УДК 004.056.53

ИСПОЛЬЗОВАНИЕ SIEM-СИСТЕМ ДЛЯ МОНИТОРИНГА СОБЫТИЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ

Кряжева Е. В.

к.псих.н., доцент,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Кашицын М.А.,

магистрант,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Шаров Н.С.,

магистрант,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Аннотация.

В статье рассматриваются особенности применения SIEM-систем (систем управления информацией и событиями безопасности) в целях обеспечения информационной безопасности организаций. Подчеркивается значение интеграции таких решений для своевременного выявления угроз, анализа инцидентов и принятия оперативных мер реагирования. Освещаются функциональные возможности SIEM-систем, включая сбор, корреляцию и визуализацию данных из различных источников. Проведен обзор преимуществ и ограничений их использования в корпоративной среде. Приведены примеры практического применения SIEM в инфраструктуре организаций различного масштаба. В конце статьи представлены выводы по проделанной работе.

Ключевые слова: информационная безопасность, SIEM-системы, мониторинг событий, инциденты безопасности, киберугрозы.

USING SIEM SYSTEMS TO MONITOR SECURITY EVENTS IN ORGANIZATIONS

Kryazheva E. V.,
Candidate of Psychological Sciences, Associate Professor,
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia
Kashitsyn M.A.,
Undergraduate,
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia
Sharov N.S.,
Undergraduate,
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia

Annotation.
The article discusses the specifics of using SIEM systems (information management systems and security events) in order to ensure the information security of organizations. The importance of integrating such solutions for timely threat detection, incident analysis, and prompt response is emphasized. The functionality of SIEM systems is highlighted, including the collection, correlation and visualization of data from various sources. The advantages and limitations of their use in a corporate environment are reviewed. Examples of practical application of SIEM in the infrastructure of organizations of various scales are given.

Keywords: information security, SIEM systems, event monitoring, security incidents, cyber threats.

В современных условиях цифровизации и роста объёмов данных организации сталкиваются с постоянно увеличивающимися угрозами информационной безопасности. Традиционные средства защиты, такие как антивирусы и межсетевые экраны, уже не способны полностью обеспечивать необходимый уровень безопасности. В связи с этим на первый план выходит необходимость внедрения более сложных и интеллектуальных систем защиты, одной из которых являются SIEM-системы (Security Information and Event Management). Эти системы предназначены для мониторинга и анализа событий безопасности в реальном времени, что позволяет организациям не только обнаруживать инциденты, но и оперативно на них реагировать.

Одной из ключевых особенностей SIEM-систем является их способность интегрировать данные из множества источников, что позволяет получить полную картину о состоянии безопасности всей организации. Это включает не только данные о возможных угрозах и инцидентах, но и информацию о сетевом трафике, действиях пользователей и состояния серверов [2].

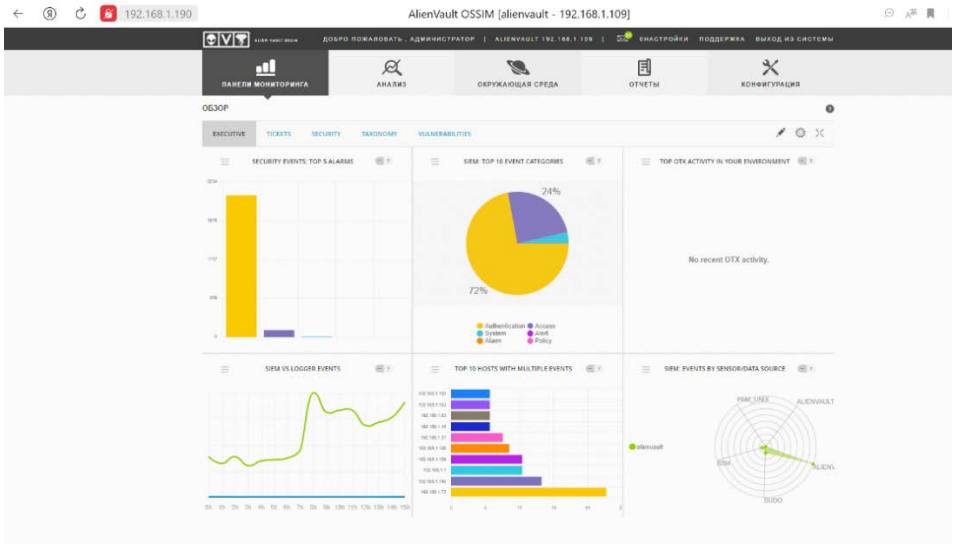

Рис. 1 - Панель мониторинга SIEM-системы AlienVault OSSIM (составлено авторами)

Пример визуализации таких данных представлен на Рисунке 1. На панели мониторинга SIEM-системы AlienVault OSSIM отображаются типы событий, активность хостов, источники инцидентов и категории угроз в реальном времени.

