УДК 004.056
DOI: 10.26102/2310-6018/2026.62.11.001

Формальная модель инцидента информационной безопасности

М.И. Синцов✉, Д.И. Правиков

Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, Москва, Российская Федерация

Резюме. В статье предложен подход к формальному описанию инцидента информационной безопасности (ИБ). Сформированы критерии перехода от события ИБ к инциденту: событие → нарушение политики ИБ → нарушение ИБ → инцидент. Проведен анализ существующих методов и подходов к описанию инцидента ИБ, которые позволяют ранжировать, группировать, объединять действия злоумышленника в отношении атакуемого объекта, выстраивать корреляции, обосновывать момент начала применения активного реагирования. Предложено описание инцидента в виде упорядоченного кортежа, предназначенного для объединения атомарных инцидентов и подозрений в цепочки атаки с учетом динамики последствий и допустимого ущерба организации. Предложенный подход позволит объединять атомарные инциденты, реагирование на которые во многих случаях не требуется, в сложные цепочки атаки, продуктивно реализовать реагирование на возникающие инциденты с учетом динамики их развития в рамках цепочки атаки. Объединение атомарных инцидентов позволяет оптимизировать ресурсы, затрачиваемые подразделениями ИБ на противостояние атакам злоумышленников, акцентируя внимание только на те действия, которые непосредственно представляют угрозу в текущий момент времени, а не являются гипотетически возможными, что в результате смещает фокус подразделений ИБ на обеспечение практической защищенности организации. В качестве возможностей практического применения предложенного подхода рассмотрен пример с проведением атаки на домен через фишинг. На текущий момент модель имеет концептуальный характер, ожидаемые эффекты для автоматизации действий аналитиков в SOAR и оптимизации ресурсов требуют дополнительного тестирования.

Ключевые слова: инцидент информационной безопасности, формальная модель, событие ИБ, нарушение политики, нарушение безопасности.

Для цитирования: Синцов М.И., Правиков Д.И. Формальная модель инцидента информационной безопасности. *Моделирование, оптимизация и информационные технологии.* 2026;14(11). URL: https://moitvivt.ru/ru/journal/article?id=2552 DOI: 10.26102/2310-6018/2026.62.11.001

A formal model of an information security incident

M.I. Sintsov✉, D.I. Pravikov

Gubkin Russian State University of Oil and Gas (National Research University), Moscow, the Russian Federation

Abstract. The article proposes an approach to formally describing an information security (IS) incident. The criteria for transitioning from an IS event to an incident are formulated: event → IS policy violation → IS violation → incident. An analysis is conducted of existing methods and approaches to describing an IS incident, which make it possible to rank, group, and combine the attacker's actions against the target object, establish correlations, and justify the moment when active response measures should be initiated. A description of the incident is proposed in the form of an ordered tuple, intended to combine atomic incidents and suspicions into attack chains, taking into account the dynamics of the consequences and the permissible damage to the organization. The proposed approach makes it possible to combine atomic incidents, the response to which in many cases is not required, into complex attack chains, and

© Синцов М.И., Правиков Д.И., 2026

to effectively implement a response to emerging incidents, taking into account the dynamics of their development within the chains. Combining atomic incidents makes it possible to optimize the resources spent by IS units on countering attacker actions, focusing attention only on those actions that directly pose a threat at the current moment in time rather than being hypothetically possible, which as a result shifts the focus of IS units toward ensuring the practical security of the organization. As a possibility for the practical application of the proposed approach, an example of an attack on a domain via phishing is considered. At present, the model is conceptual in nature; the expected effects for automating analysts' actions in SOAR and optimizing resources require additional testing.

Keywords: information security incident, formal model, information security event, policy violation, security violation.

For citation: Sintsov M.I., Pravikov D.I. A formal model of an information security incident. *Modeling, Optimization and Information Technology.* 2026;14(11). (In Russ.). URL: https://moitvivt.ru/ru/journal/article?id=2552 DOI: 10.26102/2310-6018/2026.62.11.001

Введение

Большое количество подозрений на инциденты информационной безопасности (ИБ), которые поступают для обработки в центры мониторинга ИБ, приводит к необходимости выработки соответствующих стратегий поведения, чтобы возможности ресурсного обеспечения соответствовали входному потоку. На концептуальном уровне возможны 2 стратегии – приоритезация обработки с последующим отбрасыванием незначимых подозрений либо агрегация более крупных сущностей (сложные инциденты). Приоритезация и отбрасывание могут привести к потерям значимых событий и несвоевременному реагированию. Поэтому в качестве наиболее перспективного рассмотрим агрегацию атомарных подозрений на инциденты в более сложные.

