ISSN 2782-2001
Системы анализа
и обработки данных
том 89, № 1, 2023, с. 101–113

http://journals.nstu.ru/vestnik
Analysis and data
processing systems
Vol. 89, No. 1, 2023, pp. 101–113

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

ELECTRONICS, PHOTONICS, INSTRUMENT MAKING AND COMMUNICATIONS

УДК 004.89

DOI: 10.17212/2782-2001-2023-1-101-113

Разработка системы сбора, обработки, анализа, идентификации корреляции событий информационной инфраструктуры предприятия*

А.С. СТРЕЛЬЦОВ[1,a], Г.А. ФРАНЦУЗОВА[1,b], Е.А. БАСЫНЯ[1,2,c]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет*
[2] *115409, РФ, г. Москва, Каширское шоссе, 31, Национальный исследовательский ядерный университет «МИФИ»*

[a] *andreystreltsov@bk.ru* [b] *frants@ac.cs.nstu.ru* [c] *basinya@mail.ru*

К рассмотрению предлагается система сбора, обработки, анализа, идентификации корреляции событий информационной инфраструктуры предприятия.

По мере развития корпоративных информационных систем число угроз, связанных с нарушением доступности, целостности и конфиденциальности в них, возросло в десятки раз. Обеспечение информационной безопасности является комплексной задачей по реагированию, расследованию и устранению последствий инцидентов информационной безопасности.

В работе предлагается формализованное описание данных, используемых предлагаемой системой. Помимо этого, выделены общая архитектура и принципы функционирования. Особое внимание уделено подробному описанию одной из основных частей системы (агентам сбора данных).

Подсистема сбора информации характеризуется типом собираемой информации: данными о работе приложения, хоста, сети или о межсетевых взаимодействиях. Подсистема подобного класса аккумулирует разнородные данные о системе или сети для того, чтобы в дальнейшем провести их анализ на наличие признаков реализации компьютерных атак. Для сбора данных используются специальные модули – сенсоры и агенты. Первые обычно используются для мониторинга сетевой активности, а вторые – для контроля и анализа действий в определенной системе.

Практическое применение усовершенствованной модели возможно как в рамках исследовательских работ, так и в системах автоматизированного контроля информационной безопасности. Полученные результаты будут использоваться при дальнейшем проектировании комплексной системы непрерывного мониторинга информационной инфраструктуры предприятия: планируется рассмотрение подсистемы хранения данных. Последующая работа над темой позволит детализировать архитектуру и алгоритм функционирования.

* *Статья получена 17 ноября 2022 г.*

Ключевые слова: системы обработки журналов, системы обнаружения атак, системы обнаружения и реагирования, системы сбора информации о безопасности и управления событиями, IDS, IPS, SIEM, администрирование, информационная безопасность

ВВЕДЕНИЕ

В текущих условиях проблематика возникновения атак, связанных с нарушением доступности, целостности и конфиденциальности в информационных системах, возросла в десятки раз, а задача по защите от подобного рода атак становится всё более сложной и особенно актуальной.

Среди множества атак можно выделить несколько явных векторов, которые находятся на стыке защищенности данных и автоматизации систем предприятий. При этом следует принимать во внимание тот факт, что, как правило, система защиты информации реагирует недостаточно быстро и эффективно. Отделы информационной безопасности, которые имеют соответствующие программно-технические средства, такие как системы обнаружения и предотвращения вторжений (англ. IDS/IPS, Intrusion Detection System / Intrusion Prevention System), антивирусные программы, журналы событий, сканеры уязвимостей и т. д., выявляют инциденты информационной безопасности, которые чреваты крупными потерями. В связи с этим в последнее время всё чаще используются процессы мониторинга событий информационной безопасности для обнаружения и обработки выявленных инцидентов информационной безопасности в кратчайшие сроки.

В настоящей работе рассматривается реализация предложенного подхода, который позволит управлять событиями безопасности и осуществлять проактивное (действующее до того, как ситуация станет критической) управление инцидентами и событиями безопасности. Как следствие, появится возможность проводить корректное реагирование на возникающие угрозы ИБ в разнородных информационных системах. Подобного класса решения именуются системами управления информацией о безопасности и событиями безопасности (англ. SIEM, Security information and event management). SIEM должна быть спроектирована таким образом, чтобы обеспечить надлежащую степень защищенности сети.

Основной проблемой при проектировании такой системы является разработка ее общей архитектуры. Важно четко понимать, какие подсистемы и модули должны входить в состав системы, иначе в будущем при разработке может возникнуть необходимость добавлять или удалять некоторые части.

