ИНФОРМАТИКА

Вестник Сыктывкарского университета.
Серия 1: Математика. Механика. Информатика.
Выпуск 4 (33). 2019

УДК 004.4

ВОЗМОЖНОСТИ РЕШЕНИЯ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ ПРОБЛЕМ УПРАВЛЕНИЯ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

Н. Р. Оленева, Д. С. Семяшкина

В статье рассматриваются возможности реализации мероприятий по выявлению инцидентов информационной безопасности посредством регистрации событий безопасности о возможных угрозах и уязвимостях в информационных системах организации. Также приводятся функциональные преимущества SIEM-систем отечественного и зарубежного производства.

Ключевые слова: аналитика безопасности, мониторинг информационных систем, инциденты информационной безопасности, сбор событий безопасности, угроза, уязвимость.

С развитием информационных технологий растет и актуальность проблемы обеспечения информационной безопасности информационных систем. Атакующие технологии развиваются быстрее защитных, и

поэтому любые информационные системы находятся в постоянной опасности. Вместе с развитием функциональных возможностей различных информационных систем развиваются и технические решения, обеспечивающие безопасность их функционирования.

Специалистам в области защиты информации приходится прилагать немало трудовых и временных затрат на поиски уязвимостей в автоматизированных информационных системах. На помощь приходят стремительно развивающиеся программы сбора данных от различных источников событий — SIEM (Security Information and Event Management).

SIEM (Security information event management) — класс систем обеспечения информационной безопасности, появившихся в результате слияния SEM-систем (анализ информации в режиме реального времени) и SIM-систем (анализ уже накопленной информации) [1]. Основной функцией SIEM-систем является анализ информации, поступающей от различных источников событий, таких как системы DLP, средства антивирусной защиты информации, межсетевые экраны, системы учета трафика, сканеры уязвимости и т. д. На основе анализа данных из этих источников выявляются отклонения от нормального функционирования, заданного критериями безопасности, и в случае обнаружения происходит оповещение администратора безопасности.

После установки SIEM-системы подключаются источники событий информационной безопасности и задаются правила обработки данных событий по следующей схеме, представленной на рис. 1 [2].

Российским законодательством в области защиты персональных данных даже предусмотрено обязательное применение SIEM-систем в информационных системах предприятий. Такие требования регламен-

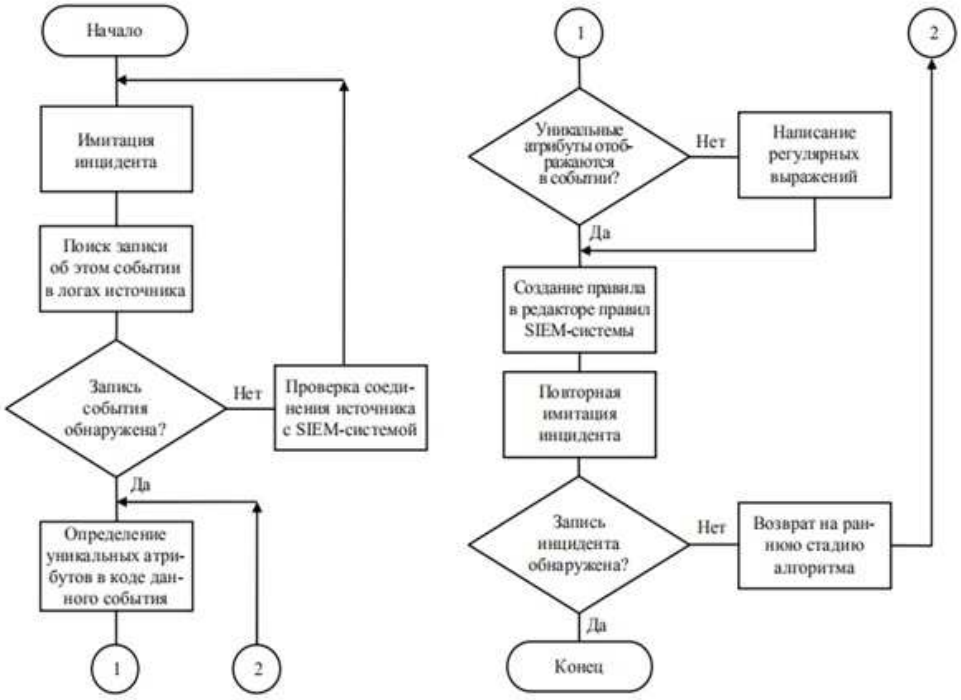

Рис. 1. Схема алгоритма описания правила

тируют: Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и др.