При этом ключевая задача состоит в том, чтобы не допустить наступления негативных последствий для организации [1]. Как показывает практика[1] [2], негативные последствия не наступают моментально. Злоумышленнику требуется провести ряд действий, которые по итогу могут привести к наступлению ущерба. Данные действия осуществляются в рамках некой цепочки атаки (либо цепочек атак). Таким образом, в статье проводится исследование инцидента ИБ, не просто как некоторого триггера (со статическими параметрами) для активации заранее определенного перечня контрмер в некий момент времени, а как непрерывно изменяющегося набора деструктивных действий потенциального злоумышленника. Предлагается ввести градацию событий ИБ (совокупности событий ИБ), в рамках которой в каждый момент времени проводится оценка ущерба от данных событий с целью организации своевременного реагирования.

Цель исследования – предложить согласованное описание инцидента (цепочки атаки), позволяющее объединять связанные события (подозрения на инциденты). Задачи исследования: провести анализ, оценить преимущества и недостатки существующих подходов, дать предложения к формальному описанию комплексного инцидента с учетом критериев перехода между уровнями, допустимого ущерба, полноты данных расследования. В качестве подтверждения – проиллюстрировать применение модели, дать ее оценку по применимости.

Любой инцидент информационной безопасности начинается с некоторого события, регистрируемого информационной системой, средством защиты информации

[1] Головко Н. *Прогноз развития киберугроз и средств защиты информации – 2026.* Anti-Malware.ru. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Threat-and-Information-Security-Forecast-2026?ysclid=mqr3zhxky1931550833 (дата обращения: 01.06.2026).

или наблюдателем, которое представляет определенный интерес с точки зрения ИБ. Процесс перехода можно представить следующей цепочкой:

1. Событие ИБ – любое зафиксированное изменение состояния информационной системы, либо некое действие, связанное с ней (например, удачная или неудачная попытка входа, запуск процесса, сетевое соединение). На этом этапе событие может быть как штатным, так и аномальным. Количество таких событий исчисляется десятками/сотнями тысяч [3].

2. Нарушение политики ИБ – событие или набор событий, которые противоречат установленным правилам и процедурам (например, попытка доступа к ресурсу вне рабочего времени, несоблюдение политики «чистого стола», не обновлены базы системы антивирусной защиты и т. д.). Это категоризация события с точки зрения нормативных требований организации. При этом данное событие или набор событий уже являются аномальными, но на данном уровне предпосылки реального ущерба еще не подтверждены. Последствия действий пользователя/потенциального нарушителя подлежат дополнительной оценке. Количество таких событий уже исчисляется тысячами/десятками тысяч [4].

3. Нарушение ИБ – факт, при котором нарушение политики ИБ приводит к реальному ущербу (но не превышающему некий порог) или создает предпосылки для реализации атаки (например, несанкционированный доступ к конфиденциальным данным, сканирование сети ботом, отказ в обслуживании). Нарушение ИБ – результат реализации угрозы (как внешней, так и внутренней). Таким образом, в данном случае уже есть некоторые последствия, но величина подтвержденного ущерба еще не превышает принятого в организации порога. Количество событий исчисляется сотнями/тысячами.

4. Инцидент ИБ – нарушение ИБ, при котором величина ущерба превышает некоторый заданный порог. Иными словами, это набор событий ИБ, которые привели к некоторому ущербу. Количество событий исчисляется сотнями (в зависимости от организации это количество может превышать возможности анализа и обработки)[2] [5].

Указанные порядки количества событий на уровнях являются иллюстративными, относятся к одному условному интервалу наблюдения и не задают статистически подтвержденных диапазонов или нормативной нагрузки SOC. Предложенная цепочка описывает уровни оценки: обязательное последовательное прохождение всех уровней не предполагается. При наличии достаточных оснований событие может сразу получить статус инцидента.

Используемый в настоящей статье порог ущерба является рабочим критерием эскалации и не заменяет применимые нормативные определения инцидента.

Таким образом, инцидент – это событие ИБ или набор событий, прошедшее через фильтры политики ИБ, оценки угрозы и ущерба для организации. Ключевым критерием перехода с одного этапа на другой является наличие последствий[3].

Анализ существующих подходов по формальному описанию инцидента. Вопрос формального описания инцидента ИБ, объединения разрозненных событий в один инцидент, объединение атомарных инцидентов в сложный активно исследуется.

