Information systems. Computer sciences. Issues of information security

Информационные системы. Информатика. Проблемы информационной безопасности

UDC 004.056
https://doi.org/10.32362/2500-316X-2024-12-3-25-36
EDN LNWLOK

RESEARCH ARTICLE

Criteria and indicators for assessing the quality of the investigation of an information security incident as part of a targeted cyberattack

Stanislav I. Smirnov @, Mikhail A. Eremeev, Shamil G. Magomedov, Dmitry A. Izergin

MIREA – Russian Technological University, Moscow, 119454 Russia
@ Corresponding author, e-mail: smirnov_si@mirea.ru

Abstract

Objectives. The currently increasing number of targeted cyberattacks raises the importance of investigating information security incidents. Depending on the available means of protection, computer forensic experts use software and hardware tools for analyzing digital artifacts of various operating systems and network traffic to create an event chronology (timeline) of the incident. However, to date, there is no formal approach for assessing the effectiveness of expert activities when investigating an information security incident within the framework of a targeted cyberattack. The present study aims to develop partial indicators of promptness, effectiveness, and resource intensity as part of the suitability criterion for investigating an information security incident.

Methods. Methods informed by purposeful process efficiency and set theory are used along with expert evaluation approaches.

Results. An analysis of works in the field of investigation of computer incidents is presented. The terminology and main guiding documents on specifics of conducting information security incident investigations are described along with examples of digital artifacts defined in the form of classification. The expediency of forming criteria and indicators for assessing the quality of an information security incident investigation is substantiated. The suitability criterion and subsequent indicators for assessing the quality of the investigation are selected: the effectiveness (completeness) indicator for detecting digital artifacts by a computer criminologist is based on the conducted activities, resource intensity indicator, and promptness indicator for investigating an information security incident.

Conclusions. The obtained results can be used not only by heads of departments but also by rank-and-file information security professionals for objective analysis of the available software and human resources, the time spent on these activities, and the identified digital artifacts as part of a cyber incident investigation.

Keywords: information security incident, targeted cyberattack, cyber incident investigation, MITRE ATT&CK matrix, digital artifact, information security threat assessment, targeted process, quality assessment criteria and indicators

• **Submitted:** 02.05.2023 • **Revised:** 22.11.2023 • **Accepted:** 05.04.2024

For citation: Smirnov S.I., Eremeev M.A., Magomedov Sh.G., Izergin D.A. Criteria and indicators for assessing the quality of the investigation of an information security incident as part of a targeted cyberattack. *Russ. Technol. J.* 2024;12(3):25–36. https://doi.org/10.32362/2500-316X-2024-12-3-25-36

Financial disclosure: The authors have no a financial or property interest in any material or method mentioned.

The authors declare no conflicts of interest.

НАУЧНАЯ СТАТЬЯ

Критерии и показатели оценивания качества проведения расследования инцидента информационной безопасности при целевой кибератаке

С.И. Смирнов [@], М.А. Еремеев, Ш.Г. Магомедов, Д.А. Изергин

МИРЭА – Российский технологический университет, Москва, 119454 Россия
[@] Автор для переписки, e-mail: smirnov_si@mirea.ru

Резюме

Цели. В настоящее время при нарастающем числе целевых атак задача расследования инцидента информационной безопасности (ИБ) приобретает важное значение. Компьютерные криминалисты, в зависимости от имеющихся средств защиты, применяют программные и программно-аппаратные средства форензики, проводят анализ цифровых артефактов различных операционных систем и сетевого трафика с построением хронологии событий (таймлайна) инцидента. На сегодняшний день отсутствует какой-либо формальный подход к оцениванию эффективности действий специалистов при проведении расследования инцидента ИБ в рамках целевой кибератаки. Целью работы является формирование частных показателей оперативности, результативности и ресурсоемкости в рамках критерия пригодности при расследовании инцидента ИБ.

Методы. Использованы методы теории эффективности целенаправленных процессов, методы экспертных оценок и теории множеств.

Результаты. Проведен анализ актуальных работ в области расследования компьютерных инцидентов. Представлены терминология и основные руководящие документы спецификации проведения расследования инцидента ИБ. Определены примеры цифровых артефактов в виде классификации. Обоснована целесообразность формирования критериев и показателей оценки качества проведения расследования инцидента ИБ. Выбраны критерий пригодности и следующие показатели оценивания качества проведения расследования: показатель результативности (полноты) выявления цифровых артефактов компьютерным криминалистом на основе проведенных мероприятий, показатель ресурсоемкости и показатель оперативности расследования инцидента ИБ.

Выводы. Полученные результаты могут быть использованы не только руководителями подразделений, но и рядовыми специалистами по ИБ для объективного анализа имеющихся программных и человеческих ресурсов, времени, затраченного на эти мероприятия, и выявленных цифровых артефактов в рамках расследования киберинцидента.

Ключевые слова: инцидент информационной безопасности, целевая кибератака, расследование киберинцидента, матрица MITRE ATT&CK, цифровой артефакт, оценка угроз безопасности информации, целенаправленный процесс, критерий и показатели оценки качества

• **Поступила:** 02.05.2023 • **Доработана:** 22.11.2023 • **Принята к опубликованию:** 05.04.2024

Для цитирования: Смирнов С.И., Еремеев М.А., Магомедов Ш.Г., Изергин Д.А. Критерии и показатели оценивания качества проведения расследования инцидента информационной безопасности при целевой кибератаке. *Russ. Technol. J*. 2024;12(3):25–36. https://doi.org/10.32362/2500-316X-2024-12-3-25-36

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

INTRODUCTION

In recent years, geopolitical events around the world have substantially influenced the increased activity of hacker groups. According to the Positive Technologies[1] company final report for 2022, the number of information security (InfoSec) incidents increased by 20.8% over the past year, among which the volume of successful targeted attacks using ransomware (encryptors) amounted to 51%. The practice of responding to modern InfoSec incidents shows that, over the last decade, the number of techniques and tools used by attackers in targeted attacks on information and telecommunications networks of organizations has been increasing daily [1].

