smart Grid; ontology; self-recovery; immunity; cyber-security.

I. INTRODUCTION

Currently, in a number of developed countries, the technology of intelligent power grids Smart Grid (active-adaptive intelligent network) is widely used to deliver electricity to the consumer using modern digital technologies.

Smart Grid technologies, when implemented in the energy systems, both existing and new, designed, can provide the required innovative properties of the systems. Thanks to Smart Grid energy saving is provided, costs are reduced, network reliability and transparency of the management process are increased. To implement large-scale programs for transforming electric grids into intelligent ones and developing appropriate standard solutions, the world's largest companies have established the Smart Energy Alliance. It includes GE Energy (General Electric), Capgemini, Cisco Systems, Siemens, HP, Intel, SAP AG, Oracle, and others [1]. However, modern power systems, which are complex distributed heterogeneous systems, do not possess the required stability for targeted operation in the current and anticipated information confrontation, because of the high complexity of construction and the potential danger of undeclared functioning of equipment and system-wide software, including hypervisors of the enemy. The relevance of the development of the cyber-security ontology for self-recovering Smart Grid is explained by the need to create an intelligent system for ensuring the sustainability of "smart" energy systems in the context of information countermeasures.

II. PROBLEMS OF RESTORING THE SUSTAINABILITY OF THE SMART GRID

Today, the most significant projects to create power grids based on the Smart Grid are carried out in the USA and Russia, in the countries of the European Union, as well as in Canada, Australia, China and Korea. In the last decade, various models have been developed to assess the readiness of electrical networks to convert to intelligent levels of Smart Grid technologies.

The first model was developed on the basis of the widely used software industry maturity model (Maturity Model), led by IBM, in 2007. As the utility industry embarks on the transformation of the outdated power grid to the new smart grid, it has to develop a shared vision for the smart grid end-state and the path to its development and deployment. The smart grid maturity model (SGMM) is presenting a consepsion of the smart grid, the benefits it can bring and the various levels of development. SGMM is helping numerous utilities worldwide develop targets for their smart grid strategy, and build roadmaps of the activities, investments and best practices that will lead them to their future smart grid state. IBM worked closely with members of the Intelligent Utility Network Coalition (IUNC) to develop, discuss and revise several drafts of the SGMM. Also, this team was assisted by APQC, a member-based nonprofit organization that provides benchmarking and best-practice research for approximately 500 organizations worldwide [2].

This model was brought to practical use by programmers from the Carnegie Mellon University, SEI (Software Engineering Institute). The Carnegie Mellon Software Engineering Institute was govern the SGMM model, working in conjunction with Carnegie Mellon University and the Carnegie Mellon Electricity Industry Center. Then, the institute was leverage its 20 years of experience with goal of working-out of the Capability Maturity Model Integration (CMMI).

In Russia, since 2011, a large-scale project to create an intelligent power system with an active-adaptive network (IPS AAN) is being implemented.

Expert working groups led by the Architectural Committee at the Scientific and Technical Council of JSC FGC UES and the Russian Academy of Sciences (RAS) developed the main provisions and approaches to the creation of a reference architecture of the said intellectual power system. As part of

the implementation of this project in the UES of the East for the period until 2014 with the prospect of up to 2020, the IPS AAN polygon was created, which is a complex of software and hardware that form the environment for supporting the development of IPS AAN solutions.

The main purpose of the Polygon is to support the implementation of projects in the field of intellectual energy (Smart Grid) at all stages of the life cycle of these projects, as well as the implementation of a unique "ecosystem" that contributes to the sustainable innovation development of the power grid complex of the Russian Federation.

It is significant that in these projects the key is to make the future Smart Grid energy systems and the development of the following two new capabilities:

- Resistance to negative impacts: the availability of special methods for ensuring sustainability and survivability, reducing the physical and information vulnerability of all components of the energy system and contributing to both prevention and rapid recovery from accidents in accordance with energy security requirements [3];
- Self-recovery in emergency situations: the power system and its elements should be able to maintain their technical condition continuously in an efficient state by identifying, analyzing and switching from management to the occurrence of a situation to a preventive (warning) occurrence. Self-recovering power system should allow maximum possible to minimize disruptions (disturbances) with the help of an intelligent control system, including its most important component - the subsystem of cyber security.

Thus, an intelligent grid based on Smart Grid should be proactive in relation to changing operational conditions and monitor the impending technical problems before they can adversely affect its safety and the sustainability of the operation as a whole. Therefore, the components of the designed intellectual subsystems of cybersecurity should include the appropriate components of containment, prevention, detection, neutralization and self-recovery.

- Multi-agent systems for coordinating control systems using a transient regimes monitoring system (RTMS) and FACTS devices, self-recovery of district power plants;
- Artificial intelligence, and, including, neural networks for solving problems of identification and management; expert systems for training and conducting training, early detection and localization of emergency pre-emergency regimes;
- Adaptive vector control of flexible AC systems for primary and secondary automatic control of voltage and reactive power, optimization of power modes;
- Adaptive automatic control for renewable energy sources, including wind, tidal, solar, and in the future, space solar power plants;
- Intellectual cybersecurity, capable of providing the required stability of the future Smart Grid energy systems in the context of information confrontation, etc.

III. ONTOLOGY OF CYBERSECURITY

One of the special issues of computer science and artificial intelligence is ontology.

