Воронежский институт МВД России

М. М. Жуков
А. О. Авсентьев

МЕХАНИЗМЫ И СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Учебно-методическое пособие

Воронеж

2024

ББК 32.972
Ж86

Рецензенты:

Г. К. Усков – заведующий кафедрой электроники физического факультета ВГУ, доктор физико-математических наук, профессор;

А. С. Бовкун – заместитель начальника отдела специальных и физико-химических экспертиз ЭКЦ ГУ МВД России по Воронежской области, подполковник полиции.

Жуков М. М.

Ж86 Механизмы и способы защиты информации в распределенных информационных системах : учебно-методическое пособие / М. М. Жуков, А. О. Авсентьев. – Воронеж : Воронежский институт МВД России, 2024. – 67 с.

ISBN 978-5-00229-139-7

В пособии рассматриваются вопросы применения системы управления инцидентами безопасности Security Capsule SIEM, содержатся теоретические сведения, необходимые для изучения дисциплины, темы с перечнем основных вопросов.

Предназначено для обучающихся по специальностям (направлениям подготовки), связанным с противодействием кибер-атакам.

Ж-47-42(1)-24 **ББК 32.972**

ISBN 978-5-00229-139-7

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В настоящее время во всем мире актуален вопрос обеспечения безопасности государства на всех уровнях. Стратегия государственной национальной политики Российской Федерации на период до 2025 года, утверждённая Указом Президента РФ от 6 декабря 2020 года № 703, одним из основных направлений деятельности государственных органов декларирует укрепление государственной безопасности. Согласно данной стратегии органы внутренних дел отдают приоритет созданию комплекса мероприятий по защите сведений, составляющих государственную тайну. Это объясняется значительным объемом служебной информации, ежедневно передаваемой сотрудниками правоохранительных органов с использованием современных телекоммуникационных систем [1].

Поскольку перехват или нарушение этой информации может серьезно угрожать национальной безопасности, защита информации и каналов связи становится одной из важнейших задач. Чтобы обеспечить эффективную защиту, органы внутренних дел могут применять различные меры, которые направлены на обеспечение безопасности передаваемой информации и предотвращение утечек или несанкционированного доступа к государственной тайне.

В современном мире информационных технологий обеспечение безопасности цифровых активов является критически важной задачей для компаний всех размеров. Физическая защита объектов инфраструктуры информационных технологий имеет огромное значение в обеспечении безопасности и предотвращении несанкционированного доступа.

Анализ известной литературы и обобщение существующих взглядов на построение SIEM-систем выявляют несколько ключевых классификационных признаков:

– тип используемого хранилища данных;

– метод получения данных от источников событий;

– степень удаленности этих источников;

– способ выявления зависимостей между событиями безопасности;

– метод распространения;

– масштаб внедрения и используемая модель обслуживания.

Эти признаки служат основой для понимания и сравнения различных SIEM-систем, что особенно важно в условиях постоянного роста числа и сложности киберугроз.

В новом подходе к классификации систем управления инцидентами безопасности, изложенном в таблице 1.2, заложена возможность наглядно структурировать и систематизировать ключевые аспекты систем SIEM. Это значительно облегчает анализ таких систем, делая его более открытым и доступным для понимания. Рассмотрим, например, вопрос хранения данных в системах SIEM. Здесь можно встретить как реляционные системы управления базами данных с поддержкой SQL, так и нереляционные хранилища. Это многообразие подходов к хранению информации отражает различные нужды и возможности организаций, реализующих данные системы.

Переходя к деталям, реляционные хранилища обычно основываются на использовании СУБД, поддерживающих SQL. Этот метод предпочтителен многими компаниями за его надежность и четкую структурированность данных. Однако с ростом объемов данных, требуемых для эффективной работы систем управления инцидентами, многие разработчики SIEM все чаще обращают внимание на нереляционные базы данных. Такие хранилища, как системы «ключ-значение» (например, Redis или Amazon DynamoDB), семейства столбцов (Apache Cassandra) или документо-ориентированные базы данных (MongoDB), привлекают своей способностью к масштабированию, высокой надежностью и возможностью параллельной обработки больших массивов информации [19].

В условиях постоянного роста объемов данных и необходимости их эффективной обработки нереляционные хранилища данных становятся всё более популярными. Они позволяют более гибко управлять данными и обеспечивают высокую производительность. В большинстве случаев коммерческие SIEM-системы поддерживают как агентский, так и безагентский способы сбора данных. Преимущество сбора данных без использования агентов заключается в отсутствии необходимости установки и обслуживания дополнительного программного обеспечения на устройствах-источниках событий, что значительно упрощает процесс внедрения.

Однако, несмотря на удобство и простоту безагентского подхода, он имеет свои недостатки. Основным из них является повышенная нагрузка на канал связи между источником и сервером, так как события пересылаются в необработанном виде. Это может привести к задержкам и снижению эффективности обработки данных. В то же время агентский способ сбора данных позволяет выполнять предварительную фильтрацию, агрегацию и нормализацию непосредственно на устройствах-источниках, снижая нагрузку на сервер обработки и улучшая общую производительность системы.

Таким образом, выбор между агентским и безагентским способом сбора данных должен основываться на конкретных потребностях и возможностях организации. Обе методики имеют свои преимущества и ограничения, и оптимальный выбор зависит от множества факторов, таких как объемы данных, доступные ресурсы и требования к скорости обработки информации.

1. СПЕЦИФИКА ФУНКЦИОНИРОВАНИЯ СИСТЕМ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ БЕЗОПАСНОСТИ

1.1. Понятие SIEM-систем

Информационная безопасность в современном мире занимает ключевую позицию в обеспечении стабильности и безопасности бизнеса. В этом контексте системы контроля доступа, объединяющие программные и аппаратные решения, становятся критически важным элементом корпоративной инфраструктуры. Они выполняют функции аутентификации и авторизации, а также мониторят активности пользователей, что позволяет эффективно управлять доступом к ресурсам. Кроме того, антивирусные программы и межсетевые экраны формируют защитный барьер против многочисленных вредоносных угроз, включая троянские программы и кейлоггеры, обеспечивая обнаружение и блокирование потенциально опасного трафика.

В сердце сложной архитектуры управления инцидентами безопасности находятся системы SIM и SEM, которые играют центральную роль в мониторинге и реагировании на угрозы. SIM анализирует данные, выявляя аномалии по отклонениям от установленных норм, в то время как SEM оперативно реагирует на возникновение инцидентов, связывая различные данные и инициируя оповещения при обнаружении аномалий. Интеграция этих технологий приводит к созданию систем SIEM, которые объединяют сбор, анализ и корреляцию данных в единую мощную систему, способную предоставлять комплексный контроль за информационной безопасностью [4].

SIEM-системы проводят глубокий анализ безопасности, интегрируя данные из разнообразных источников, таких как антивирусное программное обеспечение, межсетевые экраны, системы обнаружения вторжений и инструменты предотвращения утечек данных. Эти системы критически важны для идентификации

действий, которые нарушают нормы безопасности или процедуры реагирования на инциденты, так как они собирают и обрабатывают информацию с множества платформ.

Централизация данных, осуществляемая через специализированные агенты и инструменты сбора данных, играет ключевую роль в обеспечении соответствия требованиям безопасности и позволяет провести всесторонний анализ журналов событий.

Расширение спектра источников данных, включая системы контроля доступа и сканеры уязвимостей, расширяет возможности SIEM-систем в области всестороннего анализа безопасности. Это позволяет выявлять случаи несанкционированного доступа, мошенничество и сетевые атаки, которые могут свидетельствовать о взломах или других угрозах. С такими мощными инструментами на руках SIEM-системы становятся неотъемлемой частью стратегий обеспечения безопасности в организациях, предоставляя усовершенствованные средства для управления информационными рисками и повышения уровня защищенности.

1.2. Классификация SIEM-систем

В последнее время в области информационной безопасности наступили весьма значительные перемены, касающиеся методов работы с данными. Разработчики систем мониторинга и анализа, известных под аббревиатурой SIEM, все активнее отходят от использования традиционных реляционных баз данных. Вместо этого они обращаются к более современным и гибким нереляционным системам. Этот стремительный переход обусловлен необходимостью повышения масштабируемости и надежности, а также желанием оптимизировать обработку огромных объемов информации параллельным способом. В современных условиях, когда SIEM-системам необходимо оперативно справляться с масштабными наборами данных, такой шаг становится не просто важным, а прямо-таки критически необходимым [4].

Обратив внимание на классификации и подходы, которые традиционно применялись при построении SIEM-систем, можно выделить несколько заметных изменений. Ранее реляционные базы данных были весьма популярны благодаря их способности структурировать информацию с помощью таблиц и столбцов, что делало их неотъемлемой частью множества IT-систем. Однако они стали показывать свои ограничения, особенно когда речь заходит о масштабируемости и гибкости обработки данных, что привело к поиску более подходящих решений.

На смену приходят нереляционные, или NoSQL, базы данных. Они предлагают значительно больше возможностей для работы с неструктурированными данными и способны обеспечить высокую скорость обработки даже очень больших объемов информации. Благодаря этому такие системы становятся более адаптивными и производительными, что крайне важно для оперативного реагирования на различные инциденты безопасности и обработки массивов логов.

В конечном итоге, текущее направление в развитии SIEM-систем четко подчеркивает важность перехода к нереляционным системам хранения данных. Такая модификация не только значительно повышает производительность и оперативность систем, но и обеспечивает необходимую надежность и масштабируемость, что является критически важным для эффективного мониторинга и анализа в условиях неуклонного роста объемов данных.

Таблица 1.1

Классификации решений SIEM

№	Критерии классификации	Классы классификации	Описание классификатора
1.	Типы хранения информации	КК1.1	Реляционная система управления базами данных (СУБД)
		КК1.2	Нереляционное хранилище данных

№	Критерии классификации	Классы классификации	Описание классификатора
2.	Способ получения данных от источников событий	КК2.1	С использованием приложений-агентов (agent-based)
		КК2.2	Без использования приложений-агентов (agentless)
3.	Показатель удаленности источников событий	КК3.1	С источниками событий в пределах контролируемой зоны
		КК3.2	С территориально распределенными источниками событий
4.	Способ обнаружения зависимостей между отдельными событиями безопасности	КК4.1	Основанный на заранее заданных правилах обработки (rule-based)
		КК4.2	Конечный автомат
		КК4.3	Рассуждение на основе прецедентов
		КК4.4	Байесовская сеть
		КК4.5	Нейронная сеть
5.	Метод распространения	КК5.1	С открытым исходным кодом
		КК5.2	Коммерческий
6.	Размах внедрения	КК6.1	Малый
		КК6.2	Средний
		КК6.3	Крупный
7.	Модель сервиса	КК7.1	Локальная установка
		КК7.2	Как услуга (hosted SIEM, SIEM as a service)

Исследование влиятельных источников в литературе о проектировании систем управления инцидентами безопасности (SIEM) обнаруживает разнообразие классификационных особен-

ностей, отличающих одни системы от других. Эти особенности охватывают аспекты, начиная от типа используемого хранилища данных до способов анализа и распространения собранной информации, включая также уровень доступности источников данных и методы их интеграции.

Данные классификации подробно изложены в таблице, отражающей использование разнообразных хранилищ данных в SIEM-системах, таких как реляционные и нереляционные базы данных. Реляционные базы, поддерживающие SQL, исторически использовались широко, но современные требования к обработке больших объемов данных стимулировали переход к нереляционным моделям, таким как базы данных «ключ-значение», системы управления базами данных на основе столбцов и документо-ориентированные СУБД.

Этот переход содействует улучшению масштабируемости и надежности систем, обеспечивая возможность параллельной обработки информации и повышение общей производительности. В дополнение к изменениям в базах данных, SIEM-системы также адаптировались к использованию как агентных, так и безагентных методов сбора данных. Безагентный сбор, хотя и устраняет необходимость установки дополнительного программного обеспечения, создает дополнительные нагрузки на коммуникационные каналы, поскольку требует передачи необработанных данных напрямую на сервера.

В свете этих изменений современные SIEM-системы демонстрируют гибридный подход в сборе данных, что позволяет оптимизировать как обработку информации, так и нагрузку на инфраструктуру. Этот подход не только соответствует требованиям к масштабируемости и надежности, но и способствует более эффективному управлению ресурсами, обеспечивая высокую производительность при минимальных затратах [5].

Итоги использования системы классификации приводятся в таблице 1.2.

Таблица 1.2

Классификация современных SIEM систем

№	Критерии классификации	Решение SIEM / значение признака (класс классификации)				
		ArcSight ESM	QRadar SIEM	SC SIEM	КОМРАД	OSSIM
1.	Тип хранилища данных	КК1.1 КК1.2	КК1.1	КК1.2	КК1.2	КК1.1
2.	Способ получения данных от источников событий	КК2.1 КК2.2	КК2.1 КК2.2	КК2.1 КК2.2	КК2.1 КК2.2	КК2.1
3.	Показатель удаленности источников событий	КК3.1 КК3.2	КК3.1 КК3.2	КК3.1 КК3.2	КК3.1 КК3.2	КК3.1 КК3.2
4.	Метод выявления зависимостей между отдельными событиями безопасности	КК4.1	КК4.1	КК4.1	КК4.1	КК4.1
5.	Способ распространения	КК5.2	КК5.2	КК5.2	КК5.2	КК5.1
6.	Масштаб внедрения	КК6.3	КК6.3	КК6.3	КК6.3	КК6.2
7.	Модель обслуживания	КК7.1 КК7.2	КК7.1 КК7.2	КК7.1	КК7.1	КК7.1

SIEM является ключевым компонентом в арсенале системы информационной безопасности, играя решающую роль в обнаружении нарушений политик безопасности и сокращении потенциального ущерба от кибератак. Эта технология обеспечивает специалистов по информационной безопасности необходимыми инструментами для оценки уровня защиты информационных систем и определения текущих угроз для организации. Помимо этого, информация, собранная SIEM-системой, служит основой для подготовки отчётности в процессе расследования инцидентов.

Профессионалы в области безопасности подчеркивают, что системы SIEM предназначены для выявления аномалий в работе систем и обеспечения поддержки инструментам для обнаружения вредоносного программного обеспечения. Эти системы эффективно мониторят обмен данными в сети, выявляя любые отклонения путём сравнения наблюдаемых данных с установленными эталонами. Благодаря этим возможностям компании рассматривают SIEM как ценный инструмент, значительно укрепляющий защиту сетевых ресурсов от целенаправленных атак [5].

1.3. Функциональные задачи, типовые сценарии работы и компоненты SIEM

SIEM (Security Information and Event Management) – это передовая система для мониторинга в сфере кибербезопасности, которая позволяет в режиме реального времени анализировать информацию о безопасности, охватывая сетевые устройства и программные приложения. Она играет ключевую роль, позволяя специалистам не только своевременно обнаруживать угрозы, но и незамедлительно реагировать на них, что является решающим для предотвращения потенциальных атак и минимизации возможного ущерба [6].

Включение данных из разнообразных источников SIEM делает возможным мгновенное выявление безопасностных инцидентов. Система не только собирает и анализирует информацию, но и оценивает уровень защищенности информационных и телекоммуникационных ресурсов, способствуя тем самым улучшению управления рисками и усилению защиты. Разработки в области SIEM предлагают сложные инструменты для принятия решений и расследования, что позволяет экспертам быстро и точно реагировать на угрозы, тем самым защищая критически важные активы и поддерживая оперативную готовность при любых обстоятельствах.

Ключевая функция системы – это создание отчетов, которые обеспечивают документирование и прозрачность всех процессов. На примере логов, ведущихся всеми крупными приложениями и операционными системами, можно понять ценность SIEM. Логи регистрируют важные события и изменения в системе, но их локальное хранение снижает их практическую пользу и безопасность. Если злоумышленник вторгается в систему, действия, зарегистрированные в логах, могут быть удалены или изменены. Например, в Windows изменения фиксируются в Event Log, а в Linux – в различных файлах журнала в директории /var/log/. Включение системы SIEM в инфраструктуру IT позволяет централизованно собирать и анализировать эти данные, значительно повышая безопасность [6].

С применением SIEM информационные структуры не только улучшают мониторинг и анализ событий, но и обретают мощные инструменты для расследования инцидентов, что жизненно важно для предотвращения атак и минимизации ущерба. Внедрение таких систем существенно усиливает защиту, делая инфраструктуру более устойчивой к угрозам. В условиях усиления кибератак SIEM становится неотъемлемой частью эффективной стратегии кибербезопасности.

Однако, несмотря на многочисленные преимущества, централизованный сбор событий имеет свои ограничения. Он эффективен только при управлении ограниченным числом узлов. При увеличении объема данных и количества узлов могут возникнуть проблемы с производительностью, что потенциально приводит к потере важных данных. Поэтому критически важно учитывать масштаб сети и обеспечивать достаточные ресурсы для стабильной работы системы [7].

1.4. Обработка событий и направления развития SIEM

SIEM (Security Information and Event Management) расшифровывается как «менеджмент информации и событий безопасности». Этот подход к управлению инцидентами объединяет функции SIM (управление информацией о безопасности) и SEM (управление событиями безопасности) в единую систему для компании [8].

Принцип работы инструментов SIEM заключается в сборе и агрегации информации из множества источников, включая хост-системы, сетевые устройства и приложения, а также средства безопасности, такие как брандмауэры и антивирусные программы. Эти инструменты не только аккумулируют данные, но и осуществляют их сохранение, обработку и анализ для выявления и реагирования на подозрительные активности и угрозы безопасности.

