УДК 004.056

МЕТОДИКА ИНТЕГРИРОВАННОГО АНАЛИЗА СОБЫТИЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Сташкевич С.О., магистрант гр. 567241

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бойправ О.В. – канд. тех. наук, доцент,
заведующий кафедрой защиты информации

Аннотация. В статье представлен обзор подходов к разработке методики интегрированного анализа событий информационной безопасности. На основе анализа нормативных правовых актов Республики Беларусь выполнена классификация событий информационной безопасности, определены характеристики источников таких событий и проведена оценка современных средств их анализа. Предложена трехуровневая гибридная модель классификации, включающая технический, тактический и стратегический уровни. Полученные результаты являются основой для дальнейшей разработки методики.

Ключевые слова. события информационной безопасности, SIEM-системы, корреляция событий, управление инцидентами, классификация событий, MITRE ATT&CK.

В условиях цифровой трансформации проблема обеспечения информационной безопасности (ИБ) приобретает критическое значение. В соответствии с Концепцией информационной безопасности Республики Беларусь, утвержденной Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, формирование информационного общества рассматривается как национальный приоритет и общегосударственная задача [1].

Многочисленные средства защиты информации (СЗИ), используемые в организациях, порождают огромное количество событий безопасности, разбор которых вручную становится невозможным, а игнорирование недопустимо [2]. По данным аналитических отчетов, крупные компании используют в среднем 43 различных СЗИ, а некоторые – более 100 [3]. В таких условиях особую актуальность приобретает задача интегрированного анализа событий ИБ.

Целью настоящей работы является обзор существующих подходов к классификации событий ИБ, анализу характеристик источников событий и оценке средств их анализа как основы для последующей разработки усовершенствованной методики интегрированного анализа.

В соответствии со СТБ ISO/IEC 27000–2024 событие информационной безопасности определяется как установленное возникновение состояния системы, службы или сети, указывающее на возможное нарушение информационной безопасности [4].

Исчерпывающий перечень типов и записей событий информационной безопасности, подлежащих регистрации, установлен приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130 [5]. Указанный перечень подразделяет события на пять категорий: операционные системы, системы управления базами данных, телекоммуникационное оборудование, прикладное программное обеспечение, средства защиты информации.

Многоуровневая гибридная модель классификации. В рамках разработки методики интегрированного анализа предложена трехуровневая гибридная модель классификации событий информационной безопасности.

Первый, базовый уровень, осуществляет техническую категоризацию сырых событий (например, «сетевая атака», «нарушение политики», «ошибка аутентификации»). Данный уровень обеспечивает первичную группировку событий.

Второй, тактический уровень, вводит интеллектуальную приоритизацию через динамический расчёт показателя риска (Severity Score), учитывающего тип события, критичность актива, надежность источника данных и контекст возникновения. Динамический расчет позволяет автоматически отфильтровывать шум и выделять значимые инциденты.

Третий, стратегический уровень использует таксономию MITRE ATT&CK для описания события в терминах поведения злоумышленника (тактики и техники). Согласно современным исследованиям, привязка правил корреляции к матрице MITRE ATT&CK обеспечивает прозрачное понимание полноты мониторинга и помогает расставлять приоритеты при развитии системы обнаружения атак [6].

Под источником событий ИБ понимается любое программное или программно-аппаратное решение, обеспечивающее ведение журнала регистрации событий [7]. В рамках исследования проанализированы следующие типы источников в соответствии с категориями, установленными приказом № 130 [5].

1. Источники событий операционных систем – регистрируют запуск/остановку системы и процессов, аутентификацию пользователей, изменение конфигурации. В операционных системах семейства Windows настройка аудита осуществляется с помощью групповых политик, что позволяет

детально определять перечень регистрируемых событий в журналах безопасности, приложений и системы [8]. В операционных системах семейства Linux центральным механизмом аудита является подсистема auditd, обеспечивающая регистрацию системных вызовов, доступа к файлам, изменений конфигурации и действий пользователей [9]. Правила аудита задаются в конфигурационных файлах /etc/audit/audit.rules и могут быть настроены для отслеживания таких событий, как запуск процессов (execve), доступ к защищаемым файлам, неудачные попытки аутентификации и модификация системных настроек.

