FACTORS INFLUENCING THE CHOICE OF INFORMATION SYSTEMS PROTECTION MECHANISMS

Xadjayev Saidakbar Ismoil o'g'li
assistant of the Fergana branch of the Tashkent University of Information Technologies named after Muhammad Musa al-Khwarizmi
breddy.breddy@mail.ru
https://doi.org/10.5281/zenodo.10279775

Abstract. Ensuring information security is becoming a key task for an organization that processes data that is valuable to potential attackers. To build an optimal information system (IS) model, it is necessary to identify all the conditions that make risks more or less likely.

Keywords: provision of information processing data, attacker, optimal information system (IS) model, risk, electronic services and companies.

The main factors influencing the susceptibility of IP to threats. When creating its own data protection model, an organization must evaluate the objective phenomena that influence the degree of risk. Factors are understood as events and phenomena of two categories. Affecting the process of information processing in such a way that this may lead to a deterioration in its quality characteristics - confidentiality, integrity, availability.

Creating conditions that make the risks of theft or modification of information more or less likely. The standard proposes such a classification of risks. These include the transmission of signals over unprotected communication lines, the presence of electromagnetic, acoustic, optical radiation that can be intercepted, defects, failures and failures of equipment and programs.

These are man-made phenomena, for example, electromagnetic radiation that can damage information, failures of support systems, natural disasters, thermal risks - fires, biological risks - microbes or rodents.

Subjective internal. This is the disclosure of information by persons who have the right to access it, the transmission of data through open communication channels, their processing on unprotected technical means, publication of information in the media, its copying to an unregistered medium, loss of the medium, any unlawful actions with data - modification, copying, use hardware bookmarks, incorrect information protection, incorrect design of the control mechanism, personnel errors;

Subjective external. This is the organization of access to information from foreign or competitive intelligence services, the use of special means for external access to data, the actions of criminal groups, and sabotage activities.

The GOST list almost never forms the basis for building an organization's IP system. In this case, they rely on a more global system for identifying conditions that create risks.

In local regulations of organizations - security policies - these include:

the industry in which the organization operates;

the initial degree of security of the information system and the complexity of its architecture;

the value of the information being processed;

type of hypothetical offender;

degree of personnel training.

Assessing these parameters will allow you to develop your own information security risk management model. Identifying threats that are appropriate for a specific organization can be done through a variety of methods.

To apply the method, it is necessary to have a large amount of statistical data on information security incidents in the same or similar sectors of the economy.

Large companies involved in information security can analyze the situation at a specific enterprise, drawing on accumulated experience and using various analysis methods.

Most often, a combination of the first and second methods is used. The experiment is available to large corporations and government organizations. During the experiment, the digital model of an enterprise or facility is tested for resistance to attacks by intruders.

Depending on the sector of the economy in which the organization operates and on what principle its business is built, the parameters that create an information security threat are determined. Some industries are at greater risk than others.

Personal data operators should pay maximum attention to information security issues. PD is the most popular product on the black market for information, which means they are always under attack.

Banks and financial sector organizations. Attackers are interested in information about citizens' accounts and the possibility of stealing other people's savings.

Companies operating in the field of innovative and information technologies. Hackers show interest in new developments from the point of view of timely creation of countermeasures. There are known cases where hackers have been silently present in the developers' IP for years, recording all their findings and solutions.

Government organizations, damage to which creates a good PR reputation among the criminals.

Government electronic services and companies providing their functioning. In this case, the attacks are aimed at stealing personal data or information about citizens' fines. For example, the information infrastructure of the Moscow government is attacked every 20 seconds.

Companies working in the field of protection against hacker attacks. There is an increased demand for their developments; their theft helps hack customer systems.

Telecommunications companies. Temporary disruption of communication channels is used in cyber warfare. Organizations of housing and communal infrastructure (water utilities, nuclear power plants, etc.), accidents at which can deprive entire areas of water and electricity.

By understanding the goals of attackers, it is possible to identify conditions that create an information security threat, the elimination of which will need to be addressed first.

A separate issue is assessing the quality of information security for the information technologies used. The result of such an assessment determines the readiness of the information system to repel external and internal attacks. FSTEC certification, which reveals undeclared capabilities, is not always a panacea; many problems are hidden in the standard operating systems used, the vulnerabilities of which are well known to attackers.

In GOST, factors that create a threat to information security and belong to this class are defined as follows:

defects, malfunctions and failures of software;

processing information on unprotected servers and workstations, its transmission over unprotected communication lines;

copying data to an unregistered storage medium;

unauthorized connection to communication channels, technical means and information processing systems;

use of defects in information processing tools;

using software bookmarks;

use of viruses.

To eliminate these events and actions that create a threat to information security, and to properly configure the IS, a systematic approach is required.

