DOI: https://doi.org/10.32839/2304-5809/2021-1-89-27
UDC 004.056

Kuznetsov Denis
Kyiv National University of Technologies and Design
Zakharova Maria
Cherkasy State Business College
Liuta Maiia
Kyiv National University of Technologies and Design

CRITERIA FOR EVALUATION OF EFFICIENCY OF REMOTE ADMINISTRATION SOFTWARE

Summary. The work is devoted to solving the problem of evaluating the effectiveness of remote administration software (PZVA) according to certain criteria. The concept of efficiency of PZVA is revealed in the work, criteria of efficiency of software, actions and means for their development and use are defined. Efficiency means the ability of software to provide appropriateper formance depending on the number of computingre sources used in the established conditions. Resources may in clude other software, software and hardware configuration of the system and materials. It is noted that efficiency includes a number of characteristics such as time behavior, resource use, and efficiency matching. The advantages of the above-mentioned criteria for evaluating the ELV and their disadvantages that reduce the objectivity of the evaluation of the effectiveness of the software are identified. Another important criterion is also analyzed – the security of the remote administration software. Due to the ever-increasing number of attacks on local area networks, new vulnerabilities in the software are constantly being discovered and, as a result, a new type of attack is emerging. The risks associated with insufficient connection security are considered. In addition, a huge disadvantage of using remote access programs is the defection of the perimeter of the local network. And in this regard, with the incompetent use of such software there is a risk of attackers using remote access programs. Thus, the criteria for the effectiveness of remote administration software are defined in the paper. This will allow to effectively evaluate remote administration software according to certain criteria, increase their quality and reliability, at the stage of system design and development to select software.

Keywords: efficiency, evaluation, software, remote administration, criterion.

Кузнецов Д.В.
Київський національний університет технологій та дизайну
Захарова М.В.
Черкаський державний бізнес-коледж
Люта М.В.
Київський національний університет технологій та дизайну

КРИТЕРІЇ ОЦІНКИ ЕФЕКТИВНОСТІ ПРОГРАМНИХ ЗАСОБІВ ВІДДАЛЕНОГО АДМІНІСТРУВАННЯ

Анотація. Робота присвячена вирішенню проблеми оцінки ефективності програмних засобів віддаленого адміністрування (ПЗВА) за певними критеріями. В роботі розкрито поняття ефективності ПЗВА, визначено критерії ефективності програмних засобів, заходи та засоби для їх розробки та використання. Під ефективністю розуміється здатність програмних засобів забезпечити відповідну продуктивність в залежності від кількості використовуваних обчислювальних ресурсів в встановлених умовах. До ресурсів можуть відноситися інші програмні засоби, конфігурація програмних і апаратних засобів системи, матеріали. Відмічено, що ефективність включає ряд характеристик, таких як поведінка в часі, використання ресурсів і відповідність ефективності. Поведінка в часі – це здатність програмного засобу забезпечувати відповідні часи відгуку і обробки, а також пропускну здатність при виконанні своїх функцій в заданих умовах. Використання ресурсів – це здатність програмного засобу використовувати відповідну кількість всіх типів ресурсів при виконанні своїх функцій в заданих умовах. Відповідність ефективності – це здатність програмних засобів відповідати стандартам і угодам, пов'язаним з ефективністю. Визначено переваги вищеназваних критеріїв оцінки ПЗВА та їх недоліки, що знижують об'єктивність оцінки ефективності програмного засобу. Також проаналізовано ще один важливий критерій – безпечність програмного засобу віддаленого адміністрування. У зв'язку з постійним зростанням числа атак на локальні мережі, постійно виявляються нові вразливі місця в програмному забезпеченні і, як наслідок, з'являється новий вигляд атак. Розглянуто ризики, пов'язані з недостатньою захищеністю підключення. Величезним мінусом використання програм віддаленого доступу є порушення периметра локальної мережі. І в зв'язку з цим, при невмілому використанні такого програмного забезпечення є ризик використання зловмисниками програм для віддаленого доступу. Таким чином, в роботі визначено критерії ефективності програмних засобів віддаленого адміністрування. Це дозволить ефективно оцінити програмні засоби віддаленого адміністрування за певними критеріями, підвищити їх якість та надійність, на етапі проектування та розробки системи здійснити вибір програмних засобів.

Ключові слова: ефективність, оцінка, програмні засоби, віддалене адміністрування, критерій.

Formulation of the problem. In today's world, special attention is paid to the development and using of quality software and their effective functioning. Solving the problem of assessing the quality and reliability of software for remote administration according to certain criteria, the effective choice of software is an urgent task.

Analysis of recent research and publications modern publications on methods and tools to ensure the effective functioning of software, insufficient attention is paid to the development and effective using of software for remote administration. At the same time, some practical manuals on software development and using are devoted to recommendations for the selection of tools according to certain criteria, but these recommendations are informal. From the analysis of the modern literature on software performance evaluation, it is not entirely clear how to select effective remote administration software (PZVA), which of the many criteria to choose and how to evaluate the effectiveness of the PZVA.