Система сбора, обработки, анализа, идентификации корреляции событий основана на следующей архитектуре: «агенты» – «хранилище данных» – «сервер приложений», которая развертывается поверх защищенной информационной инфраструктуры. Агенты отвечают за сбор событий безопасности, их первоначальную обработку и фильтрацию. Собранная и отфильтрованная информация затем направляется в хранилище данных или так называемый репозиторий, где она хранится во внутреннем формате для последующего использования и анализа сервером приложений. Сервер приложений выполняет основные функции защиты безопасности и анализа собранных данных, а также генерирует отчеты и уведомления.

1. ПОСТАНОВКА ЗАДАЧИ

Необходимо разработать эффективную систему сбора, обработки, анализа, идентификации корреляции событий для привнесения глобальной наблюдаемости в информационную инфраструктуру предприятия, в том числе посредством сбора данных от различных источников (журналов системы, хранилищ информации о событиях безопасности и т. д.) с их дальнейшим распарсиванием и нормализацией.

К системе предъявляются следующие требования:

- визуализация извлекаемых данных;
- наличие программного интерфейса приложения (англ. API, Application Programming Interface);
- функциональность фильтрации или разделения извлекаемых записей по типу;
- реализация многопоточной обработки данных;
- подробное описание выходных данных.

Схематично проектируемая SIEM представлена на рис. 1.

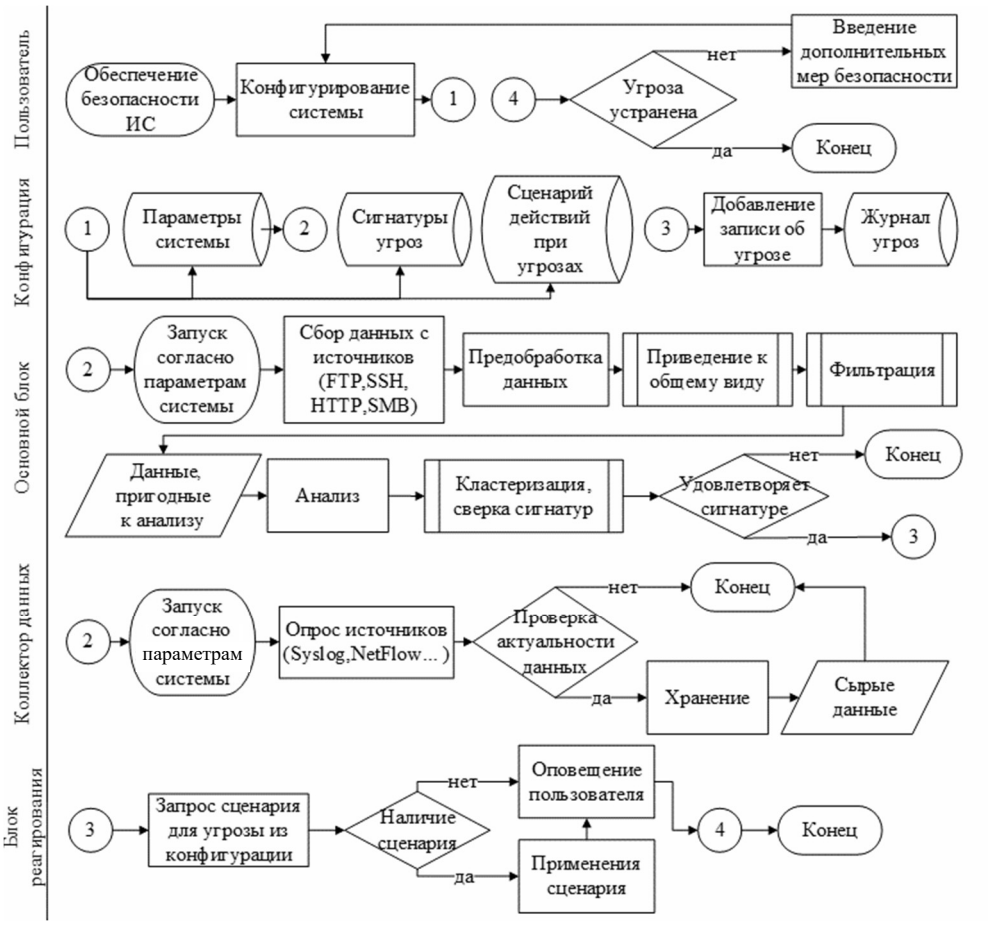

Рис. 1. Структурная блок-схема функционирования проектируемой SIEM

Fig. 1. Structural block diagram of the functioning of the designed SIEM

Для достижения поставленной цели с учетом предъявляемых требований предлагается общую задачу разделить на подзадачи:

1) определение входных данных и их структуризация;
2) определение ресурсов собранных данных;
3) определение выходных данных.

