УДК 004.046 **Информационные технологии**

Шабля Владимир Олегович, *аспирант, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, г. Краснодар*
Коноваленко Сергей Александрович*, канд. техн. наук, старший преподаватель, Краснодарское высшее военное училище, г. Краснодар*
Едунов Роман Владимирович*, оператор, Краснодарское высшее военное училище, г. Краснодар*

АНАЛИЗ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ SIEM-СИСТЕМ

Аннотация: В статье определен обобщенный перечень базовых функциональных возможностей существующих SIEM-систем, проведен системный анализ существующих отечественных и иностранных технических решений, реализующих базовые функциональных возможности SIEM-систем, а также их специфичных функциональных возможностей и недостатков. Представлена разработанная типовая модель существующей центральной подсистемы сбора, хранения и корреляции событий информационной безопасности системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также описано предназначение ее основных функциональных элементов. Определен типовой перечень технических решений, включаемых в состав подсистемы источников событий информационной безопасности системы обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Ключевые слова: SIEM-система, система обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА), автоматизированная система.

Annotation: The article defines a generalized list of basic functionality of existing SIEM systems, a system analysis of existing domestic and foreign technical

solutions that implement the basic functionality of SIEM systems, as well as their specific functionality and imperfections. The developed typical model of the existing central subsystem for gathering, storage and correlation of information security events of the system for detecting, preventing and eliminating the consequences of computer attacks is presented, and the purpose of its main functional elements is described. A typical list of technical solutions included in the subsystem of sources of information security events of the system for detecting, preventing and eliminating the consequences of computer attacks is determined.

Keywords: SIEM system, system for detecting, preventing and eliminating the consequences of computer attacks, automated system.

В настоящее время система обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА) представляет собой сложную техническую систему, состоящую из разных функциональных подсистем. Одной из таких систем является центральная подсистема сбора, хранения и корреляции событий информационной безопасности (ЦПСХКСИБ) – техническим решением которой является SIEM-система (от англ. Security Information and Event Management system) [1; 2]. Существующая SIEM-система решает одну из основных задач оптимизации структуры СОПКА, а именно – повышение ее эффективности.

В соответствии со сложившейся практикой определим обобщенный перечень базовых функциональных возможностей существующих SIEM-систем [3; 4; 5; 6; 7; 8]:

– сбор, нормализация, фильтрация, агрегация, классификация и кластеризация, корреляция и хранение событий информационной безопасности (СИБ);

– корреляция событий с данными о сетевой активности и уязвимостях автоматизированной системы (АС);

– выявление и расследование инцидентов информационной безопасности (ИИБ);

– оценка рисков, прогнозирование последствий ИИБ;

– учет данных об угрозах безопасности информации;

– наглядное визуализированное предоставление многоуровневых и разноплановых данных (отчеты, графики и т.п.);

– разноплановое информирование специалистов по защите информации (ЗИ).

На основе вышеуказанного проведем системный анализ существующих отечественных и иностранных технических решений, реализующих базовые функциональных возможности SIEM-систем, который сведем в таблицу 1 [3; 4; 5; 6; 7; 8].

Таблица 1 – Системный анализ существующих отечественных и иностранных технических решений SIEM-систем

Типовые функции SIEM-систем	SIEM-системы отечественного производства			SIEM-системы иностранного производства		
	РАМС ИБ	MaxPatrol SIEM	RuSIEM	ArcSight ESM	IBM QRadar	Alien Vault SIEM (OSSIM)
сбор, нормализация, фильтрация, агрегация, классификация и кластеризация, корреляция и хранение СИБ	+	+	+/–	+	+	+
корреляция событий с данными о сетевой активности и уязвимостях АС	+	+	+	+	+\–	+
выявление и расследование ИИБ	+\–	+	+\–	+	+\–	+\–
оценка рисков, прогнозирование последствий ИИБ	+	+\–	+\–	+	+	+
учет данных об угрозах безопасности информации	+	+	+	+	+	–

наглядное визуализированное предоставление многоуровневых и разноплановых данных	+	+	+	+	+	+/–
разноплановое информирование специалистов по ЗИ	+	+	–	+\–	+	–

Заметим, что техническим решениям SIEM-систем, представленным в таблице 1, кроме базовых функциональных возможностей также присущи и специфичные функциональные возможности, и недостатки, которые представим в таблице 2 [3; 4; 5; 6; 7; 8].

