

СПИСОК ЛИТЕРАТУРЫ

- 1 **Котлер, Ф.** Маркетинг менеджмент. Экспресс-курс / Ф. Котлер. – 2-е изд. – СПб. : Питер, 2011. – 464 с.
- 2 **Портер, М. Э.** Конкуренция : пер. с англ. / М. Э. Портер. – М. : Вильямс, 2013. – 608 с.
- 3 **Савельева, Н. А.** Управление конкурентоспособностью организации / Н. А. Савельева. – М. : Феникс, 2011. – 382 с.
- 4 **Кныш, М. И.** Конкурентные стратегии : учеб. пособие / М. И. Кныш. – СПб. : Питер, 2010. – 284 с.

Получено 02.06.2026

ISSN 2227-1155. Сборник студенческих научных работ.
Вып. 31. Гомель, 2026

УДК 004.056.5

И. В. ЗАГОРЦЕВ (ЭМ-31)

Научные руководители: старшие преподаватели *В. Е. МИНИН,*
С. В. КИСЕЛЕВА

АНАЛИЗ СИСТЕМНЫХ ЖУРНАЛОВ ОПЕРАЦИОННЫХ СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ

Рассмотрены методология и практика анализа системных журналов операционных систем Windows и Linux в контексте обеспечения информационной безопасности. Описаны уровни приоритета событий, инструменты расширенного журналирования Sysmon и Auditd, а также их конфигурирование для выявления подозрительной активности: несанкционированного доступа, изменений реестра, создания файлов в директориях автозагрузки и нетипичных сетевых соединений.

Системные журналы (логи) представляют собой хронологическую запись событий, происходящих в операционной системе (ОС): аутентификаций, запусков процессов, сетевых соединений, изменений конфигурации и возникших ошибок [1]. В условиях постоянно усложняющегося ландшафта киберугроз анализ журналов является одним из ключевых методов обнаружения вторжений и расследования инцидентов информационной безопасности.

Характерный индикатор компрометации в журналах – серия неудачных попыток аутентификации, сменяющаяся успешным входом. Подобный паттерн типичен для атак методом перебора паролей. Своевременное обнаружение таких последовательностей позволяет реагировать на инцидент на ранних стадиях, до нанесения существенного ущерба.

Пример лога аутентификации по SSH:

May 1 10:15:22 server sshd[1234]: Failed password for invalid user admin

from 192.168.1.10 port 54321 ssh2

May 1 10:15:27 server sshd[1235]: Failed password for user admin from 192.168.1.15 port 45678 ssh2

May 1 10:15:32 server sshd[1236]: Failed password for user admin from 192.168.1.15 port 45678 ssh2

May 1 10:15:37 server sshd[1237]: Failed password for user admin from 192.168.1.15 port 45678 ssh2

May 1 10:15:42 server sshd[1238]: Failed password for user admin from 192.168.1.15 port 45678 ssh2

May 1 10:15:47 server sshd[1239]: Accepted password for user admin from 192.168.1.15 port 45678 ssh2

По содержательному признаку журналы разделяются на несколько категорий. Журналы аутентификации фиксируют факты входа и выхода пользователей, успешные и неудачные попытки. Журналы приложений отражают события конкретных программ и служб. Системные журналы содержат сведения об аппаратных и программных событиях ОС. Журналы безопасности регистрируют аудит действий пользователей и политик доступа.

По критичности события классифицируются в соответствии с принятой в индустрии схемой приоритетов. Таблица 1 отражает уровни логирования и их назначение.

Практическая ценность уровней логирования определяется возможностью фильтрации. При мониторинге безопасности приоритет отдается уровням warning, error и fatal, тогда как debug и info используются преимущественно при диагностике.

Таблица 1 – Уровни логирования и их назначение

Уровень	Назначение
debug	Запись переходных состояний: запуск/остановка сервера, запросы к БД, верификация
info	Общие события штатной работы сервиса
warning	Экстренные ситуации, некорректные запросы, проблемы, не прерывающие работу
error	Основные ошибки, нарушающие функциональность
fatal/critical	Критические ошибки, требующие немедленного вмешательства

Sysmon (System Monitor) – компонент Sysinternals Suite, расширяющий штатные возможности журналирования Windows [2]. После установки в системе появляется новый журнал событий Microsoft-Windows-Sysmon/Operational, разделенный на 18 категорий задач: Process Create, Network Connect, Driver Load, ProcessAccess, File Create и др.