Таким образом, SIEM-системы становятся центральным элементом системы информационной безопасности, позволяя эффективно выявлять не только известные угрозы, но и новые, ранее незамеченные аномалии, что значительно повышает уровень защиты организации.

SIEM-системы представляют собой решения, которые позволяют централизованно собирать, хранить и анализировать информацию о событиях безопасности, происходящих в различных компонентах ИТ-инфраструктуры. Они обеспечивают корреляцию данных с различных источников, таких как серверы, приложения, сетевые устройства и базы данных, что помогает выявлять скрытые угрозы [5]. Одной из главных функций SIEM-систем является мониторинг в реальном времени, что позволяет оперативно обнаруживать аномалии и подозрительные действия, а также автоматизировать процесс уведомления администраторов.

Помимо этого, SIEM-системы обладают функцией ретроспективного анализа данных. Это означает, что, даже если инцидент не был выявлен сразу, системы позволяют провести глубокий анализ событий, произошедших в прошлом, для выявления потенциальных угроз, которые могли бы быть не замечены в ходе стандартного мониторинга. Этот аспект является критически важным для организаций, работающих в сфере, где необходимо долгое время хранить информацию, например, в финансовом секторе или в здравоохранении.

Внедрение таких систем значительно повышает уровень защищённости организации, позволяя ей проактивно реагировать на угрозы, предотвращая возможные инциденты до того, как они могут нанести серьёзный ущерб. Также важным аспектом является то, что SIEM-системы помогают обеспечить соответствие организации различным нормативным и регуляторным

требованиям, таким как законодательство о защите персональных данных или стандарты информационной безопасности, такие как PCI DSS.

Соблюдение нормативных актов и стандартов безопасности не только повышает уровень защиты, но и способствует укреплению репутации компании. Например, наличие внедрённой SIEM-системы и соответствие требованиям таких стандартов, как ISO 27001 или GDPR, является важным аспектом в отношениях с партнерами и клиентами. Компании, которые могут продемонстрировать высокий уровень защиты данных и информационных систем, имеют конкурентное преимущество и доверие со стороны клиентов.

Преимущества SIEM-систем очевидны. Во-первых, они позволяют значительно повысить эффективность реагирования на инциденты безопасности. Благодаря автоматической корреляции событий и оповещению администраторов в случае угроз, компании могут быстрее устранять уязвимости. Во-вторых, системы помогают централизовать данные, что значительно упрощает процессы аудита и анализа. На Рисунке 2 представлен пример использования SIEM-системы RUSIEM, наглядно демонстрирующий классификацию событий по источникам, хостам, типам протоколов и временным рамкам. Такая детализация облегчает аудит и выявление аномалий.

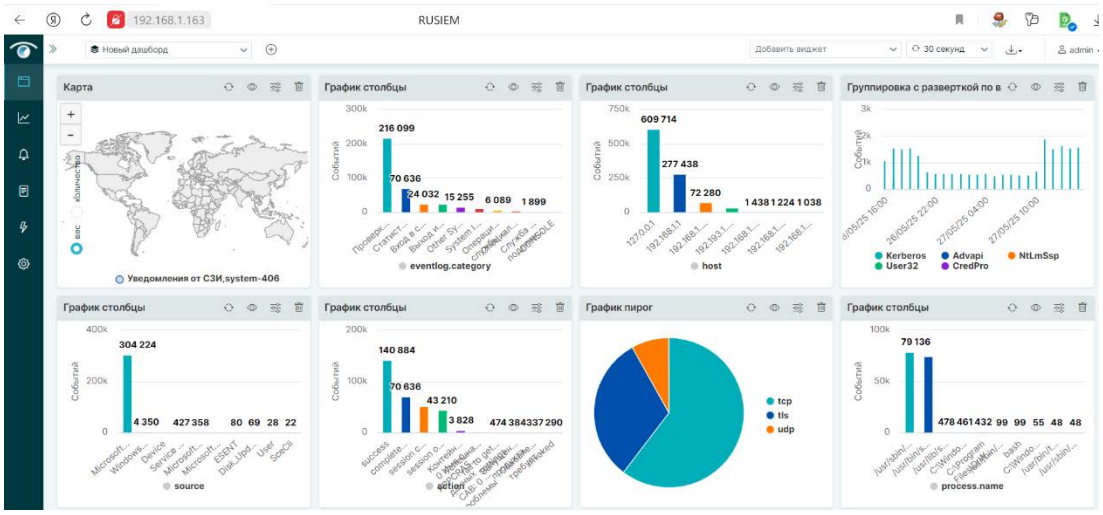

Рис. 1 - Интерфейс SIEM-системы RUSIEM (составлено авторами)

Это позволяет не только улучшить безопасность, но и оптимизировать процессы внутри организации. Одним из ключевых аспектов успешного внедрения SIEM-систем является правильная настройка и управление правилами корреляции событий. Эти правила определяют, какие данные будут собираться и как будет происходить их анализ. От их качества зависит, насколько эффективно система будет выявлять реальные угрозы и минимизировать ложные срабатывания. Это требует постоянного мониторинга и адаптации системы к новым угрозам, что делает внедрение SIEM не одноразовым процессом, а постоянной задачей для ИТ-служб [4].