In intellectual grids based on Smart Grid, it is advisable to use ontology (meta-ontology) of cyber-security as a way of representing knowledge about qualitative characteristics and quantitative patterns of information confrontation [1].

The ontology of cybersecurity, according to Thomas Grubber, is a certain specification of the conceptualization of the subject area of information confrontation [4, 5].

Previously, questions of ontological modeling and artificial intelligence were considered by T. Gruber, N. Guarino, D. Oberle, and others, and in the Russia by G. S. Pospelov, D. A. Pospelov, E. V. Popov, L. S. Mussel, A. S. Kleshchev, I. L. Artemyeva, T. N. Vorozhtsova, D. N. Biryukov, I. V. Kotenko, A. G. Lomako, and many others [3, 6-16, 17, 18]. Presently, knowledge models are known in the form of frame systems, semantic networks and production systems. Frame systems and semantic networks allow us to describe the structure of objects in the domain and the relationship between them. Systems of products (rules) are used to represent knowledge of the domain in the form of statements "if-then". On the basis of these models, various knowledge representation languages have been developed, which are the input languages for some universal shells and expert systems.

In the works of A. S. Kleschev. and Artemieva I. L. [11] formulated the main methodological principles for determining the ontology of the subject area.

1) On the substantive level, ontology is understood to mean the totality of agreements (definitions of terms of the subject domain, their interpretation, statements that limit the possible meaning of these terms, as well as the interpretation of these statements). Unlike empirical knowledge, these agreements can not be refuted by empirical observations.

2) Ontology, conceptualization, knowledge and reality must be modeled by a single mathematical construction.

3) An explicit correspondence must be established between the properties of the subject domains and the elements of this mathematical construction.

4) The ontology model of each subject area should contain both formal elements and their meaningful interpretation in terms understandable to specialists of this subject area.

5) The ontology and its model should be observable even for complex subject areas with a large number of concepts.

In the works of I.V. Kotenko [12-14] considered ontology and possible multi-agent intellectual mechanisms for managing cybersecurity in computer systems and networks that allow to:

1) Collection of information on the status of the information system and its analysis through mechanisms for processing and merging information from various sources;

2) Proactive prevention of cyberattacks and preventing their implementation;

3) Detection of abnormal activity and explicit cyberattacks, as well as illegitimate actions and deviations of users' work from the security policy, prediction of intentions and possible actions of violators;

4) Active response to attempts to implement the actions of violators by automatic reconfiguration of protection components to reflect the actions of violators in real time;

5) Misinformation of the attacker, concealment and camouflage of important resources and processes, "enticement" of the attacker into false (fraudulent) components for the purpose of disclosing and clarifying its purposes, reflexive control over the behavior of the attacker;

6) Monitoring the functioning of the network and monitoring the correctness of the current security policy and network configuration;

7) Support for decision-making on the management of security policies, including on adaptation to subsequent incursions and strengthening of critical defense mechanisms.

In the works of D. Biryukov. and Lomako A.G. [6, 10] the ontology and the system image of intellectual systems of cyber-security with the property of anticipation are grounded. In particular, a new class of systems to prevent computer attacks, which are self-learning intellectual systems of self-organizing gyromas. It is shown that the application of the proposed intellectual systems in practice allows to more successfully solve the problems associated with the prevention of risks of the implementation of cyber threats.

In 2011, based on the RDF language, basic for the Semantic Web, a general conceptual (reference) model of the Smart Grid was created, containing structured and unstructured information (authors and support of researchers from the Karlsruher Institut für Technologie Institut AIFB). Despite the fact that this ontology was the most complete, the issues of information protection in it, as well as in other Smart Grid ontologies, were not considered.

Russian scientists in [20, 21] was developed ontology Smart Grid information security as a result of the merger of two ontologies: Gridpedia and ontology of cybersecurity in the energy sector (e.g. [22, 23]). The authors based on the fact that Gridpedia can be used for a sufficiently detailed description of the Smart Grid as a power system, and the ontology of cybersecurity in the power industry allows us to describe the system from the point of view of information security. However, the practical implementation of a new ontology, like Gridpedia, or the addition of Gridpedia with new resources was not implemented (Gridpedia allows users to jointly define concepts). In addition, the Gridpedia project was not, in principle, supplemented or expanded from 2014.

In the context of information confrontation, a more advanced ontology of cyber security, Smart Grid, is required, which allows to prevent the reduction of power systems to catastrophic consequences.

This formulation of the problem required a significant revision of the well-known concept of providing information security for Smart Grid. The point is that modern power systems, which are complex distributed heterogeneous systems, do not possess the required stability for targeted operation in the current and prospective information warfare because of the high complexity of construction and the potential danger of undeclared operation of equipment and system-wide software, including, hypervisors. The means of identifying and complex neutralizing information and technical impacts combining the possibilities of joint combined use of technologies for obtaining unauthorized access, hardware-program bookmarks and malicious software are still not effective enough [1, 10, 20].