В работе [6] описывается применение алгоритма кластеризации (DBSCAN) к потоку событий, выделяя группы (кластеры) по сходству атрибутов. Подход эффективен

[2] *Итоги расследований инцидентов ИБ в 2021–2023 годах.* Positive Technologies. URL: https://ptsecurity.com/research/analytics/outcomes-of-IS-incident-investigations-in-2021-2023-years/ (дата обращения: 01.06.2026).

[3] Котенко И.В. *Аналитическая обработка больших массивов гетерогенных данных о событиях кибербезопасности в интересах оценки состояния, поддержки принятия решений и расследования компьютерных инцидентов в критически важных инфраструктурах. Отчет о НИР № 21-71-20078.* Российский научный фонд. URL: https://www.rscf.ru/project/21-71-20078/ (дата обращения: 01.05.2026).

для детектирования массовых однотипных событий (например, атака DDoS), но могут быть трудности при многозвенных атаках, где события разнородны (например, цепочка атаки: Brute Force, повышение привилегий, дамп LSASS и Pass-the-Hash с горизонтальным перемещением). При выборе метрики необходимо учитывать содержательные связи между разными атрибутами (например, событие A и B имеют общий IP, B и C – общий UserName, C и D – общий EventID, но DBSCAN может разбить их на два кластера из-за разной плотности). Сложность его применения в рассматриваемой задаче связана с выбором признаков и метрики для разнородных событий. В работе [7] предложена модель на основе рекуррентных нейронных сетей (LSTM) для прогнозирования инцидента по временной последовательности событий с использованием LLM. В статье особое внимание уделено рассмотрению существующей проблемы интерпретируемости и повторяемости полученного результата. Что в итоге приводит к тому, что для корректной работы модели требуются большие объемы исторических данных. В работе [8] рассмотрен метод моделирования компьютерных атак на основе вероятностных автоматов. Метод позволяет формализовать и анализировать атаки как последовательность этапов, приводящих целевую систему в определенное состояние. Модель может использоваться для симуляции реальных систем. Если вместо атаки, т. е. действий злоумышленника, рассмотреть инцидент ИБ, то предложенную в работе модель можно рассматривать как основу формального описания инцидента, т. к. инцидент является результатом атаки. Но при этом нужно учесть, что для возникновения инцидента недостаточно только атаки [9], необходимо иметь еще и некую уязвимость в атакуемой системе, что не учитывается в предлагаемой модели атаки[4]. В работе [10] в качестве основных проблем обозначены необходимость создания моделей кластеризации инцидента, учитывающих инвариантность к вариациям формата данных, семантическое понимание содержания инцидентов и способность к автоматическому обнаружению связей без предварительных предположений о количестве и структуре цепочек атак. По мнению авторов работы представленная реализация модели не учитывает временную последовательность событий, рассматривая все инциденты кластера как равноправные элементы множества. В рассматриваемой же задаче временная шкала имеет важное значение как для построения цепочки атаки, когда действия происходят последовательно, иногда с большим разбросом по времени, так и для вычисления в дальнейшем времени наступления недопустимого ущерба. Таким образом, требуется согласованная формализованная модель, описывающая инцидент как целостный объект с множественными атрибутами времени, источника, типа событий, последствий, величины ущерба и т. д. Многие рассмотренные алгоритмы формализации инцидента ИБ требуют для корректной работы большие объемы исторических данных, которые должны быть размечены. При этом не учитывается тот факт, что разметка данных является величиной субъективной и очень зависит от контекста организации, актуальных угроз, величины возможного ущерба. Многие работы сосредоточены на частных аспектах (корреляция, классификация [11], реагирование [12]) и не дают универсального формального описания, которое позволит рассматривать инцидент ИБ как непрерывно изменяющийся объект, взаимодействие с которым (т. е. реагирование на инцидент) может то усиливаться, то ослабевать в зависимости от его текущего состояния и ущерба для организации, к которому данное состояние может привести. Лавинообразное увеличение источников событий ИБ, а соответственно и инцидентов ИБ требует решения вопроса объединения множества атомарных инцидентов ИБ, приоритет реакции на которые определяется контекстом, в сложные инциденты ИБ. Для

[4] Levtsov V. *Анатомия таргетированной атаки.* Лаборатория Касперского. URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/?ysclid=mqr52em2w747120318 (дата обращения: 01.05.2026).

