www.volsu.ru

CC BY

DOI: https://doi.org/10.15688/NBIT.jvolsu.2025.3.3

УДК 004.056
ББК 16.8

РОЛЬ ЖУРНАЛОВ СОБЫТИЙ В ВЫЯВЛЕНИИ И РАССЛЕДОВАНИИ ИНЦИДЕНТОВ

Александр Валерьевич Лощилин

Студент, физико-технический институт,
Волгоградский государственный университет
IBm-241_889371@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Владислав Георгиевич Яриков

Кандидат педагогических наук,
доцент, кафедра компьютерной безопасности
Волгоградского государственного университета
yarikov.vladislav@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье рассматривается роль журналов событий в процессе выявления и расследования компьютерных инцидентов. Проанализированы основные виды логов, их особенности, преимущества и ограничения. Особое внимание уделено связи журналов событий с этапами модели MITRE ATT&CK, что позволяет определить их значимость на различных стадиях кибератаки. Рассмотрены практические методы работы с логами. Приведен обзор современных инструментов, применяемых для анализа и обработки журналов событий.

Ключевые слова: журналы событий, логирование, расследование инцидентов, SIEM, MITRE ATT&CK, информационная безопасность.

В 2025 г. кибератаки на российский бизнес приобрели новые масштабы и методы – атак с целью разведки и сбора информации, направленных на выявление уязвимостей, стало производиться все чаще. По данным компании Bi.Zone [6], доля атак с целью сбора данных выросла более чем в 5 раз, до почти 39 % от числа вредоносных запросов к веб-приложениям. Также за первые четыре месяца текущего года российские компании зафиксировали порядка 198 миллионов кибератак – что демонстрирует троекратный рост по сравнению с аналогичным периодом прошлого года [1]. Самыми популярными видами атак стали: фишинг, тайпсквоттинг, и атаки с использованием DNS-протокола, в том числе через домены с перенаправлением, которые сложно обнаружить классическими защитными средствами [7].

В таких условиях журналирование событий (логирование) становится не просто желательным, а критически важным компонентом системы безопасности. Системные, сетевые и прикладные логи выполняют роль «черного ящика» – они фиксируют, регистрируют и позволяют восстановить хронологию действий злоумышленников, выявить исходную точку проникновения, понять, какие

© Лощилин А.В., Яриков В.Г., 2025

объекты были повреждены или скомпрометированы, и как распространялась угроза.

Цель этой статьи – проанализировать, какую роль играют разные виды журналов событий при выявлении и расследовании инцидентов, какие трудности связаны с их сбором и анализом, и какие практические методы и инструменты позволяют максимально эффективно использовать лог-данные в борьбе с современными атаками.

Виды журналов событий

Журналы событий можно разделить на несколько ключевых категорий, каждая из которых отражает определенный уровень функционирования системы и имеет значение для расследования компьютерных инцидентов.

Системные журналы содержат сведения о работе операционной системы и ее компонентов. В них фиксируются события ядра, запуск и остановка служб, ошибки драйверов, установка обновлений, действия пользователей и попытки авторизации [3]. Основной сложностью работы с системными журналами является их объем, а также вероятность отсутствия нужных записей в случае неправильной настройки логирования.

Сетевые журналы формируются средствами сетевой инфраструктуры: межсетевыми экранами, IDS/IPS, маршрутизаторами, прокси-серверами. Они фиксируют источники и назначения подключений, порты и протоколы, блокировки и подозрительные соединения, а также аномалии в сетевом трафике. Анализ таких журналов позволяет обнаружить сканирование сети, коммуникации с управляющими серверами (C2), попытки проведения DDoS-атак [4]. Однако объем сетевых логов зачастую огромен, а наличие шифрованного трафика осложняет детальный анализ. Кроме того, данные разных производителей устройств имеют различный формат, что требует применения систем корреляции и нормализации.

