UDC 519.6
IRSTI 27.41.77

A METHOD FOR CALCULATING THE INFORMATION SECURITY RISK

D.K.Mukhayev[1,2], Marat Akhmet[3]

[1]Institute of Information and Computational Technologies
[2]Al-Farabi Kazakh National University
[3]Middle East Technical University, Ankara, Turkey
e-mail:daryn.mukhayev@gmail.com
[1]https://orcid.org/0000-0002-2985-286X
[3]https://orcid.org/0000-0002-3483-1182

Abstract. The article discusses the issues of identifying threats and vulnerabilities of information security violations. To protect information, it is necessary to create computer attack detection systems. Explanations were given on the concept of cyber attacks and their types were affected. No organization is currently sufficiently protected from cyber attacks. All organizations should develop a special plan to combat cybercriminals. A special plan allows you to prepare for emergencies, resist emerging threats and quickly restore the effect of the attack. The need to know the threatening factors and understand their tactics, methods and procedures to protect against cyber attacks is emphasized. The process of information protection should be comprehensive and continuous, carried out at all stages of the creation and use of automated data processing tools. The main methods of information protection are given.

Keywords: Information security, cyber attacks, cybercrime, information protection, threats, vulnerability.

Introduction

Due to the rapid development of science and technology, the influence of world information technologies on all spheres of production is increasing. In this regard, new social groups are being formed in society, the normal way of life of people is changing significantly. Information security issues related to the active informatization currently underway are of paramount importance. Many of them are aimed at creating a unified information space in order to optimize the processing of large amounts of information, including ensuring its reliable storage and accessibility for information exchange.

The main tasks set for the implementation of this goal are the identification, analysis and classification of information security threats that may lead to unauthorized receipt of information or disruption of the normal functioning of information systems, the definition of the main measures used to counter threats and eliminate vulnerabilities, the development of security criteria and mechanisms, as well as the relevant legislative and regulatory framework.

Analysis of existing threats and vulnerabilities of information security shows that achieving the goals and objectives of information protection, as well as ensuring a high level of security, requires a comprehensive application of available methods and means of protection. For this reason, one of the basic principles based on the development of information security concepts and specific information security tools is complexity.

The process of ensuring the protection of information should be comprehensive and continuous, carried out at all stages of the creation and use of automated data processing tools. The implementation of the information security process in these conditions is based on production conceptual approaches and the production of safety equipment. As a rule, highly qualified information security specialists are involved to create protective mechanisms and ensure their reliable and efficient operation.

Risk assessment as part of the direction of information security (risk management) is an essential tool in building protection. The risk assessment process is designed to identify the risk to an organization's business and determine the security measures taken to reduce the risk.

In the classical view, risk is the probability of the realization of an information security threat.

Risk assessment consists in modeling the picture of the occurrence of adverse conditions by taking into account all possible factors that determine the risk. From a mathematical point of

view, when analyzing risks, such factors can be considered input parameters. At the same time, it is necessary to take into account the many sources of information and the uncertainty of the information itself. At the risk assessment stage, the formulas and input data for calculating the risk value are of the greatest interest.

The article analyzes several different methods of risk calculation and presents its own methodology. The purpose of the work is to derive a formula for calculating the risk of information security, which allows obtaining an array of current risks and assessing losses.

Information security risk in the classical form is defined as a function of three variables:

probability of threat existence;

the probability of vulnerability (insecurity);

Potential impact.

If any of these variables approaches zero, then the total risk tends to zero.

Methods of risk assessment

According to the article «Information Technology. Security methods. Information security management systems. Requirements», the chosen methodology should ensure that risk assessments produce comparable and reproducible results. At the same time, the standard does not provide a specific calculation formula.

The NIST 800-30 «Risk management guide for information technology systems» provides the following classical formula for calculating risk:

$R = P(t) * S$,

Where, R is the risk value;

P(t) is the probability of an information security threat (a mixture is used qualitative and quantitative scales);

S – degree of threat impact on the asset (the asset price on a qualitative and quantitative scale).

As a result, the risk value is calculated in relative units, which can be ranked according to the degree of significance for the information security risk management procedure.

According to the article «Information Technology. Methods and means of ensuring security. Methods of information technology security management», risk calculation in contrast to the NIST 800-30 standard «Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology» occurs according to the following formula:

$R = P(t) * P(v) * S$,

where P(t) is the probability of an information security threat;

P(v) – probability of vulnerability;

S is the value of an asset (resource).

As an example of the values of probabilities P(t) and P(v), a qualitative scale with three levels (low, medium and high) is given. To assess the value of asset S, numerical values are presented in the range from 0 to 4. The comparison of qualitative values should be made by the organization in which information security risks are assessed.

According to the "Information Security Management System Specification", the risk level is calculated taking into account the following indicators: the value of the resource, the threat level and the degree of vulnerability. As the values of these parameters increase, the risk increases. Thus, the formula can be represented as follows:

$R = S * L(t) * L(v)$,

Where, S is the value of the asset (resource);

L(t) – threat level;

L(v) – level (degree of vulnerability).

