Journal of Software Engineering and Applications, **2013, 6, 23-33**
http://dx.doi.org/10.4236/jsea.2013.69A003 Published Online September 2013 (http://www.scirp.org/journal/jsea)

Critical Energy Infrastructure: Cyberterrorism Threats and Means of Protection

V. A. Vasenin

Computer Security Department, Institute for Information Security Issues, Lomonosov Moscow State University, Moscow, Russia.
Email: vasenin@msu.ru

Received July 24th, 2013; revised August 23rd, 2013; accepted August 31st, 2013

ABSTRACT

The present paper is concerned with potential cyberterrorist threats which the objects of national energy infrastructure may undergo, directions of development of counteraction means for these threats, problems arising during this development and their possible solutions. This problem field is studied by the author from scientific point of view (from point of view of computer science and information security of large systems) and this paper reflects results of such studies. Many special technical terms were omitted or substituted in order to make the statement accessible to wider range of people concerned.

Keywords: Energy Infrastructure; Cyberterrorism; Threats; Vulnerabilities; Critically Important; Information Security

1. Introduction

It is important to define what we mean by energy infrastructure before we continue to consider systematization and analysis of threats to it. We will define energy infrastructure as objects composed of a group of elements, including buildings, technical instruments and technologies, staff, and attending to solve posed tasks. Tasks are defined by functions of separate sectors of energy infrastructure, including organization of industrial and financial activities, which are directed at extraction, processing, storage and transporting of following resources:

- oil and gas resources;
- electro-energy resources;
- nuclear energetic resources.

The whole complex of listed tasks which are defined as "extractive" including extraction and primary processing can be solved in some of the countries. In other countries only a subset of such tasks is solved, such as processing, storage and transporting. These tasks are close in their aims, for which energy infrastructures are established in different countries. They are close in the ways of solving them and, as a consequence, the problems arise. But targeted purposes on organization of infrastructure activities are dictated and means of implementing them are generally controlled by state in the form of representative for these activities services and persons in each country which has such infrastructures. The reason for such attention is the fact that, unlike other infrastructures of national industrial complex, these infrastructures are critically important for state and their key forming objects are critically important.

We will include rank infrastructures as critical level if they or their elements are mentioned in the present paper.

Critically important infrastructure is a set of interacting segments and objects which compose the national industrial complex, supporting vital activities, when partial degradation or full loss of functionality can lead to impacts on components of national security or emergencies at various scales directly or within a short period of time.

Critically important information infrastructure is a composition of infrastructure elements, including computing and communication resources which provide the control of critically important state infrastructures.

Critically important components of national telecommunication infrastructure are such elements (segments, objects) of national telecommunication infrastructure which provide the control of critically important components for state infrastructures.

Critically important object is an object of critically important infrastructure, which can impact, directly or within a short period of time, on the state of national security or lead to emergencies at various scales, due to partial degradation or full loss of functionality.

Critically important segment is a composition of critically important objects united by one or several qualification characteristics such as single technological process, single department, security requirements and others.

Economical effectiveness and security of the country at international level is defined by effectiveness of single infrastructures, supporting various sectors of industrial complex. These include various industry branches, transport, science and medicine. Effectiveness depends at high degree on provision of these infrastructures with energy resources. In this meaning, absence of needed function energy resources directly impacts on one of most important components of national security—energy security.

Mutual inter-country obligations in field of acquisition and provision of one or other type of energy resources have been composed during years. Volumes and deadlines of supplies are estimated basing on planned volumes of consumption of different branches of national industrial complex. Any violation of such obligation due to different destructive factors can change composed situation. Therefore, energy security should be seen as an international, world-wide category in this context. Composed set of interacting at the conditions of aforementioned supplies and national energy infrastructures should be interpreted and defined as international energy infrastructure.

2. Key Principles, Architectural and Technological Features of Business Processes Organization

Studies which are dedicated to search of vulnerabilities and security means of controlled object for protection from destructive informational impacts as a general rule should start from analysis of environment. This is a complex, multiparametric notion for critically important objects, which required strict systematic analysis. The following can be mentioned as the basic entities of such environment:

- separate composing elements of protection object (information actives, computing and communication resources) and their architectural and technological features;
- regulations (electronic) for their support and staff, implementing these regulations;
- subjects of potentially destructive impacts and possible ways of their implementation.

Despite the certain differences basic principles of organization of retrieval (extraction or generation) and primary processing, storage and transportation of energy resources in oil and gas, electro-energy and nuclear energy sectors are equal. This fact is explained by the fact that extraction of energy resources is realized in different, locally bound places, which are spread on Russia territory. These places are defined by positions of thermoelectric stations and hydroenergy buildings, locations of nuclear stations.