Мировой рынок SIEM-систем достаточно разнообразен. Среди лидеров мирового рынка имеются продукты и отечественного производства, например «НПО «Эшелон»» КОМРАД [1]. Указом Президента РФ «Об утверждении доктрины информационной безопасности РФ» отмечает-

ся, что развитие в отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности по разработке, производству и эксплуатации средств обеспечения информационной безопасности являются национальными интересами в информационной сфере [3].

Проведем сравнительный анализ функциональных возможностей данных технологий среди следующих отобранных систем отечественного и зарубежного производства: Splunk Enterprise Security, IBM Qradar SIEM, HP ArcSight Security Intelligence, FortiSIEM, AlienVault Unified Security Management, Micro Focus ArcSight Data Platform, КОМРАД, MaxPatrol, RuSIEM, Security Capsule SIEM.

Разработки США

Splunk Enterprise Security — это SIEM, основанный из пяти различных структур, которые могут использоваться независимо друг от друга для удовлетворения широкого спектра случаев использования безопасности, включая безопасность приложений, управление инцидентами, расширенное обнаружение угроз, мониторинг в режиме реального времени. Система включает в себя:

– мониторинг в реальном времени;

– назначение приоритетов и принятие мер;

– быстрое расследование;

– многоэтапные расследования.

Решение Splunk ES может быть развернуто в виде программы или облачной службы, в общедоступном или частном облаке [4].

Продукт *IBM Qradar SIEM*. Отвечает за нормализацию и проведение анализа корреляции с целью выявления угроз безопасности. При

помощи механизма Sense Analytics обнаруживает аномалии, раскрывает угрозы и удаляет ложноположительные результаты.

Программа использует опциональное ПО IBM Security X-Force Threat Intelligence для определения действий, связанных с подозрительными IP-адресами, например при подозрении во вредоносной активности [5].

Комплексное решение *HP ArcSight Security Intelligence* компании HP ArcSight включает в себя следующие составляющие решения:

– HP ArcSight Logger — обеспечивает сбор и фильтрацию событий;

– HP ArcSight Threat Response — обеспечивает моментальную реакцию на инциденты путем анализа информации от HP ArcSight ESM, локализацию проблемы и применение ответных мер реагирования;

– HP ArcSight Configuration Management — позволяет провести конфигурацию сетевого оборудования и настроек безопасности;

– HP ArcSight Fraud Detection — решение для выявления и предотвращения мошенничества в области интернет-банкинга и банковских карт [6].

FortiSIEM — технология управления информационной безопасностью и событиями — способствует интеграции сред с адаптивной системой сетевой безопасности. Технология предусматривает создание центра по работе с сетями и обеспечению безопасности с управлением из единого окна. Центр реализует функции отслеживания и сбора актуальных данных об угрозах в рамках всей инфраструктуры.

Разработки Европейских стран

Продукт *AlienVault Unified Security Management* (Испания) сочетает в себе возможности SIEM и управления журналом с другими важными инструментами безопасности, включая обнаружение активов, оценку уязвимости и обнаружение вторжений, чтобы обеспечить централизованный мониторинг безопасности облака, помещения и гибридные среды [7]. AlienVault USM предоставляет:

– единый мониторинг безопасности;

– простое управление безопасностью и отчетность;

– непрерывный мониторинг угроз;

– быстрое внедрение;

– функции безопасности в единой консоли.

Micro Focus ArcSight Data Platform (Великобритания) — это платформа SIEM, которая объединяет сбор информации и управление журналами машинных данных для обеспечения интеллектуальной безопасности. Обладает возможностями интеграции со сторонними платформами Big Data.

Отечественные разработки

SIEM-система *КОМРАД* — разработка российской компании «НПО "Эшелон"». Особенности системы [8]:

– централизованный сбор и анализ данных журналов событий систем защиты информации, автоматизированных рабочих мест, серверов и сетевого оборудования;

– удаленный контроль параметров конфигурации и работы отслеживаемых объектов;

– оперативное оповещение и реагирование на внутренние и внешние

угрозы безопасности автоматизированной системы;

– контроль выполнения заданных требований по безопасности информации, сбор статистики и построение отчетов по защищенности;

– возможность масштабирования решения и создания системы мониторинга информационной безопасности произвольного масштаба;

– интеграция с системами защиты информации.

