Evaluation of damage to objects of critical information infrastructure under the influence of destructive electromagnetic radiation based on hierarchical rank approach

Alexey A Dvilyanskiy¹ and Mikhail Y Rytov²

¹ Academy of Federal Guard Service the Russian Federation, 35, Priborostoitelnaya Street, Oryol city, 302015, Russia
² Bryansk State Technical University, 7, Boulevard 50 let Oktyabrya, Bryansk city, 241035, Russia

E-mail: advil@mail.ru, rmy@tu-bryansk.ru

Abstract. In article is presented hierarchical rank an approach to assessing damage to objects of critical information infrastructure under the impact of destructive electromagnetic radiations, providing formalisatjon the specified objects and the account of their criticality with use of the conceptual scheme within the limits of expert system, and also distribution of influences of the opponent, with their subsequent classification as destructive electromagnetic attacks. One of the main tasks for the objects of CII facilities that provide vital public functions is the analysis and assessment of threats and consequences from exposure of electromagnetic impulses (EMI) of artificial origin, which can be used to disorganize CII control systems, suppression of technical means of protection (TMP) of specially protected objects, as well as causing significant economic damage.

Introduction
Regular development of the information and communication component, including the CII, in the direction of complicating and expanding the topology of Information and Telecommunication networks (ITN) of various kinds, ensuring their interaction and saturating them with computing equipment (CE) with strict requirements for weight and size indicators, which ultimately will lead to an increase in the number of threats to CII objects and a decrease in energy indicators in terms of their functional damage [1].

Materials and methods
The urgency of the task under consideration related to the assessment of the damage caused to the above objects is predetermined by the possibility and facts of exposure to them by destructive electromagnetic radiation (DEMR) with the aim of disrupting their functioning to achieve the requirements put forward by organizations of extremist and terrorist persuasion.

The damaging effect of DEMR is manifested in the destruction, melting and burning out of the metallization of the contact tracks, and as a result, the degradation of the parameters of the structural...
elements of the microelectronic component base of the CE, which makes it impossible to ensure continuity in the provision of information services to consumers.

A number of domestic and foreign experts have determined the following priority of the collapse of the main sectors of the country's critical infrastructure as a result of this impact: electricity (power supply systems); communication and telecommunication systems; banking and finance; fuel (systems of oil and gas supply and processing); transport infrastructure; food and water supply; emergency services (emergency response); commercial space systems.

The electric power sector (EPS) of the infrastructure on which the functioning of other sectors and industries depends is the most exposed to DEMR. Failures in this sector often have serious consequences due to the cascade effect, inevitably affecting other sectors and their infrastructure — power transmission networks distributed over a wide area are difficult to protect objects of the power grid. It is predicted that EMI will lead to a reduction in load power due to induced short circuits (destruction of insulators of power transmission lines and other effects), which, in turn, may cause overheating, explosion of transformers and the occurrence of fires.

**Literature Review**

Special attention is paid to this problem, as evidenced by a significant number of scientific works related to the prediction of the state of CII objects in non-calculated conditions - Myrova L.O., Kechiev L.N., Hafner Ch., Tak Ch., Buslenko N. P., Kuprienko V. M., Sokolov A. A., Parfenov Yu. V., Gekov V. V., Khorev A. A., etc.

As a complex spatially distributed technical system, the CII is a functionally connected set of hardware and software for transmitting, receiving and processing information [2-4].

An important requirement for CII is to maintain the specified characteristics of information security: confidentiality, integrity, availability of the information component in terms of the possible effects of the offender. In CII, in this connection, the main purpose of providing information security is the protection of information (PI) and network infrastructure from accidental and deliberate impacts of natural or artificial nature, fraught with damage to the system and users of information, which is achieved by a complex use of the whole set of organizational, legal, engineering and technical, hardware and software means of protecting information, based on the use of cryptographic and other methods of protecting the information sphere of CII, continuous control of the effectiveness of measures to ensure information security, which includes [5-7]:

- Protection of the integrity and authenticity of distributed information resources.
- Ensuring the confidentiality of stored, processed and transmitted information.
- Ensuring the authorized and timely access of legitimate users to information resources.
- Protection against powerful electromagnetic pulses of ultra-high frequency (EMP microwave).
- Protection of information from leakage through technical channels formed by spurious electromagnetic radiation and pickups (SEMRP).
- Support of the trusted system-wide software environment of informational automatized systems.

Such threats as cyberterrorism, which means a politically planned unlawful attack motivated by international or national groups or the threat of an attack using information technology against computers, networks and information stored inside them (hacking site, disabling any computer system), aimed at causing harm to life or significant economic damage, carried out in order to intimidate or coerce government or the population to promote political or social aspirations are used [1, 7, 8].