Прикладные журналы отражают работу отдельных приложений: веб-серверов, баз данных, почтовых серверов и бизнес-систем. В них фиксируются ошибки, запросы, результаты аутентификации, API-вызовы. Эти данные особенно ценны для выявления специфических атак, направленных именно на уровень приложений: SQL-инъекций, XSS, перебора паролей [3]. Ограничением является то, что многие приложения изначально не ведут достаточного объема журналирования, а форматы данных разрознены и зависят от конкретного ПО.

Журналы безопасности и аудита представляют собой специализированные логи, предназначенные для фиксации действий, затрагивающих политики доступа и параметры защиты. В них можно найти записи о попытках изменения прав пользователей, отключения защитных механизмов, запуске подозрительных команд и скриптов [3]. Их ключевая ценность – фиксация поведенческих аномалий, а не только технических ошибок. В то же время, для эффективности требуется грамотная настройка аудита.

Особое значение имеют *журналы инфраструктурных устройств*: маршрутизаторов, VPN-шлюзов, коммутаторов, оборудования в DMZ-зонах [4]. Эти данные помогают отследить перемещение злоумышленника внутри корпоративной сети, выявить несанкционированные подключения, изменения конфигурации устройств. Однако централизовать сбор таких логов сложно: у разных вендоров применяются разные форматы, а объем памяти на устройствах часто ограничен, что приводит к быстрой потере записей.

Таблица 1 демонстрирует, что каждый тип журналов событий фиксирует отдельный аспект работы информационной системы. Системные логи показывают внутреннюю жизнь операционной среды, сетевые – картину трафика и подключений, прикладные – активность пользователей и атакующих в бизнес-сервисах, журналы безопасности – действия, связанные с обходом политик, а инфраструктурные – состояние и изменения на уровне сетевого периметра [2]. Их совместный анализ позволяет собрать разрозненные артефакты в единую картину атаки и понять, как именно развивался инцидент. Важно понимать, что разные типы логов помогают выявлять различные этапы проникновения и развития инцидента. Для этого можно воспользоваться моделью MITRE ATT&CK.

Модель *MITRE ATT&CK* описывает тактики и техники злоумышленников на разных стадиях кибератаки [5]. Соотнесение техник

злоумышленников с соответствующими логами обеспечивает журналирование всех фаз атаки по системам и сети.

Согласно данным таблицы 2, каждый вид логов имеет свою «зону ответственности» в рамках MITRE ATT&CK. Системные журналы наиболее полезны для выявления локальных действий злоумышленника на уровне ОС, сетевые – для обнаружения коммуникаций и перемещений, прикладные – для фиксации атак на сервисы и базы данных, а журналы безопасности и инфраструктурные – для анализа действий по обходу защитных механизмов и контроля сети.