своевременного выявления и реагирования на современные инциденты ИБ требуется автоматизированный вывод новых паттернов корреляции из потока событий ИБ. Применение ML-подходов требует контроля ложных срабатываний и интерпретируемости результата. Для логических и автоматных моделей существенны первоначальная настройка и актуализация правил при изменении контекста. Новизна предлагаемого подхода ограничивается согласованным представлением развивающегося инцидента, связывающим граф событий с последствиями, допустимым ущербом и данными расследования. Само использование графа и причинных зависимостей не является новым подходом в формализации. В отличие от графа возможных путей атаки, здесь рассматривается граф зарегистрированных событий. От вероятностного автомата он отличается отсутствием оценивания вероятностей переходов. Это различие назначения и состава описания, а не доказательство превосходства над существующими моделями.

Другой существующей проблемой является масштабирование предлагаемых моделей на реальных нагрузках SOC. Результаты проверки на небольших или синтетических наборах данных нельзя автоматически переносить на промышленную нагрузку. В реальных условиях количество событий может превышать десятки тысяч, что требует применения особых алгоритмов. Настоящая работа на текущий момент не подтверждена испытаниями на промышленном потоке. Поэтому предложенный вклад рассматривается как концептуальная схема с формально заданными компонентами и критериями. Масштабируемость и практическая эффективность требуют дополнительной проверки.

Материалы и методы

В качестве иллюстрации нагрузки рассмотрим SOC, в который ежесекундно поступают тысячи сырых событий от различных источников. Далее проходя через фильтры правил корреляции атомарные события трансформируются в инциденты ИБ. Но, как было отмечено выше, количество инцидентов все равно превышает тот объем, который может быть обработан. Необходима дополнительная корреляция – процесс объединения атомарных инцидентов на основе некоторых атрибутов.

Предположим, E – множество сырых событий:

$$E = \{e_1, e_2, \dots, e_n\}.$$

Каждое событие e_i характеризуется набором атрибутов

$$X(e_i) = \{x^1, x^2, \dots, x_k\},$$

где x_j – пара «имя поля, его нормализованное значение» (например, EventID=4624, SourceUserName=User1 Devicehostname=PC_User1, EndTime=01.01.2026 10:23:45, ProcessId=1234).

Формально $X(e) \subseteq \bigcup_{k \in K} (\{k\} \times Val(k))$, где K – множество имен полей; Val(k) – область значений поля k, для каждого имени в событии допускается не более одного значения; E – конечное множество событий выбранного интервала.

Корреляция заключается в поиске подмножеств событий $E' \subseteq E$, связанных совпадением нормализованных атрибутов и временным либо содержательным контекстом. Такое подмножество может стать подозрением на инцидент P_I. При этом совпадение атрибутов само по себе не доказывает общую причину событий.

Для решения задачи формализации инцидента ИБ предлагается определить инцидент информационной безопасности как упорядоченный кортеж:

$$I = \langle E', X|E', S, A, T, P, R, C, D \rangle, \; E' \subseteq E,$$

где E′ – множество событий (атомарных инцидентов). X|E′ – атрибуты событий выбранного подмножества. T – множество временных меток событий, составляющих инцидент (начало, ключевые этапы, конец). $T = \{t_0, t_1, \ldots, t_n\}$. $T = \{t(e): e \in E'\}$. Совпадающие временные метки учитываются однократно, поэтому $|T| \leq |E'|$. S – множество источников (субъектов/объектов), инициировавших события: пользователи, процессы, IP-адреса, устройства. $S = \{s(e): e \in E'\}$. Пользователи, процессы и адреса инициаторов фиксируются в X(e). Число уникальных источников не обязано совпадать с числом событий, если событие требует обогащения. P – множество нарушенных политик безопасности (ссылки на конкретные правила и/или нормативные документы: P1, P2, …). Формально $P = \{p \in R \mid v_p(E') = 1\}$, где $v_p: 2^E \rightarrow \{0,1\}$. R – каталог требований безопасности. v_p – функция проверки требования p по переданным свидетельствам. A – множество затронутых ИТ-активов: хосты, файлы, базы данных, службы, оборудование. $A = \bigcup_{e \in E'} a(e)$. R – тип и тяжесть последствий (ущерб). Определяется через параметры: ⟨тип, критичность⟩, где тип – например, конфиденциальность, целостность, доступность, а критичность – числовая оценка ущерба. C – связи между событиями внутри инцидента. Представляется ориентированным графом G = (V, L), где V ⊆ события, L – ребра «причина-следствие». D – данные расследования (log-файлы, артефакты, свидетельства).

Объединение формализованных событий в единый инцидент можно осуществлять следующим образом:

1. Через транзитивные связи между событиями: Когда все события имеют цепочку пересекающихся множеств атрибутов: либо по пользователю, хосту, процессу, при согласовании временного контекста. Такая связность обеспечивает объединение в общую цепочку, которая затем проверяется.