Центральным звеном в системе SIEM является сборщик событий, который может как активно подключаться к различным источникам данных через разнообразные протоколы, так и пассивно принимать информацию, направляемую через такие стандарты, как Syslog или SNMP. Такой подход гарантирует гибкость интеграции с многообразием систем. Сборщик занимается не только агрегацией и нормализацией данных, но и их фильтрацией, преобразуя сырую информацию в стандартизированный формат, что делает возможным дальнейший анализ. Эта обработка данных включает в себя объединение похожих событий для оптимизации ресурсов, унификацию данных для обеспечения их согласованности и отсеивание излишней информации, готовя их к процессу корреляции [9].

В самом сердце системы SIEM находится процесс корреляции, где каждое событие проверяется на соответствие заранее определённым правилам, что позволяет быстро выявлять потенциальные угрозы и эффективно реагировать на них. Например,

серия неудачных попыток входа может сигнализировать о попытке несанкционированного доступа, а отсутствие актуальных обновлений антивирусных баз может указывать на уязвимость. Таким образом, SIEM не просто реагирует на инциденты, но и предупреждает их возникновение, препятствуя ущербу до его наступления.

Ключевым аспектом эффективности системы SIEM является её способность адаптироваться к расширению массива данных, включая интеграцию с облачными платформами и различными устройствами пользователей. Это расширение позволяет системе анализировать более обширный спектр данных, что необходимо для комплексного подхода к обеспечению безопасности, особенно в современном мире, где облачные технологии становятся стандартом. SIEM успешно работает с такими платформами, как AWS, Google Cloud Platform и Microsoft Azure, подчеркивая свою актуальность и важность в условиях постоянно развивающейся цифровой среды [10].

Важный стандарт SIEM-систем – это управление сервиса для эффективного мониторинга, что позволяет не расширять внутренний штаб, а сосредоточиться на информационной безопасностии управлении инцидентами.

2. ИССЛЕДОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ БЕЗОПАСНОСТИ SECURITY CAPSULE SIEM

2.1. Функциональные возможности и архитектура Security Capsule SIEM

Security Capsule SIEM, разработанная специалистами ООО «ИТБ» - Кибербезопасность, представляет собой комплексное решение для мониторинга и корреляции событий информационной безопасности. Эта система обладает функционалом для регистрации, учёта, анализа и корреляции данных, что обеспечивает эффективное выявление инцидентов. Она получила сертификацию от ФСТЭК и внесена в Единый реестр российских программ для ЭВМ и баз данных, подтверждая свою надёжность и соответствие стандартам безопасности.

Security Capsule SIEM применима в широком спектре систем, включая защиту персональных данных, управление технологическими процессами, государственные информационные системы, значимые объекты критической информационной инфраструктуры и системы обнаружения и предупреждения компьютерных атак. Это обеспечивает повышение уровня защиты, что подтверждается наличием сертификации и поддержкой со стороны ведущих государственных организаций.

Система предоставляет множество функций для мониторинга и корреляции событий на любом уровне информатизации – федеральном, региональном или объектном. Она позволяет оперативно информировать Национальный координационный центр по компьютерным инцидентам и других ответственных лиц о возникающих угрозах, что способствует быстрому реагированию и уменьшению потенциальных рисков [11].

Security Capsule SIEM собирает данные о событиях, предотвращая возможные нарушения, оценивает уровень защищённости инфраструктуры, контролирует активные директории и политики.

Система не ограничивает время хранения информации о событиях, что облегчает быструю выгрузку данных. Также система может быть развернута в виртуализированной среде и обеспечивает создание отказоустойчивого кластера, что делает её гибкой в настройке и эксплуатации [12–15].

SC SIEM интегрирует данные с разнообразных источников и мониторит процессную активность, сетевые соединения и файловые операции, что позволяет администраторам эффективно управлять доступом пользователей и минимизировать риски, связанные с человеческим фактором. Система также анализирует и оптимизирует настройки средств защиты, повышая их эффективность.

SC SIEM автоматизирует обработку данных, начиная от сбора информации из различных источников до нормализации и фильтрации событий. Это уменьшает объём ручной работы и позволяет сосредоточиться на наиболее значимых угрозах. Интерфейс системы позволяет администраторам настраивать и дополнять правила корреляции, что обеспечивает адаптивность и гибкость в управлении безопасностью.

В итоге, Security Capsule SIEM является ключевым инструментом в защите информационных систем, предоставляя обширные возможности для анализа, мониторинга и корреляции событий. Это делает систему незаменимой для обеспечения безопасности критически важных инфраструктур, отвечая на вызовы современной кибербезопасности [16,17].

Есть возможность вносить свои изменения в существующие правила нормализации (рис. 2.1).

1. SC Siem Коррелятор – «сердце» системы, осуществляющей выявление инцидентов информационной безопасности в реальном времени и в ретроспективе. Система предоставляет более 3000 правил корреляции. Настройка правил корреляции осуществляют специалист компании РТ, также специалисты партнеров на этапе пуско-наладки работ, не требует дополнительных трудозатрат со

стороны специалистов заказчика. Есть возможность вносить и создавать свои изменения в существующие правила нормализации (рис. 2.1) [18].

Рис. 2.1. Нормализованное событие

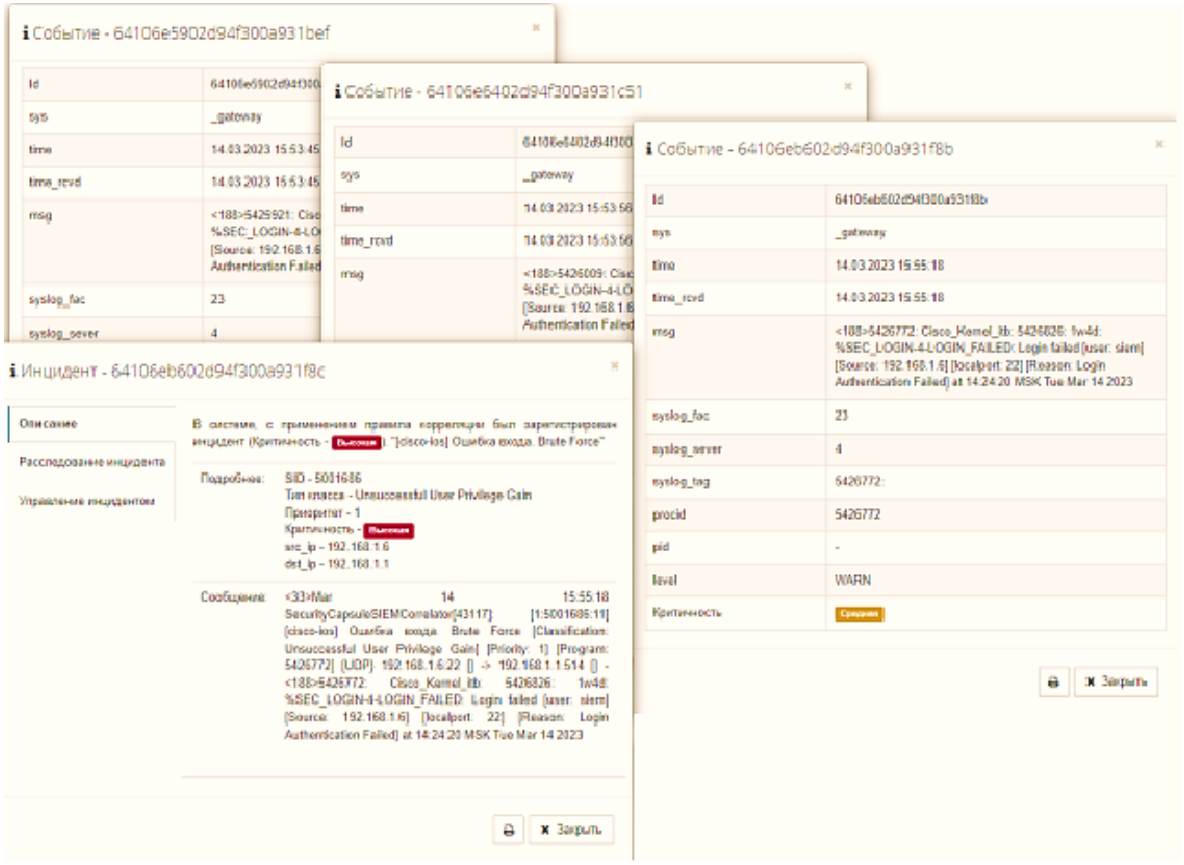

Рис. 2.2. Корреляция инцидента

2. SC Siem Агрегатор – программный модуль, по заданным правилам осуществляет обработку событий однотипных повторяющихся событий с последующим сохранением в базу данных системMongoDB (NoSQL) и PostgreSQL. Технические характеристики зависят от объемов и сроков хранения информации о событиях [18].

3. Отчетность: отдельно стоит отметить удобный механизм формирования отчетов с возможностью сохранения собственных профилей. В основу идеи реализации модуля отчетности были взяты слова итальянского скульптора и художника Микеланджело Буонарроти. На вопрос: «Как вам удается создавать такие великолепные статуи?» – он ответил: «Я беру глыбу мрамора и отсекаю все лишнее» (рис. 2.3) [18].

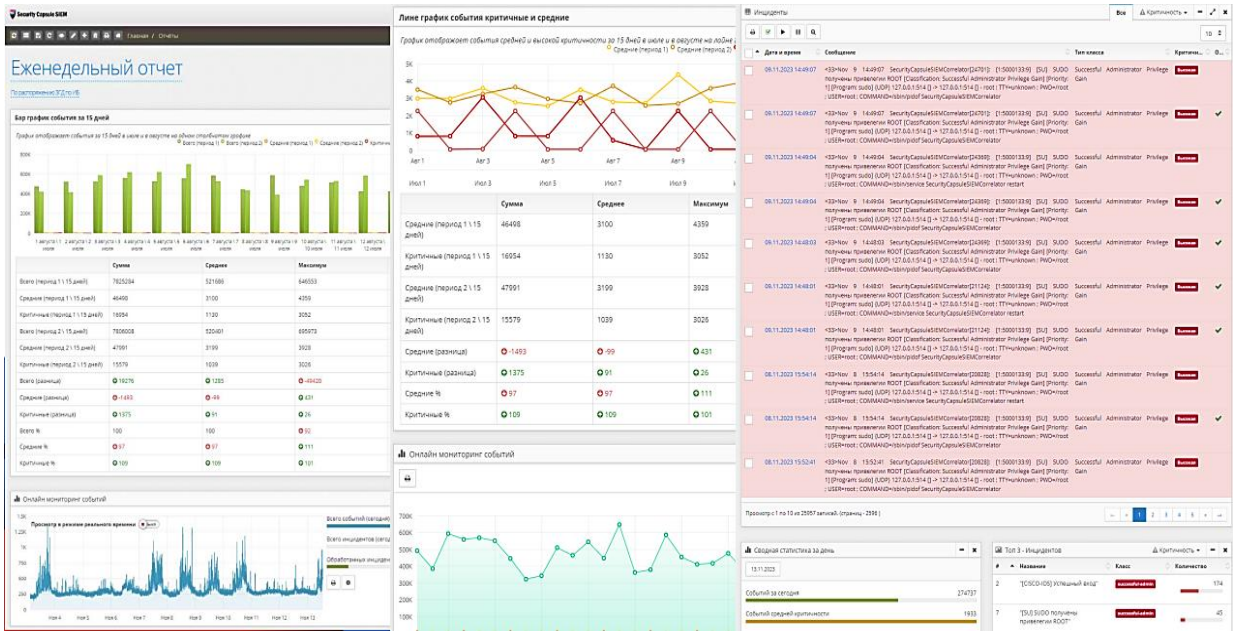

Рис. 2.3. Отчетность

5. Модуль ГосСОПКА – единый территориально распределенный комплекс центров различного масштаба, обменивающихся информацией о кибератаках [18].

6. SC SIEM Хранение – БД RAW событий, нормализованных событий, инцидентов, а также иных системных данных. Технические характеристики оборудования зависят от объемов и сроков хранения информации о событиях, инцидентах и оцениваются на этапе обследования объекта информатизации Заказчика.

7. SC SIEM MITRE ATT&CK – матрица, описывающая тактики и техники целевых атак, применяемых различными киберпреступными группами. SC SIEM позволяет выявлять техники к тактикам (табл. 2.1).

Таблица 2.1

Техники к тактикам

Тактика (ID)	**Техника (ID)**
TA0043: Разведка	T1595: Активное сканирование
TA0042: Подготовка ресурсов	T1584: Компрометация сторонней инфраструктуры
	T1587: Разработка собственных средств

Тактика (ID)	Техника (ID)
TA0001: Первоначальный доступ	T1189: Теневая (drive-by) компрометация
	T1190: Недостатки в общедоступном приложении
	T1133: Внешние службы удаленного доступа
	T1200: Подключение дополнительных устройств
	T1566: Фишинг
	T1195: Компрометация цепочки поставок
TA0002: Выполнение	T1059: Интерпретаторы командной строки и сценариев
	T1203: Эксплуатация уязвимостей в клиентском ПО
	T1559: Межпроцессное взаимодействие
	T1106: Нативный API
	T1053: Запланированная задача (задание)
	T1569: Системные службы
	T1204: Выполнение с участием пользователя
	T1047: Инструментарий управления Windows
TA0003: Закрепление	T1098: Манипуляции с учетной записью
	T1547: Автозапуск при загрузке или входе в систему
	T1037: Сценарии инициализации при загрузке или входе
	T1176: Расширения браузеров
	T1136: Создание учетной записи
	T1543: Создание или изменение системных процессов
	T1546: Выполнение по событию
	T1133: Внешние службы удаленного доступа (дублирование)
TA0004: Повышение привилегий	T1548: Обход механизмов контроля привилегий
	T1134: Манипуляции с токенами доступа
	T1547: Автозапуск при загрузке или входе в систему (дублирование)
	T1546: Выполнение по событию (дублирование)
	T1068: Эксплуатация уязвимостей для повышения привилегий
	T1055: Внедрение кода в процессы

Тактика (ID)	Техника (ID)
TA0005: Предотвращение обнаружения	T1484: Изменение доменной политики
	T1222: Изменение разрешений для файлов и каталогов
	T1564: Сокрытие артефактов
	T1562: Ослабление защиты
	T1070: Устранение индикаторов
	T1202: Непрямое выполнение команд
	T1036: Маскировка
	T1112: Изменение реестра
	T1027: Обфусцированные файлы или данные
	T1055: Внедрение кода в процессы (дублирование)
	T1553: Нарушение работы средств контроля доверия
	T1218: Выполнение с помощью системных бинарных файлов
	T1216: Выполнение через системный сценарий
	T1127: Выполнение через доверенные утилиты разработчика
	T1220: Использование сценариев XSL
TA0006: Получение учетных данных	T1056: Перехват вводимых данных
	T1040: Прослушивание сетевого трафика
	T1003: Получение дампа учетных данных
	T1558: Кража или подделка билетов Kerberos
	T1552: Незащищенные учетные данные
TA0007: Изучение	T1087: Изучение учетных записей
	T1482: Изучение доверительных отношений между доменами
	T1083: Изучение файлов и каталогов
	T1040: Прослушивание сетевого трафика (дублирование)
	T1057: Изучение процессов
	T1012: Запросы к реестру
	T1018: Изучение удаленных систем
	T1518: Изучение установленного ПО
	T1016: Изучение конфигурации сети
	T1049: Изучение сетевых подключений
	T1033: Изучение владельца или пользователей системы

Тактика (ID)	Техника (ID)
TA0008: Перемещение внутри периметра	T1563: Перехват сессии службы удаленного доступа
	T1021: Службы удаленного доступа
TA0009: Сбор данных	T1560: Архивация собранных данных
	T1123: Захват аудиоданных
	T1115: Данные из буфера обмена
	T1114: E-mail Collection \ Сбор эл. почты
	T1056: Input Capture \ Перехват вводимых данных (дублирование)
TA0011: Организация управления	T1071: Протокол прикладного уровня
	T1132: Кодирование данных
	T1001: Обфускация данных
	T1105: Передача инструментов из внешней сети
	T1090: Прокси-сервер
	T1219: ПО для удаленного доступа
TA0010: Эксфильтрация данных	T1020: Автоматизированная эксфильтрация
	T1048: Эксфильтрация по альтернативному протоколу
	T1567: Эксфильтрация через веб-службу
TA0040: Деструктивное воздействие	T1531: Прекращение доступа к учетной записи
	T1485: Уничтожение данных
	T1486: Шифрование данных
	T1496: Несанкционированное использование ресурсов
	T1489: Остановка службы

Специализированные сервисные модули [18]:

- *MongoDB* – БД используемая модулем хранения для организации хранения событий, полученных в результате сканирования модулем сбора

- *Microsoft SQL* – БД для хранения базы знаний, включает в себя данные необходимые для структурирования сведений, собранных от источников событий и объектов инфраструктуры (версия ОС, ПО, службы, типа аппаратного обеспечения), а также обнаруженных уязвимостей.

Настройка и работа системы SC SIEM SIEM осуществляется через веб-интерфейс. Интерфейс понятный и адаптивный. Для всякого пользователя существует своя роль, а возможности ролей могут быть настроены, иными словами, в системе реализована ролевая модель разграничения прав доступа, а также логирование действий пользователя в системе (рис. 2.4.).

