COUNTERING CYBERATTACKS ON THE ENERGY SECTOR IN THE RUSSIAN FEDERATION AND THE USA

VICTOR SHESTAK,

Moscow Academy of the Investigative Committee of the Russian Federation (Moscow, Russia)

ALYONA TSYPLAKOVA,

MGIMO University (Moscow, Russia)

https://doi.org/10.21684/2412-2343-2023-10-4-35-52

The USA leads the way in the Global Cybersecurity Index, in particular 1st place in 2015, 2020 and 2nd in 2017, 2018. Researchers are interested in examining their prevention of cyberattacks as one of the main cybersecurity threats, since Russia takes only 5th place since 2020. Provided the authors underline neglecting the principle of organized response to crime, the paper examines the pros and cons of countering cyberattacks in the U.S. energy sector and compares it with the Russian Federation. The researchers have found the American strategy is based on standardization and various platforms on the grounds of so-called security in depth, while Russian approach is wider, but demands for more details and miscellaneous mechanisms to share experience. Comparing the cybersecurity plans and strategies for U.S. energy facilities, the authors note that the U.S. specialists neglect physical safety in comparison to Russia. The diversity of bodies with vague powers is a con of the American system that the Russian Federation is trying to avoid, but the interaction between government and private representatives is stronger in the United States of America.

Keywords: USA; Russian Federation; cyberattacks; preventive measures; energy sector; response.

Recommended citation: Victor Shestak & Alyona Tsyplakova, *Countering Cyberattacks on the Energy Sector in the Russian Federation and the USA*, 10(4) BRICS Law Journal 35–52 (2023).

Table of Contents

Introduction

Surveys show that energy companies are exposed to cyberattacks on a daily basis. The U.S. Department of Energy reports that between 2010–2014 there were 150 successful attacks targeting critical infrastructure in the power and nuclear industries.[1] In particular, 245 cyber intrusions were successful in 2014. Half of them were rated as advanced.[2] In 2015 a cyberattack caused more than 27,62 million of U.S. dollars damage to an average energy company. In 2015–2016 35% of all cyberattacks were aimed specifically at the energy sector.[3] Nowadays, there are 24 cyberattacks on the U.S. energy sector per day.[4]

As for the Russian Federation, there is no precise data on cyberattacks on energy sector, but in 2020 over 120,000 cyberattacks on Russia's critical infrastructure were carried out. According to Rostelecom-Solar Report 2021, one in 10 critical information infrastructure entities were compromised by malwares. In 2021–2022 there was a dramatic rise of cyberattacks in general and 15% of cases were targeted repeatedly. Positive Technologies and Cisoclub data shows that in 2019 almost every third attack

---

1 Steve Reilly, *Records: Energy Department Struck by Cyber Attacks*, USA Today, 9 September 2015 (Jul. 20, 2023), available at https://www.usatoday.com/story/news/2015/09/09/cyber-attacks-doe-energy/71929786/.

2 Advanced persistent threat is a type of a large-scale cyberattack that mobilizes significant financial and technical resources and can last for several years. The goal is usually determined and studied in advance.

3 Patricio Portillo et al., *Smart & Safe: State Strategies for Enhancing Cybersecurity in the Electric Sector*, White Paper, National Governors Association, 19 April 2017 (Jul. 20, 2023), available at https://www.nga.org/wp-content/uploads/2019/04/NGA-Smart-Safe-State-Strategies-for-Enhancing-Cybersecurity-in-the-Electric-Sector.pdf; Ponemon Institute, *2016 Cost of Cyber Crime Study & the Risk of Business Innovation* (October 2016) (Jul. 20, 2023), available at https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf.

4 Pedro J. Pizarro & Tom Kuhn, *The US power sector has prevented millions of cyberattacks in 2020 – that takes 24/7 commitment*, Utility Dive, 29 October 2020 (Jul. 20, 2023), available at https://www.utilitydive.com/news/the-us-power-sector-has-prevented-millions-of-cyberattacks-in-2020-that-t/587949/.

on energy facilities resulted in confidential information leaks and 2 years later their number increased almost 150%.[5] The attacks' number on the Russian public sector roughly doubled or tripled compared to a year ago and reaches 403.[6] In comparison to the U.S. energy sector, the Russian one is primarily public, that's why researchers may also base on its statistics.

One shall take into account that consumers are also suffering. For example, a cyberattack targeting smart inverters that control the flow of electricity in household solar systems could overload parts of the grid, damage critical equipment and subsequently cut off electricity supplies to both business and households.[7] Appropriating operational-technology systems, their modifications and billing fraud with wireless smart meters can lead to a halt in power generation through wind turbines.[8] Disabling or controlling dam locks or substations used to store water and generate electricity can result in destruction and injuries of citizens.[9]

1. Methodology

This study is a description investigation of countermeasures against cyberattacks in the U.S. and Russian energy sectors. It is primarily based on genetic, systematic-functional systematization and comparison methods. Data on key mechanisms that are described in Multi-Year Plan for the Energy Sector Cybersecurity 2018 of the U.S. Department of Energy is represented as qualitative research.

2. Similarity and Distinction of Russian and American Approach to Security and Countering in General

To begin with, it is worth mentioning that the United States of America ensures primarily cybersecurity rather than information one in comparison to the Russian

---

[5] Количество кибератак на бизнес и государственные структуры выросло в России в 7 раз // Cisoclub. 24 августа 2022 г. [The number of cyberattacks on businesses and authorities in Russia has increased sevenfold, Cisoclub, 24 August 2022] (Jul. 20, 2023), available at https://cisoclub.ru/kolichestvo-kiberatak-na-biznes-i-gosudarstvennye-struktury-vyroslo-v-rossii-v-7-raz/.

