НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2026 Том 26 № 2 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2026 Vol. 26 No 2 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

COMPUTER SCIENCE

doi: 10.17586/2226-1494-2026-26-2-287-294
УДК 004.056

Метод автоматического формирования информативного пространства для выявления событий информационной безопасности в корпоративных компьютерных сетях

Абдулхамид Яхьяевич Бучаев✉

Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
abdulhamid0055@yandex.ru✉, https://orcid.org/0009-0001-1058-9125

Аннотация

Введение. Важной частью обеспечения непрерывности функционирования сложных систем является мониторинг информационной безопасности, который является непрерывным процессом, неотделимым от контекста функционирования объекта защиты. Оперативное использование результатов мониторинга требует интерпретируемости полученных данных и представления ключевых причинно-следственных связей в формальном и доказуемом виде. Если объект защиты обладает статистической, поведенческой и процессной регулярностями, то появляется возможность формирования информативного пространства для выявления событий информационной безопасности. В работе формируются и подтверждаются гипотезы о возможности выявления событий информационной безопасности при нарушении перечисленных видов регулярности и о поиске рационального интервала формирования состояния. Научная новизна результатов определяется адаптацией формальных методов построения информативного пространства для выявления событий информационной безопасности, введением и экспериментальным подтверждением гипотез о влиянии события информационной безопасности на статистическую, поведенческую и процессную регулярности и поиске рационального интервала анализа. Предложен качественно новый метод построения информативного пространства для автоматического выявления событий информационной безопасности. Исследован процесс мониторинга состояния информационной безопасности корпоративной компьютерной сети. Рассмотрены эвристические методы формирования информативного пространства для выявления событий информационной безопасности на основе статистического анализа ретроспективных данных в реальном масштабе времени. **Метод.** Представлен метод автоматического формирования информативного пространства для выявления событий информационной безопасности в корпоративных компьютерных сетях, основанный на динамике двух соседних состояний конечных устройств, определенных за дискретные промежутки времени. Множество таких переходов состояний по всем устройствам формирует матрицу состояния исследуемой компьютерной сети. **Основные результаты.** Определено информативное пространство для вычисления динамики полученных векторов состояний и найден рациональный интервал формирования состояния устройства при исследовании зависимости разницы векторов двух соседних состояний от интервала анализа в различных информативных пространствах. Выполнен анализ набора сетевых данных в формате PCAP (Packet CAPture), включающий в себя легитимную и ботнет активности устройств интернета вещей. Графическая интерпретация полученного результата позволяет определить время подготовки и начала атаки, что существенно упрощает задачу мониторинга информационной безопасности на этапе анализа входных данных и сокращает количество данных, анализируемых аналитиком информационной безопасности. **Обсуждение.** Отличительными особенностями предложенного метода является работа в режиме реального времени, отсутствие этапа предобработки входных данных и интерпретируемость выявленных событий информационной безопасности. Явно выделяющиеся тенденции динамики состояния устройств позволяют сократить объем анализируемой информации и обратить внимание на нарушения регулярностей, характеризующие возможные события информационной безопасности. Область применения метода включает в себя задачи мониторинга событий и выявление инцидентов информационной безопасности, а также обнаружение вторжений в корпоративных компьютерных сетях.

Ключевые слова

кибербезопасность, события информационной безопасности, вектор признаков, статистическая устойчивость, сетевой трафик, мониторинг информационной безопасности, статистическое управление процессами

Ссылка для цитирования: Бучаев А.Я. Метод автоматического формирования информативного пространства для выявления событий информационной безопасности в корпоративных компьютерных сетях // Научно-технический вестник информационных технологий, механики и оптики. 2026. Т. 26, № 2. С. 287–294. doi: 10.17586/2226-1494-2026-26-2-287-294

Method of automatic generation of the informative space for identifying information security events in corporate computer networks