Moreover, neither traditional means of information protection at the levels: Level 4 - ERP; Level 3 - MES; Level 2 - SCADA; Level 1 - Programmable logic controller (PLC) / Relay protection and automation (RPA); Level 0 - field devices that include traditional means: protection from unauthorized access, firewalling, traffic filtering (Modbus, OPC, IEC 104), detection and prevention of cyberattacks (IDS / IPS), antivirus protection, cryptographic protection of information, analysis security, integrity control and cyber security management in general based on SCIRT / CERT / SOC), nor the known means of ensuring the stability of power systems using backup, calibration and reconfiguration capabilities are no longer suitable for I ensure the required performance of the promising Smart Grid in the conditions of information confrontation.

IV. DEVELOPMENT OF A NEW ONTOLOGY OF CYBER-SECURITY

The analysis of probable scenarios for the purposeful informational impact on the future Smart Grid energy systems was conducted with the aim of developing a new ontology of cybersecurity. The typical structure of the mentioned power systems is considered and the characteristics of their vulnerabilities are given. The specifics of the implementation of security threats and possible risks to the performance of a typical power system are revealed. The specifics of the implementation of information and technical impacts on critical elements of prospective power systems are revealed [16].

A critical analysis of existing methods and tools for the detection and neutralization of information and technology impacts, including targeted or targeted attacks, APT. The assessment is made of the suitability of traditional means of protecting information in power systems for the prevention, detection and neutralization of information and technology impacts. The shortcomings of the organization of the means of providing and monitoring the policy of cybersecurity on the basis of IEC 62351-8 [16] are shown.

As a result, the ontology of cyber-security of self-recovering Smart Grid was proposed, which allows describing the organization of self-recovering of perspective energy systems in conditions of information confrontation on the basis of immunity to disturbances by analogy with the immune system of protection of a living organism.

The relevance of the new ontology of cyber security Smart Grid is confirmed by the requirements of the Doctrine of Information Security of Russia (2016), the federal law On the Security of the Critical Information Infrastructure of the Russian Federation (2017), GOSTs of the Federal Agency for Technical Regulation and Metrology (2016) normative and methodological documents (2007) and the order of FSTEC of Russia "On approval of the Requirements for ensuring the protection of information in automated control systems for

production and technological processes on critical issues ki important objects ... "(2014) and others.

In this article, the cyber-security ontology of self-recovering Smart Grid (hereinafter - the ontology of cybersecurity) is understood as the basis for reusable knowledge of a special kind, or the "specification of conceptualization" of such a hard-formalized subject area as ensuring the sustainability of functioning of perspective energy systems in the context of information confrontation. This means that in this area, based on the classification of the basic terms of cybersecurity, it is first necessary to isolate the basic concepts (concepts), and then to determine the connections between them (conceptualization). In this case, the ontology of cybersecurity can be represented both graphically and analytically (for example, a formal grammar and programming language or some mathematical model).

Two methodological approaches were used to develop the ontology of cybersecurity. In the first, for the graphical representation of the ontology of cybersecurity, the IDEF5 Schematic Language is used, and for the analytical description is the text language IDEF5 Elaboration Language. In order to automate the simulation of this ontology of cyber security, a demonstration prototype of the SBONT tool of Knowledge Based Systems, Inc. is used.

Implementation of the first methodological approach took 5 years (2000-2005). Currently, the ontology of cybersecurity contains a description of 800 terms from the field of information security (two volumes with a volume of 1284 pages with text and graphic schemes have been prepared), and are constantly maintained in the current state.

For the current version of the ontology of cybersecurity as the initial data were also used terms and definitions of the following regulations and recommendations of the best practice:

1. Thesaurus of normative documents "The Doctrine of Information Security of Russia" (2016), "The main directions of the state policy in the field of ensuring the safety of the automated control system of the Russian Federation" and the "System of Critical Objects ..." of the Security Council of the Russian Federation.

2. The thesaurus of the Federal Law of the Russian Federation of July 27, 2006, No. 149-FZ "On Information, Information Technologies and Information Protection", Federal Law No. 16-FZ dated February 9, 2007 "On Transport Security", Federal Law No. 256-FZ of July 21, FZ "On the Safety of Fuel and Energy Complex Facilities", Federal Law No. 116-FZ of 21.07.1997 "On Industrial Safety of Hazardous Production Facilities", Federal Law of the Russian Federation No. 170-FZ of 21.11.1995 "On the Use of Atomic Energy", Federal Law " On the Security of the Critical Information Infrastructure. "

3. Documents of FSTEC of Russia: Order No. 31 of 14.03.2014 "On Approving the Requirements for Providing Information Protection in Automated Control Systems of Production and Technological Processes on Critical Objects, Potentially Hazardous Objects, and Objects of Increased Danger to Life and Health of People and for the environment "; 2007 FSTEC documents: "Basic model of threats to information security in key information infrastructure systems", "Methodology for determining current threats to information security in key information infrastructure systems", "General requirements for ensuring information security in key information infrastructure systems", "Recommendations for ensuring information security in key information infrastructure systems", "Regulations on the registry of key information infrastructure systems"; draft documents for 2016: "Protection measures in the automated process control system", "Methodology for determining threats to information security in the automated process control system", "Procedure for identifying and eliminating vulnerabilities in the automated process control system", "Procedure for responding to incidents related to the violation of information security".