[6] Безопасность критической информационной структуры РФ // TAdviser. 16 сентября 2022 г. [Security of critical information infrastructure of the Russian Federation, TAdviser, 16 September 2022] (Jul. 20, 2023), available at https://www.tadviser.ru/index.php/Статья:Безопасность_критической_информационной_инфраструктуры_РФ.

[7] Kelsey Misbrener, *Cyberattacks threaten smart inverters, but scientists have solutions*, Solar Power Installation, 30 April 30 (Jul. 20, 2023), available at https://www.solarpowerworldonline.com/2019/04/cyberattacks-threaten-smart-inverters-but-scientists-have-solutions/.

[8] Tucker Bailey et al., *The energy-sector threat: How to address cybersecurity vulnerabilities*, McKinsey & Company, 3 November 2020 (Jul. 20, 2023), available at https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities.

[9] Gay P. Denileon, *The Who, What, Why, and How of Counter Terrorism Issues*, 93(5) Am. Water Works Assoc. J. 78 (2001).

Federation. The former's strategy considers security in depth, while the latter's is only developing in terms of technological sovereignty and a broader approach to so-called critical information infrastructure entities.[10] Such two forms of systemic effect on cyberattacks against energy facilities as prevention and suppression are implemented in the United States. By contrast, in Russia precaution measures prevail.

Historically, in both states there was an emphasis on the concept of law enforcement prevention with criminal repressions, building up the police force, strengthening the prison system, which had a short-term effect. Today, the dominant approach is community prevention which implies measures to reduce victimization and forecasting as core actions.[11] For the time being, the preventive activity involves the model of public institutions, the model of impact through the environment and the model of individual safety.[12]

American legislators and researchers focus on information-analytical and forecasting work, interaction between government officials and energy companies, as well as change of environment in order to hinder or eliminate the criminal use, weaken or neutralize the criminogenic factors. One may conclude that they neglect the third pattern unlike our domestic policy-makers who conventionally prefer taking care of physical security.

3. Comparison of Preventive Measures in Two States

The set of preventive measures consists primarily of standardizing the operation of critical infrastructure facilities. Russia has more generalized standards, inter alia referencing IEC and ISO standards so-called GOST and Technical Regulations of the Eurasian Economic Union and the Commonwealth of Independent States. It is worth mentioning the Federal Service for Technical and Export Control of Russia as an agency of Ministry of Defence with its territorial bodies that is responsible for setting up regulations for critical-information-infrastructure security, inter alia minimum requirements, and handling a register on entities to follow its orders. Non-compliance results in fines up to 500,000 rubles levied by state authorities on the basis of the Code of the Russian Federation of Administrative Offenses with amendments dated May 2021.

---

[10] Arnault Barichella, *Cybersecurity in the Energy Sector: A Comparative Analysis Between Europe and the United States*, Études de l'Ifri (February 2018) (Jul. 20, 2023), available at https://www.ifri.org/en/publications/etudes-de-lifri/cybersecurity-energy-sector-comparative-analysis-between-europe-and.

[11] *Евсеев А.В.* Зарубежный опыт организации криминологического обеспечения деятельности правоохранительных органов // Вестник ВИПК МВД России. 2020. № 2(54). С. 90–97 [Andrei V. Evseev, *Foreign Experience of the Organization Criminological Security Activities Enforcement Agency*, 2(54) Bulletin of the Advanced Training Institute of the MIA of Russia 90 (2020)].

[12] *Григорян В.К.* Предупреждение преступности в высокоразвитых зарубежных странах // Актуальные проблемы российского права. 2012. № 4. С. 272–279 [V.K. Grigoryan, *The Crime Prevention in Highly-Developed Foreign Countries*, 4 Actual Problems of Russian Law 272 (2012)].

In the USA standards and mechanisms are more diverse and specific in terms of cybersecurity, in particular, in the energy sector. First of all, it includes the activities of the non-profit North American Electric Reliability Corporation (NERC). It was appointed responsible for standardization in the field of electrical networks at the federal level in accordance with Energy Policy Act of 2015. The first version of the Critical Infrastructure Protection Standards was adopted in January 2008. The Standards have been updated annually to cover, e.g., controls, personnel training, physical security of transmission sites of the power system, and recovery plans for computer systems. However, back in 2014, in accordance with Presidential Policy Directive No. 13636 "On Improving the Cybersecurity of Critical Infrastructure" of 12 December 2013 (PPD-21), the National Institute of Standards and Technology of the U.S. Department of Commerce (NIST) developed its first Cybersecurity Program.[13] It is divided into three themes: key actions, 4 levels of implementation and a profile for a goal roadmap and comparison of current and ideal conditions. It also provides its own standards for each function.[14]

Meanwhile, the Office of Cybersecurity, Energy Security and Emergency Response (CESER) together with the U.S. Department of Energy, the U.S. Department of Homeland Security and the U.S. Nuclear Regulatory Commission promote the implementation of voluntary standards in order to minimize the risks of cyberattacks and coordinate dialogue with the private sector. In order to apply the Cybersecurity Program and receive feedback from users, the Critical Infrastructure of the Cyber Community Voluntary Program (C^3VP or C^3) was developed and maintained by the National Infrastructure Coordinating Center (NICC), which is a part of the National Operations Center of the U.S. Department of Homeland Security.[15] It is worth mentioning that there is no sole way to use it and there are no sanctions for non-use. In addition, the C^3 program encourages participating in collaboration forums, obtaining access to free technical assistance, tools and resources to strengthen cyber risk management capabilities and helps carry out cyber risk management responsibilities consistently and properly.