Таблица 2 – Специфичные функциональные возможности и недостатки существующих отечественных и иностранных технических решений SIEM-систем

Наименование SIEM-системы	Специфичные функциональные возможности	Недостатки
SIEM-системы отечественного производства		
РАМС ИБ	удаленное реагирование на появившийся ИИБ, что делает АС более безопасной и отказоустойчивой за счет своевременной ликвидации последствий КА; модульная архитектура, упрощающая применение в территориально-распределенных АС, в том числе имеющих изолированные автоматизированные рабочие места и сегменты (гибкая архитектура внедрения); возможность подключения серверов по иерархической схеме и осуществление передачи сообщений между уровнями в зависимости от некоторых условий (например, важности СИБ); надежность передачи сообщений (гарантия доставки сообщений, их криптографическая защита, независимость от среды передачи, использование альтернативных маршрутов, изолированные сети и хосты).	отсутствует возможность автоматизированного и удаленного обновления элементов SIEM-системы; отсутствует возможность конструирования правил корреляции из составных блоков; не использует алгоритмы машинного обучения; отсутствует возможность кластеризации компонентов SIEM-системы.
MaxPatrol SIEM	использование и возможность формирования пользователями	отсутствует возможность конструирования правил

	собственных даш-бордов, т.е. аналитических панелей с понятным интерфейсом для интерактивного взаимодействия с показателями о СИБ, ИИБ, срабатывании правил; детальная инвентаризация ресурсов путем пассивного и активного сбора информации о каждом активе на любой момент времени; использование пакетов экспертизы готовых правил, снижающих потребность в мониторинге актуальных КА и написании собственных правил специалистами по ЗИ), сформированных на основе мониторинга новых угроз, изучении КА и расследовании сложных ИИБ; возможность ретроспективного анализа (по индикаторам компрометации и правилам корреляции); отслеживание состояние ИБ и выявление распределенных КА на отдельное подразделение или на организацию в целом; наличие простого конструктора правил для выявления ИИБ, позволяющего выбирать необходимые СИБ и настроить их последовательность, настраивать условия для срабатывания правил; возможность гибкой настройки мониторинга источников СИБ (ИСИБ) с учетом их типичной активности; использование пользователями 11-шагового чек-листа с инструкциями и ссылками на подробные материалы по настройке системы; автоматическое построение топологии сети на основе модели инфраструктуры АС, позволяющее специалисту по ЗИ лучше понимать защищаемый объект.	корреляции из составных блоков (отсутствует графический конструктор правил корреляции); отсутствие эвристических механизмов анализа СИБ, механизмов глубокого анализа СИБ с поиском аномалий; отсутствует возможность удаленного ограничения доступа в случае нарушения политик ИБ; отсутствует возможность централизованной удаленной установки клиента.
RuSIEM	применение современных аналитических подходов, позволяющих обнаруживать отдельные угрозы и аномалии без созданных для этих случаев правил корреляции; большая база предустановленных правил корреляции (более 270);	сравнительно малое количество даш-бордов по сравнению с другими SIEM-системами; отсутствие сжатия информации о СИБ при передаче, что снижает оперативность системы;

	наличие универсальных коннекторов позволяющих подключать новые ИСИБ в кратчайшие сроки; гибкие правила корреляции, позволяющие описать любые сложные механизмы и скрипты реагирования; модульные варианты развертывания, позволяющие снизить затраты; горизонтальная (для наращивания производительности) и вертикальная (для подключения территориально удаленных объектов АС) масштабируемость системы; распределенная корреляция без необходимости сбора СИБ в одном узле; встроенный инцидент-менеджмент по ITIL, включающий постановку задач, ограничение видимости ИИБ, эскалацию ИИБ.	отсутствует оповещение об ИИБ с помощью скриптов, SMS, API, по электронной почте (оповещение происходит только по каналам SMTP); отсутствует агрегация событий по типу; отсутствует автоматическое принятие решений в рамках процесса обработки ИИБ; отсутствие формул расчета рисков (риск определяется суммой из одного или нескольких симптомов с весами и правилами корреляции); отсутствует возможность определения критичности актива; отсутствует ретроспективная корреляция; отсутствует интеграция с ITSM/CMDB и импорт IOC по сравнению с другими SIEM-системами.
SIEM-системы иностранного производства		
ArcSight ESM	наличие механизма создания коннекторов для приложений и устройств, не входящих в список разработанных коннекторов для более чем 300 устройств и приложений; наличие механизма, обеспечивающего получение готовых к работе решений с преднастроенным набором самых распространенных правил, сигналов тревоги и отчетов о СИБ и ИИБ; мониторинг и анализ СИБ на различных уровнях модели OSI в режиме реального времени; наличие большого количества различных дополнительных пакетов, позволяющих контролировать выполнение международных стандартов, таких как PCI DSS, SOX, NIST, ISO 27002:2005, HIPAA и др.; поставка в виде программного решения или в виде программно-аппаратного комплекса.	отсутствует интерфейс по созданию собственных коннекторов и правил корреляции при наличии функционала.
IBM QRadar	наличие механизма, позволяющего	отсутствует программно-