Transportation and storage of energy resources in Russia is concerned with the need of effectively transporting them to potential consumers including foreign ones. This leads to necessity of creation of big, highly-developed, spread network of resource transportation. Big, supporting needed pressure compressor stations, swap stations and other objects are built in the nodes of the network for oil and gas swap. The difference of electroenergy and nuclear energy complexes lies in the absence of necessity to accumulate and store large quantities of resources. However organization of their transport and effective delivery requires building and supporting big, spread transport network. High-voltage transfer networks are built for this purpose.

The needed level of organization of all interconnected processes of extraction and primary processing of raw material, storage, transportation and resource delivery, forming a continuous technological cycle, is possible in modern conditions only on the condition of effective industrial and financial support. This support can be achieved only on the basis of clear regulations including electronic regulations of all processes of continuous technological cycle and creation of computer systems supporting automatic support of such processes.

Complex of measures in Russia from the administrative and financial positions is supported by large subjects of non-state property with large portions of government involvement. These include “Gazprom”, “Lukoil”, “Rosneft”, “Rosenergoatom” and others. Active state involvement is explained by necessity of operative control on processes in these critically important components of national industrial complex and the ability of influencing on them, using governmental resources.

Control systems of united technological cycle in different sectors of country energy complex are in the forming stage at present. New regulations supporting united technological cycle, business processes implementing them, instrumental means and systems are formed, old and updated and mastered in the structures (corporations) working in the oil and gas field. Hierarchically functioning information systems of controlling technological processes and objects are established and functioning. These systems include automatic systems of directing plants at lower levels of architectural hierarchy and these for their turn include ones controlling linear production processes and equipment. Control of supporting environment belongs to technological processes, which are implemented during extraction, processing, storage and transportation of oil and gas resources. The first stage of work on creation of automated systems is related to corporate control of financial and administrative activities.

“Rosenergoatom” is also being reformed at smaller

scale. Regulations (including electronic) are developed implementing business processes in context of united technological process of retrieving energy resources using nuclear stations, their transportation and sale. Adequate means for automatizing these processes and effective structures of controlling technological processes, administrative and financial activities are being researched. This field utilizes positive experience from adjoining fields like oil and gas and electric energy.

Taking into account aforementioned reasons a deduction can be carried that exploitation of objects from all three considered sectors of national energy complex and means of controlling them are close. Therefore, they can be categorized as one class of objects from this point of view.

Central control of technological cycle by coordination of each of composing companies is being accomplished by each of corporations using corporate and regional communication networks. The largest burden of controlling industrial processes is carried by separate plants which support technological cycle of retrieving raw material, processing it, storing and transporting energy resources. Technical and computer means for automating the processes are formed basing on open standards. This approach allows connecting new objects and updating existing without substantial modification of basic technical and program means.

Approaches to detection of threats to critical infrastructure objects, to defining means of their implementation and to development of counteraction methods are in the large way influenced by peculiarities of architecture and technology. This is the reason why tasks of classification (clasterization) of such objects are very important. Analysis of architectural and technical peculiarities of oil and gas, electric energy and nuclear energy objects shows that they all can be considered object of one class. SCADA systems are used for operative control over the state of basic technological processes in automatic systems of all energy complex sectors. Different types of controllers present at worldwide IT market and being recommended at practice can be used at lower level for controlling mechanisms. Range of information systems used for controlling administrative and financial activeties is much wider. Both information systems of middle-performance including native ones, and resource hogging complex high-performance system of R-3 SAP level can be used at this direction.

Objects of destructive information impacts on critical energy infrastructure include:

- automated control systems for technological processes at lower level of their implementation and their components (servers, SCADA in the first place, automated working places, microprocessor controllers, telemechanics services);
- information and telecommunication networks supporting automated technological process control systems;
- information objects, supporting processes of acquiring, processing and transporting energy resources (objects, supporting compressor systems, gas swap, electric supply and others).

3. Threats and Vulnerabilities. Terrorism and Cyberterrorism

Threats of destructive information impacts on critical energy infrastructure can come from:

- single criminals or criminal groups, which aim against interests of companies in bounds of corporation and corporation in general;
- terrorist groups, pursuing aims of destabilization of social, political or economical equilibrium, creating emergency of national scale.