В свою очередь, каждой из подзадач соответствуют свои требования из общего перечня. Так, для определения входных данных и структуризации необходимо иметь их четкое описание. Для второй подзадачи следует ограничить количество собранных данных с целью получения приемлемых результатов и преобразовать их к виду, пригодному для анализа. Решение третьей подзадачи предполагает определение количества результатов и четкое описание выходных данных.

Кроме того, система спроектирована таким образом, чтобы быть масштабируемой и гибкой, поэтому она может адаптироваться к меняющимся потребностям в области безопасности и к потенциальным угрозам. Это достигается путем регулярного обновления системы новыми алгоритмами и протоколами, а также путем мониторинга производительности системы и внесения корректировок по мере необходимости. Другим важным аспектом системы является ее способность интегрироваться с другими системами и инструментами безопасности, такими как брандмауэры, системы обнаружения вторжений и системы информации о безопасности и управления событиями. Это позволяет получить всестороннее представление об общем состоянии безопасности инфраструктуры и обеспечивает быстрое реагирование на любые инциденты безопасности. В целом, проектирование и внедрение системы требует глубокого понимания различных задействованных компонентов и технологий, а также способности предвидеть и адаптироваться к меняющимся потребностям в области безопасности.

Другим важным аспектом системы является ее способность обнаруживать потенциальные угрозы безопасности и реагировать на них в режиме реального времени. Это достигается за счет использования передовых алгоритмов и методов машинного обучения, которые позволяют системе анализировать большие объемы данных и выявлять закономерности и аномалии, которые могут указывать на угрозу безопасности. Система также имеет возможность автоматически реагировать на выявленные угрозы, например, путем блокирования подозрительного трафика или изолирования зараженных систем. Кроме того, система также может быть настроена на отправку оповещений сотрудникам службы безопасности в случае обнаруженной угрозы, что позволяет им принимать немедленные меры.

Однако важно учитывать аспект конфиденциальности данных и безопасности системы. Данные, собранные системой, должны быть зашифрованы во время транспортировки и в состоянии покоя, чтобы предотвратить несанкционированный доступ или нарушения. Также важно иметь надлежащий контроль доступа, чтобы гарантировать, что только авторизованный персонал имеет доступ к данным. Проведение регулярных аудитов безопасности и тестирование на проникновение необходимо для выявления любых уязвимостей или слабых мест в системе и принятия необходимых мер по их устранению.

Таким образом, можно сказать, что разработка системы сбора, обработки, анализа, идентификации корреляции событий требует всестороннего понимания различных задействованных компонентов и технологий, а также способ-

ности прогнозировать и адаптироваться к меняющимся потребностям в области безопасности. Система должна быть способна обнаруживать потенциальные угрозы безопасности и реагировать на них в режиме реального времени, обеспечивая при этом конфиденциальность и безопасность данных.

2. ОПИСАНИЕ СИСТЕМЫ И ФОРМАЛЬНОЕ ПРЕДСТАВЛЕНИЕ ДАННЫХ

Разрабатываемая SIEM-система имеет преимущество перед рядом средств IDS в том, что она может представлять всесторонний обзор проблем и использовать накопленную статистику для отслеживания отклонений от нормального состояния информационных систем компании. Кроме того, SIEM позволяет сопоставлять события из нескольких источников, обеспечивая более полную картину потенциальных угроз безопасности [1]. Это может помочь в выявлении закономерностей и тенденций, которые могут быть не сразу очевидны с помощью одних только данных IDS. Проектируемая SIEM также имеет возможность реагирования на инциденты, предоставляя компании инструменты, необходимые для расследования инцидентов безопасности и реагирования на них.

Выделим следующие главные механизмы функционирования SIEM-системы, иерархическая модель которой показана на рис. 2:

1) сбор данных: системы SIEM собирают и объединяют данные из различных источников, таких как сетевые устройства, серверы и приложения;

2) нормализация данных: собранные данные нормализуются и сопоставляются для создания согласованного и унифицированного представления о состоянии безопасности организации;

3) корреляция событий: нормализованные данные анализируются для выявления закономерностей и взаимосвязей, а также для обнаружения потенциальных угроз безопасности;

4) генерация оповещений: если обнаружена потенциальная угроза, система SIEM создает оповещение, которое группа безопасности должна исследовать;

5) отчетность и анализ: системы SIEM предоставляют различные отчеты и инструменты анализа, которые помогают командам безопасности понять состояние безопасности своей организации и определить области для улучшения;