As a result, the organization of an integrated approach when investigating an InfoSec incident acquires increased importance. Such an integrated approach consists in aggregating identified digital artifacts from various security systems (e.g., security information and event management (SIEM), intrusion detection/prevention system (IDS/IPS), data loss prevention (DPL), next generation firewall (NGFW), etc.) to create cyberattack timelines. In case this information is not available in the organization, it becomes much more difficult for experts to search for forensically significant data, thus increasing the investigation timeframe. An important role in this process is played by the availability of live systems by means of which computer forensic experts can capture random access memory (RAM) dumps.

Thus, one of the most urgent scientific directions within the InfoSec incident investigation consists in the creation of a theoretical framework for calculating the effectiveness of computer forensics activities depending on the availability of forensic software and protection systems in the organization. The present work aims to develop partial indicators of promptness, effectiveness, and resource intensity in terms of suitability criterion for investigating an InfoSec incident from targeted attacks.

The paper continues studies [2, 3] aimed at developing a theoretical basis for assessing the effectiveness of targeted processes.

TERMINOLOGY AND KEY GUIDANCE DOCUMENTS ON THE SPECIFICS OF CONDUCTING AN INFOSEC INCIDENT INVESTIGATION

A number of regulatory documents and instructions issued by commercial organizations describe professional activities when investigating and responding to computer attacks. At the same time, state standards do not define criteria and indicators for assessing the quality of cyber incident investigation. For example, the guidance document GOST R 59709-2022[2] defines only terms and definitions, as well as their interconnections within these processes, while the GOST R 59712-2022[3] standard is limited to an organizational description of the actions of cyber incident management units.

The methodological document of the Federal Service for Technical and Export Control "Methodology for Assessing Information Security Threats" lists ten basic tactics and corresponding techniques used to build scenarios for implementing InfoSec threats.[4] The MITRE ATT&CK[5] matrix serves as a basis for developing this list. According to GOST R ISO/IEC TO 18044-2007[6], when the first signs of an InfoSec incident are detected, computer forensic experts are faced with the task of determining their causes. In this regard, digital artifacts are collected whose main sources include hard disk copies, RAM dumps, security event logs, and network device traffic.

The basic terminology of the InfoSec incident investigation is summarized below, which is essential for further research.

- *Computer attack* is a purposeful unauthorized network computer impact (or sequence thereof) on an information resource carried out by an intruder using software and/or hardware and information technologies with the aim of disrupting and/or stopping the functioning of an information resource or to implement a threat to the security of information processed by this resource.[7]
- *Targeted cyberattack* is a continuous process of unauthorized activity in the infrastructure of the information system (IS) under attack, remotely hand-operated in real time.[8]

[1] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (in Russ.). Accessed March 30, 2023.

[2] GOST R 59709-2022. National Standard of the Russian Federation. *Information protection. Detection, prevention and liquidation of the consequences of computer attacks and response to computer incidents. Terms and Definitions*. Moscow: Rosstandart; 2022 (in Russ.).

[3] GOST R 59712-2022. National Standard of the Russian Federation. *Guide to Planning and Prepare for Incident Response ISO/IEC 27035-2*. Moscow: Rosstandart; 2022 (in Russ.).

[4] https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (in Russ.). Accessed April 06, 2023.

[5] https://attack.mitre.org/. Accessed April 06, 2023.

[6] GOST R ISO/IEC TO 18044-2007. National Standard of the Russian Federation. *Information technologies. Methods and means of ensuring security. Information security incident management*. Moscow: Standartinform; 2007 (in Russ.).

[7] GOST R 59709-2022. National Standard of the Russian Federation. *Information protection. Detection, prevention and liquidation of the consequences of computer attacks and response to computer incidents. Terms and Definitions*. Moscow: Rosstandart; 2022 (in Russ.).

[8] https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (in Russ.). Accessed March 14, 2023.

- *InfoSec incident* is the occurrence of one or more undesirable InfoSec events that may cause IS failure or disruption[9]. According to GOST R ISO/IEC 13335-1-2006[10], examples of cyber incidents may include loss of equipment (devices), system user errors, failure to comply with InfoSec policy or recommendations, violation of physical protection measures, software failures, technical failures, system failures or overloads, and violation of access rules.
- *InfoSec incident investigation* is a set of actions by InfoSec experts aimed at identifying the vector of a targeted cyberattack for minimizing the damage and developing recommendations to prevent an InfoSec incident in the future [2].
- *Computer incident response* is the process (procedure, function) of automatic (automated) processing of a computer incident.[11]
- *Digital artifact* is potential evidence found on a target device (e.g., personal computer, mobile device, and network device) that can be used in forensic practice [3].
- *Forensically significant data* is computerized information used to substantiate the conclusions of forensic investigations and solve the tasks set for forensic investigation.[12]

A classification of digital artifacts that can be used by experts in investigating an InfoSec incident is presented in Figure. In the classification, significant evidence of common operating systems (OS) and network traffic is specified.