4. GOST R 53114-2008 "Ensuring information security in the organization" and GOST R 50922-2006 "Information security. Basic terms and definitions "; GOST of the Federal Agency for Technical Regulation and Metrology - Network communication industrial. Security (cybersecurity) of the network and system: GOST R 56205-2014 IEC / TS 62443-1-1-200. Part 1-1. Terminology, conceptual provisions and models, GOST R IEC 62443-2-1-2015. Part 2-1. Preparation of the program for ensuring the security (cybersecurity) of the control system and industrial automation, GOST R 56498-2015 / IEC / PAS 62443-3: 2008. Part 3. The security (cybersecurity) of the industrial measurement and control process; GOST R 56545-2015 "Information security. Vulnerabilities of information systems. Vulnerability Definition Rules (defines the content of vulnerability information that security control vendors should include in their solution database, while the document takes into account existing practices and vulnerability description tools such as Common Weakness Enumeration (CWE), the formal language the Open Vulnerability and Assessment Language (OVAL), the Common Vulnerability Scoring System (CVSS) vulnerability assessment methodology; GOST R 56546-2015 "Information security. Vulnerabilities of information systems. Classification of vulnerabilities» (defines the most common types of vulnerabilities, allowing to unify the terminology used by pentester) [24].

5. Best practice: ISO / IEC 27000 standards in the general principles of ensuring the safety of digital control systems, including ISO / IEC 27032: 2012 "Guidelines for Cybersecurity" and ISO / IEC 27000 "Information technology. Methods of ensuring safety. Information security management systems. General overview and terminology "; IEC TC57 standards: IEC 61850, IEC60870, IEC 62351 regarding the safety of communication protocols; standard INL Cyber Security Procurement Language 2008 [25].

6. Recommendations: NIST-800-82 r.2 "Guide to Industrial Control Systems (ICS Security) - Guide for the security of process control systems" dated 05.2015, Control Systems Security Program / National Cyber Security Division Recommendations for the developers of the standard), IEC 62443 and ISA 62443 (documents of the International Electrotechnical Commission (IEC) and 99 of the Committee for the Development of Safety Standards of the Automated

Automation System (ISA) of the International Automation Society (ISA), NERC CIP (Critical Infrastructure Protection) security (NERC), Departament of Homeland Security: Cyber Security Procurement for ICS, Developments of US-CERT (manuals, models of threats and infringers, rules for responding to cybercriminal, vulnerability databases, etc.)

The development of this ontology of cybersecurity was carried out in stages:

1) defining the context of the ontology of cybersecurity;

2) data collection - definition of the sources of terms and selection of terms for the ontology of cybersecurity;

3) data analysis - definition of the main terms and terms of elements, relationships, verbal description of terms;

4) development of ontology of cybersecurity - creation of a schematic and analytical description of the mentioned ontology;

5) validation of the ontology of cyber-security - checking the completeness and correctness of the ontology, compliance with the original requirements.

The ontology of cybersecurity is represented by graphical schemes in the language of IDEF5 Schematic Language (524 schemes) schemes and corresponding analytical descriptions in the text language of IDEF5 Elaboration Language. The above analytical descriptions of the ontology of cybersecurity are performed in accordance with the previously developed methodology:

1) entering the notation of basic and auxiliary terms of cybersecurity;

2) explanation of the terms-elements with the help of unrelated types;

3) assigning to each term-element a unique identifier;

4) definition of input and output links for each term;

5) fixing connections of elements;

6) verification of the correctness of descriptions.

7) if necessary, updating and clarifying the descriptions.

In the second methodological approach, the recommendations of the W3C consortium (The World Wide Web Consortium) are used to represent the ontology of cybersecurity in the context of the semantic web (web 3.0). The second approach took 4 years (2006-2010). To describe the hierarchy of possible Smart Grid cyber-security ontologies with memory, OWL is used, which provides a detailed description of ontology classes, individuals belonging to these classes, and the existing relationships between them. This language extends the capabilities of the RDF language, which provides an opportunity to operate with the basic "subject-predicate-object" structures, as well as the RDFS language that defines the basic structures and relationships between classes and individuals. At the same time, to ensure the possibility of describing the complex connections between individuals on the ontology of cyber-security Smart Grid, the variant of the OWL DL language is used.

This allowed us to use enumerated types to describe fixed vocabulary structures of the knowledge base of the domain, define multiple links to define many-to-many relationships, and apply logical (Boolean) combinations of classes to define the connections of the complex structure of the Smart Grid ontology of cyber-security with memory. It has been shown that the OWL language allows you to specify different representations of the mentioned ontology of cybersecurity.

It was decided to use the OWL representation in XML syntax as the most common and convenient for automatic processing and analysis of the texts of ontologies of cybersecurity by appropriate software tools. An example of a description of the ontology of cybersecurity using this syntax is given (Table 1).

Integration of separate parts of the cyber-ontology ontology involves the inclusion of ontologies into each other at the level of the language (the owl: imports design). This allowed us to describe the basic concepts, connections and individuals related to the named subject area.

To dynamically expand and modify the knowledge base, a description of the rules for building connections in the SWRL language, which is integrated into ontologies formed in OWL, is used. The rules are used to describe the dynamic relationships between individuals ontologies that arise when certain conditions exist.

