МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Кафедра «Прикладная математика и информатика»
(наименование)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)
Управление корпоративными информационными процессами
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему: «Методы и средства управления информационной безопасностью на основе SIEM-технологии»

Обучающийся Д.А. Казьмин _____
(Инициалы, Фамилия) (личная подпись)

Научный руководитель д.т.н., доцент, С.В. Мкртычев
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2024

Оглавление

Введение

Конечная цель любой системы безопасности информации - защитить организацию от возможных угроз и инцидентов, связанных с информацией. Однако, в современном цифровом мире, атаки становятся все более сложными и утонченными, что требует более эффективных подходов к обнаружению, анализу и расследованию инцидентов информационной безопасности.

Одним из ключевых инструментов, используемых организациями для обнаружения и расследования указанных инцидентов, являются системы безопасности информации и управления событиями (Security Information and Event Management, SIEM). SIEM-системы собирают, агрегируют и анализируют информацию о событиях безопасности из различных источников, таких как журналы аудита, системы обнаружения вторжений, брандмауэры и другие устройства, с целью обнаружения потенциальных угроз.

Тема выпускной квалификационной работы является актуальной, так как исследования компаний, занимающихся анализом информационной безопасности (ИБ), убеждают в необходимости внедрения информационных систем, которые позволяют расследовать инциденты ИБ в организациях любого уровня. Исследования, проводимые «Лабораторией Касперского», показали, что две трети ИБ-инцидентов (67%) вызваны действиями плохо информированных либо невнимательных сотрудников. При этом, согласно данным исследования ESET, 84% компаний недооценивают риски, обусловленные человеческим фактором.

«Системы управления информацией и событиями безопасности (SIEM) предназначены для того, чтобы помочь организациям отслеживать угрозы безопасности и реагировать на них в режиме реального времени. Собирая, анализируя и сопоставляя данные из нескольких источников, системы SIEM могут предоставить всестороннее представление о состоянии безопасности организации и помочь выявить потенциальные угрозы безопасности» [2].

Но, при всей функциональности и полезности этих систем, не каждой организации удается внедрить ее в свою инфраструктуру, да и не каждой компании это необходимо. Связано это с тем, что внедрение SIEM-системы зависит от множества факторов, в особенности ИТ-инфраструктуры организации, ее масштабов, наличия нужных специалистов и т.д. Эти системы считаются достаточно сложными в построении и внедрении, из-за чего может возникнуть множество проблем. Именно этим проблемам и способам их решения и посвящена данная работа.

В связи с ростом числа угроз и актуальностью использования средств защиты информации в организациях вопросам внедрения различных средств защиты уделяется достаточно много внимания. SIEM-системы сами по себе являются новым средством обеспечения информационной безопасности, только набирающим популярность. Кроме того, в последние годы ситуация осложнилась санкциями, уходом зарубежных компаний с рынка России, из-за чего организациям приходится менять инфраструктуру. Поэтому постоянно всплывают новые и новые проблемы во внедрении SIEM-систем.

Объект исследования – сетевая инфраструктура корпорации «Росатом».

Предмет исследования – методы и средства управления информационной безопасностью на основе SIEM.

Цель ВКР – исследовать методы и средства управления информационной безопасностью на основе SIEM-технологии.

Для достижения поставленной цели в работе необходимо решить следующие задачи:

- рассмотреть теоретические основы обеспечения информационной безопасности с помощью SIEM;
- проанализировать сетевую инфраструктуру предприятия и обосновать необходимость внедрения системы SIEM;
- определить алгоритм внедрения SIEM-системы и разработать модель создания универсальных правил корреляции для корректной настройки SIEM-системы и её дальнейшего эффективного использования.

Гипотеза исследования: использование разработанного в рамках диссертационного исследования порядка внедрения и настройки SIEM-системы в существующую инфраструктуру организации обеспечит повышение ее информационной безопасности.

Методы исследования. В процессе исследования будут использованы следующие положения и методы: системный анализ, аналитический и сравнительный методы, методы оценки актуальности угроз.

Новизна исследования заключается в разработке алгоритма внедрения SIEM-системы, которая обеспечит эффективное управление информационной безопасностью в компании.

Практическая значимость исследования заключается в возможности применения предлагаемых рекомендаций при внедрении SIEM-системы в реальную организацию.

Теоретической основой диссертационного исследования являются научные труды российских и зарубежных ученых, занимающихся проблемами внедрения SIEM-систем в информационную структуру предприятий.

Основные этапы исследования: исследование проводилось с 2021 по 2024 год в несколько этапов.

На первом (констатирующем) этапе была сформулирована тема исследования и его гипотеза, выполнялся сбор информации по теме исследования из различных источников, определялись цели, задачи, предмет и объект исследования, а также была определена проблематика в рамках проводимого исследования.

Второй этап – поисковый. В ходе проведения данного этапа осуществлялся анализ методов управления информационной безопасностью предприятий, разработаны алгоритмы выбора внедрения SIEM-системы в инфраструктуру предприятия, опубликована статья по теме исследования в научном издании.

На третьем этапе осуществлялась апробация предлагаемых рекомендаций, сформулированы выводы о полученных результатах по

проведенному исследованию.

На защиту выносятся:

- алгоритм внедрения SIEM-системы в существующую инфраструктуру компании;
- алгоритм разработки универсальных правил корреляции;
- результаты апробации предлагаемых проектных решений.

По теме исследования опубликована одна статья:

Казьмин, Д. А. Проблемы внедрения SIEM-систем / Д. А. Казьмин // Тенденции развития науки и образования. – 2023. – № 102-5. – С. 19-22. – DOI 10.18411/trnio-10-2023-242. – EDN JZPKBC.

Диссертация состоит из введения, трех глав, заключения и списка литературы.

Во введении обоснована актуальность темы исследования, представлены объект, предмет, цели, задачи и положения, выносимые на защиту диссертации.

В первой главе дан анализ существующих методов обеспечения информационной безопасности сетей. Особое внимание уделено SIEM-системам и проблемам их внедрения в инфраструктуру компаний.

Во второй главе проведен анализ используемых методов и средств управления информационной безопасностью в рассматриваемой организации, оценена их эффективность.

Третья глава посвящена разработке приемов и методов эффективного внедрения SIEM и её последующего использования.

В заключении приводятся результаты исследования.

Работа изложена на 112 страницах и включает 42 рисунка, 11 таблиц, 34 источника.

Глава 1 Анализ теоретических основ обеспечения информационной безопасности сетей

1.1 Методы и средства обеспечения информационной безопасности сетей

«Информационная безопасность – это защищенность информации от незаконного ознакомления с ней, ее преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, которые направлены на нарушение их работоспособности» [1].

Система защиты информации включает следующие элементы:

- «физические средства – механические, электрические, электромеханические, электронные, электронно-механические устройства и системы, функционирующие автономно и создающие различного рода препятствия на пути злоумышленника (турникеты, видеокамеры, системы доступа, замки и т.д.)» [5];
- аппаратные средства – электронные и электронно-механические устройства, встраиваемые в системы обработки данных с целью защиты информации. К ним могут быть отнесены системы контроля и управления доступом, аппаратные межсетевые экраны и т.д.;
- программные средства – программное обеспечение, внедряемое с целью защиты информации. Представляют собой самый широкий спектр средств защиты. К ним относятся криптографические средства защиты, системы обнаружения вторжений, системы резервного копирования и т.д.;
- организационные средства – организационные мероприятия, обеспечивающие и регламентирующие функционирование системы защиты информации. Самой распространенный способ защиты – это разработка политики безопасности. Также разрабатываются различные положения, например, о конфиденциальных данных, об

использовании электронной почты и т.д.;

- законодательные средства – система нормативно-правовых акты, устанавливающая права и обязанности, а также ответственность лиц и подразделений, имеющих отношение к обеспечению информационной безопасности (законы, постановления, ГОСТ, приказы и т.д.);
- психологические или морально-этические средства – моральные нормы или этические правила, сложившиеся в обществе или коллективе, и способствующие повышению уровня защищенности от угроз безопасности информации.

Одним из главных компонентов системы защиты информации любой организации является её техническая защита.

Инженерно-техническая защита – это «совокупность технических средств и мероприятий по их использованию, а также специальных органов, в интересах защиты конфиденциальной информации» [23].

«Технические средства защиты информации (ТСЗИ) используются для защиты речевой или электронной информации и применяются в отношении следующих объектов:

- помещения. Средства защиты обеспечивают безопасность речевой информации, например, во время совещаний. Используются средства, создающие акустический шум и препятствующие возможной утечке информации;
- телефонные линии. Признан наиболее опасным способом передачи информации. Для предотвращения потенциальной утечки информации применяются средства защиты, которые инициируют искусственные помехи на линии связи, осуществляют контроль подачи электрического тока и блокировку запуска устройств записи информации;
- электронные системы. Для защиты информации в различных объектах информатизации применяются генераторы шума, заглушающие

распространение информационных сигналов.

Технические средства защиты информации подразделяются на аппаратные, физические и программные средства.

К аппаратным средствам защиты относятся различные сооружения и средства, которые создают препятствие для физического доступа (или проникновения) нарушителей на объекты защиты и к материальным носителям конфиденциальной информации. Такие средства защищают материальные средства, сотрудников, информации и финансов от противоправных воздействий. К ним относятся охранная и пожарная сигнализация, система контроля и управления доступом (СКУД), системы видеонаблюдения и т.д. (рисунок 1)» [5].

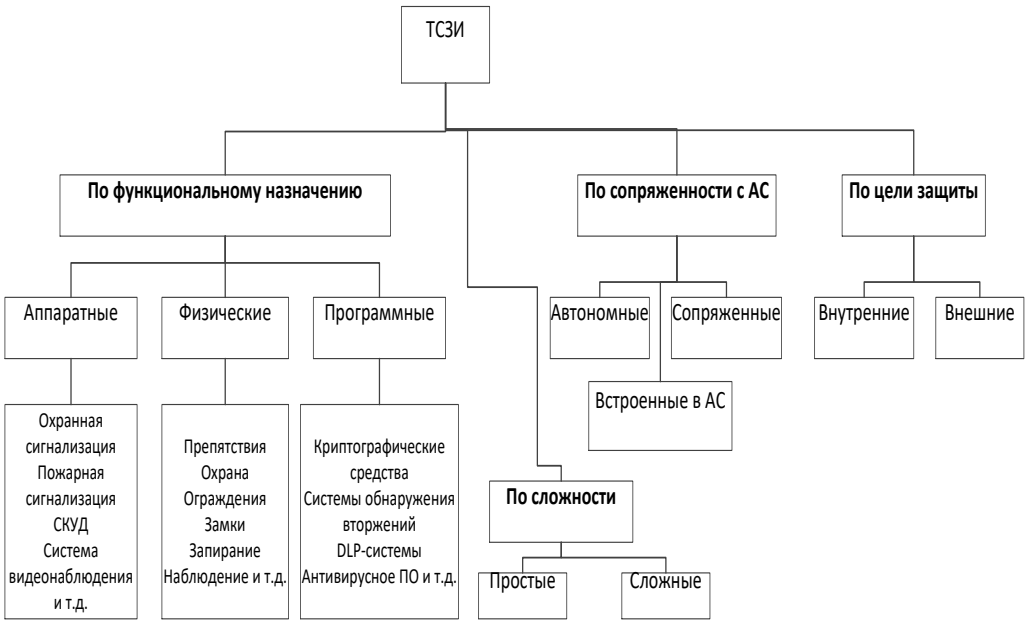

Рисунок 1 – Классификация ТСЗИ

«Аппаратные средства имеют такие преимущества, как надежность, устойчивость к модификациям.

Недостатки аппаратных средств – высокая стоимость, недостаточная гибкость, большие габариты.

Программные средства защиты включают самый широкий спектр

программ: системы защиты от НСД, межсетевые экраны, антивирусное программное обеспечение (ПО), криптографические средства, системы обнаружения вторжений, DLP-системы и т.д.

Для защиты серверов и рабочих станций можно использовать:

– средства доверенной загрузки;
– программное обеспечение СЗИ от НСД;
– программно-аппаратный комплекс СЗИ от НСД» [5].

«Доверенная загрузка – это загрузка различных операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и аппаратной идентификации/аутентификации пользователя» [6]. Схема работы приведена на рисунке 2.