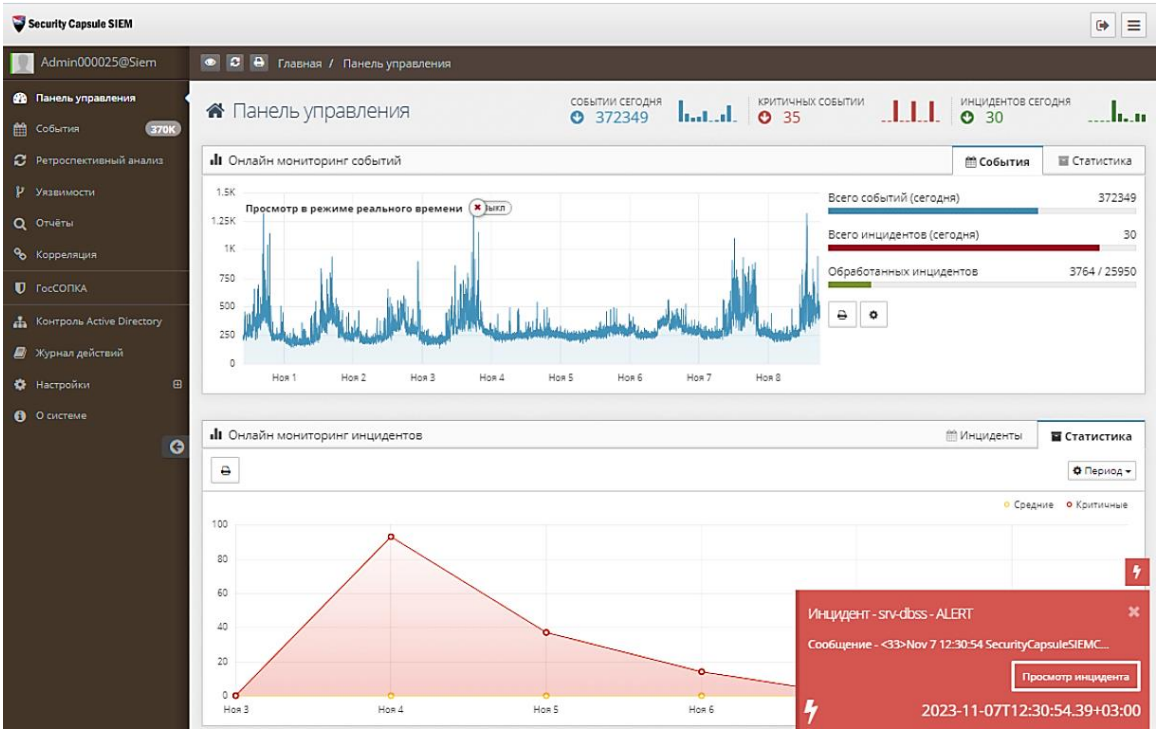

Рис. 2.4. Интерфейс

2.2. Особенности обработки событий информационной безопасности в системе Security Capsule SIEM

Система Security Capsule, являющейся технологией SIEM, для обработки информационных событий показала себя весьма надежной. Она предоставляет ключевые возможности и функции, которые делают ее более эффективной для управления событиями безопасности.

Security Capsule SIEM – это высокотехнологичная платформа для наблюдения за безопасностью, которая собирает и анали-

зирует информацию в режиме реального времени из разнообразных источников, включая брандмауэры, системы для обнаружения и предотвращения вторжений, сетевое оборудование, серверы и приложения. Платформа эффективно взаимодействует с уже существующей инфраструктурой, поддерживая широкий спектр форматов данных и протоколов, в том числе системные журналы, SNMP и HTTP. Основные элементы системы, такие как агенты и соединители, играют ключевую роль в бесперебойной передаче данных [18].

В процессе нормализации данные из многочисленных источников трансформируются в унифицированный формат, упрощая их последующий анализ. Стандартизация данных критична для точного сопоставления и интерпретации информации, что необходимо для корректной работы системы. Важной функцией является механизм корреляции, который проанализировав нормализованные данные, выявляет паттерны, сигнализирующие о потенциальных угрозах. Благодаря продвинутым алгоритмам, машинному обучению и заранее установленным правилам корреляции система становится более чуткой к новым и изменяющимся угрозам.

При обнаружении угрозы система тут же активирует механизмы оповещения, генерируя уведомления, которые ранжируются по степени важности. Способность системы передавать оповещения через различные каналы, включая электронную почту и SMS, обеспечивает, что ответственные лица получат информацию без задержек. Инструменты для управления инцидентами и реагирования на них позволяют командам безопасности оперативно расследовать и нейтрализовать угрозы, предоставляя им всю необходимую информацию и рекомендации.

Дополнительно – система SIEM расширяет свои возможности за счёт интеграции с внешними источниками информации о новых угрозах, позволяя быстро реагировать и анализировать их в контексте уже известных данных. Анализ поведения пользователей и устройств, внедрённых в систему, значительно улучшает

обнаружение угроз, создавая поведенческие профили для каждого пользователя и устройства, что помогает выявлять необычные действия. Автоматизация процесса реагирования и оркестрация действий сокращают время между обнаружением и нейтрализацией угрозы, давая возможность системе автоматически принимать меры, такие как изоляция затронутых систем и блокировка подозрительных адресов. Визуализация и информационные панели значительно улучшают понимание текущего состояния безопасности, предоставляя информацию в реальном времени и углубляя анализ.

Security Capsule SIEM также поддерживает продвинутые политики хранения данных для целей криминалистического анализа и соответствия нормативным требованиям, что позволяет сохранять значительные объёмы исторических данных. Интеграция с широким спектром безопасных технологий способствует созданию единой экосистемы безопасности, усиливая общую эффективность защиты и позволяя организациям оптимально использовать вложенные средства в области безопасности. Более того, Security Capsule SIEM взаимодействует с внешними источниками данных о потенциальных угрозах и применяет аналитику поведения для выявления необычных или подозрительных активностей. Продвинутая аналитика и машинное обучение усиливают способность системы к обнаружению и прогнозированию угроз. Возможности масштабирования и высокая производительность SIEM обеспечивают эффективную обработку больших объемов данных и адаптацию к росту организации. Инструменты для соблюдения нормативных требований и подготовки отчетов помогают компаниям выполнять законодательные обязательства, в то время как настраиваемые информационные панели и визуализация обеспечивают мгновенный доступ к данным о безопасности [18].

Аналитика поведения пользователей и объектов (UEBA) применяется для мониторинга и анализа поведенческих отклонений, что может свидетельствовать о скомпрометированных учетных записях или внутренних угрозах. Функции автоматического

реагирования и оркестрации сокращают время от обнаружения угрозы до нейтрализации её последствий, обеспечивая быстрое и согласованное реагирование. Возможности хранения данных и проведения криминалистических расследований способствуют глубокому изучению инцидентов, а гармоничная интеграция с другими средствами безопасности формирует сплоченную систему защиты.

2.3. Правила корреляции событий Security Capsule SIEM

Системы управления информацией о безопасности и событиями (SIEM) играют ключевую роль в определении и реагировании на инциденты безопасности за счет сбора и анализа данных из разнообразных источников. Чтобы эффективно выявлять сложные угрозы, которые могут оставаться незамеченными при анализе отдельных событий, необходимы специализированные правила корреляции событий.

В SC SIEM синтаксис типового правила корреляции выглядит следующим образом:

alert any $EXTERNAL_NET any -> $HOME_NET any (msg: «[CISCO GATE 1] BIG NAV DOS Attack – Система обнаружила возможную атаку отказа в обслуживании и приостановила весь трафик на пострадавший канал; *program: snmptrapd; content: «=AP_BIG_NAV_DOS_ATTACK|28|»; classtype: attempted-dos; reference:url,www.cisco.com/c/en/us/td/docs/wireless/ncs/1- 1/configuration /guide/NCS11cg/event.html; rev:3;)*

Создание правил корреляции состоит из четырех разделов.

Первое – основные настройки.

В настройках: выбирается действие для сохранения правила корреляции (либо существующая группа, либо указывается название новой группы в произвольном формате); протокол (TCP, UDP, ICMP); указывается IP-адрес источника (пример:

192.168.1.1, можно указать несколько сетей); порт источника (пример: 80, 8080); IP-адрес назначения; порт назначения.

Второе – дополнительная настройка.

Обязательным к заполнению дополнительным настройкам относятся тип класса и rev. Тип класса связывает правило корреляции с классификацией, последнее используется для определения уровня приоритета. Rev используется для учета версий правила.

Content – ключ, осуществляющий поиск в сообщениях по шаблону. Допустим: *content: «GET»*. Описывается реализация поиска событий по шаблону. В случае *content:!«* Cisco*»* будут разыскиваться все сообщения, не содержащие текст «Cisco».

Reference – ключ, который позволяет добавить к инцидентам ссылки на дополнительные ресурсы.

Ресурсами могут выступать базы уязвимостей (банк данных уязвимостей безопасности информации ФСТЭК России; Common Vulnerabilities and Exposures; Bugtraq), базы угроз (банк данных угроз безопасности информации ФСТЭК России; MITRE ATT&CK), иные ресурсы.

Дополнительные ключи, которые приведены в приложении [18]:

а) After.

б) Alert_time.

в) Append_program.

г) Flexbits.

д) Syslog_level.

е) Meta_content.

ж) Parse_dst_ip.

з) Parse_port.

и) Parse_proto.

к) Parse_proto_program.

л) Parse_hash.

м) Parse_src_ip.

н) PCRE.

о) Priority.

п) Program.

р) Threshold.

с) Xbits.

Третье – описание правила. При создании правила корреляции необходимо указать название (как правило, указывают название актива, с которым связан инцидент) и описание инцидента (рис. 2.5).

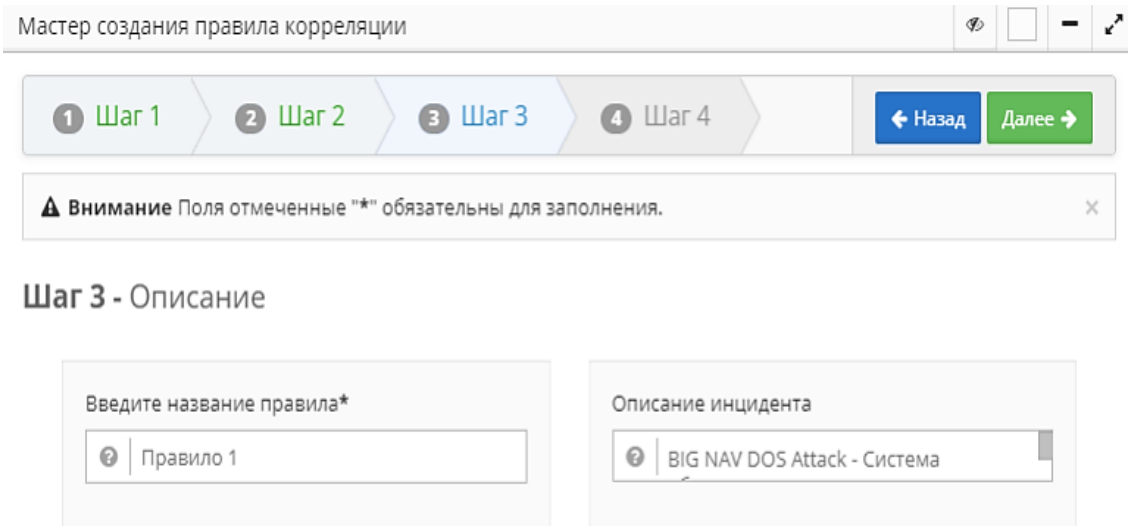

Рис. 2.5. Описание правила корреляции

Заключительная часть предполагает установление корреляции. Визуальное представление в «Правилах корреляции» (рис. 2.6) отображает подробную информацию о правилах корреляции, присутствующих в SC SIEM.

Эта информация представлена в различных столбцах, которые включают в себя:

а) Идентификатор: номер правила.

б) SID: уникальный идентификатор правила корреляции.

в) Описание происшествия: Подробное описание происшествия.

г) Тип класса: указанный тип класса для этого правила.

д) Критичность: Критичность инцидента.

е) Группа: группа, в которой сохраняется это правило.

ж) Синхронизация: статус с сервером ретроспективного анализа и/или географически.

Удаленные регионы.

Статус правила (Вкл\Выкл).

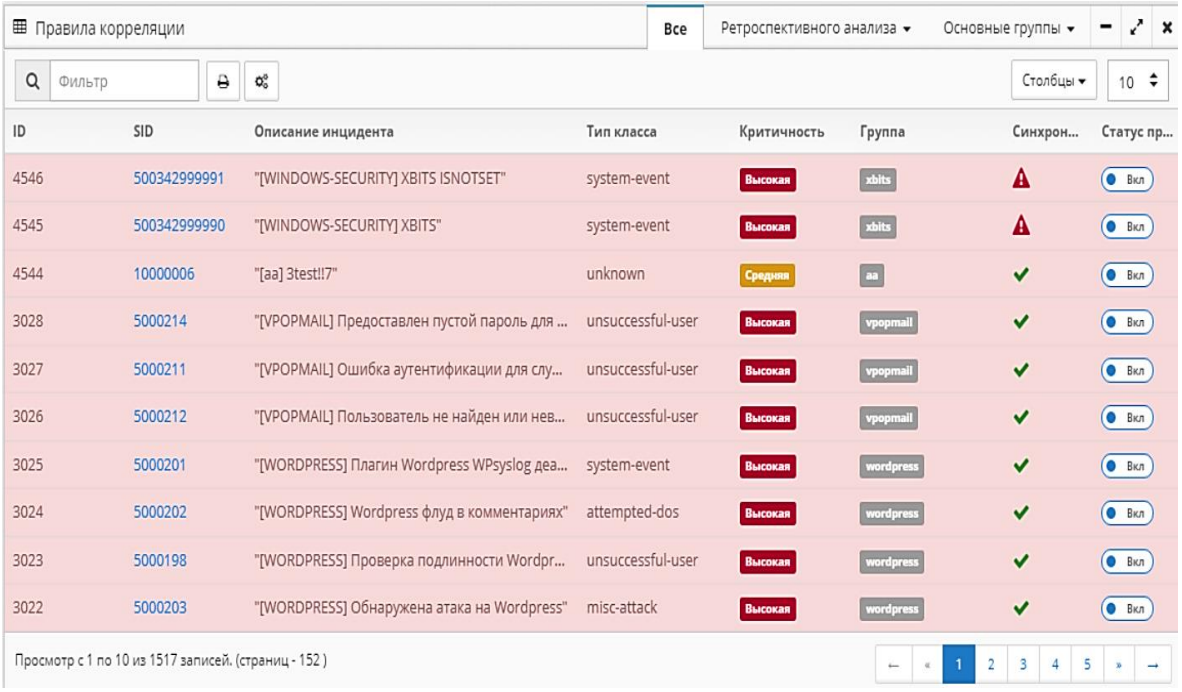

Рис. 2.6. Информация в правилах корреляции

2.4. Схема лицензирования Security Capsule SIEM

Лицензирование Security Capsule SIEM основывается на концепции пропускной способности данных, что означает объем данных, обрабатываемых системой за определенный период. Эта модель помогает точно контролировать затраты, привязывая их к реальному использованию системы. Организации могут начать с базового пакета, который соответствует их начальным потребностям в обработке данных и может масштабироваться в соответствии с их растущими потребностями. Это особенно ценно для быстро растущих компаний или тех, которые сталкиваются с переменными объемами данных, позволяя им гибко подходить к лицензированию в зависимости от текущих операционных требований.

Схема лицензирования предлагает как годовые, так и многолетние контракты, предоставляя скидки за долгосрочные обязательства, что способствует финансовой стабильности и предсказуемости для организаций. Лицензии Siem Capsule часто включают комплексные услуги поддержки и технического обслуживания, обеспечивая регулярные обновления и техническую помощь, что поддерживает оптимальную работу системы SIEM и помогает компаниям оставаться на шаг впереди угроз и соответствовать нормативным требованиям.

Кроме того, лицензирование Siem Security Capsule разработано с учетом расширенных функций безопасности, позволяя организациям поддерживать эффективные защитные механизмы без лишних затрат. Каждый уровень лицензирования предоставляет доступ к таким функциям, как мониторинг в реальном времени, обнаружение угроз и автоматическое реагирование. По мере масштабирования лицензий организации получают доступ к более сложным инструментам и аналитике, что способствует активной киберзащите.

Возможности интеграции являются ключевым аспектом лицензирования Security Capsule SIEM. Система может интегрироваться с различными инструментами и платформами безопасности, такими как брандмауэры, антивирусное ПО и системы EDR.

Базируясь на пропускной способности данных и предлагая гибкие, отраслевые и удобные варианты, лицензионная схема обеспечивает, что компании могут поддерживать эффективную оборонительную стойку без чрезмерного финансового бремени. Включение комплексной поддержки и образовательных ресурсов дополнительно усиливает ценность предложения, делая его желательным выбором для предприятий, стремящихся укрепить свои рамки безопасности.

ООО «ИТБ» - Кибербезопасность предоставляет SC SIEM как в программном, так и в программно-аппаратном виде.

Таблица 2.2

Уровни значимости запросов в техническую поддержку

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку), либо оказывающие критическое влияние	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния	До 24 часов	Не ограничено
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Когда вы обращаетесь в техническую поддержку, процесс реагирования на ваш запрос запускается мгновенно. Сразу после получения вашего сообщения начинается отсчёт времени реакции, продолжающийся до момента, когда оператор подтверждает начало работы над ним. На этой первой стадии для специалиста критически важно тщательно изучить все детали обращения. Это позволяет быстрее понять суть проблемы и эффективно переходить к её решению, что существенно ускоряет процесс обработки и повышает продуктивность службы поддержки.