2. Через метрику сходства (индекс Жаккара): $J(e_i,e_j) = |X(e_i) \cap X(e_j)| / |X(e_i) \cup X(e_j)|$; при пустом объединении J = 0. Метрика применима к парам событий как дополнительный признак, но не является достаточным или обязательным условием связи разнородных этапов атаки.

3. Через порог по числу «важных» пересечений. Для корреляции может быть достаточно, чтобы пересекались хотя бы два критичных атрибута.

Для воспроизводимого правила введем $b(e_i,e_j) = 1$, если $|t(e_i) - t(e_j)| \leq \Delta$ и выполняется либо $J(e_i,e_j) \geq \eta$ при подтвержденной контекстной совместимости, либо отдельное семантическое правило связи $r(e_i,e_j) = 1$. Семантическое правило r задается по типам источников, например, по учетной записи или связи родительского и дочернего процессов на одном хосте. Пропущенные поля совпадениями не считаются. В C ребра направляются от более раннего события к более позднему. При равном времени направление требует дополнительного обоснования. При объединении событий/атомарных инцидентов берется объединение их событий и доказательств, а P, R, C и D рассматриваются в едином контексте.

Рассмотрим пример объединения нескольких атомарных инцидентов (входные данные) в сложный инцидент «Фишинг → переход по потенциально небезопасной ссылке → загрузка полезной нагрузки → боковое перемещение»:

Атомарные инциденты (подозрения на инцидент)

1. Просто событие ИБ:

E_1 (почтовый шлюз KSMG): Атрибуты = Письмо с подозрительной ссылкой получено пользователем User1@company.ru. Источник S = KSMG, актив A = User1, категория события = PhishingLinkDetected.T = 01.06 10:30.

2. Нарушение политики ИБ/Нарушение ИБ – Переход по внешним ссылкам в письмах нарушает политику, если соответствующий запрет установлен в данной организации.

E_2 (прокси-сервер): Атрибуты = Переход по URL ссылке и загрузка исполняемого файла update.exe с IP XX.XX.XX.XX с рабочей станции Notebook_User1. S = Proxy, актив A = Notebook_User1, категория-события = SuspiciousDownload. T = 01.06 11:30.

3. Нарушение политики ИБ/Нарушение ИБ – запуск cmd недоверенным процессом и несанкционированное создание пользователя.

E_3 (EDR): Атрибуты = Процесс update.exe выполнил cmd.exe для создания нового пользователя в AD. S = EDR, актив A = Notebook_User1, категория события = PrivilegeEscalation. T = 01.06 11:45.

4. Нарушение ИБ/Инцидент – удаление базы данных (БД) приводит к ущербу в организации.

E_4 (контроллер домена, сервер БД): Атрибуты = удачная аутентификация с Notebook_User1 на сервер DB с учетной записью local_admin и последующее удаление БД. S = журнал аутентификации DC, журнал аудита DB, Notebook_User1, актив A = DC, DB, Notebook_User1, категория события = LateralMovement, DataDestruction. T = 01.06 11:50.

Объединение в сложный инцидент:

Вычисляем сходство (индекс Жаккара) попарно. E_1 и E_2 объединяются по пользователю и URL при подтвержденной привязке пользователя к рабочей станции. E_2 и E_3 связываются по активу и идентичности загруженного и запущенного файла; E_3 и E_4 – по данным процесса, учетной записи и сеанса доступа к DB. Совпадения только Notebook_User1 недостаточно. Например, для $X(E_1) = \{\langle user,User1\rangle, \langle url,url_1\rangle\}$ и $X(E_2) = X(E_1) \cup \{\langle host,Notebook_User1\rangle, \langle file,update.exe\rangle\}$ получаем $J = 2/4 = 0{,}5$; при $\eta = 0{,}5$, $\Delta = 2$ часа и подтвержденном контексте пара удовлетворяет правилу b.

В результате объединения похожих инцидентов получаем единый сложный инцидент:

$$I_{phish} = \langle \{E_1,E_2,E_3,E_4\}, X|\{E_1,E_2,E_3,E_4\}, S, A, T, P, R, C, D\rangle.$$

Атрибуты E_1–E_4 соответствуют приведенному выше описанию; временные метки условного сценария: 01.06 10:30, 11:30, 11:45 и 11:50 соответственно. E_4 сохраняет исходные записи об аутентификации и удалении как отдельные доказательства внутри сложного инцидента. Удачная авторизация на сервере БД подтверждает несанкционированный доступ злоумышленника, но не выполнение команды удаления базы данных; последнее устанавливается аудитом системы управления БД и проверкой состояния БД.