By establishing criteria and indicators for assessing the quality of a cyber incident investigation, the effectiveness of the process can be improved, as well as the consequent process of responding to a computer attack for minimizing financial and reputational damage to the organization. Thus, the better a cyber incident investigation is conducted by experts, the more quickly they are able to respond to and stop the malicious process.

REVIEW OF RELEVANT STUDIES IN THE FIELD OF INFOSEC INCIDENT INVESTIGATION

Practical issues of investigating InfoSec incidents are discussed in the works of S.I. Makarenko [4], M.A. Eremeev [5], P.D. Zegrzda, D.P. Zegzhda [6], A.G. Lomako [7], V.A. Ovcharov [8], S.A. Petrenko [9], I.B. Saenko [10], I.V. Kotenko [11], I.A. Pribylov [12], V.S. Avramenko [13], and D.S. Levshun [14].

While there are a number of existing instructions for Russian commercial organizations to describe the actions of experts in responding to a cyber incident, these instructions have a number of disadvantages.

The experts from F.A.C.C.T (formerly Group-IB in Russia) have developed an instruction[13] for responding to incidents related to remote banking systems. The main disadvantage of this document is its use only in IS of financial institutions.

In the manual[14] published by Kaspersky Lab, employees describe the actions of experts in responding to InfoSec incidents. However, this document is not a universal instruction, but only describes the use of basic tools for data collection as well as analysis of potential threats and their removal. This guide requires modifications based on knowledge of modern techniques and methods used by attackers.

In an earlier thesis[15], the present author introduced a generalized indicator of malicious authentication activity of the attacker based on the completeness indicator of detecting authentication actions performed by the attacker during "horizontal movement" in the domain, and the promptness indicator of investigating a cyber incident. This indicator can be considered only in the case of a cyberattack on the organization's domain.

The above analysis of existing studies pertaining to cyber incident investigation demonstrates that existing documents adopted at state and commercial levels describe only approximate actions of experts and fail to define timeframes for assessing the quality of cyber incident investigation.

[9] https://normative_reference_dictionary.academic.ru/23474/ (in Russ.). Accessed March 15, 2023.

[10] GOST R ISO/IEC 13335-1-2006. National Standard of the Russian Federation. *Information technology. Methods and means of ensuring security*. Part 1. Concept and models of security management of information and telecommunication technologies. Moscow: Standartinform; 2006 (in Russ.).

[11] GOST R 59709-2022. National Standard of the Russian Federation. *Information protection. Detection, prevention and liquidation of the consequences of computer attacks and response to computer incidents. Terms and Definitions*. Moscow: Rosstandart; 2022 (in Russ.).

[12] https://www.group-ib.com/wp-content/uploads/media/2016/02/Group-IB_dbo_instruction.pdf (in Russ.). Accessed March 13, 2023.

[13] https://www.group-ib.com/wp-content/uploads/media/2016/02/Group-IB_dbo_instruction.pdf (in Russ.). Accessed March 13, 2023.

[14] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07172131/Incident_Response_Guide_rus.pdf (in Russ.). Accessed March 15, 2023.

[15] Smirnov S.I. *A methodology for conducting a cyber incident investigation based on an automated analysis of domain security events*: Cand. Sci. Thesis. St. Petersburg, 2022. 124 p. https://www.elibrary.ru/item.asp?id=54428705 (in Russ.). Accessed March 25, 2023.

