Russian Technological Journal.
2024;12(3):25–36

ISSN 2782-3210 (Print)
ISSN 2500-316X (Online)

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

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.

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.

ВВЕДЕНИЕ

Геополитические события в мире за последние годы в большой степени повлияли на возросшую активность хакерских группировок. Согласно итоговому отчету за 2022 г. компании Positive Technologies[1] количество инцидентов информационной безопасности (ИБ) за прошедший год увеличилось на 20.8%, среди них объем успешных целенаправленных атак с использованием программ-вымогателей (шифровальщиков) составил 51%. Практика реагирования на современные инциденты ИБ показывает, что в последнее десятилетие количество техник и инструментов, используемых злоумышленниками при целевых атаках на информационно-телекоммуникационные сети организаций, увеличивается ежедневно [1].

В свою очередь этот факт позволяет сделать вывод о важности организация комплексного подхода при расследовании инцидента ИБ. Комплексный подход заключается в агрегации выявленных цифровых артефактов из различных систем защиты (например, SIEM-системы[2], системы обнаружения/предотвращения вторжений IDS/IPS[3], системы предотвращения утечки информации DLP[4], межсетевые экраны нового поколения NGFW[5] и др.) с построением хронологии кибератаки. В случае их отсутствия в организации специалистам намного сложнее проводить поиск криминалистически значимых данных, и поэтому увеличивается временной интервал проведения расследования. Важную роль в этом процессе играет наличие «живых» систем, в которых компьютерные криминалисты смогут снять дампы оперативной памяти.

Таким образом, можно говорить о том, что одним из перспективных научных направлений в рамках проведения расследования инцидента ИБ является создание теоретической основы с целью расчета эффективности действий компьютерных криминалистов в зависимости от имеющихся программных средств форензики и систем защиты в организации. Целью данной работы является формирование частных показателей оперативности, результативности, ресурсоемкости в рамках критерия пригодности при расследовании инцидента ИБ от целевых атак.

Статья продолжает исследования авторов [2, 3], направленные на развитие теоретического базиса при оценивании эффективности целенаправленных процессов.

ТЕРМИНОЛОГИЯ И ОСНОВНЫЕ РУКОВОДЯЩИЕ ДОКУМЕНТЫ СПЕЦИФИКИ ПРОВЕДЕНИЯ РАССЛЕДОВАНИЯ ИНЦИДЕНТА ИБ

В настоящее время существует ряд нормативных документов и инструкций коммерческих организаций, описывающих действия специалистов при расследовании и реагировании на компьютерные атаки. Вместе с тем, в государственных стандартах не определены критерии и показатели оценки качества проведения расследования киберинцидентов. Например, в руководящем документе ГОСТ Р 59709-2022[6] представлены только термины и определения, а также их взаимосвязи в рамках данных процессов. В документе ГОСТ Р 59712-2022[7] приведено только организационное описание действий подразделений управления киберинцидентами.

В методическом документе Федеральной службы по техническому и экспортному контролю «Методика оценки угроз безопасности информации»[8]

[1] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (in Russ.). Дата обращения 30.03.2023. / Accessed March 30, 2023.

[2] SIEM – security information and event management.

[3] IDS – intrusion detection system, IPS – intrusion prevention system.

[4] DLP – data leak/loss prevention.

[5] NGFW – next-generation firewall.

[6] ГОСТ Р 59709-2022. Национальный стандарт Российской Федерации. *Защита информации. Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты. Термины и определения*. М.: Росстандарт; 2022. [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.).]

[7] ГОСТ Р 59712-2022. Национальный стандарт Российской Федерации. *Руководство по планированию и подготовке к реагированию на инциденты ISO/IEC 27035-2*. М.: Росстандарт; 2022. [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.).]

[8] Методический документ «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021 г.). https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g. Дата обращения 06.04.2023. [The methodological document of the Federal Service for Technical and Export Control "Methodology for Assessing Information Security Threats". https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (in Russ.). Accessed April 06, 2023.]

