Научная статья
DOI 10.66424/2071-8217-2026-2-3
УДК 004.056.5

МЕТОД ОПРЕДЕЛЕНИЯ ТИПИЧНЫХ ВРЕМЕННЫХ ХАРАКТЕРИСТИК СОБЫТИЙ БЕЗОПАСНОСТИ НА ОСНОВЕ СТАТИСТИЧЕСКИХ ДАННЫХ ДЛЯ ЗАДАЧ КОРРЕЛЯЦИОННОГО АНАЛИЗА

А. Д. Миханько*, И. В. Машкина

Уфимский университет науки и технологий, Уфа, Республика Башкортостан, Россия

✉ *mikhanko45@gmail.com

ДЛЯ ЦИТИРОВАНИЯ

Миханько А. Д., Машкина И. В. Метод определения типичных временных характеристик событий безопасности на основе статистических данных для задач корреляционного анализа // Проблемы информационной безопасности. Компьютерные системы. 2026. № 2. С. 32–48. DOI: 10.66424/2071-8217-2026-2-3

ПОСТУПИЛА 10.04.2026
ПРИНЯТА 13.05.2026
ОПУБЛИКОВАНА 15.06.2026

Издатель: Санкт-Петербургский политехнический университет Петра Великого

АННОТАЦИЯ

Представлен метод определения типичных временных параметров событий информационной безопасности на основе анализа журналов событий. Метод ориентирован на обработку межсобытийных интервалов и позволяет выявлять характерные временные закономерности функционирования источников событий безопасности. Предложенный подход включает: формирование выборки временных интервалов, выделение структурного разрыва межсобытийных и межсессионных интервалов, фильтрацию выбросов с использованием межквартильного размаха, определение типичных значений на основе кластеризации и группового анализа. Для учета вариативности данных применяется оценка среднего значения и стандартного отклонения с последующим разбиением на интервальные окна. Проведен численный эксперимент по данным журналов реальных событий, подтверждающий работоспособность метода при анализе источников с различной интенсивностью генерации событий. Эксперимент проведен на журналах OPC-сервера, Windows Server, СУБД PostgreSQL. Полученные результаты демонстрируют устойчивость метода к выбросам, мультимодальности распределений и наличию нулевых интервалов. Разработанный метод может быть использован при построении правил корреляции в SIEM-системах, а также в задачах анализа поведения и выявления аномалий в инфраструктуре информационной безопасности.

КЛЮЧЕВЫЕ СЛОВА

Информационная безопасность, журналы событий, SIEM, временные интервалы, межсобытийные интервалы, анализ логов, обнаружение аномалий, межквартильный размах, кластеризация, статистический анализ, корреляция событий, поведенческий анализ

Original article
DOI 10.66424/2071-8217-2026-2-3

A METHOD FOR DETERMINING TYPICAL TIME CHARACTERISTICS OF SECURITY EVENTS BASED ON STATISTICAL DATA FOR CORRELATION ANALYSIS TASKS

A. D. Mikhanko*, I. V. Mashkina

Ufa University of Science and Technology, Ufa, Republic of Bashkortostan, Russia

✉ *mikhanko45@gmail.com

FOR CITATION

Mikhanko A. D., Mashkina I. V. A method for determining typical time characteristics of security events based on statistical data for correlation analysis tasks. *Problems of information security. Computer systems*. 2026. No. 2, pp. 32–48. DOI: 10.66424/2071-8217-2026-2-3 (In Russian)

RECEIVED 10.04.2026
ACCEPTED 13.05.2026
PUBLICATION 15.06.2026

ABSTRACT

The article presents a method for determining typical time parameters of information security events based on the analysis of event logs. The method is focused on processing inter-event intervals and makes it possible to identify characteristic temporal patterns of functioning of sources of security events. The proposed approach includes sampling time intervals, identifying the structural gap between event and inter-session intervals, filtering outliers using the interquartile range, and determining typical values based on clustering and group analysis. To account for the variability of the data, an estimate of the mean and standard deviation is used, followed by a division into interval windows. A numerical experiment has been conducted based on data from real-world event logs, confirming the method's operability when analyzing sources with different event generation rates. The experiment was conducted on logs of the OPC server, Windows Server, PostgreSQL database management system. The results obtained demonstrate the method's stability to outliers, multimodal distributions, and the presence of zero intervals. The developed method can be used in the construction of correlation rules in SIEM systems, as well as in the tasks of behavior analysis and detection of anomalies in the information security infrastructure.

KEYWORDS

Information security, event logs, SIEM, time intervals, event intervals, log analysis, anomaly detection, interquartile range, clustering, statistical analysis, event correlation, behavioral analysis

1. ВВЕДЕНИЕ

Системы мониторинга информационной безопасности в информационной среде объекта защиты анализируют угрозы на основе событий безопасности. В информатике под событием понимается действие, инициированное пользователем, программой, устройством или операционной системой и зафиксированное средствами регистрации событий. Упорядоченная по времени последовательность записей о событиях образует журнал событий (или лог-файл) [1], являющийся основным источником данных для анализа информационной безопасности [2].

При этом практическая ценность журналов событий определяется не только объемом собираемых данных, но и возможностью их нормализации и последующего автоматизированного анализа [3].

В центрах обеспечения безопасности одной из основных задач является мониторинг поступающих событий информационной безопасности. Для решения этой задачи используются системы управления событиями безопасности – Security Information and Event Management (SIEM). Такие системы обеспечивают централизованный сбор, агрегацию и анализ событий, поступающих из различных источников инфраструктуры информационной системы (антивирус, межсетевой экран, системы управления базами данных (СУБД), операционные системы…) [4]. Помимо агрегации событий безопасности современные SIEM-системы, системы нового поколения (Next-Generation SIEM, SIEM-NG) и платформы аналитики безопасности (Security Analytics Platform, SAP) позволяют выявлять угрозы и инциденты информационной безопасности на основе анализа журналов событий.

Современное развитие SIEM-системы связано с их переходом от средств централизованного сбора и корреляции событий к комплексным платформам аналитики безопасности и технологическому ядру центров мониторинга безопасности (SOC). В современных SOC такие решения используются совместно с решениями классов SOAR и XDR, платформами Threat Intelligence, средствами долговременного хранения данных и компонентами поведенческой

аналитики. В результате SIEM-система рассматривается не только как средство регистрации и корреляции событий, но и как элемент единой инфраструктуры обнаружения, расследования и реагирования на инциденты информационной безопасности [4–7].

Одновременно возрастает объем и разнородность обрабатываемых журналов событий. В высоконагруженных инфраструктурах потоки событий могут достигать десятков и сотен тысяч событий в секунду, что требует масштабируемых механизмов сбора, нормализации, хранения и последующего анализа как исходных, так и нормализованных данных. В этих условиях качество предварительной обработки журналов, корректная настройка правил корреляции и учет временных характеристик событий напрямую влияют на точность выявления инцидентов и снижения числа ложноположительных срабатываний. Поэтому разработка формализованных методов определения типичных временных параметров источников событий является актуальной задачей для SIEM-систем нового поколения и последующего корреляционного анализа [4, 6–8].

В современных исследованиях отмечается, что эффективность SIEM во многом определяется количеством источников событий безопасности, качеством предварительной нормализации событий и подготовки правил [9, 10].