Terrorism will be viewed as a demonstration of extremism in action, based on disagreements (national, international) of separate groups of people with state interests and institutes (in politics, social sphere, on religious or criminal basis) and directed at creating an atmosphere of fear and tension in the society, on formation of factors, directly or indirectly destabilizing state of national security with the aim of advancing requirements to governmental structures, which cannot be fulfilled on the current law basis.

Cyberterrorism is viewed as one of the terrorism directions which:

- utilizes information complexes and network segments supporting critically important from national security point systems for pursuing its aims;
- computer services are used as objects of impact.

Cyberterrorist act is a terrorist act which is performed using computer means using which can directly or potentially impact health or lives of people, large-scale destruction of material objects and other consequences affecting national security.

Destructive information impact on an automated control system (ACS) is an unsanctioned impact on single information actives, communication and telecommunication resources. Such impacts lead to violation of regular (determined by regulation) procedures of system functioning as a result of breach or total destruction of supporting information and telecommunication infrastructure. Destructive impacts can be aimed at single components of ACS, such as SCADA server, backup server, AWP of dispatcher, AWP of the specialist, local automated control system, controller, connection device and other, including supporting information actives.

Destructive information depending on the ways of impact can have the following aims:

- violation of ACS information confidentiality;
- violation of ACS information integrity (unsanctioned data modification);
- violation of ACS information resources availability.

Violation of confidentiality of ACS information, which is stored or processed by ACS, assumes disclosing information by persons, who do not have rights of accessing it. Violation of integrity is an unsanctioned modification of data. An example of destructive impact, which has aims of violating confidentiality and integrity, is a typical remote attack when the false ACS object is created.

Principally different aim of destructive impact is a violation of availability of ACS resources. Unsanctioned access to information by malicious person is not required in this case. His primary objective is making resources of the attacked object unavailable for other elements of ACS and as a consequence access to its resources and controlled technological devices impossible.

It should be noted that system can be made unavailable by means of physical or other impact at the ACS hardware and software.

The following vulnerabilities are commonly used for implementation of confidentiality threats:

- errors in access control mechanisms implementation in operating systems;
- lack of needed physical protection of communication channels;
- vulnerabilities of communication environments, allowing unsanctioned connections to data transfer channels;
- vulnerabilities of network control protocols allowing packet rerouting to the other host of the network;
- absence of secure cyphering methods.

In case of implementation of integrity threats vulnerabilities of corresponding network protocols are required. Such vulnerabilities allow malicious person to modify data on its own discretion.

Vulnerabilities, which are used for implementing availability attacks include:

- errors in access control mechanisms implementation in operating systems;
- lack of needed physical protection of communication channels;
- vulnerabilities of communication environment to potential noises.

Implementation of attack is possible in absence of efficient methods of counteracting possible distributed denial of service attacks. Such means as a rule are presented by systems for monitoring communication environment for detecting destructive impacts and counteracting.

The most important element supporting information interaction in the bounds of the ACS is a telecommunication (network) infrastructure. Network infrastructure can be viewed at three levels: communication, application and level of connection between devices and technological objects.

Communication level includes data transfer channels, a set of required communication hardware, system of monitoring and controls the state of communication hardware (including software supporting control protocols and automated system services) on the purpose of controlling availability and absence of destructive impacts.

Network application level includes software, working on ACS over control protocols of communication level (for example, web-servers, e-mail servers, DBMS, electronic documents systems).

Connection level includes controllers and other hardware, which is installed directly on the technological object and cannot be separated from that object.

Let us discuss main classes of vulnerabilities of ACS network infrastructure elements and classes of destructive information impacts connected with them. Vulnerability of network infrastructure of ACS is a property of its elements which can allow an offender in given environment disturb safe functioning regiments of system, determined by security policy. Primarily, vulnerabilities which allow a violation of confidentiality or integrity of information processed by ACS, or loss of ACS services availability, or physical damage to ACS elements should be reviewed. It is important to mention that the large part of ACS network vulnerabilities is composed of errors in software, which is responsible for supporting operating system kernel of user applications working on single hosts of automated systems. These errors usually do not depend on the purpose of the program.

4. Need for Consolidation

Analysis of destructive information impacts with the terrorist purposes on the industrial objects of energy infrastructure lets us make the following conclusions.

- The most probable scenarios of cyberterrorist attack on the objects of energy infrastructure are the ones which allow not only temporary or full loss of functionality but as a consequence (a secondary effect) create a large-scale emergency with high level of damages (material, casualties and others) and/or threat to national security.
- Implementation of such scenarios will with high probability be carried out by a group of agents, coordinating their actions, from different points of network environment, located outside of the attacked country.
- The most valuable actions from the scale of potential damage are the following:
- distributed denial of service attacks which are hard to prevent in the efficient manner;
- complex attacks, which result in overriding control on

industrial object and important technological processes, allowing it to function.