MaxPatrol SIEM — средство безопасности от производителя Positive Technologies, в основе которого лежит сбор и анализ информации обо всех активах и событиях защищаемой системы в режиме реального времени. Системы класса SIEM, функционал которых предполагает не только сбор данных от различных устройств и приложений, но и автоматическое выявление инцидентов, призваны обеспечить всесторонний мониторинг событий информационной безопасности в информационной инфраструктуре как государственных организаций, так и частных компаний [9].

RuSIEM — российская разработка отечественной компании РУСИЕМ. Решение позволяет организовать централизованный и распределенный сбор событий с систем любого класса, автоматическое обнаружение инцидентов ИТ, ИБ и бизнес-процессов по правилам корреляции и с применением механизмов искусственного интеллекта.

RuSIEM имеет широкий набор визуализаций данных: карту взаимосвязей, выборку по событиям, аналитику, отчеты, инциденты. Решение позволяет отслеживать входы и доступы персонала с новых мест и приложений — из других браузеров, IP–адресов и операционных систем [10].

Система *SIEM «Security Capsule»* предназначена для регистрации,

учета, анализа, корреляции и разбора инцидентов событий ИБ [11]. Обеспечиваются следующие возможности:

– организация сбора и передачи информации о событиях ИБ;

– встроенный «мастер» настройки модулей;

– нормализация событий;

– корреляция событий;

– разбор инцидентов ИБ;

– управление учетными записями пользователей системы;

– хранение информации о событиях ИБ, фильтрация данных по заданным критериям;

– формирование отчетов о событиях ИБ;

– отправка сообщения о событиях ИБ в реальном масштабе времени и по расписанию;

– отправка отчетов о событиях ИБ в зашифрованном виде;

– просмотр и анализ результатов регистрации и реагирование на них;

– восстановление работоспособности системы после сбоев и отказов.

Сравнительная характеристика SIEM-систем отечественного и зарубежного производства представлена в табл. 1.

Таблица 1

Сравнительная характеристика SIEM-систем

	Параметр сравнения	Splunk Enterprise Security	IBM Qradar SIEM	HP ArcSight Security Intelligence	Forti SIEM	AlienVault Unified Security Management
1	2	3	4	5	6	7
	Страна	США	США	США	США	Испания
1	Целевой сегмент	Средний и крупный бизнес	Малый и средний бизнес, корпорации	Малый и средний бизнес, корпорации	Корпорации	Средний и малый бизнес, корпорации
2	Платформа	Linux/ Windows	Linux, Windows	Red Hat Enterprise Linux, Windows Server	Linux, Windows	Windows
3	Интерфейс	Английский	Английский, русский	Английский, русский	Английский	Английский, русский
4	Отчетность	+	+	+	+	+
5	Сбор событий	+	+	+	+	+
6	Обновление баз угроз	–	+	+	+	+

Продолжение таблицы 1

1	2	3	4	5	6	7
7	Принцип работы	Сбор и последующий анализ событий	Сбор и анализ событий	Сбор и последующий анализ событий	Сбор и анализ событий	Сбор и анализ событий
8	Мониторинг	+	+	+	+	+
9	Оповещение об инцидентах	+	+	+	+	+
10	Технология клиент-сервер	+	–	+	–	+
11	Управление инцидентами	+	+	+	+	+
12	Фильтрация событий	–	+	+	+	+
13	Управление хранилищем данных	+	+	+	–	+
14	Стоимость	От 500 тыс. руб.	От 3 млн руб.	От 4 млн руб.	От 500 тыс. руб.	От 300 тыс. руб.
15	Сертификация ФСТЭК	–	–	+	–	–

Продолжение таблицы 1

	Параметр сравнения	Micro Focus ArcSight Data Platform	КОМРАД	MaxPatrol	RuSIEM	Security Capsule SIEM
	8	9	10	11	12	13
	Страна	Великобритания	Россия	Россия	Россия	Россия
1	Целевой сегмент	Крупный и средний бизнес	Крупные корпоративные клиенты, госсектор	Корпоративные клиенты, средний бизнес, госсектор	Малый и средний бизнес, корпорации	Малый и средний бизнес, корпорации
3	Интерфейс	Английский, русский	Русский	Русский	Английский, русский	Русский
4	Отчетность	+	+	+	+	+
5	Сбор событий	+	+	+	+	+
6	Обновление баз угроз	+	+	+	+	–