Secondly, the U.S. Department of Homeland Security Transportation Security Administration (TSA) also obtains the power to issue pipeline security standards and it issued previously voluntary guidelines in March 2018 and updated in April 2021.[16] A month after the cyberattack on the Colonial Pipeline (7 May 2021), the TSA first issued mandatory standards preliminarily approved by the U.S. Department of

---

[13] Presidential Policy Directive 21, U.S. Department of Energy (Jul. 20, 2023), available at https://www.energy.gov/ceser/presidential-policy-directive-21.

[14] Benjamin A. Powell & Jason C. Chipman, *Getting the Deal Through: Cybersecurity 2021* (2021).

[15] CISA, *C3 Voluntary Program Frequently Asked Questions* (Jul. 20, 2023), available at https://us-cert.cisa.gov/sites/default/files/c3vp/sltt/CCubed_VP_FAQ.pdf.

[16] TSA, *Pipeline Security Guidelines* (April 2018) (Jul. 20, 2023), available at https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.

Homeland Security for certain pipeline operators as a part of the Security Directive Pipeline 2021-01.[17]

Although NERC is entitled to impose fines up to 1 million of the U.S. dollars per day for non-compliance with standards.[18] In 2016, on February a company was charged with 1,7 million of the U.S. dollars for 36 violations. 21 violations were a high danger for BPS due to low physical security. On October there was another fine (1,1 million of the U.S. dollars) due to insufficient security of physical access to the control systems.[19] Still, the practice is too extraordinary and rarely takes place. Comparing to the Russian Federation, American regulation framework is more rigid, though it is unconventional for non-profit organization to punish.

A set of preventive measures also contains information, experience and technology exchange programs and training. Site inspections are annually carried out by Intervention teams and every two years joint studies of federal and local authorities and the private sector are held with simulated cyber incidents on the bulk power system (the Grid Security and Emergency Response Exercise or GridEx). The U.S. Department of Homeland Security has been conducting Cyberstorm since 2006.[20] The importance of participation in such events has been emphasized. For instance, there were more than 120 participants in New York in 2014 and more than 2 thousand participants in 2020.[21] Also, there are monthly seminars within the framework of the Energy Sector Security Consortium Inc. (EnergySec) and an annual expert exchange conference to update standards.

In this respect Russia is not falling behind and, for the time being, the authorities are actively engaged in collaborative activities. For instance, in 2021 Ministry of Energy and Rostelecom organized joint cyber training in the electric power sector.[22] However, one may notice a lack of interaction between government agencies and the private sector. In order to coordinate efforts, it would be appropriate to carry out relevant activities in the strongholds at the National Cyber Training Area. Seven

---

17 Catherine D. Little et al., *Mandatory Homeland Security Cybersecurity Directive*, Pipelaws, 17 June 2021 (Jul. 20, 2023), available at https://www.pipelaws.com/2021/06/mandatory-homeland-security-cybersecurity-directive/.

18 Barichella, *supra* note 10.

19 NERC Increasing Penalties for Fundamentally Failing to Comply with Cyber Standards, Lexology, 17 November 2016 (Jul. 20, 2023), available at https://www.lexology.com/library/detail.aspx?g=b992afce-5d8f-4fcd-8852-828435873f27.

20 Cyber Storm 2020: National Cyber Exercise, CISA (Jul. 20, 2023), available at https://www.cisa.gov/cyber-storm-2020.

21 Portillo et al., *supra* note 3.

22 Минэнерго и «Ростелеком» провели совместные киберучения в электроэнергетическом комплексе // Министерство энергетики РФ. 6 июля 2021 г. [Ministry of Energy and Rostelecom conducted collaborative cyber exercises in electricity sector, Ministry of Energy of the Russian Federation, 6 July 2021] (Jul. 20, 2023), available at https://minenergo.gov.ru/node/20932.

centers have already been launched as part of the federal project called Information Security of the national program called Digital Economy.[23]

The first Multilateral Information Sharing Agreement on security was adopted in 2015 and required the authorities in the field of defense, health, justice, intelligence and energy to work collaboratively on information sharing capabilities, inter alia in terms of cybersecurity.[24] A military-industrial base has been established on the grounds of the voluntary cyber and information security program. It ensures communication between corporations and the U.S. Department of Defense by reporting cyber intrusions and reviewing plans. Every energy sector has its own Information Sharing and Analysis Center (ISAC), in particular oil & natural gas, electricity and downstream natural gas. They provide shared intelligence on cyber incidents and vulnerabilities and best practices to enhance cybersecurity in the energy industry.[25] The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) also aids protection and develops analytical products combining threat assessments and incident reports and strategies. For instance, Target Selection Matrix identifies the potential prone to specific hazards and scenario catalogue in order to enhance supervision over the safety of the facility.[26]

While the Russian Federation issued the Doctrine of Information Security adopted in 2016 with general provisions and principles and has not updated it in terms of cybersecurity and precise mechanisms, The U.S. Department of Energy Multi-Year Plan for the Energy Sector Cybersecurity of 2018 is more detailed and covers the majority of present mechanisms (*see* Table 1[27]).