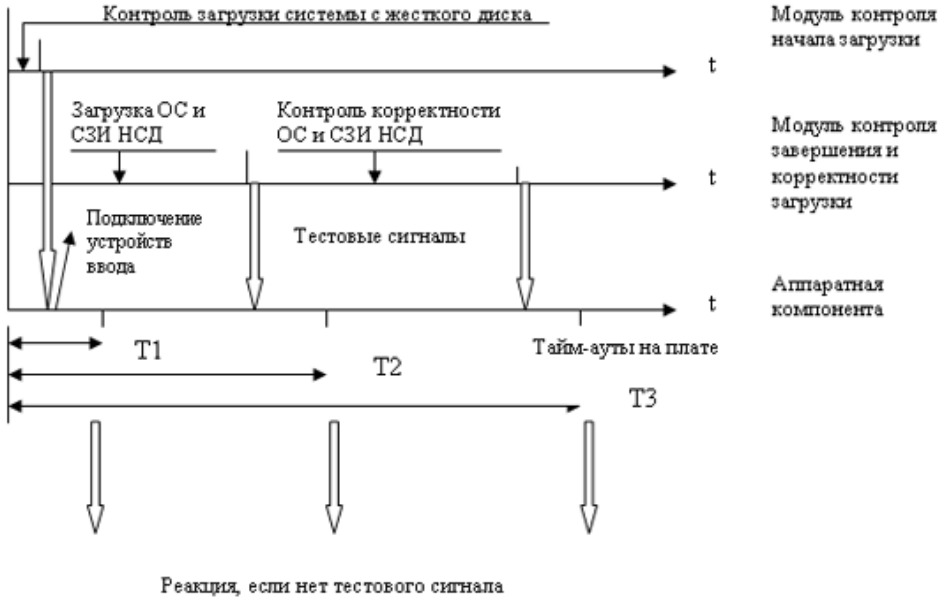

Рисунок 2 – Средства доверенной загрузки

«На различных этапах загрузки компьютера доверенная загрузка может быть выполнена различными средствами, и, следовательно, будет обладать различной функциональностью» [31].

«Средства защиты информации от НСД делятся на два типа:

– программное обеспечение СЗИ от НСД;

– программно-аппаратный комплекс (ПАК) СЗИ от НСД» [14].

«Для защиты данных, передаваемых по указанным каналам связи, необходимо использовать межсетевые экраны и/или программные средства, позволяющие создавать виртуальные частные сети» [7].

«Межсетевой экран (МЭ) – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача – не пропускать пакеты, не подходящие под критерии, определённые в конфигурации» [33].

Принцип работы межсетевого экрана приведен на рисунке 3.

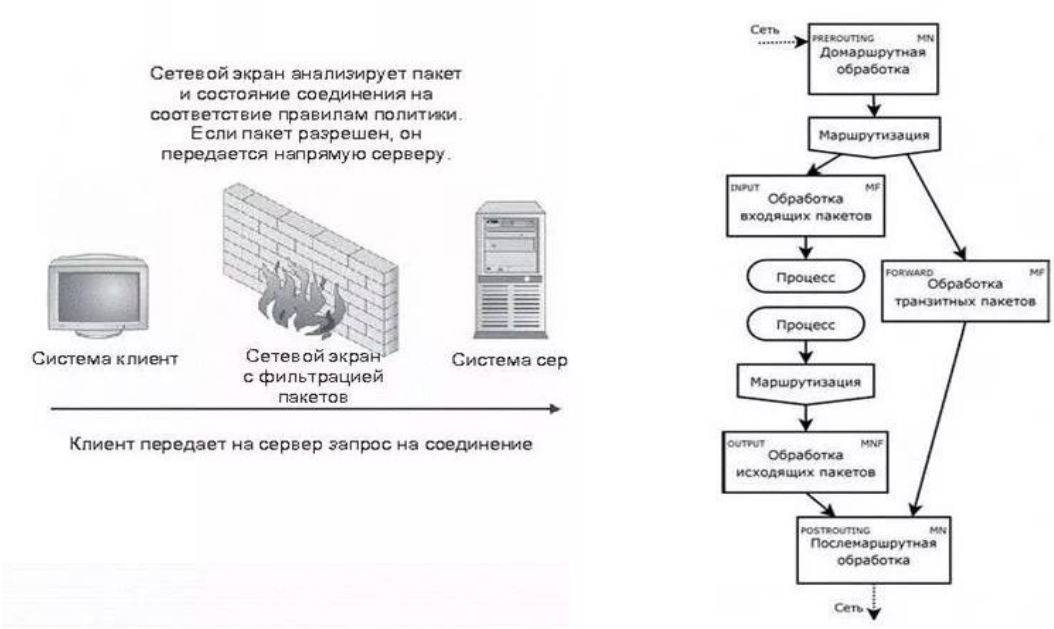

Рисунок 3 – Принцип работы межсетевого экрана

Защищенная передача данных по технологии VPN используется для объединения физически удалённых объектов (сетей или отдельных хостов) в общую виртуальную сеть, используя сети общего пользования, и исключая

при этом необходимость прокладывать дополнительные каналы связи. Для обеспечения безопасности передаваемого трафика применяется туннелирование и различные средства кодирования (шифрования) [10].

На Западе чаще всего для защиты трафика применяются протоколы IPSec, PPTP, L2TP и др., использующие алгоритмы DES (56-bit), 3DES (168-bit) и AES (128-bit / 256-bit) [3].

Схема работы VPN приведена на рисунке 4.

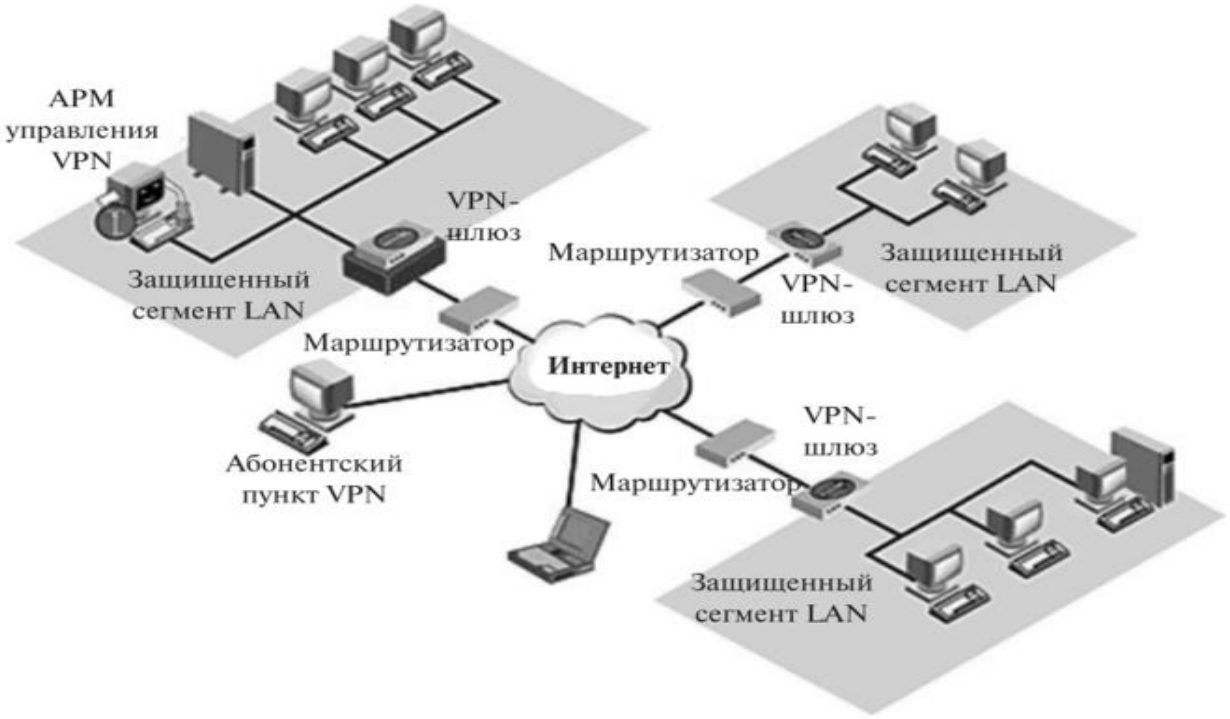

Рисунок 4 – Схема работы VPN

В нашей стране вопрос применения криптографических средств регулируется ФСБ России. Опуская формальные аспекты, скажем лишь, что для защиты данных, отнесённых к категориям конфиденциальных, секретных, совершенно секретных или особой важности, требуется применение сертифицированных средств, реализующих алгоритм ГОСТ 28147-89 [18].

Существуют две основные схемы построения VPN сетей. Схема «сеть-сеть» обычно применяется для соединения удалённых офисов предприятия,

которые могут находиться в разных городах и даже странах. В каждом из офисов устанавливается VPN-шлюз, который бывает встроен в межсетевой экран. Следует иметь в виду, что трафик защищается только внутри самого VPN-туннеля – внутри каждой из сетей он не защищён.

Схема «точка-сеть» чаще всего служит для подключения к сети компании удалённых сотрудников, при нахождении последних вне офиса (например, в командировке). Для этого на компьютере пользователя должен быть установлен VPN-клиент, которым пользователь будет подключаться к VPN-шлюзу компании через Интернет [20].

«Система обнаружения (предупреждения) вторжений (СОВ) – программное или аппаратное средство, предназначенное для выявления фактов или попыток неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими через сеть Интернет» [5]. В английской терминологии данное техническое решение носит название «Intrusion Detection System (IDS)».

DLP-системы являются комплексным инструментом для реализации стратегии по предотвращению утечек чувствительных и значимых для компании данных. Системы данного класса позволяют предотвратить возможные утечки конфиденциальной информации из информационных систем компании во внешнюю сеть. [34].

Средства криптографической защиты информации (СКЗИ) – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении [31].

1.2 Характеристика информационных систем класса SIEM, их роль, значение и функционал в информационной инфраструктуре компании

Инструменты SIEM – это программные платформы, которые объединяют данные журналов событий по нескольким системам и приложениям, серверам и устройствам безопасности. Исторические данные журнала и события в реальном времени также можно комбинировать с контекстной информацией о пользователях, активах, угрозах и уязвимостях.

Основополагающие принципы любой SIEM-системы заключаются в объединении соответствующих данных из нескольких источников, выявлении отклонений от нормы и принятии соответствующих мер. Например, при обнаружении потенциальной проблемы система SIEM может регистрировать дополнительную информацию, генерировать предупреждение и давать указания другим средствам контроля безопасности остановить выполнение операции.

Основными принципами работы SIEM-системы являются:

- «сбор событий: SIEM-система собирает и агрегирует лог-файлы, события и алерты (предупреждения) из различных источников, таких как сетевые устройства, серверы, приложения и системы безопасности;
- анализ: SIEM-система анализирует собранные события и использует различные методы, такие как корреляция, профилирование, анализ поведения, детектирование атак и машинное обучение, для идентификации потенциальных угроз и инцидентов;
- уведомление: SIEM-система уведомляет ответственных лиц об инцидентах, используя различные методы оповещения, такие как электронная почта, SMS-сообщения, сообщения в службе тикетов и т.д.» [6];
- расследование: SIEM-система позволяет проводить расследование

инцидентов, используя собранные данные и результаты анализа. Она помогает выявить причины инцидентов, определить масштаб ущерба, установить последствия и принять меры для предотвращения повторения подобных инцидентов в будущем.

Основные этапы работы системы приведены на рисунке 5.

На самом базовом уровне система SIEM может основываться на правилах или использовать механизм статистической корреляции для установления связей между записями журнала событий. Продвинутые системы SIEM эволюционировали, чтобы включать аналитику поведения пользователей и объектов, а также организацию безопасности, автоматизацию и реагирование(SOAR).

Рисунок 5 – Этапы работы системы

Системы SIEM работают путем иерархического развертывания нескольких агентов сбора данных для сбора событий, связанных с безопасностью, с устройств конечных пользователей, серверов и сетевого оборудования, а также специализированного оборудования безопасности,

такого как брандмауэры, антивирусные программы или системы предотвращения вторжений (IPSE). Сборщики (коллекторы) событий информационной безопасности пересылают события на централизованную консоль управления, где аналитики безопасности анализируют полученные данные, расставляя при этом приоритеты инцидентов безопасности.

На рисунке 6 приведены наиболее популярные задачи внедрения SIEM-системы.