6) автоматическое реагирование: некоторые системы SIEM также могут включать в себя функции автоматического реагирования, которые позволяют им выполнять предварительно заданные действия в ответ на определенные типы событий, такие как блокировка IP-адреса или завершение работы скомпрометированной системы;

7) управление соответствием: системы SIEM можно настроить для мониторинга и составления отчетов о соответствии различным стандартам и нормам безопасности, таким как стандарт безопасности индустрии платежных карт (англ. PCI-DSS, Payment Card Industry Data Security Standard) и акт о передаче и защите данных учреждений здравоохранения (англ. HIPAA, Health Insurance Portability and Accountability Act);

8) криминалистическая экспертиза: системы SIEM также можно использовать для сбора и анализа криминалистических данных, таких как файлы журналов, сетевой трафик и образы системы, чтобы помочь в реагировании на инциденты и их расследовании;

9) аналитика угроз: некоторые системы SIEM также могут включать каналы аналитики угроз, чтобы улучшить обнаружение и реагирование на известные угрозы;

10) интеграция: системы SIEM можно интегрировать с другими инструментами безопасности, такими как брандмауэры, системы обнаружения вторжений и сканеры уязвимостей, чтобы обеспечить комплексное решение для обеспечения безопасности.

Рис. 2. Обобщенная иерархическая модель данных в SIEM

Fig. 2. A generalized hierarchical data model in SIEM

Следует иметь в виду, что с уменьшением количества обрабатываемых событий возрастает сложность их обработки (рис. 2), т. е. можно предположить, что повышается эффективность всей системы. Взаимосвязь между рабочими механизмами в системе SIEM нового поколения показана функциональной моделью на рис. 3.

Таким образом, в SIEM-системе можно выделить основные функциональные подсистемы:

1) сбора данных;
2) обработки;
3) хранения;
4) анализа;
5) идентификации корреляции;
6) представления.

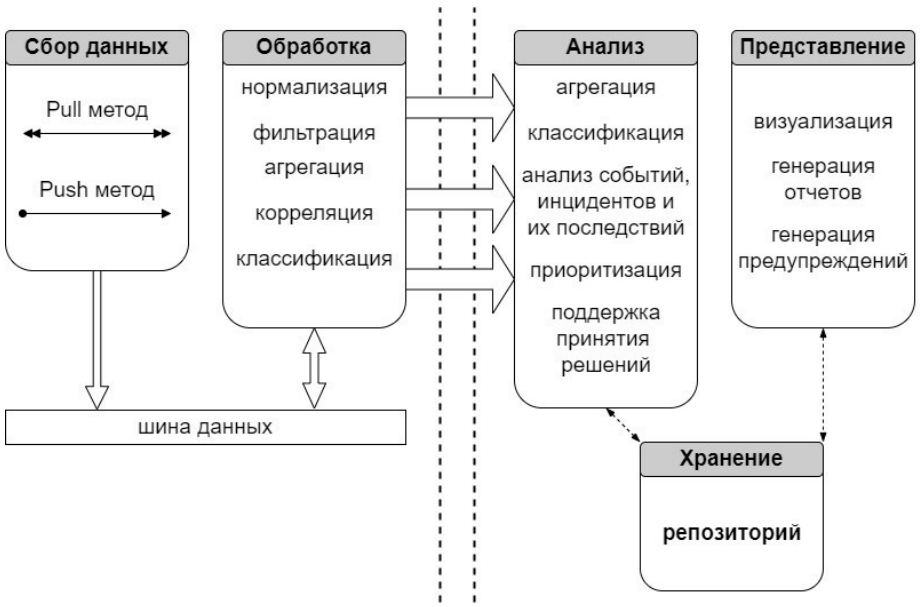

Рис. 3. Функциональная модель SIEM

Fig. 3. The SIEM functional model

Отметим, что первые две подсистемы функционируют в режиме online, а остальные близки к нему.

При этом стоит учитывать, что данные, обрабатываемые защищаемой системой, представляют собой конфиденциальную информацию, составляющую коммерческую тайну. В соответствии с Федеральным законом «О коммерческой тайне» такой информацией могут являться любые сведения, которые имеют коммерческую ценность, обусловленную их неизвестностью третьими лицами. Обладатель таких сведений может на законном основании ограничить доступ к ней путем ввода режима коммерческой тайны на предприятии [2].

Тестовый сегмент информационной структуры (ИС), рассматриваемый в рамках настоящей работы, является обобщенной типовой информационной системой обработки конфиденциальной информации, составляющей коммерческую тайну. Данная ИС включает некоторые популярные корпоративные ресурсы, например, сервер веб-сайта, хранилище данных и автоматизированные рабочие места (АРМ) сотрудников. Информационная структура схематично представлена на рис. 4.