Для минимизации ложных срабатываний важным аспектом является использование методов машинного обучения и искусственного интеллекта в современных SIEM-системах. Эти технологии позволяют системе обучаться на основе исторических данных и адаптировать свои алгоритмы для повышения точности обнаружения угроз. Со временем, чем больше данных обрабатывает система, тем более точными становятся её прогнозы и реакции.

Однако внедрение и эксплуатация SIEM-систем сопряжены с определёнными трудностями. Во-первых, их установка требует значительных затрат, как на программное обеспечение, так и на оборудование. Во-вторых, для успешного функционирования системы необходимо наличие квалифицированных специалистов, которые смогут настроить и поддерживать её работу. Также внедрение таких систем может быть осложнено интеграцией с устаревшими информационными системами, которые не поддерживают современные стандарты логирования и мониторинга. Наконец, высокая чувствительность SIEM-систем к количеству и качеству входных данных может привести к появлению ложных срабатываний, что требует тщательной настройки и постоянного обновления правил корреляции.

Тем не менее, несмотря на все сложности, использование SIEM-систем становится необходимостью для большинства крупных организаций, особенно тех, которые работают с критически важной информацией или обязаны

соблюдать строгие требования безопасности. Например, в банковской сфере такие системы позволяют не только защищать данные клиентов, но и эффективно отслеживать попытки мошенничества, в том числе с использованием социальных инженерий. В секторе здравоохранения SIEM-системы помогают обеспечивать защиту персональных медицинских данных, что критически важно для соблюдения законов о защите конфиденциальной информации.

В связи с растущими угрозами и постоянной эволюцией методов атак на организации, важно понимать, что роль SIEM-систем будет только возрастать. Их возможности расширяются с каждым годом, а новые решения позволяют интегрировать дополнительные модули, такие как управление инцидентами, прогнозирование угроз на основе аналитики и автоматизация реакции на инциденты [3]. Это даёт возможность не только предотвращать атаки, но и в дальнейшем анализировать их для улучшения системы защиты.

Внедрение SIEM-систем требует комплексного подхода, включая анализ текущей инфраструктуры, выбор подходящего решения и обучение персонала. Важно учитывать особенности бизнеса, масштабы организации и требования к безопасности. В дальнейшем успешное использование таких систем зависит от постоянного обновления и оптимизации правил мониторинга, а также от готовности организации оперативно реагировать на выявленные инциденты.

Таким образом, SIEM-системы играют ключевую роль в обеспечении информационной безопасности организаций, позволяя повысить уровень защиты от киберугроз и улучшить общую безопасность ИТ-инфраструктуры. Несмотря на высокие затраты на внедрение и необходимость в квалифицированных кадрах, преимущества, которые они предоставляют, значительно превосходят эти издержки, обеспечивая долгосрочную защиту и соответствие всем необходимым стандартам.

Библиографический список:

1. Джуракулов, Т.Х. SIEM-системы управления событиями / Т.Х. Джуракулов, А.А. Петросян, В.А. Евстропов // Молодой учёный. - 2023. - №4 (451). - С. 10–11. 4

2. Кузнецова, А.Д. Обзор состояния исследований информационной безопасности и применение SIEM-систем / А.Д. Кузнецова, Д.В. Сахаров // Сборник научных статей VIII Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО 2019). Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. - 2019.- С. 626–631.

3. Медведева, А.О. О необходимости внедрения SIEM-системы как важного элемента системы защиты информации / А.О. Медведева // Сборник материалов V Всероссийской молодёжной научно-практической конференции «Информационные технологии обеспечения комплексной безопасности в цифровом обществе». - Уфа: Башкирский государственный университет. - 2022. - С. 141–145. 1

4. Токарев, М.Н. SIEM-система как инструмент обеспечения информационной безопасности в организации / М.Н. Токарев // Актуальные исследования. - 2024. - №2 (184). Ч. I. С. 51–53

5. Шабля, В.О. Анализ процесса функционирования SIEM-систем / В.О. Шабля, С.А. Коноваленко, Р.В. Едунов // E-Scio. - 2022. - №5 (68). - С. 284–295.

Оригинальность 80%