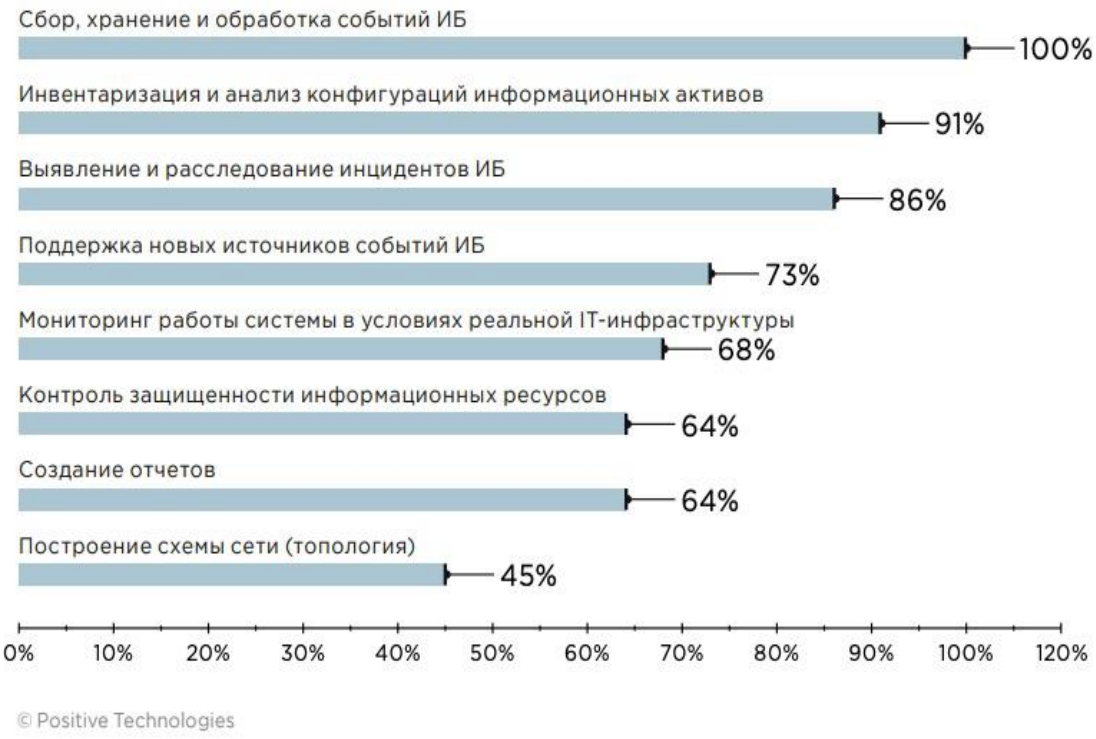

Рисунок 6 – Список популярных задач для пилотного внедрения SIEM (доля проектов)

SIEM – это не отдельное приложение, а набор компонентов. Системы SIEM отличаются функциями, но большинство систем имеют приведенные ниже компоненты и функционал.

Первый компонент – агрегация. Платформы SIEM собирают данные из тысяч различных источников, потому что данные события предоставляют данные, необходимые для анализа работоспособности и безопасности

локальной вычислительной сети в целом. Чтобы получить наиболее полное представление, необходимо объединить все собираемые сведения о событиях в рамках единой платформы. Агрегация – это процесс перемещения данных и файлов журналов событий из разрозненных источников в общий репозиторий. Собранные данные помещаются в однородное хранилище данных – обычно это специально созданные репозитории файлов или реляционные базы данных, - где происходит анализ, формируется отчетность, выполняются криминалистические операции, применяются архивные политики.

Процесс агрегирования – компиляции этих разнородных каналов сбора событий в общий репозиторий – является фундаментальным для управления журналами и большинства платформ SIEM. Агрегирование данных может выполняться путем отправки данных непосредственно на платформу SIEM (которая может быть развернута на нескольких уровнях), или промежуточный хост может собирать данные журнала из источника и периодически перемещать их в систему SIEM. Агрегация имеет решающее значение, поскольку необходимо управлять данными согласованным образом: необходимо систематически применять политики безопасности, хранения и архивирования. Наличие всех данных на общей платформе позволяет проводить корреляцию событий и анализ данных, которые являются ключевыми для решения описанных вариантов использования.

Существуют некоторые недостатки в объединении данных на общей платформе. Во-первых, это масштаб: анализ становится экспоненциально сложнее по мере роста набора данных. Централизованный сбор означает огромные хранилища данных, что значительно увеличивает вычислительную нагрузку на платформу SIEM. Архитектура SIEM может предполагать её масштабирование, однако, в конечном итоге этим системам требуется значительная мощность для обработки корпоративных данных. Системы, использующие централизованную политику фильтрации и хранения, требуют, чтобы все данные перемещались и сохранялись, как правило, несколько раз,

что увеличивает нагрузку на сеть.

Некоторые системы масштабируются с помощью распределенной обработки, когда фильтрация и анализ выполняются за пределами центрального репозитория, обычно в точке сбора распределенных данных. Это снижает вычислительную нагрузку на центральный сервер и позволяет выполнять обработку небольших, более управляемых наборов данных. Для этого требуется, чтобы политики вместе с кодом для их обработки распространялись и обновлялись по всей сети. Распределенные процессы агентов – достаточно удобная модель, но предъявляющая повышенные требования к ИТ-администрированию. Эта стратегия также увеличивает вычислительную нагрузку на точки сбора данных, снижая их производительность и потенциально замедляя работу настолько, что входящие данные могут быть утрачены.

Следующий обязательный компонент - обработка и нормализация. Если процесс агрегации заключается в объединении разнородных каналов событий в одну общую платформу, нормализация, в свою очередь, сводит разнородные записи к стандартным атрибутам событий. Дело в том, что большинство источников данных собирают одни и те же базовые атрибуты событий: время, пользователь, операция, сетевой адрес и так далее. Подобные средства syslog не только группируют общие атрибуты, но и предоставляют средства для сбора дополнительной информации, которая не соответствует основному шаблону. Нормализация – это когда известные атрибуты данных вводятся в общий шаблон, а все, что не подходит, просто исключается из нормализованного журнала событий.

В зависимости от поставщика некоторые SIEM, предусматривают возможность хранения исходных ненормализованных записей в отдельном репозитории для целей судебной экспертизы перед последующим архивированием или удалением, либо они могут быть просто отброшены. На практике отказываться от исходных данных — плохая идея, поскольку полные записи требуются для любого вида правоприменения. Таким образом,

большинство продуктов хранят необработанные журналы событий в течение заданного пользователем периода перед архивированием. В некоторых случаях платформа SIEM сохраняет ссылку на исходное событие в нормализованном журнале событий, что обеспечивает возможность «развертывания» для простого обращения к дополнительной информации, собранной с устройства.

Нормализация обеспечивает предсказуемое и согласованное хранение всех записей и индексирует эти записи для быстрого поиска и сортировки, что является ключевым моментом при расследовании инцидента. Кроме того, нормализация позволяет формировать отчеты и производить анализ по каждому событию независимо от источника данных.

Технически нормализация больше не является требованием на текущих платформах. Нормализация была необходимостью на заре SIEM, когда объемы хранилищ данных и вычислительная мощность были дорогостоящими, а платформы SIEM использовали системы управления реляционными базами данных для внутреннего управления данными. Достижения в области индексирования и поиска в репозиториях неструктурированных данных теперь позволяют хранить полные исходные данные, сохраняя исходные данные и устраняя накладные расходы на нормализацию.

Следующий обязательный компонент – корреляция. «После сбора, анализа и сохранения полученных данных следующим шагом в системах SIEM является корреляция событий из разных источников данных. Эта корреляционная работа основана на правилах, которые либо предоставляются различными инструментами SIEM, предопределены для различных сценариев атак, либо создаются и настраиваются аналитиком» [32].

Корреляция - один из ключевых компонентов любого инструмента SIEM. Она помогает определить, на что обратить внимание в огромном массиве выделенных потенциальных угроз. SIEM обрабатывает значительные объемы данных из всей цифровой среды и сравнивает последовательности

действий с предопределенными правилами для выявления возможных атак или угроз. Правила могут быть предварительно определены поставщиком SIEM или изменены по мере необходимости.

Если в используемом инструменте SIEM есть соответствующие правила, он сможет идентифицировать потенциальную угрозу из серии неудачных попыток входа в систему. Большинство продуктов SIEM, доступных на рынке, поставляются с предустановленными правилами корреляции. Рекомендуется изучить их и решить, какие из них будут полезны для бизнеса, и при необходимости разработать новые правила. Возможности SIEM можно обобщить следующим образом:

- интеграция аналитики угроз – инструменты SIEM интегрируются с внешними каналами и базами данных аналитики угроз, чтобы повысить их способность обнаруживать известные вредоносные действия и реагировать на них. Используя актуальную информацию об известных вредоносных программах, подозрительных IP-адресах и других признаках компрометации, они повышают свои возможности обнаружения угроз;
- предупреждения и уведомления – инструменты SIEM генерируют предупреждения и уведомления при обнаружении определенных событий или шаблонов безопасности. «Эти оповещения могут быть доставлены аналитикам безопасности или администраторам по различным каналам, таким как электронная почта, SMS или интеграция с платформами реагирования на инциденты, что способствует быстрому реагированию на инциденты» [21];
- отчетность о соответствии стандартам – инструменты SIEM помогают организациям соблюдать нормативные требования, предлагая готовые отчеты и шаблоны. Анализируя соответствующие данные о событиях безопасности, они создают отчеты о соответствии, демонстрирующие соблюдение определенных стандартов, таких как PCI DSS, HIPAA или GDPR;

- аналитика поведения пользователей и объектов (UEBA). «Инструменты SIEM включают возможности UEBA для обнаружения аномального поведения, демонстрируемого пользователями или объектами в ИТ-среде. Установив базовые уровни нормального поведения, они могут выявить отклонения, которые могут указывать на внутренние угрозы, взломанные учетные записи или другие злонамеренные действия» [9];
- криминалистический анализ – инструменты SIEM позволяют проводить тщательный криминалистический анализ событий и инцидентов, связанных с безопасностью. Они обеспечивают возможность поиска и исследования исторических данных журналов, проведения углубленного анализа и восстановления временных диаграмм событий. Это помогает в реагировании на инциденты и расследованиях после инцидентов.

Инструменты SIEM предлагают интуитивно понятные информационные панели и визуализации, которые представляют данные о событиях безопасности в ясной и понятной форме. Эти визуальные представления, такие как диаграммы, графики и схемы, позволяют аналитикам безопасности быстро выявлять тенденции, шаблоны и потенциальные риски безопасности.

Роль SIEM-системы в процессе обнаружения и расследования инцидентов заключается в том, что она позволяет сократить время реакции на инциденты, увеличить эффективность мониторинга и анализа событий, а также обеспечить единый централизованный доступ к информации о безопасности для всех заинтересованных сторон.

SIEM-система играет важную роль в процессе расследования инцидентов, предоставляя информацию о том, что произошло, когда произошло, кто был замешан и какие данные были украдены или повреждены. Эта информация позволяет анализировать источник инцидента, его характеристики и оценивать ущерб, который был причинен.

Например, на рисунке 7 приведена Панель управления SIEM для AWS в

Logz.io. На рисунке видно, какая информация имеется в системе для анализа инцидентов.

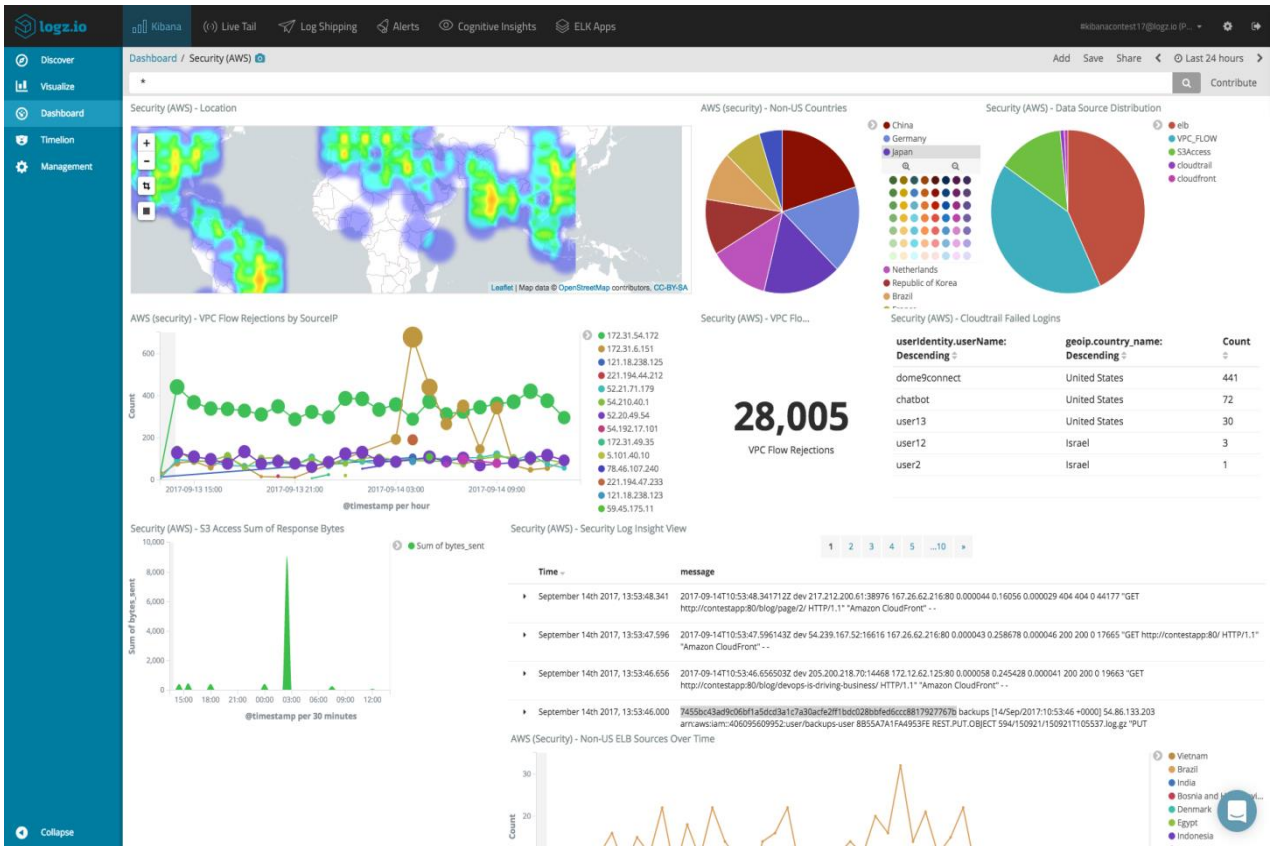

Рисунок 7 – Панель управления SIEM для AWS в Logz.io

Однако, несмотря на все преимущества SIEM-системы, существует ряд проблем и ограничений, связанных с расследованием инцидентов, которые можно решить с помощью применения нейросетей.