Abdulhamid Y. Buchaev✉

ITMO University, Saint Petersburg, 197101, Russian Federation

abdulhamid0055@yandex.ru✉, https://orcid.org/0009-0001-1058-9125

Abstract

An important part of ensuring the continuity of operation of complex systems is information security monitoring which is a continuous process inseparable from the context of the functioning of the protected object. The operational use of monitoring results requires the interpretability of the obtained data and the presentation of key cause-and-effect relationships in a formal and provable form. If the protected object exhibits statistical, behavioral, and process regularities, it becomes possible to form an informative space for identifying information security events. This paper formulates and validates hypotheses regarding the possibility of identifying information security events when the above-mentioned types of regularity are violated as well as the search for a rational interval for the formation of a state. The scientific novelty of the results is determined by the adaptation of formal methods for constructing an informative space for identifying information security events, the introduction and experimental confirmation of hypotheses regarding the impact of an information security event on statistical, behavioral, and process regularities, and the search for a rational analysis interval. The goal of this paper is to provide a qualitatively new method for constructing an informative space for the automatic detection of information security events. The object of the study is the process of monitoring the information security status of a corporate computer network. The subject of this study is heuristic methods for forming an informative space for identifying information security events based on the statistical analysis of retrospective data in real time. This paper proposes a method for automatically forming an informative space for identifying information security events in corporate computer networks. This method is based on the dynamics of two adjacent states of end devices determined over discrete time intervals. The set of such state transitions across all devices forms the state matrix of the computer network under study. This study defined an informative space for calculating the dynamics of the obtained state vectors and found a rational interval for forming the device state when studying the dependence of the difference in the vectors of two adjacent states on the analysis interval in various informative spaces. To experimentally confirm the operability of the proposed solution, a set of network data in the PCAP (Packet CAPture) format was analyzed, including legitimate and botnet activity of Internet of Things devices. Graphical interpretation of the obtained result allows one to determine the attack preparation and attack start times, which significantly simplifies the task of information security monitoring at the input data analysis stage and reduces the amount of data analyzed by the information security analyst. Distinguishing features of the proposed method include real-time operation, the absence of a preprocessing stage for input data, and the interpretability of detected information security events. Clearly discernible trends in device status dynamics allow for a reduction in the volume of analyzed information and the focus on irregularities that characterize potential information security events. The scope of application of the proposed method includes monitoring information security events, identifying information security incidents, and detecting intrusions in corporate computer networks.

Keywords

cybersecurity, information security events, feature vector, statistical stability, network traffic, information security monitoring, statistical process control

For citation: Buchaev A.Y. Method of automatic generation of the informative space for identifying information security events in corporate computer networks. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2026, vol. 26, no. 2, pp. 287–294 (in Russian). doi: 10.17586/2226-1494-2026-26-2-287-294

Введение

Согласно статистике, за 2023 и 2024 года в Российской Федерации увеличилось количество инцидентов информационной безопасности (ИБ), а наиболее актуальными точками деструктивного воздействия являются конечные устройства (например, персональные компьютеры) и сетевое оборудование[1]. Наиболее уязвимыми оказались государственные учреждения и объекты критической информационной инфраструктуры.

Рынок программно-аппаратных решений в области аналитики ИБ растет[2], однако классические подходы сигнатурного и эвристического анализов не подходят для выявления zero-day и zero-click угроз, порождаемых, например, шпионским программным обеспече-

[1] Positive Technologies. Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (дата обращения: 05.06.2025).

[2] Б1. Информационная безопасность — один из ключевых драйверов роста российского ИТ-рынка и может достичь порядка 681 млрд руб. или 14 % от общего объема ИТ-рынка к 2030 году [Электронный ресурс]. Режим доступа: https://b1.ru/insights/news/media-center/b1-russian-information-security-market-survey-press-release-19-march-2025/ (дата обращения: 21.06.2025).

нием Pegasus (NSO Group, Израиль) [1, 2]. Актуальные программные средства[1] при анализе сетевого трафика в задачах выявления инцидентов ИБ в компьютерных сетях используют специализированные шаблоны, основанные на метаданных уже известных и прошедших атак. Такой подход ограничивает набор обнаруживаемых воздействий, а также требует периодичной актуализации используемой базы знаний.

В работе [3] определена таксономия техник анализа ИБ организаций, которая разделена на две группы: кибербезопасность и надежность (safety). В свою очередь, техники анализа кибербезопасности, как части ИБ, имеют четыре подхода: агрегирование табличных данных и вычисление ключевых метрик качества [4]; построение деревьев событий, приводящих к реализации угроз [5]; построение моделей для оценки рисков кибербезопасности [6, 7] и моделирование сценариев, описывающих риски кибербезопасности [8].

Работы [4–8] объединяет анализ ретроспективы прошедших атак, например, статистических данных при использовании методов Монте-Карло, построении деревьев событий, а также необходимость характеризовать защищаемую систему в ручном режиме. Они задают вектор исследования эвристических методов выявления событий ИБ, который ограничен своей применимостью, так как требует априорного описания сценариев и постоянного сопровождения и актуализации. Таким образом, результат мониторинга ИБ опирается на интегральную ретроспективную оценку рисков, которая напрямую зависит от репрезентативности используемых в ретроспективе данных.

В настоящей работе предлагается метод автоматического формирования информативного пространства для выявления событий ИБ в корпоративной компьютерной сети (ККС) на основе статистического анализа информационного обмена конечных устройств без использования сигнатурных шаблонов или процесса обучения.

Представляется качественно новый метод построения информативного пространства для автоматического выявления событий ИБ. Исследуется процесс мониторинга состояния ИБ ККС. Рассмотрены эвристические методы формирования информативного пространства для выявления событий ИБ на основе статистического анализа ретроспективных данных в реальном масштабе времени.

Предложенный метод

Гипотеза и основание исследования. В контексте управляемого процесса [9] мониторинг ИБ предоставляет возможность использования нескольких видов регулярности: статистическая (описывает статистическую стабильность динамики векторов состояния [10]); поведенческая (предсказуемость поведения и изменения сетевого трафика во время штатного функционирования компьютерной сети [11]); процессная (описывает соответствие наблюдаемых векторов состояния и их изменения согласно ожидаемым шаблонам).

