УДК 004.056:004.415

Мавлеткулов Александр Вячеславович, магистрант,
Амурский государственный университет

Галаган Татьяна Алексеевна,
канд. техн. наук, доцент,
Амурский государственный университет

АРХИТЕКТУРА ПРОТОТИПА SIEM-СИСТЕМЫ ДЛЯ ИНФРАСТРУКТУРЫ ГОСУДАРСТВЕННОГО ОРГАНА

Аннотация. Рассмотрена задача централизованного мониторинга событий информационной безопасности в инфраструктуре государственного органа. Предложен исследовательский прототип SIEM-системы на стеке РЕД ОС, PostgreSQL, Python и FastAPI. Приведены сравнение операционных сред, выбранный технологический стек и границы стендовой реализации.

Ключевые слова: Информационная безопасность, SIEM-система, мониторинг событий, РЕД ОС, PostgreSQL, FastAPI.

В инфраструктуре государственного органа журналы событий распределены между рабочими станциями, серверами, сетевым оборудованием и средствами защиты информации. При разборе инцидента администратор собирает записи вручную и сопоставляет временные метки. Рост числа событий и различие форматов журналов затрудняют выделение повторяющихся ошибок авторизации, нетипичной сетевой активности и сбоев сервисов [5]. Для государственных организаций задача осложняется переходным периодом в выборе средств мониторинга и высокой стоимостью промышленных SIEM-систем [1, 2].

Цель работы – исследовательский прототип SIEM-системы для локальной вычислительной сети государственного органа. Прототип не заменяет промышленную платформу и не выполняет функции центра мониторинга безопасности: рассматриваются ограниченный набор источников и базовый набор правил. Цепочка обработки едина. Событие передаётся в систему, приводится к общему формату, сохраняется, анализируется по правилам и предъявляется оператору. Источники не изменяются: используются журналы, которые компоненты инфраструктуры уже формируют.

К прототипу предъявлены требования централизованного сбора, нормализации разнородных записей, хранения событий в течение заданного периода, анализа типовых ситуаций и интерфейса с поиском и фильтрацией [4]. Отдельно предусмотрено базовое разграничение доступа. Анализ в этой версии ограничен правилами порогового типа, правилами по ключевым словам и простыми комбинациями условий.

Программные средства сопоставлены по четырём зонам: среда исполнения, хранение, серверная логика и сбор событий. Критериями приняты импортонезависимость, совместимость с инфраструктурой, достаточность для стенда и сложность сопровождения. Сравнение операционных систем приведено в таблице 1. Для прототипа принята РЕД ОС. Для хранения выбрана PostgreSQL, для ядра – Python и FastAPI, для сбора – собственный модуль на Python. Промышленные системы, в том числе MaxPatrol SIEM, решают близкие задачи, но не используются как основа открытого исследовательского стенда [3].

Таблица 1

Сравнение операционных систем для прототипа SIEM-системы

Операционная система	Преимущества	Ограничения
Astra Linux Сервер	высокий уровень защищённости; широкое применение в госсекторе; развитые механизмы ИБ	более высокие требования к квалификации администрирования; более высокий «порог входа» при настройке
РЕД ОС Сервер	сбалансированность серверного применения; удобство сопровождения; стабильная серверная среда	набор возможностей зависит от редакции и канала поставки
Альт Сервер	гибкость настройки; отечественная разработка	возможна вариативность совместимости оборудования и пакетной базы в конкретных конфигурациях

Состав выбранного стека и направление потока данных показаны на рисунке 1. Среда исполнения – РЕД ОС. Сбор выполняет собственный модуль на Python, обработку и API – FastAPI, хранение – PostgreSQL, результат видит оператор в интерфейсе мониторинга.

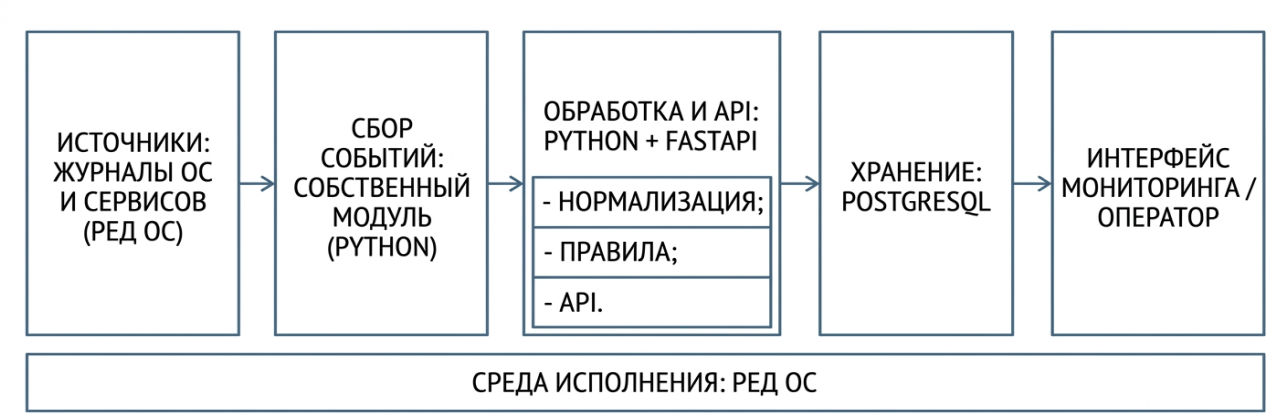

Рисунок 1. Функциональные зоны прототипа SIEM-системы,
выбранный технологический стек и поток обработки событий

Детальное решение делит прототип на уровни источников, сбора, серверного ядра, хранения и представления. Модуль сбора дополняет запись временем получения и идентификатором источника и передаёт её в ядро по протоколу HTTP в формате JSON. Ядро на FastAPI проверяет структуру, выделяет поля, приводит время к единому формату, сохраняет событие в PostgreSQL и применяет правила. Веб-интерфейс получает данные через REST API.

Логическая модель включает пять сущностей: источник, событие, правило, срабатывание и пользователя. Стенд состоит из сервера РЕД ОС, на котором размещены FastAPI, PostgreSQL и модуль сбора, а также из тестовых источников журналов. Требования, выбранный стек и структура прототипа задают основу для программной реализации и оценки применимости подхода в инфраструктуре государственного органа.

Список литературы:

1. Казьмин Д.А. Проблемы внедрения SIEM-систем // Тенденции развития науки и образования. 2023. № 102-5. С. 19–22.

2. Обзор мирового и российского рынка SIEM-систем [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem (дата обращения: 06.10.2026).

3. MaxPatrol SIEM. Система мониторинга событий информационной безопасности и выявления инцидентов [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/products/mpsiem/ (дата обращения: 06.10.2026).

4. ГОСТ Р ИСО/МЭК 27002-2021. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. М.: Российский институт стандартизации, 2021. 74 с.

5. Kent K., Souppaya M. Guide to Computer Security Log Management: NIST Special Publication 800-92. Gaithersburg: NIST, 2006. 72 p. URL: https://doi.org/10.6028/NIST.SP.800-92 (дата обращения: 06.10.2026).