2. Источники событий систем управления базами данных – обеспечивают регистрацию действий администраторов, команд манипуляции данными, событий авторизации. Большинство современных СУБД (как коммерческих, так и с открытым исходным кодом) предоставляют встроенные механизмы аудита. Регистрация событий может включать успешные и неуспешные попытки входа, выполнение операторов DDL (CREATE, ALTER, DROP), DML (INSERT, UPDATE, DELETE), а также изменения прав доступа (GRANT, REVOKE). Журналы аудита обычно хранятся в собственных форматах или могут направляться в системный журнал (syslog). Для централизованного сбора требуется настройка расширенного аудита, включая включение соответствующих политик и использование коннекторов для нормализации данных.

3. Источники событий телекоммуникационного оборудования – фиксируют изменения топологии, ошибки передачи данных, сетевые соединения. К ним относятся маршрутизаторы, коммутаторы, межсетевые экраны. Основным протоколом для передачи событий является Syslog, поддерживаемый подавляющим большинством устройств. Регистрируемые события включают изменение конфигурации, включение/отключение интерфейсов, ошибки протоколов маршрутизации, а также (для межсетевых экранов) разрешенные и заблокированные соединения с указанием IP-адресов, портов и протоколов. Для сбора информации о потоках трафика также используются протоколы NetFlow, sFlow и IPFIX. Особенностью является высокая интенсивность потока событий и необходимость фильтрации для снижения нагрузки на систему сбора.

4. Источники событий прикладного программного обеспечения – включают серверные и клиентские приложения, генерирующие события аутентификации, доступа к данным, изменения конфигурации. Типичными представителями являются веб-серверы (регистрируют HTTP-запросы, ошибки, попытки несанкционированного доступа), почтовые серверы (фиксируют отправку, получение, аутентификацию), системы электронного документооборота. Форматы логирования значительно варьируются – от стандартизированных (например, Combined Log Format для веб-серверов) до проприетарных. Это требует нормализации данных при централизованном сборе для приведения к единому формату, что является одной из ключевых задач SIEM-систем [3].

5. Источники событий средств защиты информации – антивирусные комплексы, системы обнаружения и предотвращения вторжений (IDS/IPS), средства защиты от несанкционированного доступа. Эти системы генерируют события, связанные с обнаружением вредоносного ПО, срабатыванием сигнатур атак, изменениями в политиках безопасности. Форматы журналов также разнообразны (многие используют Syslog или собственные форматы). Важной особенностью является необходимость корреляции событий от СЗИ с событиями от других источников для выявления сложных многоэтапных атак. Использование модели MITRE ATT&CK позволяет систематизировать события от различных СЗИ в соответствии с этапами атаки [6].

Важной характеристикой источников является максимальный набор событий, которые могут быть зарегистрированы. В работе [7] предложен подход к определению подмножества регистрируемых событий на основе анализа правил корреляции, что позволяет минимизировать ресурсные затраты при сохранении необходимого уровня обнаружения инцидентов.

Классификация средств анализа событий ИБ. Средства анализа событий ИБ можно разделить на следующие классы.

1. SIEM-системы (Security Information and Event Management) – централизованные платформы для сбора, нормализации, корреляции и хранения событий, а также управления инцидентами. Как отмечается в исследованиях, SIEM обеспечивает интеграцию управления информацией о безопасности (SIM) и управления событиями безопасности (SEM), предоставляя организациям целостное представление о состоянии защищенности [10].

2. Системы управления логами (Log Management) – обеспечивают сбор, хранение и поиск по журналам событий, но не содержат развитых механизмов корреляции (например, Elastic Stack, Graylog).

3. Системы анализа сетевого трафика (NTA/NDR) – анализируют сетевые потоки и полные захваты пакетов для выявления аномалий и атак (Zeek, RITA).

4. Платформы поведенческого анализа (UEBA) – используют методы машинного обучения для выявления аномального поведения пользователей и сущностей.

5. SOAR-платформы – обеспечивают автоматизированное реагирование на инциденты, включая анализ событий и выполнение сценариев.

Методы корреляции событий ИБ. Корреляция событий является ключевым механизмом интегрированного анализа. Согласно исследованиям, методы корреляции классифицируются на следующие типы [11].

1. Правила на основе порогов и временных окон – срабатывают при достижении заданного количества событий определенного типа в установленном временном интервале.
2. Последовательная корреляция – выявляет заданную последовательность событий (например, «неудачный вход» → «успешный вход»).
3. Корреляция на основе топологии – учитывает зависимости между компонентами инфраструктуры.
4. Корреляция на основе машинного обучения – использует алгоритмы для автоматического выявления сложных паттернов [12].

Современные подходы к корреляции событий все чаще используют методы машинного обучения. В работе [13] предложена архитектура на основе ансамбля глубоких нейронных сетей (LSTM, CNN, BRNN) с механизмами внимания для выявления временных и контекстных паттернов в данных безопасности, а также нечеткая логика для приоритизации оповещений.