Таблица 1

Виды журналов событий и их характеристика

Вид журнала	Фиксируемая информация	Пример артефактов	Трудности и особенности
Системные журналы (Operating System Logs)	События ядра ОС, сервисов, драйверов; информация об авторизации, запуск / остановка служб, ошибки ОС, установка патчей, процессы, привилегии	Windows Event Logs (Security, System, Application), Linux syslog, auditd. Как злоумышленник получил доступ, какие процессы запускал, как поднял уровень привилегий	Большой объем; отсутствие нужных записей, если ОС / службы неправильно настроены; возможна фильтрация / удаление логов злоумышленником. Временные метки могут быть не синхронизированы; форматы разных ОС различаются
Сетевые журналы (Network Logs)	Сетевые соединения, источники и назначения, порты и протоколы, трафик на межсетевых экранах, маршрутизаторах, IDS/IPS, журналы сетевых устройств, логи прокси	Можно обнаружить необычные соединения с внешних IP, попытки сканирования, коммуникации с C2 (command & control), DDoS-активность	Большой объем данных; часто шифрованный трафик, что усложняет анализ; нужда в агрегаторах и фильтрации; сбор логов сетевых устройств может быть сложным из-за специфики производителя
Прикладные (Application) журналы	События, свойственные приложениям: запросы к веб-серверу, аутентификация в приложении, ошибки, бизнес-операции, логи баз данных, API-вызовы	Веб-сервера (Apache, Nginx): логи ошибок и запросов, приложения: логирование попыток SQL-инъекций, отклоненных запросов, неудачных логинов, неожиданных исключений	Часто приложения по умолчанию не логируют все, что нужно; отсутствие единого формата, разнообразие языков, фреймворков; может быть много «шума», сложно отделить полезное
Журналы безопасности / аудита (Security / Audit Logs)	Специализированные логи, предназначенные для фиксирования действий, связанных с политиками безопасности: изменения прав, попытки доступа, отключение защитных механизмов, подозрительные команды и т. д.	Правила корреляции по событиям, связанным с попытками подбора пароля, запуском команд вроде systeminfo / whoami, выполнением скриптов. Эти события часто идут из разделов ОС Security, auditd, модулей безопасности приложений	Требуют тонкой настройки, чтобы не порождать слишком много ложных срабатываний; нужны четкие политики аудита; возможна утечка через отсутствие шифрования или слабых прав доступа
Журналы инфраструктурных / сетевых устройств и периметра	Это логи роутеров, свичей, межсетевых экранов, VPN шлюзов, DMZ-зон, проксей; может включать логи физического доступа, панелей управления, устройств сетевого мониторинга	Полезны, чтобы установить точки входа, пути передвижения злоумышленника по сети, зафиксировать внешние подключение или подключение через VPN, маршрутизация, изменения конфигураций устройств	Сложно централизовать; разные форматы, производители; оборудование может не поддерживать нужный уровень детализации; возможны ограничения по памяти / ресурсам на устройствах

Эффективное расследование компьютерных инцидентов невозможно без применения системного подхода к работе с журналами событий. Практика показывает, что ценность логов проявляется не только в их хранении, но и в умении правильно организовать сбор, анализ и корреляцию данных. Ключевые методы работы с логами представлены на рисунке.

Централизованный сбор и хранение – все логи должны собираться в единую систе-

Таблица 2

Соответствие MITRE ATT&CK и журналов событий

Стадия атаки (MITRE ATT&CK)	Основные индикаторы	Полезные журналы событий
Initial Access (первоначальный доступ)	Попытки входа, SQL-инъекции, XSS, массовые запросы	Системные (аутентификация), Прикладные (веб-сервера, БД), Сетевые (необычные внешние подключения)
Execution (выполнение кода)	Запуск скриптов (PowerShell, bash), запуск новых процессов	Системные (процессы, команды), Журналы безопасности (отключение защитных механизмов)
Persistence (закрепление)	Изменения автозагрузки, служб, создание учетных записей	Системные (службы, задачи), Журналы безопасности и аудита
Privilege Escalation (эскалация привилегий)	Повышение прав, запуск системных утилит с ошибками доступа	Системные (попытки доступа), Журналы безопасности (изменение прав)
Defense Evasion (уклонение от защиты)	Отключение антивируса, остановка сервисов мониторинга, удаление логов	Журналы безопасности (изменения в защите), Системные (обрывы в логах)
Credential Access (доступ к учетным данным)	Множественные неудачные входы, дамп памяти	Системные (аутентификация), Прикладные (БД, почтовые сервисы)
Discovery (разведка)	Команды systeminfo, net user, сканирование сети	Системные (команды ОС), Сетевые (аномальная активность, сканирование)
Lateral Movement (горизонтальное перемещение)	Новые соединения RDP/SMB, повторные входы на хосты	Сетевые (VPN, RDP, SMB), Системные (входы с одних и тех же учетных данных)
Collection & Exfiltration (сбор и вынос данных)	Массовые выгрузки данных, рост исходящего трафика	Прикладные (БД, почта), Сетевые (увеличение внешнего трафика)
Command & Control (управление и контроль)	Регулярные соединения с C2, нестандартные порты, туннели	Сетевые (подозрительные IP, DNS/HTTPS-трафик)



Методы работы с журналами событий

му, что позволяет избежать их фрагментации и потерь. Также, использование протоколов Syslog, агента Windows Event Forwarding или специализированных коннекторов обеспечивает доставку данных с разных источников. Централизация снижает риск подмены журналов злоумышленником.