перечислены десять основных тактик и соответствующие им типовые техники, используемые для построения сценариев реализации угроз безопасности информации. При разработке данного перечня за основу взята матрица MITRE ATT&CK[9]. Согласно ГОСТ Р ИСО/МЭК ТО 18044-2007[10] при обнаружении первых признаков инцидента ИБ перед компьютерными криминалистами появляется задача определения их причин. В связи с этим производится сбор цифровых артефактов, основными источниками которых являются: копии жестких дисков, дампы оперативной памяти, журналы событий безопасности, а также трафик сетевых устройств.

Ниже приведена базовая терминология процесса расследования инцидента ИБ, которая будет необходима при дальнейшем исследовании.

Компьютерная атака – целенаправленное несанкционированное сетевое компьютерное воздействие (или их последовательность) на информационный ресурс, осуществляемое нарушителем с применением программных и (или) программно-аппаратных средств и информационных технологий в целях реализации попыток нарушения и (или) прекращения функционирования информационного ресурса или реализации угрозы безопасности информации, обрабатываемой таким ресурсом[11].

Целевая кибератака – это непрерывный процесс несанкционированной активности в инфраструктуре атакуемой информационной системы (ИС), удаленно управляемый вручную в реальном времени[12].

Инцидент ИБ – это появление одного или нескольких нежелательных событий ИБ, которые могут вызвать сбой или нарушение функционирования ИС[13]. Согласно ГОСТ Р ИСО/МЭК 13335-1-2006[14] примерами киберинцидентов могут являться: утрата оборудования (устройств), ошибки пользователей системы, несоблюдение политики ИБ или рекомендаций, нарушение физических мер защиты, сбои программного обеспечения (ПО), отказы технических средств, системные сбои или перегрузки, нарушение правил доступа.

Расследование инцидента ИБ – это совокупность действий специалистов ИБ, направленных на выявление вектора целевой кибератаки, с целью минимизации ущерба и разработки рекомендаций для предотвращения инцидента ИБ в будущем [2].

Реагирование на компьютерный инцидент – это процесс (процедура, функция) автоматической (автоматизированной) обработки компьютерного инцидента[15].

Цифровой артефакт – это потенциальное доказательство, обнаруженное на целевом устройстве (например, на персональном компьютере, мобильном устройстве, сетевом устройстве), которое может использоваться в судебной практике [3].

Криминалистически значимые данные – это компьютерная информация, используемая для обоснования выводов криминалистических исследований и позволяющая решить задачи, поставленные перед криминалистическим исследованием[16].

Классификация цифровых артефактов, которые могут быть использованы специалистами при расследовании инцидента ИБ, представлена на рисунке.

В классификации авторами определены значимые доказательства распространенных операционных систем (ОС) и сетевого трафика.

---

[9] https://attack.mitre.org/. Дата обращения 06.04.2023. / Accessed April 06, 2023.

[10] ГОСТ Р ИСО/МЭК ТО 18044-2007. Национальный стандарт Российской Федерации. *Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент инцидентов ИБ*. М.: Стандартинформ; 2007. [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.).]

[11] ГОСТ Р 59709-2022. Национальный стандарт Российской Федерации. *Защита информации. Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты. Термины и определения*. М.: Росстандарт; 2022. [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.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (in Russ.). Дата обращения 14.03.2023. / Accessed March 14, 2023.

[13] https://normative_reference_dictionary.academic.ru/23474/ (in Russ.). Дата обращения 15.03.2023. / Accessed March 15, 2023.

[14] ГОСТ Р ИСО/МЭК 13335-1-2006. Национальный стандарт Российской Федерации. *Информационная технология. Методы и средства обеспечения безопасности.* Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. М.: Стандартинформ; 2006. [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.).]

[15] ГОСТ Р 59709-2022. Национальный стандарт Российской Федерации. *Защита информации. Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты. Термины и определения*. М.: Росстандарт; 2022. [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.).]

[16] https://www.group-ib.com/wp-content/uploads/media/2016/02/Group-IB_dbo_instruction.pdf (in Russ.). Дата обращения 13.03.2023. / Accessed March 13, 2023.

ЦИФРОВЫЕ АРТЕФАКТЫ (ДОКАЗАТЕЛЬСТВА)

Устройства под управлением ОС Windows

Корневые ветки реестра:
- SYSTEM;
- SOFTWARE;
- NTUSER.DAT (для каждого пользователя);
- USRCLASS.DAT (для каждого пользователя).