There are several standards that allow you to evaluate the operation of the system as a whole and the quality of software configuration. ISO/IEC 15408, Information Technology Security Assessment Criteria, is key. The application of the standard provides working tools that can assess the safety and performance of technologies. In fact, this is a set of libraries containing security standards and typical protection profiles. These solutions will not always save you from targeted attacks, but in 90% of cases they will eliminate external and internal risks. The standard contains 11 functional classes, 66 families, and 135 information security components. They are familiar to many system administrators, but in practice only some of them are often implemented.

A well-protected system should have the following software mechanisms implemented:

identification and authentication, often two-step;

protecting user data from misappropriation for the purpose of logging into the system under someone else's account;

protection of security functions (requirements relate to the integrity and control of these security services and the mechanisms that implement them);

managing security, its attributes and parameters, setting up security monitoring, auditing management results, which means identifying, recording, storing, analyzing data related to ensuring system security, and responding to information security incidents.

Each position has its own protection methods using specific hardware and software. Creating an information structure in accordance with the standard increases the level of information security.

When working with solution providers and outsourcing organizations that have received an order to create a secure information system, the standard offers criteria for authorization and performance assessment that help eliminate the occurrence of risks for information security.

The actions of developers and implementation engineers must be additionally checked at each stage of creating the system architecture:

the development is tested at every stage - from a brief specification to full implementation;

Lifecycle support must be monitored from launch;

testing during commissioning is carried out with the participation of independent experts;

acceptance is required upon delivery;

the user manual is tested for clarity and completeness;

The system is additionally tested for compliance with security profiles.

When ordering software or IP development, compliance with the requirements for monitoring the work of information service providers will help to avoid many mistakes. The costs of hiring external experts are often worth it.

The value of data becomes a separate issue. It is difficult to develop general criteria for assessing the cost of information and determine how the limit is formed, after reaching which the data is at risk, and its cost becomes a key parameter that creates a threat to information security.

In any case, the following are subject to significant protection due to their unconditional value:

state secret;

bank secrecy;

personal data of citizens;

scientific developments of high significance;

new information technologies;

development of startups with commercial potential. Such organizations, which have not yet accumulated significant resources, cannot build a reliable information security system. And many competitors are targeting new technological and not yet patented solutions, ready to steal and resell them.

In the work of an ordinary company that does not have information of these classes, the value of information is determined by the interest of competitors in it. A company operating in a saturated market must more carefully protect its business plans, marketing developments, and customer bases from theft and leaks. Information systems often come under attack if a company participates in a government procurement tender. There are known cases of attempts to eliminate a competitor by collapsing its information system. Certain risks are identified in the work of companies that install and maintain numerous devices with Internet access - temperature sensors, video cameras. These devices are increasingly being used as bots in DDoS attacks.

In practice, the level of personnel training turns out to be the most important reason creating a threat to information security. The Information Security Doctrine of Russia directly states that one of the threats to the country's information security is the small number of experienced personnel, the low level of education and training of new specialists.

In addition to all the risks listed in GOST that pose a threat to information security, there are additional ones. The desire to spend large budgets, increasing the importance of the department, and concentrating on complex products, rather than on constant monitoring of system performance, increases the likelihood of threats being implemented.

To minimize the impact of poor staff training, it is necessary to regularly conduct personnel audits and certifications, and, if necessary, organize additional training. The involvement of outsourcers in certain areas of work must be carried out in compliance with all security requirements, including the inclusion in contracts of a clause on the protection of trade secrets with a high level of financial liability.

Fine-tuning the company's information security system, taking into account the influencing parameters and the degree of their significance, will minimize risks and eliminate the

possibility of causing damage to the organization. In practice, factor analysis is more complex than statistical analysis, but it helps create a more reliable defense system.

References:

1. Kochkorova G., Irmatova D., Abdurasulova D. ASSOCIATION OF VIRTUAL REALITY INTO HUMAN CONSCIOUSNESS //International Bulletin of Applied Science and Technology. – 2023. – Т. 3. – №. 10. – С. 326-329.
2. Abdurasulova, D. B. kizi, & Irmatova , D. B. (2023). USE OF DIFFERENT ALGORITHMS AND APPLICATION OF SOFTWARE PRODUCT CREATION SEQUENCES IN ORGANIZING COMPLEX STRUCTURED PROJECTS // Educational Research in Universal Sciences, 2(11), 170–173. Retrieved from http://erus.uz/index.php/er/article/view/3947
3. Xadjayev S. Information Security: Strategies, Challenges, and Emerging Trends //Journal of technical research and development. – 2023. – Т. 1. – №. 2. – С. 253-257.
4. Saidakbar X. USING MODERN WEB TECHNOLOGIES IN CREATING WEB APPLICATIONS //Journal of technical research and development. – 2023. – Т. 1. – №. 2.
5. Saidakbar X. DIGITAL TECHNOLOGIES IN MEDICINE: ADVANTAGES AND PROSPECTS //Journal of technical research and development. – 2023. – Т. 1. – №. 2.
6. Xadjayev S. NEURAL NETWORKS AND ARTIFICIAL INTELLIGENCE IN PYTHON: REVIEW OF LIBRARIES AND FRAMEWORKS //Journal of technical research and development. – 2023. – Т. 1. – №. 2.
7. Кочкорова Г. Д., Ирматова Д. Б. РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАНИИ //Journal of Integrated Education and Research. – 2023. – Т. 2. – №. 5. – С. 59-64.
8. Кочкорова Г. Д. ВЫСШЕЕ ОБРАЗОВАНИЕ В УЗБЕКИСТАНЕ В РАМКАХ КОНЦЕПЦИИ «УНИВЕРСИТЕТ 3.0» ЎЗБЕКИСТОНДА «УНИВЕРСИТЕТ 3.0» КОНСЕПСИЯСИ ДОИРАСИДА ОЛИЙ ТАЛИМ //HIGHER EDUCATION IN UZBEKISTAN WITHIN THE CONCEPT//Таълим тизимида ижтимоий-гуманитар фанлар. – 2021. – С. 16.
9. Кочкорова Г. Д. Инновационный подход-требование современного образования //Современные инновации. – 2018. – №. 2 (24). – С. 64-65.
10. Кочкорова Г. Д. СОЦИАЛЬНО-ЭТИЧЕСКИЕ АСПЕКТЫ ДЕЯТЕЛЬНОСТИ ННО //Российская наука в современном мире. – 2017. – С. 13-14.
11. Кочкорова Г. Д., Усмонов Н. У. ИСПОЛЬЗОВАНИЯ ИННОВАЦИОННЫХ МЕТОДОВ В ОБРАЗОВАНИИ-ЭТО ПОДГОТОВКА ВЫСОКОКВАЛИФИЦИРОВАННЫХ СПЕЦИАЛИСТОВ //Теория и практика современной науки. – 2018. – №. 12. – С. 228-233.
12. Kutbeddinov, A. K. (2023). GENERALIZATION OF URANIUM RADIO FEATURES IN TEACHING NATURAL SCIENCES. Молодые ученые, 1(15), 129-134.
13. Кочкорова, Гульнара Дехканбаевна. "золотой век исламского возрождения." Европейский журнал гуманитарных наук и достижений в области образования 3.10 (2022): 127-129.
14. Мамадалиев Н., Кочкорова Г. ИСТОРИЧЕСКИЙ ПЕРИОД ИСЛАМСКОГО РЕНЕССАНСА //Интернаука. – 2021. – Т. 10. – №. 186 часть 2. – С. 24.
15. Ирматова Д., Хаджаев С. НЕЙРОННЫЕ СЕТИ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ НА ЯЗЫКЕ PYTHON: ОБЗОР БИБЛИОТЕК И ФРЕЙМВОРКОВ //Research and implementation. – 2023.

16. Зулунов Р. М., Ирматова Д. Б., Гоибова Х. Исследование и создание программного обеспечения алгоритма расчета показателей оценки управления инновационной деятельностью //Journal of Integrated Education and Research. – 2023. – Т. 2. – №. 5. – С. 54-58.
17. Shakhnoza, K. (2022). The History of Chemical Industry Development in Navoi Region. International Journal of Early Childhood Special Education, 14(6).
18. Расулов А.М., Иброхимов Н.И., Ирматова Д.Б. КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА РОСТА ТОНКОЙ ПЛЁНКИ // ИННОВАЦИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ В НЕФТЕГАЗОВОМ ДЕЛЕ – 2021. ISBN: 978-5-93105-464-3 –С. 399-401.
19. Kochkorova, G., & Mamirov, N. (2023). PHYSICAL CULTURE AND SPORTS IN THE LIFE OF MODERN SOCIETY. В INTERNATIONAL BULLETIN OF APPLIED SCIENCE AND TECHNOLOGY (Т. 3, Выпуск 11, сс. 184–187). Zenodo. https://doi.org/10.5281/zenodo.10117728
20. Кочкорова, Г. Д. (2023). КАК ИСПОЛЬЗОВАТЬ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБРАЗОВАНИИ ДЕТЕЙ. В INTERNATIONAL BULLETIN OF APPLIED SCIENCE AND TECHNOLOGY (Т. 3, Выпуск 11, сс. 533–538). Zenodo. https://doi.org/10.5281/zenodo.10225888