Окончание таблицы 1

	8	9	10	11	12	13
7	Принцип работы	Сбор и анализ событий	Управление событиями ИБ	Подключение к системе, аутентификация, авторизация, сбор событий	Сбор событий систем любого класса	Syslog, Eventlog, SNMP, SQL, собственный протокол
8	Мониторинг	+	+	+	+	+
9	Оповещение об инцидентах	+	+	+	+	+
10	Технология клиент-сервер	–	+	–	+	+
11	Управление инцидентами	+	+	+	+	+
12	Фильтрация событий	–	–	+	+	+
13	Управление хранилищем данных	+	+	+	+	+
14	Стоимость	От 1 млн руб.	От 200 тыс. руб..	От 3 млн руб.	От 300 тыс. руб.	От 200 тыс. руб.
15	Сертификация ФСТЭК	+	+	+	+	+

Анализ отобранных программных продуктов производился на основании мониторинга сайтов-производителей и сайтов с экспертными оценками. Можно заметить, что российские продукты не уступают в функциональности мировым и способны с ними конкурировать.

Наиболее полным функционалом обладают Splunk Enterprise Security (США), AlienVault Unified Security Management (Испания), КОМРАД, Security Capsule SIEM (Россия), RuSIEM (Россия). Наименьшим функционалом обладают FortiSIEM (США) не обеспечивает управление хранилищем данных, Micro Focus ArcSight Data Platform (Великобритания) отсутствует фильтрация событий.

Рынок SIEM-систем представлен достаточно разнообразно. Каждая SIEM-система обладает своими достоинствами и недостатками. Какой продукт выбрать, решает сам потребитель в зависимости от того какие функциональные возможности необходимы для выполнения поставленных целей и задач. Статистические данные об инцидентах безопасности, собранные системой, позволяют сделать выводы о том, насколько надежно работают применяемые компанией средства защиты и насколько эффективно применение в ней разработанной системы безопасности.

Список литературы

1. **Дрозд А.** Обзор SIEM-систем на мировом и российском рынке [Электронный ресурс] // Сайт Anti-Malware. URL: https://www.antimalware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market (дата обращения: 09.12.2019).

2. **Шабуров А. С., Борисов В. И.** Разработка модели защиты информации корпоративной сети на основе внедрения SIEM-системы // *Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2016. № 19. С. 111–124. [Электронный ресурс] // Научная электронная библиотека «КиберЛенинка». URL: https://cyberleninka.ru/article/n/razrabotka-modeli-zaschity-informatsii-korporativnoy-seti-na-osnove-vnedreniya-siem-sistemy/viewer (дата обращения: 09.12.2019).*

3. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 N 646 [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 09.12.2019).

4. SIEM для обеспечения безопасности на основе аналитики [Электронный ресурс] // Сайт компании Splunk. URL: https://www.splunk.com/ru_ru/products/premium-solutions/splunk-enterprise security.html (дата обращения: 09.12.2019).

5. На страже безопасности: IBM QRadar SIEM [Электронный ресурс] // Сайт Habr. URL: https://habr.com/company/muk/blog/325330/ (дата обращения: 09.12.2019).

6. HP Arcsight [Электронный ресурс] // Сайт компании Hewlett Packard Enterprise. URL: http://arcsight-russia.ru/products-hp-arcsight/products-hp-arcsight (дата обращения: 09.12.2019).

7. **Alien Vault** Unified Security Management [Электронный ресурс] // Сайт AlienVault. URL: https://alienvault.ru/products/ (дата обращения: 09.12.2019).

8. КОМРАД [Электронный ресурс] // Эшелон. URL: https://npo-echelon.ru/production/65/11174 (дата обращения: 09.12.2019).

9. MaxPatrol SIEM [Электронный ресурс] // SIEM. URL: http://siem.su/MaxPatrol_SIEM.php (дата обращения: 09.12.2019).

10. **Сапрыкина А.** Обзор мирового и российского рынка SIEM-систем 2017 [Электронный ресурс] // Сайт Anti-Malware. URL: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem (дата обращения: 09.12.2019).