Отдельные папки или файлы из реестра:
- Amcache.hve (RecentFileCache.bcf);
- Shimcache (AppCompatCache);
- \Prefetch (*.pf);
- OBJECTS.DATA;
- \Tasks (запланированные задачи);
- базы данных User Access Loging (только для серверов).

Журналы событий:
- Security.evtx;
- System.evtx;
- WindowsPowerShell.evtx;
- Microsoft-Windows-TaskScheduler-Operational.evtx;
- Microsoft-Windows-TerminalServices-LocalSessionManager-Operational.evtx;
- Application.evtx;
- MS Exchange Management.evtx (только для серверов).

Базы данных из браузеров:
- WebCacheV*.dat (Microsoft Edge);
- *.default* (Mozilla Firefox);
- Default (Google Chrome).

Журналы средств защиты безопасности:
- журналы антивирусных средств (ESET Internet Security; Kaspersky Security; AVAST Antivirus);
- журнал Support (Windows Defender).

Устройства под управлением Unix-подобных ОС

Информация об ОС и пользовательских учетных записях:
- /etc/os-relaese;
- /etc/passwd;
- /etc/group;
- /etc/sudoers.

Информация о конфигурации ОС:
- /etc/hostname;
- /etc/tiezone;
- /etc/network/interfaces;
- команда netstat;
- команда ps;
- /etc/hosts;
- /etc/resolv.conf.

Определение используемых механизмов закрепления на ОС:
- /ect/crontab;
- /ect/init.d;
- /etc/bash.bashrc;
- /ect/profile.

Выявление следов эксплуатации системы:
- команда grep в /var/log/auth.log;
- bash_history;
- ~/.viminfo.

Выявление следов действий злоумышленника посредством журнала событий:
- /var/log/syslog;
- /var/log/auth;
- /var/log/apache2.

Анализ сетевого трафика

Примеры фильтрации в трафике:
- фильтрация по определенным протоколам;
- фильтрация по определенным ip-адресам;
- фильтрация по определенным номерам портов;
- фильтрация по определенным mac-адресам;
- фильтрация TCP сегментов по флагам;
- фильтрация прикладного уровня по методам передачи/отправления данных;
- фильтрация для поиска файлов определенного типа;
- поиск по содержимому сертификатов;
- фильтрация по выявлению проксирования;
- фильтрация Wi-Fi-трафика;
- следование по определенному потоку протокола TCP.

Примеры аномалий в трафике:
- длинные доменные имена;
- активное сканирование внешних ip-адресов по всем портам;
- большое количество сегментов с флагом SYN по определенному порту (атака типа «перебор пароля»);
- перехват сессий служб удаленного доступа;
- большой объем передаваемых данных с рабочих станций или серверов во внешнюю среду.

Рисунок. Классификация цифровых артефактов. TCP – Transmission Control Protocol

Стоит отметить, что формирование критериев и показателей оценки качества проведения расследования киберинцидента может повысить эффективность данного процесса, и, следовательно, процесса реагирования на компьютерную атаку с целью минимизации финансового и репутационного ущерба для организации. Таким образом, чем качественнее будет проведено специалистами расследование киберинцидента, тем оперативнее они смогут на него отреагировать и остановить данный вредоносный процесс.

ОБЗОР АКТУАЛЬНЫХ РАБОТ В ОБЛАСТИ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ ИБ

Практическим вопросам расследования инцидентов ИБ посвящены работы С.И. Макаренко [4], М.А. Еремеева [5], П.Д. Зегжды, Д.П. Зегжды [6], А.Г. Ломако [7], В.А. Овчарова [8], С.А. Петренко [9], И.Б. Саенко [10], И.В. Котенко [11], И.А. Прибылова [12], В.С. Авраменко [13], Д.С. Левшуна [14].

В настоящее время существуют отечественные инструкции коммерческих организаций, описывающие действия специалистов по реагированию на киберинциденты. Эти инструкции имеют ряд недостатков.

Сотрудники компании F.A.C.C.T (ранее Group-IB в России) разработали инструкцию[17] по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания. Недостатком данного документа является возможность его использования только в ИС кредитно-финансовых организаций.