Highlighting previously unsolved parts of the general problem to which the article is devoted. When designing effective PZVA of any type, it is necessary to formulate requirements, develop methods for determining their effectiveness. Therefore, it is important to reveal the concept of the effectiveness of PZVA, to define a set of criteria for effective remote administration software, measures and tools for their development and using [1, p. 268].

The goal of this work is to determine the criteria for the effectiveness of remote administration software, which will improve the quality of both the software itself and the system as a whole.

Presentation of the main material. Efficiency means the ability of software to provide appropriate performance depending on the number of computing resources used in the established conditions. Resources may include other software, software and hardware configuration of the system and materials.

Efficiency includes a number of characteristics such as time behavior, resource use, and efficiency matching.

Time behavior is the ability of a software tool to provide appropriate response and processing times, as well as when performing its functions under specified conditions.

Resource utilization is the ability of a software tool to use the appropriate amount of all types of resources when performing its functions under specified conditions.

Efficiency compliance is the ability of software to meet performance standards and agreements. This characteristic refers primarily not to the properties of the software, but to the degree of satisfaction in its development of the provisions of regulations related to efficiency.

The criterion "behavior in time" determines or predicts the temporary attributes of the software (response time, duration of the processing cycle). The evaluation of temporary attributes is carried out without taking into account the resource costs of these attributes. Criteria for the characteristics of the use of resources measure or predict the use of resources of the system, part of which is a software tool, during its operation. Such metrics include, for example, memory usage, information transfer usage [2, p. 1140]. Evaluation of the use of system resources is performed without taking into account the impact of their minimization on the temporary properties of the software. The following general shortcomings of the performance criteria listed in the standards can be identified:

– these standards recommend a small number of performance criteria compared to the number of criteria for other characteristics;

– the vast majority of the criteria have different physical meaning and are presented in absolute units (seconds, bytes, bits per second); this complicates their joint use in a comprehensive assessment of the quality of the software;

– those criteria that are presented in relative units, do not ensure that their values fall into the range of 0–1 recommended by the standards, which also complicates the joint use of criteria in the integrated assessment of software quality;

– for the vast majority of criteria, the following relationship is valid: the lower the measured value of the criterion, the higher the value of its effectiveness; therefore, these criteria do not satisfy such properties of validity of criteria as correlation, tracing and consistency;

– the criteria measure either the speed or resource properties of the aircraft and do not take into account their mutual influence; thus, the optimality (minimization) of the ratio of speed and resource properties of the software by the existing criteria is not analyzed and, therefore, remains outside the assessment of the characteristics of the effectiveness of the software within the current quality model regulated by the standard;

– the criteria do not take into account the interest of the customer (user) in minimizing the ratio of speed and resource properties of the software.

The above criteria have shortcomings that reduce the objectivity of the evaluation of the effectiveness of the software. Currently, the most common and used multi-level model of software quality, presented in the set of standards ISO 9126 [3]. The basis for regulating the quality of systems is the international standard ISO 9126 "Information Technology. Software product evaluation. Quality characteristics and guidance on their application". This standard describes a multilevel distribution of software characteristics. At the top level there are six main characteristics of software quality, each of which is determined by a set of attributes that have the appropriate criteria for further evaluation.

According to this model:

– Functionality – a set of properties of the software, which is determined by thepresence and specific features of a set of functions that can meet the specified or indirect needs of quality, along with its reliability as a technical system.

– Reliability – the ability of the software to perform the required tasks in the specified conditions for a specified period of time or a specified number of operations.

– Usability – a set of properties of the software that characterizes the effort required for its use, and evaluation of the results of its use by a given circle of users of the software.

– Efficiency – the ability of the software to provide the required level of performance in accord-

ance with the allocated resources, time and other specified conditions.

– Maintainability – the ease with which the software can be analyzed, tested, modified to correct defects, to implement new requirements, to facilitate further maintenance and to adapt to the name of the environment.

– Portability – a set of properties of the software that characterizes the In general, if the software meets all the criteria described above to evaluate the effectiveness of the software, then it can be considered effective and safe to use.

In addition to the above criteria, another important criterion should be noted – the security of the remote administration software. Due to the ever-increasing number of attacks on local area networks, new vulnerabilities in the software are constantly being discovered and, as a result, a new type of attack is emerging.

In such conditions, the systems responsible for the security of remote access must be able to withstand a variety of attacks, both external and internal, automated and coordinated attacks. Sometimes the attack lasts a split second; sometimes the probing of vu lnerable places is carried out slowly and stretches for hours, so that the suspicious activity is almost invisible. The purpose of attackers can be a violation of all components of information security – accessibility, integrity or confidentiality [4, p. 22].

The main threats to network safety include:

– disclosure of confidential information:

– compromising information;

– unauthorized use of resources of the local computer network;

– wrong of its resources;

– unauthorized exchange of information;

– refusal of information;

– denial of service.

Unauthorized access to databases, eavesdropping on LAN channels, and so on can be a means of realizing the threat of disclosure of confidential information. In any case, obtaining information that is the property of a person (or group) causes significant harm to its owners.