Various methods of attack are aimed at different vulnerabilities in computer systems CII and include various types of weapons, which are currently used by terrorist groups.

In the group of factors determining the forms and methods of conducting modern terrorist operations, let us emphasize a shift in focus to the area of information-rich management systems for various industries and the state. The tendencies of development of these factors reveal a close causal
relationship, the elements of which are currently highlighted in a special subject area, known as the Cybernetic threat [1, 9].

In accordance with the classification, on the basis of international experience and research on countering cyber-terrorism, impact actions on CII are divided into:

1. Cyber-attacks on computer systems, including the use of malicious programs that are used as weapons to infect computers by exploiting software gaps, system configurations or weaknesses in ensuring the organization's computer security and having the goal of disrupting the equipment, change of control over operations, or damage or theft of stored data, including information retrieving through PEMI and pickups.

2. Electromagnetic attacks (EMA), which imply the use of electromagnetic energy as a weapon, mainly EMP, for overvoltage in CII computer systems. Means that implement electronic attack are electromagnetic pulse generators (EPG), which in the aspect of terrorist threat acquire the character of a weapon, or more precisely, an electromagnetic weapon (EMW), which affects technical systems with high-intensity electromagnetic fields in the form of high-frequency radiation (microwave and EHF). ranges), has an area of action of the order of tens of kilometers, as well as highly sensitive spectrum analyzers, in order to obtain unauthorized access to information on the SEMR. In the future, EMW is considered to the means of force during the conduct of terrorist actions and may become one of the main types of damaging effects in the near future, with the help of which the following tasks are solved:

- Disorganization of government, military and civilian control systems.
- Suppression of technical means of protection of specially protected objects.
- Causing significant economic damage.

Thus, with regard to the security of CII facilities, there are two sides of the threat: the first is the theft of protected information, the second is the destruction of the information resource, which manifests itself both in the destruction of information and in the malfunctioning realized by destructive electromagnetic interference.

Let us consider the method of forming characteristic scenarios of cyberterrorism effects on the space of CII, carried out in two stages, in each of which each section of the scenario is assigned a set, elements of which, in turn, can be other sets [1].

At the first stage the sets are formed:

- Critical elements of the object.
- Characterizing the facility’s security features located on the intruder’s route to the critical element. Each element of this set describes the types of means used, their quantity, location on the general plan, etc.
- Characteristics of threats, vulnerabilities and violators, as well as methods of actions of the offender.

At the second stage the synthesis of the full set of characteristic EMA scenarios is carried out through the complete enumeration of all possible combinations of elements of the formed sets.

An arbitrary scenario of terrorist attacks on objects is also possible, which is a sequence of n components containing a description of the object, a description of the offenders and a description of their actions.

Before proceeding to the assessment of risks and damage caused to the facilities of the CII, let us present an expert system that assumes taking into account the following characteristics of the facilities of the CII under the conditions of the effects of the EMA [7-9]:

1. «degree of criticality» and the value of the assets of the object;
2. model of threats to the object from the side of potential violators («the model of the violator»);
3. security functions of the facility CII;
4. security policy (SP), defining a certain «model of the intruder» and determining the degree of effectiveness of the security functions in countering the threats to the object;
5. architecture (internal structure) of the object.

In order to formalize the objects within the expert system, a hierarchical rank approach (HRA) is proposed. It envisages the use of a tree-like structure of entities – ranks as a group of discrete objects connected by varying degrees of commonality of properties and attributes and thanks to this gives grounds for assigning them a certain hierarchical rank category. To each considered rank there is a separate component of the CII and some type of it, which allows to group objects with the same similar (similar) properties and functionality. The objects corresponding to the leaf nodes of the tree are root (all-encompassing) ranks, that is, higher ranks.

Each rank has a set of attributes that include the following information about the protected object [13]: identifier, structure, functionality, «significance level» in relation to the CII, value of assets (in numerical terms), possible threats and a list of preconditions required for implementation (for example, the attacker has local access to the object), security policy and «multiple access» (as a subject of the CII) to other objects.

To the number of objects CII and their subspecies we will assign the following:

- Subsystems (components) of the facilities of the CII: workstation - server, network and specific equipment, premises, workplace, its configuration and parameters.
- Operating systems (OS, Windows family, Linux) and installed software (software), ensuring the operation and execution of the assignment tasks.
- Software for monitoring the state of functionality of the main hardware and software (MTA) and auditing the facilities of the CII for the detection of destructive information impacts and rapid response.
- Regulation of the functioning of the facilities of the CII.

Let us consider an approach to the formation of a dynamic model based on the RPI, which can be used as the basis for the operation of the system for analyzing the protection of objects of the CII in the EMA conditions. For each individual object, such a model should be formed taking into account its features and environmental conditions, including the formulation of the problem.