In practice, information security risks are calculated according to the positioning table of the threat level values, the degree of probability of vulnerability use and the value of the asset. The risk value can vary in the range from 0 to 8, as a result, a list of threats with different risk values is obtained for each asset. The standard offers the following risk ranking scale: low (0-2), medium (3-5) and high (6-8). This allows you to identify the most critical risks.

According to the «Methodology for assessing the risks of information security violations», the assessment of the degree of the possibility of implementing an information security threat is carried out on the following qualitative and quantitative scale: unrealizable threat - 0%, average – from 21% to 50%, etc.

To perform a qualitative assessment of information security risks, a table of compliance with the severity of the consequences and the probability of threat realization is used. If it is necessary to make a quantitative assessment, then the formula can be presented as follows:

$R = P(v) * S,$

Where, S is the severity of the consequences.

Having considered all of the above methods of risk assessment in terms of calculating the value of information security risk, it is worth noting that the risk calculation is performed using the threat value and asset value. A significant disadvantage is the valuation of assets (the amount of damage) in the form of conditional values. Conditional values do not have units of measurement applicable in practice.

As a result, this does not give a real representation of the level of risk that can be transferred to the real assets of the object of protection.

Thus, it is proposed to divide the risk calculation procedure into the following stages:

calculation of the technical risk value;

calculation of potential damage.

Technical risk is understood to mean the importance of information security risk, consisting of the probabilities of the implementation of threats and the use of vulnerabilities of each component of the information infrastructure, taking into account the level of their confidentiality, integrity and availability. For the first stage , the following formulas can be given:

$Rc = Kc * P(T) * P(V);$

$Ri = Ki * P(T) * P(V);$

$Ra = Ka * P(T) * P(V),$

where Rc is the value of privacy risk;

Cc – coefficient of confidentiality of an information asset (resource);

P(T) – probability of threat realization;

P(V) – the probability of using the vulnerability;

Ri – value of integrity risk;

Ki is the integrity coefficient of an information asset (resource);

Ra – availability risk value;

Ka – coefficient of availability of an information asset (resource).

In the future, it is possible to calculate the damage value. To do this, the average value of the risk of each information asset and the amount of potential losses are used. The damage value (L) is calculated using the following formula:

$L = Ravg * S,$

Where, Ravg is the average risk value;

Conclusion

The use of this algorithm will make it possible to make a more detailed risk assessment, as a result, to obtain a dimensionless value of the probability of the risk of compromising each information asset separately.

Also, the proposed methodology allows you to correctly assess the value of information security risk and assess losses in the event of security incidents.

As part of future research, it is planned to consider ways to improve the quality of the forecast about threats and vulnerabilities of information security.

References

[1] Kirsanov, K.A. Information security: Textbook K. A. Kirsanov, A.V. Malyavina, N. V. Popov; Moscow. acad. Economics and Law. – Moscow: MAEP, 2020

[2] Koneev, I.R. Information security of the enterprise: [Inform. safety. Classification of attacks. Risk management methodology. Cryptographer. tools and mechanisms] Iskander Koneev, Andrey Belyaev. – St. Petersburg: BHV-Petersburg, 2021

[3] Melnikov, V.V. Information protection in computer systems: – M.: Finance and Statistics. Electroinform, 2014

[4] Shakovets, A.N. Fundamentals of computer information protection and information security: Lecture by A.N. Shakovets, N.V. Rymareva; M-in internal. Affairs of Russia, Far East. jurid. in- – Khabarovsk: Far East. jurid. in-t of the Ministry of Internal Affairs of the Russian Federation, 2021

[5] Smagin A.A., Poletaev V.S. Algorithm for forecasting threats to information security. Infocommunication technologies. 2018. 16(2). 192-198.

[6] Yazan Alshboul, Kevin Streff. Analyzing Information Security Model for Small-Medium Sized Businesses: Twenty-first Americas Conference on Information Systems, Puerto Rico. 2015. DOI: https://core.ac.uk/download/pdf/301365935.pdf

[7] Julian Jang-Jaccard, Surya Nepal. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences. 2014. 80(5). 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

[8] Top cybersecurity threats on enterprise networks: https://www.ptsecurity.com/ww-en/analytics/network-traffic-analysis-2020/

[9] Eran Toch, Claudio Bettini, Erez Shmueli, Laura Radaelli, Andrea Lanzi, Daniele Riboni, and Bruno Lepri.2018. The Privacy Implications of Cyber Security Systems: A Technological Survey.ACM Comput. Surv.51,2, Article 36 (February 2018), 27 pages. https://doi.org/10.1145/3172869

[10] Obotivere B. A., Nwaezeigwe A. O.. Cyber Security Threats on the Internet and Possible Solutions, IJARCCE 9(9). 2020. 92-97. DOI: 10.17148/IJARCCE.2020.9913

[11] Information technology. Security methods. Information security management systems. Requirements: ISO/IEC 27001. – Introduction. 06.01.2018. – Moscow: Standartinform, 2018. 54.