---

[23] Чернышенко: в РФ появляется два опорных центра национального киберполигона // Национальные проекты РФ. 4 марта 2022 г.[Chernyshenko: two reference centers of the national cyber training ground appear in the Russian Federation, National Projects of the Russian Federation, 4 March 2022] (Jul. 20, 2023), available at https://национальныепроекты.рф/news/chernyshenko-v-rossii-poyavyatsya-dva-opornykh-tsentra-natsionalnogo-kiberpoligon.

[24] CISA, *Federal Multilateral Information Sharing Agreement* (January 2019) (Jul. 20, 2023), available at https://www.cisa.gov/sites/default/files/publications/Federal%20MISA%20Oct2019%20Final_0.pdf.

[25] Powell & Chipman 2021.

[26] *Белоус А.И.* Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения: практическое пособие [Anatoly I. Belous, *Cybersecurity of Fuel and Energy Complex Facilities. Concepts, Methods and Tools for Ensuring*] (2020).

[27] U.S. Department of Energy, *Multiyear Plan for Energy Sector Cybersecurity* (2018) (Jul. 20, 2023), available at https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf.

Table 1: **Mechanisms of Multi-Year Plan for the Energy Sector Cybersecurity 2018 of the U.S. Department of Energy**

Source	Information type	Information Flow	Receiver
Homeland Security Information Network of the U.S. Department of Homeland Security (HSIN)	Information sharing on threats, inter alia analysts', investigators' and private sector partners' collaboration	Mutual	Vetted federal, state, local, tribal, and territorial and private sector members. State Energy Emergency Assurance Coordinators Agreement (EEAC) may also request access
FBI InfaGrad Program	Threats, attacks vulnerabilities, risk mitigation	Mutual	Private and public sectors
State Energy Emergency Assurance Coordinators Agreement (EEAC) between the National Association of State Energy Officials (NASEO), the National Association of Regulatory Utility Commissioners (NARUC), the National Governors Association (NGA), the National Emergency Management Association (NEMA), CESER and Infrastructure Security and Energy Restoration (ISER) Division	All potential energy supply hazards, inter alia disruptions, incidents, events and responses	Mutual	The U.S. Department of Energy, CESER, state authorities of the impacted region

ISAC	Threats, attacks vulnerabilities, risk mitigation	Mutual	State Fusion Centers and chief information officers of energy companies
Electric Utilities	Electric disturbance events report (OE-417 form)	One-sided	The U.S. Department of Energy, CESER
Electric Utilities	Threats and attacks	Mutual	ISAC
Electric Utilities	Threats and attacks	Mutual	NERC
Electric Utilities	Threats and attacks	One-sided	State public utility commissions that have adopted rules, guidance and procedures
Oil and Natural Gas Utilities	Threats and attacks	Mutual	Oil and Natural Gas ISAC (ONG ISAC)
Natural Gas Transmission and Distribution Companies	threats and attacks	Mutual	Natural Gas Transmission and Distribution ISAC (NG ISAC)
Pipeline Operators	Incidents of abnormal operations and SCADA systems	Mutual	Pipeline and Hazard-ous Materials Safety Administration of the U.S. Department of Transportation
The Energy Sector Security Consortium Inc. (EnergySec)	Threats, attacks vulnerabilities	One-sided	State commissions and EnergySec members
National Management Risk Center of the U.S. Department of Homeland Security (NRMC)	Strategic and cross- cutting understanding of risk analysis and planning	Mutual	Federal, state, local, tribal, and territorial authorities, public and private sectors, inter alia state fusion centers
NCCIC, U.S. Computer Emergency Readiness Team (US-CERT) CISA and Industrial Control Systems-Cyber Emergency Response Teams (ICS-CERT)	Information sharing, threats, attacks and collaboration	Mutual	Federal, state, local, tribal, and territorial authorities, public and private sectors, inter alia state fusion centers

For example, the Cybersecurity Capability Maturity Model (C2M2), which helps to strengthen operational resilience, effectively assessing risks and rendering best practices to establish enhanced cybersecurity architecture.[28] Version 2.0 was released in July 2021 and comprises 145 energy sector practitioners representing 77 organizations for the time being.

The Plan should be treated as a security roadmap for both prevention and suppression as to cyber sleuthing and intrusions. For instance, the Cybersecurity Risk Information Sharing Program (CRISP) covers 26 corporations serving 75% of electricity consumers and provides near-real-time data on cyberattacks or malware and machinery responses in order to facilitate timely situational awareness. By 2019, half of the energy companies have joined this system facility. The application analyzes the data received and, using information provided, inter alia by the U.S. Department of Energy's Office of Intelligence and Counterintelligence and the U.S. Intelligence Community. It receives input data from various devices and security sensors as network firewalls and intrusion prevention systems, web authentication systems and classifies the threat.[29] The alerts with mitigation measures for potentially harmful activity are uploaded in near real-time directly to company's detection and prevention systems for further restraining intrusions.

Therefore, the Cybersecurity for the Operational Technology Environment (CyOTE) is designed to unify approach to countering cyber threats in operational technology and the Department of Homeland Security Information Network (HSIN) provides the exchange of software products for cyber incident response.[30] Along with this, there is a 24-hour cyber surveillance program (Cyber Watch) which receives reports through the iGuardian (formerly eGuardian, created in 2007) and provides for cooperation of the Federal Bureau of Investigation and infrastructure representatives.[31]

4. Detecting, Reporting and Monitoring Cyberattacks as Suppression Method

Back in 2009, NERC developed a system for detecting cyberattacks recording 41 cases and in 2016 (after 2 advanced ones) obliged corporations to report on cyber incidents.[32] Both PPD-21-2013 and the Cybersecurity Information Sharing

---

[28] Cybersecurity Capability Maturity Model (C2M2), U.S. Department of Energy (Jul. 20, 2023), available at https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

[29] Sourav Mukherjee, *Implementing Cybersecurity in the Energy Sector* (2019).

