Труды МАИ. 2026. № 148.

Trudy MAI. 2026. No. 148. (In Russ.)

Научная статья
УДК 004.056.52
URL: https://trudymai.ru/published.php?ID=188518
EDN: https://www.elibrary.ru/DSPNUX

АКТУАЛЬНЫЕ МЕТОДЫ ПОСТРОЕНИЯ ПРАВИЛ ОБНАРУЖЕНИЯ И СПОСОБЫ ИХ РЕАЛИЗАЦИИ НА СТЕКЕ OPENSEARCH

П.В. Пилькевич, А.Г. Спеваков✉, С.В. Спевакова

Федеральное государственное автономное образовательное учреждение высшего образования «Московский политехнический университет»,
г. Москва, Россия

✉ aspev@yandex.ru

Цитирование: Пилькевич П.В., Спеваков А.Г., Спевакова С.В. Актуальные методы построения правил обнаружения и способы их реализации на стеке Opensearch // Труды МАИ. 2026. № 148. URL: https://trudymai.ru/published.php?ID=188518

Аннотация. В статье рассматриваются способы формирования новых правил обнаружения в условиях развивающегося центра мониторинга инцидентов с целью ускорения реагирования на опасные происшествия в контуре предприятия авиационной отрасли. Научная новизна заключается в применении нового метода конвертации правил обнаружения формата Sigma в формат, поддерживаемый плагином Opensearch Alerting. Практическая ценность заключается в возможности поддержки унифицированного формата правил обнаружения, что способствует быстрой актуализации центра мониторинга с современными практиками обнаружения. Проведено исследование плагина Opensearch Alerting, отвечающего за поддержку правил обнаружения. Анализ структуры сущностей плагина показал широкий функционал и высокий порог входа для начала разработки. Была определена ключевая составляющая центров мониторинга – правила обнаружения инцидентов и процесс их непрерывной разработки, в связи с чем сформирована таблица с возможными источниками данных для разработки новых правил. В ходе сравнительного анализа установлен самый эффективный источник данных – открытые репозитории с

правилами в формате Sigma. На примере Sigma-правила, включающего в себя сложные функциональные элементы, было установлено соответствие сущностей в структуре правил двух форматов – Opensearch Alerting и Sigma. В результате установления соответствия, был разработан универсальный шаблон в формате Jinja2 для бесшовной конвертации Sigma-правил в правила Opensearch Alerting.
Ключевые слова: информационная безопасность; мониторинг безопасной разработки; SIEM-системы; обнаружение инцидентов; корреляция событий; правила обнаружения Opensearch.

CURRENT METHODS FOR CONSTRUCTING DETECTION RULES AND APPROACHES FOR THEIR IMPLEMENTATION ON THE OPENSEARCH STACK

P.V. Pilkevich, A.G. Spevakov✉, S.V. Spevakova

Moscow Polytechnic University, Moscow, Russia

✉ aspev@yandex.ru

Citation: Pilkevich P.V., Spevakov A.G., Spevakova S.V. Current methods for constructing detection rules and approaches for their implementation on the Opensearch stack // Trudy MAI. 2026. No. 148. (In Russ.). URL: https://trudymai.ru/published.php?ID=188518

Abstract. This article examines methods for developing new detection rules within an evolving Security Operations Center (SOC) to accelerate the response to security incidents in the infrastructure of an aviation industry enterprise. The scientific novelty of the work lies in the application of a novel method for converting detection rules from the Sigma format into a format supported by the OpenSearch Alerting plugin. The practical significance is the ability to maintain a unified detection rule format, which facilitates the rapid updating of the SOC with modern detection practices. A study of the OpenSearch Alerting plugin, which is responsible for supporting detection rules, was conducted. An analysis of the plugin's entity structure revealed extensive functionality but also a high barrier to entry for initial development. The key component of SOCs incident detection rules and their continuous development process was identified. Consequently, a table of potential data sources for developing new rules was compiled. A comparative analysis established the most effective data source: open repositories with rules in the Sigma format. Using a sample Sigma rule that included complex

functional elements, a correspondence between the entities in the structure of the two rule formats—OpenSearch Alerting and Sigma—was established. Based on this established correspondence, a universal Jinja2 template was developed for the seamless conversion of Sigma rules into OpenSearch Alerting rules.