Нормализация и стандартизация форматов – журналы, поступающие от разных устройств и приложений, имеют различные форматы, поэтому приведение событий к единому виду (например, через Common Event Format – CEF или Log Event Extended Format – LEEF) упрощает анализ и корреляцию.

Фильтрация и выделение значимых событий – для исключения «шума» избыточных сообщений применяются правила фильтрации, настраиваются пороговые значения (например, количество неудачных попыток входа за определенный промежуток времени).

Корреляция событий – объединение информации из разных источников позволяет обнаружить сложные атаки. Например, совпадение системного события запуска скрипта, сетевого соединения с внешним адресом и ошибки в приложении может указывать на единый инцидент компрометации системы.

Анализ временных рядов – важным приемом является сопоставление событий по временным меткам, что помогает выстраивать полную хронологию атаки. Для этого требуется обязательная синхронизация времени (например, через NTP-сервера).

Для успешного использования методик по работе с логами данных необходимы соответствующие инструменты. Примерами таких инструментов для работы с журналами событий являются:

1. SIEM-системы (Splunk, IBM QRadar, ArcSight, ELK (Elasticsearch–Logstash–Kibana), LogRhythm): обеспечивают сбор, нормализацию, хранение и корреляцию логов, а также визуализацию событий и автоматическую генерацию оповещений.

2. Системы централизованного лог-менеджмента (Graylog, Fluentd, Wazuh, Rsyslog): используются для масштабного хранения и поиска по логам, позволяют быстро обрабатывать миллионы записей при расследовании.

3. EDR/XDR-платформы (Kaspersky, MaxPatrol, BI.Zone, R-Vision, CrowdStrike Falcon, Microsoft Defender for Endpoint): сфокусированы на анализе событий конечных устройств: процессы, сетевые соединения, активности пользователей.

4. Forensic-утилиты и средства анализа (Volatility, Autopsy, EnCase, FTK): позволяют использовать логи в совокупности с дампами памяти, образами дисков и другими цифровыми артефактами для углубленного расследования.

5. Threat Intelligence и OSINT-платформы (MISP, VirusTotal, Shodan, Maltego): интеграция с логами позволяет сопоставлять события с внешними индикаторами компрометации (IOC) и выявлять связь с известными кибергруппировками.

Современные тенденции в развитии киберугроз показывают, возрастающая сложность атак требует от организаций внедрения системного подхода к сбору, хранению и анализу журналов событий. Рассмотренные в статье виды журналов событий отражают разные уровни функционирования информационной системы. Их комплексное использование обеспечивает полноту картины при расследовании, а корреляция данных между ними позволяет обнаружить даже сложные многоэтапные атаки. Применение современных инструментов делает процесс анализа логов более точным и оперативным.

СПИСОК ЛИТЕРАТУРЫ

1. В 2025 году на российский бизнес приходится рекордное количество кибератак. – Электрон. текстовые дан. – Режим доступа: https://www.iksmedia.ru/news/6051271-V-2025-godu-na-rossijskij-biznes.html

2. Журналирование событий безопасности // Security Vision. – Электрон. текстовые дан. – Режим доступа: https://www.securityvision.ru/education/cyberwiki/zh-rus/zhurnalirovanie-sobytiy-bezopasnosti/

3. Инструменты и техники проведения эффективного анализа журналов событий безопасности // OTUS на Habr. – Электрон. текстовые дан. – Режим доступа: https://habr.com/ru/companies/otus/articles/854440/

4. Инструменты и техники проведения эффективного анализа журналов событий безопасности // CISO Club. – Электрон. текстовые дан. – Режим доступа: https://cisoclub.ru/instrumenty-i-tehniki-

provedenija-jeffektivnogo-analiza-zhurnalov-sobytij-bezopasnosti-2/

5. Расследование инцидентов информационной безопасности // Falcongaze. – Электрон. текстовые дан. – Режим доступа: https://falcongaze.com/ru/pressroom/publications/rassledovaniye-intsidentov-informatsionnoy-bezopasnosti.html