[30] Belous 2020.

[31] Cyber Resources, Domestic Security Alliance Council (Jul. 20, 2023), available at https://www.dsac.gov/topics/cyber-resources & iGuardian, FBI (Jul. 20, 2023), available at

[32] Russ Banham, *How energy companies are leading the way in cybersecurity*, Spectra by Mitsubishi Heavy Industries Group, 27 June 2019 (Jul. 20, 2023), available at https://spectra.mhi.com/how-energy-companies-are-leading-the-way-in-cybersecurity.

Act of 18 December 2015 required owners and operators to report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency within reasonable time, but no later than 12 hours after the incident. If it is impossible to provide a full report immediately, at least an internal report with materials must be provided. However, in accordance with Cyber Incident Reporting Law of 15 March 2022, now energy companies must regularly report to CISA within 72 hours from the moment of a cyberattack about the causes, consequences and methods or within 24 hours in case of making a ransom payment.[33] Non-compliance results in fines and the Attorney General has power to enforce the CISA decision.[34] Now there are the National Cyber-Awareness System (NCAS) of CISA and the National Vulnerability Database of NIST.

According to CISA, there is a continuous monitoring methodology that enables to prevent or, at least, mitigate consequences of cyberthreats via the Continuous Diagnostics and Mitigation (CDM) Program. A wider approach is presented by the Enhanced Cybersecurity Services (ECS) Program that facilitates IT protection and offer intrusion detection in terms if sink-holing and email filtering. Alike Intervention Teams there are incident response teams that fall under the guidance of the CISA Central Hunt and Incident Response Team (HIRT) and have 4 engagements: remote assistance, advisory, remote and on-site deployment. Generally, it takes about 1–2 months to reduce risks, limit damage and deliver a report.

In accordance with the Execute Order of the President of the United States "Improving National Cybersecurity" of 12 May 2021, CISA issued Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems of 24 January 2022.[35] They proposed general schemes for the sequence of actions of a company in case of a cyberattack using the Trusted Automated Exchange of Indicator Information (TAXII). Previously, there was a situation Manual "Elections cyber tabletop exercise package" of January 2020 (SitMan) that provided the scenario narratives to prevent ordinary online hazards.

---

[33] Lisa M. Ropple et al., *President Biden Signs Cyber Incident Reporting for Critical Infrastructure Act*, Lexology, 1 March 2022 (Jul. 20, 2023), available at https://www.lexology.com/library/detail.aspx?g=aec4634f-68ed-4040-a89f-60ff5c78a66a.

[34] Peters and Portman Introduce Bipartisan Legislation Requiring Critical Infrastructure, U.S. Senate, Committee on Homeland Security and Governmental Affairs (2021) (Jul. 20, 2023), available at https://www.hsgac.senate.gov/media/majority-media/peters-and-portman-introduce-bipartisan-legislation-requiring-critical-infrastructure-entities-to-report-cyber-attacks.

[35] CISA releases incident and vulnerability response playbooks to strengthen cybersecurity for federal civilian agencies, CISA, 24 January 2022 (Jul. 20, 2023), available at https://www.cisa.gov/news/2021/11/16/cisa-releases-incident-and-vulnerability-response-playbooks-strengthen & CISA, *Cybersecurity Incident & Vulnerability Response Playbooks Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems* (November 2021) (Jul. 20, 2023), available at https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

In Russia a similar system was developed earlier, in 2013. The state system of detection, prevention and elimination of consequences of computer attacks (GosSOPKA) is designed for collection and storage of detected threats or identified incidents, about which the so-called subjects of critical information infrastructure are required to notify within 24 hours. It also provides for means of information exchange and is governed pursuant to the Decree of the President of the Russian Federation on creation of the state system of detection, prevention and liquidation of consequences of computer attacks on information resources of the Russian Federation dated 15 January 2013, the Federal Law on critical information infrastructure security in the Russian Federation dated 26 July 2017 and a range of Orders of the Federal Secure Service dated 2018 and 2019. Still, the experts doubt that it is suitable for sharing experience, although there is an idea of launching a platform for sharing information about cyber incidents between information-security companies.[36] The authors hope that in future such a platform is going to cover both public and private sectors, Federation, regional and local levels as a core suppression method.

5. Results and Discussion

There are lots of general principals in establishing a common cybersecurity baseline. Examining various cybersecurity strategies and plans one may assume that the USA promotes the following oil and gas industry-specific cyber-resilience principals:

(a) Creating a complex model, inter alia handling third parties' risk, leads to the *cyber-resilience governance*;[37]

(b) *Resilience by design* is supposed to be at the stage of project, construction and operation[38] and requires secure-by-design and secure-by-default systems, services and interfaces, which demands for qualified personnel;

(c) *Corporate responsibility for resilience* means data systematisation on cyber incidents and countermeasures and establishment of access controls and management of critical assets;

(d) *Holistic risk management approach* involves standard and safety practice implementation[39] and configuration management;

---

[36] Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак ГосСОПКА // TAdviser. 1 сентября 2022 г. [State System of Detection, Prevention and Elimination of Computer Attacks GosSOPKA, TAdviser, 1 September 2022] (Jul. 20, 2023), available at https://www.tadviser.ru/index.php/Статья:Государственная_система_обнаружения,_предупреждения_и_ликвидации_последствий_компьютерных_атак_(ГосСОПКА).