Implementation of efficient counteraction to the mentioned attack needs detailed study of environment, which influences their preparation and implementation. All aspects of cybercounteraction need to be accounted: from motivation of subjects of attack to features of counteractt ion computer means. Therefore, it seems to be important to transfer from verbal definition of cyberterrorist actions at political level to the strict formal definition and study at scientific and technological level. This fact is stated based on our own experience of carrying out studies of this phenomenon being applied to critical infrastructure objects during more than 10 years. Two-volume edition "Critically important objects and cyberterrorism" [1,2] is based on the results in this direction.

One of the features of each presented attack is the fact, that implementation scenarios assume that distributed agents actions are coordinated and prepared at several stages. This fact shows the necessity of detailed study of such scenarios, development of counteraction means at all levels of information security of critically important objects. Effective use of such knowledge and means can be achieved only on the basis of coordinated actions of all organizations involved in supporting computer systems and communication environment which can be used for preparing cyberterrorist attacks. Such consolidation is required at all stages—from analysis of possibility of different attacks, implementation scenarios, information infrastructure state monitoring to the joint actions at the stage of generating efficient counteraction measures and means.

Given the transnational origin of network environment and energy infrastructure which the environment supports an important role in creation of efficient cyberterrorist threat counteraction system is fulfilled by international force consolidation.

5. Approaches to Counteraction Organization

Reviewing approaches to organisation of protection against cyberattacks on objects of critically important energy sectors, the mentioned above belonging of objects of all three sectors to one class from information security point of view will be taken into consideration. It should also be taken into consideration that many characterizing attributes of these objects, including threats, ways of implementation and counteraction means are common for the most critically important objects of other infrastructures. Noting these considerations we will omit the belonging of object to critical energy infrastructure later where it is not required.

As mentioned before, implementation of efficient counteraction to cyberterrorism requires thorough analysis of this field, its systematization and formal definition. This definition must contain:

- ways of identification, systematization and categoryzation of protection objects as elements of one or another critical infrastructure, having it's peculiarities;
- ways of detecting protection level of the complexly organized critically important object and methods of risk assessment of destructive information impacts;
- ways (mechanisms and models, methods and means) of organizing counteraction to cyberterrorist threats at all level of complex approach to critical objects information security ensuring.

Without mentioning methods of identification, systematization and categorization the questions of defining protection level and risk management for critically important objects which are not the target of the present paper let us consider organizing the complex approach to information security ensuring. This approach assumes combining coordinated methods and actions, mechanisms, models and instrumental means at several levels of objects' information security. These levels include law, administrative, procedural and technical levels. Levels will be reviewed now, on the example of russian problems.

5.1. Law Level of Ensuring Information Security

Law level of ensuring information security of any object, including objects of critically important infrastructures is based on using:

- law norms of present legislation;
- statues of documents, developing law norms and regulating the activities of different type of organizations, state members, responsible for these activities;
- standards and recommendations, both native and international.

Laws and regulating documents create a base for all actions at other levels of information security ensuring.

Analysis of law norms established in Russia shows that the law field at the present time is not adequate to the current requirements in protecting even less important from the state point of view and less architecturally complex objects. Without mentioning the details of the inadequateness it should be noted that specifics of critically important object is referenced in a very general way in the legislation. This specifics lies in the very crude (very general) separation of information, and therefore, protection methods applied by access categories on open and confidential, including personal data, working information and state secrets. The problem field which is defined by approaches to protecting critical infrastructure objects is influenced by this separation very indirectly. As a consequence, there are no documents, regulating actions on ensuring information security of critically

important objects.

It should be noted, in view of given theses, that in the last years, with the initiative membership of Security Council of Russian Federation attention to questions of ensuring information security of critical infrastructure objects and cyberterrorist threat has gone up significantly. It reflects in discussion at different levels of government. These questions are seriously studied in scientific environment at different forums. An example of the results of such discussions is the material of International conferences on information security issues and cyberterrorism counteraction, which were made in 2005-2010 at Lomonosov Moscow State University. Attendants from USA, Germany, UK, China and other countries took paticipation there. There problems are discussed last 5 years on international forums at Garmisch-Partenkirohen in Germany and other countries. It should be noted that automated systems for controlling technological processes, industry and financial activities in the extraction, processing, storage and transportation fields discussed earlier belong to these objects.