«SIEM-система обычно использует множество различных технологий и методов для обнаружения и расследования инцидентов. Она может интегрировать данные из различных источников, таких как журналы аутентификации и авторизации, системы противодействия вторжениям, системы детектирования вирусов и другие инструменты мониторинга» [13].

SIEM-система может существенно повысить эффективность расследования инцидентов в организации, предоставив оперативным службам множество полезных инструментов и функций для обнаружения,

классификации и анализа инцидентов.

«Еще одним важным аспектом работы SIEM системы является ее способность к анализу и корреляции больших объемов данных из различных источников. В обычных условиях анализ такого количества данных может занять значительное время и потребовать большого количества ресурсов. Однако, благодаря применению современных технологий, SIEM-системы могут осуществлять анализ и обработку данных в режиме реального времени, что позволяет оперативно реагировать на возможные угрозы безопасности информации» [32].

Помимо обнаружения и анализа инцидентов, SIEM-системы могут использоваться и для их предотвращения. Для этого в систему могут быть включены правила и политики, которые определяют допустимое поведение пользователей и устройств в сети. В случае нарушения таких правил система может срабатывать и принимать меры для предотвращения возможных угроз безопасности.

Существует два основных варианта развертывания и запуска SIEM-решений:

- «традиционный - поставщик поставляет программное обеспечение и часто обеспечивает поддержку в рамках покупки или в рамках отдельного контракта на поддержку, но повседневные функции находятся в руках заказчика. Этот подход может быть привлекательным для организаций, которые хотят сохранить полный контроль над своей сетевой безопасностью» [9];
- программное обеспечение как услуга (SaaS) - сторонние организации предоставляют SIEM как услугу. Поставщик предоставляет базовую архитектуру и осуществляет техническое сопровождение системы. Заказчик выполняет повседневные операции, включая обновления, тонкую настройку и реагирование на инциденты. Некоторые из основных поставщиков SaaS SIEM также предоставляют управляемые службы безопасности (MSS) и

управляемое обнаружение и реагирование (MDR).

Таким образом, SIEM системы играют важную роль в обеспечении безопасности информации в современных условиях, когда количество источников потенциальных угроз постоянно растет. Правильно настроенная и использованная SIEM система позволяет оперативно обнаруживать, анализировать и расследовать инциденты, а также предотвращать возможные угрозы безопасности информации.

1.3 Этапы внедрения SIEM-систем в существующую инфраструктуру компании

Поскольку сами по себе системы кибербезопасности достаточно сложны, процессы их внедрения и развертывания в инфраструктуре любой организации требуют дополнительного внимания.

Этапы внедрения SIEM:

- определение требований;
- исследование продуктов;
- планирование внедрения;
- развертывание и обзор.

Внедрение в каждой компании будет отличаться, но эти шаги имеют решающее значение для эффективной работы после развертывания.

Первым шагом к запуску процесса внедрения SIEM является определение требований к проекту и планирование сроков его реализации.

Этот этап включает в себя определение масштаба проекта наряду с необходимыми информационными, бюджетными и физическими ресурсами. Здесь компаниям следует определить свои цели и определить все необходимые ресурсы.

Большинство компаний преследуют схожие цели, которые связаны с созданием централизованной системы управления сетевой безопасностью.

Предприятиям необходимо установить базовые правила, определить необходимое соответствие требованиям политики безопасности, а также структурировать свой план управления SIEM после внедрения.

Продукты SIEM требуют подключения практически ко всей сетевой инфраструктуре и программным ресурсам для оптимальной производительности, поэтому для начала рекомендуется определить источники журналов. Журналы поступают от разных объектов в сети компании.

Рассмотрим наиболее часто подключаемые источники событий (доля проектов).

Это такие источники, как:

- средства антивирусной защиты;
- сервер;
- сетевое оборудование;
- контроллер домена;
- рабочая станция;
- файловое хранилище;
- средства виртуализации;
- системы обнаружения и предотвращения вторжений.

Распределение наиболее часто подключаемых источников событий (доля проектов) представлено на рисунке 8.

Рисунок 8 – Наиболее часто подключаемые источники событий (доля проектов)

Исследование продукта - это этап, который каждый бизнес решает индивидуально. Есть три основных информационных ресурса, которые следует рассмотреть, прежде чем принимать окончательное решение о внедрении SIEM в компании:

- анализ поставщиков обычно проводится двумя или тремя способами. Первый заключается в использовании информации от самих поставщиков. Ряд онлайн-ресурсов, а также сами поисковые системы могут помочь быстро определить основных поставщиков SIEM. Затем предприятия могут связаться с поставщиком для получения дополнительной информации, относящейся к их конкретной ситуации;
- информация, поступившая от компаний, оказывающих аналитические услуги по анализу рынка программного обеспечения, и эмпирическое

тестирование также могут использоваться в качестве ресурсов для оценки. Поставщики услуг исследований и тестирования дают представление о рынках и инструментах;

– обзорные Интернет-сайты - отличные ресурсы, где можно из первых рук ознакомиться с инструментами SIEM, используемыми в реальном мире. Лица, принимающие решения в компании, могут ознакомиться с продуктами, различающимися по популярности и характеристикам.

Оценка варианта использования применительно к бизнесу, скорее всего, потребует общения с поставщиками потенциальных продуктов. Многие из них предоставят по запросу заказчика отраслевые сценарии, тематические исследования и демонстрации продуктов.

После выбора продукта следует описать ряд процедур внедрения, чтобы обеспечить плавный и эффективный переход. Вот несколько компонентов, которые следует включить в план.

На этапе планирования внедрения нужно определить все источники данных, которые планируется подключить к SIEM. В дополнение к агрегированию данных со всех подключенных устройств, системы SIEM интегрируют как внутренние, так и сторонние данные об угрозах и уязвимостях. Системы хранения и оповещения также должны обеспечивать надлежащую функциональность после развертывания.

Нужно убедиться, что механизмы корреляции функционируют в соответствии с базовыми политиками, и определить индивидуальные правила и политики для внедрения в долгосрочной перспективе. Эти правила предназначены для оптимизации документации и оповещения без ущерба для производительности сети. Их также следует настроить с учетом любых необходимых требований соответствия, изложенных ранее.

Перед развертыванием следует разработать план передачи полномочий по управлению SIEM от группы внедрения работникам заказчика. Также следует описать любые другие долгосрочные процессы управления. Компании должны обучать персонал общему управлению SIEM,

а также правилам и способам разработки и модификации правил корреляции, а также приемам эффективного технического сопровождения SIEM. По мере того, как проект по развертыванию становится реальностью, необходимо предпринять несколько немедленных действий после ввода в эксплуатацию нового SIEM:

- сбор данных. Необходимо убедиться, что данные собираются и шифруются надлежащим образом. В зависимости от решения, системы на основе агентов следует проверять и контролировать во время предварительного развертывания, чтобы убедиться, что они правильно собирают данные. Те, кто внедряет безагентные решения, должны просто убедиться, что все точки мониторинга должным образом обмениваются данными с SIEM;
- после надлежащего сбора информации необходимо убедиться, что все действия, журналы и события хранятся правильно. Компании, использующие внешние системы хранения данных, должны убедиться, что передача и интеграция безопасны и функциональны, что базы данных правильно отформатированы и к информации можно обратиться после сохранения;
- тестирование - нужно протестировать систему для визуализации подключенных устройств и отображения их в соответствии с запланированными. Пользователи могут протестировать новое решение SIEM, имитируя события. Следует проводить моделирование угроз и имитационные тесты. Они имитируют реальные угрозы безопасности для проверки работоспособности всех операций.

После завершения процессов тестирования и проверки команды внедрения должны передать управление на полный рабочий день командам безопасности.

Решения SIEM требуют постоянного обновления и мониторинга. Командам следует продолжать тестировать свои решения на предмет

новейших видов атак. Любые действия по тестированию и уменьшению количества ложных срабатываний также являются обоснованными.

Команды должны поддерживать связь своих SIEM с источниками данных об угрозах, чтобы быть готовыми выявлять все виды возникающих угроз, даже тех, которые отсутствовали во время внедрения.

Корректировки и обновления неизбежны, и политики, скорее всего, будут развиваться. Процесс управления так же сложен, как и процесс внедрения. Если следовать приведенным выше шагам и постоянно отслеживать производительность SIEM, ИТ-инфраструктуре и бизнес-процессам компании в целом станет только лучше.

Таким образом, особенности внедрения SIEM-систем в существующую инфраструктуру компании зависят от масштабов инфраструктуры компании. Вполне возможно, что компании такая система не нужна, если в ней имеется всего несколько компьютеров. Внедрение SIEM в таком случае будет экономически нецелесообразно, так как расходы на внедрение и обслуживание будут превышать ущерб от возможных потерь информации. Или внедрение SIEM может не решить все имеющиеся проблемы. Особенности внедрения также зависят от использующихся средств защиты информации, так как система SIEM откуда-то должна собирать информацию - от антивирусного ПО, брандмауэров и т.д.

1.4 Анализ научной литературы и публикаций, посвященных проблемам внедрения SIEM-систем в ИТ-инфраструктуру

Как было сказано выше, проекты по внедрению SIEM-систем отличаются своей сложностью и высокими техническими требованиями, поэтому нередко компании сталкиваются с неудачами при попытках самостоятельного ввода решения в эксплуатацию.

Можно выделить типичные ошибки, с которыми компании могут столкнуться при реализации таких проектов.

Ошибка № 1: Недостатки планирования перед реализацией проекта.

Это ошибка касается не только SIEM, но и всех проектов в целом, ведь планирование – это важная компонента любого проекта. Чем точнее и правильнее было планирование, тем больше вероятность успеха. Если правильно все запланировать, это позволит компании сэкономить временные и финансовые ресурсы.

При рассмотрении вопроса о внедрении SIEM компании должны учитывать экономические аспекты, такие как стоимость лицензий на программное обеспечение поставщиков и необходимые аппаратные ресурсы, если они не выбирают облачное решение SIEM. Адекватное планирование и определение объема этих элементов имеют решающее значение для правильного развертывания SIEM.

Кроме того, перед внедрением SIEM в организации необходимо ответить на несколько ключевых вопросов, в том числе:

- какие источники должны быть включены в коллекцию событий?
- какой сетевой периметр следует учитывать?
- какую информацию следует сохранить?
- знает ли персонал о возможных вариантах использования, которые должны быть определены в соответствии со сценариями рисков компании?

Ошибка № 2: Неправильная оценка масштаба, сложности и специфики бизнеса.

Использование систем управления информацией и событиями безопасности на предприятиях сегодня вызвано необходимостью борьбы с постоянно развивающимися угрозами кибербезопасности и необходимостью соблюдения нормативных требований. Некоторые предприятия предпочитают использовать два отдельных решения SIEM - одно для соответствия требованиям, а другое - для безопасности данных. Причина этого в том, что система очень ресурсоемкая, и таким образом предприятие получает максимальную отдачу для каждой цели.

Небольшим предприятиям сложнее запускать SIEM именно из-за этого. Поскольку малые и средние предприятия ограничены денежными ресурсами, они не могут нести расходы на обслуживание программного обеспечения и найм квалифицированных работников, чтобы поддерживать его работу на постоянной основе. Более дешевая альтернатива локальному SIEM - это предоставление его в виде программного обеспечения как услуги от аутсорсинговых поставщиков. Однако, учитывая связанные с этим риски передачи конфиденциальных данных сторонним организациям, немногие компании заинтересованы в проведении аналитики в облаке.

Таким образом, если не учитывать масштабы компании и данных, которые необходимо принять, это может привести к тому, что система будет вынуждена обрабатывать объемы данных, на которые не была рассчитана.

Ошибка № 3: Недостаток ресурсов у компании.

Несмотря на то, что многие процессы SIEM полностью автоматизированы, для настройки и оптимизации по-прежнему требуются квалифицированные аналитики. Для развертывания SIEM может потребоваться значительное количество специалистов, чтобы обеспечить эффективную работу. Из-за нехватки опытных специалистов по безопасности предприятиям сложно поддерживать развертывание SIEM.