При анализе перечисленных видов регулярности процесс мониторинга ИБ соответствует главным идеям статистического управления процессами, где отклонение от регулярного поведения сигнализирует о проблемах в процессе [12]. В результате была сформулирована следующая гипотеза.

Гипотеза А. Нарушение статистической, поведенческой или процессной регулярностей при изменении вектора состояния устройства, сформированного путем анализа информационного обмена в течение фиксированного интервала времени с другими устройствами, свидетельствует о наличии события ИБ.

Модель состояния ККС. Предположим, что модель ККС представлена набором образов конечных устройств $D = \{d_1, d_2, \ldots, d_n\}$, время работы ККС описывается дискретными величинами $T = \{t_1, t_2, \ldots, t_m\}$. В результате статистического анализа формируются компоненты вектора, описывающего текущее состояние устройства за определенный промежуток времени. Таким образом, за какой-либо дискретный промежуток времени $\Delta t_j = t_j - t_{j-1}$ каждое устройство, производящее информационный обмен с другими устройствами в сети, имеет вектор состояния $\mathbf{d}_i(\Delta t_j) = \langle c_1, c_2, \ldots c_k \rangle$, где $i = \overline{1, n}$; $j = \overline{1, m}$; k — количество компонентов вектора состояния; c_k — компонент вектора состояния устройства. Стоит отметить, что в настоящей работе используются непосредственно наблюдаемые показатели и сформированные на их основе авторские синтетические показатели информационного обмена устройств в сетевой инфраструктуре, которые являются компонентами вектора состояния устройства.

Под динамикой состояния устройства понимается разница между векторами состояний в промежутки Δt_j и Δt_{j-1}. Для определения динамики состояния каждого устройства необходимо ввести информативное пространство. Под множеством элементов информативного пространства понимается пространство векторов состояний, а в качестве функций отличия рассматриваются:

— косинусное расстояние (cosine distance), которое позволяет провести оценку направления двух векторов. При этом «0» означает полное сходство, «0,5» — ортогональность и «1» — полную противоположность:

$$cosine\ distance = 1 - \frac{1 + \cos(\mathbf{A}, \mathbf{B})}{2}, \qquad (1)$$

где $\cos(\mathbf{A}, \mathbf{B})$ — косинус угла между векторами **A** и **B**;

— энтропия абсолютной разности двух векторов состояний (H) оценивает неопределенность распределения компонентов разницы двух векторов состояния в соседние промежутки времени:

$$H(\mathbf{S}) = -\sum_{i=1}^{k} p(s_i)\log_2 p(s_i), \qquad (2)$$

где $H(\mathbf{S})$ — энтропия Шеннона вектора **S**, $\mathbf{S} = |\mathbf{A} - \mathbf{B}|$; k — длина векторов **A** и **B**; $p(s_i)$ — эмпирическая вероятность (частота) компонента вектора **S**;

[1] Positive Technologies. Network Attack Discovery [Электронный ресурс]. Режим доступа: https://ptsecurity.com/ruru/products/networkattackdiscovery/ (дата обращения: 20.05.2025).

— квадратный корень из дивергенции Йенсена–Шеннона:

$$JSD(\mathbf{A}, \mathbf{B}) = \sqrt{\frac{1}{2}((\mathbf{A}, \mathbf{M}) + D_{KL}(\mathbf{B}, \mathbf{M}))}, \quad (3)$$

где D_{KL} — дивергенция Кульбака–Лейблера; $\mathbf{M} = \frac{1}{2}(\mathbf{A} + \mathbf{B})$;

— расстояние Хеллингера:

$$Hellinger\ (\mathbf{A}, \mathbf{B}) = \sqrt{1 - \sum_{i=1}^{k} \sqrt{a_i b_i}}. \quad (4)$$

Выбор функций (1)–(4) обоснован необходимостью качественной и количественной оценок разницы соседних состояний. При использовании функций (1) и (2) теоретически могут возникнуть случаи неразличимости состояний устройств: для выражения (1) — коллинеарность векторов; для (2) — нулевой вектор с одним единичным элементом.

Однако с точки зрения характеристик ККС такие случаи не могут являться признаком события ИБ, что снимает ограничения на их применимость для данной предметной области.

В ходе исследования из известных расстояний также рассматривались евклидово расстояние, прямоугольная метрика, расстояние Чебышева и расстояние Хэмминга, однако они показывают абсолютную разницу между векторами, не учитывая, например, распределение компонентов разницы векторов [13].

За каждый промежуток времени Δt_j при $j = \overline{2, m}$ определяется состояние объекта d_i при $i = 1, n$ следующим образом:

$$s_{ij} = M(\mathbf{d}_i(\Delta t_{j-1}), \mathbf{d}_i(\Delta t_j)), \quad (5)$$

где M — функция отличия.