3. КОРРЕЛЯЦИЯ ДАННЫХ В SIEM-СИСТЕМАХ

На этапе корреляции взаимосвязи между разнородными событиями SIEM-система позволяет выявить следующие угрозы:

- нарушения соответствия: системы SIEM могут обнаруживать и предупреждать о действиях, которые нарушают политики безопасности или нормативные требования [4];
- внутренние угрозы: системы SIEM могут обнаруживать и предупреждать о подозрительных действиях внутренних сотрудников, таких как доступ сотрудников к конфиденциальным данным или системам без авторизации или попытки сотрудников эксфильтровать данные;

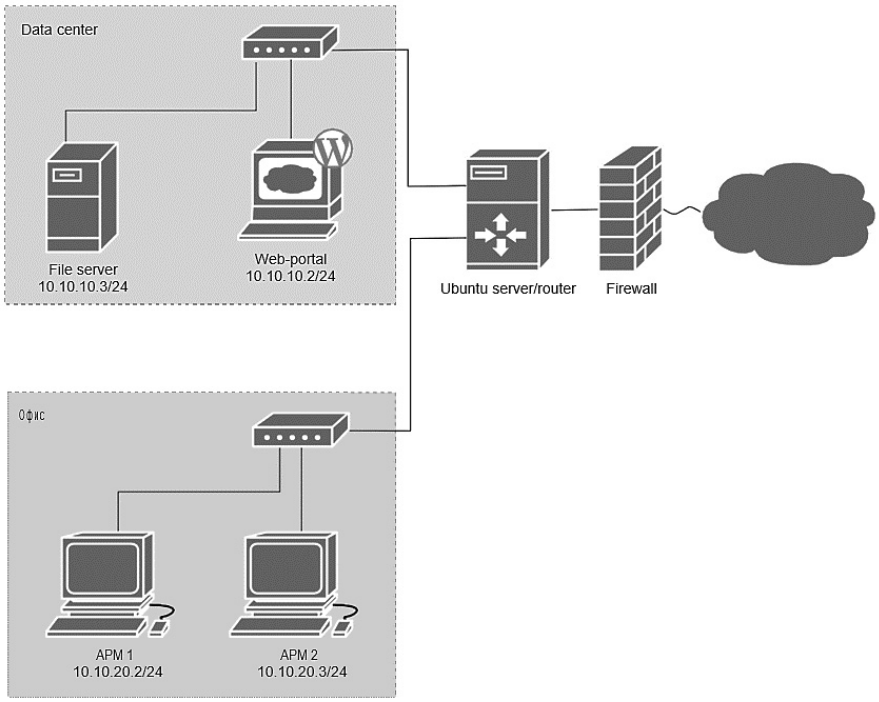

Рис. 4. Схема сегмента информационной структуры

Fig. 4. The information structure segment diagram

- эксфильтрация данных: системы SIEM могут обнаруживать и предупреждать о подозрительной передаче данных, например, о передаче больших объемов данных на подозрительный IP-адрес или передаче данных с использованием неожиданного протокола [3];
- усовершенствованная постоянная угроза (англ. APT, advanced packaging tool), или атаки, обычно организуемые организованными преступными группами: системы SIEM могут обнаруживать изощренные и длительные кибератаки и предупреждать о них;
- атаки типа «отказ в обслуживании» (англ. DoS, Denial of Service)) и «распределенный отказ в обслуживании» (англ. DDoS, Distributed Denial of Service): системы SIEM могут обнаруживать и предупреждать о попытках перегрузить сеть или систему трафиком, что фактически делает ее недоступной для законных пользователей [5];
- фишинг и социальная инженерия: системы SIEM могут обнаруживать и предупреждать о попытках обманом заставить пользователей выдать конфиденциальную информацию, такую как учетные данные для входа или финансовую информацию [9].

Стоит отметить, что SIEM-системы не могут обнаруживать все типы угроз, и возможности обнаружения системы варьируются в зависимости от качества и количества данных, правил, возможностей корреляции и анализа SIEM-системы. Разрабатываемая система мониторинга способна в автоматическом режиме обнаруживать все типы описанных выше инцидентов и в реальном времени классифицировать их по уровню опасности для всей инфраструктуры предприятия.

ЗАКЛЮЧЕНИЕ

Предъявляемые к системе требования распределены по подзадачам, совокупное решение которых позволит спроектировать эффективную систему мониторинга инфраструктуры предприятия. Представлена общая архитектура системы и алгоритм ее функционирования.

При выполнении предварительного тестирования подсистема сбора информации соответствует заявленным ожиданиям: происходит корректный сбор информации из разнородных источников данных (журналов системы, хранилищ информации о событиях безопасности и т. д.), выполняется логирование запускаемых процессов и выявляются вредоносные файлы, обнаруженные антивирусной системой.