One of the crucial factors assisting perfection of practical activities in the field of ensuring information security of any country is an effective usage of composed international system of standards and regulating this field documents. Discussion and adoption as recommendations of several international standards for using them at stages of development, supporting and enhancement of information security products is a sign of perception of importance of such actions. The most valuable from the point of view of this paper are the following documents: GOST R ISO/IEC 15408-1,2,3-2002 "Methods and means of information security", "Criteria of information security assessment", GOST R ISO/IEC 13335-1-2006, "Information technology, Part 1: Conception and management models of information security management", GOST R ISO/IEC 17799-2005, "Information technologies, Practical rules of controlling information security".

There exist a whole set of other government standards, special requirements and recommendations, which were brought to regulate such activities in Russian Federation. They include the set of "Directing documents", which were published in 1992-1994 by Federal Technical Committee by the President of Russian Federation and a number of government standards. These standards include:

- GOST R 50739-95 "Information technology. Protection from unsanctioned access to information";
- GOST R 50922-96 "Information security. Basic terms and definitions";
- GOST R 51188-98 "Information security. Software testing for detecting computer viruses".

Standards GOST R ISO/IEC 17799-2005, GOST R ISO/IEC 13335-1-2006 and such define general ways to forming policy of secure usage of object resources, which must be protected, to the assessment of protection level and risks of implementing destructive impacts on them. Regulations of these standards are mostly directed at simple from the architectural and administrative point of view objects. Measures for securing such objects at each level of complex approach to its implementation can be defined in the boundaries of single company supporting this object. In reality automated information systems are usually supported by interconnected multiple companies. Their relations to the object in general to the usage of its separate elements and actives can be different. Harmonisation of such relations, unification of requirements on enforcing security policy for the object in general is a separate and very important task. Methods of solving it are not present in the aforementioned documents. Some approaches to its solution and first results in the form of mechanisms of unification access control models in different subsystems of complex object were presented in already mentioned "Critically important objects and cyberterrorism".

Standard GOST R ISO/IEC 15408-2002 describes a systematic catalog of requirements on the information security technologies. This document defines the regulations and gives methodological recommendations on using it during definition of requirements at stages of development, supporting and enhancement, during product and information systems assessment and certification from security point of view. This document was approved in 2002. It includes requirements, which were defined in the set of analogous documents developed in different countries earlier.

It should be noted, however, that existing standards, including mentioned above, do not satisfy modern requirements, given to complex from functional and architectural points of view systems of automatization and controlling technological processes in objects, being secured, including critically important, on several positions. The GOST R ISO/IEC 15408-2002 standard as well as Directing documents consider questions of securing information from position of ensuring confidentiality, integrity of information actives, protecting software from undeclared abilities and making requirements on specific technical protection means (such as firewalls). However, this list does not cover all potentially existing technically implemented security threats to functioning automated systems, including control systems of critically important objects.

Threat classes of a different character should be taken into consideration at present time. These classes, presence of which can significantly impact the state of security of automated system, include the following:

- threats of distributed denial of service attacks;

- threats of breaching cryptographic algorithms used in subsystems of identification and authentication;
- threats of exploiting vulnerabilities and undeclared functions of other kind in programs;
- threats of confidentiality violation during user interaction with network applications such as distributed databases, web-browsers.

The mentioned regulating documents underline the necessity for partial verification of software using formal methods. Implementation of these regulations could resolve part of the threats but the practical questions are not discussed there.

Approaches given in GOST R ISO/IEC 15408-2002 and in Directing documents allow to set security aims and requirements to the facilities implementing them basing on the purpose of the analyzed object, characteristic of secured actives, threats and relation of supporting organization to them and number of other environment elements. Therefore, high level of universality is maintained during assessment of information security valuation, means and systems of such evaluation compared to other approaches preceding Directing documents and GOST R ISO/IEC 15408-2002. However, it must be noted that descriptiveness of the valuation lowers because of the loss of applicability of the valuation after the change of the tasks or the environment. Analysis of complex from functional or architectural point of view automatization and technological process control systems used in the critically important objects shows that these systems should not be viewed as typical products but as complexes functioning in permanently modifying environment. Structure and components in such system can change during its life cycle. Protection of the system depends not only on characteristics of security mechanisms of its components but at the equal scale at methods of integrating them and ways of maintaining interaction. Therefore, a model of higher level, defining "meta-requirements" on development of security requirements on the single components of the system should be created. During the study of such components, including "Automated systems, Protection from unsanctioned access to information, and Classes of automated systems", directing document can be taken as a prototype. Such components are controlled by requirements of this document, so we can get methods of protection uniformly spread among structural elements of big system. This approach takes into consideration the peculiarities of all complex distributed information systems. On the other hand it allows using positively Russian and international standards.