S – Источники событий (шлюз KSMG, Transport Log Exchange прокси-сервер, EDR, контроллер домена, журналы аутентификации DC и аудита DB).

A – Актив (User1, Notebook_User1, DC, DB).

P – нарушенные правила организации: запрет несанкционированного запуска программного обеспечения, создания учетных записей и доступа к БД. PhishingDetected, SuspiciousDownload, PrivilegeEscalation и LateralMovement обозначают категории событий и гипотезы об этапах атаки.

R – пары «тип, критичность». Для указанного примера примем возможный простой БД 7 часов при $M_{доступность} = 10$ часов и $\rho_{доступность} = 6$. Тогда $r_{доступность} = 10 \cdot 7/10 = 7 > 6$. Результат 7 превышает порог. Оценки конфиденциальности и целостности до проверки равны W. Поэтому $R = \{\langle$доступность, 7$\rangle$, $\langle$конфиденциальность, W$\rangle$, $\langle$целостность, W$\rangle\}$. Таким образом, максимум известных оценок равен 7, но не является полной оценкой всех последствий. Значения времени и порога условны, не получены экспериментально.

C – граф событий, соответствующих этапам «письмо → URL-ссылка → исполняемый файл → предполагаемое повышение привилегий → горизонтальное перемещение до сервера с БД».

Для контроля качества реагирования вводится метрика полноты собранных данных:

$$\text{Completeness(D)} = (|\text{D(actual)} \cap \text{D(expected)}|) / |\text{D(expected)}|,$$

где D (expected) – минимальный набор артефактов, необходимых для конкретного типа инцидента (например, дамп памяти, триаж, сетевые логи, журналы авторизации, IP-адрес и т. д.). Если полнота меньше некоторого заданного значения, то необходимо выполнять задачу дополнительного анализа.

Для каждого типа инцидента задается каталог обязательных требований Req(c). D(expected) = Req(c), а D(actual) в формуле означает множество выполненных требований, подтвержденных пригодными артефактами из D. Требование включает вид данных, актив, интервал и критерий пригодности; дубликаты не увеличивают полноту. При пустом D(expected) метрика не определена. Для рассматриваемого сценария зададим шесть требований: исходное письмо; журнал загрузки; дерево процессов с хэшем файла; журнал аутентификации; аудит выполнения команды удаления; подтверждение простоя и восстановления БД. Если выполнены пять требований, полнота равна 5/6 ≈ 0,83. При пороге 1 требуется получить недостающий артефакт либо отметить его недоступность. При этом покрытие списка не доказывает правильность всей реконструкции атаки.

Атомарно все перечисленные в примере инциденты могут быть некритическими и не требовать немедленных действий, но иногда все определяет последнее действие злоумышленника, на которое требуется незамедлительная реакция. В частности, если бы не было факта удаления БД, то все остальные действия не требовали немедленной реакции со стороны подразделения ИБ. Нужно отметить, что объединение событий уточняет приоритет реагирования, но не отменяет реагирование на опасные промежуточные этапы. Пример оценки полноты проведенного расследования (на основании сбора перечня необходимых артефактов). Может применяться в том числе для оценки качества анализа подозрений на инциденты со стороны дежурных аналитиков [13].

Результаты и обсуждение

Полученный результат – согласованное кортежное представление сложного инцидента, дополненное критерием превышения допустимого ущерба и требованиями к данным расследования. Предложенное формальное описание может служить основой для автоматизации корреляции атомарных инцидентов в цепочку событий в системах класса IRP/SOAR.

Предложенное формальное описание учитывает следующие проблемы, возникающие при анализе инцидентов:

1. Многомерность: инцидент может обладать разнородным количеством атрибутов: временными, пространственными, причинными, нормативными и контекстными характеристиками. В предложенном описании выбор атрибутов обусловлен информацией, которая содержалась в используемых автором решениях класса SIEM и IRP. В случае наличия система класса управления активами, управления уязвимостями набор атрибутов может быть расширен.

2. Нечеткость: границы между событием, нарушением политики ИБ, нарушением ИБ и инцидентом размыты, решение о классификации субъективно и зависит от контекста организации. В качестве решения указанной проблемы возможно использование формализованных требований в нормативных документах ФСТЭК

России в отношении государственных информационных систем, информационных систем персональных данных и объектов критической информационной инфраструктуры, нарушение которых можно транслировать как нарушение защищенности исследуемого объекта мониторинга.

3. Динамичность: инцидент может развиваться во времени, один инцидент может состоять из множества вложенных подинцидентов. Модель обладает свойствами гибкого изменения временного контекстного окна.