	пользователям создавать приложения, расширяющие возможности системы; поддерживает интеграцию дополнительных источников данных об угрозах с помощью STIX/TAXII; включает в себя средства аналитики угроз, которые анализируют данные о сети, конечных точках, ресурсах, пользователях, рисках и угрозах для точной идентификации известных и неизвестных угроз; несколько вариантов развертывания в виде программного и программно-аппаратного комплекса или виртуальной машины для локальных сред или IaaS); централизованный доступ к журналам, потокам данных и событиям в локальных и гибридных мультиоблачных средах, SaaS и IaaS с помощью сотен готовых средств интеграции; простые процедуры сбора журналов любых облачных служб посредством REST API; оснащение специалистов по ЗИ инструментами интеллектуального расследования, позволяющими автоматизировать сортировку и классификацию, что ускоряет расследование в 60 раз; автоматизация подготовки отчетов о нормативном соответствии с помощью готовых шаблонов основных нормативных актов.	аппаратная реализация; не поддерживает технологию клиент-сервер; отсутствует возможность централизованной удаленной установки клиента.
Alien Vault SIEM (OSSIM)	открытый исходный код; программное, программно-аппаратное и облачное исполнение; модульная архитектура; единый центр управления для территориально-распределенных объектов.	не поддерживает мониторинг облачных платформ (например, AWS или Azure); отсутствует управление логами, визуализация, автоматизация и интеграция со сторонними сервисами.

Используя базовые и специфичные функциональные возможности технических решений, приведенных в таблицах 1, 2 построим и опишем типовую модель существующей ЦПСХКСИБ СОПКА (рисунок 1).