В руководстве[18] сотрудниками Лаборатории Касперского описаны действия специалистов по реагированию на инциденты ИБ. Данный документ не является универсальной инструкцией. В нем описано только применение основных инструментов для сбора данных, анализа потенциальных угроз и их удаления. Данное руководство требует внесения изменений на основе знаний о современных техниках и способах, применяемых злоумышленниками.

В диссертационной работе[19] автором введен обобщенный показатель вредоносной аутентификационной активности злоумышленника, основанный на показателе полноты выявления аутентификационных действий, совершаемых злоумышленником при «горизонтальном перемещении» в домене, и показателе оперативности расследования киберинцидента. Данный показатель можно рассматривать только в случае кибератаки на домен организации.

Анализ указанных работ в области расследования киберинцидентов показал следующее. Существующие документы, принятые на государственном и коммерческом уровне, описывают только примерные действия специалистов и не определяют временные интервалы, позволяющие оценивать качество проведения расследования киберинцидента.

ОПИСАНИЕ КРИТЕРИЕВ И ПОКАЗАТЕЛЕЙ ОЦЕНИВАНИЯ КАЧЕСТВА ПРОВЕДЕНИЯ РАССЛЕДОВАНИЯ ИНЦИДЕНТА ИБ В РАМКАХ ЦЕЛЕВОЙ КИБЕРАТАКИ

В теории эффективности целенаправленных процессов определено следующее понятие: *эффективность* – это комплексное операционное свойство целенаправленного процесса функционирования, характеризующее его приспособленность к выполнению стоящей перед системой задачи [15].

Понятие эффективности напрямую связано с понятием качества. *Качество* – это свойство или совокупность свойств объекта, обуславливающих его пригодность для использования по предназначению. Каждое из свойств объекта может быть описано количественно с помощью некоторой переменной, значение которой характеризует меру (интенсивность) его качества относительно этого свойства. Эту меру называют *показателем свойства* или единичным, *частным показателем качества* объекта [15].

При оценивании качества любого объекта, описываемого n-мерным векторным показателем, реализуется совокупность критериев, каждый из которых в общем случае может принадлежать одному из трех классов:

- класс $\{G\}$ критериев пригодности;
- класс $\{O\}$ оптимальности;
- класс $\{S\}$ превосходства [15].

Критерии могут быть представлены как в векторном, так и в скалярном виде.

Критерий оценивания эффективности – совокупность условий, определяющих цели операции (расследование инцидента ИБ) и в соответствии с ним пригодность, оптимальность или превосходство исследуемой операции [15].

В данной работе для исследования авторами выбран *критерий пригодности G*.

С целью оценивания качества проведения расследования инцидента ИБ в рамках целевой

[17] https://www.group-ib.com/wp-content/uploads/media/2016/02/Group-IB_dbo_instruction.pdf (in Russ.). Дата обращения 13.03.2023. / Accessed March 13, 2023.

[18] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07172131/Incident_Response_Guide_rus.pdf (in Russ.). Дата обращения 15.03.2023. / Accessed March 15, 2023.

[19] Смирнов С.И. *Методика проведения расследования киберинцидента на основе автоматизированного анализа событий безопасности домена*: дис. … канд. техн. наук. СПб., 2022. 124 с. https://www.elibrary.ru/item.asp?id=54428705. Accessed March 25, 2023. [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. (in Russ.). https://www.elibrary.ru/item.asp?id=54428705. Accessed March 25, 2023.]

кибератаки (в т.ч. и продолжающейся) авторами предложены следующие показатели:

- показатель результативности (полноты) выявления цифровых артефактов компьютерным криминалистом на основе проведенных мероприятий – *r*;
- показатель ресурсоемкости (наличие программных продуктов форензики и затраты людских ресурсов) – *p*;
- показатель оперативности расследования инцидента ИБ – *t*.