Кроме того, технология SIEM обеспечивает оповещение об угрозах безопасности в режиме реального времени, и для использования этой функции требуется круглосуточный мониторинг. Это только усугубляет кадровую проблему, потому что штатные сотрудники не всегда имеют необходимую подготовку, достаточную для обеспечения современных технических процессов.

Ошибка № 4: Желание закрыть все проблемы одним решением.

Некоторые предприятия, внедряющие SIEM, рассчитывают решить таким образом все проблемы, связанные с информационной безопасностью, имеющиеся в компании. Потом в результате аудита оказывается, что требуется целый комплекс программ для решения этих проблем.

SIEM-система собирает и анализирует информацию с различных источников. Этими источниками являются другие программы для защиты информации. Зачастую надо сначала внедрить их, а только потом SIEM.

В результате статистического исследования, проведенного компанией «СёрчИнформ» выяснилось, что SIEM-системами оснащены не более 25% отечественных компаний. При этом «основной акцент во время указанного опроса респондентов делался на проблемы эксплуатации и внедрения систем, в том числе на субъектах критической информационной инфраструктуры (КИИ), где применение этих решений фактически обязательно. Представители некоторых субъектов КИИ заявили, что не нуждаются в системах мониторинга событий. Например, большинство (56%) респондентов из здравоохранения заявляют об отсутствии задач для SIEM в своих организациях и не знают, что внедрять такие системы их обязывают нормативные требования (рисунок 9)» [34].

Рисунок 9 – Инструменты ИБ компании

«Но главные причины, которые тормозят внедрения – это отсутствие бюджетов, сложность внедрения и отсутствие кадров для работы с SIEM.

37% опрошенных сообщили, что считают SIEM слишком дорогой – они не смогли найти средства на закупку и отказались от идеи. Даже среди компаний, где SIEM установлена, 47% назвали согласование бюджета на закупку самой большой сложностью, связанной с решением» [13].

Стоимость SIEM очень часто упоминается в качестве проблемы при внедрении. Исследования, приведенные ниже, это подтверждают.

С целью изучения личного опыта специалистов по безопасности, компания Panther Labs заказала независимое исследование, чтобы понять, на сколько хорошо устаревшие SIEM соответствуют потребностям групп безопасности сегодня. В рамках данного исследования было опрошено «более 400 специалистов по безопасности, которые активно используют платформу SIEM в своей работе.

В группу респондентов вошли директора по информационной безопасности, директора по информационным технологиям, технические директора, инженеры по безопасности, аналитики по безопасности и архитекторы по безопасности» [29].

Опрос показал, что более половины опрошенных, участвовавших в развертывании своей текущей системы SIEM, начали получать важные значимые оповещения о событиях безопасности спустя полгода после внедрения. Причины подобных продолжительных периодов можно связать с многочисленными аспектами, неподконтрольными службе безопасности.

Взаимодействие с различными смежными службами, обслуживающими ИТ-инфраструктуру при развертывании инструментов безопасности сопряжено с задержками.

Существует также «кривая обучения», которая может негативно повлиять на время окупаемости (рисунок 10).

Рисунок 10 – Сроки внедрения по результатам опроса

Наиболее распространенные проблемы по результатам опроса представлены на рисунке 11.

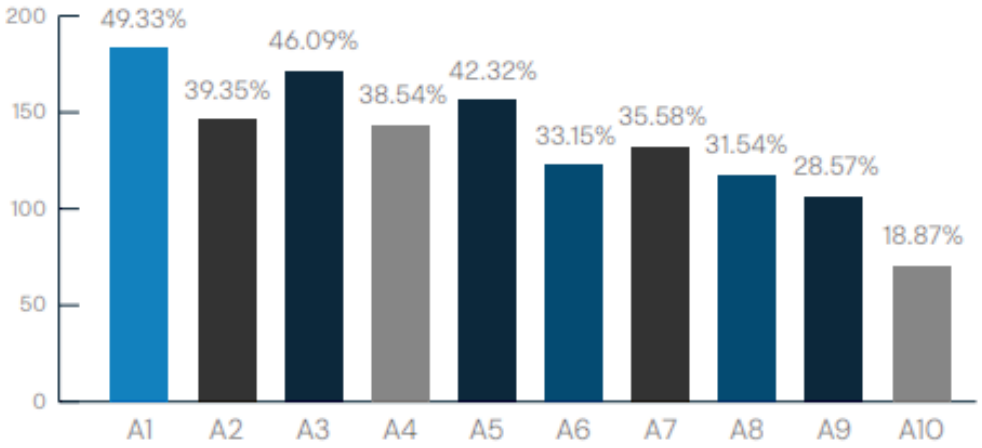

Рисунок 11 – Наиболее распространенные проблемы

A1 – скорость запроса;

A2 – недостаток опыта у персонала;

A3 – сложность решения;

A4 – недостаточный бюджет;

A5 – корпоративная культура;

A6 – операционные накладные расходы;

A7 – сложность добавления новых каналов данных/журналов;

A8 – невозможность интеграции в существующие системы;

A9 – слабая поддержка, предоставляемая поставщиком;

A10 – меня не было в компании, когда мы осуществляли.

Когда респондентов попросили оценить возможности традиционной SIEM в соответствии с тем, насколько они удовлетворены своей имеющейся в наличии программной платформой, возникла интересная картина. Это не была картина крайнего удовлетворения в противовес полному разочарованию.

Вместо этого результаты данного опроса создали впечатление согласованности по всем направлениям.

Победителями в категории «Очень довольны» стали:

- ведение журнала: 190 очень удовлетворенных и 63 неудовлетворенных ответа;
- аналитика поведения пользователей и сущностей: 182 очень удовлетворенных и 69 неудовлетворенных ответа;
- подключения к каналу анализа угроз: 180 очень удовлетворенных и 59 неудовлетворенных ответов.

Категория «Неудовлетворенные» дает:

- встроенное обнаружение: 74 неудовлетворенных и 179 очень удовлетворенных ответов;
- видимость в сети: 73 неудовлетворенных и 173 очень удовлетворенных ответа;
- корреляция событий безопасности: 69 неудовлетворенных и 176 очень удовлетворенных ответов.

И по всем возможностям разброс оценок «очень доволен» и «не

удовлетворен» составил едва ли более 4 процентов (рисунок 12).

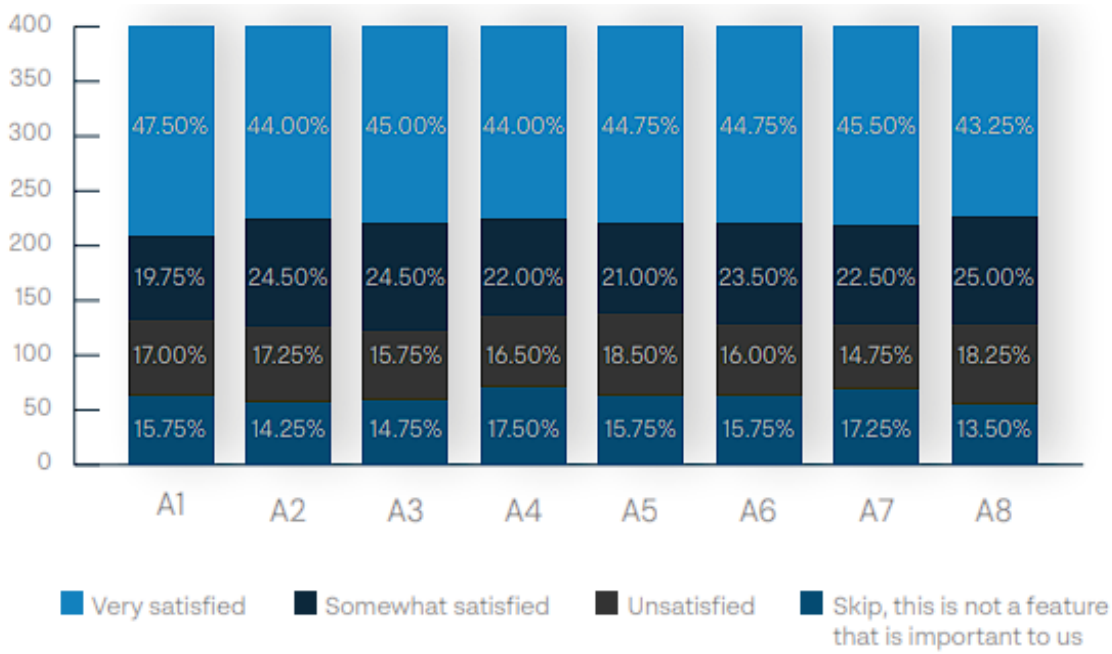

Рисунок 12 – Наиболее важные возможности

A1 – возможности управления журналами;

A2 – возможности корреляции событий безопасности;

A3 – возможности подключения к каналам сбора информации об угрозах;

A4 – возможности автоматизированного реагирования;

A5 – встроенные возможности обнаружения;

A6 – возможности визуализации данных;

A7 – возможности анализа поведения пользователей и сущностей;

A8 – возможности просмотра сети.

Менее 77 процентов респондентов считают, что их SIEM покрывает даже 75% их данных. Почти 17% понимают, что их существующая платформа охватывает менее четверти их данных

На вопрос «Какой процент ваших данных о безопасности защищен существующей платформой SIEM?» были получены следующие данные

(рисунок 13).

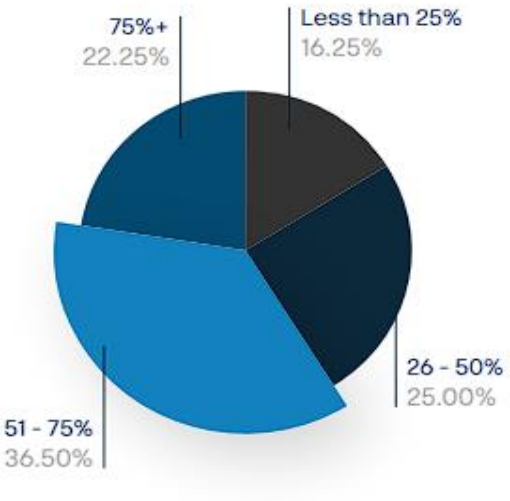

Рисунок 13 – Ответы на вопрос «Какой процент ваших данных о безопасности защищен существующей платформой SIEM?»

Ответы на другие вопросы представлены на рисунках 14-16.

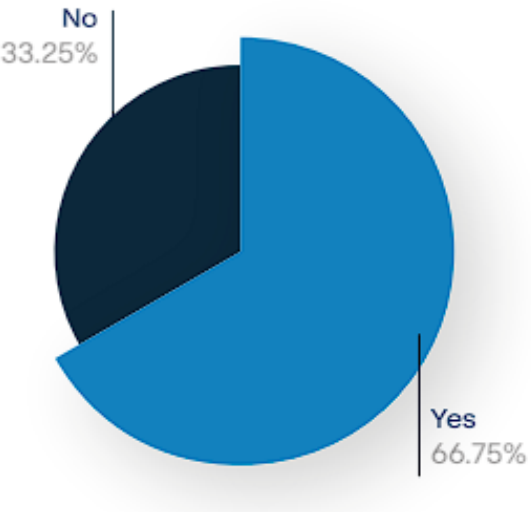

Рисунок 14 – Ответы на вопрос «Считаете ли вы, что ваша текущая платформа SIEM будет способна обрабатывать объем данных о безопасности, генерируемых вашей организацией в будущем?»

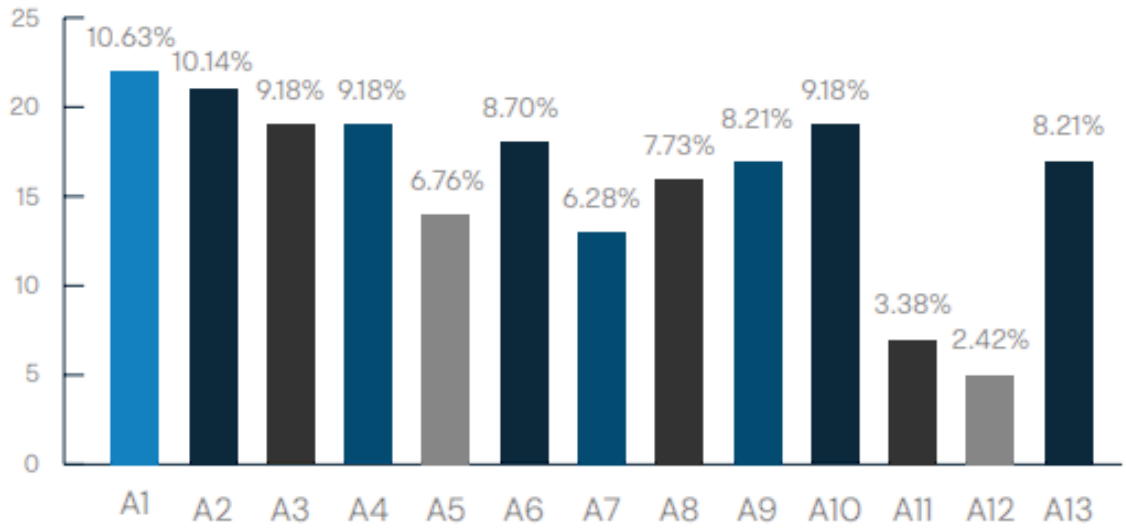

Рисунок 15 – Ответы на вопрос «Если вы недовольны, то какова ваша основная причина, по которой вы недовольны своей текущей платформой?»

