УДК 004.056
https://doi.org/10.47533/2023.1606-146X.3

A. A. AMRENOV[1], A. M. NURUSHEVA[1]*

[1]L.N. Gumilyov Eurasian National University,Astana, Kazakhstan

SURVEY AND ANALYSIS OF COMPUTER EMERGENCY RESPONSE TEAM SERVICES

This article discusses the functions and services of CERTs. First CERT was created with the goal to have more organized and structured approach to the computer security incident handling process. The creation of such CERTs contributes to an increase in the country's global cybersecurity index. Services that KZ-CERT provide to protect people using the Internet from malicious activity of intruders are analyzed. KZ-CERT is the center for users of national information systems and the Internet segment, which provides the collection and analysis of information on computer incidents, advisory and technical support to users in preventing computer security threats. The competence of the service includes the processing of the computer incidents in order to identify and neutralize them.

Key words*: Information Security, Global Cyber Security Index, CERT, CSIRT*

Introduction. Information processes occurring throughout the world bring to the fore, along with the tasks of efficient processing and transmission of information, the most important task of ensuring information security. This is explained by the special importance for the development of the state of its information resources, the growing cost of information in the market, its high vulnerability and often-significant damage as a result of its unauthorized use. There are many studies on security and reliability in various information systems [1]-[12].

The growth of cybercrime is the most urgent problem of our time. External influence can directly or indirectly harm the interests of the state, jeopardizing information security. The concept of "Cyber Shield" was created in the country to prevent such a phenomenon.

One of the expected results of the implementation of the concept is the constant growth of the global cybersecurity index of Kazakhstan, which includes a set of measures aimed at improving the country's cybersecurity. So, with the goal to increase the global cybersecurity index CERTs are being created as one of the technical measures to build a global cybersecurity program [13].

CERT - Computer Emergency Response Team. First malware (computer worm) influenced society as a wake-up call, after which people suddenly realized a strong need for cooperation and coordination of joint actions between system administrators and IT managers to further dealing with such incidents. Considering the fact, that downtime is the main critical factor in this situation, it is necessary to have more organized and structured approach to the computer security incident handling process. Thus, first CERT was created. There are several types of CERTs: academic, commercial, National and etc.

According to the FIRST [14] there are 635 CERT teams.

National CERTs (nCERTs) help with incident prevention and response, but they are not the only actors involved in computer incident response and prevention at the national

* E-mail корреспондирующего автора: nurusheva.assel@mail.ru

level. The growing centralization of nCERT National Services structures under government control raises important questions about the nCERT's responsibilities and how they interact with other stakeholders that play a role in cybersecurity.

National CERTs are mostly embedded in government bodies (ministries).

For example, the German National Service CERT-Bund is part of the Federal Office for Information Security (BSI), which reports to the Ministry of the Interior. CERT-Hungary operates as part of the Special National Security Service, under the Ministry of the Interior; The Mexican CERT-MX is hosted by the National Security Commission, which is part of the Mexican Ministry of the Interior that deals with internal security.

In addition to operating within government departments, some nCERTs are part of national cybersecurity centers, such as US-CERT, which is located at the National Cybersecurity and Communications Integration Center (NCCIC), or CERT Australia, which is co-located with the cybersecurity centers of other Australian government organizations in Australian National Cyber Security Centre. Other government nCERTs are part of a public institution but have public-private structures, such as NCSC.nl in the Netherlands and CERT.at in Austria.

The Australian Cyber Security Center (ACSC) leads the Australian Government's efforts to improve cyber security. Monitor cyber threats around the world 24 hours a day, seven days a week to give Australians advance warning of what to do. Provide advice and information on how to protect people and their business online. When a cybersecurity incident occurs, provides clear and timely advice to individuals, companies and critical infrastructure operators. There are National Cybersecurity Centers where they collaborate with nearly 2,000 partners from business, government and academia on current cybersecurity issues.

CERT of Kazakhstan KZ-CERT is the center for users of national information systems and the Internet segment, which provides the collection and analysis of information about computer incidents, consultations and technical support users in preventing computer security threats. The competence of the service includes the processing of the following computer incidents in order to identify and neutralize them: brute forcing of passwords or other authentication data, hacking security systems, hostile scanning of national information networks and hosts, unauthorized access to information resources, spreading the malware and unsolicited mail (spam), attacks on network infrastructure and server resources.