The following attributes will be valeted to the inems identifying CII objects:

1. Attribute «security level of CII objects» (L): L = 1 - minimum baseline; L = 2 - medium; L = 3 - high and L = 4 - maximum.
2. Attribute «security functions of CII objects»:
   - requirements and assumptions on ensuring the security policy adopted at the facility, with ensuring the correct union (integration) of policies of various sub-systems as part of the CII facilities;
   - physical and logical protection of objects, equipment and channels between the subsystem-mi objects CII;
   - monitoring the status of available services of the facilities of the CII, provided by the staff mode of operation.
3. Attribute «threats inherent to this CII object (from the EMA)»:
   - failure - functional and / or catastrophic equipment failures (multiplexers, routers, CE, life support systems, power supply, etc.);
   - complete loss of functionality (lack of access to the assets of the main services of CII facilities);
the threat of violation of the staffing regulations for the interaction of individual components of CII objects with each other and with external information systems;

- the threat of violation of the integrity of information assets;

- the threat of breach of confidentiality of information assets in relation to external and internal subsystems;

- device compromise – the attacker gains partial or full control over the device with the ability to gain access to the transmitted data;

- personnel erroneous actions - an authorized employee may incorrectly configure the object protection system, violating the security policy.

4. Attribute «the state of the CII object, during the implementation of EMA», as a consequence of the realization of threats.

We set the following notation: \( \alpha_1, \ldots, \alpha_n \) a list of all possible values of the taxonomy attributes for all objects of the CII.

The state of \( Cd_{(x,y)} \) CII objects will be called a vector \( \bar{\alpha}_s = (\alpha_1, \ldots, \alpha_n) \), where:

\[
\bar{\alpha}_s = \begin{cases} 
1, & \text{if the value of the corresponding attribute is } \alpha_i; \\
0, & \text{other.} 
\end{cases}
\]

The functioning of the specified expert system should be preceded by the formation of a table containing information on the dependencies of actions taken in the course of implementing threats to CIA facilities, on functions aimed at ensuring the security of these objects, proposals on security measures and, possibly, some other attributes, some of which are presented above (Table 1). In the model under consideration, these dependences are determined by the set of weights of various attributes that indicate the «degree of influence» of the attribute value of the CII objects on the possibility of implementing EMA.

**Table 1.** Information about the dependencies of actions taken in the course of the implementation of threats to objects.

| Name of the indicator | Indicators |
|-----------------------|------------|
| Rang of CII objects, \( s = 1, \ldots, n-1, n \) | \( Rng_s \) |
| Security level of CII objects, \( j = 1, \ldots, 4 \) | \( L_j \) |
| Attribute values | \( \alpha_1, \alpha_2, \ldots, \alpha_n \) |
| Weight of attributes inherent to the objects of CII(Thr) | \( w_1^{Thr}, w_2^{Thr}, \ldots, w_n^{Thr} \) |
| Condition of CII objects | \( Cd_{(0,0)}, Cd_{(1,1)}, \ldots, Cd_{(x-1,y-1)}, Cd_{(x,y)} \) |

The table uses the following notation: \( Rng_i \) - rank of the CII object; \( \alpha_1, \ldots, \alpha_n \) – a list of all possible attribute values; \( w_s^{Thr} \in W \) - «weight» of the corresponding attribute value of the CII objects in relation to the threat Thr. This table is necessary to describe the dynamic model of the behavior of CII objects under destructive influences.

We assume that for each cyber threat Thr there are a couple of functions:

- \( F_{Ch} : [0,1] \) - the function sets the probability of cyber threat implementation in a given state of CII objects;

- \( H_{Cd} : Cd_{(x,y)} \rightarrow Cd_{(l,i)} \) - the function sets the rule for moving the CII objects to the next state according to its current state.
In addition, we will assume that a function is defined as $D_c : \mathbb{R} \rightarrow [0, 1]$, which, according to this condition, determines the amount of damage inflicted to the facilities of the CII, if this state is achieved.

We describe the work of the dynamic model using the functions $F_{Cth}, H_{Cn}, D_c$.

Each attribute affects the probability $p_{x,y}$ of an object moving to the next state according to its current state, regardless of the values of other attributes. In this case $W = \mathbb{R}^+$ and $F_{Cth} = \prod_{i=1}^{l} \tilde{a}_i W_i^{Thr}$.

The implementation of each $Thr$ threat provides one new access to the resources of CII objects, characterized by non-zero vector positions $\tilde{e} \in \{0, 1\}^n$. That is $H_{Cn}(\alpha_1, \ldots, \alpha_n) = (\alpha_1 \vee e_1, \ldots, \alpha_n \vee e_n)$.