В дальнейшем планируется проектирование и разработка комплексной системы непрерывного мониторинга инфраструктуры предприятия. Это позволит представить архитектуру системы и алгоритм функционирования в более детальном виде.

СПИСОК ЛИТЕРАТУРЫ

1. *Басыня Е.А.* Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия // Безопасность информационных технологий. – 2018. – Т. 25, № 4. – С. 42–51.

2. *Рыболовлев Д.А., Карасёв С.В., Поляков С.А.* Классификация современных систем управления инцидентами безопасности // Вопросы кибербезопасности. – 2018. – № 3 (27). – С. 47–53.

3. *Худайназаров Ю.К., Пермяков А.С., Лепешкин Е.О.* Задачи системы интеллектуального мониторинга информационной безопасности инфотелекоммуникационной сети // XVIII Всероссийская научная конференция «Нейрокомпьютеры и их применение»: тезисы докладов. – М., 2020. – С. 198–200.

4. *Королев И.Д., Попов В.И., Ларионов В.А.* Анализ проблематики системы управления информацией и событиями безопасности в информационных системах // Инновации в науке. – 2018. – № 12 (88). – С. 19–26.

5. *Cinque M., Cotroneo D., Pecchia A.* Challenges and directions in security information and event management (SIEM) // 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW). – IEEE, 2018. – P. 95–99.

6. *Мельник Э.В., Клименко А.Б.* Применение концепции «туманных» вычислений при проектировании высоконадежных информационно-управляющих систем // Известия Тульского государственного университета. Технические науки. – 2020. – № 2. – С. 273–283.

7. *Sievierinov O., Ovcharenko M.* Analysis of correlation rules in Security information and event management systems // Computer and Information Systems and Technologies, April 22–23, 2020. – Kharkiv, 2020. – P. 24–25.

8. *Сизов В.А., Киров А.Д.* Проблемы внедрения SIEM-систем в практику управления информационной безопасностью субъектов экономической деятельности // Открытое образование. – 2020. – Т. 24, № 1. – С. 69–79.

9. *Sadowski G., Kavanagh K., Bussa T.* Critical capabilities for security information and event management. – Gartner Group Research Note, 2020.

10. Система идентификации информационных угроз на основе открытых данных сети интернет / Д.О. Маркин, С.М. Макеев, Н.В. Изотов, А.Ю. Андросов // Известия Тульского государственного университета. Технические науки. – 2020. – № 9. – С. 86–94.

11. *Котенко И., Хмыров С.С.* Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак // Вопросы кибербезопасности. – 2022. – № 4 (50). – С. 52–79.

12. *González-Granadillo G., González-Zarzosa S., Diaz R.* Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures // Sensors. – 2021. – Vol. 21, N 14. – P. 4759.

13. *Гутников И.В., Гутников К.В.* Организация подсистемы защиты персональных данных на предприятии // Научно-практические исследования. – 2019. – № 8-3. – С. 55–57.

14. *Штеренберг С.И., Данилова Ю.С.* Разработка методики внедрения и выявления эффективности SIEM-системы // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1, Естественные и технические науки. – 2020. – № 3. – С. 40–45.

15. *Файзулин Р.Ф., Демичев М.С.* Роль SIEM-системы в обеспечении информационной безопасности // Решетневские чтения. – Красноярск, 2021. – Ч. 2. – С. 452–453.

16. *Абденов А., Дронова Г., Трушин В.* Современные системы управления информационной безопасностью. – Новосибирск: Изд-во НГТУ, 2017. – 48 с.

17. *Попков Г.В.* Применение SIEM решений на мультисервисных сетях связи // Интерэкспо Гео-Сибирь. – 2019. – Т. 9. – С. 61–65.

18. *Давдян Т.А.* Современные корпоративные решения по защите информации и выявлению инцидентов информационной безопасности // Вестник науки. – 2022. – Т. 4, № 11 (56). – С. 232–237.