ОПИСАНИЕ ПОКАЗАТЕЛЯ РЕЗУЛЬТАТИВНОСТИ

Показатель результативности определен степенью полноты выявления цифровых артефактов *r* напрямую зависит от девяти основных мероприятий, предложенных авторами, реализуемых при проведении расследования:

1) сбор и анализ журналов событий контроллера домена и рабочих станций или серверов;
2) анализ процессов из дампа оперативной памяти рабочих станций или серверов;
3) анализ истории браузеров рабочих станций;
4) анализ почтовых сообщений рабочих станций;
5) анализ журналов антивирусных систем, имеющихся в организации;
6) анализ копий жестких дисков с рабочих станций или серверов;
7) анализ трафика с имеющихся сетевых устройств (маршрутизаторы, межсетевые экраны) и с системы обнаружения/предотвращения вторжений (при ее наличии);
8) анализ событий SIEM-системы (при ее наличии);
9) построение хронологии (таймлайна) целевой атаки.

Основные мероприятия определены на основе практических рекомендаций сотрудников Управления «К» МВД РФ[20]. Используя собранные цифровые доказательства, специалист должен сформировать отчет о проводимых мероприятиях, в котором будут даны рекомендации по оперативному устранению нештатной ситуации.

[20] Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации. 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 Дата обращения 30.03.2023 г. [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.]

На основе описанных выше мероприятий составлена таблица, в которой представлены условные обозначения *показателя результативности* (*полноты*) *r* в *s* мероприятиях и, соответственно, требуемых значений с его описанием (табл. 1).

Таблица 1. Описание требуемого уровня результативности при проведении мероприятий с целью расследования инцидента ИБ

№ мероприятия	Условное обозначение показателя результативности мероприятия *s*	Описание типовых результатов при проведении каждого мероприятия
1	r_1	Выявление нестандартных способов аутентификации злоумышленника (например, техники Pass-the-Hash, Kerberoasting), методов перебора пароля, аутентификация пользователей домена в нерабочее время
2	r_2	Выявление вредоносных процессов из дампа оперативной памяти «зараженных» машин или серверов
3	r_3	Выявление веб-ресурса, посредством которого произошло заражение рабочей станции
4	r_4	Выявление «фишингового» письма, посредством которого произошло заражение рабочей станции
5	r_5	Выявление в журналах антивирусных систем предупреждений или вредоносного ПО
6	r_6	Выявление в копиях жестких дисков вредоносных файлов или ПО
7	r_7	Выявление вредоносных файлов или ПО, наличие сетевых подключений к командному серверу злоумышленника из трафика
8	r_8	Выявление предупреждений SIEM-системы о кибератаке посредством правил корреляции, нормализации событий безопасности
9	r_9	Построение хронологии целевой атаки с указанием вектора проникновения злоумышленника

Таким образом, показатель результативности (полноты) выявления цифровых артефактов r равен сумме показателей успешных проведенных мероприятий из множества $\{r_s\}$, которые описываются в бинарном виде (выполнено / не выполнено). Формула для расчета показателя результативности имеет вид:

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

Критерий пригодности по показателю результативности (полноты) выявления цифровых артефактов можно представить в виде неравенства $r > r_{req}$. Значение требуемого показателя результативности ($r_{req} = 7$) определено на основе метода экспертных оценок, исключая следующие мероприятия: № 3 или № 4 в зависимости от вектора целевой кибератаки (применено логическое сложение).

ОПИСАНИЕ ПОКАЗАТЕЛЯ РЕСУРСОЕМКОСТИ

Показатель ресурсоемкости p определен наличием программных средств форензики при расследовании киберинцидента и людских ресурсов. Авторами предложено провести разделение программных средств на три подмножества. Данные ОС являются самыми распространенными в организациях при построении информационно-коммуникационных сетей, при этом необходимо проведение анализа сетевого трафика с сетевого оборудования для полноты картины об инциденте ИБ:

- для анализа Windows-подобных систем – $\{p_{win}\}$;
- для анализа Unix-подобных систем – $\{p_{unix}\}$;
- для анализа сетевого трафика – $\{p_{traf}\}$.

Предложенные подмножества рассчитываются на основе имеющихся в арсенале программных средств для расследования инцидента ИБ (имеются / не имеются). Ниже представлены примеры данных программ.

