Мавлеткулов Александр Вячеславович, магистрант,
Амурский государственный университет

Галаган Татьяна Алексеевна,
Амурский государственный университет

ПРОТОТИП SIEM-СИСТЕМЫ МОНИТОРИНГА СОБЫТИЙ В СРЕДЕ ОТЕЧЕСТВЕННОГО ПО

Аннотация. В работе рассматривается организация мониторинга и анализа событий информационной безопасности в информационной среде государственного органа. Показана необходимость создания прототипа SIEM-системы с учётом увеличения числа киберугроз и перехода организаций на отечественное программное обеспечение.

Ключевые слова: SIEM, информационная безопасность, мониторинг событий, корреляция, отечественное ПО, импортозамещение.

1. ОБОСНОВАНИЕ ВЫБОРА ТЕМЫ КВАЛИФИКАЦИОННОГО ИССЛЕДОВАНИЯ

Развитие цифровых технологий привело к тому, что информационные системы стали использоваться практически во всех направлениях деятельности государственных организаций. В их работе применяются системы электронного документооборота, базы данных, почтовые службы, сетевые ресурсы и средства межведомственного обмена информацией. Вместе с расширением такой инфраструктуры увеличивается и количество потенциальных угроз, которые могут нарушать конфиденциальность, целостность или доступность данных [7, 8].

Отдельной проблемой остаётся рост числа атак на государственные информационные ресурсы. Для получения доступа к системам могут использоваться украденные или подобранные учетные данные, уязвимости программного обеспечения, вредоносные программы и фишинговые методы. Подобные действия могут быть направлены как на крупные федеральные структуры, так и на государственные организации регионального уровня [1].

Поэтому одной из практических задач информационной безопасности становится своевременное обнаружение подозрительной активности. Для этого требуется получать информацию о происходящих в инфраструктуре событиях. Серверы, рабочие станции, сетевое оборудование и прикладные системы постоянно формируют журналы, в которых сохраняются сведения о действиях пользователей, работе сервисов и изменении состояния оборудования [8].

При этом информация о событиях обычно распределена между большим количеством технических средств. Например, часть журналов может находиться непосредственно на рабочих станциях, другая – на серверах или сетевых устройствах. Дополнительные данные формируются средствами защиты информации. Если анализировать такие записи отдельно, специалисту приходится самостоятельно сопоставлять информацию из разных источников. При значительном количестве событий такой способ работы становится трудоёмким и может привести к пропуску важных признаков инцидента [11].

Для автоматизации данной работы используются SIEM-системы (Security Information and Event Management). Их основное назначение заключается в объединении событий из различных источников и последующей обработке полученной информации. В рамках единой системы выполняются сбор, хранение и анализ журналов, а также поиск взаимосвязанных событий. Это позволяет сократить время обнаружения потенциальных инцидентов и упростить работу специалиста по информационной безопасности [2].

В течение длительного периода для подобных задач применялись зарубежные программные решения, включая Splunk и инструменты, построенные на базе ELK Stack. Они предоставляют развитые возможности работы с журналами и позволяют обрабатывать значительные объёмы данных. Однако для государственных организаций использование зарубежных продуктов связано с рядом ограничений, в том числе с вопросами поставки, сопровождения и дальнейшего получения технической поддержки. В связи с этим возрастает необходимость поиска решений, которые могут применяться в отечественной программной среде [6].

На российском рынке уже представлены коммерческие продукты соответствующего назначения. К ним относятся MaxPatrol SIEM, SearchInform SIEM и КОМРАД SIEM. Такие решения рассчитаны на применение в российских организациях и обладают широким набором функций для мониторинга событий. Вместе с тем их внедрение может потребовать значительных расходов на лицензирование, настройку и последующее сопровождение. Дополнительным фактором является необходимость наличия специалистов, способных обслуживать подобные системы [3–5].

Актуальность разработки собственного прототипа также связана с проводимой политикой импортозамещения. Для государственных организаций важной задачей становится использование отечественных программных продуктов и технологий. В результате появляется потребность в системах, которые способны работать с российскими операционными системами и при этом сохранять необходимые функции мониторинга информационной безопасности [6, 10].

Информационная среда государственного органа представляет собой совокупность различных технических и программных компонентов. В неё входят пользовательские рабочие места, серверы, сетевое оборудование, системы электронного документооборота и другие информационные ресурсы. Сбои или нарушения безопасности отдельных компонентов могут отразиться на работе всей организации. При отсутствии единого средства мониторинга специалисту сложнее получить целостную картину происходящих событий и своевременно выявить признаки атаки.

В связи с этим разработка прототипа SIEM-системы представляет практический интерес. Такой прототип позволяет проверить организацию централизованного сбора данных, определить порядок обработки событий и реализовать базовые механизмы их анализа. Использование открытых технологий и отечественного программного обеспечения также даёт возможность оценить применимость выбранного подхода для информационной среды государственного органа [2, 10].

Таким образом, необходимость проведения исследования связана сразу с несколькими факторами: увеличением количества киберугроз, ростом объёма регистрируемых событий, сложностью их ручного анализа и переходом государственных организаций на отечественное программное обеспечение. Создание прототипа SIEM-системы направлено на построение централизованного механизма сбора и анализа событий информационной безопасности в информационной среде государственного органа [1, 6].

Список литературы:

1. Актуальные киберугрозы: итоги 2023 года [Электронный ресурс] / Positive Technologies. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023/ (дата обращения: 15.06.2026).

2. Казьмин Д. А. Проблемы внедрения SIEM-систем // Тенденции развития науки и образования. – 2023. – № 102-5. – С. 19–22. – URL: https://www.elibrary.ru/item.asp?id=54811197 (дата обращения: 15.06.2026).

3. MaxPatrol SIEM: система мониторинга событий ИБ [Электронный ресурс] / Positive Technologies. – URL: https://www.ptsecurity.com/ru-ru/products/mpsiem/ (дата обращения: 15.06.2026).

4. SearchInform SIEM [Электронный ресурс] / SearchInform. – URL: https://searchinform.ru/products/searchinform-siem/ (дата обращения: 15.06.2026).

5. КОМРАД SIEM [Электронный ресурс] / Infotecs. – URL: https://infotecs.ru/products/komrad/ (дата обращения: 15.06.2026).

6. О внесении изменений в некоторые акты Президента Российской Федерации по вопросам импортозамещения: Указ Президента РФ от 30.03.2022 № 166 (ред. от 07.05.2022) // Собрание законодательства РФ. – 2022.

7. Жук А. П., Жук Е. П., Лепешкин О. М., Тимошкин А. И. Защита информации: учебное пособие. – 2-е изд. – М.: ИЦ «РИОР»: НИЦ «ИНФРА-М», 2019. – 392 с.

8. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2021. – 24 с.

9. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3448.

10. РЕД ОС: документация [Электронный ресурс] / РЕД СОФТ. – URL: https://redos.red-soft.ru/ (дата обращения: 15.06.2026).

11. Фахрутдинова И. Р., Трофимова Н. О. Информационная безопасность на предприятии // Современные научные исследования и инновации. – 2016. – № 2. – URL: http://web.snauka.ru/issues/2016/02/64549 (дата обращения: 15.06.2026).

12. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.