Analysis and results. According to the Law of the Republic of Kazakhstan "On informatization" CERT is a legal entity or a structural subdivision of a legal entity, carrying out activities in accordance with the competence established by this Law. And it implements next functions:

1) collects and analyzes information about information security incidents and current information security threats, and provides recommendations for their elimination

2) develop recommendations aimed at countering information security threats

3) informs owners of informatization objects, as well as the National Information Security Coordination Center about information security incidents and threats that have become known.

The main tool that is used by CERTs for incident response are SIEM systems. SIEM is an advanced detection system for malicious activity and various system anomalies. The

operation of SIEM allows to see a more complete picture of network activity and security events. By help of SIEM system CERT detect some malicious activity and investigate it. Other tools according to [15] which are used by CERTs in incident response process are OSINT tools and other free tools. Author says that the choice of these tools depends on the type of incident, role and expertise of CERT member. Most used OSINT tools are free, while some are commercial tools for very specific areas of investigation such as digital forensics. Table 1 describes some tools that are used in CERTs' processes.

Table 1 – Tools that are used in processes of CERTs [15]

Tool	Tool
VirusTotal	OSINT, freeware without open-source, malware intelligence and analysis
AlienVault OTX	OSINT, freeware without open-source, online threat indicators
Shodan	OSINT, freeware without open-source, for searching into the IoT
IntelMQ	OSINT, OS, for collecting and processing security feeds
REMnux	FW, malware analysis
Wireshark	OS, network protocol analyser
Apache Flink	OS, for netflow analysis
Kali Linux	FW+OS, security-enhanced Linux distribution with many useful tools
Nmap	OS, for network discovery and security auditing

To provide services of CERT in Kazakhstan it is necessary to obtain the license. For this purpose, CERT should meet some qualification requirements: requirements for employees, requirements for search tools.

Requirements for employees:

The list of specialists with higher or professional technical education who have undergone retraining, advanced training in the area of information security:

1) at least three specialists with diplomas of higher and (or) professional technical education in the profile of information security (information protection);

2) at least two specialists with certificates in the field of auditing the requirements of the international standard ISO 27001;

3) at least one specialist in computer forensics (for example, EC-Council Certified Security Analyst, GIAC Certified Forensic Analyst and others);

4) at least one specialist in reverse engineering and (or) malware analysis (for example, GIAC Reverse Engineering Malware and others);

5) at least one specialist in ethical hacking and (or) penetration testing (for example, Offensive Security Certified Professional, EC-Council Certified Ethical Hacker, GIAC Penetration Tester and others)

Requirements for search tools:

CERT should have at least minimal set of search tools which consist of IRP (Incident response platform), Threat Intelligence Platform, Static Malware Static Analysis Tool, Sandbox Dynamic Malware Analysis Tool.

Incident response process. In different sources, the phases of the process of incident response are separated in different ways. For example, NIST 800-61 R2 distinguishes 4 response phases (Preparation, Detection & Analysis, Containment & Eradication & Recovery, Post-Incident Activity). The ISO/IEC 27035:2016 standard has 5 phases, while the SANS institute divides the process into 6 phases, but they all come down to the following points: preparation, analysis, containment, eradication, recovery, post-incident activity.

Preparation. The Preparation phase consists of planning, building a team, preparing tools, places, compiling documentation and materials for the response, etc.

Identification. Incident response begins with the detection of a cyberattack or data breach. At this stage, an incident is notified, experts assess the threat and collect data about it. Usually, the process of identification comes down to the study of logs.

Analysis. Then a purely analytical phase begins: it is necessary to figure out what happened and how it could happen, assess the level of danger of what happened and, based on the received data, decide on further actions. Several attack vectors are being tested. The indicators of compromise found during the check (hash sums, file names, IP addresses, URLs) must then be checked against reputation databases. The analysis phase will determine whether the infection was successful, search for related and previous events on the infected host, determine the extent of distribution and determine the severity of the incident, and classify the malware.

The response team takes action to stop the spread of the threat. These may include isolating affected devices, isolating affected network segments, temporarily shutting down the Internet, and so on. One of the additional goals of this stage is to prevent the destruction of traces of the attack, which will be required during the investigation.