Предложенная формальная модель на взгляд авторов позволяет обеспечить баланс между абстракцией для обобщения и детальным представлением атрибутов кортежа для практического применения. По сравнению с применением только кластеризации предлагаемый кортеж дополнительно хранит объяснение связи и основание эскалации, временную последовательность событий. По сравнению с вероятностными автоматами, с одной стороны, не оценивает вероятности скрытых состояний и не прогнозирует следующий шаг атаки, но, с другой стороны, содержит описание нарушения (уязвимость), которое привело к успешной атаке. Данное нарушение можно использовать в качестве отправной точки для формирования контрмер. Граф и автомат могут использоваться как внешние источники гипотез для заполнения кортежа. Преимущество такой интеграции предполагается, но сравнительными измерениями не подтверждено.

Результат корреляции зависит от качества идентификации сущностей, синхронизации времени и полноты журналирования. Транзитивная связность может ошибочно объединять независимые действия через общий сервис или учетную запись. Ограничение Δ способно пропускать медленные атаки. Изменение η влияет на баланс ошибочных объединений и разрывов цепочек. Подбор параметров и правила разделения компонентов требуют дополнительной проверки на размеченных последовательностях. Следует измерять точность и полноту объединения событий, задержку эскалации, долю ошибочных слияний, пропускную способность и память при явно заданной интенсивности потока. Дополнительно требуется анализ чувствительности к Δ, η. Эти измерения являются планом дальнейшей работы.

Важно отметить, что при анализе многомерных данных важно учитывать вычислительную сложность.

Заключение

Предложенное описание инцидента в виде кортежа представляет собой гибкий и расширяемый инструмент для формализации инцидента информационной безопасности.

Приведенные в статье примеры демонстрируют применимость предложенной формальной модели в SOAR-системах, что подтверждает ее практическую полезность для Центров управления ИБ.

Дальнейшее усовершенствование предложенного кортежа может быть применено в следующих исследовательских и практических направлениях:

1. Автоматическая классификация инцидентов: на основе сравнения (например, парно выбирая два параметра) можно строить таксономии и применять алгоритмы кластеризации.

2. Корреляция множественных инцидентов: если два инцидента I_1 и I_2 имеют пересекающиеся S и C, то их можно объединить в один инцидент (потенциально целенаправленная атака).

3. Оценка эффективности реагирования: сравнивая D (собранные данные) с полнотой T и C, можно выявлять пробелы в расследовании.

4. Прогнозирование развития: на основе известных шаблонов C (например, последовательности «разведка → эксплуатация → закрепление») можно предсказывать следующие события.

5. Проверка соответствия политикам: автоматическое определение, какие политики P были нарушены, и были ли они корректно настроены.

6. Построение графов атак: извлечение C из логов и визуализация многоэтапных атак.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Синцов М.И. Снижение вероятности последствий компрометации ИТ-инфраструктуры предприятия за счет синергии применения перспективных методов выявления угроз и последующего их ретроспективного анализа. Подходы к оценке качества разработанных правил корреляции для ретроспективного анализа. В сборнике: *Актуальные проблемы защиты информации: современность и перспективы: Материалы II Научно-практической конференции, 09–10 апреля 2024 года, Москва, Россия*. Москва: Московский государственный технический университет имени Н.Э. Баумана; 2025. С. 37–42.
2. Ракинцев Н.А. Инциденты информационной безопасности 1-го полугодия 2020 года в транспортной отрасли. Введение мер по их предотвращению. *Молодой ученый.* 2020;(27):61–63.
3. Котенко И.В., Федорченко А.В., Саенко И.Б., Кушнеревич А.Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей. *Вопросы кибербезопасности.* 2017;(5):2–16.
   Kotenko I., Fedorchenko A., Saenko I., Kushnerevich A. Big data technologies for security event correlation based on event type accounting. *Voprosy kiberbezopasnosti.* 2017;(5):2–16. (In Russ.).
4. Кузнецов А.В. Организация раздельного хранения данных о событиях безопасности. *Вопросы кибербезопасности.* 2024;(2):22–28. https://doi.org/10.21681/2311-3456-2024-2-22-28
   Kuznetsov A.V. The organization of separate security event data storage. *Voprosy kiberbezopasnosti.* 2024;(2):22–28. (In Russ.). https://doi.org/10.21681/2311-3456-2024-2-22-28
5. Букин А.В., Самонов А.В., Тихонов Э.И. Обнаружение инцидентов информационной безопасности на основе технологии нейронных сетей. *Вопросы кибербезопасности.* 2022;(5):61–73.
   Bukin A., Samonov A., Tihonov E. Detecting information security incidents based on neural network technology. *Voprosy kiberbezopasnosti.* 2022;(5):61–73. (In Russ.).
6. Landauer M., Skopik F., Wurzenberger M., Rauber A. System log clustering approaches for cyber security applications: A survey. *Computers & Security.* 2020;92:101739. https://doi.org/10.1016/j.cose.2020.101739
7. Brown A., Tuor A., Hutchinson B., Nichols N. *Recurrent Neural Network Attention Mechanisms for Interpretable System Log Anomaly Detection.* arXiv. URL: https://arxiv.org/abs/1803.04967 [Accessed 1st May 2026].
8. Тумоян Е.П. Метод моделирования компьютерных атак на основе вероятностных автоматов. *Известия ЮФУ. Технические науки.* 2008;(8):120–126.
   Tumoyan E.P. Probabilistic automata based computer attack modeling approach. *Izvestiya SFedU. Engineering Sciences.* 2008;(8):120–126. (In Russ.).