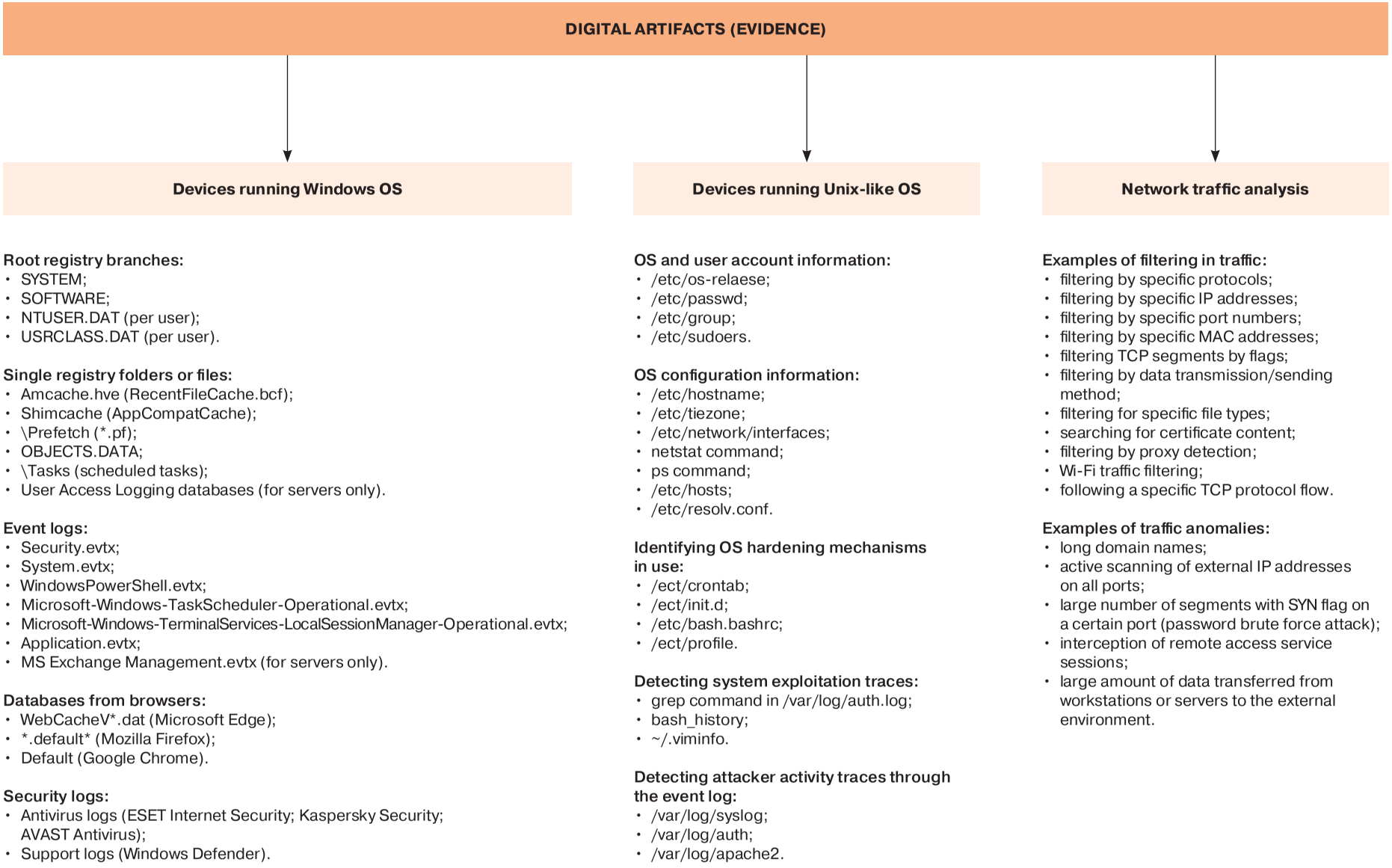

Figure. Classification of digital artifacts. TCP—Transmission Control Protocol

DESCRIPTION OF CRITERIA AND INDICATORS FOR ASSESSING THE QUALITY OF CONDUCTING THE CYBER INCIDENT INVESTIGATION WITHIN TARGETED CYBERATTACK

The theory of efficiency of purposeful processes defines the following concept: *efficiency* is a complex operational property of a purposeful functioning process that characterizes its adaptability to perform the task facing the system [15].

The concept of efficiency is directly related to the concept of quality. *Quality* is a property or a set of properties of an object that determine its suitability for intended use. Each of the properties of an object can be described quantitatively using some variable, whose value characterizes the measure (intensity) of its quality in relation to this property. This measure is called the *property indicator* or single, *partial indicator of quality* of the object [15].

When assessing the quality of any object described by an n-dimensional vector index, a set of criteria is implemented, each of which can belong to one of three classes in general case:

- class $\{G\}$ of suitability criteria;
- class $\{O\}$ of optimality;
- class $\{S\}$ of superiority [15].

Criteria can be represented either in vector or scalar form.

The effectiveness assessment criterion comprises a set of conditions defining operation objectives (InfoSec incident investigation) and the suitability, optimality, or superiority of the investigated operation based on it [15].

In the paper, *the suitability criterion G* is selected for the study.

For assessing the quality of InfoSec incident investigation within the targeted cyberattack (including an ongoing one), the following indicators are proposed:

- effectiveness (completeness) indicator for detecting digital artifacts by a computer forensic investigator based on the conducted activities, r;
- resource intensity indicator (availability of forensics software products and expenditure of human resources), p;
- promptness indicator of the InfoSec incident investigation, t.

DESCRIPTION OF EFFECTIVENESS INDICATOR

The effectiveness indicator, which is determined by the degree of completeness of detecting digital artifacts r, directly depends on nine main activities implemented during the investigation:

1) collecting and analyzing event logs of the domain controller and workstations or servers;
2) analyzing processes from the RAM dump of workstations or servers;
3) analyzing browser history of workstations;
4) analyzing mail messages of workstations;
5) analyzing logs of antivirus systems available in the organization;
6) analyzing hard disk copies from workstations or servers;
7) analyzing traffic from available network devices (routers, firewalls) and intrusion detection/prevention systems (if any);
8) analyzing SIEM-system events (if any);
9) building a timeline of the target attack.

The main activities are determined on the basis of practical recommendations of experts from Division "K" of the Ministry of Internal Affairs of the Russian Federation[16]. Using the collected numerical evidence, an expert should form a report on the conducted activities, providing recommendations for the prompt elimination of the abnormal situation.

Based on the activities described above, a table has been compiled to present the notation of the *effectiveness (completeness) indicator r* in s activities and, accordingly, the required values with its description (Table 1).

Table 1. Description of the required effectiveness when investigating an InfoSec incident

Event No.	Notation of the effectiveness indicator for event s	Description of typical results for each activity
1	r_1	Detecting non-standard methods of attacker authentication (e.g., Pass-the-Hash, Kerberoasting techniques), password brute force methods, and authentication of domain users after hours
2	r_2	Detecting malicious processes from RAM dump of "infected" machines or servers
3	r_3	Detecting the web resource through which the workstation is infected
4	r_4	Detecting the phishing email infected the workstation
5	r_5	Detecting warnings or malware in antivirus logs
6	r_6	Detecting malicious files or software in hard disk copies
7	r_7	Detecting malicious files or software as well as the presence of network connections to the attacker's command and control server from traffic

[16] Department of Information Technologies, Communications and Information Protection of the Ministry of Internal Affairs of the Russian Federation. https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/%D1%83%D0%B1%D0%BA/%D0%BF%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5 (in Russ.). Accessed March 30, 2023.