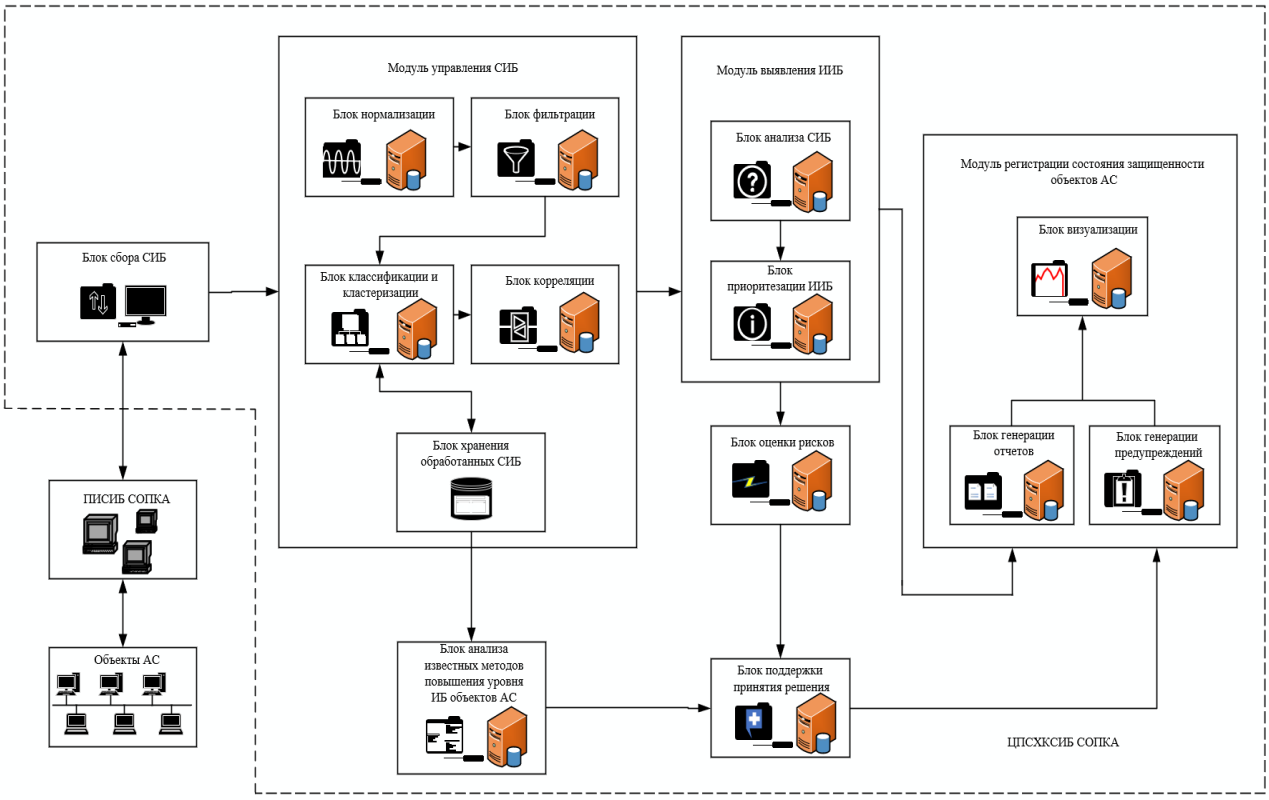

Рисунок 1 – Типовая модель существующей ЦПСХКСИБ

Описание процесса функционирования модели, существующей ЦПСХКСИБ осуществим путем задания предназначений ее модулей и блоков (таблица 3).

Таблица 3 – Предназначение основных функциональных элементов типовой ЦПСХКСИБ

Функциональные элементы SIEM-системы	Предназначение
Блок сбора СИБ	обеспечивает получение потока данных от подсистемы источников событий информационной безопасности (ПИСИБ). При этом могут использоваться два основных метода сбора: прямой и обратный. В прямом методе – ПИСИБ посылает данные самостоятельно. При обратном методе – блок сбора СИБ запрашивает данные от ПИСИБ.
Модуль управления СИБ	блок нормализации осуществляет приведение СИБ к единообразному виду для последующей централизованной обработки; блок фильтрации обеспечивает требуемую полноту представления данных обо всех потенциальных критических СИБ и возможность исключения дублирующих событий, ошибочной и избыточной информации; блок классификации и кластеризации обеспечивает

	выявление логических связей между анализируемыми СИБ, формируя обобщающие признаки и кластеры (группы) СИБ; блок корреляции обеспечивает выявление скрытых отношений между различными СИБ, происходящими в разное время и на разных объектах АС; блок хранения обработанных СИБ используется для хранения отфильтрованных и нормализованных данных о СИБ, в последующем используемых для принятия решения о состоянии защищенности объектов АС.
Модуль выявления ИИБ	блок анализа СИБ обнаруживает факт возникновения ИИБ на объекте АС; блок приоритезации ИИБ определяет значимость и критичность ИИБ на основании заданных правил.
Блок оценки рисков	обеспечивает прогнозирование состояния защищенности объекта АС и определение соответствующей ему степени угрозы на основании анализа последствий ИИБ.
Блок поддержки принятия решения	Обеспечивает определение текущего состояния защищенности объектов АС и выработку мер, направленных на ликвидацию последствий выявленных ИИБ.
Блок анализа известных методов повышения уровня ИБ объектов АС	представляет собой базу знаний об известных методах противодействия КА, способах закрытия уязвимостей и других аспектах проведения мероприятий по повышению уровня ИБ, в последующем используемых для принятия решения о состоянии защищенности объектов АС.
Модуль регистрации состояния защищенности объектов АС	блок генерации отчетов генерирует отчеты о СИБ и формирует карточки ИИБ; блок генерации предупреждений формирует предупредительные сигналы об выявленных ИИБ; блок визуализации обеспечивает представление в графическом или печатном виде данных, характеризующих состояние защищенности объектов АС.