«A1 – стоимость;

A2 – отсутствие функций/функциональности;

A3 – удобство использования продукта;

A4 – отсутствие возможности настраивать или расширять продукт;

A5 – сложность решения;

A6 – трудно работать в больших масштабах;

A7 – переход на управляемую службу;

A8 – больше инноваций от нового поставщика;

A9 – слишком сложно добавлять новые каналы данных / журналы» [34];

A10 – проблемы с технической поддержкой;

A11 – низкое качество продукции;

A12 – плохое обнаружение и оповещение;

A13 – другой.

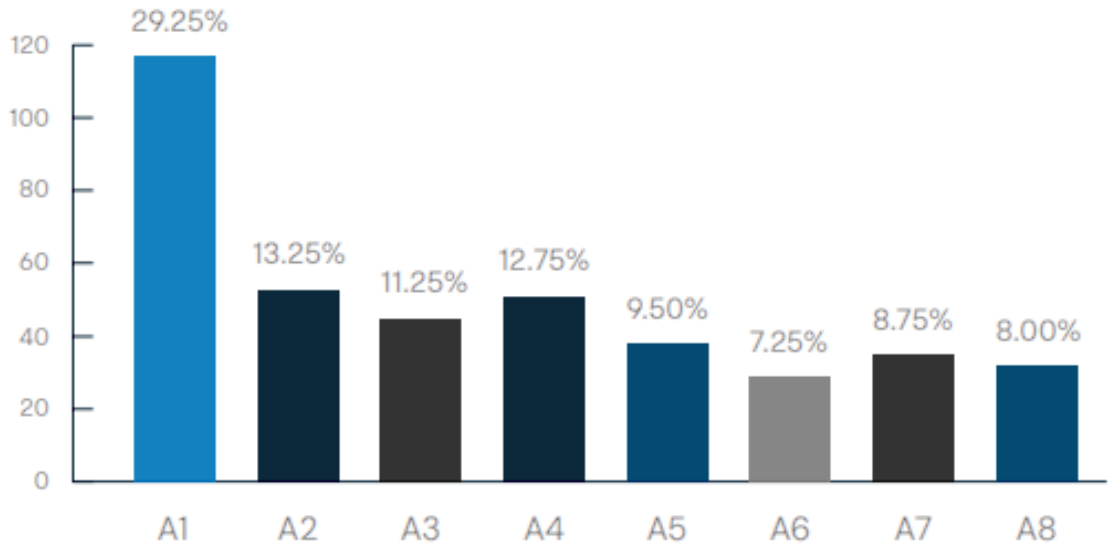

Рисунок 16 – Наиболее важные функции по результатам опроса

«A1 – инфраструктура больших данных с неограниченной масштабируемостью;

A2 – простой ввод данных журнала;

A3 – возможности визуализации;

A4 – обнаружение в реальном времени» [34];

A5 – сортировка инцидентов и углубленное расследование;

A6 – расширенный анализ поведения с помощью машинного обучения;

A7 – автоматический/полуавтоматический ответ;

A8 – гибкие и понятные цены.

Ответы на этот опрос ясно указывают на то, что традиционные платформы SIEM не в состоянии обеспечить достаточно надежное решение для масштабного обнаружения. Службы безопасности, по большей части, вынуждены использовать эти инструменты, даже несмотря на то, что они и близко не могут приблизиться к масштабу и гибкости, необходимым им для выполнения своей работы.

Как видно, одной из наиболее частых проблем с SIEM, на которую ссылаются предприятия, является ее стоимость. Первоначальные затраты на

традиционное решение SIEM включают затраты на лицензирование, затраты на внедрение и затраты на продление. Кроме того, предприятию необходимо учитывать затраты на обучение сотрудников для надлежащего обслуживания внедренного технического решения.

Однако эти расходы не должны оказаться чрезмерными по сравнению с другими решениями в области кибербезопасности, такими как управление идентификацией и безопасность конечных точек. Однако AlienVault утверждает, что две проблемы способствуют восприятию SIEM как дорогостоящего:

- предприятия продолжают вкладывать деньги в устаревшие решения, которые не могут работать по сравнению с современным ландшафтом угроз;
- предприятия не вкладывают ресурсы, время или энергию в поддержку своего решения SIEM в долгосрочной перспективе.

Предприятия считают, что работать с SIEM будет слишком дорого, и поэтому опасаются инвестировать в него должным образом.

Следует рассматривать SIEM как крупную долгосрочную инвестицию в общую кибербезопасность и уделять ей столько времени и энергии, сколько она заслуживает. Кроме того, обучение, необходимое для работы с SIEM, повысит уровень профессиональных знаний специалистов по ИТ-безопасности в долгосрочной перспективе.

Часть проблем SIEM, с которыми сталкиваются предприятия, заключается в том, что они не могут поддерживать его с надлежащей корреляционной информацией о событиях безопасности. Решения SIEM не работают в вакууме; они используют аналитику угроз для обнаружения потенциальных угроз, обитающих в сети, и создают предупреждения, которые специалисты по безопасности должны анализировать и при необходимости расследовать.

Отсутствие в решении SIEM достаточной информации об угрозах и правилах корреляции означает, что оно пропустит серьезные и постоянно

меняющиеся угрозы. Однако предоставление слишком большого объема информации может привести к тому, что команды безопасности могут быть перегружены предупреждениями безопасности; кроме того, многие из этих предупреждений оказываются ложными срабатываниями, что приводит к трате времени и энергии на бесполезные расследования.

В связи с этим группа ИТ-безопасности должна тщательно изучить все обновления и изменения системы, чтобы убедиться, что действующие правила корреляции по-прежнему актуальны. Кроме того, необходимо тщательно выбирать источники информации об угрозах. Не каждое предприятие сталкивается с одинаковыми типами цифровых угроз. Подготовка решения SIEM к поиску маловероятных кибератак приводит к большему количеству ложных срабатываний в будущем. Однако по мере того, как меняются каналы информации об угрозах, должны меняться и правила корреляции.

«Совокупно более 70% респондентов считают работу с SIEM сложной – опасаются чрезмерных трудозатрат на внедрение, настройку и кастомизацию. Для 14% опрошенных компаний без SIEM потенциальные трудозатраты на внедрение стали главной причиной отказа от закупки (рисунок 17)» [29].

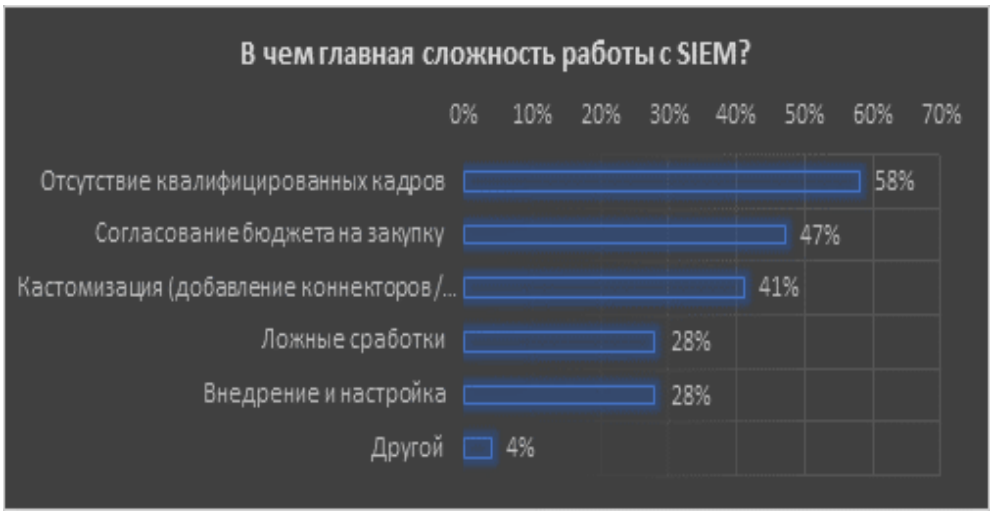

Рисунок 17 - Основные сложности работы с SIEM

Сложность остается одной из наиболее часто упоминаемых проблем SIEM. По сравнению с безопасностью конечных точек и управлением идентификацией SIEM, безусловно, выглядит пугающе. В связке с постоянно надвигающимся кадровым кризисом в области кибербезопасности это выглядит еще более устрашающе.

Решение этой проблемы состоит в том, чтобы найти решение SIEM с пользовательским интерфейсом, который лучше всего подходит для группы ИТ-безопасности и эксплуатации в конкретной ИТ-среде. Не следует выбирать решение вслепую или опрометчиво решать проблему.

Чтобы решение SIEM было эффективным, оно должно точно и всесторонне фиксировать и анализировать все события безопасности, генерируемые каждой операционной системой, приложением, базой данных, сервером, маршрутизатором, коммутатором и устройством безопасности, используемым во всей сети. В большинстве организаций развернуты различные разрозненные сетевые устройства и приложения, что может вызвать проблемы совместимости с SIEM и создать пробелы в безопасности. Поскольку решения SIEM лучше работают в сочетании с другими решениями по обеспечению безопасности, такими как защита конечных точек, корректная интеграция с существующими средствами сетевой безопасности и управления имеет решающее значение для получения максимальной отдачи от решения SIEM. Получение актуальной информации о безопасности из устаревших систем, которые могут создавать журналы в проприетарных форматах, усложняет внедрение SIEM.

Для каждой пятой организации отсутствие профильных специалистов послужило причиной для отказа от закупки решения. На нехватку кадров пожаловались и 58% компаний, где SIEM уже внедрена.

«Исследование показало, что только 11% компаний смогли выделить для работы с SIEM профильного специалиста. В подавляющем большинстве случаев это дополнительная нагрузка на ИБ-специалистов» [29].

Если мы тратим 80 % своего времени на выполнение задач

обслуживания, таких как развертывание агентов, анализ журналов или выполнение обновлений, то, скорее всего, мы не получим максимальную отдачу от своего SIEM. Автоматизация имеет решающее значение для успешного внедрения SIEM. Среда постоянно меняется, и автоматизация необходима, чтобы не отставать от нее, чтобы мы могли тратить свое время на анализ действительно важных событий в системе.

Необходимо также отметить, что «при всех сложностях внедрения и эксплуатации SIEM-систем, никто из респондентов не усомнился в их эффективности – даже те, у кого решение пока не внедрено, признают его пользу и целесообразность внедрения. Опрошенные представители компаний сходятся во мнении, что это важный инструмент для противостояния растущему количеству угроз. Для 41% владельцев решения это стало главным мотиватором внедрения. Другая популярная причина, почему компании решаются на закупку, – расширение инфраструктуры и наличие в ней специфических источников, например, отечественного ПО и оборудования (40%). Еще 36% на это мотивируют требования регулятора (рисунок 18)» [14].

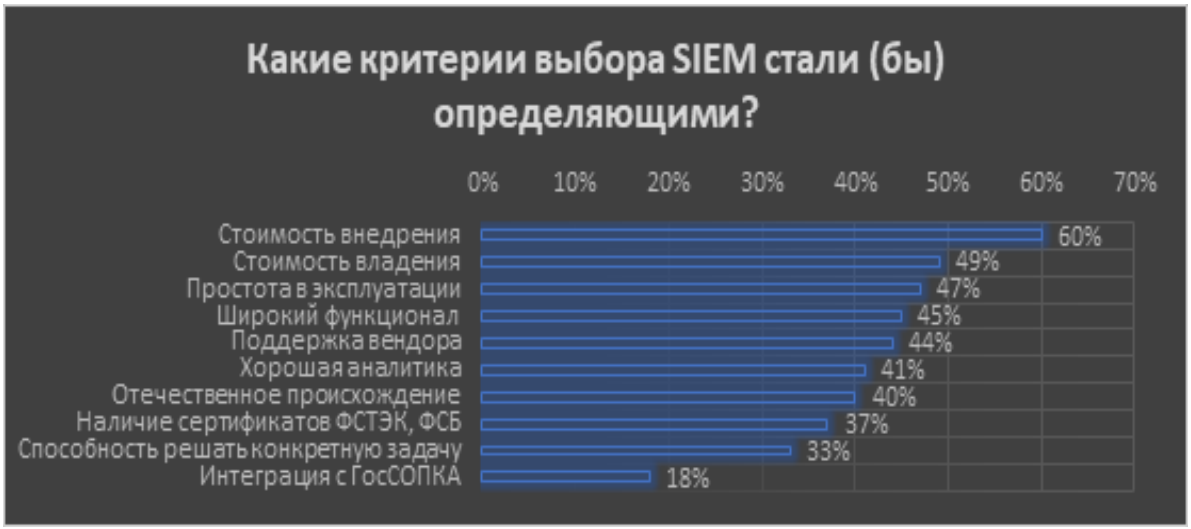

Рисунок 18 – Критерии выбора SIEM

В.А. Сизов, А.Д. Киров в статье «Проблемы внедрения SIEM-систем в

практику управления информационной безопасностью субъектов экономической деятельности» рассмотрели проблемы внедрения SIEM-систем в практику управления информационной безопасностью.