Таким образом, последовательность наблюдаемых показателей функционирования ККС (D) во временной области (T) преобразуется в представление в информативном пространстве признаков (5), а множество таких представлений образует модель состояния ККС в виде матрицы размером $(n, m - 1)$:

$$\mathbf{S}(D, T) = \begin{pmatrix} s_{11} & \cdots & s_{1m-1} \\ \vdots & \ddots & \vdots \\ s_{n1} & \cdots & s_{nm-1} \end{pmatrix}.$$

Метод автоматического формирования информативного пространства состояний ККС для выявления событий ИБ. Пусть исходными параметрами являются $\theta = \{\Delta t, M\}$, выбор которых определятся спецификой конкретной компьютерной сети. Выбор параметров также влияет на дисперсию и смещение при выявлении событий ИБ, поэтому необходимо найти такой интервал анализа, при котором достигается малая дисперсия и малое смещение, т. е. найти компромисс между дисперсией и смещением [14, 15]. Экспериментально подтверждается, что слишком малый промежуток Δt не накапливает достаточный объем наблюдений, обеспечивающий достоверную характеристику состояния устройства, и ведет к высокой дисперсии, а слишком большой временной промежуток приводит к чрезмерному усреднению, что негативно влияет на выявление инцидентов ИБ, так как появляется систематическое смещение.

На основании этого формулируется гипотеза о выборе рационального интервала анализа.

Гипотеза Б. Для каждой конкретной сети, способа формирования вектора состояния ее объектов и выбранной функции отличия существует рациональный интервал анализа (Δt), при котором качество обнаружения событий ИБ максимизируется при фиксированных эксплуатационных ограничениях.

Ранее выбранные функции отличия (1)–(4) характеризуют разницу между двумя векторами специфически. В настоящей работе рассматривается работа ботнета, а именно проведение атаки Distributed Denial of Service (DDoS) распределенного и централизованного типов, поэтому ключевыми функциями отличия были выбраны энтропия абсолютной разности (2) и косинусное расстояние (1). Эти метрики оценивают разницу распределения компонентов вектора состояния, т. е. направление вектора и количественную разницу в случае коллинеарных векторов.

Предлагается метод автоматического формирования информативного пространства состояний для выявления событий ИБ в ККС, учитывающий: рациональный интервал анализа состояний устройств; функцию отличия для вычисления динамики состояний, зависящую от контекста анализируемой системы; ретроспективу информационного обмена между устройствами и предоставляющий исходные данные для проведения мониторинга ИБ компьютерной сети.

Данный метод позволяет в автоматическом режиме строить информативное пространство для выявлений событий ИБ ККС на основе статистического анализа информационного обмена конечных устройств и включает в себя несколько шагов.

Шаг 1. Извлечение непосредственно наблюдаемых сетевых данных:

— программное зеркалирование трафика (например, Switched Port Analyzer);

— аппаратное зеркалирование трафика (например, Network TAP);

— снятие сетевых пакетов с помощью специализированных приложений (Wireshark[1], Tcpdump[2] и т. п.).

Шаг 2. Выделение и преобразование наблюдаемых и синтезированных компонентов в векторы состояния устройств d_i (например, [12]).

Шаг 3. Определение рационального интервала анализа Δt.

Шаг 4. Выбор функции M (1)–(4).

Шаг 5. Формирование вектора состояния устройства за промежуток Δt_j.

Шаг 6. Сравнение с вектором состояния за промежуток Δt_{j-1}.

[1] [Электронный ресурс]. Режим доступа: https://www.wireshark.org/ (дата обращения: 20.05.2025).

[2] [Электронный ресурс]. Режим доступа: https://www.tcpdump.org/ (дата обращения: 20.05.2025).

Шаг 7. Формирование последовательности изменений состояний устройства и вывод данных для дальнейшей обработки в ручном или автоматизированном режиме.

Наибольший интерес вызывают шаги 3 и 4, так как зависят от конкретной системы.

Особенности ботнет активности подразумевают изменения в поведении устройства во время информационного обмена внутри компьютерной сети, именно поэтому важно оценивать распределение компонентов вектора состояния, т. е. направление этого вектора, при вычислении динамики состояния. Это соответствует анализу процессной регулярности, описывающей ожидаемые шаблоны состояния и ожидаемые изменения состояний в компьютерной сети.

Описание эксперимента

Рассмотрим подробнее шаг 3 предлагаемого метода.

Для проверки продуктивности метода формирования и использования информативного пространства выполнен компьютерный эксперимент по выявлению событий ИБ в ККС.

Используемый набор данных. В рамках проведения экспериментов был выбран набор сетевых данных в формате Packet CAPture (PCAP) [16], который не подвергался предобработке и изменениям. Он содержит сетевые пакеты, описывающие информационный обмен устройств интернета вещей и нескольких серверов. Работа компьютерной сети протоколировалась почти сутки, сетевой трафик включает в себя легитимную работу используемых устройств до и после проведения атаки, а также этап активности ботнета и проведение DDoS-атаки.

