# АНАЛИЗ И МОНИТОРИНГ СЕТИ ПРЕДПРИЯТИЯ В РЕАЛЬНОМ ВРЕМЕНИ

***Комаров Александр Николаевич***
*Магистрант*
*Донской государственный технический университет*
*Россия, г. Ростов-на-Дону*

**Аннотация**. В статье рассматривается метод позволяющий производить анализ и мониторинг сети предприятия в реальном времени. Также в статье уделено внимание источникам данных для обработки информации SIEM-системой, а именно рассмотрен механизм обработки данных. Рассмотрены примеры правил корреляции в SIEM-системе. Проанализирована эффективность использования SIEM-системы.

**Abstarct**. The article discusses a method that allows you to analyze and monitor an enterprise network in real time. Also, the article focuses on data sources for processing information by a SIEM system, namely, the data processing mechanism is considered. Examples of correlation rules in a SIEM system are considered. The efficiency of using a SIEM system has been analyzed.

**Ключевые слова:** SIEM-системы, таксономия, анализ, классификация.

**Key words:** SIEM systems, taxonomy, analysis, classification.

---

Изобретение и всеобщее использование цифровых устройств привело к тому, что большинство организаций и людей хранят информацию в электронном виде. Возникает проблема защиты информационных ресурсов, так как способы несанкционированного доступа постоянно совершенствуются, поэтому задача защиты информации – актуальна.

Интенсивность информационных событий в корпоративных сетях может достигать нескольких миллионов в день, поэтому возникает проблема нахождения и локализации вредоносной информации в огромных информационных массивах. При этом обработка подобных событий в ручном режиме не представляется возможной, так как потребовала бы значительных человеческих и временных затрат, а также недопустимых с точки зрения эффективности аппаратно-программных ресурсов [1].

Одно из ключевых средств, используемое для её решения – это SIEM-системы (сокращение от англ. Security information and event management) – системы управления событиями информационной безопасности. Основные задачи, решаемые современным SIEM-приложением: сбор, анализ и предоставление пользователю в удобном виде информации, полученной с различных сетевых компонентов и устройств безопасности. Подобные инструменты позволяют оперативно и с наименьшими трудозатратами реагировать как на уже существующие, так и на потенциальные угрозы безопасности ИТ-инфраструктуры.

SIEM-система решает следующие задачи:

– консолидация данных;
– хранение событий безопасности;
– корреляция и обработка событий безопасности;
– контекстное обогащение инцидентов;
– предоставление инструментов для экспертного анализа;
– автоматическое оповещение администратора сети.

Задача SIEM-системы получить данные от источников (рисунок 1). Источник данных может быть «активным», который самостоятельно может передавать данные по указанному пути приемника, а также и «пассивным» к которому SIEM-система обращается сама. После получения информации от источника происходит нормализация данных, SIEM-система преобразует данные в единообразный формат.

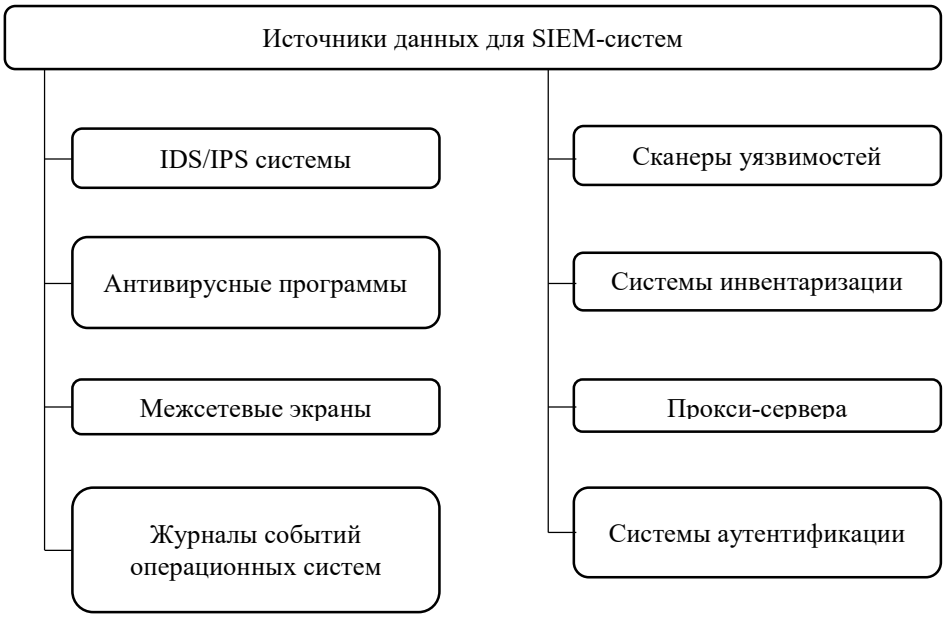


*Рисунок 1 – Источники данных для SIEM-систем*

Следующий шаг системы – таксономия, т.е. классификация уже нормализованных данных в зависимости от их содержания: какое событие означает об успешной сетевой коммуникации, какое – о срабатывании антивируса, а какое – о входе пользователя на ПК. Таким образом формируется цепочка событий с временной последовательностью наступления такого события. Далее срабатывает механизм SIEM-систем – корреляция. Корреляция в SIEM – это соотношение межу собой событий, соответствующих тем или иным заданным условиям. Пример правила корреляции: если на трех или более ПК в течении 3-х минут сработал антивирус, то это может означать что на предприятие произошла вирусная атака. Более сложное правило если в течении 2-х дней фиксировались попытки удаленно зайти на сервер, которые увенчались успехом, а после началось копирование данные на внешнее устройство, то это может означать что злоумышленник сумел подобрать пароль к учетной записи и копирует данные. По итогам срабатывания правила корреляции в SIEM-системы формируется инцидент информационной безопасности (далее – ИБ).

Дальнейший анализ зарегистрированных инцидентов ложится также на отдел ИБ. Где при помощи встроенных инструментов формируют отчеты, реагируют на события, и не допускают повторного инцидента в дальнейшем.

В основе работы таких систем лежат, в основном, статистические и математические технологии, работа с большими потоками событий, хранение и поиск информации в десятках терабайт данных.

Перечислим некоторые из известных SIEM-систем:

– «КОМРАД» от НПО «Эшелон».

Так как всё больше руководителей предприятий осознают необходимость тщательного подхода к защите информации, SIEM-системы активно развиваются, а количество представляемых решений на рынке стабильно растет.

Внедрение и последующее совершенствование SIEM-системы позволяют повысить уровень защищенности информации на предприятии. Кроме того, SIEM-система заметно облегчает работу специалистов по ИБ любого предприятия за счет аккумулирования данных об инциденте, возможности определения ответственного за обработку конкретного инцидента, а также сроков обработки инцидента. В свою очередь, собранные и обработанные статистические данные позволяют судить об эффективности работы, как отдельных средств защиты информации, так и системы безопасности в целом.

**Список литературы**

Шабуров А.С., Борисов В.И. О применении сигнатурных методов анализа информации в SIEM-системах // Вестник УрФО. Безопасность в информационной среде. – Челябинск: Изд. центр ЮУрГУ, 2015. – № 17. – С. 23–