9. Горев А.И., Горева Е.Г. Кибератаки: некоторые подходы к системному анализу. *Математические структуры и моделирование.* 2024;(1):110–116. https://doi.org/10.24147/2222-8772.2024.1.110-116
10. Котенко И.В., Саенко И.Б., Лаута О.С., Куракин А.С. Семантическая кластеризация инцидентов на основе алгоритма DBSCAN и большой языковой модели. *Вопросы кибербезопасности.* 2026;(2):2–15. https://doi.org/10.21681/2311-3456-2026-2-2-15
Kotenko I.V., Saenko I.B., Lauta O.S., Kurakin A.S. Semantic clustering of incidents based on the DBSCAN algorithm and a large language model. *Voprosy kiberbezopasnosti.* 2026;(2):2–15. (In Russ.). https://doi.org/10.21681/2311-3456-2026-2-2-15
11. Жуков В.Г., Шаляпин А.А., Соколов М.М. Исследование алгоритма прецедентного анализа в задаче классификации инцидентов информационной безопасности. *Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева.* 2015;16(3):572–579.
Zhukov V.G., Shalyapin A.A., Sokolov M.M. Research of the case analysis algorithm in the classification of problem of information security incidents. *Vestnik SibSAU. Aerospace Technologies and Control Systems.* 2015;16(3):572–579. (In Russ.).
12. Резниченко С.А., Турабов Д.Р. Методология выбора критериев эффективности системы информационной безопасности при имитационных атаках Red Team. *Вестник Дагестанского государственного технического университета. Технические науки.* 2025;52(3):135–151. https://doi.org/10.21822/2073-6185-2025-52-3-135-151
Reznichenko S.A., Turabov D.R. Methodology for selecting effectiveness criteria of information Security Systems during Red Team simulated attacks. *Herald of Dagestan State Technical University. Technical Sciences.* 2025;52(3):135–151. (In Russ.). https://doi.org/10.21822/2073-6185-2025-52-3-135-151
13. Синцов М.И. Выбор подхода для расчета оптимального времени выявления и реагирования на угрозы информационной безопасности в условиях ограниченных ресурсов. *Проблемы информационной безопасности. Компьютерные системы.* 2025;(4):23–34. https://doi.org/10.48612/jisp/mp7a-vpp7-xu6f
Sintsov M.I. Determining the optimal response time to information security threats in a limited resource environment. *Problems of Information Security. Computer Systems.* 2025;(4):23–34. (In Russ.). https://doi.org/10.48612/jisp/mp7a-vpp7-xu6f

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Синцов Михаил Игоревич, аспирант, Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, Москва, Российская Федерация.
e-mail: sinzovmi@gmail.com
ORCID: 0009-0004-4143-7302

Mikhail I. Sintsov, Postgraduate, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, the Russian Federation.

Правиков Дмитрий Игоревич, кандидат технических наук, заведующий кафедрой комплексной безопасности критически важных объектов, Российский государственный университет нефти и газа (национальный

Dmitri I. Pravikov, Candidate of Engineering Sciences, Head of the Department of Comprehensive Security of Critical Facilities, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, the Russian Federation.

исследовательский университет) имени И.М. Губкина, Москва, Российская Федерация.
e-mail: dip@gubkin.pro
ORCID: 0000-0001-5217-4537

Статья поступила в редакцию 03.08.2026; одобрена после рецензирования 16.10.2026; принята к публикации 02.11.2026.

The article was submitted 03.08.2026; approved after reviewing 16.10.2026; accepted for publication 02.11.2026.