[37] The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources in accordance with such standards as NIST SP 800-160 Vol. 2 NIST SP 800-172 from NIST SP 800-160 Vol. 2. *See more* Cyber resilience, NIST (Jul. 20, 2023), available at https://csrc.nist.gov/glossary/term/cyber_resiliency.

[38] For instance, the building information modeling may help foresee and estimate cyber-risks.

[39] For instance, ISO/IEC 27000, C2M2, NIST Cybersecurity Framework.

(e) *Ecosystem-wide collaboration* means information sharing measures;

(f) *Ecosystem-wide cyber-resilience plans* include developing the cyber literacy and education of employees, assessment and annual update of the list of measures implied.[40]

Taking into account the reasons for cyberattacks in the U.S. energy sector, it is worth mentioning the following actions that are recommended by CISA and TSA within the Pipeline Cybersecurity Initiative (PCI) of 2018. These rules may be referred as good security habits.

(a) Implementation of protected subnet in order to divide operational technologies and control system via Virtual Dispersive Networking (VDN) and to secure Incident Command System (ICS) and the Internet via proxy server in corporate network or virtual private network (VPN), using encryption and multi-factor authentication;

(b) Use of different devices, inter alia protected computers, in order to get access and administer Information Technology (IT) and Operational Technology (OT);

(c) Monitor key internal security capabilities and analyze anomalous traffic and user behavior (for instance, several simultaneous logging, logging outside domestic network or during non-working hours)[41];

(d) annual audit and keep software up to date, monitoring types and versions, installation data;

(e) adopt policy that oblige to put down any changes to the systems and their software and incidents;

(f) restrict access to the OT and classify it (for instance, only for essential personnel).[42]

Such principles may be implemented as a guidance for the Russian Federation, although we can conclude that it's a common situation that the U.S. sectors don't follow them and suffer. Every forth energy company is vulnerable and reason for that in a half of cases is out of date software or devices that do not comply with the necessary security level in the USA. The same applies to Russia, since about half of energy sector uses foreign software and hardware. Still, According to Positive Technologies Report 2021, 87% of unacceptable events were confirmed in verification projects in the sphere of industry and energy.[43] Under these grounds, companies are

---

[40] World Economic Forum, *Advancing Supply Chain Security in Oil and Gas: An Industry Analysis*, White Paper (August 2021) (Jul. 20, 2023), available at https://www3.weforum.org/docs/WEF_Advancing_Supply_Chain_Security_in_Oil_and_Gas_2021.pdf.

[41] Steven Bowcut, *Protecting the power grid: Cybersecurity in the energy sector*, Cybersecurity Guide, 25 June 2021 (Jul. 20, 2023), available at https://cybersecurityguide.org/industries/energy/.

[42] The US pipeline attack shows the energy sector must act now on cybersecurity. Here are 6 ways how, World Economic Forum, 17 May 2021 (Jul. 20, 2023), available at https://www.weforum.org/agenda/2021/05/oil-gas-cybersecurity-ransomware-colonial-pipeline/.

[43] Весь кибербез за один час. Итоги 2021 года и прогнозы на 2022-й в области кибербезопасности по версии Positive Technologies // Positive Technologies. 21 января 2022 г. [Everything about cybersecurity in an hour. Results of 2021 and forecasts for 2022 in terms of cybersecurity by Positive Technologies, Positive Technologies, 21 January 2022] (Jul. 20, 2023), available at https://www.ptse-

to switch domestic tools and in 2022 FSTEC announced a tender to create a unified environment for the development of secure domestic software.

Such does a great concern arise after cyberattack on the Colonial Pipeline[44] that quiet radical idea of baring ransom payments, as it has become a common practice for business.[45] Such initiatives are promoted in some states such as New York and North Carolina, Pennsylvania, Texas. The information bulletin of the U.S. Department of the Treasury's Office of Foreign Assets Control "Updated Advisory on Potential Sanctions Risks for Facilitating Ransom" of 21 September 2021 also disapproves of it.[46] According to the provisions of International Emergency Economic Powers Act of 18 October 1977 and Trading with the Enemy Act of 6 October 1917, it is prohibited for U.S. citizens and legal entities to conclude any transactions with certain persons, organizations, states, included the black-listed or they are liable for fines from 1,000 to 307,922 U.S. dollars.[47] However, this approach is criticized by American cybersecurity experts, since the safety of significant data and the need for a prompt solution to the problem often come first.[48] To achieve indispensable position, following the Executive Order of the U.S. President to improve National cybersecurity of 12 May 2021, the FBI, CISA and the U.S. Department of Energy disseminate information to owners and operators of critical infrastructure that should help to identify ransomware and mitigate its consequences. Now within the company, state and federation cyber resilience plans are adopted and Cyber Incident Reporting Law requires tacking other ways to resolve the issue before paying a ransom.

On 30 June 2021, a desktop application which was released by CISA and called Cyber Security Evaluation Tool (CSET) has got a new module Ransomware Readiness Assessment (RRA) that asses itself risks and reports in both summarized and detailed manner. It is advisable for Russia to take precautions and avoid such bad practice.

---

curity.com/upload/corporate/ru-ru/analytics/Positive_Technologies_Whitepaper_ves-kiberbez-zachas_20_01_2022.pdf.