Compromise of information is usually carried out by making unauthorized changes to the database, as a result of which its user is forced to either abandon it or spend extra effort to detect changes and restore true information. In the case of using compromised information, the user may make incorrect decisions with all the consequences that follow.

Unauthorized use of local area network resources, on the one hand, is a means of disclosing or compromising information, and on the other – has its own meaning, because, even without touching user or system information, can cause some damage to subscribers or local area network administration. The amount of losses can vary widely – from reduced financial resources to complete failure of the network.

Wrongly authorized use of local area network resources can also lead to the destruction, disclosure or compromise of these resources. This threat is most often the result of errors in the software of the local area network.

Unauthorized exchange of information between the subscribers of the local computer network may lead to the receipt of information by one of them, access to which he is prohibited, which in its consequences is equal to the strong disclosure of information.

Refusal of information consists in non-recognition by the addressee or sender of this information, the facts of its receipt or sending. This, in particular, may serve as a reasoned reason for the rejection of one of the parties from before supported agreement (financial, trade, diplomatic, etc.) "technically", without formally abandoning it, thereby may cause significant damage to the other party.

Denial of service is a very significant and widespread threat, the source of which is the local computer network itself. Such a refusal is especially dangerous in situations where a delay in the provision of network resources to the subscriber can lead to serious consequences for him. For example, a subscriber's lack of data needed to make decisions may be the cause of his irrational or suboptimal actions.

Many of all attacks on the company's corporate network from the outside are related to vulnerable web applications. There may be shortcomings in the software configuration – for example, primitive settings of access policies, a simplified algorithm for registering new users, and the fact that employees are allowed to use simple passwords to log in. All this facilitates the task of attackers who seek to penetrate the internal network of the company, where commercial information is stored.

Also popular is the exploitation of vulnerabilities in protocols and software used for remote access. Examples: security error in Windows – in versions 7, Server 2008 and Server 2008 R2 – known as BlueKeep (code CVE-2019-0708), error CVE-2019-19781 in Citrix software, vulnerability of the Laravel framework (CVE-2018-15133), as well as a number of vulnerabilities in network equipment for VPN connections.

Companies that have their own Internet Security department are more likely to close known "holes" and bugs. However, even skilled security professionals are unlikely to protect against zero-day vulnerabilities. Is it worth talking about the risks for companies that do not have an Internet Security Specialist in their staff, and even a basic software and OS update has not been established.

In addition, a huge disadvantage of using remote access programs is the defection of the perimeter of the local network. And in this regard, with the incompetent use of such software, the risk of attackers using remote access programs as backdoor criminals to infect the network with viruses or steal data from public folders.

There are risks jointed with insufficient connection security. Remote access programs have the ability to use the clipboard.

– There is a possibility that when copying, the file may be replaced with a malicious one with the same name and size.

– Risk of losing control over the connection.

– The risk that someone may use your connection later.

As a result of the above risks, at best, you can get an infected system with a Trojan, and at worst – to get a miner virus or coder, not to mention the stolen information.

Conclusions and suggestions. Thus, the criteria for the effectiveness of remote administration software are defined in the paper. Efficiency characteristics such as time behavior, resource utilization, and efficiency matching are also considered. The criteria for evaluating the effectiveness according to the model of software quality considered in the work, the functionality of the software, its reliability, ease of use of the software, efficiency, ease of maintenance and portability of the software. This will allow to effectively evaluate remote administration software according to certain criteria, increase their quality and reliability, at the stage of system design and development to select software. Therefore, the choice of software for remote administration and access in general should be approached with maximum responsibility. Taking into account all the above criteria for ease of use, efficiency and, most importantly, the safety of PZVA.

References:

1. Lyuta M.V., Kuznetsov D.V. (2020) Remote administration of computer networks. *Innovation in education, science and business: challenges and opportunities. Kyiv National University of Technology and Design*, pp. 267–272.
2. ISO 9126 Information Technology. Assessment of the software product. Quality characteristics and guidance for their application.
3. Zakharova M.V. (2013) The methodology of building a system for assessing IS security based on the intensities of attacks. *Bulletin of the Kyiv National University of Technology and Design*, no. 3(71), pp. 19–24.
4. Zharko E.F. (2015) Assessment of the quality of software for automated control systems: theoretical foundations, main trends and problems. *System identification and control tasks SICPRO '15*, vol. 1(32), pp. 1129–1143.

Список літератури:

1. Люта М.В., Кузнецов Д.В. Віддалене адміністрування комп'ютерних мереж. *Інновати ка в освіті, науці та бізнесі: виклики та можливості.* 2020. С. 267–272.
2. ISO 9126. Інформаційна технологія. Оцінка програмного продукту. Характеристики якості та керівництво по їх використанню.
3. Захарова М.В. Методика побудови системи оцінки захищеності ІС з урахуванням інтенсивностей атак. *Вісник Київського національного університету технологій та дизайну*. 2013. № 3(71). С. 19–24.
4. Жарко Е.Ф. Оцінка якості програмного забезпечення автоматизованих систем управління: теоретичні основи, основні тенденції та проблеми. *Ідентифікація систем та завдання управління SICPRO '15*. 2015. № 1(32). С. 1129–1143.