Containment. The response team takes action to stop the spread of the threat. These may include isolating affected devices, isolating affected network segments, temporarily shutting down the Internet, and so on. One of the additional goals of this stage is to prevent the destruction of traces of the attack, which will be required during the investigation.

Eradication. The response team takes action to stop the spread of the threat. These may include isolating affected devices, isolating affected network segments, temporarily shutting down the Internet, and so on. One of the additional goals of this stage is to prevent the destruction of traces of the attack, which will be required during the investigation.

Recovery. Once the incident is isolated and its further spread is excluded, it is necessary to "cure" the affected assets.

The result of the actions taken at this stage should be, for example, confirmation that the affected assets are no longer malware and that they do not pose a threat to the rest of the network. Sometimes response team travels to the customer to take the necessary remedial action. In most cases, it can be done remotely. All actions are documented in detail, the information in the incident card is supplemented.

Post-incident activity. After completing all the steps in the processing of the incident, you need to conduct a Lesson learned.

Based on the information collected and documented in the incident card, CERT can:

develop recommendations for strengthening security for the identified attack vector;

adjust the settings of protection tools and rules for detecting incidents;

adjust regulatory and reference documentation for responding to information security incidents;

apply administrative measures to increase the awareness of employees in the field of information security or disciplinary sanctions.

After analyzing several CERTs' webpages and the services they provide, it is proposed to divide the functions into the categories, which are presented in Table 2:

Table 2 – Functions of CERT

CERT Functions		
Reactive	Proactive	Quality management
Handling information security incidents	Monitoring and detection of information security events	Increasing the awareness of employees in the field of information security
Computer forensics	Providing regular reporting	Conducting trainings and studying for colleagues
Field and remote response	Audit of information system assets	Information security consulting
Coordination of internal and external departments	Security Management	Publication of information security bulletins and other materials
Fixing vulnerabilities	Proactive Threat Hunting	Development and adjustment of regulations and information security policies
Operation of protective equipment	Computer systems security assessment	Participation in building information security architecture and choosing specific solutions
Accumulation of experience and recommendations for strengthening security	Support for information security tools	Assessment and analysis of information security risks for the organization

There is a huge number of services that CERTs can provide to its clients, but so far, none of the existing CERTs provides all these services taken together. Therefore, choosing the appropriate list of provided services is extremely important task.

These services can be classified as reactive services, proactive services, and quality management services.

On a specific example, we can consider the services provided by KZ-CERT. According to the KZ-CERT's website, they provide the following services:

• Gathering computer incident reports and assistance regarding the issues of prevention and investigation of computer incidents in the Internet

• Delivery of consulting assistance and instruction on prevention computer legal violations (hacking attempts or virus attacks etc.)

• Cooperation with public or private organizations on computer security issues as well as with computer security solutions vendors and distributors

• Providing information exchange with users through KZ-CERT's call-center.

In this study, KZ-CERT was chosen to analyze the services provided by Computer Emergency Response Team.

Information about number of handled cybersecurity incidents [16] was analyzed. Total number of security incidents in the first half of 2022 is presented on figure 1:

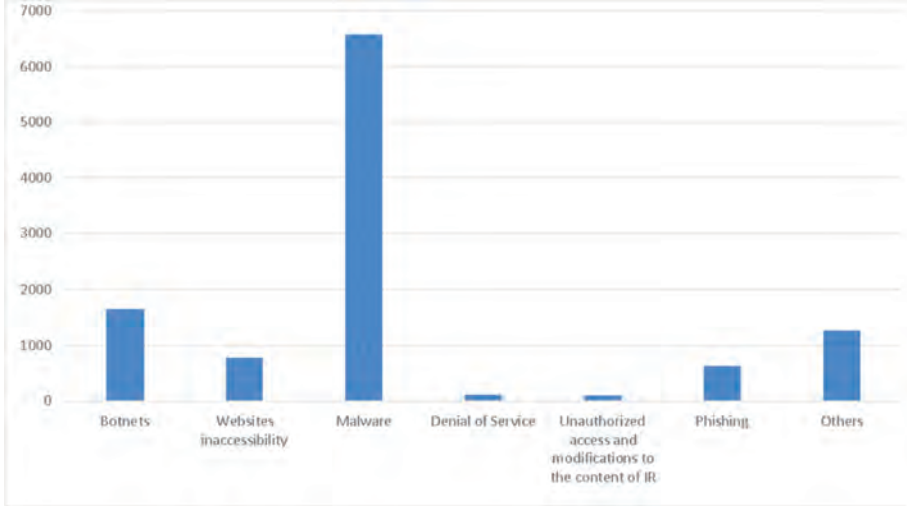

Figure 1 – Number of information security incidents that were processed in first half of 2022[16]