Taking into account outlined earlier considerations on standards and law basis of information security from point of view of applicability to automated information systems in the composition of critically important objects the utter importance of solving the appearing tasks should be underlined. The mentioned shortages of law basis of information security of critically important objects apply at the full scale to objects of national energy infrastructure.

5.2. Administrative Level of Information Security

Actions at administrative level of ensuring information security of critically important infrastructure object are directed at:

- formation of policy of secure usage of its resources;
- formation of requirements to environment and specification of protection profiles;
- at development of specifications of means used at controlled object.

Taking into consideration the aforementioned absence of required law basis and documents regulating measures of ensuring information security of critically important infrastructure objects, systematized requirements or even recommendations on organizing activity at this level does not exist at the present time. The same situation due to the same reasons exists in other countries. This fact is a negative factor which lowers effectiveness of creation of automated information systems as parts of critically important infrastructures. These shortages can be fully applied to the national energy infrastructure.

In view of present arguments development of recommendations on organizing actions at administrative level of information security of critically important infrastructure objects is very important. Approaches of application of these recommendations to single infrastructures of national industrial complex including energy which would consider specifics of these infrastructures are seen as a continuation of this work.

5.3. Procedural Level of Information Security

Procedural measures are oriented on protection of critically important objects from destructive information impacts through the complex of measures engaged by staff administering the object and its users. These measures should be directed at:

- staff management;
- physical protection;
- functionality maintenance;
- response to security breaches;
- planning of repair activities.

Mechanisms supporting interaction of separate information systems in the composition of complex critically important objects must be strictly documented with the aim of maintaining united approach of administering staff to tasks of ensuring correct and reliable functioning. Documented regulations of this level must be aimed at maintaining coordinated work of staff during develop-

ment, maintaining and testing systems in interactive mode.

Actions at procedural level of information security are regulated by mentioned GOST R ISO/IEC 17799-2005 and the number of special regulations and recommendations on technical protection of confidential information. However, implementation of such recommendations in case of complex automated information systems in critically important objects, including objects of national energy infrastructure, meets difficulties. One of the examples is ensuring high level of reliability using permanent monitoring of state of separate elements of such objects seems to be impossible without use of special systems with high level of autonomy. Greater difficulties are connected with online analysis of erroneous situations and measures of efficient reaction to them. These and other difficulties of implementing measures of information security of critically important infrastructure objects at procedural level require development of special systems with high level of automatization, containing sufficient intelligence and capable of autonomous actions in case of erroneous situations.

5.4. Technical Level of Information Security

Traditional view on technical level of information security is a complex of protection measures for information actives and other resources of controlled object. This complex includes mathematical models, software, hardware and communication mechanisms. The modern information technology market includes a large variety of technical measures for protecting information which are aimed primarily at protecting confidentiality and integrity of data. Measures for protecting from denial of service attacks are presented at much lesser grade, for protecting from distributed denial of service attacks—even less. However, architecturally and technically complex automated information systems in the composition of critically important infrastructures have high categories of importance and as a consequence high requirements on securing their resources.

Analysis of computer equipment and automated systems present at international IT market from point of view of approaches and criteria presented in GOST R ISO/IEC 15408-2002, Directing documents and other regulatory documents shows that only the small fraction of market can meet these regulations. The reason for this is the fact that these measures are oriented mostly at common user. They have very large functionality and as a consequence hold additional sources of vulnerabilities and do not open their source code. This circumstance reflects the fact that "untypical" critically important objects require corresponding "untypical" approaches to ensuring their security. As a consequence, task of developing such measures, including mathematics, algorithms and software, computing and telecommunication measures, which would take specifics of critically important objects from both user properties and higher level of security requirements, is one of the most important for the state. Development of such means, which should be carried out on regulations of responsible for the state services, should include active involvement of business. These include companies and corporations serving energy complex of the country. Acting as potential consumers of protection mechanisms and information security systems, investing into these works business should influence deadlines and work results. The following instruments can be named as basic on this direction: operating systems and mechanisms of their enhancement (implementation of interaction) to the key services of information security-identification and authentication, access control, enciphering, system state audit for functional monitoring and efficient counteraction and a number of others. Let us discuss these instruments in more detail.