Table 1. Continued

Event No.	Notation of the effectiveness indicator for event *s*	Description of typical results for each activity
8	r_8	Detecting SIEM system warnings about a cyberattack through correlation rules and normalization of security events
9	r_9	Creating a chronology of the target attack specifying the attacker's penetration vector

Thus, the effectiveness (completeness) indicator of detection of digital artifacts r is equal to the sum of success rates of activities from the set $\{r_s\}$ described in binary form (completed/not completed). The formula for calculating the effectiveness indicator is as follows:

$$r = r_1 + r_2 + (r_3 \vee r_4) + r_5 + r_6 + r_7 + r_8 + r_9. \quad (1)$$

The suitability criterion for the effectiveness (completeness) indicator of digital artifact detection can be represented as the inequality $r > r_{req}$. The value of the required effectiveness indicator ($r_{req} = 7$) is determined based on the method of expert assessments excluding the following measures: #3 or #4 depending on the vector of the target cyberattack (logical addition is applied).

DESCRIPTION OF RESOURCE INTENSITY INDICATOR

The resource intensity indicator p is determined by the availability of forensic software tools in cyber incident investigation along with human resources. It is proposed that the software tools be divided into three subsets. Since these OSs are most common in organizations when building information and communication networks, it is necessary to conduct the analysis of network traffic from network equipment for a complete picture of the InfoSec incident:

- for analyzing Windows-like systems $\{p_{win}\}$;
- for analyzing Unix-like systems $\{p_{unix}\}$;
- for analyzing network traffic $\{p_{traf}\}$.

The proposed subsets are calculated based on available InfoSec incident investigation software tools (available/not available). Examples of these programs are presented below.

For analyzing *Windows-like systems*, computer forensic investigators should possess the necessary set of software tools such as *UserAssist*[17], *ESEDatabaseView*[18], *wmi-parser*[19], *RegRipper*[20], *NirSoft*[21] utilities (e.g., *winprefetchview*, *fulleventlogview*), Eric Zimmerman's toolkit[22] (e.g., *AmcacheParser*, *Registry Explorer*, *MFTECmd*, *AppCompatCacheParser*, and *PECmd*), and Microsoft's *Sysinternals Suite*[23] (e.g., *PSLoglist*, *Process Monitor*, *Process Explorer*, *Autoruns*, *Autologon*, etc.).

For studying *Unix-like systems*, the built-in utilities such as *dc3dd*, *ddrescue*, *Autopsy*, *LiME*, *Bulk Extractor*, *Dumpzilla*, and others should be used.

For analyzing traffic, the *wireshark*, *NetworkMiner*[24], *tcpdump*[25], *Kismet*[26], *SolarWinds Network Bandwidth Analyzer*[27], *Xplico*[28], and others are used.

The *FTK Imager*[29], *volatility3*[30], *artifactcollector*[31], *osquery*[32], and *ir-rescue*[33] utilities are cross-platform and suitable for studying popular OSs.

When investigating an InfoSec incident, department heads should understand the number of experts available for promptly conducting the event. In the study, the maximum number of computer forensic experts is defined as the staffing of the department.

Human resource (HR) costs of investigating an InfoSec incident are roughly categorized into three subsets:

- Up to 2 specialists $\{p_{two}\}$;
- Group of experts (3–5 persons) $\{p_{group}\}$;
- In-house department (10–12 persons) $\{p_{dep}\}$.

Mathematically, the relation of these sets is represented by disjunction. The coefficient k demonstrating a direct

[17] https://www.nirsoft.net/utils/userassist_view.html. Accessed April 30, 2023.

[18] https://www.nirsoft.net/utils/ese_database_view.html. Accessed April 30, 2023.

[19] https://github.com/woanware/wmi-parser/releases. Accessed April 30, 2023.

[20] https://github.com/keydet89/RegRipper3.0. Accessed April 30, 2023.

[21] https://nirsoft.net/. Accessed April 30, 2023.

[22] https://github.com/EricZimmerman/. Accessed April 30, 2023.

[23] https://learn.microsoft.com/ru-ru/sysinternals/downloads/sysinternals-suite/ (in Russ.). Accessed April 30, 2023.

[24] https://networkminer.softonic.ru/ (in Russ.). Accessed April 30, 2023.

[25] https://www.microolap.ru/products/tcpdump-for-windows/ (in Russ.). Accessed April 30, 2023.

[26] https://ru.freedownloadmanager.org/Windows-PC/Kismet-FREE.html (in Russ.). Accessed April 30, 2023.

[27] https://softradar.com/solarwinds-network-bandwidth-analyzer-pack/. Accessed April 30, 2023.

[28] https://www.xplico.org/download. Accessed April 30, 2023.

[29] https://accessdata-ftk-imager.software.informer.com/3.1/. Accessed April 30, 2023.

[30] https://github.com/volatilityfoundation/volatility3. Accessed April 30, 2023.

[31] https://github.com/forensicanalysis/artifactcollector. Accessed April 30, 2023.

[32] https://github.com/osquery/osquery. Accessed April 30, 2023.

[33] https://github.com/diogo-fernan/ir-rescue. Accessed April 30, 2023.

dependence on the number of computer forensic specialists involved in the investigation is introduced: $k_{two} = 0.8$, $k_{group} = 1$, $k_{dep} = 1.2$. These coefficients are determined on the basis of the expert evaluation method for investigating modern cyber incidents. For successfully solving the task assigned to computer forensic experts, a group of experts is required; therefore, a coefficient equal to one is assigned to this subset.