The largest number of incidents that occurred in 2022 related to malware. Malware is malicious software that can cause harm in a variety of ways, including:

- blocking or inability to use the device
- theft, deletion or encryption of data
- taking control of your devices to attack other organizations
- Obtaining credentials that allow you to access organization's systems or services that you use
- "mining" of cryptocurrencies.
- using services that may cost you money (such as premium phone calls).

To protect against malware, KZ-CERT suggests the following recommendations: make regular backups, prevent the delivery and distribution of malware to devices, and prevent malware from running on devices.

The next two most spread types of incident that occurred in the first half of 2022 were botnets and website unavailability. KZ-CERT monitors and detects suspicious activity on the network that is associated with botnets by means of information security tools. After botnet identification, they take measures to mitigate the effects of botnet activity. For example, they give recommendations to those whose computers have become part of the botnet.

KZ-CERT services also include tracking websites for availability. Unstable work or complete unavailability of websites can be caused by numerous reasons. Most common are technical malfunctions on servers, high attendance, website problems, actions of hackers. To avoid the outflow of customers, lower positions when ranking by search engines, you

need to monitor constantly the operation of the resource, receive information about the availability of the site in time and troubleshoot.

Figure 2 below provides information about the number of handled information security incidents related to botnets in different years.

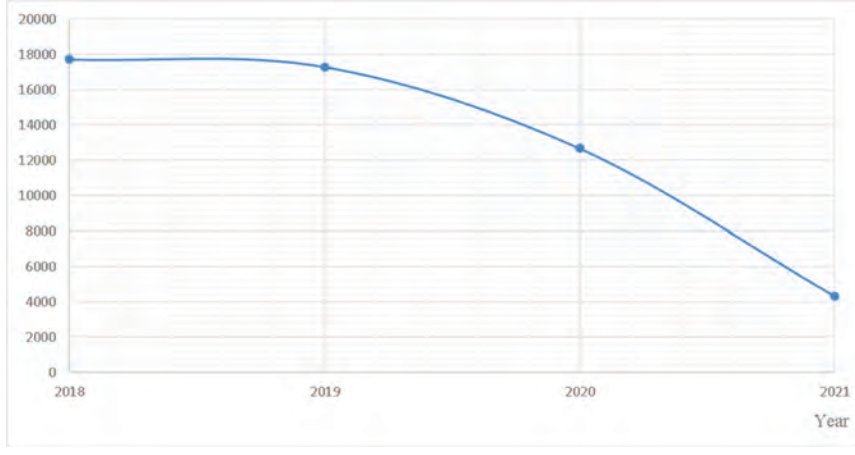

Figure 2 **–** The number of handled incidents related to botnets depending on the year [16]

Exactly 17724 botnet-related information security incidents were registered by KZ-CERT in 2018. During next few years (17300 in 2019, 12670 in 2020, 4304 in 2021) this number is decreased, which most likely connected with optimization processes conducted by KZ-CERT. After detecting botnets cybersecurity experts inform owners [17] of internet resources with recommendations for elimination and send notifications to foreign providers from whose address space attacks have been detected.

Figure 3 below provides information about the number of handled information security incidents related to websites unavailability in different years.