Большинство SIEM оснащены подсистемой корреляции событий – механизмом, предназначенным для выявления взаимосвязей между событиями безопасности. Анализ функциональных возможностей решений, представленных в ежегодном отчете Magic Quadrant компании Gartner, показывает, что несмотря на внедрение методов машинного обучения и поведенческого анализа, значительная часть механизмов корреляции по-прежнему основана на правилах корреляции, предварительно сформированных экспертами для защищаемой инфраструктуры [11].

2. АКТУАЛЬНОСТЬ ИССЛЕДОВАНИЯ

При разработке правил корреляции событий безопасности перед экспертом по информационной безопасности стоит задача формализации сценария потенциальной атаки. Для построения такого сценария, необходимо знать не только статический состав инфраструктуры (перечень узлов, систем и программного обеспечения), но и динамику протекающих процессов – скорость и последовательность действий нарушителя [12]. Ключевым источником этих сведений являются временные метки событий – это точный момент времени регистрации события в последовательности данных.

При анализе временных интервалов необходимо учитывать их распределение и вариативность. Для решения этой задачи применяется кластеризация.

Для анализа временных интервалов между событиями могут применяться различные методы кластеризации. В статье Т. А. Шевцовой [13] приводится сравнение трех методов. Метод K-means обеспечивает высокую скорость обработки данных, однако требует предварительного задания числа кластеров. Алгоритм DBSCAN позволяет автоматически выделять группы интервалов различной плотности, но чувствителен к выбору параметров. Иерархическая кластеризация позволяет выявлять структуру данных без предварительных предположений о числе кластеров, однако характеризуется высокой вычислительной сложностью.

Актуальность настоящего исследования обусловлена тем, что временные интервалы между событиями не являются детерминированной и постоянной величиной. Обычно события распределены случайным образом на рассматриваемом временном отрезке [14]. Это обстоятельство усложняет выявление взаимосвязи событий и требует применения специальных математических методов для выявления как аномалий, так и закономерностей.

В задачах информационной безопасности анализ временных и поведенческих характеристик событий обычно сопровождается применением методов выявления выбросов и аномалий, поскольку исходные данные отличаются неоднородностью и слабой предсказуемостью [15].

Целью работы является разработка метода определения типичных временных параметров событий безопасности по данным из журналов событий. Предлагаемый

метод основан на фильтрации статистических выбросов интервалов и последующей кластеризации для разделения межсобытийных и межсессионных промежутков, что позволяет вычислить эталонные значения с использованием среднего значения.

3. ПОСТАНОВКА ЗАДАЧИ

В качестве исходных данных используется журнал событий источника безопасности за продолжительный период T. Журнал событий представлен упорядоченной последовательностью событий:

$$E = \{e_1, e_2, ..., e_i, ..., e_I\},$$

где e_i – i-е событие в журнале, $i = \{1, 2, ..., I\}$; I – количество записей в журнале.

Каждому событию e_i соответствует момент времени t_i. Предполагается, что временные метки упорядочены неубывающим образом:

$$t_1 \le t_2 \le ... \le t_I .$$

Выборка временных интервалов между соседними событиями представлена множеством Δ как

$$\Delta = \{\delta_1, \delta_2, ..., \delta_{I-1}\},$$

где $\delta_i = t_i - t_{i-1}$.

Распределение межсобытийных интервалов в журнале событий может быть неоднородным. В выборке могут присутствовать как короткие интервалы между соседними событиями в рамках одной активности, так и длительные интервалы между рабочими сессиями. Таким образом, множество временных интервалов Δ может быть представлено как объединение нескольких подмножеств, соответствующих различным типам временных интервалов. Задача исследования заключается в определении типичных временных параметров событий источника безопасности на основе анализа журнала событий.

Формально требуется по выборке межсобытийных интервалов Δ разделить интервалы между соседними событиями и интервалы между рабочими сессиями; исключить из анализа аномальные значения интервалов; определить типичный временной интервал регистрации событий и допустимые границы его изменения. Для решения поставленной задачи используются статистические характеристики распределения интервалов.

Межквартильный размах – это мера статистической дисперсии, показывающая диапазон, в котором сосредоточено некоторое количество (чаще всего 50 %) центральных значений выборки. Квартили – значения, разделяющие множество на четыре части [14]. Стандартное отклонение – мера рассеивания значений, относительно среднего, характеризующая вариативность данных.

Использование указанных характеристик позволяет выделить типичный диапазон временных интервалов между событиями и определить допустимые границы их изменения для рассматриваемого источника событий безопасности.

Математическое описание метода определения временных параметров событий безопасности на основе журнала событий. Интервалы δ_i – являются вещественными числами. Тогда из выборки Δ удаляются нулевые значения, после чего оставшиеся интервалы сортируются по возрастанию. Обозначим через *sort*(Δ) последовательность элементов множества Δ, упорядоченных по возрастанию. Тогда полученная упорядоченная выборка обозначается S:

$$S = sort\left(\{\delta_i \in \Delta | \delta_i > 0\}\right),$$

$$S = \{s_1, s_2, ..., s_m, ..., s_M\},$$

где $s_1 \le s_2 \le ... \le s_M$, $M = |S|$ – размер выборки S.

Упорядоченная выборка межсобытийных интервалов может содержать интервалы различной природы: короткие между соседними событиями и более длительные интервалы между сессиями активности. Для разделения этих типов определяется точка максимального структурного разрыва между соседними элементами выборки. Распределение интервалов выборки S можно представить функцией, показанной на рис. 1.

Поскольку выборка упорядочена по возрастанию, структурный разрыв представляет собой точку перехода к максимальным

значениям – предполагаемым интервалам между рабочими сессиями. Искомый структурный разрыв представлен точкой на рис. 1.

Для определения структурного разрыва выборки S необходимо ввести последовательность разностей между соседними элементами:

$$G = \{g_1, g_2, \ldots, g_m, \ldots, g_{M-1}\},$$

где $g_m = s_{m+1} - s_m$; $|G| = M - 1$ – мощность последовательности G.

Последовательность G можно представить функцией, изображенной на рис. 2.

Поскольку элементы выборки S – это упорядоченные межсобытийные интервалы, то в начале выборки расположены самые короткие временные переходы между событиями, в конце – самые длинные.