В табл. 1 приведена краткая характеристика вредоносной части используемого набора данных, логически разделенная по разновидностям и режимам работы ботнета.

В наборе присутствует несколько типов устройств интернета вещей, для снижения объема вычислений отобраны 8 адресов, соответствующих включенным в набор устройствам.

Каждое устройство во время легитимной работы взаимодействовало с сервером по адресу «192.168.10.100», во время работы ботнета и проведения DDoS-атаки устройства атаковали сервер по адресу «192.168.10.60». Средняя длительность атаки составляла 59 мин.

Определение рационального интервала анализа. Величина рационального интервала анализа зависит от статистической и поведенческой регулярности конкретной компьютерной сети, поэтому важно предварительно проанализировать ее работу. Требуется найти такой интервал анализа, при котором вектор состояния до атаки будет максимально отличаться от вектора состояния после начала атаки. Таким образом, в работе измеряется информативность, полученная от конкретного интервала анализа в конкретном пространстве.

Для проверки гипотезы исследования проведено 360 экспериментов, усредненные результаты которых представлены на рис. 1.

Каждый эксперимент проводился на новом интервале анализа Δt с увеличением интервала анализа каждой итерации на 1 мин. Другими словами, последний эксперимент содержит сравнение вектора состояния за 6 ч (360 мин), включая время легитимной работы до начала атаки, и вектора состояния за 6 ч после начала атаки, включая саму атаку и легитимную работу после нее.

На рис. 1 видно, что статистические характеристики усредняются, признаки наличия атаки «размываются», при использовании интервалов анализа с 60 до 120 мин, затем статистическая характеристика компонентов векторов состояния до и после начала атаки почти не отличается.

Красной линией по дополнительной (правой) оси обозначено среднее время сбора, обработки и преобразования непосредственно наблюдаемых значений сетевых пакетов, т. е. полное время формирования вектора состояния. С увеличением интервала анализа растет и количество непосредственно наблюдаемых значений, так как активность устройства продолжается.

Полученные результаты. Автоматическая реализация предложенного метода обеспечила возможность решения задачи выявления событий ИБ в ККС с использованием достоверного набора данных.

При проведении экспериментов использовалось произведение двух функций отличия — косинусного расстояния (1) и энтропии разности (2), а интервал анализа Δt принимал значения от 2 до 5 мин. Рациональным интервалом анализа является промежуток 3 мин, позволяющий накопить достаточно данных для выявления событий ИБ (рис. 2).

Таблица 1. Характеристика вредоносной части используемого набора данных

Table 1. Characteristics of the malicious part of the used dataset

Файл сетевого дампа	Размер, КБ	Количество пакетов, шт.	Описание
bashlite_mal_CC_all.pcap	235 962	627 498	Трафик, порождаемый ботнетом bashlite типа C&C
bashlite_mal_spread_all.pcap	295 234	3 284 392	Трафик, порождаемый ботнетом bashlite распределенного типа
mirai_mal_CC_all.pcap	665 596	842 673	Трафик, порождаемый ботнетом mirai типа C&C
mirai_mal_spread_all.pcap	148 395	401 129	Трафик, порождаемый ботнетом mirai распределенного типа
torii_mal_all.pcap	24 800	321 776	Трафик, порождаемый ботнетом torii распределенного типа и C&C