Принятие запроса в работу отмечает начало следующего этапа обработки. С этого момента вы будете держаться в курсе предпринимаемых действий по решению вашей проблемы до того момента, пока она не будет устранена. В зависимости от осо-

бенностей случая запрос может быть классифицирован как техническая неисправность или ошибка программного обеспечения, что обязательно потребует вмешательства специализированных специалистов. В течение этого периода ключевую роль играет глубокий анализ проблемы и скорость выполнения всех необходимых действий. Такой подход не только способствует предоставлению качественной поддержки, но и повышает удовлетворенность клиентов.

Следует учитывать, что время реакции и время обработки зависят от уровня значимости запроса, указанного вами. Различные запросы могут иметь разные уровни приоритета, и время реакции и обработки могут варьироваться в зависимости от этого уровня.

2.5. Возможности масштабирования (расширения)

В системе SC SIEM реализованы два метода масштабирования: вертикальное и горизонтальное. Вертикальное масштабирование происходит за счет увеличения аппаратных ресурсов в существующей инфраструктуры, путем усиления серверов с помощью новых процессоров, увеличение объема оперативной памяти и расширение хранилища баз данных. Такой подход позволяет системе обрабатывать увеличенные объемы данных без добавления новых физических устройств.

Горизонтальное масштабирование, напротив, включает добавление дополнительных модулей SC SIEM в сеть, обеспечивающих распределение рабочей нагрузки между большим количеством узлов. Этот метод увеличивает общую производительность системы, позволяя ей эффективно обрабатывать большие объемы данных и выполнять сложные операции без снижения скорости обработки. Преимущества метода горизонтального масштабирования в повышенной отказоустойчивости, а также облегчении управления. Допустим, если один из модулей выходит из строя, другие могут перенять его функции, обеспечивая непрерывность

работы. Горизонтальное масштабирование также обеспечивает гибкость в расширении системы, что важно для быстрорастущих и крупномасштабных сред [18].

Был проведен сравнительный анализ, результат которого представлен в таблице 2.3, где указаны различия, преимущества.

Таблица 2.3

Сравнительный анализ масштабирования в SC SIEM

Характеристика	**Горизонтальное масштабирование**	**Вертикальное масштабирование**
Описание	Добавление новых систем или модулей в сеть.	Модернизация существующих аппаратных ресурсов системы.
Масштабируемость	Достигается увеличением числа модулей.	Достигается за счёт улучшения возможностей текущего оборудования.
Затраты	Первоначальная настройка может быть дороже из-за дополнительных затрат на оборудование и интеграцию, но система становится более гибкой и модульной.	Часто менее затратная на начальном этапе, но может стать дорогостоящей по мере достижения пределов оборудования.
Сложность	Требует сложной сети и синхронизации модулей.	Менее сложный процесс, так как включает модернизацию одной системы.
Производительность	Может повысить производительность за счёт распределения нагрузок и поэтапного масштабирования без значительных простоев.	Повышает производительность за счёт увеличения мощности одного модуля, но могут возникать узкие места, такие как диск I/O.
Избыточность	Высокая избыточность, так как отказ одного модуля не влияет на другие.	Низкая избыточность, так как вся система может пострадать от отказа в одной точке.
Обслуживание	Более сложное управление и обслуживание множества систем.	Легче обслуживать одну систему, чем несколько распределённых систем.

Характеристика	Горизонтальное масштабирование	Вертикальное масштабирование
Отказоустойчивость	Повышенные возможности отказоустойчивости за счёт передачи функций вышедшего из строя модуля другим модулям.	Ограниченные возможности отказоустойчивости; сбой основной системы может прервать работу всего сервиса.
Сценарий использования	Подходит для систем, требующих высокой доступности и частого масштабирования.	Может использоваться приложениями с ограниченной масштабируемостью и высокими вычислительными требованиями.

2.6. Преимущества Security Capsule SIEM

Security Capsule SIEM объединяет в себе возможность централизованного мониторинга действий на всех уровнях ИТ-инфраструктуры, включая сетевые устройства, серверы, базы данных и приложения. Мониторинг позволят проводить глубокий анализ потенциальных угроз и поверхностное наблюдение.

Команда безопасности может мгновенно реагировать и принимать мер при обнаружении, благодаря функции реального времени и заранее настроенным параметрам, т.к. SC SIEM оперативно реагирует на инциденты.

Системы Security Capsule SIEM оснащены инструментами для создания отчетов о состоянии безопасности, что способствует соблюдению таких стандартов, как GDPR, HIPAA и PCI DSS. Эти отчеты не только формализуют процессы проверки, но и обеспечивают документальное подтверждение соблюдения необходимых требований.

SC SIEM выполняет ряд требований нормативно-методических документов, таких как:

1. Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и

технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Требования выполняются в части регистрации событий безопасности, выявления инцидентов, приводящих к сбоям и нарушению работоспособности информационной системы.

2. Приказ ФСТЭК России № 17 от 11 февраля 2013 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Здесь выполняются требования по обеспечению защиты, соответствуя документации по использованию и организационно-распорядительными документами по ЗИ, включая администрирование мониторинга и анализа зарегистрированных событий, обеспечивающие безопасность, информирование пользователей, включая администраторов о возникновении инцидентов, анализ инцидентов, определение источников и причин возникновения, оценка их последствий. Согласно требованиям, происходит реализация мер регистрации к мерам ЗИ.

3. ФЗ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», выполняются требования по безопасности персональных данных. Такие как: обнаружение, предупреждение несанкционированного доступа к персональным данным. Требования по ликвидации последствий атак.

4. Приказа ФСБ России от 13 февраля 2023 г. № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных», в части обеспечения взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий

компьютерных атак на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

Security Capsule SIEM является масштабируемым и гибким решением, которое развивается вместе с организацией, адаптируясь к новым источникам данных и увеличению трафика. Мониторинг безопасности этом случае остается эффективным и соответствует меняющимся потребностям.

Он легко интегрируется с другими инструментами безопасности, такими как антивирусные программы, межсетевые экраны и системы обнаружения и предотвращения вторжений (IDS и IPS). Такая интеграция укрепляет общую архитектуру безопасности и улучшает координацию реагирования на угрозы.

Расширенные функции Security Capsule SIEM включают анализ поведения пользователей и объектов (UEBA) для обнаружения внутренних угроз, взлома учетных записей и других вредоносных действий.

Несмотря на первоначальные инвестиции, SIEM-системы Security Capsule могут оказаться экономически эффективными в долгосрочной перспективе. Автоматизация мониторинга безопасности и снижение частоты нарушений помогают, как ни странно, минимизировать потенциальные потери и эксплуатационные расходы.

Security Capsule SIEM предлагает настраиваемые отчеты, которые можно адаптировать к конкретным потребностям организации.

3. РЕКОМЕНДАЦИИ ПО ИНТЕГРАЦИИ СИСТЕМЫ МОНИТОРИНГА И КОРРЕЛЯЦИИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SECURITY CAPSULE SIEM В ТЕЛЕКОММУНИКАЦИОННУЮ СЕТЬ ОВД

3.1. Исходное состояние телекоммуникационной сети ОВД

Объектом исследования является телекоммуникационная сеть ОВД.

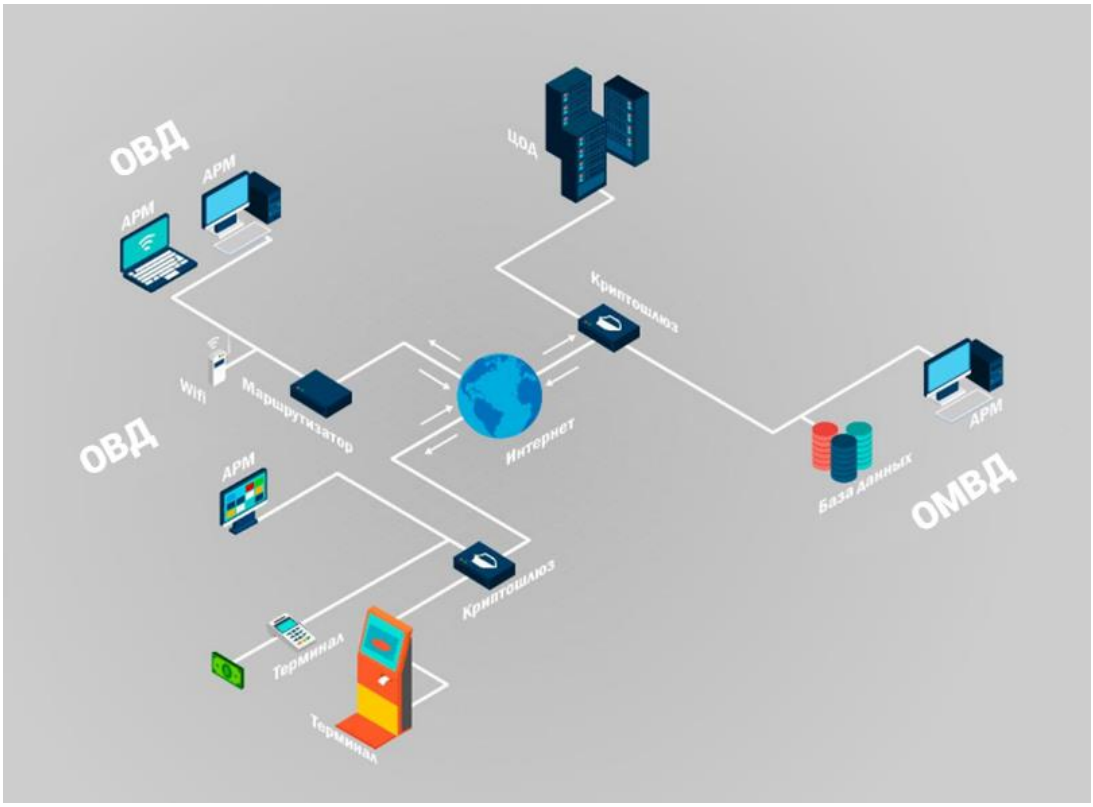

Рис. 3.1. Структура телекоммуникационной сети

Телекоммуникационная сеть состоит из 18 локальных сегментов, которые соответствуют подразделениям или отделам полиции. Внутри каждого из 18 подразделений развернут сегмент локальной сети, связывающий компьютеры сотрудников между собой.

В здании расположена серверная комната, где осуществляется коммутация и установлены хранилище данных. В качестве маги-

стральных маршрутизаторов, а также для связи используются Juniper MX40. Центральные узловые маршрутизаторы используются второго и третьего уровня: Riverstone Networks RS3100.

Компьютерная сеть построена на основе топологии – звезда, центром которой является коммутатор, а лучами – присоединенные автоматизированные рабочие места сотрудников. Для передачи данных используется кабель витая пара CAT-5e, для подключения витых пар используется коннекторы RJ-45. Пропускная способность локальной сети – 100 Мб/с. Присутствует сетевая печать, принтеры подключены к рабочим станциям.

В ходе анализа телекоммуникационной сети ОВД выяснено: в локальную сеть входят ~4000 автоматизированных рабочих мест, из которых 2200 являются подключены к единой информационно-аналитической системе обеспечения деятельности ОВД (ИСОД), а ~1800 имеют доступ в сеть Интернет. Инцидент информационной безопасности, пришедшая со стороны сети интернет способна нанести вред информации, обрабатываемой на любой АРМе локальной сети.

3.2. Подготовка к развертыванию системы

Для обеспечения эффективного управления и мониторинга в рамках системы безопасности сервер управления должен обладать безограниченным доступом к сети, включая все подключенные серверы и рабочие станции. Это критически важно для осуществления комплексных сканирований, которые позволяют проводить инвентаризацию данных, таких как узлы, уязвимости и программное обеспечение.

В процессе внедрения системы важно строго следовать инструкциям по настройке источников событий. Перед запуском системы необходимо завершить ряд подготовительных мероприятий. К ним относится распределение IP-адресов и DNS-имен для серверов, определение мест установки и точек подключения, рас-

пределение рабочих мест для персонала, а также выбор узлов, которые будут контролироваться. Кроме того, должны быть настроены сетевые средства защиты для обеспечения надежного взаимодействия между компонентами системы и эффективного сканирования. Также к этому времени должны быть созданы сервисные учетные записи для доступа к контролируемым узлам.

Перед началом работы с системой Security Capsule персонал, который будет ею управлять, должен не только ознакомиться с эксплуатационной документацией, но и пройти специализированное обучение. Обучение проводится на официальных курсах, организованных компанией, что гарантирует высокий уровень квалификации сотрудников.

Сотрудники, задействованные в работе с SC SIEM, должны уметь осуществлять пусконаладку и настройку системы, подключать и настраивать источники событий, анализировать информационную безопасность из различных источников данных. Они также отвечают за написание и оптимизацию правил корреляции событий, реагирование на инциденты информационной безопасности, взаимодействие с национальным координационным центром по компьютерным инцидентам, подготовку отчетов и контроль за работоспособностью модулей SC SIEM.

3.3. Требования к функциям, выполняемым системой

3.3.1. Требования к управлению активами, обработке событий и к хранению событий

В системе Security Capsule SIEM (SC SIEM) ключевым является управление активами, обработка и хранение данных о событиях, что имеет критическое значение для обеспечения безопасности.

1. Управление активами в SC SIEM охватывает комплексное слежение за всей инфраструктурой – от аппаратуры до программных и сетевых ресурсов. Система способна автоматически обнаруживать все активы как локальные, так и в облаке,

используя для идентификации пассивное и активное сканирование. Поддерживается актуальный список активов, включая ОС, приложения, сетевое оборудование и устройства. Регулярное сканирование активов на предмет уязвимостей и ошибок. Анализируются риски, связанные с каждым активом.

2. Обработка данных о безопасности в реальном времени позволяет принимать оперативные решения для защиты организации. Интегрируются данные из разнообразных источников, осуществляется преобразование данных в единый формат, происходит корреляция событий.

3. Надежное хранение информации о событиях обеспечивает возможность анализа и соответствия нормативным требованиям.

3.3.2. Требования к управлению инцидентами, визуализации и отчетности и к обеспечению безопасности

Для обеспечения эффективного функционирования системы Security Capsule SIEM (SC SIEM) следует учитывать несколько важных требований, касающихся таких аспектов, как управление инцидентами, визуализация и отчетность, а также обеспечение безопасности.

Управление инцидентами:

– обнаружение в реальном времени;

– автоматическое реагирование;

– приоритеты инцидентов по уровню серьезности и срочности.

Визуализация и отчетность. Вместо того чтобы полагаться на стандартные отчеты, пользователи имеют возможность настраивать информационные панели, которые могут представлять ключевые данные. Это значительно упрощает мониторинг и управление, поскольку им нужно сосредоточиться только на самой важной информации. Аналитика в реальном времени играет решающую роль в предоставлении немедленной информации о любых обнаруженных угрозах безопасности, что позволяет опе-

ративно принять меры. Кроме того, анализ исторических данных помогает выявить закономерности или слабые места в системе, которыми можно было воспользоваться ранее.

Безопасность. Первая линия защиты безопасности заключается в обеспечении защиты всех данных с помощью методов шифрования, которые делают их недоступными для чтения, кроме уполномоченных лиц. Контроль доступа должен быть реализован не только для конфиденциальных данных, но и для критически важных функций системы – они должны быть доступны только уполномоченным лицам. Любое действие, предпринятое в системе, должно быть тщательно зафиксировано, чтобы его можно было отследить, если это потребуется в дальнейшем для целей расследования.

Более того, регулярные обновления наряду с управлением исправлениями должны выполняться последовательно в рамках превентивных мер безопасности, направленных на устранение любых уязвимостей, которые могут быть использованы злоумышленниками – это снижает вероятность успешного взлома систем, развернутых в вашей среде. Таким образом, безопасность всегда должна оставаться высоким приоритетом при рассмотрении любых изменений или улучшений, которые могут повлиять на вашу ИТ-инфраструктуру и ее компоненты.

Первый момент, который следует обсудить, – это интеграция и соответствие требованиям, которым SC SIEM помогает путем слияния с другими системами безопасности в дополнение к автоматизации соответствия таким стандартам, как GDPR и HIPAA. Это происходит за счет более продвинутых возможностей обработки данных и отчетности. Для доступа к нему необходимо принять модель управления доступом на основе ролей (RBAC), которая предоставляет роли и разрешения, как показано в таблице 3.1 [18].

Таблица 3.1

Требования к ролям и разрешениям

№	Роль	Объект	Права
1.	Администратор	Операции с пользователями	Чтение/запись
		Задачи сканирования и сбора событий ИБ	Чтение/запись
		Группы активов	Чтение/запись
		Правила корреляции	Чтение/запись
		Создание объектов: учетная запись; профиль	Чтение/запись
		Настройка оповещений	Чтение/запись
2.	Аналитик	Правила корреляции	Чтение/запись
		Создание фильтров событий	Чтение/запись
		Просмотр событий	Чтение/запись
		Просмотр инцидентов	Чтение/запись
		Выпуск отчетов	Чтение/запись
		Создание инцидентов	Чтение/запись
		Просмотр активов	Чтение/запись
		Создание динамических групп	Чтение/запись
		Настройка визуальных панелей	Чтение/запись
3.	Оператор	Создание фильтров событий	Чтение/запись
		Просмотр событий	Чтение/запись
		Просмотр инцидентов	Чтение/запись
		Выпуск отчетов	Чтение/запись
		Создание инцидентов	Чтение/запись
		Просмотр активов	Чтение/запись
		Создание динамических групп	Чтение/запись
		Настройка визуальных панелей	Чтение/запись

3.3.3. Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие

Инициирование процесса запуска системы автоматизации безопасности Security Capsule (SC SIEM) представляет собой комплексную задачу, требующую не только глубокого понимания технологий, но и внимания к деталям. В самом начале необходимо удостовериться, что все компоненты системы точно соответству-

ют установленным требованиям и правильно установлены. Это действительно критично, ведь правильная конфигурация сетевых параметров играет ключевую роль в эффективной работе SC SIEM и её взаимодействии с другими сетевыми устройствами.