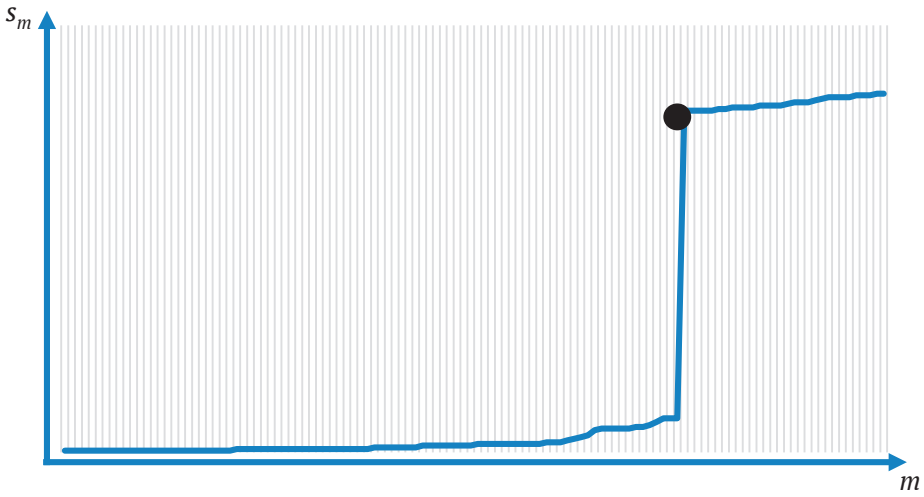

Рис. 1 | Распределение упорядоченной выборки межсобытийных интервалов времени

Fig. 1 | Distribution of an ordered sample of inter-event time intervals

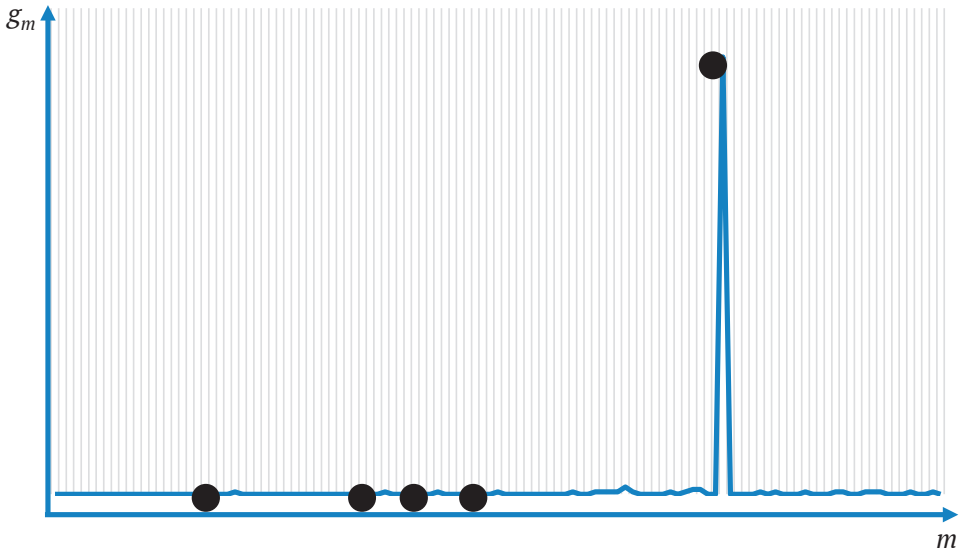

Рис. 2 | График распределения разностей элементов множества S
● – ненулевые разности

Fig. 2 | Graph of the distribution of the differences of the elements of the set S
● – nonzero differences

Тогда отмеченные на рис. 2 точки – это те точки, когда события на источнике начинают регистрироваться в логе с новым временным интервалом. Эти точки принимаем за точки структурного разрыва выборки *S*.

Тогда индекс точки максимального структурного разрыва определяет переход между короткими и длинными интервалами:

$$m^* = \arg\max_{1 \le m \le M-1} G,$$

где max*G* – поиск максимального значения последовательности *G*; arg max*G* – выбор индекса максимального элемента последовательности *G*.

Определенный индекс m^* – это точка, когда выборка *S* разделяется на интервалы между событиями и интервалы между рабочими сессиями. Формируется выборка потенциальных временных интервалов между событиями и между рабочими сессиями. Упорядоченная выборка *S* содержит интервалы двух типов: между соседними событиями и между рабочими сессиями.

Предполагается, что интервалы между событиями меньше интервалов между рабочими сессиями, что позволяет разделить выборку с использованием m^*. Тогда выборка потенциальных временных интервалов между событиями определена как S_{ev}, выборка потенциальных интервалов между сессиями – как S_s:

$$S_{ev} = \{s_1, s_2, ..., s_{m^*}\},$$

$$S_s = \{s_{m^*+1}, ..., s_M\},$$

где $s \in S$.

Таким образом, выполняется соотношение $S = S_{ev} \cup S_s$.

Если max*G* = 0, то в выборке *S* отсутствует структурный разрыв и разделение на S_{ev} и S_s не выполняется. Поскольку основная выборка *S* упорядочена по возрастанию, производные выборки S_{ev} и S_s также упорядочены по возрастанию.

После формирования S_{ev} и S_s должно выполняться следующее условие: $\min S_s > \max S_{ev}$, в противном случае разделение выборки *S* выполнено некорректно.

Для выборки потенциальных межсобытийных интервалов S_{ev} вычисляет межквартильный размах. Выборка *S* содержит временные интервалы между событиями безопасности за продолжительный период *T*. Предполагается, что за рассматриваемое время зарегистрированы как легитимные события, так и события, вызванные действиями нарушителя или сбоями в работе системы регистрации. Цель исследования – определение временных характеристик нормального поведения источника событий безопасности, поэтому нелегитимные события необходимо исключить из анализа.

Пусть упорядоченная выборка потенциальных межсобытийных интервалов имеет вид:

$$S_{ev} = \{s_1, ..., s_{m^*}\}.$$

Тогда квартиль первой четверти Q1 выборки S_{ev} соответствует значению, ниже которого находится приблизительно 25 % элементов выборки [16], и определен как:

$$Q_1 = s_{\lceil 0{,}25m^* \rceil}.$$

Квартиль третьей четверти Q3 соответствует значению, ниже которого находится приблизительно 75 % элементов выборки [16], и определен как:

$$Q_3 = s_{\lceil 0{,}75m^* \rceil}.$$

Использование границ 25 и 75 % выборки введено Джоном Тьюки как компромисс между устойчивостью и чувствительностью к выбросам. Использование этих границ позволяет выделить центральные 50 % данных, характеризующие типичное поведение выборки. Индексы квартилей округляются вверх до ближайшего целого значения.

Межквартильный размах определен как:

$$IQR = Q_3 - Q_1.$$

Межквартильный размах характеризует диапазон значений, содержащий центральную часть выборки, и используется для определения границ фильтрации аномальных интервалов [16].

Выборка S_{ev} может содержать как типичные интервалы между событиями, так

и аномальные значения. Тогда отфильтрованные промежутки времени формируют выборку S'_{ev} как:

$$S'_{ev} = \left\{ s_i \in S_{ev} \middle| \left(Q_1 - 1{,}5IQR\right) \le s_i \le \left(Q_3 + 1{,}5IQR\right) \right\},$$

где 1,5 – стандартная практика *IQR* для сохранения баланса между чувствительностью (выявлением аномалий) и сохранением данных.

На рис. 3 представлено распределение выборки S_{ev} до и после фильтрации.