5.5. Operating System Distributions

Operating system is one of basic elements supporting functioning of modern computer complexes. It is designed to manage hardware resources and organize user interface, allowing running and execution of user programs, application and system services. Operating system includes the largest part of basic mechanisms and services for ensuring security of computer complexes. Taking into account higher demands for security given to the computer systems for controlling critically important objects at early stages of their design and implementation allows using the required mechanisms of operating system efficiently. The stability of operating system and security mechanisms functioning defines the large part of protection of automated control system for critically important object.

Traditional approaches to creating operating systems often result in superfluity of software implementation. This circumstance makes auditing automated systems using such operating systems for ensuring security regulations harder. An important aspect of such superfluity are extensively complex methods of controlling security measures, for example, access control. One of the effecttive approaches to solving this problem is a multi-profile architecture of a set of distributions of operating system. This approach allows controlling superfluity without generating a large number of independently developed software complexes. Each distribution from developed set must be oriented at its own profile, assuming support for specialized services included in it.

Important role in operating systems from security point of view is occupied by basic security services such identification and authentication and access control. Im-

plementation of the former service can be enhanced in comparison to traditional approaches by implementing hardened protocols of communication between persons and algorithms using steady authentication data. Effective functioning of access control service in context of ensuring security of critically important objects requires using modern models of access control which allow automated checking of their correctness against the given set of rules (security requirements). These enhancements allow creating means of sound separation of software components in operating system and complexes where it is used.

Development of UNIX-like operating systems based on Linux kernel and open-source software can be presented as a perspective approach to creating operating systems for objects of critically important infrastructures. Stage-by-stage development of such operating systems must include full-range auditing of included software for program errors and vulnerabilities using both static code analysis (for example, basing on formal verification methods) and testing of software during its functioning. Carrying out such measures during development process and creation of program means for verifying security requirements allows making level of reliability of complex computer complexes sufficiently higher.

5.6. Monitoring of Functionality State

Support for regular, allowed by regulations, modes of functioning of computer systems for controlling critically important objects is one of the defining measures in complex of measures for ensuring information security. Hardware and software components of critically important objects including system and user services, communication services are potentially susceptible to inner and outer destructive impacts. Definition of parameters which describe the state of functionality of the object in its regular state, constant monitoring and analysis of values of these parameters allows opportunely detect anomalous situations, react to them and ensure stable and highly effective functioning of both single components and critically important object in general.

A separate service must be included in the system for controlling critically important object in order to solve the presented tasks–the system for monitoring functionality state of key elements, supporting work of the object in regular state. The primary aims of this service is the automatic detection of malfunctions in software and hardware components of the protected object, preparation of proposals and actions for localization and elimination of such malfunctions.

5.7. Active Audit Subsystem

One of the primary requirements in complex approach to information security of automated systems for controlling critically important objects is echelonment placing of technical means of protection information security. The need for this requirement is based on several reasons including:

- the lack of set of security mechanisms in operating systems adequate to modern requirements;
- existence of vulnerabilities in software implementation and system administration;
- constant flow of new errors and vulnerabilities, unaccounted at forming information security policy and at assessing risks of security threats to computer systems' functioning.

These reasons are due to human factor and objective deficiencies of security mechanisms. Complex character of protected objects, lack for scientific, methodological, technological base and means for solving these tasks are key problems.

Considering mentioned above problems a supplementary echelon of protection in current situation can be created by active audit subsystem. Such system is designed for:

- early detection of anomalous activity of computer systems due to malicious activity, errors of legal users and a number of other possible reasons;
- operative reaction to not regular situations and prevention of large damage to protected computer system.

It should be noted that active audit subsystem must be modular, integrated and highly configurable, which means the following:

- ability to efficiently add and remove new algorithms for anomalous activity detection in computer system, which will allow reacting on new types of threats and vulnerabilities;
- ability to collect and analyze in central place information from all components of a distributed system, which will allow to make correct decisions in case of distributed attack on the protected system.

Ability to make decisions in real-time manner, which will allow reacting efficiently to anomalous situations, is an additional requirement.

5.8. Tools for Analyzing Source Code for Vulnerabilities

One of the most important requirements for information security subsystem in automated system for controlling critically important objects is an inclusion of source code vulnerability analysis tools in it. High degree of attention to this problem is determined by high probability of existence of vulnerability in source code, which may be brought by errors of developers or the malicious intent. Usage of such vulnerabilities by a malicious person can result in breaching regular functioning state of the controlled critically important object an to unallowed by the

security policy escalation of privileges of the plotter on one of the system hosts, which is one of the stages of computer attack.