Далее, в дополнение к описанию процесса функционирования типовой ЦПСХКСИБ СОПКА (таблица 3) определим типовой перечень технических решений, включаемых в состав ПИСИБ СОПКА:

- антивирусные приложения, генерирующие события о работоспособности ПО, базах данных, изменении конфигураций и политик, вредоносном ПО;

- межсетевые экраны, предоставляющие сведения об КА, вредоносном ПО и прочем;

- сканеры уязвимостей, предоставляющие данные об уязвимостях системы, инвентаризации активов, сервисов, ПО, поставке инвентаризационных данных,

топологической структуры;

- системы web-фильтрации, предоставляющие данные о посещении или попытки посещения пользователями подозрительных или запрещенных сайтов;

- системы инвентаризации, поставляющие данные для контроля активов в инфраструктуре и выявление новых активов;

- сетевое активное оборудование, используемое для контроля доступа, учета сетевого трафика;

- журналы событий серверов и автоматизированных рабочих мест должностных лиц, применяемые для контроля доступа, обеспечения непрерывности, соблюдения политик информационной безопасности;

- IDS/IPS-системы, предоставляющие данные о сетевых атаках, изменении конфигурации и доступа к устройствам;

- DLP-системы, предоставляющие данные о попытках инсайдерских утечек, нарушении прав доступа;

- системы авторизации и аутентификации, применяемые для мониторинга контроля доступа к информационным системам, и использования привилегии;

- другие источники СИБ.

Таким образом, проведенный анализ процесса функционирования технических решений, включенных как в состав анализируемой ЦПСХКСИБ СОПКА, так и в состав ПИСИБ СОПКА, свидетельствует, что несмотря на достаточно расширенный перечень их функциональных возможностей они не способны осуществлять анализ состояния процесса функционирования специализированных средств СОПКА в целом. При этом указанный функциональный недостаток оказывает существенное влияние на эффективность алгоритмов, способных обеспечить синтез оптимальной структуры СОПКА на АС и обосновывает практическую значимость дальнейшего проведения исследования по изучению существующих моделей, методик, способов и алгоритмов, описывающих исследуемый процесс.

Библиографический список:

1. Кузнецова, А.Д. Обзор состояния исследований информационной безопасности и применение SIEM-систем / А.Д. Кузнецова, Д.В. Сахаров // Актуальные проблемы в инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-методической конференциями: в 4 т., Санкт-Петербург, 27-28 февраля 2019 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. Проф. М.А. Бонч-Бруевича, 2019. – С. 626-631.

2. Кравцов, А. А. SIEM – инструмент управления информационной безопасностью / А. А. Кравцов // Студенческая наука: современные реалии: сборник материалов VII Международной научно-практической конференции, Чебоксары, 11 декабря 2018 года. – Чебоксары: Общество с ограниченной ответственностью “Центр научного сотрудничества “Интерактив плюс”, 2018. – С. 59-67. DOI 10/21661/r-474921.

3. Система регистрации, анализа и мониторинга событий информационной безопасности (Система РАМС ИБ) [Электронный ресурс] // Центр Специальной Системотехники [Офиц. сайт]. Режим доступа: http://www.ssec.ru/2014-rams-ib.htm (дата обращения 30.04.2022).

4. MaxPatrol Security Information and Event Management (MaxPatrol SIEM) [Электронный ресурс] // Positive Technologies [Офиц. сайт]. Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/products/mpsiem/MP-SIEM_PB_A4_15-2021.pdf (дата обращения 30.04.2022).

5. RuSIEM [Электронный ресурс] // RuSIEM [Офиц. сайт]. Режим доступа: https://rusiem.com/ru/products/rusiem (дата обращения 30.04.2022).

6. ArcSight ESM [Электронный ресурс] // Microfocus [Офиц. сайт]. Режим доступа: https://www.microfocus.com/ru-ru/products/siem-security-information-event-management/overview (дата обращения 30.04.2022).

7. IBM QRadar [Электронный ресурс] // IBM [Офиц. сайт]. Режим доступа: https://www.ibm.com/ru-ru/qradar/security-qradar-siem (дата обращения 30.04.2022).

8. Alien Vault SIEM (OSSIM) [Электронный ресурс] // Cybersecurity [Офиц. сайт]. Режим доступа: https://cybersecurity.att.com/products/ossim (дата обращения 30.04.2022).