44 The U.S. Department of Justice discloses that FBI succeeded in partial returning the ransom (different resources report on various sum: 63,7 or 66 out of 75 bitcoins).

45 *Вадимова Е.* Цифра против ТЭК // Нефть и капитал. 29 июня 2021 г. [Ekaterina Vadimova, *Digital Against Fuel and Energy Complex*, Oil and Capital, 29 June 2021] (Jul. 20, 2023), available at https://oilcapital.ru/news/2021-06-29/tsifra-protiv-tek-1031234.

46 The U.S. Department of the Treasury's Office of Foreign Assets Control, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransom*, 21 September 2021 (Jul. 20, 2023), available at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

47 Anthony C. LoMonaco & Peter A. Nelson, *Taking the Ransom Out of Ransomware? Debate on Ransomware Payments Picks Up*, Lexology, 27 July 2021 (Jul. 20, 2023), available at https://www.lexology.com/library/detail.aspx?g=f1ee994a-0874-473b-9117-04676b06b811.

48 Edward Segal, *Banning Ransomware Payments Could Create New Crisis Situations*, Forbes, 8 June 2021 (Jul. 20, 2023), available at https://www.forbes.com/sites/edwardsegal/2021/06/08/banning-ransomware-payments-could-create-new-crisis-situations/?sh=58292f872982.

Physical safety is also a great concern in terms of information security, because it increases the likelihood of unauthorized access to computers. Under the Federal Law of the Russian Federation on fuel and energy complex facilities security dated 21 July 2011, the National Guard of the Russian Federation (Rosgvardiya) is entitled to carry out on-site inspections of fuel and energy complex facilities, whose number reaches 6501, and check their security passport. About 25 thousand of violations were detected, which implies 65% don't follow the requirements.[49]

Unlike Russian authorities, American ones pay almost no attention to the physical security of energy utilities. There is a satellite-based map called Analysis of Geo-Located Energy Information or simply EAGLE-1 that allows monitoring oil and natural gas utilities, electricity bulk power systems nearly in real time, but the information is collected and downloaded by energy companies themselves. Apparently, they do it after some incidents or even fail to do it. Moreover, on September 2016, the U.S. Department of Energy announced transition of EAGLE-1 to Oak Ridge National Laboratory (ORNL).[50] Thus, one may conclude that apart from standards there are no mechanisms or schemes to provide physical security.

One may assume that the competence of some authorities is unclear, though they are aimed at collaboration in depth between federal, state, local, tribal, and territorial levels and private sector in general. For instance, ISACs and Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) of the U.S. Department of Defense provide assistance not only in terms of information sharing coordination, but also response scenarios while detecting cyberattacks (and other cyberthreats), although, for instance, the National Cybersecurity and Communications Integration Center (NCCIC) is in charge of the latter. There are lots of centers and divisions within the scope of the U.S. Department of the Interior, the U.S. Department of Defense, the U.S. Department of Justice and the Federal Bureau of Investigation. For instance, Internet Crime Complaint Center (IC3), Digital Cyber Crime Center (DC3). Some bodies may be rearranged as huger groups such as Unified Coordination Group (Cyber UCG) that was established under Presidential Policy Directive "United States Cyber Incident Coordination" of 26 July 2016 (PPD-41) in order to evaluate, assess and handle cyber incidents and coordinate provision of necessary resources to the victims. Currently, a Cyber UCG is formed at the direction of CISA NCCIC. Previously Cyber UCG was introduced in SolarWinds case in 2019, but there is no data on activity

---

[49] Объектам ТЭК нужны действенные системы безопасности // ITR Group. 21 марта 2022 г. [Fuel and energy facilities need effective safety systems, ITR Group, 21 March 2022] (Jul. 20, 2023), available at https://itr.group/press/bezopasnost-obektov-tek/.

[50] DOE Announces Transition of EAGLE-I to Oak Ridge National Laboratory (ORNL), Taking Advantage of the Laboratory's World-class Capabilities and Expertise, U.S. Department of Energy, 27 September 2016 (Jul. 20, 2023), available at https://www.energy.gov/oe/articles/doe-announces-transition-eagle-i-oak-ridge-national-laboratory-ornl-taking-advantage.

in energy sector.[51] Ambiguous competence and responsibility of the authorities leads to confusion, which body and how a representative of an energy company (victim) should apply. Another example is NIST that elaborates guidance and standards and meanwhile created the National Vulnerability Database (NVD) similar to NCAS CISA. Thus, one may doubt why such a great number of bodies should exist and be spent money on, taking into account the fact that institutions work out separately on their own.

The large number of new divisions within departments and agencies and other bodies in the cybersecurity sphere is a complex bureaucracy. In 2013 there was an experiment which implied intentional abruption of electricity facilities and lack of federal control in California. It led to blackouts and delays, which has been estimated as one of the most serious problems.[52] Authors assume that the issue hasn't been properly solved yet. Poor efficiency and lack of a consistent comprehensive approach complicate the systemic impact on cyberattacks in the U.S. energy sector.

Fortunately, the Russian Federation doesn't repeat American mistakes and the system is supposed to be more coordinated. On federal level there are the National Computer Incident Response and Coordination Center (NCIRCC) within Federal Security Service and Unified Industry Center for Coordination and Counteraction to Cyberattacks (Energy ERT) as a pilot project within the Ministry of Energy. NCIRCC is going to have sectoral centers.[53] On regional level each constituent entity has its own specialized cybersecurity Headquarters.[54]

Conclusion

In conclusion, there is no doubt that cybersecurity is one of key elements of the national security in both states, although their approaches to defining it differ which has influence on preventive measures, monitoring mechanisms, information

---

51 Feds Stand Down UCG 'Surge' Responses to Solar Winds, Microsoft Hacks, MeriTalk, 19 April 2021 (Jul. 20, 2023), available at https://www.meritalk.com/articles/feds-stand-down-ucg-surge-responses-to-solar-winds-microsoft-hacks/.