[12] Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology : NIST 800-30. – Introduction. 06.01.2020. – USA. 2020. 56.

[13] Information technology. Methods and means of ensuring security. Part 3. Methods of information technology security management: GOST R ISO/IEC T13335-3-2017. – Introduction. 01.09.2017. Moscow: Standartinform, 2017. 76.

[14] Specification of the information security management system: BS 7799-2:2005. –Introduction. 01.07.2019. – England. 2019. 86.

[15] Ensuring information security of organizations of the banking system of the Russian Federation. Methodology for assessing the risks of information security violations: RS BR IBBS-2.2-200. – Introduction. 06.01.2019. – Moscow: Standartinform, 2019. 23.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТӘУЕКЕЛІН ЕСЕПТЕУ ӘДІСІ

Д.К.Мухаев[1,2], Марат Ахмет[3]
[1]Ақпараттық және есекптеуіш технологиялар институты, Алматы, Қазақстан
[2]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Казақстан
[3]Таяу Шығыс техникалық университеті, Анкара, Түркия
e-mail:daryn.mukhayev@gmail.com
[1]https://orcid.org/0000-0002-2985-286X
[3]https://orcid.org/0000-0002-3483-1182

Аңдатпа. Мақалада ақпараттық қауіпсіздікті бұзудың қатерлері мен осалдықтарын анықтау мәселелері талқыланады, ақпаратты қорғау үшін компьютерлік шабуылдарды анықтау жүйелерін құру қажеттілігі негізделеді. Кибершабуылдар түсінігі бойынша түсіндірмелер беріледі және олардың түрлері әсер етеді. Қазіргі уақытта ешбір ұйым кибершабуылдардан абсолютті қауіпсіздікті қамтамасыз етпейді. Барлық ұйымдар пайда болатын қауіптерге қарсы тұру және тез

қалпына келтіру үшін арнайы киберқылмыстық жоспарларды әзірлейді (осылайша шабуылдың әсерін азайтады). Қауіпті факторларды білу және кибершабуылдардан қорғау тактикасын, әдістері мен процедураларын түсіну қажеттілігі атап өтіледі. Ақпаратты қорғау процесі ақпаратты өңдеудің автоматтандырылған құралдарын жасау мен пайдаланудың барлық кезеңдерінде жүзеге асырылатын жан-жақты және үздіксіз болуы керек. Ақпаратты қорғаудың негізгі әдістері келтірілген.

Түйінді сөздер. Ақпараттық қауіпсіздік, кибершабуыл, киберқылмыскер, ақпаратты қорғау, қауіптер, осалдықтар.

МЕТОД РАСЧЕТА РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.К.Мухаев[1,2], Марат Ахмет[3]
[1]Институт информационных и вычислительных технологий КН МОН РК, Казахстан
[2]Казахский национальный университет имени аль-Фараби, Казахстан
[3]Ближневосточный технический университет, Анкара, Турция
e-mail:daryn.mukhayev@gmail.com
[1]https://orcid.org/0000-0002-2985-286X
[3]https://orcid.org/0000-0002-3483-1182

Аннотация. В статье рассматриваются вопросы выявления угроз и уязвимостей нарушения информационной безопасности, обоснована необходимость создания систем обнаружения компьютерных атак для защиты информации. Даны разъяснения по понятию кибератак и затронуты их виды. В настоящее время ни одна организация не обеспечивает абсолютную защищенность от кибератак. Все организации разрабатывают специальные планы по борьбе с киберпреступниками, позволяющие противостоять возникающим угрозам и быстро восстанавливаться (тем самым уменьшая последствия от эффект атаки). Подчеркивается необходимость знания угрожающих факторов и понимания тактики, методов и процедур для защиты от кибератак. Процесс защиты информации должен быть комплексным и непрерывным, осуществляться на всех этапах создания и использования автоматизированных средств обработки данных. Приведены основные методы защиты информации.

Ключевые слова. Информационная безопасность, кибератака, киберпреступность, защита информации, угрозы, уязвимость.

Авторлар жайында мәлімет:
Қаз: Мухаев Дарын – Әл-Фараби атындағы Қазақ ұлттық университетінің докторанты, daryn.mukhayev@gmail.com
Рус: Мухаев Дарын – докторант Казахского национального университета им. аль-Фараби, daryn.mukhayev@gmail.com
Англ: Mukhayev Darin – a doctoral student at Al-Farabi Kazakh National University, daryn.mukhayev@gmail.com

Қаз:Марат Ахмет, профессор, Таяу Шығыс техникалық университеті, Анкара, Түркия
Рус: Марат Ахмет, профессор, Ближневосточный технический университет, Анкара, Турция
Англ:Marat Akhmet, professor, Middle East Technical University, Ankara, Turkey
Орынбай Мажит Темирбекулы – студент Казахского национального университета имени Аль-Фараби, temirbek.majit@gmail.com