For example, such relationships can describe the applicability of the method for solving the problem of ensuring the required stability of the Smart Grid in the conditions of information confrontation, depending on the characteristics of the input data. Using the construction of dynamic relationships in conjunction with the inclusion of ontology makes it possible to implement a partial logical inference already at the level of interpretation of the ontological structure. To do this, a set of active facts, formed in the process of interaction with the user, is formalized as a separate ontology using the inclusion of a basic ontological structure. Interpretation of the received structure allows to carry out the analysis of the basic ontological structure taking into account the entered facts.

TABLE I. EXAMPLE ONTOLOGY REPRESENTATION OF CYBERSECURITY

The view of the ontology of cybersecurity in the syntax of OWL / XML
<?xml version="1.0"?> <!DOCTYPE rdf:RDF [<!ENTITY dl-safe "http://owldl.com/ontologies/dl-safe.owl#"> <!ENTITY swrl "http://www.w3.org/2003/11/swrl#" > <!ENTITY owl "http://www.w3.org/2002/07/owl#" > <!ENTITY xsd "http://www.w3.org/2001/XMLSchema#" > <!ENTITY rdfs "http://www.w3.org/2000/01/rdf-schema#" > <!ENTITY rdf "http://www.w3.org/1999/02/22-rdf-syntax-ns#" > <!ENTITY ruleml "http://www.w3.org/2003/11/ruleml#" > <!ENTITY escience "http://escience.sec.ru/escience.owl#" >]>

```
<rdf:RDF
  xml:base="http://escience.sec.ru/escience.owl#"
   xmlns="http://escience.sec.ru/escience.owl#"
    xmlns:owl="http://www.w3.org/2002/07/owl#"
   xmlns:rdf="http://www.w3.org/1999/02/22-rdf-
                  syntax-ns#"
    xmlns:rdfs="http://www.w3.org/2000/01/rdf-
                   schema#"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
   xmlns:swrl="http://www.w3.org/2003/11/swrl#"

xmlns:ruleml="http://www.w3.org/2003/11/ruleml#">

            <!-- Field of knowledge-->
      <owl:Class rdf:ID="FieldOfKnowledge"/>

             <!-- Solution method-->
           <owl:Class rdf:ID="Method"/>

                    <!-- Task-->
           <owl:Class rdf:ID="Problem"/>

      <!-- A set of data (input or output)-->
           <owl:Class rdf:ID="DataSet"/>

       <!-- Generalization of the method-->
    <owl:ObjectProperty rdf:ID="generalizedBy">
                     <rdf:type
     rdf:resource="&owl;TransitiveProperty"/>
        <rdfs:domain rdf:resource="#Method"/>
         <rdfs:range rdf:resource="#Method"/>
               </owl:ObjectProperty>

       <!-- Parametrization of the method-->
    <owl:ObjectProperty rdf:ID="hasParameter">
                   <rdfs:domain>
                     <owl:Class>
        <owl:unionOf rdf:parseType="Collection">
             <owl:Class rdf:about="#Method"/>
            <owl:Class rdf:about="#Problem"/>
                    </owl:unionOf>
                    </owl:Class>
                  </rdfs:domain>
       <rdfs:range rdf:resource="#DataSet"/>
               </owl:ObjectProperty>

             <!-- Input parameter-->
      <owl:ObjectProperty rdf:ID="hasInput">
                <rdfs:subPropertyOf
         rdf:resource="#hasParameter"/>
               </owl:ObjectProperty>

            <!-- Output parameter-->
      <owl:ObjectProperty rdf:ID="hasOutput">
                <rdfs:subPropertyOf
         rdf:resource="#hasParameter"/>
               </owl:ObjectProperty>

                    </rdf:RDF>
```

To perform queries on the ontological structure, the SPARQL language is used, which allows using the existing ontological interpretation tools to analyze the Smart Grid ontology of cyber security with memory (including the construction of dynamic rule relationships). An example of a query is shown in Table 2.

TABLE II. EXAMPLE OF A QUERY FOR AN ONTOLOGICAL STRUCTURE

The query code for an ontological structure in SPARQL

PREFIX nano:
<http://escience.ru/sec.owl#>
PREFIX escience:
<http://escience.ru/escience.owl#>
PREFIX rdf: <http://www.org/1999/02/22-rdf-syntax-ns#>
PREFIX rdfs: <http://www.org/2000/01/rdf-schema#>
 	
SELECT ?E ?L ?C WHERE {
?E rdf:type escience:DataSet .
?E rdfs:label ?L .
OPTIONAL {?E rdfs:comment ?C} .
nano:Hf escience:hasInput ?E .
?E escience:isValue ?V .
?V rdf:type escience:SelectedValue
}

V. EXAMPLE OF STRUCTURE OF ONTOLOGY

Here is a possible structure of the ontology of cyber-security for describing the set of knowledge used in organizing the self-recovering of the Smart Grid in an information confrontation. This structure was tested in 2012 in joint studies of the scientific schools of cybersecurity LETI, ITMO and the faculty of Computational Mathematics and Cybernetics of Lomonosov Moscow State University.

In the ontology we distinguish two main layers: the description of concepts (classes) and individuals that implement concepts [26]. Thus individuals can be connected by the relations defined at level of concepts. In addition, the relationship between individual concepts is acceptable (for example, the generalization ratio). In the simplest case, the set of relations can be bounded by two-dimensional relations. Another element of ontology is the attributes (characteristics) of individuals, detailing their description. In addition, one of the possible extensions is the association of characteristics not only with individuals (as class implementations), but also with the relationships between them (as implementations of classes of admissible connections).