Thus, the resource intensity indicator p is equal to the product of the resource intensity indicators of three types of software described in binary form (available/not available) by the sum of the logical addition of HR availability using k factor.

Mathematically, calculation of the resource intensity indicator is represented by the following formula:

$$p = (\{p_{win}\} + \{p_{unix}\} + \{p_{traf}\}) \cdot (k_{two}\{p_{two}\} \vee \vee k_{group}\{p_{group}\} \vee k_{dep}\{p_{dep}\}). \quad (2)$$

The suitability criterion in terms of resource intensity (availability of software and HR) can be represented as inequality $p > p_{req}$. Since, in targeted cyberattacks, attackers primarily target the organization's domain in order to encrypt all data, the value of the required resource intensity indicator ($p_{req} = 3$) is determined based on the expert evaluation method excluding software tools for Unix-like systems. This also includes the value of the required resource intensity of HR availability.

DESCRIPTION OF PROMPTNESS INDICATOR

The InfoSec incident investigation timeliness indicator t is calculated based on timeframes of events ($s = 9$) conducted by the computer forensic investigator. It defines time aspects of the investigation.

The InfoSec incident investigation timeliness indicator t is calculated using the following formula:

$$t = \sum_{i=1}^{s} t_i, \quad (3)$$

where t_i is the time spent on one event.

The required timeframes for 9 events in investigating the incident given in Table 2 are calculated on the basis of the expert evaluation method in past Russian investigations. The total required investigation time t_{req} should not exceed 2 h.

The suitability criterion for the promptness indicator in conducting the InfoSec incident investigation can be represented as inequality $t < t_{req}$. The value of the required effectiveness indicator is $t_{req} = 2$.

Thus, suitability criterion G is mathematically represented based on three indicators described earlier, as follows:

$$G : \bigcap_{i=1}^{n}((r_j^i > \{r_j^{req}\}),(p_j^i > \{p_j^{req}\}),(t_j^i > \{t_j^{req}\})) \cong \cong U, [j = 1(1)m)], \quad (4)$$

Table 2. Timeframes required for nine events in InfoSec incident investigation

Event No.	Notation of the promptness indicator for event s	Required value of the event timeframe when investigating InfoSec incident, h
1	t_{1_req}	0.25
2	t_{2_req}	0.15
3	t_{3_req}	0.25
4	t_{4_req}	0.25
5	t_{5_req}	0.1
6	t_{6_req}	0.3
7	t_{7_req}	0.2
8	t_{8_req}	0.15
9	t_{9_req}	0.35
10	t_{req}	2

where U is a valid event (true statement); ∩ is a Boolean intersection symbol for events; $j = 1(1)m$ is an ordered set of variables at which the linear objective function reaches the extreme value with all constraints in the form of equalities or inequalities satisfied.

CONCLUSIONS

The paper describes indicators for assessing the quality of an investigation on the basis of the suitability criterion. An attempt has been undertaken to provide a scientific basis for the process of InfoSec incident investigation into a targeted attack, namely, to form indicators and criteria for assessing the quality of the investigation at the qualitative and quantitative level based on purposeful process efficiency theory. Since the scientific results presented in the paper more deliberative than definitive, the authors hope that they will represent a useful starting point for managers and computer forensic experts when developing scientific approaches in their professional activities.

Further planned studies will develop the mathematical apparatus for this research area to increase the number of indicators/criteria for assessing the process of investigating an InfoSec incident from modern targeted attacks.

Authors' contributions

S.I. Smirnov—description of criteria and indicators for assessing the quality of an information security investigation.

M.A. Eremeev—the idea of research, the development of aims and objectives, the formulation of conclusions.

Sh.G. Magomedov—study of digital evidence and software tools in the investigation of an information security incident.

D.A. Izergin—justification of the expediency of forming criteria and indicators for assessing the quality of the investigation of an information security incident.