Далее следует этап интеграции системы с разнообразными источниками данных, такими как брандмауэры и серверы, что обеспечивает возможности для глубокого контроля и мониторинга сетевых процессов. Не менее важно тщательно настроить ключевые параметры системы, включая управление пользователями, систему оповещений и правила корреляции, что существенно усиливает управленческие функции.

После настройки системы проводятся обширные тесты. Они необходимы для проверки адекватности функционирования SC SIEM под различными рабочими нагрузками и оценки уровня безопасности для определения потенциальных уязвимостей. Этот шаг помогает обеспечить, что система будет работать стабильно и безопасно.

Затем наступает время для создания подробной документации, охватывающей все аспекты работы системы, от её конфигурации до точек интеграции. Руководство для пользователя и руководство по устранению неполадок составляются параллельно с документированием операционных процедур, включая методы обработки предупреждений, управление инцидентами и проведение технического обслуживания.

Кроме того, необходимо настроить шаблоны и графики отчетов для регулярной оценки работы системы и её соответствия политикам безопасности. Финальный этап включает всестороннюю проверку системы и одобрение плана её запуска.

Осуществляя такое тщательное планирование и реализацию, мы создаем надежную и функциональную систему SC SIEM, способную эффективно минимизировать безопасностные угрозы и соответствовать всем необходимым нормам и стандартам.

3.4. Схемы развертывания

Развертывание SC SIEM на объекте информатизации делится на 4 условных этапа:

– обследование объекта информатизации;

– определение перечня источников событий подключаемых к SC SIEM;

– развертывание модулей SC SIEM;

– настройка модулей SC SIEM, а также источников событий.

3.4.1. Обследование объекта информатизации

1) SC SIEM, при содействии специалистов осуществляются работы по обследованию объекта информатизации.

Модель объекта информатизации отображена (рис. 3.2).

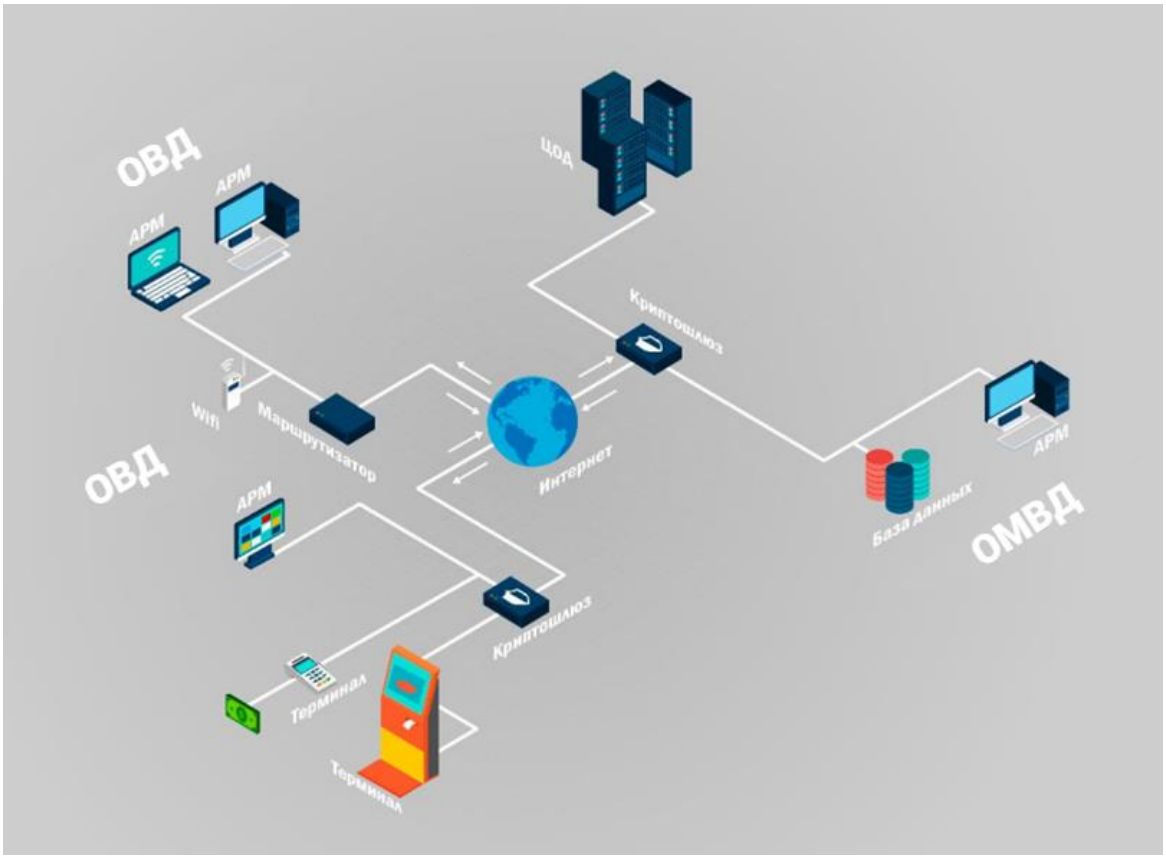

Рис. 3.2. Модель территориально-распределенного объекта информатизации

На данном этапе определяется модель построения ЛВС объекта, используемые технические средства, а также программное обеспечение, в том числе средства защиты информации. В результате действий, выполняемых на первом этапе формируется предварительная конфигурация поставляемых модулей SC SIEM.

3.4.2. Определение перечня источников событий, подключаемых к Security Capsule SIEM

На втором этапе внедрения системы SC SIEM основное внимание уделяется определению и согласованию списка источников событий, которые будут подключены к системе. Важно подчеркнуть, что процесс лицензирования в SC SIEM тесно связан с количеством этих источников. Различные категории источников, интегрируемых в SC SIEM, демонстрируют многообразие и специфику подключаемых систем, что отражено в документации к продукту, в частности в разделе, иллюстрирующем этот процесс (рис. 3.3).

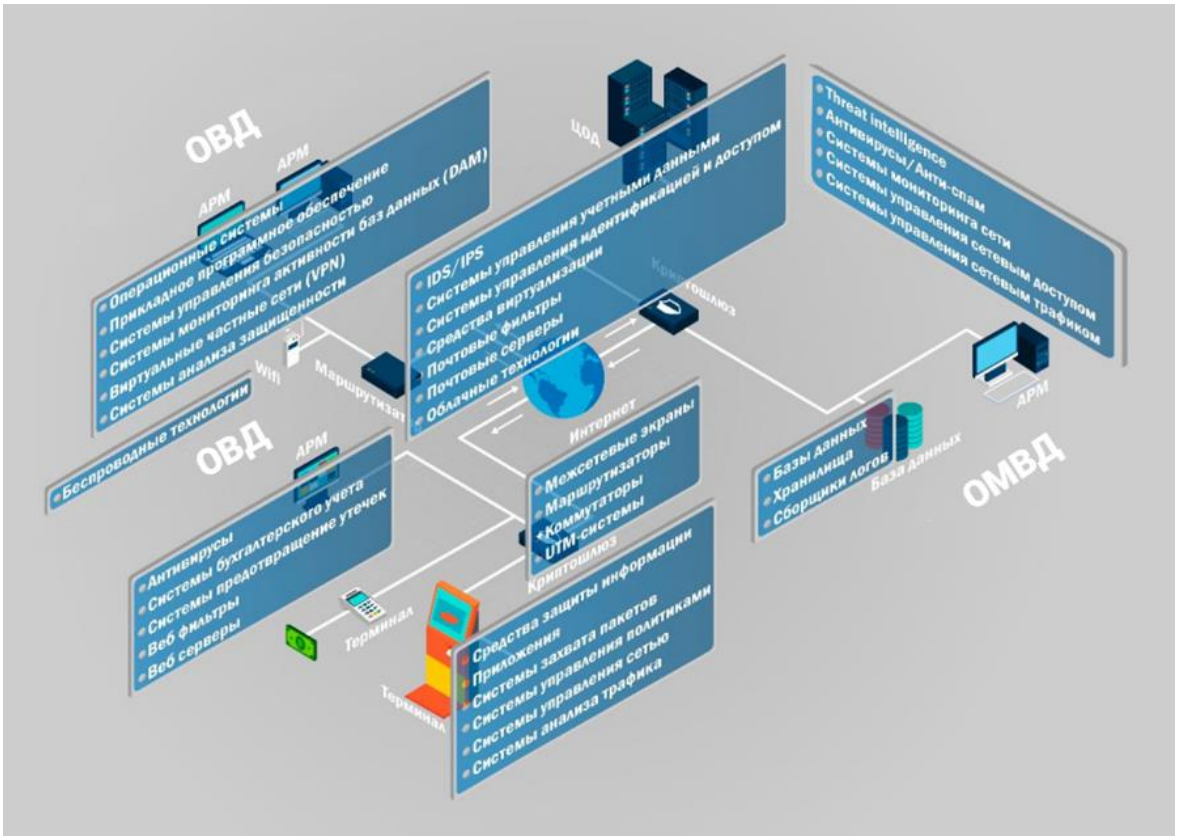

Рис. 3.3. Категории подключаемых источников событий к SC SIEM

Перечень типовых категорий источников событий, доступных для подключения к SC SIEM, включает широкий спектр систем и технологий. В этот перечень входят IDS/IPS, системы управления учетными данными (IDM) и системы управления идентификацией и доступом (IAM). Также учитываются сборщики логов и почтовые фильтры, mainframe и почтовые серверы. Системы обнаружения вредоносных программ и управления сетевым доступом также играют значительную роль.

К ним добавляются системы управления сетевым трафиком и операционные системы, а также системы Network Behavior Anomaly Detection (NBAD). Интеграция Threat intelligence, приложений и антивирусов/анти-спама также является необходимой частью. Важное место занимают средства защиты информации и прикладное программное обеспечение.

Не менее значимы облачные технологии, системы бухгалтерского учета и базы данных. Системы предотвращения утечек (DLP), межсетевые экраны и коммутаторы также находятся в этом списке. UTM-системы и средства виртуализации дополняют картину, как и системы управления безопасностью, маршрутизаторы и системы мониторинга активности баз данных (DAM).

Кроме того, важны виртуальные частные сети (VPN), системы анализа защищенности и веб-фильтры. Веб-серверы и беспроводные технологии также включены в перечень. Системы захвата пакетов, управления политиками и управления сетью, а также системы анализа трафика и хранилища не остаются без внимания. Завершают список системы мониторинга сети.

На втором этапе выполнения действий уточняется и дополняется конфигурация поставляемых и развертываемых модулей SC SIEM, обеспечивая оптимальную интеграцию и функциональность системы [18].

3.4.3. Развертывание Security Capsule SIEM

На заключительном этапе внедрения SC SIEM производится установка его модулей в текущую инфраструктуру информационного объекта. Ниже представлена схема размещения компонентов SC SIEM на территориально-распределенном информационном объекте (рис. 3.4).

На данном этапе специалисты занимаются непосредственной интеграцией модулей SC SIEM в инфраструктуру объекта. Разработанная схема позволяет наглядно представить процесс и расположение компонентов системы на объекте с территориальной распределённостью. Таким образом, схема (рис. 3.4.) является ключевым элементом, демонстрирующим порядок и этапы интеграции компонентов SC SIEM в информационную структуру объекта.

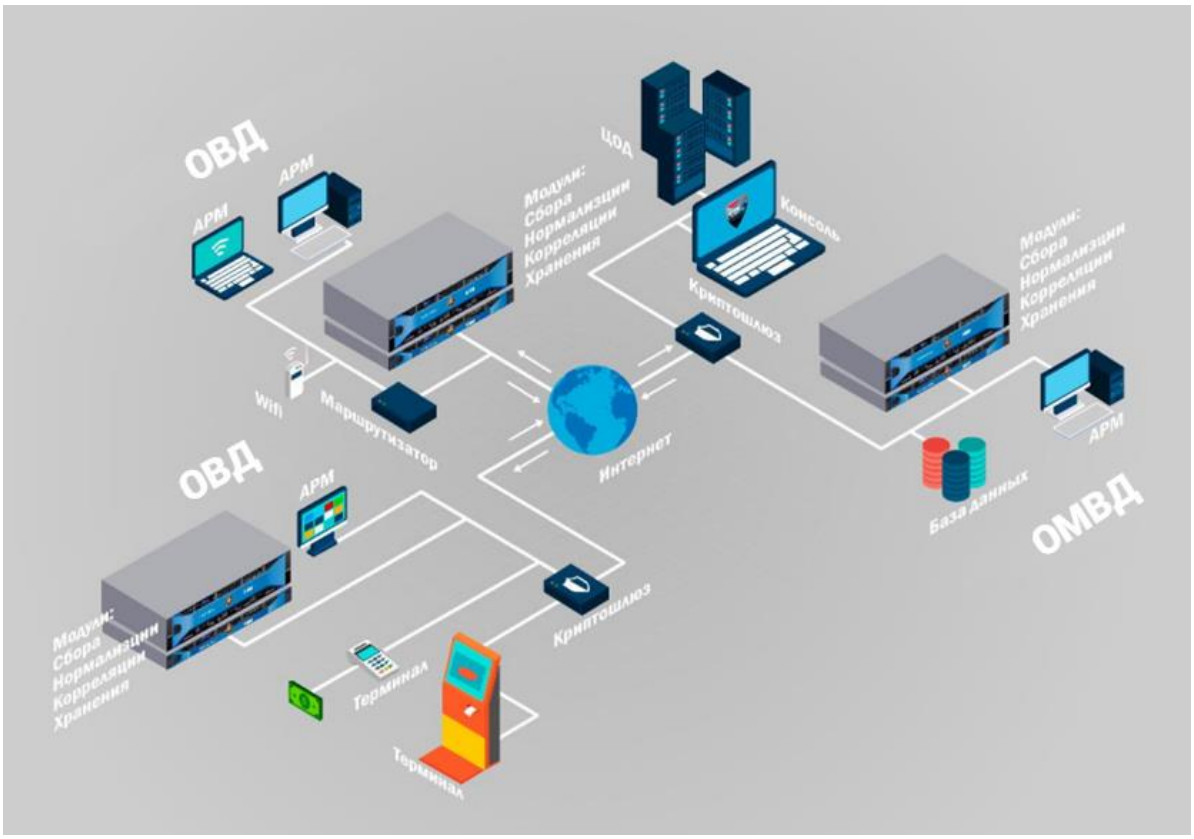

Рис. 3.4. Схема установки компонентов SC SIEM
на территориально-распределенном объекте информатизации

В случае наличия сетевой доступности, а также достаточной пропускной способности каналов связи между территориально-удаленными площадками возможно реализовать централизованный сбор событий.

3.4.4. Настройка модулей Security Capsule SIEM, а также источников событий

На четвёртом этапе развёртывания системы SC SIEM ключевое внимание уделяется настройке взаимодействия её модулей. Это включает в себя определение транспортных механизмов, которые обеспечивают передачу данных между источниками событий и самой системой SC SIEM. Важно, что каждый из этих источников настраивается индивидуально для эффективной интеграции и точности передачи информации.

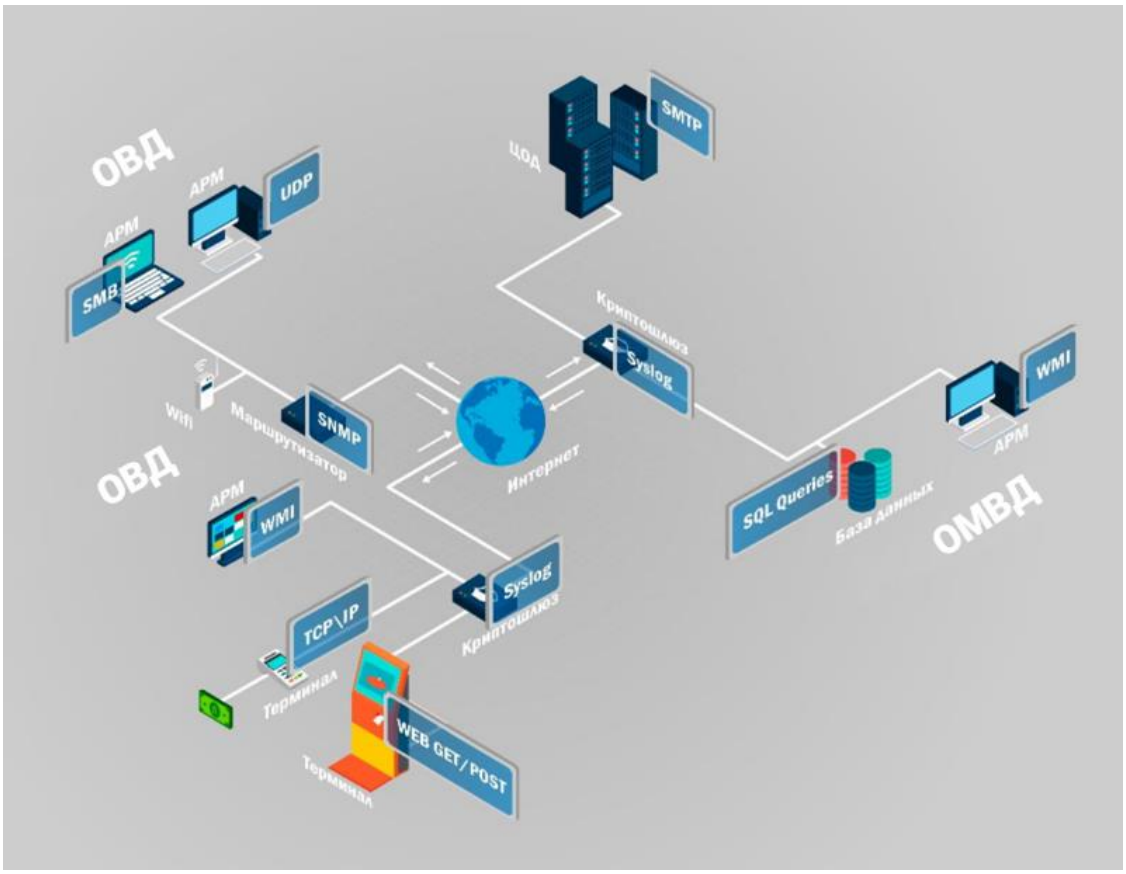

Рис. 3.5. Перечень транспортов

3.5. Запуск программного обеспечения и настройки приложения

SC SIEM поддерживает следующие операционные системы:

- Microsoft Windows Server 2012;
- Microsoft Windows Server 2012 R2;
- Astra Linux Special Edition.