Formally, the ontology class layer is defined as a graph

$$O = \langle C, R \rangle$$

where C – is the set of classes, R – is the set of abstract relations connecting classes.

Similarly, a layer of individuals ontology is defined as a graph

$$\tilde{O} = \langle \tilde{C}, \tilde{R} \rangle$$

where $\tilde{C}$ – is the set of individuals, and $\tilde{R}$ – is the set of relations between individuals. Thus for each element layer of individuals identified:

a) generalization ratio

$$gn^{(C)} : \tilde{C} \to C$$

$$gn^{(R)} : \tilde{R} \to R$$

which determines the relationship of individuals and the connections between them with the corresponding classes and class relationships;

b) "guard condition", determining the applicability of the elements in these conditions

$$gc^{(C)}(F) : \tilde{C} \to \{0,1\}$$

$$gc^{(R)}(F) : \tilde{R} \to \{0,1\}$$

where F – is the set of active facts defined for the current task;

c) criterion estimation function

$$k^{(C)}(F) : \left\{\tilde{c} \in \tilde{C} \mid gc^{(C)}(\tilde{c}) = 1\right\} \to \Psi^{(C)}$$

$$k^{(R)}(F) : \left\{\tilde{r} \in \tilde{R} \mid gc^{(R)}(\tilde{r}) = 1\right\} \to \Psi^{(R)}$$

where $\Psi^{(C)}$ and $\Psi^{(R)}$, respectively, the space of criteria for evaluating individuals and the relationships between them.

The inference block allows us to determine the way of solving the problem as a tuple $S = (s_1, s_2 \ldots s_N)$ of a fixed structure whose i-th element is a set of the form

$$s_i = \left\{\tilde{c} \in \tilde{C} \mid gn^{(C)}(\tilde{c}) = c_i\right\}$$

where the sequence of classes $c_i \in C$ and requirements for sets s_i determines the overall structure of the solution. To evaluate the solution constructed by the criteria system, graph analysis is used

$$\tilde{O}' = \left\langle \tilde{C}', \tilde{R}' \right\rangle : \tilde{C}' = \bigcup_i s_i \cup \tilde{C}_S$$

where

$$\tilde{C}_S = \left\{ \tilde{c}_S \mid \tilde{c}_S \notin \bigcup_i s_i, \exists \tilde{c}_1 \in \bigcup_i s_i : rch(\tilde{c}_S, \tilde{c}_1) \right\}$$

it is an attached class system,

$$rch(\tilde{c}_1, \tilde{c}_2)$$

it is the ratio of the reachable on the graph.

The estimation is carried out in the space of criteria Ψ, defined by the intersection of the sets of criteria describing the spaces $\Psi^{(C)}$ and $\Psi^{(R)}$.

A possible scheme for the formation of immunity to disturbances is shown (see Fig. 1 and Fig 2).

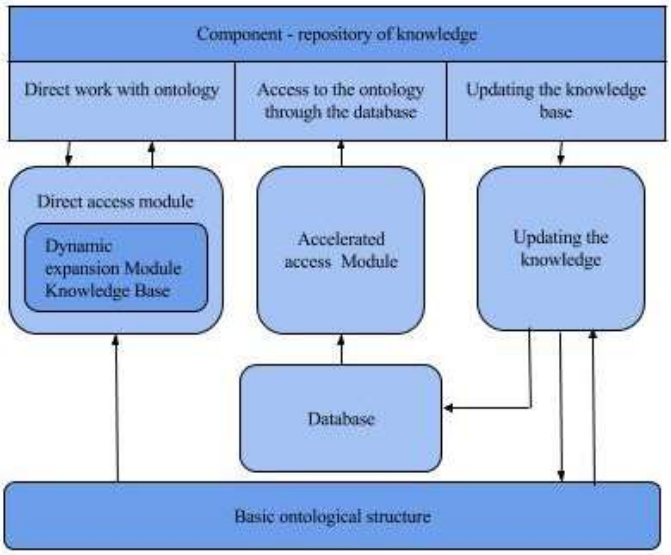

Fig. 1. The scheme of formation of immunity

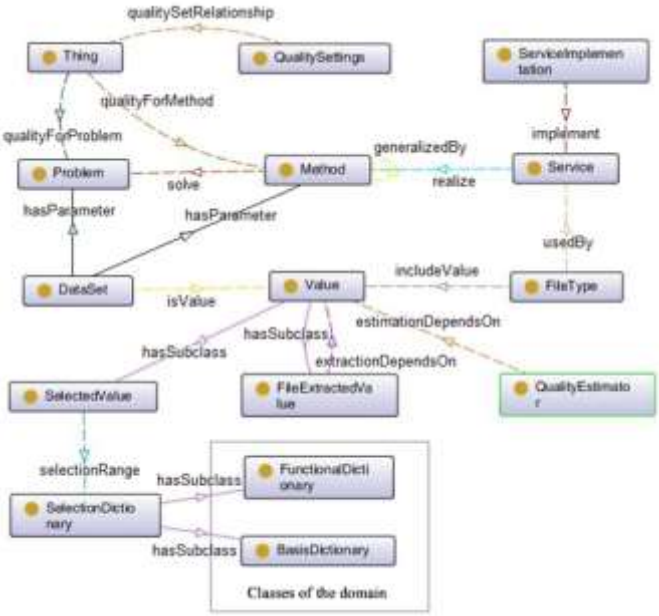

Fig. 2. The structure of the ontology classes of cybersecurity

Here:

Problem - the problem solved within the scope of the subject area;

Method - a method that provides a solution to the task;

Service - the computing service that implements this method;

ServiceImplementation - a copy of the service, available as part of the software package;

DataSet - a set of input or output data for a given method or task;

Value - the size of the domain used as input and output data for solving problems. There are two specific classes of quantities that differ in the way they are assigned:

FileExtractedValue - retrieved from the files of the value. The extraction method is described as a class (in the component source code) that implements the IFileValueExtractor standard interface.