Keywords: cybersecurity; software development life cycle; monitoring of secure development; SIEM systems; incident detection; event correlation, Opensearch detection rules.

Введение

За последний год рынок SOC в России вырос более чем на 30%. Особенно остро ощущается рост атак на предприятия авиационной сферы, что вынуждает соответствующие компании развивать свою инфраструктуру защиты. Такая тенденция связана с продолжающимся ростом кибератак на ключевую информационную инфраструктуру крупных компаний [1]. Эта же тенденция замечена и в других странах. Основой борьбы с атаками является бесперебойный мониторинг событий внутри всей информационной инфраструктуры, именно эту услугу и оказывают современные SOC. В основе своевременного обнаружения и реагирования на инциденты в контуре лежит грамотно построенный набор правил, отвечающих за поиск критических цепочек событий, которые информируют о возможных угрозах и нарушителях [2].

Целью работы является повышение эффективности обнаружения инцидентов системами мониторинга на базе Opensearch за счёт обеспечения их совместимости с правилами корреляции Sigma.

Объект исследования: процесс обеспечения безопасности информационной инфраструктуры с использованием систем мониторинга на базе OpenSearch.

Предмет исследования: механизм построения и оптимизации правил обнаружения киберугроз в системах мониторинга на базе OpenSearch.

Материалы и методы

Одной из наиболее подходящих векторных баз данных для построения SOC в нынешних условиях является Opensearch. Обусловлено это широким спектром функциональных возможностей, полностью открытым исходным кодом, что

позволяет доработать систему под требования заказчиков, использование проверенных практикой и временем технологий из Elasticsearch. Однако, механизм разработки правил обнаружения является трудоёмким из-за сложного синтаксиса плагина Alerting, который и отвечает за правила обнаружения в данной системе. На рисунке 1 представлена упрощённая схема, которая описывает взаимодействие компонентов правила обнаружения Opensearch между собой. Анализ диаграммы позволяет сделать вывод о широком функционал в области обнаружения и преобразования данных, но вместе с тем, очень высокий порог входа и отсутствие унификации с другими системами обнаружения. Основной сущностью является Monitor, который, фактически, и представляет из себя цельное правило обнаружение. В Monitor присутствует Trigger (механизм, отвечающий за срабатывание правила по какому-либо условию), Action (действие при сработке правила), Notification (специальная сущность для оповещения узлов о сработке правила), а также Input, в котором находятся поисковые запросы и агрегации, собирающие данные из событий для правила.