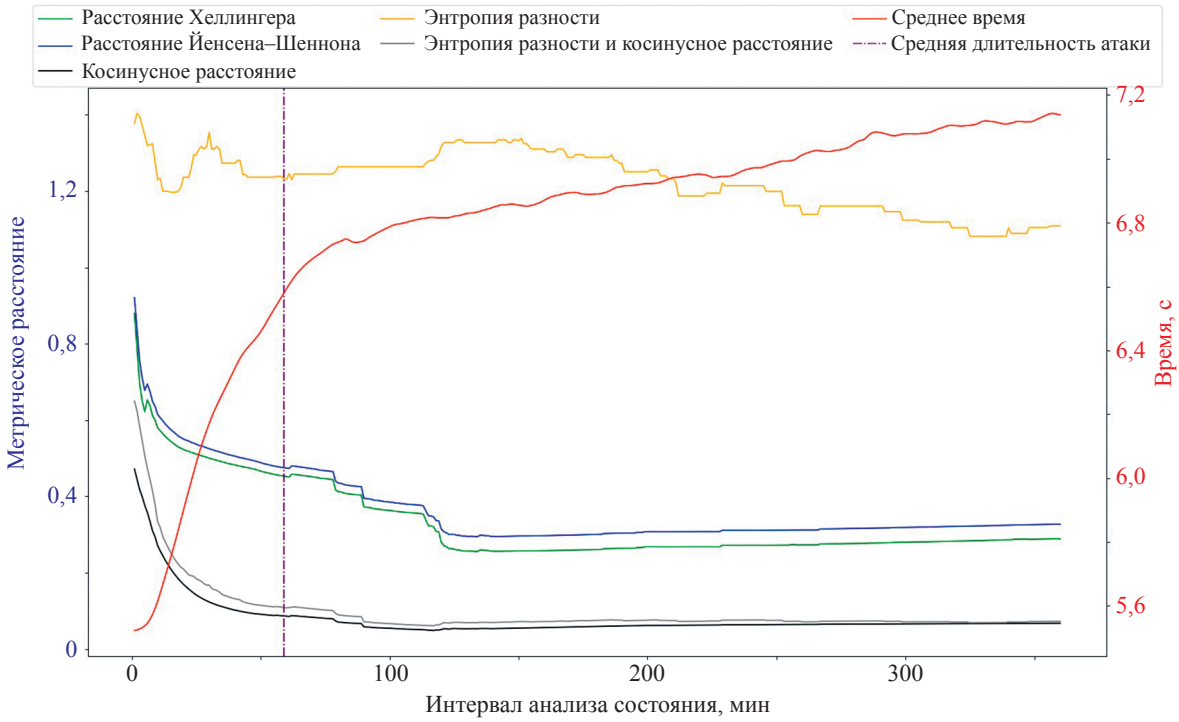

Рис. 1. Зависимость разницы между двумя соседними состояниями от интервала анализа в различных пространствах. Среднее время атаки (пунктирная фиолетовая линия)

Fig. 1. Dependence of the difference between two adjacent states on the analysis interval in different metric spaces

Предлагаемый метод создает условия для полностью автоматического решения задачи выявления событий ИБ в ККС. Однако, в зависимости от специфики объекта защиты, может потребоваться автоматизированный анализ результатов выполнения шага 3 (определение рационального интервала анализа Δt) (рис. 1).

Результаты эксперимента свидетельствуют об отсутствии опровержения гипотез А и Б, дополнительная проверка которых может быть реализована в процессе применения предлагаемых решений к другим классам систем.

Обсуждение

Практическая значимость результатов заключается в снижении количества данных, обрабатываемых аналитиком в процессе анализа ИБ ККС. А возможность в автоматическом режиме анализировать динамику взаимодействия устройств ККС и выявлять события ИБ закладывает возможности для проактивной защиты систем.

Графическая интерпретация экспериментального подтверждения выдвинутых гипотез позволяет определить момент начала атаки и момент запуска ботнета (рис. 2, «Подготовка к атаке»).

Формализованное представление динамики взаимодействия элементов ККС обеспечивает, в том числе, автоматическое обнаружение событий ИБ (рис. 2, «Проведение атаки»).

Предложенное решение отличается отсутствием шага предобработки данных и работой в режиме реального времени, что достигается потоковой обработкой входящих сетевых пакетов и формированием скользящего окна размером в одно состояние для вычисления

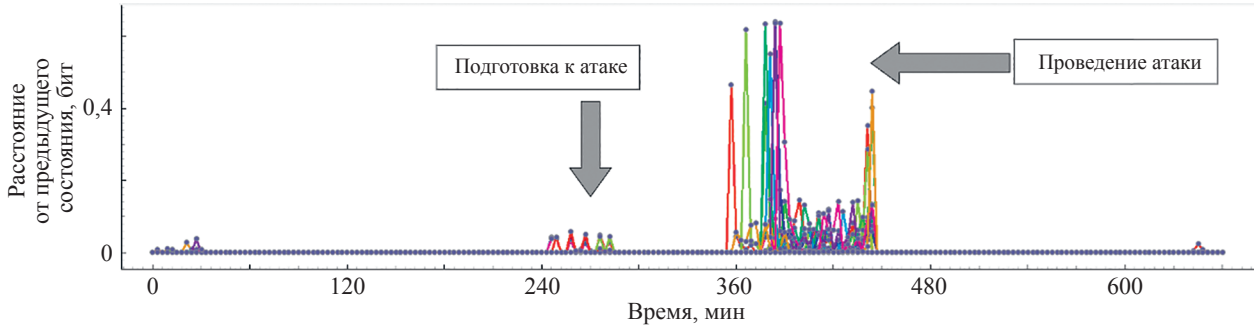

Рис. 2. Визуализация результатов выявления событий информационной безопасности в компьютерной сети

Fig. 2. Visualization of the results of identifying information security events in a computer network

динамики. Вычислительная сложность решения составляет $O(n)$, где n — длина обрабатываемой последовательности.

Заключение

Представлен метод автоматического формирования информативного пространства для выявления событий информационной безопасности в корпоративных компьютерных сетях. Сформулированы и экспериментально подтверждены гипотезы на примере необработанного набора сетевых данных в формате PCAP (Packet CAPture), что демонстрирует практическую применимость решения.

В основе предложенного метода лежат апробированные и математически доказуемые зависимости, обеспечивающие интерпретируемость результатов. Низкая вычислительная сложность $O(n)$ обусловлена потоковой обработкой сетевых пакетов, которая обеспечивает работу метода в режиме реального времени.