SelectedValue - values selected from the list of available. The list of available values is specified in the ontology by individuals belonging to the subclasses of the SelectionDictionary class.

FileType - file containing the values available for extraction.

The structure of the accumulated immunity database is specified by the ADO.NET Entity Framework model. To organize access to the database, a library is built that provides access to the entity instances stored in the database through the ADO.NET Entity Framework. This approach provided the possibility of accessing the database as a set of interrelated collections storing instances of classes equivalent to database entities. The implementation of direct access to the ontological structure using the Pellet API (RunLib variant) is proposed. The interface implemented by this module includes the following basic methods of working with an ontological structure:

CreateSession () - creates a session, returns the string identifier of the session.

AddOWLModel (<session id>, <ontology>) is an ontological structure extension that is specified in OWL in the form of a separate ontology with possible references to existing elements.

ExecuteQuery (<session id>, <query>) is a request to the ontological structure extended within the current session. The query is specified in SPARQL, the result of which is a string containing the results in XML format.

The general scheme of interaction of RunLib implementation with the ontology interpreter is presented (see Fig. 3).

VI. CONCLUSIONS

As a result of the work done, the imperfection of the traditional means of monitoring and restoration of the operability of the Smart Grid power systems is revealed. The ways of ensuring the stability of the functioning of power systems under hostile mass information and technical influences are investigated. The goals and objectives of ensuring the sustainability of these prospective power systems in the context of information confrontation are formalized.

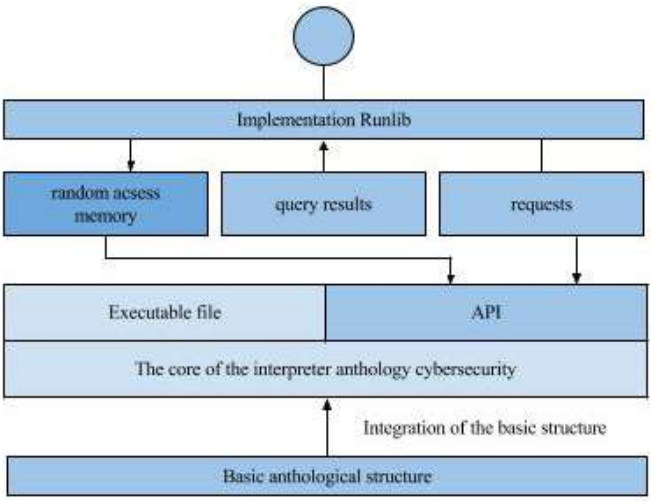

Fig. 3. Scheme of interaction between implementations

The choice of a scientific and methodical apparatus suitable for solving the problems of the organization of self-recovering of the Smart Grid was carried out. The use of the theory of formal languages and grammars for the generation and recognition of possible types of mass perturbation structures is proposed. The formation of immunity to destructive disturbances with the use of the results of the theory of control and restoration of the functioning of the Smart Grid

The conceptual bases of self-recovery of perspective energy systems in the conditions of information confrontation are put forward and substantiated and a new, more perfect, ontology of cyber-security of self-recovering Smart Grid is developed.

REFERENCES

[1] Petrenko S.A., Stupin D.D. Natsional'naya sistema rannego preduprezhdeniya o komp'yuternom napadenii [National system of advance computer attacks alerting]. Innopolis, Afina Publ., 2017. 440 p. *(In Russ.)*.

[2] Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological Framework for Analysis and Synthesis of a Set of Secure Software Development Controls, Journal of Theoretical and Applied Information Technology, 2016, vol. 88, No 1, pp. 77-88.

[3] Massel L., Voropay N., Senderov S., Massel A. Cyber Danger as One of the Strategic Threats to Russia's Energy Security. Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2016. No 4 (17), pp. 2-10. DOI: https://doi.org/10.21681/2311-3456-2016-4-2-10.

[4] Gruber T. A translation approach to portable ontology specifications. Knowledge Acquisition, 1993, V. 5, I. 2, pp. 199-220. DOI: 10.1006/knac.1993.1008.

[5] Gruber T. Toward Principles for the Design of Ontologies Used for Knowledge Sharing? International Journal Human-Computer Studies, 1995, V. 43, I. 5–6, pp. 907-928. DOI: 10.1006/ijhc.1995.1081.

[6] Biryukov D. N., Lomako A. G., Rostovtsev Yu. G. The appearance of anti-cyber systems to prevent the risks of cyber-threat [Proc. SPIIRAN]. 2015, V. 39, pp. 5 - 25. DOI: http://dx.doi.org/10.15622/sp.39.1.