Existing approaches to solving this task usually demand that a group of specifically prepared experts analyses the source code manually. As a consequence the high probability of an error in expert work exists, which increases with the increase of volumes to process. This circumstance is not possible when creating automated systems for controlling critically important objects, so demand for more sophisticated solutions arises. One of such solutions is using tools for automated analysis of source code with the purpose of finding potentially vulnerable places. When using these tools, experts need to analyze only these parts of code, which are detected by automatic "analyzer". It should be underlined, that no such effective and wide-spread tools exist at the current time. However, there exist a number of theoretical approaches to developing such tools, but the practical implementation is hard to achieve for a number of reasons. One of the reasons is that used programming languages, such as C and C++, are hard to analyze. On the other hand, preliminary experiments have shown the high potential of creating effective tools for automatic analysis of programs for a number of typical vulnerabilities connected with memory access. Such tools have been tested on several systems with open code, including key elements of operating system distribution, like kernel, base applications, libraries for working with executable code, key network applications (web-server, web-client), and graphical sub-system.

5.9. Automated System for Information Analysis

Administrative staff awareness of new threats, vulnerabilities, attacks, carried out on similar by purpose and architectural and technological class objects, and methods of counteracting them plays a key role in process of protecting information security of critically important infrastructure objects. In order to maintain actual state of information, considering security of controlled objects the permanent search and theme analysis of large volumes of information is required. Usage of automated systems for theme analysis of information seems to be worthwhile in this context. These systems include configured monitoring for information sources selected by user, annotating and visualizing search results, storage of text information in different formats, engaging search, theme analysis, classification, filtration and ranging text information. Automation of listed processes will allow using actual information effectively in processes of development, modernization of software, forming rules of security policy, carrying out audit of software and hardware complexes for security regulations ensuring. Existence of such system in each of critical infrastructures, targeted at infrastructures' specifics and purposes can significantly alter level of information security of its objects.

6. Conclusions

The results of studies which connected with analysis of protection of critically important objects of energy infrastructure from destructive information impacts with terrorist intentions allow making the following conclusions.

- ✧ Problem field reflecting questions of protection of critical infrastructure objects in general, specifically, energy infrastructure is not well studied and systematized, which prevents from making reliable deductions on potential threats, means of carrying them out and approaches to counteracting them.
- ✧ Objects which are potentially vulnerable to cyberterrorist attack on the objects of critically important energy infrastructure, need protection in the first place, include the following:

- automated control system for technological processes at lower level of implementation and their components (servers, primarily SCADA servers, automated working places, microprocessor controllers, telemechanics means);
- information and telecommunication networks, supporting automated control systems;
- information objects, supporting processes of extraction (retrieval), processing and transportation on energy resources (objects, supporting compressor systems, gas swap, electric energy traffic and similar).

- ✧ Threats of cyberterrorist which impact on objects of critically important infrastructure can have the following purposes:

- confidentiality of ACS information;
- integrity of ACS information (unsanctioned data modification);
- availability (functionality) of ACS information resources, successful implementation of which separately on in composition would result in emergencies, other losses which modifies state of national security.

- ✧ Analysis of implementation means, for destructive information impacts, with terrorists aim on industrial objects of energy infrastructure, allows underlining the following features.

- the most probable scenarios of a cyberterrorist attack on objects of energy infrastructure are the ones which allow not only temporary or full loss of their functionality but also create large-scale emergency with high level of losses (material, casualties and other) as a consequence, and/or threats to national security.
- implementation of such scenarios will be carried out with high probability by group of individuals from

different points of network environment to coordinate their actions, including ones outside the country.

- from the point of view, the most important potential damages are:
- distributed denial of service attacks, which can hardly be efficiently prevented;
- complex attacks, which result in gaining control over industrial object and important maintaining technological processes.

✧ The following actions are important during development of system of measures for counteracting cyberterrorist threats on objects of energy infrastructure:

- systematic scientific research and applied works at this direction under control of government and with active involvement of business in this field;
- tight interaction of state services, companies and businesses at national level and consolidation of efforts of countries at international level;
- complex approach to ensure information security of controlled objects, assume coordinated system of means and measures, models, mechanisms, instrumental methods and law, administrative, operational and technical levels of implementation.

REFERENCES

[1] V. A. Vasenin, "Critically Important Objects and Cyberterrorism. Part I: System Approach to Counteraction (in Russian)," MCCME Publishing, Moscow, 2008, 398 p.

[2] V. A. Vasenin, "Critically Important Objects and Cyberterrorism. Part II: Implementation Aspects of Counteraction's Software Tools (in Russian)," MCCME Publishing, Moscow, 2008, 607 p.