Даже после фильтрации выборка интервалов между событиями содержит неоднородные данные. Необходимо определить тот интервал, который считается нормальным для рассматриваемого источника событий. Допускается, что после фильтрации в выборке преобладает искомое значение. Тогда можно предположить, что среднее значение выборки будет близко к искомому. Среднее значение выборки S'_{ev} определяется как:

$$\overline{S'_{ev}} = \frac{1}{\left|S'_{ev}\right|} \sum_{s_i \in S'_{ev}} s_i .$$

В идеальной среде интервалы между событиями источника имеют стабильное значение. Однако на практике на источник событий воздействуют внешние факторы, поэтому легитимный интервал меняется. Предлагается в качестве допустимых границ изменения искомого значения использовать стандартное отклонение от среднего значения выборки:

$$\sigma = \sqrt{\frac{1}{\left|S'_{ev}\right|} \sum_{s_i \in S'_{ev}} \left(s_i - \overline{S'_{ev}}\right)^2} .$$

Среднее значение является максимально близким к искомому значению, но не эталонным. Предполагается, что в отфильтрованной выборке значения, принадлежащие интервалу допустимого отклонения и имеющие наибольшую плотность распределения, будут являться искомыми. Тогда необходимо определить все возможные интервальные окна выборки S'_{ev}, после чего определить интервальное окно с самым большим количеством элементов. Поскольку интервалы положительные, окна определяются как:

$$K_j = \left\{ s_i \in S'_{ev} \middle| (j-1)\sigma < s_i \le j\sigma \right\},$$

где σ – стандартное отклонение S'_{ev}, если $\sigma = 0$, то все элементы равны, типичное значение интервала определяется как $\overline{S'_{ev}}$, без разбиения на окна; j – порядковый номер окна интервалов, $j \in \{1, 2, \ldots, J\}$; J – количество окон интервалов, $J = \left\lceil \frac{\max\left(S'_{ev}\right)}{\sigma} \right\rceil$, с округлением вверх до целого. Скобками «$\lceil\ \rceil$» обозначается округление до целого числа.

Индекс окна интервалов, которое можно считать типичным окном временных интервалов между событиями на источнике, определен как:

$$j^* = \arg\max_{1 \le j \le J} \left| K_j \right| .$$

Поскольку j^* – индекс интервального окна с самым большим количеством элементов, то окно интервалов перехода между событиями для источника K_{j^*}.

Таким образом, типичный временной интервал между событиями определяется границами окна K_{j^*}.

Проверка структурной значимости интервального окна. Для проверки рассмотрим исходную выборку событий $E = \{e_1, \ldots, e_I\}$, где каждому событию e_i соответствует временная метка t_i. В рамках проверки структурной значимости интервального окна дополнительно учитывается тип события. Тогда событие можно представить кортежем:

$$e_i = \left(c(e_i), t_i\right),$$

где $c(e_i)$ – тип события; t_i – временная метка события.

В основном методе анализа нулевые значения временных интервалов исключаются из дальнейшего рассмотрения, поскольку они не характеризуют временной переход между событиями. Для сохранения этой логики необходимо сформировать временной слой – события, зарегистрированные в одно время.

Пусть множество уникальных временных меток определяется как:

$$\tau = \left\{ \tau_1, \ldots, \tau_H \right\},$$

где $\tau_1 < \tau_2 \ldots < \tau_H$, а каждая τ_h является одной из временных меток исходного журнала.

Для каждой уникальной временной метки τ_h формируется временной слой событий:

$$B_h = \{e_i \in E | t_i = \tau_h\}.$$

Множество всех временных слоев обозначим как $B=\{B_1,\ldots,B_h\}$. Временной слой B_h не является новым самостоятельным событием и не заменяет события исходного журнала. Он представляет собой служебный контейнер неопределенного внутреннего порядка, содержащий все события, зарегистрированные с одной временной меткой. Неопределенность внутреннего порядка означает, что для событий внутри одного слоя отсутствует ненулевой временной интервал, поэтому на основании временных меток нельзя обоснованно утверждать, какое из этих событий произошло раньше или позже.

Пусть C_h – множество типов событий, входящих во временной слой B_h:

$$C_h = \{c(e_i) | e_i \in B_h\}.$$

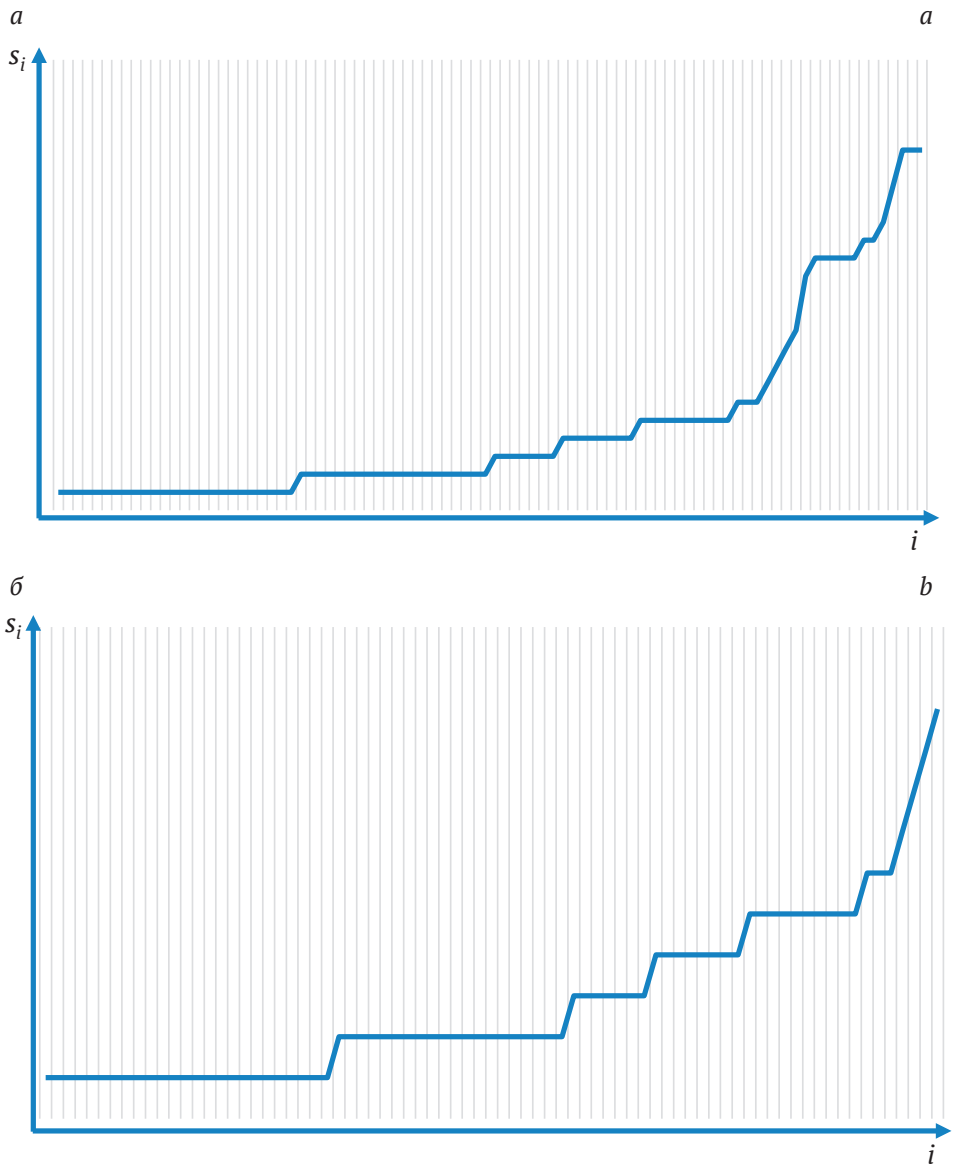

Рис. 3 | Распределение выборки S_{ev} (*а*) и отфильтрованной выборки S'_{ev} (*б*)

Fig. 3 | Distribution of S_{ev} sample (*a*) and filtered S'_{ev} sample (*b*)

Тогда для двух временных слоев B_h и B_p множество потенциальных переходов между типами событий определяется как:

$$R_h = \{(a,b) | a \in C_h, b \in C_p,$$
$$0 < \tau_p - \tau_h \le \max(S'_{ev}), p > h\}.$$

Здесь пара (a, b) означает, что событие типа a зарегистрировано в предыдущем временном слое, а событие типа b в следующем, при этом время между этими слоями не превышает максимально найденный интервал времени между событиями. Такая связь не утверждает наличие причинно-следственной зависимости между событиями, а фиксирует только потенциальный временной переход между типами событий.