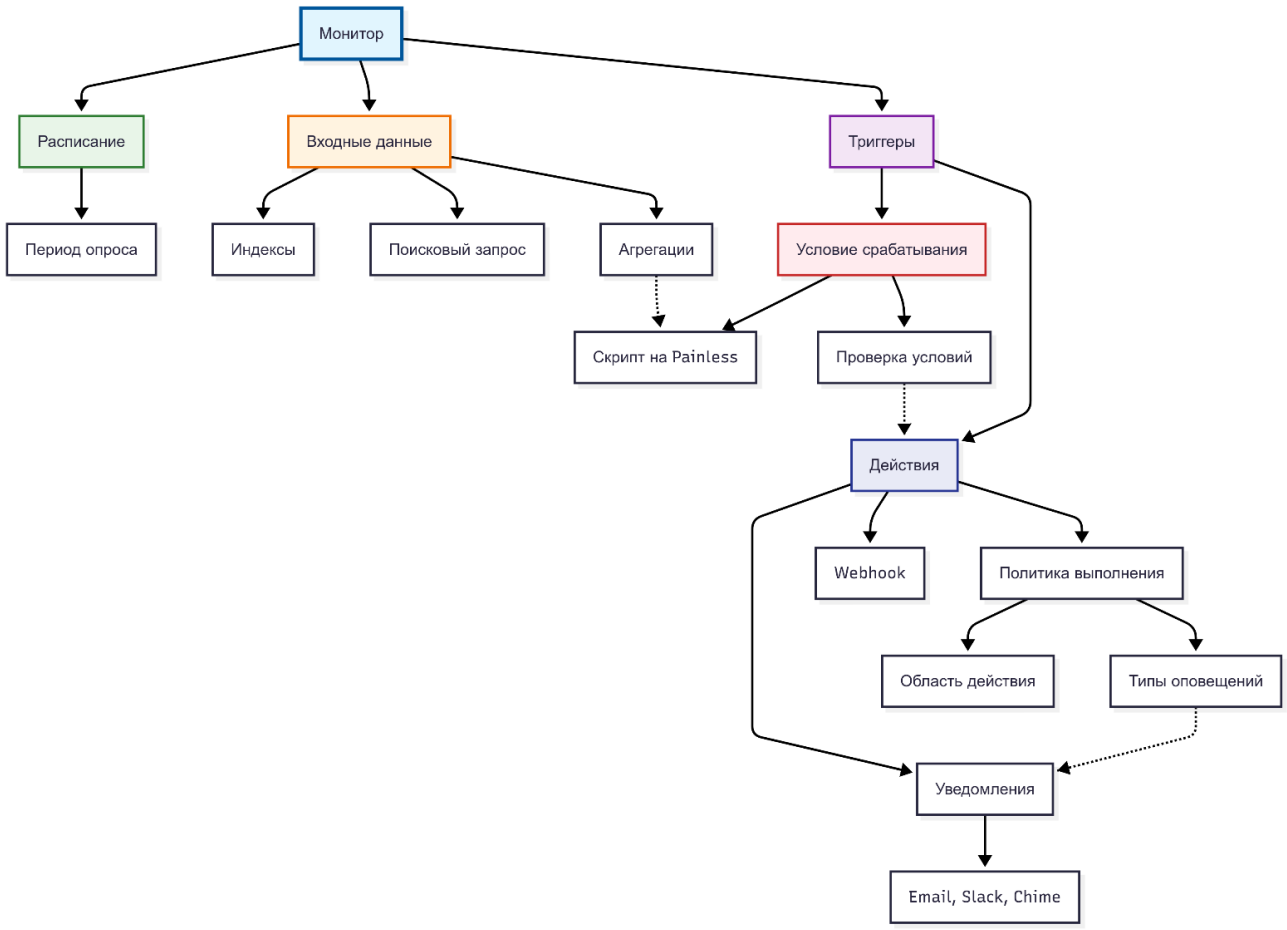

Рисунок 1 – Общая схема взаимодействия компонентов правила обнаружения Opensearch

Основой эффективно функционирующей системы мониторинга являются актуальные правила обнаружения и эффективная методика их создания. Методика должна определять набор сценариев, для которых требуется подготовить правила, а также обеспечивать быстрое создание, тестирование и внедрение данных правил [3]. Подбор сценариев обнаружения является проблематичной и трудоёмкой задачей, так как большое количество угроз может помешать сформировать вектор развития разрабатываемой системы мониторинга [4]. В таблице 1 приведены источники, которые могут послужить основой для построения правил системы мониторинга.