Андрей Сергеевич Стрельцов, аспирант кафедры автоматики Новосибирского государственного технического университета. Основное направление научных исследований: разработка и исследование систем сбора и анализа данных. E-mail: andreystreltsov@bk.ru

Галина Александровна Французова, доктор технических наук, профессор кафедры автоматики Новосибирского государственного технического университета. Основное направление научных исследований: анализ и синтез нелинейных систем автоматического регулирования. E-mail: frants@ac.cs.nstu.ru

Евгений Александрович Басыня, кандидат технических наук, доцент кафедры криптологии и кибербезопасности Национального исследовательского ядерного университета «МИФИ» и кафедры автоматики Новосибирского государственного технического университета. Основное направление научных исследований: разработка автоматизированных систем сбора и обработки результатов. E-mail: basinya@mail.ru

Andrey Sergeevich Streltsov, a post-graduate student at the Department of Automation, Novosibirsk Technical University. The main field of his scientific research is development and research of data collection and analysis systems. E-mail: andreystreltsov@bk.ru

Galina Aleksandrovna Frantsuzova, D.Sc. (Eng.), professor, Department of Automation, NSTU. The main field of her scientific research is analysis and synthesis of nonlinear automatic control systems. E-mail: frants@ac.cs.nstu.ru

Evgeniy Aleksandrovich Basinya, Ph.D., an associate professor of the Department of Cryptology and Cybersecurity, MEPhI and Department of Automation NSTU. The main field of scientific his research is development of automated systems for collecting and processing results. E-mail: basinya@corp.nstu.ru

DOI: 10.17212/2782-2001-2023-1-101-113

Development of a system for collecting, processing, analyzing, identifying and correlating events in the information infrastructure of the enterprise[*]

A.S. STRELTSOV[1,a], *G.A. FRANTSUZOVA*[1,b], *E.A. BASINYA*[1,2,c]

[1] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation*

[2] *National Research Nuclear University "MEPhI", 31 Kashirskoye hwy., Moscow, 115409, Russian Federation*

[a] *andreystreltsov@bk.ru* [b] *frants@ac.cs.nstu.ru* [c] *basinya@mail.ru*

Abstract

A system for collecting, processing, analyzing, and identifying correlation of events of the enterprise information infrastructure known as SIEM, is proposed for consideration.

With the development of corporate information systems, the number of threats related to the violation of accessibility, integrity, and confidentiality in them has increased tenfold. Ensuring information security is a complex task of responding, investigating, and eliminating the consequences of information security incidents (IS).

The paper proposes a formalized description of the data that the proposed system uses. In addition, the general architecture and algorithm of functioning are highlighted. Special attention is paid to a detailed description of one of the main parts of the system (data collection agents).

The information collection subsystem is characterized by the type of information collected: data on the operation of the application, host, and network or on inter-network interactions. A subsystem of this class accumulates heterogeneous data on a system or network to further analyze them for signs of computer attacks. To collect data, special modules -sensors and agents -are used, Tthe former are usually used to monitor network activity, and the latter are used to monitor and analyze actions in a particular system.

The practical application of the improved model is possible both in the framework of research work and in automated information security control systems. The results obtained will be used in the further design of a complex system of continuous monitoring of the enterprise infrastructure. It is planned to consider the data storage subsystem. Subsequent work on the topic will allow us to specify the architecture and algorithm of functioning.

Keywords: log processing systems, intrusion detection systems, detection and response systems, security information collection and event management systems, IDS, IPS, SIEM, administration, information security

REFERENCES

1. Basinya E.A. Raspredelennaya sistema sbora, obrabotki i analiza sobytii informatsionnoi bezopasnosti setevoi infrastruktury predpriyatiya [Distributed system of collecting, processing, and analysis of security information events of the enterprise network infrastructure]. *Bezopasnost' informatsionnykh tekhnologii = IT Security*, 2018, vol. 25, no. 4, pp. 42–51.

2. Rybolovlev D.A., Karasev S.V., Polyakov S.A. Klassifikatsiya sovremennykh sistem upravleniya intsidentami bezopasnosti [Classification of modern security incident management systems]. *Voprosy kiberbezopasnosti = Cybersecurity Issues*, 2018, no. 3 (27), pp. 47–53.

3. Khudainazarov Yu.K., Permyakov A.S., Lepeshkin E.O. [Tasks of the intelligent monitoring system for the information security of the infotelecommunication network]. *XVIII Vserossiiskaya*

[*] *Received 17 November 2022.*

nauchnaya konferentsiya «Neirokomp'yutery i ikh primenenie» [Neurocomputers and their application]. Moscow, 2020, pp. 198–200. (In Russian).

4. Korolev I.D., Popov V.I., Larionov V.A. Analiz problematiki sistemy upravleniya informatsiei i sobytiyami bezopasnosti v informatsionnykh sistemakh [Analysis of the problems of information management and security events in information systems]. *Innovatsii v nauke = Innovations in Science*, 2018, no. 12 (88), pp. 19–26.

5. Cinque M., Cotroneo D., Pecchia A. Challenges and directions in security information and event management (SIEM). *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*. IEEE, 2018, pp. 95–99.