Полное множество наблюдаемых переходов по журналу определяется как объединение переходов между всеми соседними временными слоями:

$$R = \bigcup_{h=1}^{H-1} R_h .$$

Для оценки устойчивости переходов каждому ребру $(a, b) \in R$ ставится в соответствие вес:

$$\omega(a,b) = \left|\{h | a \in C_h, b \in C_{h+1}, h = 1,...,H-1\}\right|.$$

Вес $\omega(a,b)$ показывает, сколько раз переход от события типа a к событию типа b наблюдается между соседними временными слоями журнала. Тогда граф переходов между временными слоями можно определить как взвешенный ориентированный граф:

$$G = (V, R, \omega),$$

где $V = \bigcup_{h=1}^{H} C_h$ – множество вершин графа, соответствующих типам событий; R – множество ориентированных ребер между типами событий, сформированных по соседним временными слоям; ω – вес ребра, определяющий частоту наблюдения соответствующего перехода.

Построенный граф отражает все потенциальные переходы между типами событий, наблюдаемые между соседними временными слоями. Однако наличие ребра в таком графе не означает, что существующий переход является устойчивым или полезным для последующего корреляционного анализа. Часть ребер может возникнуть случайно за счет высокой плотности регистрации событий, частого появления отдельных типов событий или пакетного характера логирования.

Для оценки статистической обоснованности ребра введем ожидаемую частоту перехода между типами событий. Она показывает, сколько раз переход ($a \to b$) мог бы возникнуть в рассматриваемом графе при условии независимого появления типов событий в соседних временных слоях.

Пусть $a, b \in V$ – типы событий. Вероятность появления типа события a во временном слое определяется как доля временных слоев, наблюдающих хотя бы одно событие данного типа:

$$P(a) = \frac{\left|\{h | a \in C_h, h = 1,...,H\}\right|}{H}.$$

Аналогично для типа b:

$$P(b) = \frac{\left|\{h | b \in C_h, h = 1,...,H\}\right|}{H}.$$

Суммарный вес всех ребер графа определяется как:

$$W = \sum_{(a,b) \in R} \omega(a,b).$$

Тогда математическое ожидание частоты перехода от типа событий a к типу событий b определяется как:

$$M(a, b) = WP(a)P(b).$$

Величина $M(a,b)$ показывает ожидаемое количество появлений перехода (a,b) в рассматриваемом графе при случайном независимом распределении типов событий по соседним временным слоям.

Если фактический вес ребра $\omega(a,b)$ меньше ожидаемого значения $M(a,b)$, то такой переход встречается реже, чем можно было бы ожидать при случайном сочетании типов событий. Такое ребро рассматривается как статистически слабое и исключается из дальнейшего анализа. На основе сравнения фактического ребра с ожидаемой частотой выделим множество статистически подтвержденных переходов:

$$R^* = \{(a,b) \in R \mid \omega(a,b) \ge M(a,b)\}.$$

Переходы множества R^* обладают статистическим основанием и могут рассматриваться как более устойчивые по сравнению со связями, возникшими реже ожидаемого уровня.

Для количественной оценки структуры графа введет коэффициент структурной устойчивости:

$$Q_{global} = \frac{\sum_{(a,b)\in R^*}\omega(a,b)}{\sum_{(a,b)\in R}\omega(a,b)}.$$

Значение Q_{global} показывает, какая доля наблюдаемых переходов в исходном графе приходится на статистически подтвержденные связи. Чем выше значение Q_{global}, тем большая часть переходов между временными слоями объясняется устойчивыми сочетаниями типов событий, а не случайными связями.

Для каждого найденного окна K_j формируется частный граф переходов: $G_j = (V_j, R_j, w_j)$, в котором учитываются только переходы между такими временными слоями B_h и B_p, для которых временной интервал между слоями принадлежит рассматриваемому окну:

$$R_{hj} = \left\{(a,b)\middle| a \in C_h, b \in C_p, \tau_p - \tau_h \in K_j, p > h\right\}.$$

Тогда все возможные связи между событиями в частном графе R_j определяются как:

$$R_j = \bigcup_{hj=1}^{Hj-1} R_{hj}.$$

После применения метода очистки графа от случайных связей определяется частная Q_j, отражающая какая доля переходов внутри интервального окна K_j приходится на статистически подверженные связи. Если значение Q_j превышает или не меньше значения Q_{global}, то рассматриваемое временно окно сохраняет не меньшую долю устойчивых переходов, чем исходных граф журнала:

$$Q_j \geq Q_{global}.$$

Такое окно можно считать структурно подтвержденным для задач последующего корреляционного анализа. Если анализ выявляет несколько допустимых интервальных окон, то каждое такое окно характеризует нормальный режим работы источника событий. В этом случае результатом метода является не единственное типичное значение, а множество допустимых интервальных окон, отражающих вариативность штатного функционирования источника.

Полученная математическая модель формализует процедуру определения типичных временных параметров событий безопасности по журналам событий и позволяет последовательно решить четыре взаимосвязанные задачи: отделить межсобытийные интервалы от межсессионных, исключить аномальные значения из анализа, выделить наиболее характерные интервальные окна нормального функционирования источника событий и выполнить их структурную проверку для задач последующего корреляционного анализа. В отличие от прямого усреднения исходной выборки, предложенная модель учитывает неоднородность временных распределений, наличие выбросов и вариативность реальных журналов регистрации и возможность существования нескольких нормальных режимов работы источника безопасности. Полученная модель формализует процедуру определения типичных временных параметров событий безопасности.

Методика определения типичных межсобытийных интервалов. На основе разработанной математической модели предложена методика, предназначенная для определения типичных временных интервалов между событиями и интервалов между рабочими сессиями источника безопасности. Методика позволяет разделить межсобытийные интервалы на короткие и длинные, удалить аномальные значения и определить типичные временные параметры генерации событий источника. Поскольку на реальный источник событий могут воздействовать внешние факторы, метод также позволяет определить допустимое отклонение временных интервалов. Методики реализуются в виде последовательности этапов обработки журнала событий.

Этап 1. Получение данных. Метки времени событий, зарегистрированных в лог-файлах, могут быть представлены

строкой даты и времени, только временем либо количеством миллисекунд от начала Unix эпохи [17].

Этап 2. Формирование выборки временных интервалов. Извлеченные метки времени отображают момент регистрации событий. Однако для анализа требуется определить временные интервалы между соседними событиями.

Этап 3. Упорядочивание выборки временных интервалов. Полученные промежутки между соседними событиями распределены по всей выборке случайным образом. Поскольку метод не зависит от последовательности событий в процессах, полученную выборку интервалов можно упорядочить по возрастанию.