Таблица 1

Источники данных для построения новых правил обнаружения

Источник	Описание	Примеры
Модели угроз (Threat Models)	Формализованное представление угроз для конкретной инфраструктуры.	MITRE ATT&CK – главный источник. Представляет из себя набор тактики, техник и процедур (TTPs) злоумышленников.
Бенчмарки	Описывают нормальное и безопасное состояние систем.	CIS Benchmarks, рекомендации производителей ОС (Microsoft, Linux), сетевого оборудования.
Анализ инцидентов	Анализ зарегистрированных ранее инцидентов	Результаты расследования прошлых инцидентов, анализ корневых причин.
Новости и отчеты ИБ	Актуальная информация о новых угрозах, уязвимостях (CVEs) и методах атак.	Отчеты Kaspersky, Mandiant, CrowdStrike, CISA (US-CERT), SANS Internet Storm Center.
Открытые сообщества и GitHub	Готовые правила и обсуждения от сообщества.	Sigma репозитории (основной репозиторий SigmaHQ), форумы по конкретным SIEM (Splunk, Elastic, ArcSight).
Уже существующие логи	Набор сырых событий от существующих источников системы мониторинга.	Документация к приложению, логирование действий администраторов и пользователей.

Ряд источников из приведённой выше таблицы подразумевает наличие уже функционирующей системы мониторинга, что делает невозможным их

применение ранних этапах создания системы. Наиболее эффективным вариантом в данном случае является использование уже ранее подготовленных правил, которые написаны в универсальном формате Sigma [5]. Преимуществом использования данного источника является большое количество существующих открытых репозиториев с готовыми правилами. Такие репозитории не только служат непосредственным источником данных, но и позволяют определить дальнейший вектор развития своей собственной методики формирования сценариев [6]. Вторым фундаментальным преимуществом использования Sigma является унифицированный формат описания правил, который не привязан ни к одной из платформ. При этом, данный формат поддерживает написание не только простых правил, работающих в роли фильтра событий, но и сложных, включающих в себя группировки полей, обратные фильтры, подсчёт количества вхождений и другое [7].

Opensearch не поддерживает формат Sigma, поэтому необходимо проанализировать структуру объектов правил обнаружения обеих систем, разработать шаблон и стратегию конвертации формата сценариев Sigma в формат сценариев Opensearch [8]. На рисунке 2 представлен пример сложного Sigma-правила.

```
detection:
  selection:
    process|contains:
      - 'New-LocalUser'
      - 'net user /add'
  filter:
    src|endswith:
      - '-adm01.domain.com'
      - '.management.domain.com'
    user|endswith:
      - '@domain.com'
  aggregation:
    timeframe: 5m
    group-by:
      - src_ip
    count: 3
    condition: selection and not filter
  condition: aggregation
```

Рисунок 2 – Основные поля правила в формате Sigma для обнаружения инцидента нелегитимного создания нового локального пользователя через Powershell

Основная логика правила заложена в секции detection, где указывается требование к полю process по содержанию строчек New-LocalUser и net user /add [9]. При этом, с помощью секции filters, исключаются все события с определённым именем хоста (по полю src), а также создание доменных пользователей (по полю users) [10]. В секции aggregation представлена группировка событий, подпадающих под фильтр, по полю хоста источника события. За 5 минут ожидается увидеть, как минимум 3 события, после чего следует создание инцидента информационной безопасности [11].

Все функциональные элементы формата Sigma, в том числе для сложных правил, могут быть воспроизведены в Opensearch. На рисунке 3 представлена схема соответствия сущностей Opensearch и Sigma.