Принципиальным преимуществом Sysmon является гибкая система конфигурирования на основе XML-файла. Применение конфигурации выполняется командой sysmon -с путь_к_файлу\config.xml

Изменения вступают в силу немедленно после успешной загрузки конфигурации без перезагрузки системы. Конфигурация позволяет задавать правила включения и исключения для каждой категории событий, что существенно снижает объем нерелевантных записей.

Среди практически значимых возможностей Sysmon следует выделить:

- регистрацию создания файлов в директориях автозагрузки (индикатор закрепления вредоносного ПО);

- вычисление и запись контрольных сумм MD5 и SHA256 для всех запускаемых процессов (позволяет верифицировать исполняемые файлы через VirusTotal);

- журналирование изменений ключей реестра с указанием инициатора;

- запись сетевых соединений, инициируемых процессами, отличными от браузеров.

Auditd (Linux Audit Daemon) – нативная подсистема аудита ядра Linux, разрабатываемая компанией Red Hat [3]. В отличие от Sysmon, Auditd интегрирован непосредственно в ядро ОС, что обеспечивает перехват системных вызовов на самом низком уровне и существенно затрудняет его обход вредоносным программным обеспечением.

Управление осуществляется набором утилит:

- auditctl – управление системой аудита и добавление правил;

- autrace – аудит системных вызовов конкретного процесса;

- ausearch – поиск событий в журналах по заданным критериям;

- aureport – формирование аналитических отчетов.

Конфигурирование Auditd производится путем создания правил наблюдения. Правило для мониторинга файловой системы в формате auditctl:

```
auditctl -w /путь/к/директории -p rwx -k метка_события
```

Параметр -w задает наблюдаемый путь, -p rwx определяет типы отслеживаемых операций (чтение, запись, выполнение, изменение атрибутов), -k присваивает событию метку для последующего поиска через ausearch.

Системные журналы являются незаменимым источником информации при расследовании инцидентов информационной безопасности.

Пример журнала Безопасность представлен на рисунке 1.

Рисунок 1 – Журнал Безопасность

Инструменты Sysmon и Auditd существенно расширяют стандартные

возможности журналирования Windows и Linux соответственно, обеспечивая детализированную регистрацию событий, критичных для обнаружения атак. Практическое использование описанных инструментов в комплексе с системами SIEM позволяет автоматизировать выявление подозрительных паттернов и значительно сократить время реагирования на инциденты.

СПИСОК ЛИТЕРАТУРЫ

1 **Chuvakin, A.** Logging and Log Management: The Authoritative Guide / A. Chuvakin, K. Schmidt, C. Phillips. – Syngress, 2012. – 460 p.

2 **Russinovich, M.** Sysinternals Suite Documentation: Sysmon / M. Russinovich. – Microsoft Learn. – URL: <https://learn.microsoft.com/sysinternals/downloads/sysmon> (date of access: 03.04.2026).

3 Red Hat Enterprise Linux Security Guide: System // Red Hat Inc. – URL: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/ (date of access: 05.04.2026).

4 **Sanders, C.** Applied Network Security Monitoring: Collection, Detection, and Analysis / C. Sanders, J. Smith. – Syngress, 2014. – 496 p.

Получено 11.06.2026

ISSN 2227-1155. Сборник студенческих научных работ.
Вып. 31. Гомель, 2026

УДК 004.056.5

И. В. ЗАГОРЦЕВ (ЭМ-31)

Научный руководитель – ст. пр. *В. Е. МИНИН*

УЧЕБНЫЙ СТЕНД ПО ИЗУЧЕНИЮ УЯЗВИМОСТЕЙ WEB-ПРИЛОЖЕНИЙ

Рассмотрены методология и практика тестирования безопасности web-приложений на основе специализированной учебной платформы OWASP Juice Shop. На реальных сценариях атак проанализированы типичные уязвимости: межсайтовое выполнение скриптов (XSS), SQL-инъекции, атаки на JWT-токены, нарушения контроля доступа (Broken Access Control). Для каждого класса угроз представлены конкретные векторы эксплуатации с входными данными и ожидаемыми результатами.

Подготовка специалистов в области информационной безопасности требует практических навыков работы с реальными уязвимостями в контролируемой среде. OWASP Juice Shop – намеренно уязвимое web-приложение, представляющее собой полнофункциональный интернет-магазин, – является де-факто стандартом для обучения пентесту [1]. Все уязвимости класси-