52 James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, Washington, D.C. (December 2002) (Jul. 20, 2023), available at https://www.ojp.gov/ncjrs/virtual-library/abstracts/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats.

53 Ого, какая ИБ! Особо горячие обстоятельства из мира кибер-безопасности. Итоги 2022-го и прогнозы на 2023 год по версии Positive Technologies // Positive Technologies. 13 января 2023 г. [Wow, what an IS! Particularly hot circumstances from the world of cyber security. Results of 2022 and predictions for 2023 by Positive Technologies, Positive Technologies, 13 January 2023] (Jul. 20, 2023), available at https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Ogo-kakaya-IB.pdf.

54 Дмитрий Чернышенко: В каждом регионе России созданы и функционируют штабы по борьбе с киберугрозами // Правительство России. 7 сентября 2022 г. [Dmitry Chernyshenko: Every region of Russia has created operating headquarters to combat cyberthreats, Government of the Russian Federation, 7 September 2022] (Jul. 20, 2023), available at http://government.ru/news/46461/.

sharing plans and reporting. There are diverse ways to counter cyberattacks as one of the main cyberthreats, inter alia developing operate response and reporting on cyber incidents.

Preventive measures include programs for the exchange of information, experience and technologies, exercises and standardization of the critical-infrastructure-facility operation. An effective way to significantly enhance the energy sector cybersecurity is application of standards and methodologies in order to establish control mechanisms, eliminate vulnerabilities of operational-technology system and have minimum requirements for physical and virtual access to it. However, therein lies the problem as to its non-compulsoriness, as well as low practice-oriented tools, taking into account the noxious practice of paying a ransom that the FBI occasionally fails to return (the Colonial Pipeline case confirms). Paying ransoms is a malicious practice that should be fought against rather encouraged, which the Russian Federation should take into account. Although the supervision of standards, technical regulations and appropriate safety passports seems to be more effective, the guidelines are to be updated in terms of cybersecurity.

The main suppressive measures are various cyber surveillance and near-real-time monitoring programs, as well as platforms that furnish the best solutions to minimize cyber risks and to eliminate the consequences of cyber incidents based on protocols. Russian specialists traditionally signify physical safety of facilities and they are actively elaborating cyber issues, while American ones prefer the latter.

Nevertheless, the lack of a systematic approach exacerbates the effectiveness of the applicable tools for assessing the state of cybersecurity and investigating cyber incidents, as well as automatic detection of intrusions. The activities of law enforcement agencies and companies are aimed largely at developing measures to prevent, rather than suppress, cyberattacks in the U.S. energy sector, while non-following centralized response leads to an increase in the vulnerability of the object of crime. That's why the government and representatives of energy companies should reshape their approach in order to effectively work together. As for Russia, there are some developing mechanisms, but the interaction is to be strengthened.

It is also worth taking into account social preventive measures that depends on economic, technological, cultural and social grounds for cyber-criminality. It implies actions that provide physical security of energy utilities and affect such phenomena as disgruntled employees (insiders), intruders (commercial spies), cyber-terrorism and cyber-extremism. This issue calls for further detailed investigation and be subject to future research.

References

Ballou T.M. et al. *U.S. Energy Sector Cybersecurity: Hands-Off Approach or Effective Partnership?*, 15(1) Journal of Information Warfare 44 (2016).

Carr M. *Public-Private Partnerships in National Cyber-Security Strategies*, 92(1) International Affairs 43 (2016). https://doi.org/10.1111/1468-2346.12504

Denileon G.P. *The Who, What, Why, and How of Counter Terrorism Issues*, 93(5) American Water Works Association Journal 78 (2001). https://doi.org/10.1002/j.1551-8833.2001.tb09208.x

Krause T. et al. *Cybersecurity in Power Grids: Challenges and Opportunities*, 21(18) Sensors 6225 (2021). https://doi.org/10.3390/s21186225

Mukherjee S. *Implementing Cybersecurity in the Energy Sector* (2019). https://doi.org/10.6084/m9.figshare.9728051

Powell B.A. & Chipman J.C. *Getting the Deal Through: Cybersecurity 2021* (2021).

Sklavidis I. et al. *Enhancing SIEM Technology for Protecting Electrical Power and Energy Sector*, in 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (2021). https://doi.org/10.1109/CSR51186.2021.9527944

Белоус А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения: практическое пособие [Belous A.I. *Cybersecurity of Fuel and Energy Complex Facilities. Concepts, Methods and Tools for Ensuring*] (2020).

Information about the authors

Victor Shestak (Moscow, Russia) – Professor, Department of Criminal Procedure, Moscow Academy of the Investigative Committee of the Russian Federation (12 Vrubelya St., Moscow, 125080, Russia; e-mail: viktor_shestak@mail.ru).

Alyona Tsyplakova (Moscow, Russia) – Lecturer, Department of Criminal Law, Criminal Procedure and Criminology, MGIMO University (76 Vernadskogo Ave., Moscow, 119454, Russia; e-mail: tsyplakova.a.d@my.mgimo.ru).