«В процессе установки и настройки SIEM-системы у коллектива заказчиков и исполнителей могут возникнуть следующие типовые проблемы:

- сложность построения SIEM-систем. Эта проблема уже рассматривалась выше и подразумевает, что необходимо собирать данные с различных источников и анализировать их. Это требует высокой квалификации кадров, это еще одна проблема, которая тоже рассмотрена выше;
- необходимость выделения зачастую неоднородных аппаратных платформ, что может ограничить внедрение SIEM-системы в существующую информационную инфраструктуру;
- достаточно высокие требования к техническим характеристикам аппаратных платформ. Это приводит к тому что внедрение SIEM обходится еще дороже. Кроме закупки самой системы, оплаты труда специалистов, добавляется еще одна большая статья расходов – расходы на замену оборудования» [14];
- сложности построения системы приводит к большой трудоемкости разработки технической документации. А это, в свою очередь, может привести к ошибкам в документации, увеличению сроков внедрения.

Авторы статьи рассмотрели не только проблемы, но и пути их решения. Например, они предложили отказаться от некоторых модулей системы, которые используются редко, но усложняют работу с системой. Также предложили автоматизировать процесс установки и настройки SIEM-системы. Для этого нужно разработать методику автоматизации и программный модуль, реализующий эту методику. Также они предложили комбинированный подход, представляющий собой совместное применение двух вышеуказанных подходов.

Если рассматривать исследования зарубежных авторов, то согласно

исследованию McAfee и Калифорнийского университета в Беркли:

- 45% респондентов заявили, что отсутствие функциональной совместимости мешает их работе с SIEM;
- 43% столкнулись с трудностями при сопоставлении данных о событиях SIEM с известными методами и тактиками;
- 36% сообщили о слишком большом количестве ложных срабатываний их системы SIEM.

Значительные расходы на внедрение и последующую эксплуатацию SIEM также являются проблемой и в зарубежных компаниях. Компании платят значительные суммы за системы, которые не соответствуют их требованиям к масштабу, слишком громоздки и медленны в работе. В будущем технологии SaaS и облачные хранилища данных станут необходимой частью SIEM-решений. Без решений SaaS, облачных технологий и больших данных мало надежды на то, что будущие решения SIEM будут соответствовать потребностям бизнеса.

Почти половина опрошенных специалистов по ИТ-безопасности ответили, что ключевой проблемой при внедрении SIEM является сложность решения. Выводы, предоставленные респондентами этого опроса, служат хорошим аргументом в пользу нового подхода к SIEM, созданного с нуля для облачных сред, чтобы упростить внедрение и повседневные операции.

Облачные платформы постоянно развиваются в сторону упрощения и абстрагирования чрезвычайно сложных концепций, таких как pub-sub, оркестровка контейнеров, организация очередей и многое другое. По мере продолжения этой эволюции традиционные платформы SIEM будут заменены бессерверными архитектурами, которые упрощают операции и улучшают масштабируемость.

Более 42% респондентов указали, что «они работают в организации, культура которой так или иначе создает дополнительные препятствия для их команды. В среде, где локальное программное обеспечение, серверы и сети по-прежнему выполняют основную рабочую нагрузку, внедрение SIEM

требует высокой степени координации и сотрудничества с ИТ-отделами и операционными группами. Эта парадигма имеет долгую историю формирования культуры, в которой безопасность рассматривается как неизбежное зло и не получает места за столом, где принимаются решения, влияющие на направление деятельности компании» [33]. Достаточно взглянуть на заголовки сегодняшних новостей, чтобы подтвердить, что безопасность должна быть частью важных бизнес-решений.

Около четверти респондентов указали, что главная проблема с их текущей SIEM заключается в том, что она часто генерирует слишком много предупреждений. Это обстоятельство приводит к задержкам в обнаружении утечек данных, что может экспоненциально увеличить последствия от реализации угроз безопасности информации.

Многие устаревшие подходы к локальной инфраструктуре имеют строгие ограничения на прием и хранение данных. Почти 14% респондентов заявили, что их самая большая повседневная проблема связана с отсутствием видимости определенных участков внутренней информационной инфраструктуры. Учитывая высокую стоимость, связанную с традиционными решениями SIEM, службы безопасности часто вынуждены выбирать, какие источники данных наиболее важны для сбора событий. Это ограничивает видимость всего спектра важных для безопасности данных, что приводит к слепым зонам и недостаточным возможностям для полного исследования угроз.

Самая большая проблема почти для 10% респондентов заключается в том, что их неспособность написать четкие и эффективные правила обнаружения ограничивает их способность настраивать логику оповещения и уменьшать количество ложных срабатываний. Традиционные платформы SIEM часто не имеют возможности редактировать существующие правила или создавать настраиваемые правила, проверенные надежными модульными тестами.

Контекстуализация – одна из наиболее привлекательных особенностей

современных SIEM-решений. Контекстные оповещения содержат информацию о вовлеченных пользователях, местоположении, времени и других важных обстоятельствах, связанных с оповещением. Понимая контекст предупреждения безопасности, SIEM может уменьшить количество ложных срабатываний, различая нормальное поведение и подозрительные действия. Контекстуализация также позволяет решениям SIEM предоставлять практические рекомендации по обработке предупреждений.

SIEM должны создавать аналитики для аналитиков. Это означает, что когда аналитик просматривает предупреждения или журналы, SIEM должен предоставить контекст и информацию осмысленным образом. К счастью, обогащение журнала или искусство добавления контекста в журнал — это то, в чем SIEM чрезвычайно успешен. К сожалению, большинство реализаций SIEM отдают предпочтение сбору данных, а не обогащению журналов.

Технологии SIEM собирают и анализируют огромные объемы данных о событиях безопасности, что приводит к информационной перегрузке. Предприятия должны расставить приоритеты для наиболее важных событий и убедиться, что их система SIEM может управлять огромными объемами данных.

Выводы по главе 1

Таким образом, в данной главе были рассмотрены методы обеспечения информационной безопасности локальной сети компании.

Одним из эффективных инструментов обеспечения безопасности информации являются SIEM-системы. Но существуют проблемы при их внедрении в ИТ-инфраструктуру предприятия, так как пока не хватает квалифицированных кадров, системы достаточно дорогие. Бывают ложные срабатывания, проблемы из-за сложности самой системы и т.д.

Глава 2 Анализ используемых методов и средств управления информационной безопасностью

2.1 Характеристика ИТ-инфраструктуры организации-заказчика внедрения SIEM-системы (на примере предприятия Госкорпорации «Росатом»)

«Росатом» – корпорация по атомной энергии, 100% акций которой принадлежат государству. Представляет собой многопрофильный холдинг, объединяющий активы в энергетике, машиностроении, строительстве.

«Стратегические цели корпорации:

- повышение доли на международных рынках;
- снижение себестоимости продукции и сроков протекания процессов;
- разработка новых продуктов для российского и международного рынков.

Направления деятельности корпорации:

- ядерная энергетика;
- ветроэнергетика. Ветроэнергетический дивизион Росатома обеспечивает производство электроэнергии на основе ветроэлектростанций (ВЭС), сервисное обслуживание и эксплуатацию ВЭС, локализованное производство ветроустановок. В настоящее время в эксплуатации находятся семь действующих ВЭС Росатома общей мощностью 780 МВт;
- композитные материалы. Композитные материалы — современный подход к проектированию изделий, предполагающий осмысленное комбинирование разнородных компонентов для получения требуемых свойств прочности, жесткости, химической и климатической стойкости. Углеволокно обладает высокой прочностью и упругостью при растяжении. Ткани на основе

углеродного волокна - это высокотехнологичный текстиль с превосходными эксплуатационными качествами. Углеродные ткани имеют высокие показатели прочности на растяжение, устойчивы к воздействию большинства химически агрессивных реагентов;

- ядерная медицина. Госкорпорация «Росатом» входит в пятерку крупнейших мировых поставщиков сырьевой изотопной продукции и является ключевым поставщиком изотопной продукции медицинского назначения на российском рынке. Росатом имеет самую широкую в мире номенклатуру производимых изотопов, на отечественном рынке представлены все наиболее востребованные радиофармпрепараты для терапии, а также для высокоточной диагностики онкологических заболеваний;
- создание цифровых продуктов. «Цифровые амбиции Росатома — технологическое лидерство как на российском рынке, так и в мире. Росатом активно участвует в цифровизации российской экономики, создавая IT-решения не только для атомной энергетики, но и для других отраслей промышленности по семи приоритетным направлениям: «Математическое моделирование и НИОКР», «Управление предприятием и производством», «Цифровая инфраструктура», «Управление сооружением крупных инженерных объектов», «Информационная и физическая безопасность», «Цифровизация городских сервисов и процессов», «Системная интеграция и разработка ПО»;
- системы накопления энергии. К 2024 году в России планируется выпустить не менее 25 тыс. электромобилей и открыть более 9 тыс. зарядных станций. Внутренний спрос на накопители энергии достигнет 17,5 ГВт•ч, из них 16 ГВт•ч в год придется на электромобили. Топливный дивизион Росатома занимается производством литий-ионных аккумуляторных батарей для энергетики, электротехники и электротранспорта, в том числе тяговых

литий-ионных батарей для транспорта, стационарных систем накопления энергии для электросетевого комплекса и промышленных предприятий.

- водородная энергетика;
- АСУ ТП и электротехника;
- «аддитивные технологии. Деятельность Росатома охватывает все составляющие аддитивного рынка: производство 3D-принтеров, выпуск оборудования для создания порошков, разработка ПО и организация центров аддитивного производства. Развитию аддитивного направления уделяется большое внимание на федеральном уровне. Центр аддитивных технологий Росатома в Москве — единственный в России, работающий на отечественном оборудовании собственного производства. Центр укомплектован 3D-принтерами Rusmelt 300M, Rusmelt 600M и Rusmelt 600RM для печати металлическими порошками по технологии SLM. Все принтеры работают на отечественном ПО;
- развитие Северного морского пути. Повышение объема перевозок по Северному морскому пути (СМП) имеет первостепенное значение для решения поставленных задач в области транспорта и доставки грузов. Развитие этого логистического коридора обеспечивается за счет налаживания регулярных грузоперевозок, постройки новых атомных ледоколов и модернизации соответствующей инфраструктуры. Росатом принимает активное участие в этой работе, обеспечивая проводку судов в акватории СМП в замерзающие порты России, проведение высокоширотных научно-исследовательских экспедиций, аварийно-спасательные операции во льдах акватории СМП. Транспортировка углеводородной и прочей продукции на рынки Азии и Европы по трассе СМП может служить реальной альтернативой существующим транспортным связям между странами Атлантического и Тихоокеанского бассейнов» [24];

– оборудование для тепловой энергетики;
– судостроение и т.д.» [24].

Всего насчитывается 22 вида деятельности.

В структуре корпорации – предприятия ядерного оружейного комплекса, ядерного топливного цикла, атомного машиностроения и отраслевые научно-исследовательские институты.