Этап 4. Очистка от нулевых значений. Если система регистрации событий зарегистрировала несколько событий в одно и то же время, то интервал между ними будет нулевым. Такие интервалы не несут информации о временной динамике событий и исключаются из дальнейшего анализа.

Этап 5. Определение максимального структурного разрыва выборки. Сформированная выборка содержит промежутки как между событиями, так и между рабочими сессиями. Для их разделения определяется наибольшая разница между соседними интервалами.

Этап 6. Формирование выборок потенциальных интервалов между событиями и потенциальных интервалов между рабочими сессиями. Определенный ранее разрыв позволяет разделить исходную выборку на две части. Допущение метода – интервал между событиями будет меньше, чем интервал между сессиями. На основе разрыва формируются две новые выборки: в первую попадают значения, индекс которых меньше индекса разрыва – потенциальные интервалы между событиями, во вторую – оставшиеся элементы, т.е. потенциальные интервалы между сессиями. Если максимальный разрыв равен нулю, значит, все промежутки между событиями одинаковые. Тогда выборка остается целой.

Этап 7. Фильтрация данных. Среди элементов новой выборки находятся как легитимные, так и ошибочные данные. Чтобы исключить ошибочные элементы множества, необходимо воспользоваться фильтрацией на основе межквартильного размаха. Допущение метода – считается, что основную часть времени источник событий работает в штатном режиме, значит промежуток времени между событиями будет встречаться чаще других интервалов, и, исключив значения, выходящие за пределы межквартильного диапазона, можно допустить, что легитимные элементы будут преобладать в остатке.

Этап 8. Ввод допустимого отклонения отфильтрованной выборки. Несмотря на очистку выборки от ошибочных данных, выборка все еще содержит разнородные элементы, среди которых необходимо определить тот элемент, который считается типичным временем между двумя соседними событиями. Для определения типичного интервала вычисляется среднее значение отфильтрованной выборки. Если на шестом этапе не было проведено разделение выборки на две, то среднее значение является типичным промежутком между соседними событиями.

В реальных условиях интервалы между событиями могут изменяться под воздействием внешних факторов. Необходимо определить допустимое отклонение на основе среднего значения. Стандартное отклонение используется для определения ширины интервалов (окон), применяемых при группировке временных интервалов.

Этап 9. Разбиение выборки на окна. Поскольку для реального объекта типичное время перехода между событиями – это строгая оценка, необходимо определить окно интервалов. После определения стандартного отклонения выборка разбивается на интервальные окна. Каждое окно содержит значения интервалов, попадающие в соответствующий диапазон. Интервальное окно с наибольшим количеством элементов рассматривается как основной кандидат на типичное временное окно источника событий.

Этап 10. Проверка структурной значимости каждого найденного интервального окна. Для каждого найденного интервального окна проводится проверка его пригодности для последующего корреляцион-

ного анализа. Для этого строится частный граф потенциальных связей между типами событий, в который включаются только те связи, временной интервал между которыми принадлежит рассматриваемому окну. Для полученного графа вычисляется коэффициент структурной устойчивости Q_j, отражающий долю статистически подтвержденных связей. Затем значение Q_j сравнивается с базовым коэффициентом Q_{global}, рассчитанным для графа потенционых связей без ограничения конкретным интервальным окном. Если $Q_j \geq Q_{global}$, то соответствующее окно считается структурно подтвержденным. Если проверку проходят несколько окон, они рассматриваются как различные нормальные режимы работы источника событий.

Этап 11. Этапы 7–10 выполняются независимо для каждой из выборок, сформированных на шестом этапе.

В результате выполнения описанных этапов определяется интервальное окно, соответствующее типичным временным интервалам между событиями источника.

4. РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Для системы мониторинга информационной безопасности характерна обработка разнородных событий, отличающихся по частоте регистрации, структуре записи и механизмам логирования (Данилова & Абельдинов, 2024). Поэтому для апробации предложенного метода использовались журналы событий, полученные с сервера промышленной сети. Проанализированы журналы OPC-сервера, журнал безопасности Windows и журнал СУБД PostgreSQL. Предложенные источники событий информационной безопасности функционируют на действующем промышленном объекте, характеризуются различной интенсивностью регистрации событий. В табл. 1 представлены результаты сравнения.

Журнал OPC-сервера содержит 1500000 записей за час работы системы. Реализация алгоритма произведена средствами MS Excel для наглядного представления этапов обработки данных. В результате анализа установлено, что значительная часть событий имеет нулевые межсобытийные интервалы, что связано с пакетной фиксацией событий OPC-сервером. После удаления нулевых интервалов и применения фильтрации методом межквартильного размаха определен типичный интервал регистрации событий сервером. Это окно подтверждено методом проверки, однако, так как для анализа использована небольшая выборка за час работы, для достижения порога устойчивости $Q_{global} = 0{,}87$ необходимо было, чтобы максимальное число связей, полученное после фильтрации временными рамками, оказалось статистически подтвержденными. В рассматриваемой выборке только первое окно достигло 100 % сохраненных связей, остальные окна не достигли 10 %.

Журнал событий безопасности Windows содержит 29000 записей за 2 мес работы и примерно 95 % нулевых интервалов между событиями с точностью 1 с. Это связано с особенностями системы регистрации событий безопасности Windows Server. По результатам исследования выборки выявлена мультимодальность распределения, т.е. два выраженных пика: окно 1 = 48 % интервалов между событиями, окно 3 = 33 %. Проверка этих окон

Таблица 1 | Сравнение выборок для численного эксперимента

Table 1 | Comparison of samples for numerical experiment

Источник	Количество анализируемых событий	Средняя частота, соб./ч	Интенсивность регистрации событий
OPC-сервер	1500000	1,5 млн	Высокая
PostgreSQL	52000	42 тыс.	Средняя
Журнал безопасности Windows Server	29000	20	Низкая

показала, что при пороге Q_{global}=0,77 показывают примерно одинаковые показатели сохранения связей, при этом менее плотное окно сохраняет на 11 % больше связей, чем более плотное. По этим результатам можно сделать вывод, что мультимодальность является следствием двух равнозначных режимов работы.

Механизм логирования СУБД PostgreSQL записывает в файл все SQL. Каждый файл содержит не больше 10 Гб записей, после чего формируется новый файл. Так, за 80 мин зафиксировано 52500 событий, 97 % нулевых интервалов с точностью 1 с. Поскольку отфильтрованная выборка содержит одинаковые значения, то и последующая работа не требуется, стандартный интервал между событиями СУБД PostgreSQL равен 1 с. Результаты экспериментов представлены в табл. 2.

Для проведения сравнительного анализа рассчитаны значения медианы и моды по выборке межсобытийных интервалов после удаления выбросов методом межквартильного размаха. Медиана определялась как центральное значение упорядоченной выборки, а при четном количестве элементов – как среднее двух центральных значений. Мода – это значение самого частого межсобытийного интервала в очищенной выборке. Полученные значения применены в методе проверки структурной значимости. Результаты представлены в табл. 3.