6. Хакеры в 2025 году стали в пять раз чаще атаковать российские компании. – Электрон. текстовые дан. – Режим доступа: https://www.cnews.ru/news/top/2025-08-12_hakery_v_2025_godu_stali_v_pyat

7. Число кибератак в России и в мире // TAdviser. – Электрон. текстовые дан. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире

REFERENCES

1. *V 2025 godu na rossiyskiy biznes prikhoditsya rekordnoe kolichestvo kiberatak* [A Record Number of Cyberattacks Accounted for Russian Business in 2025]. URL: https://www.iksmedia.ru/news/6051271-V-2025-godu-na-rossijskij-biznes.html

2. Zhurnalirovanie sobytiy bezopasnosti [Security Event Logging]. *Security Vision*. URL: https://www.securityvision.ru/education/cyberwiki/zh-rus/zhurnalirovanie-sobytiy-bezopasnosti/

3. Instrumenty i tekhniki provedeniya effektivnogo analiza zhurnalov sobytiy bezopasnosti [Tools and Techniques for Effective Security Event Log Analysis]. *OTUS na Habr* [OTUS on Habr]. URL: https://habr.com/ru/companies/otus/articles/854440/

4. Instrumenty i tekhniki provedeniya effektivnogo analiza zhurnalov sobytiy bezopasnosti [Tools and Techniques for Effective Security Event Log Analysis]. *CISO Club*. URL: https://cisoclub.ru/instrumenty-i-tehniki-provedenija-jeffektivnogo-analiza-zhurnalov-sobytij-bezopasnosti-2/

5. Rassledovanie intsidentov informatsionnoy bezopasnosti [Investigation of Information Security Incidents]. *Falcongaze*. URL: https://falcongaze.com/ru/pressroom/publications/rassledovaniye-intsidentov-informatsionnoy-bezopasnosti.html

6. Khakery v 2025 godu stali v pyat raz chashche atakovat rossiyskiye kompanii [Hackers Have Become Five Times More Likely to Attack Russian Companies in 2025]. URL: https://www.cnews.ru/news/top/2025-08-12_hakery_v_2025_godu_stali_v_pyat

7. Chislo kiberatak v Rossii i v mire [The Number of Cyberattacks in Russia and in the World]. *TAdviser*. URL: https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире

THE ROLE OF EVENT LOGS IN DETECTING AND INVESTIGATING INCIDENTS

Alexander V. Loshchilin

Student, Institute of Physics and Technology,
Volgograd State University
IBm-241_889371@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Vladislav G. Yarikov

Candidate of Sciences (Pedagogy),
Associate Professor, Department of Computer Security,
Volgograd State University
yarikov.vladislav@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. This article analyzes the critical role of event logs in the detection and investigation of computer security incidents. In the context of a significant increase in cyberattacks on Russian businesses in 2025, including reconnaissance and data collection attacks, systematic logging has become an essential security component. The study provides a detailed classification of main log types: system, network, application, security/audit, and infrastructure device logs. Each category is examined in terms of recorded information,

practical artifacts for investigations, and inherent challenges related to volume, format diversity, and collection complexities. A central focus is establishing the correlation between different event log types and various stages of a cyberattack as outlined in the MITRE ATT&CK framework. The analysis demonstrates how specific logs provide crucial indicators for tactics such as initial access, execution, lateral movement, and data exfiltration, enabling a comprehensive reconstruction of attack timelines. The article further reviews practical methodologies for effective log management, including centralized collection, normalization, filtration, correlation, and time-series analysis. Finally, the work presents an overview of modern tools that facilitate log analysis, such as SIEM systems (Splunk, ELK stack), centralized log management platforms (Graylog), EDR/XDR solutions, forensic utilities, and threat intelligence platforms. The conclusion emphasizes that a holistic approach integrating diverse log sources with advanced analytical tools is fundamental for effectively combating evolving cyber threats and conducting thorough incident investigations.

Key words: event logs, logging, investigating incidents, SIEM, MITRE ATT&CK, information security.