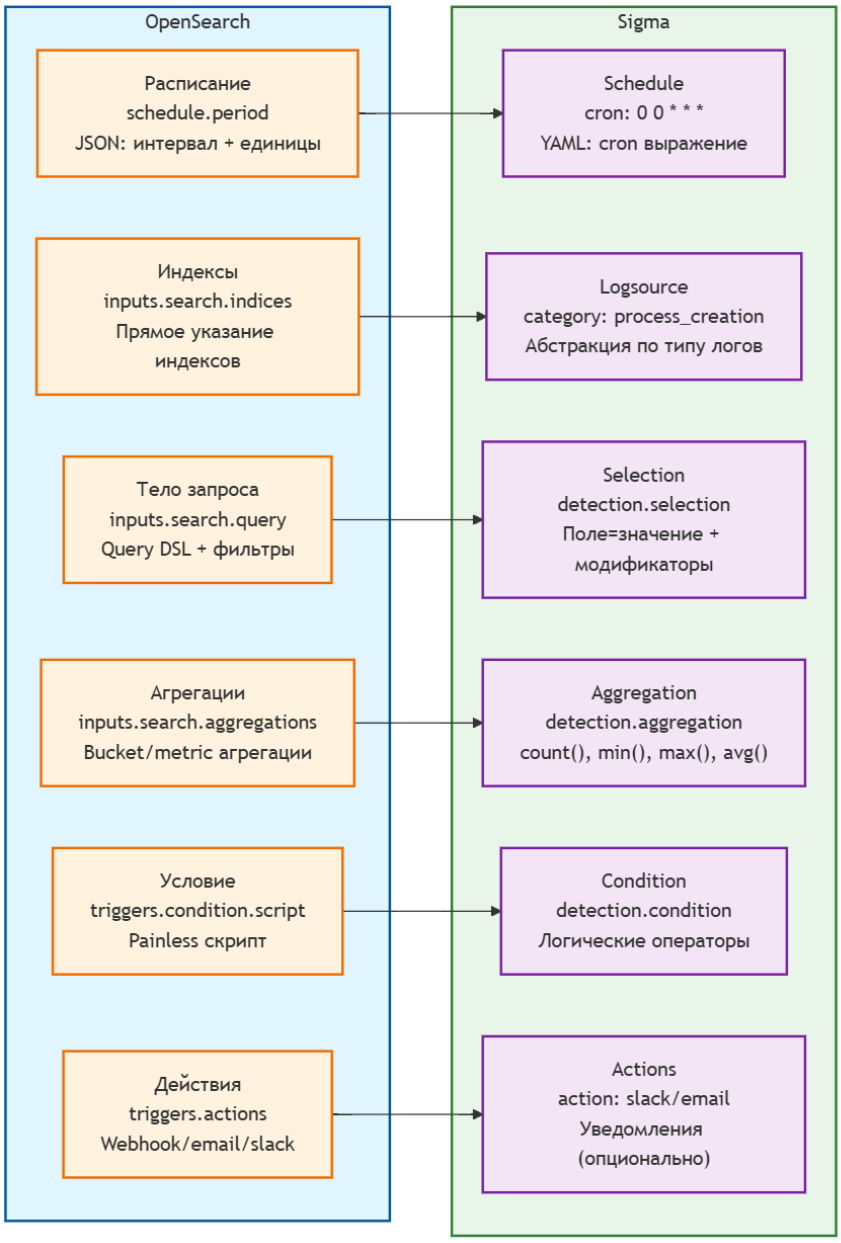

Рисунок 3 – Соответствие сущностей Opensearch и Sigma

На основании полученной схемы, можно разработать универсальный шаблон правила Opensearch, позволяющий обеспечить совместимость двух систем. На рисунке 4 представлен результат.

```
{
 "schedule": {
  "period": {
   "interval": {{sigma.aggregation.timeframe | default: 5}}
  }
 },
 "inputs": [
  {
   "search": {
    "indices": ["{{sigma.logsource.category}}"],
    "query": {
     "query": {
      "bool": {
       "must": [
        {{#each sigma.detection.selection}}
        {"term": {"{{@key}}": "{{this}}"}}{{#unless @last}},{{/unless}}{{/each}}
       ]
      }
     },
     {{#if sigma.aggregation}}
     "aggregations": {
      "group_by": {
       "terms": {
        "field": "{{sigma.aggregation.group-by.0}}",
        "size": 100
       }
      }
     }
     {{/if}}
    }
   }
  }
 ],
 "triggers": [
  {
   "{{#if sigma.aggregation}}bucket_level_trigger{{else}}query_level_trigger{{/if}}": {
    "name": "trigger",
    "severity": "{{sigma.level | default: 'medium'}}",
    "condition": {
     {{#if sigma.aggregation}}
     "script": {
      "source": "params._count >= {{sigma.aggregation.count}}"
     }
     {{else}}
     "script": {
      "source": "ctx.results[0].hits.total.value > 0"
     }
     {{/if}}
    },
   }
  }
 ]
}
```