Применение разработанного метода автоматического формирования информативного пространства для выявления событий информационной безопасности не ограничивается компьютерной сетью, так как возможна реализация для других объектов защиты и признаковых пространствах иной размерности, что подтверждается ранее выполненными исследованиями по выявлению аномальных фрагментов изображений.

Полученные результаты могут быть использованы на последующих этапах обработки событий информационной безопасности, в том числе для решения задач автоматического обнаружения и реагирования на инциденты информационной безопасности.

Литература

1. Rudie J.D., Katz Z., Kuhbander S., Bhunia S. Technical analysis of the NSO Group's Pegasus Spyware // Proc. of the International Conference on Computational Science and Computational Intelligence (CSCI). 2021. P. 747–752. https://doi.org/10.1109/csci54926.2021.00188
2. Chourasiya S., Samanta G., Sardar D.K., Sharma P., Kumar C.N.S.V. Pegasus Spyware: a vulnerable behaviour-based attack system // Proc. of the 2nd International Conference on Edge Computing and Applications (ICECAA). 2023. P. 287–292. https://doi.org/10.1109/icecaa58104.2023.10212163
3. Babeshko I., Giandomenico F.D. Safety and cybersecurity assessment techniques for critical industries: a mapping study // IEEE Access. 2023. V. 11. P. 83781–83793. https://doi.org/10.1109/access.2023.3297446
4. Abakumov A., Kharchenko V. Combining IMECA analysis and penetration testing to assess the cybersecurity of industrial robotic systems // Proc. of the 12th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2022. P. 1–7. https://doi.org/10.1109/dessert58054.2022.10018823
5. Tân S.-G., Liu I.-H., Li J.-S. Threat analysis of cyber security exercise for reservoir testbed based on attack tree // Proc. of the 10th International Symposium on Computing and Networking Workshops (CANDARW). 2022. P. 375–379. https://doi.org/10.1109/candarw57323.2022.00023
6. Guo H., Ding L., Xu W. Cybersecurity risk assessment of industrial control systems based on order-α divergence measures under an interval-valued intuitionistic fuzzy environment // IEEE Access. 2022. V. 10. P. 43751–43765. https://doi.org/10.1109/access.2022.3169133
7. Boudermine A., Khatoun R., Choyer J.-H. Attack graph-based solution for vulnerabilities impact assessment in dynamic environment // Proc. of the 5th Conference on Cloud and Internet of Things (CIoT). 2022. P. 24–31. https://doi.org/10.1109/ciot53061.2022.9766588
8. Wang W., Cammi A., Maio F.D., Lorenzi S., Zio E. A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants // Reliability Engineering and System Safety. 2018. V. 175. P. 24–37. https://doi.org/10.1016/j.ress.2018.03.005
9. Уилер Д., Чамберс Д. Статистическое управление процессами. Оптимизация бизнеса с использованием контрольных карт Шухарта. М.: Альпина Паблишер, 2016. 410 с.
10. Kotenko I., Saenko I., Bortniker P. Detecting attacks against industrial Internet of things by integrating wavelet and statistical analysis // Proc. of the International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). 2025. P. 896–901. https://doi.org/10.1109/icieam65163.2025.11028572
11. Yu J., Guo J., Globa L., Li S., Zhang M., Li X., Liu J. Construction of a social security monitoring and early warning platform driven by big data // Proc. of the IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference

References

1. Rudie J.D., Katz Z., Kuhbander S., Bhunia S. Technical analysis of the NSO Group's Pegasus Spyware. *Proc. of the International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021, pp. 747–752. https://doi.org/10.1109/csci54926.2021.00188
2. Chourasiya S., Samanta G., Sardar D.K., Sharma P., Kumar C.N.S.V. Pegasus Spyware: a vulnerable behaviour-based attack system. *Proc. of the 2nd International Conference on Edge Computing and Applications (ICECAA)*, 2023, pp. 287–292. https://doi.org/10.1109/icecaa58104.2023.10212163
3. Babeshko I., Giandomenico F.D. Safety and cybersecurity assessment techniques for critical industries: a mapping study. *IEEE Access*, 2023, vol. 11, pp. 83781–83793. https://doi.org/10.1109/access.2023.3297446
4. Abakumov A., Kharchenko V. Combining IMECA analysis and penetration testing to assess the cybersecurity of industrial robotic systems. *Proc. of the 12th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2022, pp. 1–7. https://doi.org/10.1109/dessert58054.2022.10018823
5. Tân S.-G., Liu I.-H., Li J.-S. Threat analysis of cyber security exercise for reservoir testbed based on attack tree. *Proc. of the 10th International Symposium on Computing and Networking Workshops (CANDARW)*, 2022, pp. 375–379. https://doi.org/10.1109/candarw57323.2022.00023
6. Guo H., Ding L., Xu W. Cybersecurity risk assessment of industrial control systems based on order-α divergence measures under an interval-valued intuitionistic fuzzy environment. *IEEE Access*, 2022, vol. 10, pp. 43751–43765. https://doi.org/10.1109/access.2022.3169133
7. Boudermine A., Khatoun R., Choyer J.-H. Attack graph-based solution for vulnerabilities impact assessment in dynamic environment. *Proc. of the 5th Conference on Cloud and Internet of Things (CIoT)*, 2022, pp. 24–31. https://doi.org/10.1109/ciot53061.2022.9766588
8. Wang W., Cammi A., Maio F.D., Lorenzi S., Zio E. A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants. *Reliability Engineering and System Safety*, 2018, vol. 175, pp. 24–37. https://doi.org/10.1016/j.ress.2018.03.005
9. Wheeler D.J., Chambers D.S. *Understanding Statistical Process Control*. SPC Press, 2010, 406 p.
10. Kotenko I., Saenko I., Bortniker P. Detecting attacks against industrial Internet of things by integrating wavelet and statistical analysis. *Proc. of the International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, 2025, pp. 896–901. https://doi.org/10.1109/icieam65163.2025.11028572
11. Yu J., Guo J., Globa L., Li S., Zhang M., Li X., Liu J. Construction of a social security monitoring and early warning platform driven by big data. *Proc. of the IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference*