Компьютерные криминалисты для анализа *Windows-подобных систем* должны иметь в своем арсенале необходимый набор программных средств таких как *UserAssist*[21], *ESEDatabaseView*[22], *wmi-parser*[23], *RegRipper*[24], утилиты *NirSoft*[25] (например, *winprefetchview*, *fulleventlogview*), набор инструментов Эрика Циммермана[26] (например, *AmcacheParser*, *Registry Explorer*, *MFTECmd*, *AppCompatCacheParser*, *PECmd*), набор программ *Sysinternals Suite* от компании Microsoft[27] (например, *PSLoglist*, *Process Monitor*, *Process Explorer*, *Autoruns*, *Autologon* и др.).

Для исследования *Unix-подобных систем* стоит использовать встроенные утилиты такие как *dc3dd*, *ddrescue*, *Autopsy*, *LiME*, *Bulk Extractor*, *Dumpzilla* и др.

Для анализа *трафика* стоит применять *wireshark*, *NetworkMiner*[28], *tcpdump*[29], *Kismet*[30], *SolarWinds Network Bandwidth Analyzer*[31], *Xplico*[32] и др.

Утилиты *FTK Imager*[33], *volatility3*[34], *artifactcollector*[35], *osquery*[36], *ir-rescue*[37] являются кроссплатформенными и подходят для исследования популярных ОС.

При расследовании инцидента ИБ руководителям подразделений необходимо понимать количество специалистов, которые смогут оперативно провести данное мероприятие. Максимальное значение количества компьютерных криминалистов авторами определено в исследовании как штатная численность отдела.

Затраты людских ресурсов при расследовании инцидента ИБ условно разделены на три подмножества:

- до 2 специалистов – $\{p_{two}\}$;
- группа специалистов (3–5 чел.) – $\{p_{group}\}$;
- штатный отдел (10–12 чел.) – $\{p_{dep}\}$.

[21] https://www.nirsoft.net/utils/userassist_view.html. Дата обращения 30.04.2023. / Accessed April 30, 2023.

[22] https://www.nirsoft.net/utils/ese_database_view.html. Дата обращения 30.04.2023. / Accessed April 30, 2023.

[23] https://github.com/woanware/wmi-parser/releases. Дата обращения 30.04.2023. / Accessed April 30, 2023.

[24] https://github.com/keydet89/RegRipper3.0. Дата обращения 30.04.2023. / Accessed April 30, 2023.

[25] https://nirsoft.net/. Дата обращения 30.04.2023. / Accessed April 30, 2023.

[26] https://github.com/EricZimmerman/. Дата обращения 30.04.2023. / Accessed April 30, 2023.

[27] https://learn.microsoft.com/ru-ru/sysinternals/downloads/sysinternals-suite/ (in Russ.). Дата обращения 30.04.2023. / Accessed April 30, 2023.

[28] https://networkminer.softonic.ru/ (in Russ.). Дата обращения 30.04.2023. / Accessed April 30, 2023.

[29] https://www.microolap.ru/products/tcpdump-for-windows/ (in Russ.). Дата обращения 30.04.2023. / Accessed April 30, 2023.

[30] https://ru.freedownloadmanager.org/Windows-PC/Kismet-FREE.html (in Russ.). Дата обращения 30.04.2023. / Accessed April 30, 2023.

[31] https://softradar.com/solarwinds-network-bandwidth-analyzer-pack/. Дата обращения 30.04.2023. / Accessed April 30, 2023.

[32] https://www.xplico.org/download. Дата обращения 30.04.2023. / Accessed April 30, 2023.

[33] https://accessdata-ftk-imager.software.informer.com/3.1/. Дата обращения 30.04.2023. / Accessed April 30, 2023.

[34] https://github.com/volatilityfoundation/volatility3. Дата обращения 30.04.2023. / Accessed April 30, 2023.

[35] https://github.com/forensicanalysis/artifactcollector. Дата обращения 30.04.2023. / Accessed April 30, 2023.

[36] https://github.com/osquery/osquery. Дата обращения 30.04.2023. / Accessed April 30, 2023.

[37] https://github.com/diogo-fernan/ir-rescue. Дата обращения 30.04.2023. / Accessed April 30, 2023.