Таблица 2 | Результаты численного метода

Table 2 | Results of the numerical method

Метрика	OPC-сервер	Windows Server	СУБД PostgreSQL
Нулевые значения, %	79	94,5	97
Максимальный структурный разрыв	66 мс	112184 с	1 с
Разделение межсобытийных интервалов	216458	1522	1359
Разделение межсобытийных интервалов после фильтрации	184657	1520	
Средний интервал	2,124 мс	3235 с	
Стандартное отклонение	2,253 мс	2873 с	
Сформировано окон	6	5	
Наиболее плотное окно	1	1	
Q важных окон	Окно 1: 1	Окно 1: 0.83 Окно 3: 0.94	
Плотность окна	144454 (78 %)	731 (48 %)	
Допустимый временной интервал источника	$0<\delta\leq$ 2,253 мс	$0<\delta\leq$ 2873 с	1 с

Таблица 3 | Результаты сравнения методов

Table 3 | Results of comparison of methods

Метрика	Журнал OPC	Журнал безопасности Windows Server
Допустимый временной интервал	$0<\delta\leq$ 2,253 мс	$0<\delta\leq$ 2873 с
Медиана	1 мс	30 с
Мода	1 мс	30 с
Q допустимого интервала	1	0,83
Q медианы	0,87	0,74
Q моды	0,87	0,74

По результатам сравнения, представленным в табл. 3, видно, что медиана и мода после фильтрации *IQR* дают близкие к границе Q_{global} характеристики, однако предложенный метод создает условия, при которых межсобытийная связь более устойчивая. Попадание медианного или модального значения в границы найденного интервального окна не противоречит результатам предложенного метода, напротив, оно показывает, что точечная оценка может находиться внутри области типичного поведения, однако сама по себе не позволяет определить границы этой области.

Анализ данных, представленных в табл. 2, подтверждает гипотезу о высокой доле избыточной информации в исходных журналах событий: наличие нулевых интервалов свидетельствует о специфике механизмов логирования, фиксирующих группы событий в рамках одной секунды или миллисекунды. Предложенный метод успешно нивелирует влияние этой избыточности, позволяя выделить значимые межсобытийные интервалы. В то время как классические статистические методы могли бы дать смещенную оценку из-за наличия нескольких типичных окон активности, использование группового анализа и выделение «наиболее плотного окна», а также метод подтверждения структурной значимости каждого выявленного окна, позволили корректно определить границы типичного поведения источника.

Полученные результаты демонстрируют, что фильтрация на основе межквартильного размаха в сочетании с поиском максимального структурного разрыва эффективно отделяет штатную активность от редких сессионных всплесков и случайных выбросов. Сформированные для каждого источника «типичные окна» (например, до 2,253 мс для OPC-сервера и ровно 1 с для СУБД PostgreSQL) являются готовыми параметрами для настройки поведенческих профилей. Это позволяет формализовать границы нормальности для каждого типа источника в инфраструктуре, что критически важно для минимизации ложных срабатываний при последующем корреляционном анализе в SIEM-системах.

5. ЗАКЛЮЧЕНИЕ

Описывается метод определения типичных временных параметров событий безопасности на основе анализа журналов событий. Предложенный подход позволяет по накопленным данным выявлять характерные межсобытийные интервалы, отделять их от интервалов между рабочими сессиями и определять допустимые границы изменения временных параметров источника событий.

В отличие от прямого статистического усреднения всей выборки, предложенный метод последовательно учитывает особенности реальных журналов событий: наличие нулевых интервалов, выбросов, неоднородности данных и мультимодальности распределения. Для этого используется сортировка межсобытийных интервалов, поиск максимального структурного разрыва, фильтрация методом межквартильного размаха и последующее выделение наиболее плотного интервального окна на основе стандартного отклонения, после чего все найденные окна подтверждаются или отклоняются на основе проверки структурной значимости окна.

По результатам численного эксперимента на журналах OPC-сервера, Windows Server и СУБД PostgreSQL подтверждена работоспособность метода для источников событий с высокой, средней и низкой интенсивностью регистрации. Установлено, что метод сохраняет применимость даже при значительной доле нулевых интервалов между событиями, достигающей 79–97 %, и позволяет выделять типичные временные параметры в условиях различной структуры логирования.

Для журнала OPC-сервера определено типичное окно межсобытийных интервалов $0 < \delta <= 2{,}253$ мс, содержащее 78 % элементов отфильтрованной выборки. Для журнала безопасности Windows Server метод позволил корректно выделить наиболее плотное окно $0 < \delta <= 2873$ с, в то же время определить наиболее значимое окно $5746 < \delta <= 8619$ с в условиях мультимодального распределения, где ручной выбор интервала мог привести к ошибке.

Для СУБД PostgreSQL установлено, что после фильтрации все значения интервалов совпадают, вследствие чего типичный интервал определяется однозначно – 1 с.

Практическая значимость работы заключается в том, что полученные типичные временные параметры могут быть использованы при формировании правил корреляции событий в SIEM-системах, а также при решении задач профилирования поведения источников событий и выявления отклонений от нормального режима функционирования.

Дальнейшее развитие исследования целесообразно связать с распространением метода на совокупность источников событий безопасности, автоматизацией обработки в специализированном программном модуле, а также с разработкой критериев объединения временных окон отдельных источников в рабочие сессии всей информационной системы.

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

Авторы заявляют об отсутствии конфликта интересов / The authors declare no conflict of interests.

СПИСОК ИСТОЧНИКОВ

1. **Шамсутдинова Т. М.** Цифровой след как источник больших данных (Big Data) в образовании // Открытое образование. 2024. Т. 28. № 6. С. 13–21. DOI: 10.21686/1818-4243-2024-6-13-21.
2. **Жаксыбай С. М.** Управление событиями информационной безопасности с помощью SIEM-системы // Интеллектуальные технологии в транспорте. 2023. № 1. С. 66–69.
3. **Москвичева К. С., Сай С. В.** Нормализация журналов событий с использованием регулярных выражений // Мировые исследования в области естественных и технических наук, 30 апреля 2023 г., Ставрополь. Ставрополь: ООО «Ставропольское издательство “Параграф”». С. 215–219.
4. **Коклянов А. Е.** Применение SIEM-систем в ходе проведения учений на платформе киберполигона // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2025. № 1. С. 45–51. DOI: 10.24412/2541-9269-2025-1-45-51.
5. **Листратор И. С., Милославская Н. Г., Сирбай И. С., Рейносо Б. А.** Расширенная модель зрелости SOC компании Cybereason // Безопасность информационных технологий. 2025. Т. 32. № 1. С. 68–84.
6. **Кузнецов А. В.** Организация раздельного хранения данных о событиях безопасности // Вопросы кибербезопасности. 2024. Т. 60. № 2. С. 22–28.
7. **Пахомов В. В.** Оценка эффективности центров мониторинга и реагирования на киберугрозы: ограничения временных метрик и операционные индикаторы качества // Моделирование, оптимизация и информационные технологии. 2025. Т. 13. № 4. DOI: 10.26102/2310-6018/2025.51.4.040.
8. **Долгачев М. В., Костюнин В. А.** Комплексный анализ поведения системы Windows для обнаружения киберугроз // Вопросы кибербезопасности. 2025. Т. 66. № 2. С. 71–77.
9. **Данилова О. Т., Абельдинов Р. М.** Практическое применение SIEM-модели на базе платформы Elastic Stack для мониторинга системы информационной безопасности // Динамика систем, механизмов и машин. 2024. Т. 12. № 1. С. 105–113. DOI: 10.25206/2310-9793-2024-12-1-105-113.
10. **Путято М. М., Макарян А. С., Черкасов А. Н., Кучер В. А.** Оценка функционирования SIEM-систем на основе комплекса критериев эффективности // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2024. № 1. С. 36–42. DOI: 10.53598/2410-3225-2024-1-336-36-42.