Рисунок 4 – Универсальный шаблон правила обнаружения для Opensearch

Sigma-синтаксис полностью совместим с синтаксисом правил на Opensearch, поисковые запросы могут быть выполнены с помощью lucene-фильтров, а агрегации используются в формате Query DSL, который полностью закрывает потребности в глубоком взаимодействии с данными для обнаружения более сложных инцидентов.

Заключение

Методика формирования правил для системы мониторинга на базе существующих сценариев в формате Sigma позволяет одномоментно получить доступ к большому объёму подготовленных и протестированных сценариев, которые можно доработать под конкретные нужды. Функциональность плагина Alerting делает полностью возможным правила из формата Sigma в Query DSL. В дальнейших работах планируется разработка модуля по автоматическому переводу Sigma в Query DSL.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest

The authors declare no conflict of interest.

Список источников

1. Лесик Е. С., Падалко С. Н., Станкевич А. М. Цифровая модель организации: определение, построение, использование. //Труды МАИ. – 2025. – №. 141.

2. Касатиков Н. Н., Брехов О. М., Николаева Е. О. Интеграция технологий искусственного интеллекта и интернета вещей для расширенного мониторинга и оптимизации энергетических объектов в умных городах //Труды МАИ. – 2023. – №. 131.

3. Шаблий А. Д. Оптимизация состава комплектаций программного обеспечения. //Труды МАИ. – 2025. – №. 143.

4. Синь М. И др. Разработка системы мониторинга силовых агрегатов беспилотных летательных аппаратов в режиме реального времени. //Труды МАИ. – 2024. – №. 137.

5. Смирнов Д. В., Евсютин О. О. Методика сбора данных об активности вредоносного программного обеспечения под ОС Windows на базе MITRE ATT&CK //Информатика и автоматизация. – 2024. – Т. 23. – №. 3. – С. 642-683.

6. Герчин И. А., Анацкая А. Г. Цифровизация и кибербезопасность: современная теория и практика. – Сибирский государственный автомобильно-дорожный университет (СибАДИ) Конференция: Цифровизация и кибербезопасность: современная теория и практика Омск, 30–31 октября 2024 года Организаторы: Сибирский государственный автомобильно-дорожный университет (СибАДИ).

7. Космачева И. М. и др. Система событийного мониторинга для автоматизированного обнаружения инцидентов //Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2023. – №. 3. – С. 76-86.

8. Saulaiman M. N. E. et al. Cloud-Based Cybersecurity and Data Management System for Near Real-Time Monitoring and Alerting in Vehicle-SOC-a Proof of Concept //2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI). – IEEE, 2025. – С. 000165-000170.

9. Долгачев М. В., Костюнин В. А. Комплексный анализ поведения системы windows для обнаружения киберугроз //Вопросы кибербезопасности. – 2025. – №. 2 (66). – С. 71-77.

10. Толганбаев Т. К. Доменные службы active directory и ядро сервера //Вестник магистратуры. – 2014. – №. 6-1 (33). – С. 27-29.

11. Зефиров С. Л., Щербакова А. Ю. Оценка инцидентов информационной безопасности //Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – №. 2 (32). – С. 77-81.