Математически соотношение данных множеств представлено посредством дизъюнкции. Авторами работы введен коэффициент k, который показывает прямую зависимость от числа задействованных в расследовании компьютерных криминалистов: $k_{two} = 0.8$, $k_{group} = 1$, $k_{dep} = 1.2$. Данные коэффициенты определены на основе метода экспертных оценок исходя из практики расследования киберинцидентов современности. Для успешного решения поставленной перед компьютерными криминалистами задачи необходимо иметь группу специалистов, поэтому данному подмножеству присвоен коэффициент, равный единице.

Таким образом, показатель ресурсоемкости p равен произведению показателей ресурсоемкости трех разновидностей ПО, которые описываются в бинарном виде (в наличии / отсутствуют) на сумму показателей по логическому сложению наличия людских ресурсов с применением коэффициента k.

Математически расчет показателя ресурсоемкости представлен формулой:

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

Критерий пригодности по показателю ресурсоемкости (наличия программных средств и людских ресурсов) можно представить в виде неравенства $p > p_{req}$. Значение требуемого показателя ресурсоемкости ($p_{req} = 3$) определено на основе метода экспертных оценок, исключая программные средства для Unix-подобных систем, т.к. при целевых кибератаках злоумышленники в первую очередь нацелены на домен организации с целью шифрования всех данных. Также в него входит значение требуемого показателя ресурсоемкости наличия людских ресурсов.

ОПИСАНИЕ ПОКАЗАТЕЛЯ ОПЕРАТИВНОСТИ

Показатель оперативности расследования инцидента ИБ t рассчитывается на основе временных интервалов мероприятий ($s = 9$), проводимых компьютерным криминалистом. Он определяет временные аспекты проведения расследования.

Показатель оперативности расследования инцидента ИБ t рассчитывается по формуле:

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

где t_i – время, затраченное на одно мероприятие.

Требуемые временные интервалы 9 мероприятий при расследовании инцидента приведены в табл. 2. Они рассчитаны на основе метода экспертных оценок. Общее требуемое время расследования t_{req} не должно превышать двух часов.

Таблица 2. Требуемые временные интервалы девяти мероприятий при расследовании инцидента ИБ

№ мероприятия	Условное обозначение требуемого показателя оперативности мероприятия s	Требуемое значение временного интервала мероприятия при расследовании инцидента ИБ, час
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

Критерий пригодности по показателю оперативности проведения расследования инцидента ИБ можно представить в виде неравенства $t < t_{req}$. Значение требуемого показателя результативности ($t_{req} = 2$).

Таким образом, критерий пригодности G математически представлен следующим образом на основе трех описанных ранее показателей:

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

где U – достоверное событие (истинное высказывание); $\cap$ – символ булева пересечения событий, $j = 1(1)m$ – упорядоченная совокупность переменных, при которых линейная целевая функция достигает экстремального значения и при этом выполняются (или удовлетворяются) все ограничения в форме равенств или неравенств.

ЗАКЛЮЧЕНИЕ

В статье на основе критерия пригодности описаны показатели оценки качества проведения расследования. Авторами предпринята попытка подвести научную основу под процесс расследования инцидента ИБ от целевой атаки, а именно – на качественном и количественном уровнях сформировать показатели и критерии оценки качества его проведения на основе теории эффективности целенаправленных процессов. Научные результаты, представленные в данной работе, не являются окончательными, а носят дискуссионный характер. Авторы надеются, что

статья станет своеобразной «отправной точкой» для руководителей и специалистов в сфере компьютерной криминалистики при формировании научных подходов в их служебной деятельности.

В дальнейших работах планируется развитие математического аппарата в данной области исследования и увеличение числа показателей/критериев оценивания процесса расследования инцидента ИБ от целевых атак современности.

Вклад авторов

С.И. Смирнов – описание критериев и показателей оценивания качества проведения расследования ИБ.

М.А. Еремеев – идея исследования, развитие цели и задач, формулировка выводов.

Ш.Г. Магомедов – изучение цифровых доказательств и программных средств при расследовании инцидента ИБ.

Д.А. Изергин – обоснование целесообразности формирования критериев и показателей оценки качества проведения расследования инцидента ИБ.

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.

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.

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.).

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

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