REFERENCES

1. Smirnov S.I., Eremeev M.A., Gorbachev I.E., Nefedov V.S., Izergin D.A. Analysis of techniques and tools used by an attacker when moving horizontally in the corporate network. *Zashchita Informatsii. Insaid*. 2021;1(97):58–61 (in Russ.). https://www.elibrary.ru/pltlpq
2. Smirnov S.I. Cyber incident investigation methodology based on intelligent analysis of domain security events. *Zashchita Informatsii. Insaid*. 2022;4(106):60–69 (in Russ.). https://www.elibrary.ru/mefhpc
3. Smirnov S.I., Kiselev A.N., Azerskii V.D., Karel'skii D.V., Kumurzhi G.M. Comprehensive methodology for conducting an information security incident investigation. *Zashchita Informatsii. Insaid*. 2023;2(110):14–26 (in Russ.). https://www.elibrary.ru/fdhgzq
4. Makarenko S.I. Criteria and parameters for estimating quality of penetration testing. *Voprosy kiberbezopasnosti = Cybersecurity Issues J*. 2021;3(43):43–57 (in Russ.). https://www.elibrary.ru/udlknn
5. Smirnov S.I., Eremeev M.A., Pribylov I.A. Approach to Recognition of Malicious Behavior Based on Autoregression Model upon Investigation into Cyberincident. *Aut. Control Comp. Sci*. 2021;55(8):1099–1103. http://doi.org/10.3103/S0146411621080290, https://www.elibrary.ru/ubwpai
6. Zegzhda D.P., Lavrova D.S., Pavlenko E.Y. Management of a Dynamic Infrastructure of Complex Systems Under Conditions of Directed Cyber Attacks. *J. Comput. Syst. Sci. Int.* 2020;59(3):358–370. https://doi.org/10.1134/S1064230720020124 [Original Russian Text: Zegzhda D.P., Lavrova D.S., Pavlenko E.Y. Management of a Dynamic Infrastructure of Complex Systems Under Conditions of Directed Cyber Attacks. *Izvestiya Rossiiskoi akademii nauk. Teoriya i sistemy upravleniya*. 2020;3:50–63 (in Russ.). https://doi.org/10.31857/S0002338820020134]
7. Kalinin V.N., Lomako A.G., Ovcharov V.A., Petrenko S.A. Investigation of information security incidents using the behavior profiling of dynamic network objects. *Zashchita Informatsii. Insaid*. 2018;3(81):58–67 (in Russ.). https://www.elibrary.ru/xqlamp
8. Ovcharov V.A., Romanov P.A. Investigation of computer incidents based on the identification of discrete IS events and reverse analysis by final outcomes. *Trudy Voenno-kosmicheskoi akademii imeni A.F. Mozhaiskogo = Proceedings of the Mozhaisky Military Aerospace Academy*. 2015;648:84–89 (in Russ.). https://www.elibrary.ru/uzmkox
9. Lomako A.G., Ovcharov V.A., Petrenko S.A. Method for investigating security incidents based on behavior profiles of network objects. In: *Distance Educational Technologies: Materials of the Third All-Russian Scientific and Practical Conference*, September 17–22, 2018. Yalta: Arial; 2018. P. 366–373 (in Russ.). https://www.elibrary.ru/uzzdah
10. Saenko I.B., Lauta O.S., Karpov M.A., Kribel A.M. Model of threats to information and telecommunication network resources as a key asset of critical infrastructure. *Elektrosvyaz*. 2021;1:36–44 (in Russ.). https://doi.org/10.34832/ELSV.2021.14.1.004

11. Bystrov I.S., Kotenko I.V. Analysis of user behavior models for the task of detecting cyber insiders. In: *Actual Problems of Infotelecommunications in Science and Education: collection of scientific articles*: in 4 v. V. 1. St. Petersburg: Bonch-Bruevich St. Petersburg State University of Telecommunications; 2021. P. 139–143 (in Russ.). https://www.elibrary.ru/sqzvma
12. Eremeev M.A., Smirnov S.I., Pribylov I.A. Detection of malicious actions of an attacker based on event logs when investigating an ongoing cyber incident. In: *Innovative Aspects of the Development of Science and Technologies: Collection of articles of the 7th International Scientific and Practical Conference*. Saratov: Tsifrovaya nauka; 2021. P. 22–28 (in Russ.). https://www.elibrary.ru/ygoyfz
13. Avramenko V.S., Malikov A.V. Neural network model for diagnosing computer incidents in special purpose infocommunication systems. In: *Problems of Technical Support of Troops in Modern Conditions: Proceedings of the Forth Interuniversity Scientific and Practical Conference*. St. Petersburg; 2019. P. 41–45 (in Russ.). https://www.elibrary.ru/flomvh
14. Levshun D.S. Building an attacker model for a modern cyberphysical system. In: *Actual Problems of Infotelecommunications in Science and Education* (*APINO 2020*). *The 9th International Scientific-Technical and Scientific-Methodological Conference: collection of scientific articles*. V. 1. St. Petersburg: Bonch-Bruevich St. Petersburg State University of Telecommunications; 2020. P. 679–682 (in Russ.). https://www.elibrary.ru/krafgr
15. Petukhov G.B., Yakunin V.I. *Metodologicheskie osnovy vneshnego proektirovaniya tselenapravlennykh protsessov i tseleustremlennykh system* (*Methodological Foundations of External Design of Purposeful Processes and Purposeful Systems*). Moscow: AST; 2006. 504 p. (in Russ.).