11. Gartner Magic Quadrant for Security Information and Event Management // Gartner Research. URL: https://www.gartner.com/en/documents/7040298 (дата обращения: 10.03.2026).
12. **Машкина И. В., Уразаева А. М.** Метод разработки базы знаний сценариев угроз для системы реагирования на инциденты (IRP) // Известия Южного федерального университета. Технические науки. 2024. № 5. С. 79–88.
13. **Шевцова Т. А.** Выявление аномалий в сложных данных с помощью кластеризации // Профессиональный бюллетень: Информационные технологии и безопасность. 2024. № 4. С. 39–46.
14. **Yang Chen, Yijia Ma, Wei Wu**. Rank-Based Mixture Models for Temporal Point Processes // Front. Appl. Math. Stat. 2022. Vol. 8. DOI: 10.3389/fams.2022.852314.
15. **Кечеджиев А. С., Цветкова О. Л.** Исследование обнаружения аномалий с использованием Isolation Forest в машинном обучении // Вестник Дагестанского государственного технического университета. Технические науки. 2024. Т. 51. № 1. С. 106–112. DOI: 10.21822/2073-6185-2024-51-1-106-112.
16. **Дорофеев В. С., Волосатова Т. М.** Ансамблирование методов обнаружения выбросов при подготовке обучающей выборки данных // Научный журнал Моделирование, оптимизация и информационные технологии. 2022. Т. 10. № 3. С. 1–13. DOI: 10.26102/2310-6018/2022.38.3.013.
17. Timestamp formats in logs // new relic. URL: https://docs.newrelic.com/docs/logs/ui-data/timestamp-support/ (дата обращения: 03.03.2026).

REFERENCES

1. **Shamsutdinova T. M.** Digital Footprint as a Source of Big Data in Education. *Open Education*. 2024. Vol. 28. No. 6, pp. 13–21. DOI: 10.21686/10.21686/1818-4243-2024-6-13-21. (In Russian)
2. **Zhaksybay S. M.** Information Security Event Management Using SIEM System**.** *Intellektual'nye tehnologii v transporte*. 2023. No. 1, pp. 66–69. (In Russian)
3. **Moskvicheva K. S., Say S. V.** Normalizing event logs using regular expressions. World Research in the field of natural and technical sciences, 30 April 2023, Stavropol. Stavropol: OOO "Stavropol'skoe izdatel'stvo 'Paragraf'", pp. 215–219. (In Russian)
4. **Koklyanov A. E.** Application of SIEM systems during exercises on the cyber range platform. *Matematicheskoe modelirovanie, komp'yuternyj i naturnyj ehksperiment v estestvennyh naukah*. 2025. No. 1, pp. 45–51. DOI: 10.24412/2541-9269-2025-1-45-51. (In Russian)
5. **Listratov I. S., Miloslavskaya N. G., Sirbay I. S., Reinoso B. A.** Extended Cybereason's SOC maturity model. *Bezopasnost informacionnyh tehnology*. 2025. Vol. 32. No. 1, pp. 68–84. (In Russian)
6. **Kuznetsov A. V.** The organization of separate security event data storage. *Voprosy kiberbezopasnosti*. 2024. Vol. 60. No. 2, pp. 22–28. (In Russian)
7. **Pakhomov V. V.** Evaluating the effectiveness of cyber-threat monitoring and response centers: limits of time-based metrics and operational quality indicators. *Modeling, Optimization and Information Technology*. 2025. Vol. 13. No. 4. DOI: 10.26102/2310-6018/2025.51.4.040. (In Russian)
8. **Dolgachev M. V., Kostyunin V. A.** Comprehensive analysis of windows system behavior for cyber threat detection. *Voprosy kiberbezopasnosti*. 2025. Vol. 66. No. 2, pp. 71–77. (In Russian)
9. **Danilova O. T., Abeldmov R. M.** Practical application of SIEM-model based on elastic stackplatform for monitoring information security system. *Dinamika sistem, mehanizmov i mashin*. 2024. Vol. 12. No. 1, pp. 105–113. DOI: 10.25206/2310-9793-2024-12-1-105-113. (In Russian)
10. **Putyato M. M., Makaryan A. S., Cherkasov A. N., Kucher V. A.** Estimation of siem-systems functioning on the basis of set of effectiveness criteria. *The Bulletin of the Adyghe State University. Ser.: Natural-Mathematical and Technical Sciences*. 2024. No. 1, pp. 36–42. DOI: 10.53598/2410-3225-2024-1-336-36-42. (In Russian)

11. Gartner Magic Quadrant for Security Information and Event Management. Gartner Research. URL: https://www.gartner.com/en/documents/7040298 (accessed: 10.03.2026).
12. **Mashkina I. V., Urazaeva A. M.** Method of development of threat scenarios knowledge base for incident response platform (IRP). *Izvestia SFedU. Engineering Sciences*. 2024. No. 5, pp. 79–88. (In Russian)
13. **Shevtsova T. A.** Anomaly detection in complex data using clustering. *Professional Bulletin: Information Technology and Security*. 2024. No. 4, pp. 39–46. (In Russian)
14. **Yang Chen, Yijia Ma, Wei Wu**. Rank-Based Mixture Models for Temporal Point Processes. *Front. Appl. Math. Stat*. 2022. Vol. 8. DOI: 10.3389/fams.2022.852314.
15. **Kechedzhiev A. S., Tsvetkova O. L.** Anomaly detection research using Isolation Forest in Machine Learning. *Herald of Dagestan State Technical University. Technical Sciences*. 2024. Vol. 51. No. 1, pp. 106–112. DOI: 10.21822/2073-6185-2024-51-1-106-112. (In Russian)
16. **Dorofeev V. S., Volosatova T. M.** Ensemble methods for detecting outliers in the preparation of a training data set. *Modeling, Optimization and Information Technology*. 2022. Vol. 10. No. 3, pp. 1–13. DOI: 10.26102/2310-6018/2022.38.3.013. (In Russian)
17. Timestamp formats in logs. *new relic*. URL: https://docs.newrelic.com/docs/logs/ui-data/timestamp-support/ (accessed: 03.03.2026).

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

МИХАНЬКО Антон Дмитриевич – аспирант, Уфимский университет науки и технологий, Россия, Республика Башкортостан, 450076, Уфа, ул. Заки Валиди, д. 32
E-mail: mikhanko45@gmail.com
ORCID: 0009-0007-7389-0429

MIKHANKO Anton D. – Postgraduate Student, Ufa University of Science and Technology, Russia, Republic of Bashkortostan, 450076, Ufa, Zaki Validi str., 32

МАШКИНА Ирина Владимировна – д-р техн. наук, профессор, Уфимский университет науки и технологий, Россия, Республика Башкортостан, 450076, Уфа, ул. Заки Валиди, д. 32
E-mail: profmashkina@mail.ru
ORCID: 0009-0003-2546-4354

MASHKINA Irina V. – Doctor of Engineering Sciences, Professor, Ufa University of Science and Technology, Russia, Republic of Bashkortostan, 450076, Ufa, Zaki Validi str., 32