Поддерживаемые браузеры:

- Google Chrome 49 (и выше);
- Microsoft Internet Explorer 11 (и выше);
- Mozilla Firefox 45 (и выше).

Параметры платформы:

- узлов сети до 4000;
- EPS – до 10000;

Высоко-нагруженная система.

Для использования SC SIEM потребуется один виртуальный или физический АРМ со следующими техническими характеристиками:

- 4 ядра;
- 8 Гб ОЗУ;
- 500 Гб жесткий диск;
- ОС debian 10/11, ubuntu 20/22, redos 7.2/7.3 или любая иная отечественная ОС.

Если будет развернута виртуальная машина, то в среде виртуализации необходимо будет пробросить USB порт до виртуальной машины.

Для запуска программы необходимо в строке браузера указать IP-адрес веб-интерфейса консоли.

При первом запуске необходимо ввести пароль для предустановленной учетной записи администратора SC SIEM (рис. 3.6). Учетные данные будут приведены в бланке лицензии.

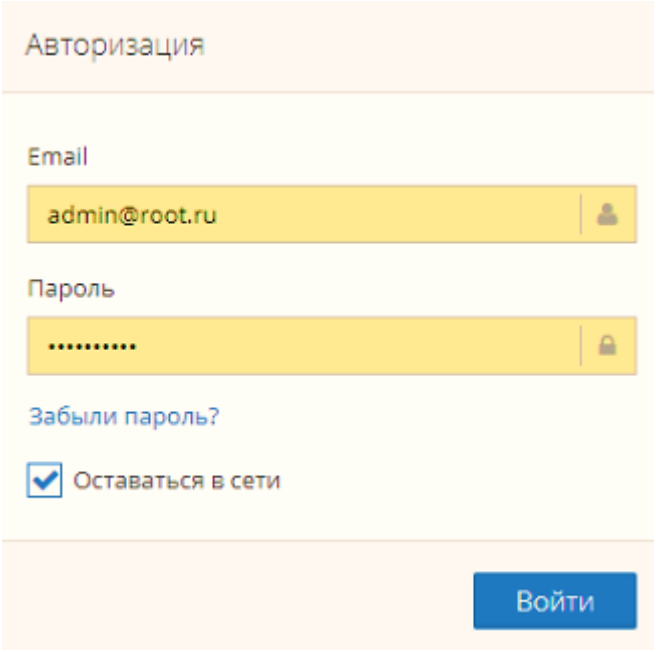

Рис. 3.6. Авторизация в SC SIEM

При успешной авторизации, открывается главное окно приложения «Панель управления» (рис. 3.7).

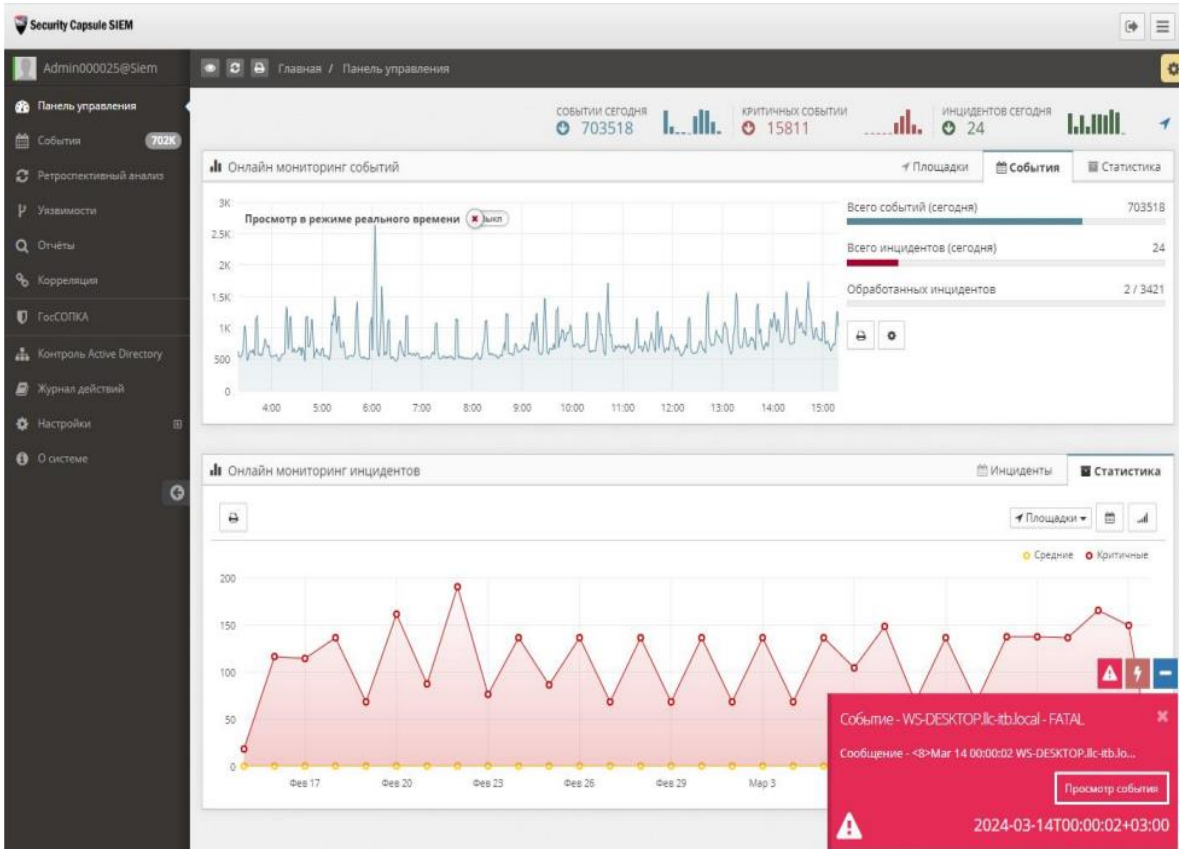

Рис. 3.7. Панель управления

Панель управления является главным окном. В этом разделе оператор просматривает оперативную статистику о работе. В панели управления находятся виджеты онлайн мониторинга событий и инцидентов (рис. 3.8).

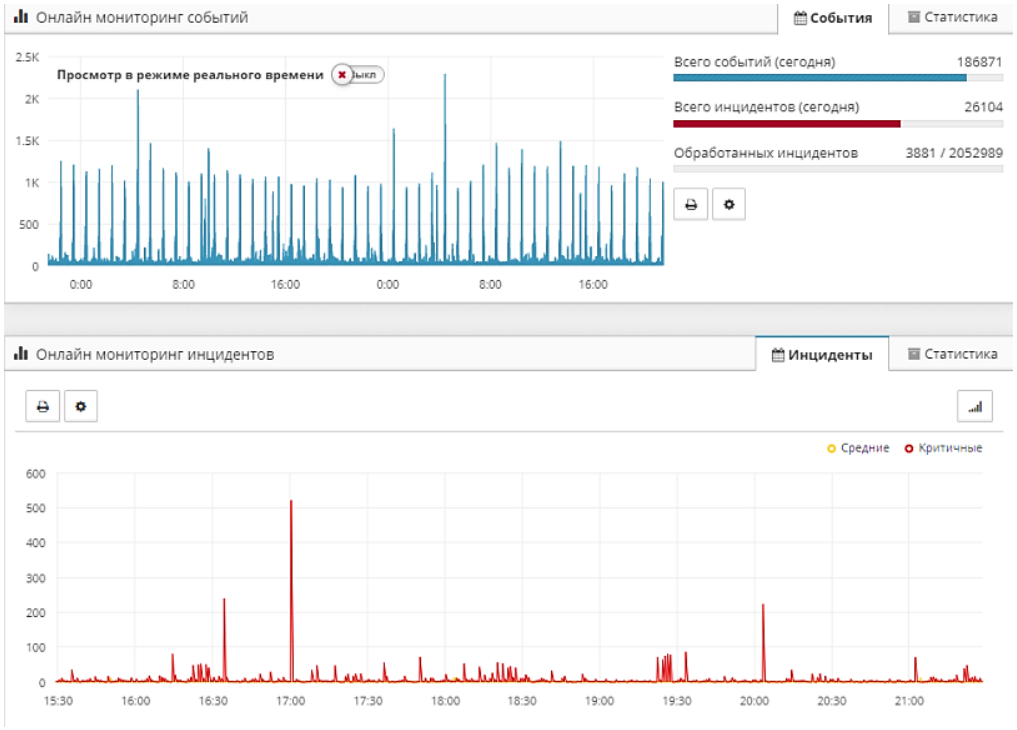

Рис. 3.8 Мониторинг событий и инцидентов

Оператору SC SIEM доступна возможность настройки раздела «Панель управления» в части отображаемых виджетов. Здесь можно вывести любые из имеющихся карточек в смежных разделах (рис. 3.9).

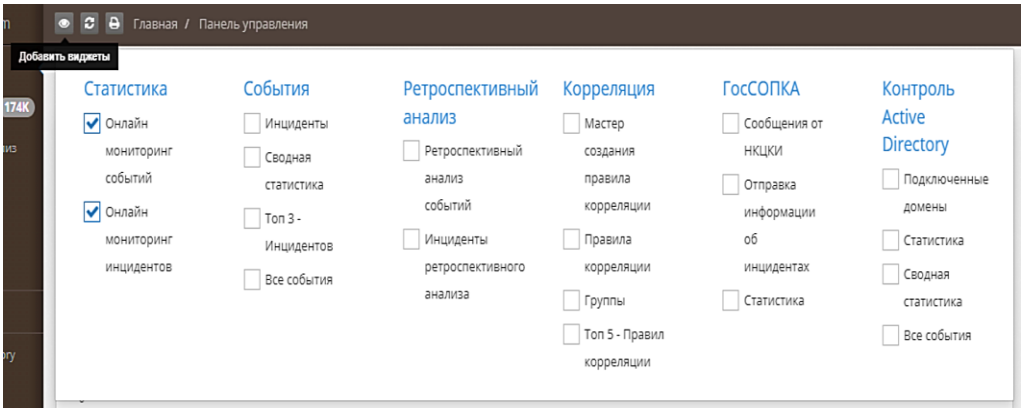

Рис. 3.9. Добавление виджетов

Присутствует возможность просмотра сводного графика о зафиксированных в SC SIEM событий и инцидентов разной степени критичности за временной интервал. При необходимости оператор SC SIEM может задать произвольный период для вывода данных, также ознакомиться с данными по интересующей его площадке, а также скрыть для отображения данные по той или иной степени критичности событий (рис. 3.10, рис. 3.11).

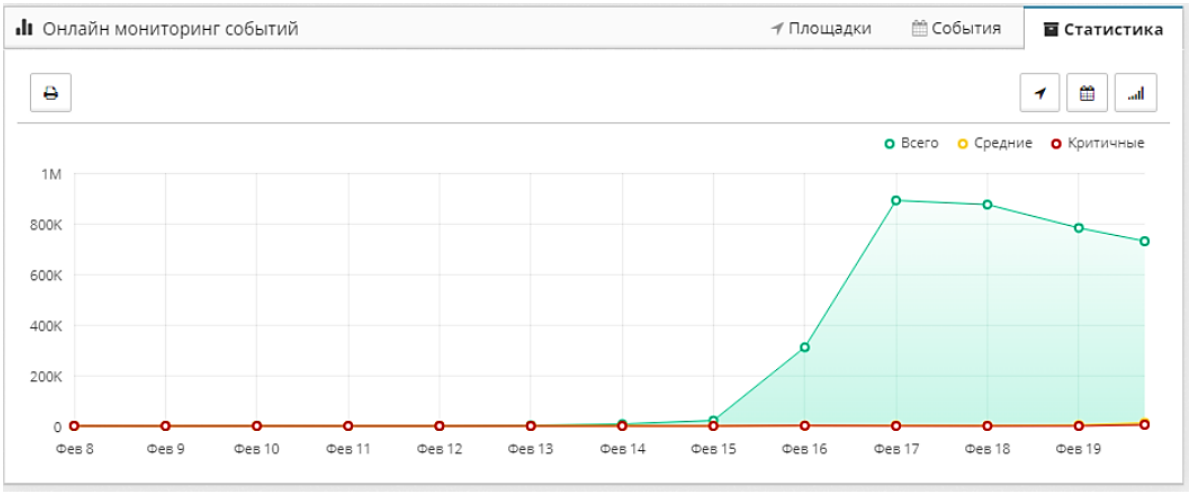

Рис. 3.10. Статистика о событиях

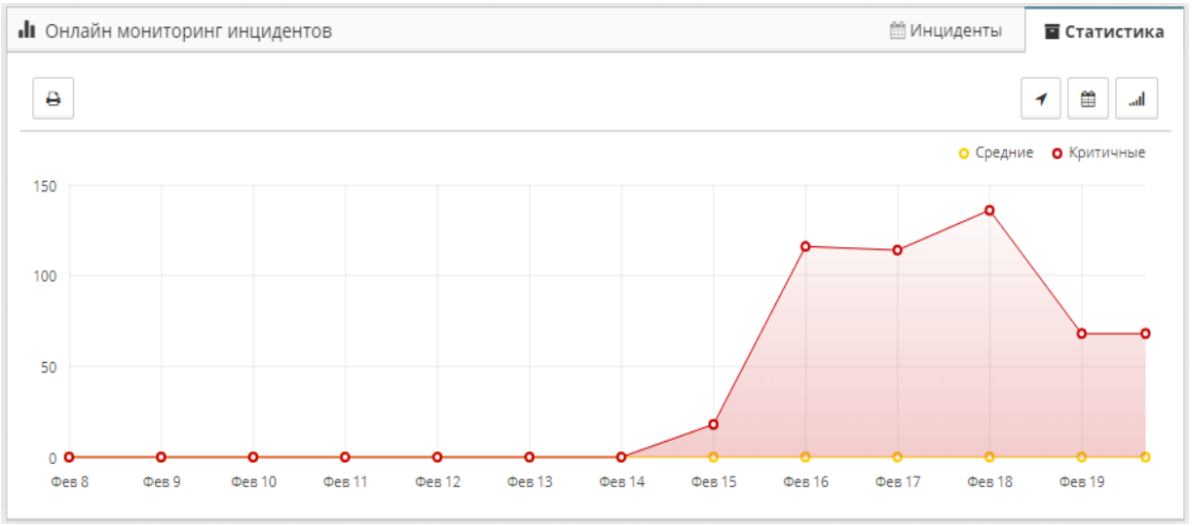

Рис. 3.11. Статистика об инцидентах

Инциденты являются результатом работы «Коррелятора», на основе предустановленных правил в режиме реального времени

осуществляет сопоставление событий с данными правилами (рис. 3.12).