6. Melnik E.V., Klimenko A.B. Primenenie kontseptsii «tumannykh» vychislenii pri proektirovanii vysokonadezhnykh informatsionno-upravlyayushchikh sistem [A fog-computing concept applying for high-reliable management information system design]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki = News of the Tula state university. Technical sciences*, 2020, no. 2, pp. 273–283.

7. Sievierinov O., Ovcharenko M. Analysis of correlation rules in Security information and event management systems. *Computer and Information Systems and Technologies*, April 22–23, 2020. Kharkiv, 2020, pp. 24–25.

8. Sizov V.A., Kirov A.D. Problemy vnedreniya SIEM-sistem v praktiku upravleniya informatsionnoi bezopasnost'yu sub"ektov ekonomicheskoi deyatel'nosti [Problems of implementing SIEM systems in the practice of managing information security of economic entities]. *Otkrytoe obrazovanie = Open Education*, 2020, vol. 24, no. 1, pp. 69–79.

9. Sadowski G., Kavanagh K., Bussa T. *Critical capabilities for security information and event management*. Gartner Group Research Note, 2020.

10. Markin D.O., Makeev S.M., Izotov N.V., Androsov A.Yu. Sistema identifikatsii informatsionnykh ugroz na osnove otkrytykh dannykh seti internet [The system for identifying information threats based on open data from the Internet]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki = News of the Tula state university. Technical sciences*, 2020, no. 9, pp. 86–94.

11. Kotenko I., Khmyrov S.S. Analiz modelei i metodik, ispol'zuemykh dlya atributsii narushitelei kiberbezopasnosti pri realizatsii tselevykh atak [Analysis of models and techniques used for attribution of cybersecurity violators in the implementation of targeted attacks]. *Voprosy kiberbezopasnosti = Cybersecurity Issues*, 2022, no. 4 (50), pp. 52–79.

12. González-Granadillo G., González-Zarzosa S., Dias R. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*, 2021, vol. 21, no. 14, p. 4759.

13. Gutnikov I.V., Gutnikov K.V. Organizatsiya podsistemy zashchity personal'nykh dannykh na predpriyatii [Organization of personal data protection subsystem at the enterprise]. *Nauchno-prakticheskie issledovaniya = Scientific and practical research*, 2019, no. 8-3, pp. 55–57.

14. Shterenberg S.I., Danilova Yu.S. Razrabotka metodiki vnedreniya i vyyavleniya effektivnosti SIEM-sistemy [Implementation methodology and calculation of the efficiency of a SIEM-system]. *Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tekhnologii i dizaina. Seriya 1, Estestvennye i tekhnicheskie nauki = Vestnik of St. Petersburg State University of Technology and Design. Series 1. Natural and Technical Sciences*, 2020, no. 3, pp. 40–45.

15. Faizulin R.F., Demichev M.S. [Role of the SIEM system in providing information security]. *Reshetnevskie chteniya* [Reshetnev Readings], Krasnoyarsk, 2021, pt. 2, pp. 452–453. (In Russian).

16. Abdenov A., Dronova G., Trushin V. *Sovremennye sistemy upravleniya informatsionnoi bezopasnost'yu* [Modern information security management systems]. Novosibirsk, NSTU Publ., 2017. 48 p.

17. Popkov G.V. Primenenie SIEM reshenii na mul'tiservisnykh setyakh svyazi [Application of SIEM solutions on multi-service communication networks]. *Interekspo Geo-Sibir' = Interexpo Geo-Siberia*, 2019, vol. 9, pp. 61–65.

18. Davdyan T.A. Sovremennye korporativnye resheniya po zashchite informatsii i vyyavleniyu intsidentov informatsionnoi bezopasnosti [Modern corporate solutions for information protection and identification of information security incidents]. *Vestnik nauki*, 2022, vol. 4, no. 11 (56), pp. 232–237. (In Russian).

Для цитирования:

Стрельцов А.С., Французова Г.А., Басыня Е.А. Разработка системы сбора, обработки, анализа, идентификации корреляции событий информационной инфраструктуры предприятия // Системы анализа и обработки данных. – 2023. – № 1 (89). – С. 101–113. – DOI: 10.17212/2782-2001-2023-1-101-113.

For citation:

Streltsov A.S., Frantsuzova G.A., Basinya E.A. Razrabotka sistemy sbora, obrabotki, analiza, identifikatsii korrelyatsii sobytii informatsionnoi infrastruktury predpriyatiya [Development of a system for collecting, processing, analyzing, identifying and correlating events in the information infrastructure of the enterprise]. *Sistemy analiza i obrabotki dannykh = Analysis and Data Processing Systems*, 2023, no. 1 (89), pp. 101–113. DOI: 10.17212/2782-2001-2023-1-101-113.