СПИСОК ЛИТЕРАТУРЫ

1. Смирнов С.И., Еремеев М.А., Горбачев И.Е., Нефедов В.С., Изергин Д.А. Анализ техник и инструментов, используемых злоумышленником при горизонтальном перемещении в корпоративной сети. *Защита информации. Инсайд*. 2021;1(97):58–61. https://www.elibrary.ru/pltlpq
2. Смирнов С.И. Методика расследования киберинцидента, основанная на интеллектуальном анализе событий безопасности домена. *Защита информации. Инсайд.* 2022;4(106):60–69. https://www.elibrary.ru/mefhpc
3. Смирнов С.И., Киселев А.Н., Азерский В.Д., Карельский Д.В., Кумуржи Г.М. Комплексная методика проведения расследования инцидента информационной безопасности. *Защита информации. Инсайд*. 2023;2(110):14–26. https://www.elibrary.ru/fdhgzq
4. Макаренко С.И. Критерии и показатели оценки качества тестирования на проникновение. *Вопросы кибербезопасности*. 2021;3(43):43–57. https://www.elibrary.ru/udlknn
5. Smirnov S.I., Eremeev M.A., Pribylov I.A. Approach to Recognition of Malicious Behavior Based on Autoregression Model upon Investigation into Cyberincident. *Aut. Control Comp. Sci*. 2021;55(8):1099–1103. http://doi.org/10.3103/S0146411621080290, https://www.elibrary.ru/ubwpai
6. Зегжда Д.П., Лаврова Д.С., Павленко Е.Ю. Управление динамической инфраструктурой сложных систем в условиях целенаправленных кибератак. *Известия РАН. Теория и системы управления*. 2020;4(3):50–63. https://doi.org/10.31857/S0002338820020134
7. Калинин В.Н., Ломако А.Г., Овчаров В.А., Петренко С.А. Расследование ИБ-инцидентов с использованием профилирования поведения динамических сетевых объектов. *Защита информации. Инсайд*. 2018;3(81):58–67. https://www.elibrary.ru/xqlamp
8. Овчаров В.А., Романов П.А. Расследование компьютерных инцидентов на основе идентификации дискретных событий информационной безопасности и обратного анализа по конечным исходам. *Труды Военно-космической академии имени А.Ф. Можайского*. 2015;648:84–89. https://www.elibrary.ru/uzmkox
9. Ломако А.Г., Овчаров В.А., Петренко С.А. Метод расследования инцидентов безопасности на основе профилей поведения сетевых объектов. В сб.: *Дистанционные образовательные технологии: Материалы III Всероссийской научно-практической конференции*, 17–22 сентября 2018 г. Ялта: ООО «Издательство Типография «Ариал»; 2018. С. 366–373. https://www.elibrary.ru/uzzdah
10. Саенко И.Б., Лаута О.С., Карпов М.А., Крибель А.М. Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры. *Электросвязь*. 2021;1:36–44. https://doi.org/10.34832/ELSV.2021.14.1.004
11. Быстров И.С., Котенко И.В. Анализ моделей поведения пользователей для задачи обнаружения кибер-инсайдеров. В сб.: *Актуальные проблемы инфотелекоммуникаций в науке и образовании: сборник научных статей*: в 4 т. Т. 1. СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича; 2021. С. 139–143. https://www.elibrary.ru/sqzvma
12. Eremeev M.A., Smirnov S.I., Pribylov I.A. Detection of malicious actions of an attacker based on event logs when investigating an ongoing cyber incident. В сб.: *Инновационные аспекты развития науки и техники: Сборник статей VII Международной научно-практической конференции.* Саратов: НОО «Цифровая наука»; 2021. С. 22–28. https://www.elibrary.ru/ygoyfz
13. Авраменко В.С., Маликов А.В. Нейросетевая модель диагностирования компьютерных инцидентов в инфокоммуникационных системах специального назначения. В сб.: *Проблемы технического обеспечения войск в современных условиях: Труды IV Межвузовской научно-практической конференции*. Т. 1. СПб.; 2019. С. 41–45. https://www.elibrary.ru/flomvh

14. Левшун Д.С. Построение модели атакующего для современной киберфизической системы. В сб.: *Актуальные проблемы инфотелекоммуникаций в науке и образовании* (*АПИНО 2020*). *IX Международная научно-техническая и научно-методическая конференция: сборник научных статей*. Т. 1. СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича; 2020. С. 679–682. https://www.elibrary.ru/krafgr
15. Петухов Г.Б., Якунин В.И. *Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем*. М.: АСТ; 2006. 504 с.

About the authors

Stanislav I. Smirnov, Cand. Sci. (Eng.), Assistant Professor, Department of Intelligent Information Security Systems, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: smirnov_si@mirea.ru. Scopus Author ID 57475289100, ResearcherID HZM-3994-2023, RSCI SPIN-code 1472-6572, https://orcid.org/0000-0003-4387-0850

Mikhail A. Eremeev, Dr. Sci. (Eng.), Professor, Department of Information and Analytical Cybersecurity Systems, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: eremeev_m@mirea.ru. Scopus Author ID 57188205500, RSCI SPIN-code 3609-5733, https://orcid.org/0000-0002-5511-4000

Shamil G. Magomedov, Cand. Sci. (Eng.), Associate Professor, Head of the Department of Intelligent Information Security Systems, Institute of Cyber Security and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). msgg@list.ru. Scopus Author ID 57204759220, ResearcherID M-5782-2016, RSCI SPIN-code 5029-8310, https://orcid.org/0000-0001-8560-1937

Dmitry A. Izergin, Cand. Sci. (Eng.), Assistant Professor, Department of Digital Data Processing Technologies, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: izergin@mirea.ru. Scopus Author ID 57224822181, RSCI SPIN-code 2318-9152, https://orcid.org/0000-0002-3174-4550

Об авторах

Смирнов Станислав Игоревич, к.т.н., доцент, кафедра интеллектуальных систем информационной безопасности, Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: smirnov_si@mirea.ru. Scopus Author ID 57475289100, ResearcherID HZM-3994-2023, SPIN-код РИНЦ 1472-6572, https://orcid.org/0000-0003-4387-0850

Еремеев Михаил Алексеевич, д.т.н., профессор, кафедра информационно-аналитических систем кибербезопасности, Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: eremeev_m@mirea.ru. Scopus Author ID 57188205500, SPIN-код РИНЦ 3609-5733, https://orcid.org/0000-0002-5511-4000

Магомедов Шамиль Гасангусейнович, к.т.н., доцент, заведующий кафедрой интеллектуальных систем информационной безопасности, Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: msgg@list.ru. Scopus Author ID 57204759220, ResearcherID M-5782-2016, SPIN-код РИНЦ 5029-8310, https://orcid.org/0000-0001-8560-1937

Изергин Дмитрий Андреевич, к.т.н., доцент, кафедра цифровых технологий обработки данных, Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: izergin@mirea.ru. Scopus Author ID 57224822181, SPIN-код РИНЦ 2318-9152, https://orcid.org/0000-0002-3174-4550

Translated from Russian into English by Kirill V. Nazarov
Edited for English language and spelling by Thomas A. Beavitt