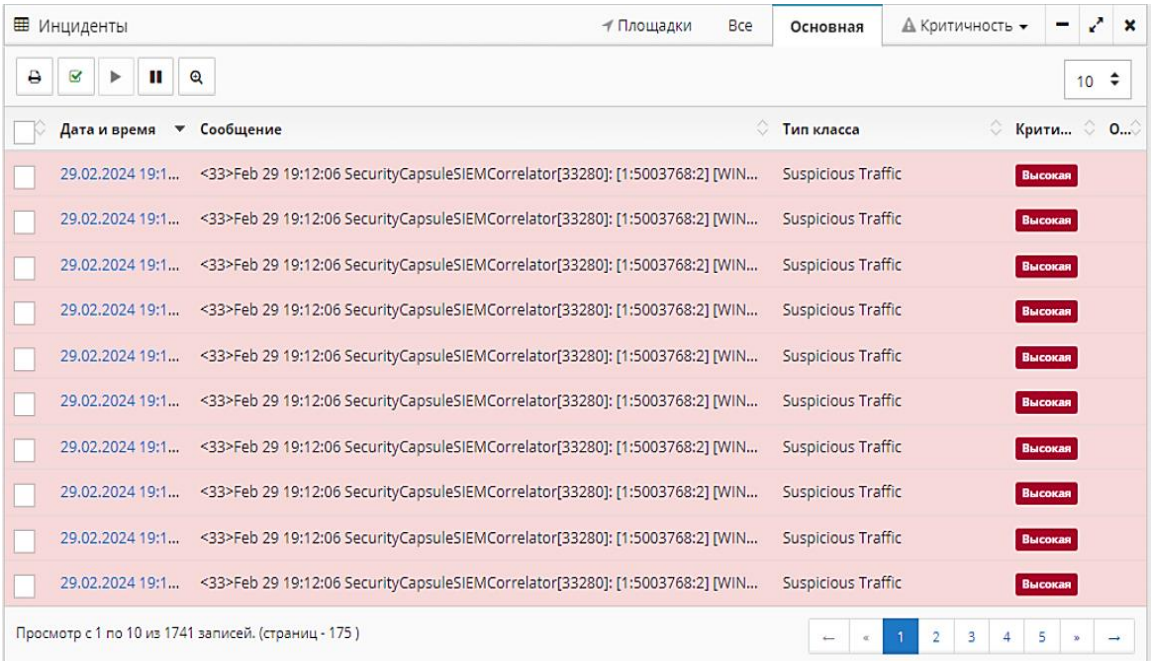

Рис. 3.12. Инциденты

«Общие настройки приложения» (рис. 3.13) представляет следующие опции:

- регистрация пользователей (самостоятельная регистрация пользователей);
- логотип (необходимо предварительно загрузить в директорию с соответствующими именем: …/graf/img/any/any.png. Рекомендованный размер 356x52 пикселей);
- уведомление по e-mail;
- интервал уведомления (секунд) (в течение какого интервала времени будут проверяться новые инциденты);
- критичность;
- максимальное количество инцидентов в интервал времени;
- логирование отправки уведомлений.

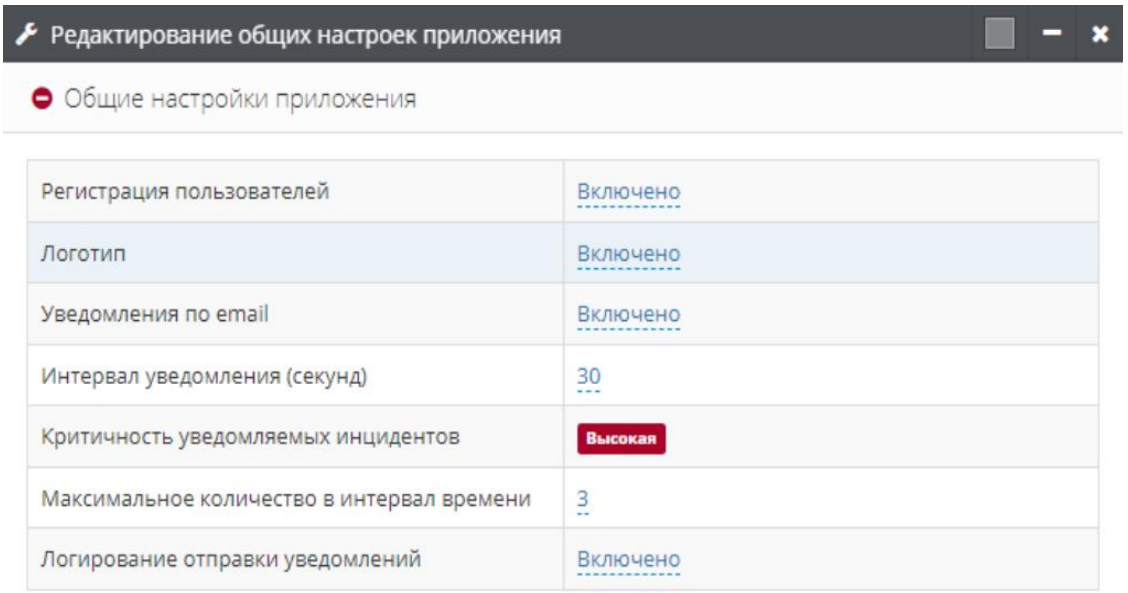

Рис. 3.13. Общие настройки

Настройка сервисов SC SIEM отображает все настройки сервисов, за исключением ГосСОПКА (рис. 3.14)

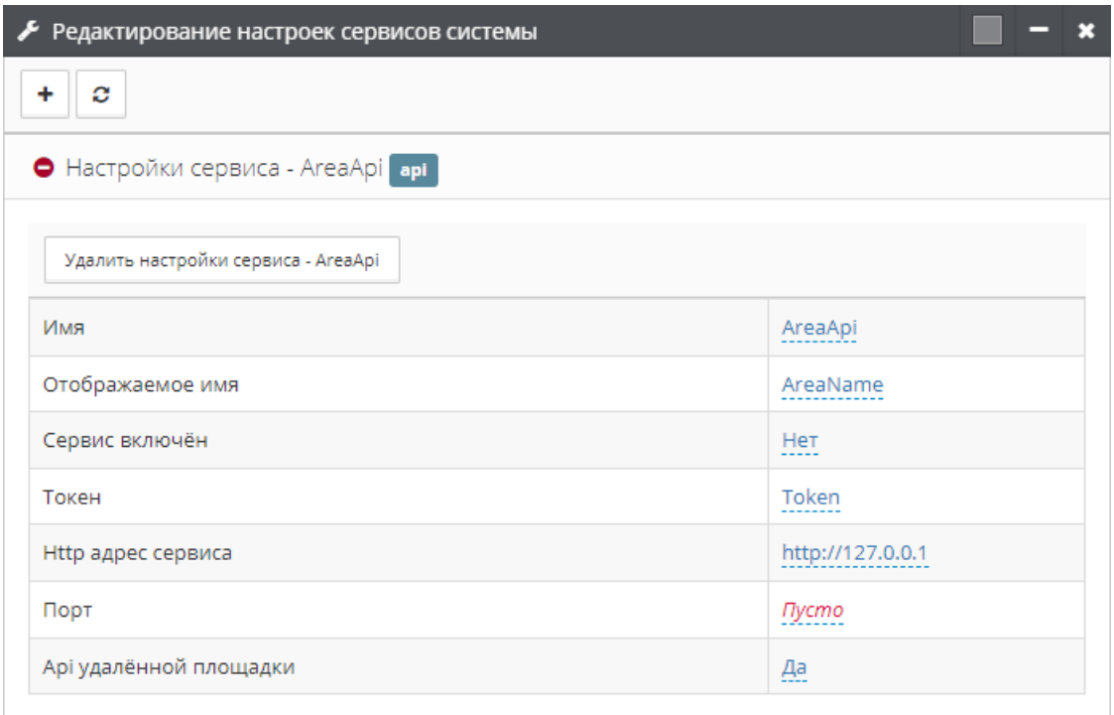

Рис. 3.14. Настройка сервисов

JWT (JSON Web Tokens) является открытым стандартом (RFC 7519), который широко применяется для создания токенов

доступа в формате JSON. Этот метод находит применение преимущественно в клиент-серверных приложениях для обмена данными, необходимыми для аутентификации пользователей. В процессе работы сервер генерирует токен, который затем защищается секретным ключом и передается клиенту. После получения токена клиент использует его для подтверждения своей идентичности в системе, обеспечивая таким образом безопасный доступ к ресурсам.

Сервера баз данных событий и инцидентов (рис. 15, рис. 16) содержит настройки подключения к соответствующим коллекциям mongo. Стоит отметить, что, поле «Хранение событий дней» определяет TTL индекс для соответствующей коллекции. Даная настройка не доступна для коллекции событий, которая назначена для сервера корреляции ретроспективного анализа (так как в эту коллекцию восстанавливаются архивные события).

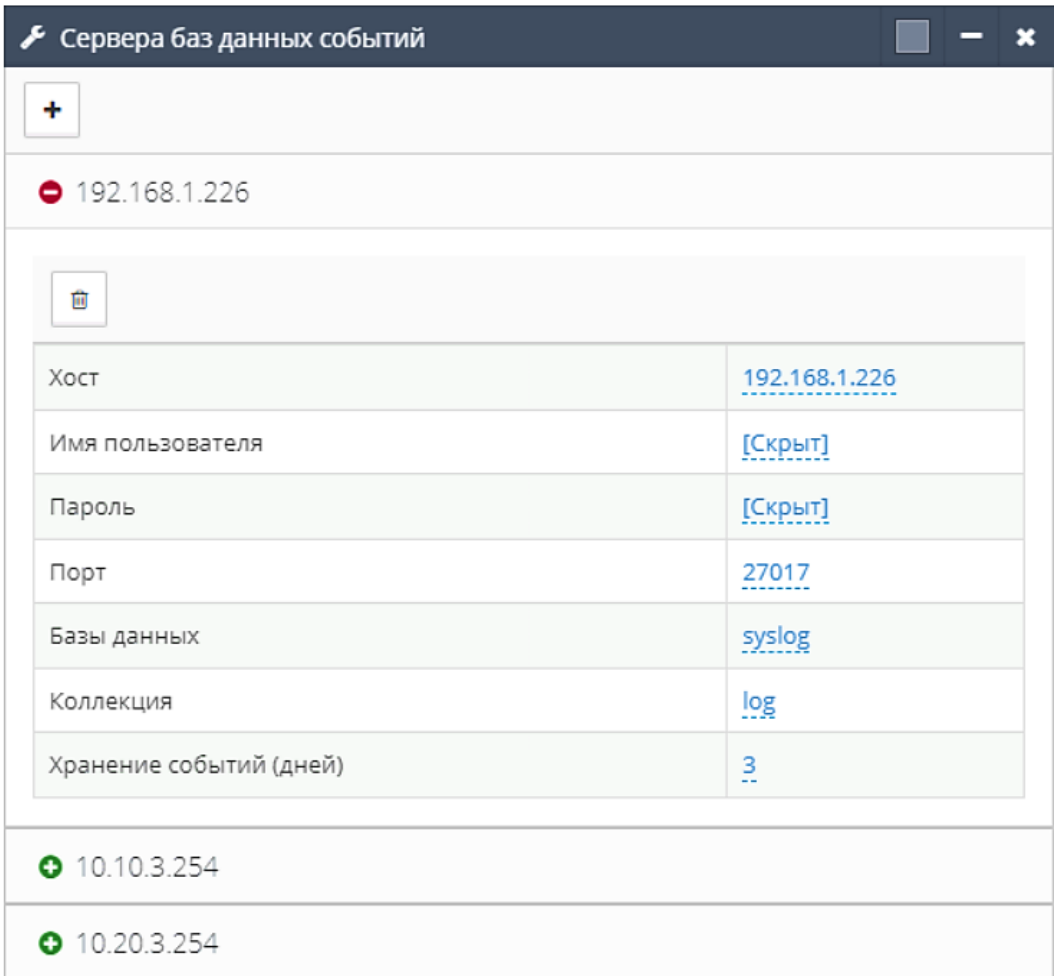

Рис. 3.15. Сервера БД событий

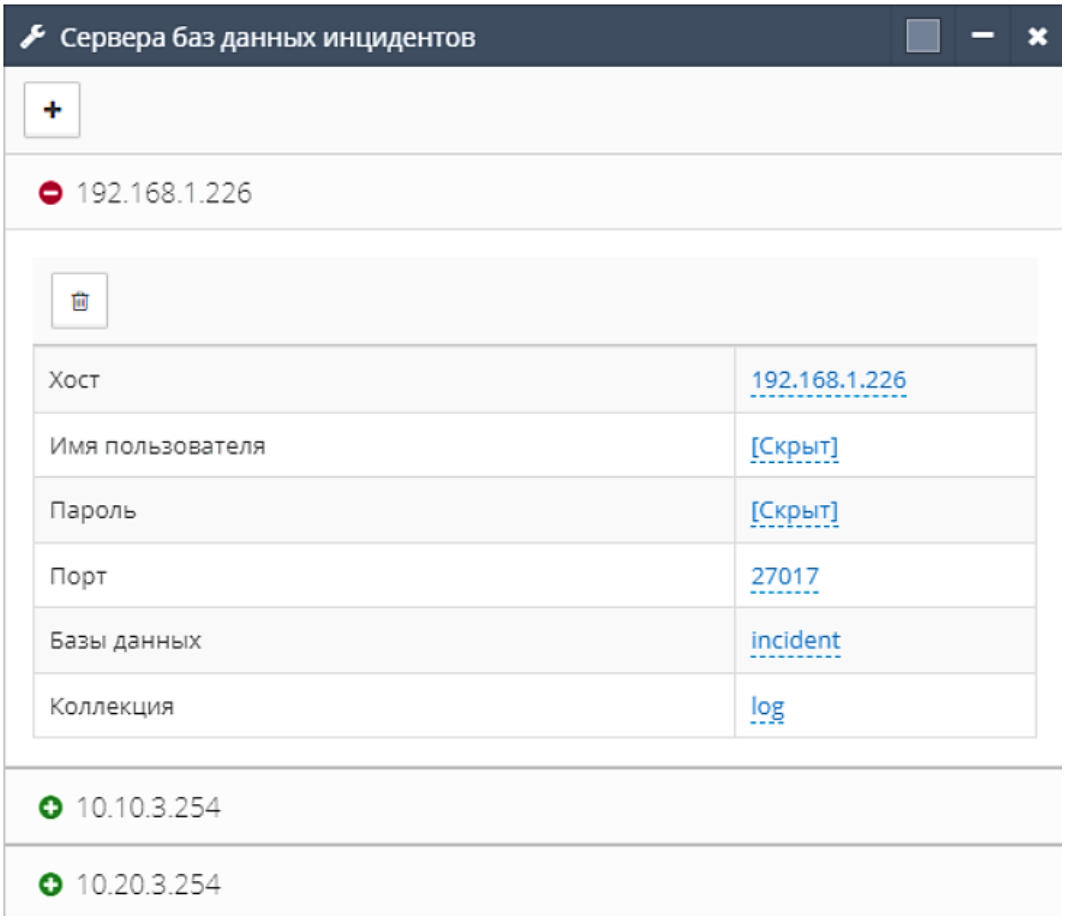

Рис. 3.16. Сервера БД инцидентов

Для сервера корреляции (рис. 3.17) предусмотрены следующие настройки:

а) IP-адрес сервера корреляции.

б) Порт сервера корреляции.

в) Имя пользователя для управления сервером корреляции.

г) Пароль для управления сервером корреляции.

д) Директория правил – где хранятся файлы правил корреляции на сервере.

е) Основной сервер – для главного сервера корреляции необходимо установить значение «ДА».

ж) Сервер ретроспективного анализа – для ретроспективного сервера корреляции необходимо установить значение «ДА».

з) Сервер БД событий – выбор коллекции событий из настроенных в виджете «Сервера баз данных событий».

и) Сервер БД инцидентов – выбор коллекции инцидентов из настроенных в виджете «Сервера баз данных инцидентов».
к) Директория хранения архива – настройка доступна для главного сервера корреляции, в том числе указывает, где хранятся файлы архивных событий

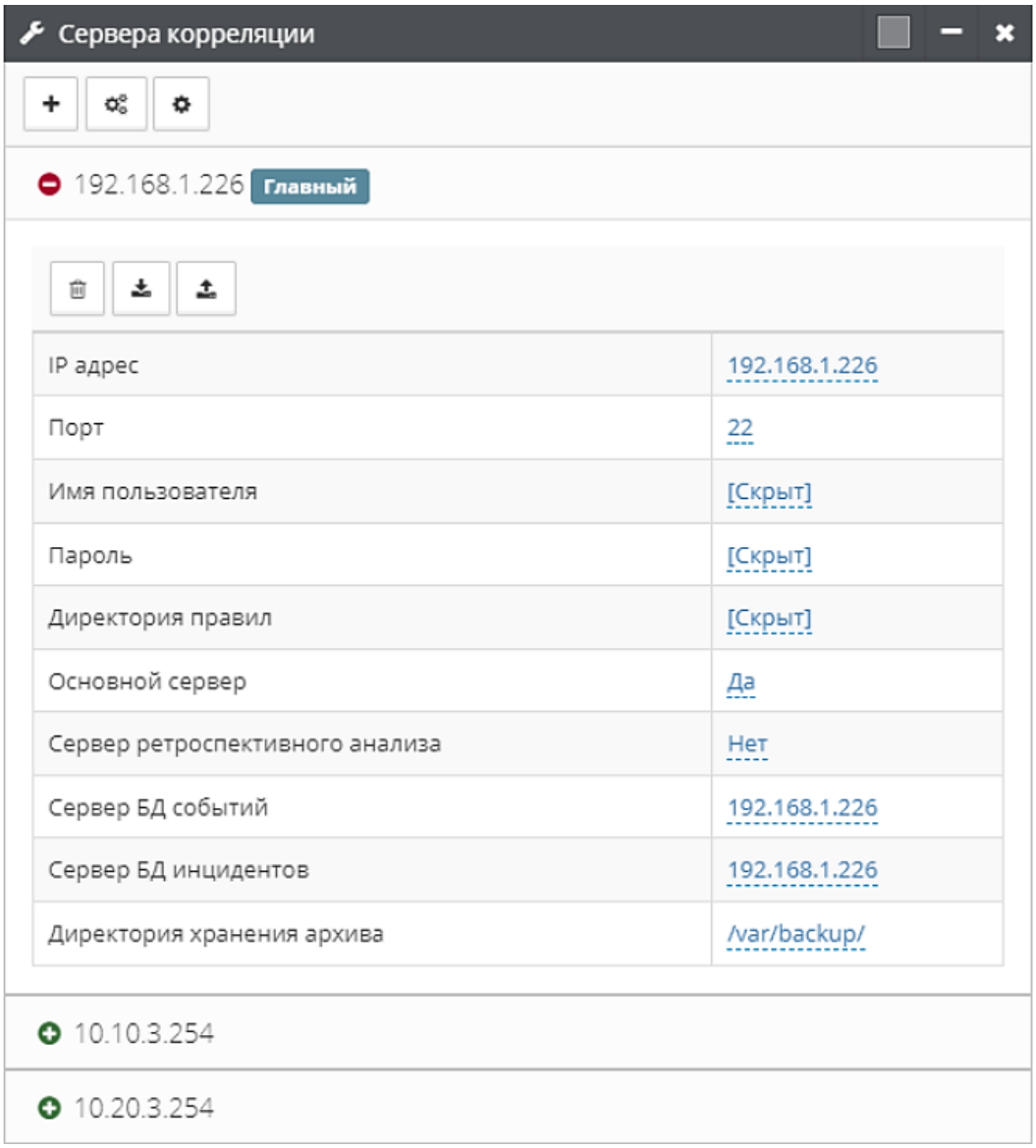

Рис. 3.17. Сервера корреляции

Ретроспективный анализ (рис. 3.18) настраивает отправку событий на сервер ретроспективного анализа, содержащая:
а) IP-адрес коллектора.
б) Порт коллектора.