Критерии выбора средств анализа с учетом их взаимодействия. Выбор средств анализа событий не сводится к оценке каждого класса изолированно. В современных системах обеспечения информационной безопасности различные средства функционируют как взаимосвязанный комплекс, где SIEM выступает центральным узлом сбора и корреляции, NTA/NDR предоставляет данные о сетевой активности, UEBA обогащает контекст поведенческими аномалиями, а SOAR автоматизирует реагирование. Поэтому критерии выбора должны учитывать не только индивидуальные характеристики, но и способность к интеграции.

Общие критерии выбора следующие.

1. Соответствие функциональным требованиям – необходимость централизованного сбора, нормализации, корреляции, хранения, визуализации и автоматизированного реагирования.
2. Производительность и масштабируемость – способность обрабатывать ожидаемый объем событий в секунду (EPS) и масштабироваться при росте инфраструктуры.
3. Поддержка источников – наличие коннекторов для существующих типов СЗИ, сетевого оборудования, операционных систем и прикладного ПО.
4. Соответствие регуляторным требованиям – возможность регистрации событий в соответствии с обязательными перечнями и форматами (например, приказ № 130) [5].
5. Гибкость настройки – возможность создания пользовательских правил корреляции, настройки дашбордов.
6. Безопасность – наличие ролевой модели доступа, шифрования данных, возможность работы в изолированных средах.
7. Стоимость владения – включая лицензирование, внедрение, поддержку и требуемые вычислительные ресурсы.

Критерии, обеспечивающие взаимодействие средств следующие.

1. Единый формат обмена данными – поддержка стандартизированных форматов (Syslog, CEF, LEEF, STIX/TAXII) позволяет безболезненно интегрировать разнородные системы. Наличие встроенных коннекторов или возможности кастомизации приема событий снижает затраты на интеграцию.
2. Наличие программных интерфейсов (API) – открытость REST API, GraphQL или других интерфейсов необходима для двустороннего обмена данными, автоматизации настройки и извлечения информации. SIEM должен предоставлять API для выгрузки оповещений в SOAR, а SOAR – API для запроса статуса задач.
3. Совместимость с моделью данных – способность средств анализировать и обогащать события в рамках единой контекстной модели (например, привязка к единому каталогу активов, пользователей, идентификаторов). Особенно важно для совместной работы UEBA и SIEM.
4. Возможность централизованного управления и оркестрации – наличие единой панели управления или возможность передачи управляющих команд между системами (например, SIEM → SOAR → межсетевой экран). SOAR должен уметь автоматически блокировать угрозы на основе оповещений SIEM.
5. Единая политика хранения и жизненного цикла данных – согласование сроков хранения событий, ротации и архивации между системами для обеспечения целостности расследований.
6. Встроенные или сертифицированные интеграции – наличие предварительно настроенных связок между конкретными продуктами разных классов снижает риски и ускоряет внедрение.

Специфические критерии для отдельных классов с учетом взаимодействия:

7. SIEM: кроме собственных возможностей корреляции, важна возможность передачи обогащенных событий в SOAR (через API или webhooks), а также приема результатов поведенческого анализа от UEBA.

8. SOAR: ключевыми являются наличие готовых плейбуков для реагирования на типовые оповещения SIEM, поддержка двусторонней синхронизации инцидентов с SIEM и возможность управления сетевым оборудованием/СЗИ.

9. NTA/NDR: должна поддерживать экспорт детектируемых событий в SIEM в стандартном формате (Syslog, CEF) и предоставлять API для запроса детальной информации о соединениях.

10. EBA: должна уметь передавать аномалии и скоринговые оценки в SIEM, обогащая контекст инцидента.

11. Log Management: должна обеспечивать быстрый доступ к сырым логам для углубленного расследования по запросу из SIEM или SOAR.

Таким образом, выбор средств анализа событий должен осуществляться как выбор экосистемы, в которой каждый компонент выполняет свою функцию, а интеграционные механизмы обеспечивают бесшовную передачу данных и автоматизацию процессов обнаружения и реагирования.

В результате проведенного обзора определены основные направления разработки усовершенствованной методики интегрированного анализа событий информационной безопасности. Выполнены три поставленные задачи исследования.

1. Классификация событий ИБ. На основе анализа нормативных правовых актов Республики Беларусь выделены пять категорий событий. Предложена трехуровневая гибридная модель классификации, включающая технический, тактический и стратегический уровни.