12. Onsamlee W. et al. The Cyber Threat Detection and Alert System Using MISP Threat Sharing Database.

References

1. Lesik E. S., Padalko S. N., Stankevich A. M. Cifrovaya model' organizacii: opredelenie, postroenie, ispol'zovanie. //Trudy MAI. – 2025. – №. 141.
2. Kasatikov N. N., Brekhov O. M., Nikolaeva E. O. Integraciya tekhnologij iskusstvennogo intellekta i interneta veshchej dlya rasshirennogo monitoringa i optimizacii energeticheskih ob"ektov v umnyh gorodah //Trudy MAI. – 2023. – №. 131.
3. SHablij A. D. Optimizaciya sostava komplektacij programmnogo obespecheniya. //Trudy MAI. – 2025. – №. 143.
4. Sin' M. I dr. Razrabotka sistemy monitoringa silovyh agregatov bespilotnyh letatel'nyh apparatov v rezhime real'nogo vremeni. //Trudy MAI. – 2024. – №. 137.
5. Smirnov D. V., Evsyutin O. O. Metodika sbora dannyh ob aktivnosti vredonosnogo programmnogo obespecheniya pod OS Windows na baze MITRE ATT&CK //Informatika i avtomatizaciya. – 2024. – T. 23. – №. 3. – S. 642-683.
6. Gerchin I. A., Anackaya A. G. Cifrovizaciya i kiberbezopasnost': sovremennaya teoriya i praktika. – Sibirskij gosudarstvennyj avtomobil'no-dorozhnyj universitet (SibADI) Konferenciya: Cifrovizaciya i kiberbezopasnost': sovremennaya teoriya i praktika Omsk, 30–31 oktyabrya 2024 goda Organizatory: Sibirskij gosudarstvennyj avtomobil'no-dorozhnyj universitet (SibADI).
7. Kosmacheva I. M. i dr. Sistema sobytijnogo monitoringa dlya avtomatizirovannogo obnaruzheniya incidentov //Vestnik Astrahanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika. – 2023. – №. 3. – S. 76-86.
8. Saulaiman M. N. E. et al. Cloud-Based Cybersecurity and Data Management System for Near Real-Time Monitoring and Alerting in Vehicle-SOC-a Proof of Concept //2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI). – IEEE, 2025. – S. 000165-000170.
9. Dolgachev M. V., Kostyunin V. A. Kompleksnyj analiz povedeniya sistemy windows dlya obnaruzheniya kiberugroz //Voprosy kiberbezopasnosti. – 2025. – №. 2 (66). – S. 71-77.
10. Tolganbaev T. K. Domennye sluzhby active directory i yadro servera //Vestnik magistratury. – 2014. – №. 6-1 (33). – S. 27-29.

11. Zefirov S. L., SHCHerbakova A. YU. Ocenka incidentov informacionnoj bezopasnosti //Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. – 2014. – №. 2 (32). – S. 77-81.

12. Onsamlee W. et al. The Cyber Threat Detection and Alert System Using MISP Threat Sharing Database.

Информация об авторах

Павел Вадимович Пилькевич, магистрант, Московский политехнический университет, г. Москва, Россия; e-mail: pavel.piksel2012@mail.ru

Александр Геннадьевич Спеваков, к.т.н., доцент, Московский политехнический университет, г. Москва, Россия; e-mail: aspev@yandex.ru

Светлана Викторовна Спевакова, ассистент, Московский политехнический университет, г. Москва, Россия; e-mail: sspev@yandex.ru

Information about the authors

Pavel V. Pilkevich, Master's Student, Moscow Polytechnic University, Moscow, Russia; e-mail: pavel.piksel2012@mail.ru

Alexander G. Spevakov, Candidate of Technical Sciences, Associate Professor, Moscow Polytechnic University, Moscow, Russia; e-mail: aspev@yandex.ru

Svetlana V. Spevakova, Assistant, Moscow Polytechnic University, Moscow, Russia; e-mail: sspev@yandex.ru

Получено 12 ноября 2025 ● Принято к публикации 13 мая 2026 ● Опубликовано 25 июня 2026
Received 12 November 2025 ● Accepted 13 May 2026 ● Published 25 June 2026