в) Протокол коллектора.
г) Задержка (миллисекунд) между отправкой событий.
д) Сервер корреляции – в данном поле значение сопоставимо со значением сервера корреляции в виджете «Сервера корреляции».

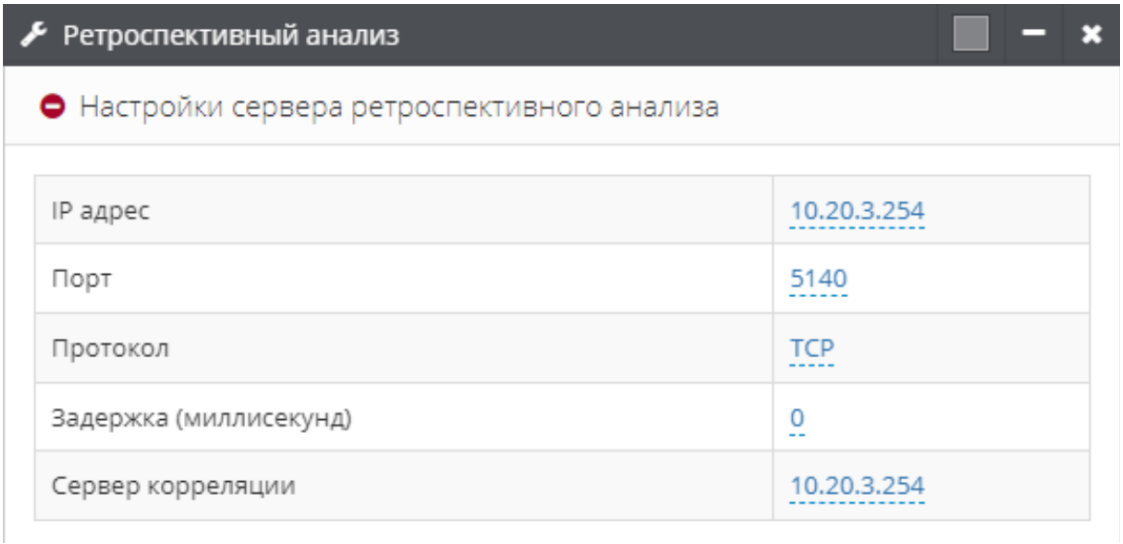

Рис. 3.18. Ретроспективный анализ

Сообщения о результатах работы компонентов SC SIEM, в том числе ошибки и предупреждения, приведены в «Системном журнале» в виде списка. В списке указывается дата и время получения сообщения, область приложения, которая сгенерировала сообщение, поле сообщения, критичность на основе уровне syslog (рис. 3.19).

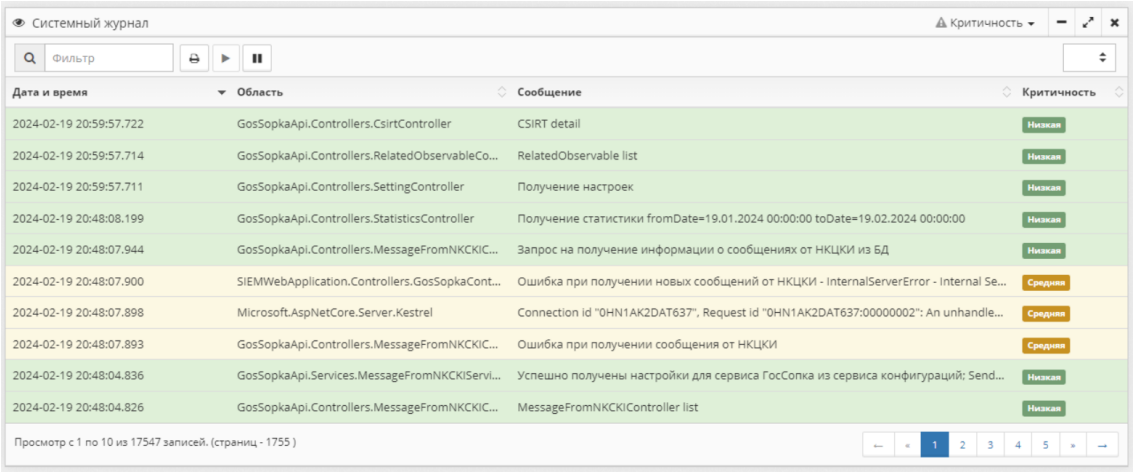

Рис. 3.19. Системный журнал

В SC SIEM возможно также редактирование настроек инцидентов и событий. Представлены три группы настроек: настройки графиков SparkLine и сводной статистики, инциденты, события.

В первом случае возможно внесение изменений в такие параметры как:

- частота обновления информации о количестве событий и инцидентов на SparkLine (рис. 3.20);

Рис. 3.20. SparkLine

- максимальное количество дней, за которые будут выводиться данные в SparkLine (блоке оперативной статистики);
- частота обновления Сводной статистики (секунд) (рис. 3.21).

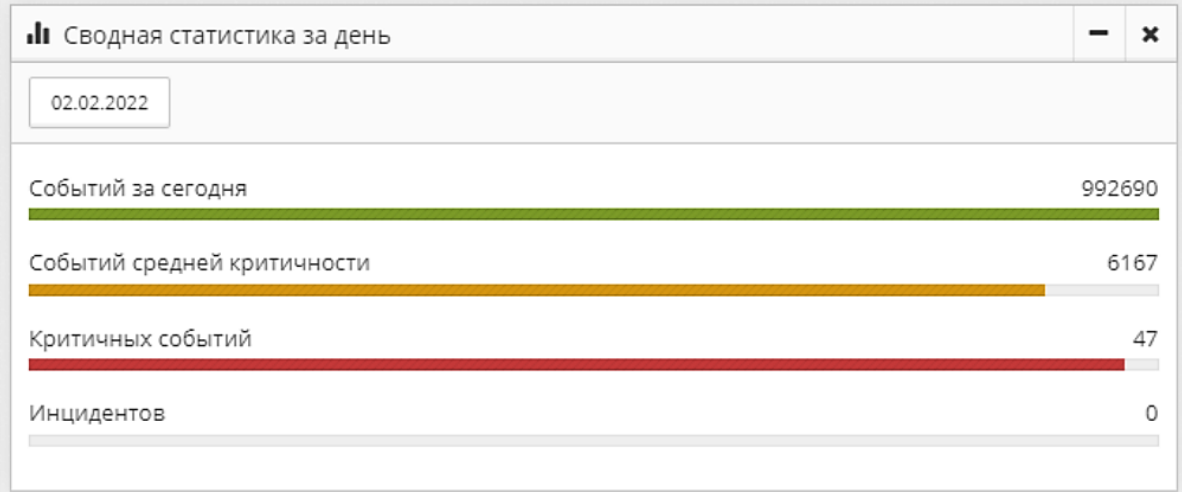

Рис. 3.21. Сводная статистика

Во втором случае вносятся изменения в параметры работы с инцидентами:

- Интервал времени, за который проверяется появление инцидентов для отображения всплывающих уведомлений об инцидентах.
- Количество дней, за которые будут отображаться необработанные инциденты во всплывающих уведомлениях.

- Показывать уведомления с установленным уровнем критичности и выше.
- Максимальное количество всплывающих уведомлений об инцидентах, отображаемых одновременно, если установлен 0 уведомления не появляются.
- Частота обновления.
- Глубина поиска. Используется для установки «по умолчанию» фильтра поиска «Дата и время».

И в третьем случае – в параметры работы с событиями. Используются такие же параметры, как и во втором случае.

Редактирование настроек «Статистика» (рис. 3.22).

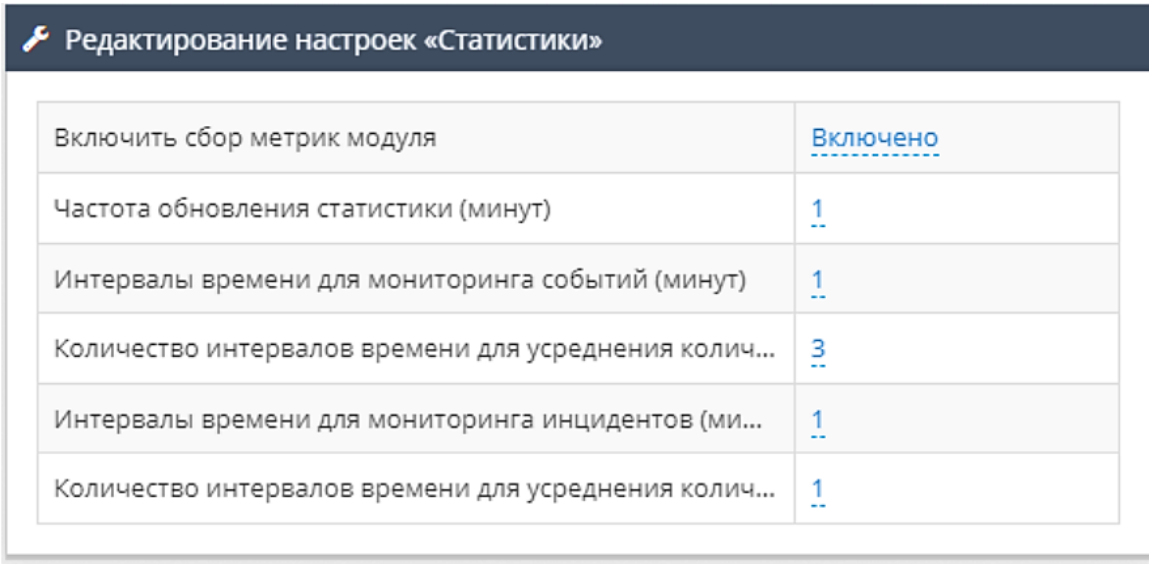

Рис. 3.22. Настройки «Статистики»

Параметр «Включить сбор метрик модуля» – включает запись информации о работе службы сбора статистики в лог работы приложения,

ЗАКЛЮЧЕНИЕ

Управление событиями безопасности на рабочих пространствах, серверах, сетевых устройствах и других узлах локальной сети – это сложная задача, которая требует автоматизации для эффективного исполнения. Современная система мониторинга и корреляции событий информационной безопасности (SIEM) предоставляет администраторам информационной безопасности возможность контролировать работу всех защищаемых активов. Включение автоматизации в процесс управления событиями безопасности существенно повышает эффективность и надежность системы. Это подтверждает необходимость внедрения передовых технологий в сфере информационной безопасности.

Система SIEM обладает уникальной способностью агрегировать данные о безопасности с множества устройств, произведённых различными компаниями, а также с компьютеров, функционирующих на разнообразных операционных системах. Одно из ведущих достоинств этой системы заключается в её возможности нормализации данных. Она анализирует журналы аудита и представляет результаты в структурированной форме, что значительно облегчает обращение с информацией о безопасности и ускоряет процесс поиска необходимых данных. Такой подход позволяет экспертам сконцентрироваться на анализе и оперативном реагировании на угрозы, минимизируя время, затрачиваемое на первичную обработку информации.

Система также оснащена механизмами управляемых правил корреляции и автоматизированного выявления инцидентов, что способствует быстрому реагированию на возможные угрозы. Встроенные функции управления задачами по расследованию инцидентов и координации действий команды информационной безопасности обеспечивают организованность и систематичность во всех аспектах работы с данными. Эти особенности делают SIEM неоценимым инструментом для эффективного управления

безопасностью в информационных средах, где время и точность являются критически важными факторами [19, 20].

SIEM можно использовать в инфраструктурах любого масштаба. Высокая производительность компонентов и возможность масштабирования позволяют адаптироваться к любому количеству узлов в сети и оптимально использовать аппаратные ресурсы для развертывания системы. Это делает систему гибкой и способной к адаптации под любые требования бизнеса. Дополнительным преимуществом для крупных инфраструктур является поддержка ролевого доступа администраторов безопасности. Это позволяет обеспечить доступ к отдельным функциям продукта и контролируемым узлам для сотрудников различных уровней. Таким образом, система становится более управляемой и безопасной.

В учебно-методическом пособии приведены следующие результаты: проведен анализ специфики функционирования современных систем управления инцидентами безопасности, рассмотрены особенности системы мониторинга и корреляции Security Capsule SIEM (Security Information and Event Management), определены требования для интеграции Security Capsule SIEM, предложены рекомендации по аппаратной части и схеме расположения компонентов Security Capsule SIEM.

СПИСОК ИСТОЧНИКОВ

1. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 года № 149-ФЗ // СПС «КонсультантПлюс»

2. О персональных данных : Федеральный закон от 27 июля 2006 года № 152-ФЗ // СПС «КонсультантПлюс».

3. Доктрина информационной безопасности Российской Федерации : утв. Президентом Российской Федерации № 646 от 05.12.2016 // СПС «КонсультантПлюс».

4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

5. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – Введ. 2009-10-01.

6. Воробьев А. В. Создание системы защиты информации в составе информационно-технологической инфраструктуры МВД России с учетом ее «облачной архитектуры» / А. В. Воробьев, В. В. Поваров // Информационные технологии, связь и защита информации МВД России. – 2015.

7. Ершов А. Л. Подход к формированию модели данных события информационной безопасности / А. Л. Ершов, С. В. Карасёв, С. А. Поляков, Д. А. Рыболовлев // Информационные системы и технологии. – 2017. – № 6 (104). – С. 124–129.

8. Завгородний В. И. Комплексная защита информации в компьютерных системах : учебное пособие / В. И. Завгородний. – Москва : Логос; ПБОЮЛ Н.А. Егоров, 2008. – 264 с.

9. Технические средства и методы защиты информации : учебник для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков [и др.]; под ред. А. П. Зайцева и А. А. Шелупанова. – Москва : Горячая линия – Телеком, 2009. – 616 с.

10. Котенко И. В. SIEM-системы для управления информацией и событиями безопасности / И. В. Котенко, И. Б. Саенко // Защита информации. Инсайд. – 2012. – № 5. – С. 54–65.

11. Новиков А. А. Уязвимость и информационная безопасность телекоммуникационных технологий : учебное пособие для вузов / А. А. Новиков, Г. Н. Устинов ; Под ред. Г. Н. Устинова. – Москва : Радио и связь. 2013. – 296 с.

12. Панов Н. Д. Инфорационная безопасность компьютерных систем / Н. Д. Панов, Д. А. Мотюк // Information Security. – Мосва : СОП-С. – V. 4. 5. – С. 10–21.

13. Романов О. А. Организационное обеспечение информационной безопасности : учебник для студ. высш. учеб. заведений / О. А. Романов, С. А. Бабин, С. Г. Жданов. – Москва : Академия, 2013. – 192 с

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

15. Хорев А. А. Техническая защита информации : учеб. пособие для студентов вузов. В 3-х т. / А. А. Хорев. – Москва : Аналитика, 2012. – 2014.

16. Грани SIEM. Эволюция Security Capsule SIEM // А. А. Графов, С. А. Графов, В. И. Тимченко, А. А. Жорин, ООО «ИТБ». – URL: https://www.itsec.ru/articles/grani-siem-evolyuciya-security-capsule-siem).

17. Иванов О. Что такое SIEM-системы и для чего они нужны?/ О. Иванов. – URL: https://www.anti-malware.ru.

18. ИТБ. Security Capsule SIEM описание применения. – URL: https://www.itb.spb.ru/upload/docs/Security_Capsule_SIEM.

19. Медведев В. А. Обзор SIEM-систем на мировом и российском рынке / В. А. Медведев. – URL: https://www.anti-malware.ru/.

20. Москвин А. Обзор российского рынка SIEM-систем 2024 /А. Москвин. – URL: https://www.antilware.ru/analytics/Market_

Учебное издание

Михаил Михайлович Жуков,
кандидат технических наук, доцент;
Александр Олегович Авсентьев,
кандидат технических наук

МЕХАНИЗМЫ И СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Учебно-методическое пособие

Редактор А. Г. Лиопа

Компьютерная верстка А. О. Авсентьева

Подписано в печать 24.10.2024
Формат 60x84 1/16
Усл. печ. л. 4,15
Тираж 50 экз.
Заказ № 131

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53