2. Анализ характеристик источников событий ИБ. Проведен анализ пяти типов источников событий с учетом требований приказа № 130, определены особенности регистрации событий для каждого типа: для операционных систем (Windows – групповые политики, Linux – auditd), для СУБД – встроенные механизмы аудита, для телекоммуникационного оборудования – Syslog, NetFlow, для прикладного ПО – разнообразие форматов, для СЗИ – сигнатурные и поведенческие события.

3. Оценка характеристик средств анализа событий ИБ. Проанализированы функциональные возможности основных классов средств анализа (SIEM, Log Management, NTA/NDR, UEBA, SOAR), рассмотрены методы корреляции (правила, временные окна, топология, машинное обучение), сформулированы общие и специфические критерии выбора платформ с акцентом на их взаимодействие.

Полученные результаты являются основой для выполнения следующих этапов работы: обоснование средств для реализации методики, разработка порядка конфигурирования средств, апробация методики в тестовой среде.

Список использованных источников:

1. О Концепции информационной безопасности Республики Беларусь : постановление Совета Безопасности Респ. Беларусь от 18 марта 2019 г., № 1 // ЭТАЛОН : информ.-поисковая система (дата обращения 23.03.2026).

2. Модель взаимодействия компьютерных инцидентов, событий и инцидентов информационной безопасности // Научно-аналитический журнал Санкт-Петербургского университета ГПС МЧС России. – 2025. – № 2. – С. 91–101.

3. Как управление событиями (SIEM) структурирует хаос и упрощает работу ИБ-специалиста [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/How-SIEM-Makes-Work-Easier (дата обращения: 12.03.2026).

4. СТБ ISO/IEC 27000–2024. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь. – Введ. 01.10.2024. – Минск : Госстандарт : Бел. гос. ин-т стандартизации и сертификации, 2024. – 56 с.

5. О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40 : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 25 июля 2023 г. № 130 // Оперативно-аналитический центр при Президенте Республики Беларусь. – URL: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf (дата обращения 23.03.2026).

6. Козлов, А.А. Методология применения матрицы MITRE ATT&CK для оценки эффективности систем мониторинга событий / А.А. Козлов, В.А. Смирнов // Вопросы кибербезопасности. – 2024. – № 5. – С. 28–36.

7. Кузнецов, А.В. Способ определения регистрируемых событий / А.В. Кузнецов, С.М. Ненашев // Вопросы кибербезопасности. – 2024. – № 3. – С. 45–52.

8. Смотрук, Г.С. Настройка аудита безопасности в операционных системах семейства Windows / Г.С. Смотрук // Информационная безопасность : сборник материалов 60-й научной конференции аспирантов, магистрантов и студентов БГУИР. – Минск : БГУИР, 2024. – С. 92–96.

9. Audit – ROSA Wiki [Электронный ресурс]. – Режим доступа: https://wiki.rosa.ru/index.php/Audit (дата обращения: 23.03.2026).

10. Федорченко, А.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 / А.В. Федорченко, Д.С. Левшун, А.А. Чечулин, И.В. Котенко // Труды СПИИРАН. – 2016. – № 6(49). – С. 208–225.

11. Wang, Y. Advanced Techniques for Alert Management in Security Information and Event Management Systems With Ensembled Deep Learning, Hybrid Optimization, and Multi-Feature Extraction / Y. Wang, L. Zhang, H. Li [Электронный ресурс] // IEEE Xplore. – 2025. – Режим доступа: https://ieeexplore.ieee.org/document/11142305 (дата обращения: 23.03.2026).

12. Cloud Security Alliance. AI Log Analysis for Event Correlation in Zero Trust [Электронный ресурс]. – Режим доступа: https://cloudsecurityalliance.org/blog/2025/09/26/ai-log-analysis-for-event-correlation-in-zero-trust (дата обращения: 23.03.2026).

UDC 004.056

INTEGRATED ANALYSIS METHODOLOGY FOR INFORMATION SECURITY EVENTS IN INFORMATION SYSTEMS

Stashkevich S.O., master's student gr. 567241

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Boiprav O.V. – PhD in Technical Sciences, Associate Professor, Head of the Information Security Department

Annotation. The article presents a review of approaches to the development of an integrated methodology for the analysis of information security events. Based on the analysis of regulatory legal acts of the Republic of Belarus, the classification of information security events is carried out, the characteristics of event sources are determined, and modern event analysis tools are evaluated. A three-level hybrid classification model is proposed, including technical, tactical and strategic levels. The obtained results form the basis for further development of the methodology.

Keywords. information security events, SIEM systems, event correlation, incident management, event classification, MITRE ATT&CK