The size of damage to objects of the CII under the conditions of exposure to ECA is characterized by certain attribute values, such as, for example, the functional impairment of the SEDT of objects and $l$ or the attacker's access to confidential information:

$$D_c(\alpha_1, \ldots, \alpha_n) = \begin{cases} N \text{ damage units, } & \text{if } \alpha_s = e_s = 1, \text{ for some } s; \\ 0 & \text{other.} \end{cases}$$

The methodology for assessing the risks and damage of CII facilities under the impact of DEMR is based on the work of the dynamic model and the marked transition system, the states $Cd_{(x,y)}$ of which correspond to the states of the facilities of CII under destructive influences, and the transitions to the steps of potential cyber-attacks.

The first stage of the methodology involves the presentation of the source CII object in the form of a hierarchy of taxonomy elements and the assignment of values for all attributes (setting the structural model of CII objects). The result of performing the work at the initial stage will be a vector $\tilde{c}Cd_0 \in \{0, 1\}^n$ showing the initial state of the CII objects in the transition system.

At the 2nd stage, for each unprocessed state $Cd_{s(x,y)} = (\alpha_1, \ldots, \alpha_n)$ with a condition $D_c(Cd_{(x,y)}) \leq \Delta$ (where $\Delta$ is the upper threshold of the damage value, at which it is not considered to be essential for the functioning of the facilities of the CII), for each cyber threat $Thr$ the state probability value $H_{Cn}(Cd_{(0,0)} \rightarrow Cd_{(1,1)}) \tilde{a}_i$ is calculated.

If it turns out that $p_{x,y} \geq \sigma$ (where $\sigma$ is the lower threshold for the probability value of the state of CII objects, at which it is still attainable), then in the current transition system a new state of the CII objects is generated, which is also determined by $H_{Cn}$ the probability value $p_{x,y}$. If the transition system $H_{Cn}$ already exists, the new state is not generated, but only the probability of its occurrence is recalculated.

This sequence of steps is repeated as long as it is possible to generate new states of objects of the CII. At the end of the second stage, the transition system will be a labeled, oriented graph in which simple paths leading from the initial vertex correspond to possible scenarios for the development of the attack.

At the third stage, a picture of the risk of adverse events for the source facility is built. By risk $R$, we mean the value characterizing for each resulting scenario of an attack of a type $Att_0 \rightarrow Att_1 \rightarrow \ldots \rightarrow Att_k$, the possibility of inflicting some damage on the CII objects, and defined as the product of the probability $p_{x,y}$ and $D_c(\alpha_1, \ldots, \alpha_n)$:

$$R = D_c(\alpha_1, \ldots, \alpha_n) \cdot p_{x,y}. $$
Results

The approach proposed in the article will allow defining a list of possible scenarios for cyber-attacks, assessing the degree of danger (risks) of implementing possible destructive information impacts on facilities of the CII in the form of EMA, identifying possible weaknesses in the system of protecting these objects in order to eliminate adverse events, followed by determining adequate proposals to improve the security policy of data objects.

References

[1] Dvilyanskiy A A and Ivanov V A 2019 Methodology for assessing integrated security of information and communication systems from the effects of destructive electromagnetic radiation (Orël: Academy FSO of Russia)
[2] Kruk B I 2004 Telecommunication systems and networks: studies ed V P Shuvalov (Moscow: Hotline-Telecom)
[3] Ustinov G N 2000 Fundamentals of information security systems and data networks (Moscow: SINTEG)
[4] Kechiev L N and Stepanov P V 2005 EMC and information security in telecommunication systems (Moscow: Tekhnologii Publishing House)
[5] Devyanin P N 2000 Theoretical foundations of computer security (Moscow: Radio and communications)
[6] Novikov A A and Ustinoc G N 2003 Vulnerability and information security of telecommunication technologies (Moscow: Radio and communication)
[7] Dvilyanskiy A A e al 2007 Ensuring the security of information and telecommunications facilities when exposed to an electromagnetic pulse Proceedings of the Second International Scientific Conference on Security Issues and Counter Terrorism. Moscow State University, 2006
[8] Klimovsky A A, Bolshakov F M and Puchkov F M 2007 Objects of critical infrastructures: security analysis and risks of successful implementation of computer attacks Proceedings of the Second International Scientific Conference on Security Issues and Counter-Terrorism pp 317-35
[9] Vasiliev V 2013 Information security of critical objects PC Week Review: IT security
[10] Pozharsky V N, Lesnikh V V and Ivanov E A 2007 Development of models and methods for managing the security of critical objects of the fuel and energy complex Proceedings of the Second International Scientific Conference on Security Issues and Counter Terrorism pp 628-35