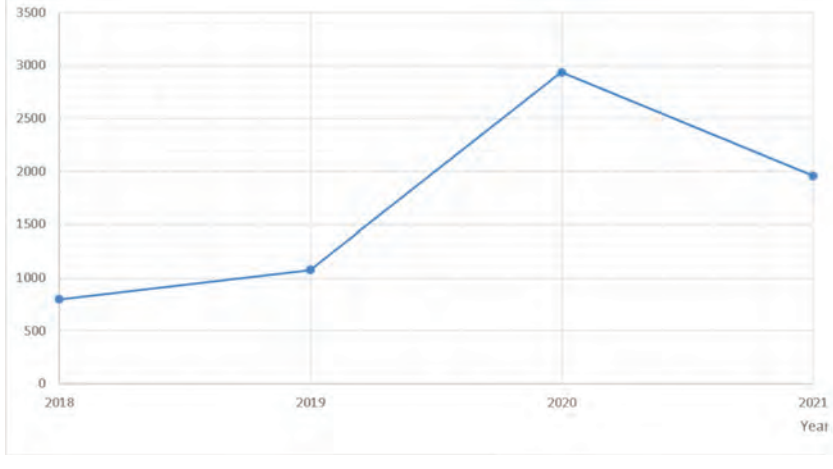

Figure 3 **–** The number of handled incidents related to websites inaccessibility depending on the year[16]

According to the figure 3 the largest number (2937) of websites' unavailability was in 2020. This is apparently because big amount of people who began to use online services during COVID. This could lead to freezing and slow operation of online services or to a complete stop of the functioning of Internet resources. This may also be due to markedly increased number of DDoS attacks in 2020. Compared to 2019, the number of DDoS attacks increased by 42% [18]. In case when some DDoS attack occurs and websites stop working, they send notification with recommendations to an owner of sites. After the owner of the information system is notified, he can take further steps to restore the site. At the next stage, if the owner has difficulties, he can request assistance from the CERT.

Conclusions. Security incident response depends on a type of incident and demand different approaches to handle them. For example, KZ-CERT for each type of information security incident make specific recommendations and send them to users who suffered from malicious activity. The services provided by the CERT to Internet users play an important role in ensuring information security locally and globally. There are many types of CERTs from commercial to government. Every day CERTs mitigate and process a large number of security incidents. And their responsibilities (incident response, reporting, user notification) is aimed at reducing or preventing the consequences of cyberattacks on different information systems. The creation of such CERTs contributes to an increase in the country's global cybersecurity index.

REFERENCES

1 Boranbayev, S. & Goranin, Nikolaj & Nurusheva, Assel. (2018). The methods and technologies of reliability and security of information systems and information and communication infrastructures. Journal of Theoretical and Applied Information Technology. 96. 6172-6188.

2 A.Boranbayev, S.Boranbayev, A.Nurusheva, K.Yersakhanov. The Modern State and the Further Development Prospects of Information Security in the Republic of Kazakhstan // 15th International Conference of Information Technology, Information Technology – New Generations, 2018. - pp. 33-38.

3 A. Boranbayev, S. Boranbayev, K. Yersakhanov, A. Nurusheva, and R.Taberkhan. Methods of Ensuring the Reliability and Fault Tolerance of Information Systems // 15th International Conference of Information Technology, Information Technology – New Generations, 2018. - pp.729-730.

4 Боранбаев А.С., Боранбаев С.Н., Ерсаханов К.Б., Нурушева А.М. Выявление потенциальных отказов программного обеспечения и их нейтрализация //Сб.докл. IV Межд. науч-практ. конф., Астана, 2017. – С.338-340.

5 Боранбаев С.Н., Нурушева А.М., Ерсаханов К.Б. Анализ состояния информационной безопасности Республики Казахстан и перспективы его развития // Сборн. докл. IV Межд. науч-практ. конф., Астана, 2017 – С.341-344.

6 Boranbayev, A., Boranbayev, S., Nurusheva A., Yersakhanov K. (2018). Development of a Software System to Ensure the Reliability and Fault Tolerance in Information Systems. Journal of Engineering and Applied Sciences, 13(23), 10080–10085.

7 Boranbayev, S., Goranin, N., Nurusheva, A. The methods and technologies of reliability and security of information systems and information and communication infrastructures // Journal of Theoretical and Applied Information Technology. – 2018. – 96(18) – С. 6172–6188.

8 Boranbayev A.S., Boranbayev S.N., Nurusheva A.M., Yersakhanov K.B., Seitkulov Y.N. Development of web application for detection and mitigation of risks of information and automated systems // Eurasian Journal of Mathematical and Computer Applications. – 2019. – 7(1) – pp. 4-22.