(IMCEC). 2021. P. 370–373. https://doi.org/10.1109/imcec51613.2021.9482215
12. Бучаев А.Я., Бегаев А.Н., Комаров И.И. Метод автоматического обнаружения аномалий в пространстве событий информационной безопасности // Промышленные АСУ и контроллеры. 2024. № 2. С. 31–41. https://doi.org/10.25791/asu.2.2024.1488
13. Senevirathna T., Siniarski B., Liyanage M., Wang S. Deceiving post-hoc explainable AI (XAI) methods in network intrusion detection // Proc. of the IEEE 21st Consumer Communications & Networking Conference (CCNC). 2024. P. 107–112. https://doi.org/10.1109/ccnc51664.2024.10454633
14. Barr J.R., Abu-Khzam F.N., Shaw P. Feature selection via independent domination // Proc. of the 5th International Conference on Transdisciplinary AI (TransAI). 2023. P. 197–200. https://doi.org/10.1109/transai60598.2023.00048
15. Scampicchio E. Arcari E., Zeilinger M.N. Error analysis of regularized trigonometric linear regression with unbounded sampling: a statistical learning viewpoint // IEEE Control Systems Letters. 2023. V. 7. P. 3066–3071. https://doi.org/10.1109/lcsys.2023.3291690
16. Guerra-Manzanares A., Medina-Galindo J., Bahsi H., Nõmm S. MedBIoT: Generation of an IoT botnet dataset in a medium-sized IoT network // Proc. of the 6th International Conference on Information Systems Security and Privacy. 2020. V. 1. P. 207–218. https://doi.org/10.5220/0009187802070218

(IMCEC), 2021, pp. 370–373. https://doi.org/10.1109/imcec51613.2021.9482215
12. Buchaev A.Ya., Begaev A.N., Komaro I.I. Method for automatic detection of anomalies in the information security event space. *Industrial Automatic Control Systems and Controllers*, 2024, no. 2, pp. 31–41. (in Russian). https://doi.org/10.25791/asu.2.2024.1488
13. Senevirathna T., Siniarski B., Liyanage M., Wang S. Deceiving post-hoc explainable AI (XAI) methods in network intrusion detection. *Proc. of the IEEE 21st Consumer Communications & Networking Conference (CCNC)*, 2024, pp. 107–112. https://doi.org/10.1109/ccnc51664.2024.10454633
14. Barr J.R., Abu-Khzam F.N., Shaw P. Feature selection via independent domination. *Proc. of the 5th International Conference on Transdisciplinary AI (TransAI)*, 2023, pp. 197–200. https://doi.org/10.1109/transai60598.2023.00048
15. Scampicchio E. Arcari E., Zeilinger M.N. Error analysis of regularized trigonometric linear regression with unbounded sampling: a statistical learning viewpoint. *IEEE Control Systems Letters*, 2023, vol. 7, pp. 3066–3071. https://doi.org/10.1109/lcsys.2023.3291690
16. Guerra-Manzanares A., Medina-Galindo J., Bahsi H., Nõmm S. MedBIoT: Generation of an IoT botnet dataset in a medium-sized IoT network. *Proc. of the 6th International Conference on Information Systems Security and Privacy*, 2020, vol. 1, pp. 207–218. https://doi.org/10.5220/0009187802070218

Автор

Бучаев Абдулхамид Яхьяевич — аспирант, преподаватель, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57219568840, https://orcid.org/0009-0001-1058-9125, abdulhamid0055@yandex.ru

Author

Abdulhamid Y. Buchaev — PhD Student, Lecturer, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57219568840, https://orcid.org/0009-0001-1058-9125, abdulhamid0055@yandex.ru

Статья поступила в редакцию 30.06.2025
Одобрена после рецензирования 12.05.2025
Принята к печати 16.03.2026

Received 30.06.2025
Approved after reviewing 12.05.2025
Accepted 16.03.2026