11. Security Capsule SIEM [Электронный ресурс] // ООО «ИТБ». URL: https://www.itb.spb.ru/docs/SC/Security_Capsule_SIEM_Description_of_application.pdf (дата обращения: 09.12.2019).

Summary

Oleneva N. R., Semyashkina D. S. Possibilities of solving by information systems problems of information security events management in organizations

The paper discusses the possibilities of implementing measures to identify information security incidents by registering security events about

potential threats and vulnerabilities in the organization's information systems. The functional advantages of SIEM-systems are observed.
Keywords: security analytics, information systems monitoring, information security incidents, security event gathering, threat, vulnerability.

References

1. Drozd Aleksey, Obzor SIEM-sistem na mirovom i rossiyskom rynke (Overview of SIEM systems in the world and Russian markets) [Electronic resource], Anti-Malware site: Access mode: https://www.antimalware.ru/ analytics/Technology_Analysis/ Overview_SECURITY_systems_global_and_Russian_market (date of the application: 09.12.2019).

2. **Shaburov A. S., Borisov V. I.**, Razrabotka modeli zashchity informatsii korporativnoy seti na osnove vnedreniya SIEM-sistemy (Development of a corporate network information security model based on the implementation of the SIEM system), *Bulletin of the Perm National Research Polytechnic University. Electrical engineering, information technology, control systems*, 2016, No 19, pp. 111–124 [Electronic resource], Scientific electronic library «CyberLenink». Access Mode: https://cyberleninka.ru/article/n/razrabotka-modeli-zaschity-informatsii-korporativnoy-seti-na-osnove-vnedreniya-siem-sistemy/viewer (date of the application: 09.12.2019).

3. Ukaz Prezidenta RF ot 05.12.2016 N 646 «Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii» (Decree of the President of the Russian Federation of 05.12.2016 N 646 «On approval

of the Doctrine of information security of the Russian Federation») [Electronic resource], Website Consultant Plus. Access Mode: http://www.consultant.ru/document/cons_doc_LAW_208191/ (date of the application: 09.12.2019).

4. SIEM dlya obespecheniya bezopasnosti na osnove analitiki (SIEM for security based on analytics) [Electronic resource], Splunk company website: Access mode: https://www.splunk.com/ru_ru/products/premium-solutions/splunk-enterprise security.html (date of the application: 09.12.2019).

5. Na strazhe bezopasnosti: IBM QRadar SIEM (Security Watch: IBM QRadar SIEM) [Electronic resource], Habr website: Access mode: https://habr.com/company/muk/blog/325330/ (date of the application: 09.12.2019).

6. HP Arcsight [Electronic resource], Hewlett Packard Enterprise website: Access mode: http://arcsight-russia.ru/products-hp-arcsight/products-hp-arcsight (date of the application: 09.12.2019).

7. AlienVault Unified Security Management [Electronic resource], Alien Vault website: Access mode: https://alienvault.ru/products/ (date of the application: 09.12.2019).

8. COMRAD [Electronic resource], Echelon: Access mode: https://npo-echelon.ru/production/65/11174 (date of the application: 09.12.2019).

9. MaxPatrol SIEM [Electronic resource], SIEM: Access mode: http://siem.su/MaxPatrol_SIEM.php (date of the application:

09.12.2019).

10. Saprykina Anastasia, Obzor mirovogo i rossiyskogo rynka SIEM-sistem 2017 (Overview of the global and Russian market of SIEM systems 2017) [Electronic resource], Anti-Malware site: Access mode: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and- russian-market-siem (date of the application: 09.12.2019).

11. Security Capsule SIEM [Electronic resource], ITB LLC: Access mode: https://www.itb.spb.ru/docs/SC/Security_Capsule_SIEM_ Description_of_application.pdf (date of the application: 09.12.2019).

Для цитирования: Оленева Н. Р., Семяшкина Д. С. Возможности решения информационными системами проблем управления событиями информационной безопасности в организации // *Вестник Сыктывкарского университета. Сер. 1: Математика. Механика. Информатика. 2019. Вып. 4 (33). С. 68–85.*

For citation: Oleneva N. R., Semyashkina D. S. Possibilities of solving by information systems problems of information security events management in organizations, *Bulletin of Syktyvkar University. Series 1: Mathematics. Mechanics. Informatics*, 2019, 4 (33), pp. 68–85.

СГУ им. Питирима Сорокина *Поступила 09.12.2019*