[7] Guarino N. Formal Ontology and Information Systems. In Proc. International Conference on Formal Ontology in Information Systems (FOIS'98). Amsterdam, IOS Press, 6-8 June, 1998, pp. 3-15.

[8] Guarino N., Musen M. Applied ontology: The next decade begins. Applied Ontology. - 2015. - V. 10, no. 1, pp. 1-4. DOI: 10.3233/AO-150143.

[9] Guarino, N. Services as Activities: Towards a Unified Definition for (Public) Services. In Proc. Enterprise Distributed Object Computing Workshop (EDOCW), 2017 IEEE 21st International. Quebec City, QC,

Canada, 10-13 Oct., 2017, pp. 102 - 105. DOI: 10.1109/EDOCW.2017.25.

[10] Kharzhevskaya, A.V, Lomako, A.G, Petrenko S.A. Representing programs with similarity invariants for monitoring tampering with calculations. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017. No. 2(20), pp. 9-20. DOI: 10.21681/2311-3456-2017-2-9-20.

[11] Kleschev A.S. Artemyeva I.L. Mathematical models of ontologies of subject domains. Part 2. Components of the model. Novosibirsk State University Journal of Information Technologies, 2001, ser. 2, no. 3, pp. 19 – 29. *(In Russ.)*.

[12] Kotenko I. Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security. In Proc. IEEE Fourth International Workshop on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS'2007). Dortmund, Germany, 6-8 September, 2007, pp. 614-619. DOI: 10.1109/IDAACS.2007.4488494.

[13] Kotenko I., Novikova E. Visualization of Security Metrics for Cyber Situation Awareness. In Proc. 2014 Ninth International Conference on Availability, Reliability and Security. Fribourg, Switzerland, 2014, pp. 506 - 513. DOI: 10.1109/ARES.2014.75.

[14] Kotenko I., Polubelova O., Saenko I., Doynikova E. The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems. In Proc. 2013 International Conference on Availability, Reliability and Security. Regensburg, Germany, 2013, pp. 638 - 645. DOI: 10.1109/ARES.2013.84.

[15] Mussel L.V. Problems of creating a Smart Grid in Russia from the standpoint of information technology and cyber security. In Proc. All-Russian Seminar with International Participation "Methodological issues of reliability research of large energy systems": Issue 64. Reliability of energy systems: achievements, problems, prospects. Irkutsk, ESI SB RAS, 2014, pp. 171-181. *(In Russ.)*.

[16] Nardi J., Falbo R., Almeida J., Guizzardi G., Pires L., Sinderen M., Guarino N. An Ontological Analysis of Value Propositions. In: Enterprise Distributed Object Computing Conference (EDOC), 2017 IEEE 21st International. Quebec City, QC, Canada, 10-13 Oct. 2017, pp. 184-193. DOI: 10.1109/EDOC.2017.32.

[17] Pospelov D.A. Introduction to applied semiotics. News of Artificial Intelligence, 2002, no. 6. *(In Russ.)*.

[18] Pospelov G.S. Artificial intelligence is the basis of the new information technology. Moscow, Nauka, 1988. 280 p. *(In Russ.)*.

[19] Pashchenko I. N., Vasilyev V. I., Guzairov M. B. Smart Grid security system on the basis of intelligent technologies: rule base design. Izvestiya SFedU. Engineering Sciences *[News of SFedU. Technical science]*, 2015, pp. 28–37. *(In Russ.)*.

[20] Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K. Organization of the entrusted calculations in crucial objects of informatization under uncertainty. In Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements (24-26 May 2017, St. Petersburg, Russia). SCM 2017, 2017, pp. 299 - 300. DOI: 10.1109/SCM.2017.7970566.

[21] Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K. Analysis of computer security incidents using fuzzy logic. In Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements (24-26 May 2017, St. Petersburg, Russia). SCM 2017, 2017, pp. 369 - 371. DOI: 10.1109/SCM.2017.7970587.

[22] Vorozhtsova T.N., Pyatkova N.I. Ontology engineering threats to energy security. In: Critical Infrastructures: Contingency Nanagement, Intelligent, Agent-Based, Cloud Computing and Cyber Security Proceeding of International Workshop CI:CM/IACC/CS – 2017 . 2017. P. 24-26.

[23] Massel A.G., Tyuryumin V.O. Events ontologies and their application for description of energy security threats. In Proc. of the Microwave & Telecommunication Technology (CriMiCo), 2014 24th International Crimean Conference, 2014, pp. 443-444. DOI: 10.1109/CRMICO.2014.6959470.

[24] Markov A.S., Fadin A.A., Tsirlov V.L. Multilevel Metamodel for Heuristic Search of Vulnerabilities in The Software Source Code, International Journal of Control Theory and Applications, 2016, vol. 9, No 30, pp. 313-320.

[25] Barabanov A., Markov A., Fadin A., Tsirlov V., Shakhalov I. Synthesis of Secure Software Development Controls. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN ‘15. ACM New York, NY, USA, 2015, pp. 93-97 DOI: 10.1145/2799979.2799998.

[26] Bazaron S., Rukavichnikov A. Method specifications subject area discipline based on ontological approach. Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2014. No 5 (8), pp. 52-58. DOI: https://doi.org/10.21681/2311-3456-2014-5-43-46.