9 Turskis, Z., Goranin, N., Nurusheva, A., Boranbayev S. Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach // Informatica. – 2019. – 30, No. 1 – pp.265-289.

10 Turskis, Z., Goranin, N., Nurusheva, A., Boranbayev S. A Fuzzy WASPAS-Based Approach to Determine Critical Information Infrastructures of EU Sustainable Development // Sustainability. – 2019. – 11(2) – 424 p.

11 Boranbayev A., Boranbayev S., Nurusheva A. Development of a software system to ensure the reliability and fault tolerance in information systems based on expert estimates // Advances in Intelligent Systems and Computing. – 2018. – Vol. 869. – pp.924-935.

12 Boranbayev A., Boranbayev S., Nurusheva A., Yersakhanov K., Seitkulov Y. A software system for risk management of information systems // Proceedings of the 2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT 2018). – 17-19 Oct. 2018. – Almaty, Kazakhstan. – pp. 284-289.

13 https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/

14 https://www.first.org/members/teams/

15 S. R. B. Mohd Kassim, S. Li, and B. Arief, “How national CERTs leverage public data, OSINT and free tools in operational practices: An empirical study,” Cyber Security: A Peer-Reviewed Journal, vol. 5, no. 3, pp. 1– 26, 2022.

16 https://cert.gov.kz/press_club/infographics

17 https://cert.gov.kz/news/11/2064

18 https://sts.kz/2020/07/22/%D0%9E%D0%B1%D0%B7%D0%BE%D1%80-%D0%B8%D0%BD%D1%86%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%BE%D0%B2-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9-%D0%B1%D0%B5%D0%B7/

А. К. АМРЕНОВ[1], А. М. НУРУШЕВА[1*]

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

КОМПЬЮТЕРЛІК ИНЦИДЕНТТЕРГЕ ӘРЕКЕТ ЕТУ ТОБЫ ҚЫЗМЕТТЕРІНЕ ШОЛУ ЖӘНЕ ТАЛДАУ

Бұл мақалада CERT мүмкіндіктері мен қызметтері талқыланады. Бірінші CERT компьютерлік қауіпсіздік инциденттерін өңдеу процесіне негұрлым ұйымдасқан және құрылымдық көзқарас мақсатымен жасалған. Мұндай CERT құру елдің жаһандық киберқауіпсіздік индексін жақсартуға ықпал етеді. Интернетті пайдаланатын адамдарды зиянкестердің әрекетінен қорғау үшін KZ-CERT ұсынатын қызметтері талданды. KZ-CERT – ұлттық ақпараттық жүйелерді және интернет сегментін пайдаланушыларға арналған орталық, ол компьютерлік инциденттер туралы ақпаратты жинауды және талдауды, компьютерлік қауіпсіздікке төнетін қатерлердің алдын алуда пайдаланушыларға кеңес беру және техникалық қолдау көрсетуді қамтамасыз етеді. Қызметтің құзыретіне компьютерлік инциденттерді анықтау және бейтараптандыру мақсатында өңдеу кіреді.

Түйін сөздер*: ақпараттық қауіпсіздік, жаһандық киберқауіпсіздік индексі, CERT, CSIRT.*

***А. К. АМРЕНОВ*[1], *А. М. НУРУШЕВА*[1*]**

[1]*Евразийский университет имени Л.Н. Гумилева, Астана, Казахстан*

ОБЗОР И АНАЛИЗ УСЛУГ СЛУЖБЫ РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

В статье обсуждаются функции и сервисы CERT. Первый CERT был создан с целью более организованного и структурированного подхода к процессу обработки инцидентов компьютерной безопасности. Создание таких CERT способствует повышению глобального индекса кибербезопасности страны. Проанализированы услуги, которые KZ-CERT предоставляет для защиты людей, использующих Интернет, от деятельности злоумышленников. KZ-CERT — центр для пользователей национальных информационных систем и интернет-сегмента, обеспечивающий сбор и анализ информации о компьютерных инцидентах, консультационную и техническую поддержку пользователей в предотвращении угроз компьютерной безопасности. В компетенцию службы входит обработка компьютерных инцидентов с целью их выявления и нейтрализации.

***Ключевые слова**: иинформационная безопасность, глобальный индекс кибербезопасности, CERT, CSIRT.*