«Ключевые показатели деятельности (по итогам 2022 года):

– выработка электроэнергии на АЭС: 223,371 млрд кВт.ч (222,436 млрд кВт.ч в 2021 году);
– грузопоток по СМП в 2022 году превысил целевой показатель федерального проекта более чем на 2 млн тонн;
– портфель заказов «Атомфлота» составил 3,5 млрд рублей (+1,7 млрд рублей к 2021 году);
– сооружаются три новых ледокола: «Чукотка», «Якутия», а также уникальный, самый мощный в мире ледокол проекта 10510 «Россия» (120 МВт);
– в ноябре сдан в эксплуатацию второй серийный ледокол проекта 22220 «Урал»;
– открыто новое направление по производству защитных полимерных покрытий, которые активно используются в строительстве;
– в Ульяновской области открылся Центр компетенций «Технологии композитов»;
– в состав Росатома вошли предприятия по выпуску стекловолокна и изоляционных материалов во Владимирской и Тверской областях, а также подразделение в Республике Беларусь;
– коэффициент использования установленной мощности (КИУМ): 86,21% (83,18% по итогам 2021 года)» [24];
– открыт центр аддитивных технологий в Республике Татарстан. Запущено серийное производство порошков нержавеющей стали и открыт центр аддитивных технологий в г. Новоуральске

(Свердловская область);

- «осуществлена первая коммерческая поставка промышленного 3D-принтера по технологии селективного лазерного спекания собственной разработки;
- запущена оперативная линия, на которую смогут обращаться компании, испытывающие нехватку импортных запчастей, деталей, материалов и комплектующих, которые возможно изготовить методом 3D-печати (АО «Русатом — Аддитивные технологии»);
- создан экспериментальный образец 16-кубитного квантового компьютера, выполнены двухкубитные квантовые операции;
- реализовано 10 пилотных проектов в области сквозных цифровых технологий и управления данными, экономический эффект — 105,88 млн рублей;
- завершен пятый этап продуктизации цифрового продукта «Логос»: расширены функционально-технические возможности базовых программных модулей «Логос Аэро-Гидро», «Логос Тепло», «Логос Прочность» и «Логос Платформа». Создана международная версия продукта «Логос»;
- продукты линейки Multi-D (Multi-D Platform и Multi-D Project) включены в Единый реестр российских программ для ЭВМ и баз данных;
- выведен на рынок продукт Multi-D ESB;
- портфель зарубежных проектов на 31.12.2022 включал 33 блока в 11 странах мира» [24].

В состав ЛВС входят 300 автоматизированных рабочих мест (АРМ). Все АРМ находятся в сети 192.168.5.0/24 и входят в домен Active Directory. Active Directory предоставляет информацию об объектах, позволяет организовывать объекты, управлять доступом к ним, а также устанавливает правила безопасности, причём независимо от географического распределения офисов компании.

Таблица 1 – Перечень используемого серверного оборудования

«Наименование ТС	Функция
Прокси-сервер (Сервер FreeBSD 8.2 (Squid, PF, OpenVPN)	Для организации доступа к сети интернет
СХД QNAP TS-1673U	поддерживает работу в высокоскоростной сетевой среде 10 Gigabit Ethernet и имеет встроенный двухпортовый 10GbE SFP+ PCI адаптер, гарантирующий впечатляющую производительность при работе, как с медными, так и с оптическими трансиверами
Коммутатор 3Com Baseline 2250Plus	управляемые стекируемые коммутаторы корпоративного класса для рабочих групп, обеспечивающие коммутацию в сетях 10/100 Мбит/с с использованием интерфейсов восходящей связи
Коммутатор 3Com Baseline 2016	Неуправляемый коммутатор
Сервер ПДН	Сервер для хранения ПДН
Система резервного питания (ИБП) APC Smart UPS 2200 и APC Smart UPS SC 1500	Обеспечение резервного питания» [23]

В открытой однорамной телекоммуникационной стойке установлены коммутаторы 3Com Baseline 2250Plus и 3Com Baseline 2016.

В таблице 2 указан перечень используемого программного обеспечения.

Таблица 2 – Перечень используемого программного обеспечения

«Программное обеспечение	Наименование
ОС для серверов	Windows Server 2019
ОС для рабочих станций	Microsoft Windows 10
Прикладное ПО	1С «Бухгалтерия» версия 8, 1С «Зарплата и кадры бухгалтерии версия 8
Офисные программы	Microsoft Office 2016, Парус Бюджет 7.71
Браузеры	Yandex Browser
Антивирусное ПО	Kaspersky Endpoint Security» [23]
АСУ ТП	

АСУ ТП предназначена для автоматизированного контроля и управления технологическими процессами при производстве.

Система «Бухгалтерия и кадры» предназначена для обеспечения технологических процессов работы компании, связанных с учетом работников и обработкой их персональных данных, в целях обеспечения соблюдения законов и иных нормативно-правовых актов [27].

«В ИСПДн «Бухгалтерия и Кадры» обрабатываются персональные данные менее 100 субъектов, являющихся сотрудниками компании. В компании используется только лицензионное ПО, проводится регулярное обновление общесистемного ПО и приложений. Прикладные программы, используемые для обработки ПДн, лицензионные, несанкционированному изменению не подвергаются (перечень ПО приведен в таблице 2). Антивирусное ПО имеет сертификат ФСТЭК России, вирусные базы регулярно обновляются» [28]. Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении не актуальны для информационной системы компании.

В настоящее время в СУБД используется разделение ролей для локальных и удаленных пользователей. В качестве СУБД используется Microsoft SQL Server.

Средствами СУБД ведется сбор информации о действиях пользователей. Каждые 30 минут создается инкрементная копия данных, 1 раз в сутки (в ночное время) создается полная копия данных.

Анализ ИТ-инфраструктуры компании невозможен без анализа ее цифровых продуктов. Цифровизация экономики и повседневной жизни – важнейший тренд современности.

Опираясь на многолетний опыт решения сложных технологических задач, Госкорпорация «Росатом» создает эффективные инновационные решения для работы в цифровом мире будущего.

Краткое описание цифровых продуктов приведено в таблице 3.

Таблица 3 – Описание цифровых продуктов компании

Наименование цифрового продукта	Назначение	Описание
CAE-система «Логос»	Решение сложных задач производства методом математического моделирования.	Состоит из различных модулей: «Логос Аэро-Гидро» - для моделирования процессов в водной и воздушной средах; «Логос Тепло» – для оценки тепловых характеристик и режимов деталей и узлов; «Логос Прочность» - для решения инженерных задач прочности в высокотехнологичных отраслях; промышленности «Логос Платформа» - для интеграции различных модулей «Логоса»; «Логос Гидрогеология» - для решения круга гидрогеологических задач в промышленности
Multi-D	интегрированная технология управления жизненным циклом сложных инженерных объектов, позволяющая реализовывать проекты по их возведению и эксплуатации в заданные стоимость и сроки с необходимым качеством	Модуль Multi-D Docs and Resources (документооборот на зарубежных площадках) «Мульти-Д Объединенный график» (Multi-D Unified Time Schedule) - для управления сроками и централизованного контроля рисков сооружения сложных инженерных объектов.
ПВК «Волна»	для моделирования и мониторинга различных режимов работы газотранспортных систем и используется для решения инженерных задач в области проектирования и эксплуатации газопровода, а в связке со SCADA-системами – для взвешенного принятия диспетчерских решений	ПВК «Волна» позволяет оптимизировать производительность газопровода, отслеживать и прогнозировать аварийные ситуации, моделировать и предотвращать их последствия, обеспечивая безопасную и эффективную работу газотранспортных систем.

Продолжение таблицы 3

Наименование цифрового продукта	Назначение	Описание
«Сарус»	использует модульный принцип организации (ключевые элементы - «Управление предприятием», «Управление производством», «Управление персоналом», «Управление жизненным циклом изделий»)	Система позволяет автоматизировать проектирование, конструирование, документооборот, управление персоналом, логистику и другие процессы.
«Призма 2.0»	автоматизированная система управления дискретным производством, учитывающая особенности деятельности приборостроительных предприятий Госкорпорации «Росатом» и других отраслей	Система обеспечивает управление всеми процессами на мелкосерийном и серийном производстве
Электронный магазин технической документации	современный онлайн-сервис поиска, заказа и получения нормативно-правовой, научной и проектной технической документации, регламентирующей все стадии жизненного цикла АЭС с реакторами ВВЭР	На конец 2023 года в магазине было размещено свыше 1100 технических документов (более 75 тыс. страниц) с аннотациями. Для удобства зарубежных пользователей предусмотрена возможность приобретения материалов на английском языке.
Сервис «Атомбот. Закупки» (ПО «Система интеллектуальной проверки документации»)	Для автоматизации закупочной деятельности	«Атомбот» состоит из более чем 14 роботов класса RPA (Robotic process automation), системы распознавания текста, интеграционной шины и искусственного интеллекта, он автоматизирует процессы, не требующие верификации или экспертизы с участием человека.
Система контроля и управления доступом (СКУД) «Пилот	для проверки пропускных документов в реальном времени с использованием бесконтактных технологий считывания различных идентификаторов, в том числе с использованием биометрического анализа лица	позволяет обеспечить контроль, безопасность и одновременно удобство посетителей на массовых мероприятиях и охраняемых объектах, включая спортивные объекты, театры, музеи, концертные залы, аэропорты, вокзалы, учебные заведения.

Организация является субъектом критической информационной инфраструктуры, так как основным видом деятельности является производство электроэнергии, в соответствии с положениями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [26].

В инфраструктуре Организации функционирует значительное количество объектов критической информационной инфраструктуры (КИИ) [21], категории значимости которых определены в соответствии с Постановлением Правительства РФ № 127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений» [16].

Для предупреждения возможных инцидентов информационной безопасности в организации и минимизации негативных последствий существует установленный план реагирования на инциденты информационной безопасности и порядок их расследования [17].

Примерный порядок действий при расследовании инцидента информационной безопасности изображен на рисунке 19.

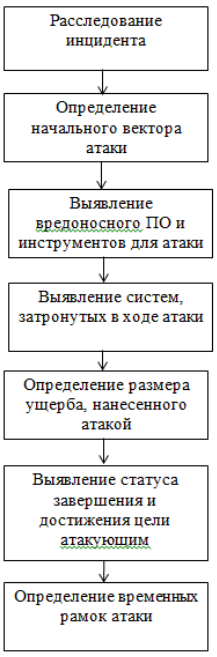

Рисунок 19 – Определение параметров инцидента

После того, как определены эти параметры, разрабатывается дальнейший план по восстановлению системы, с использованием информации, полученной при расследовании.

2.2 Описание порядка расследования инцидентов в компании

Так как для эффективного реагирования необходима предварительная подготовка, то персонал корпорации «Росатом», ответственный за информационную безопасность, обеспечивает защиту информационных систем при помощи программных средств, а также информирует пользователей и ИТ-специалистов о том, как важно выполнять организационные меры по обеспечению информационной безопасности, а также информирует об ответственности в случае ее нарушения.

Сотрудники, занимающиеся реагированием на инциденты, определяют самостоятельно, является ли обнаруженное ими с помощью различных систем обеспечения информационной безопасности событие инцидентом или нет.

При расследовании инцидентов администраторы безопасности при помощи программ администрирования и мониторинга обнаруживают индикаторы компрометации, определяют этап атаки, которому они соответствуют. Также они выявляют слабые места в системе защиты, которые были использованы вредоносным ПО и устраняют их. Но чтобы точно определить тип вредоносного ПО, необходимо найти достаточное количество уникальных индикаторов, в этом и заключается основная сложность.

На сегодняшний момент «Росатом» использует набор бесплатных программ Sysinternals. Утилиты устранения неполадок Sysinternals были объединены в единый набор инструментов. Этот файл содержит отдельные средства устранения неполадок и файлы справки. Он не содержит инструментов, не связанных с устранением неполадок, таких как экранная заставка BSOD или NotMyFault. Утилиты Sysinternals используются администраторами безопасности для того чтобы собирать первоначальные

данные об инциденте. Рассмотрим наиболее используемые в исследуемой компании утилиты:

PsTools - это набор инструментов командной строки, которые позволяют выполнять широкий спектр административных задач локально и удаленно.

Возможно, один из самых мощных инструментов в наборе, PsExec позволяет подключаться к удаленным компьютерам и выполнять любую административную команду. Это не только позволяет получить полный контроль над удаленным компьютером и использовать его для выполнения ряда задач, но также не требует предварительной установки клиента на удаленных компьютерах.

Программа может пригодиться в самых разных ситуациях, например, для проверки состояния системы при запуске скрипта или для выяснения того, уязвимы ли компьютеры и может ли к ним получить доступ посторонний персонал.

Process Monitor - это расширенный инструмент мониторинга, который показывает в реальном времени файловую систему, реестр и активность процессов. Он сочетает в себе функции двух устаревших утилит Sysinternals, Filemon и Regmon, и добавляет ряд других улучшений. Монитор процессов можно использовать для отслеживания активности системы и программного обеспечения для устранения некоторых проблем с продуктом, особенно когда необходимо отслеживать, какое конкретное приложение или процесс обращается к файлу или разделу реестра.

Process Explorer – лучший инструмент для понимания того, как различные приложения работают в системе. Благодаря инновационной древовидной структуре он покажет, какие файлы, каталоги и другие процессы контролируются каждым родительским процессом.

Антивирусная утилита AVZ. Это решение для системного анализа и восстановления, предназначенное для автоматического или ручного поиска и удаления следующих вирусов:

– шпионские, рекламные программы и модули (ключевая функция

этого приложения);

- руткиты и вредоносные программы, которые скрывают свои процессы;
- сетевые и почтовые черви;
- трояны (все разновидности, в частности Trojan-PSW, Trojan-Downloader и Trojan-Spy) и бэкдоры (программы, используемые для скрытого удаленного управления компьютерами);
- регистраторы нажатий клавиш и другие приложения, которые шпионят за пользователем.

Google Rapid Response (GRR) - это платформа реагирования на инциденты на основе Python, которая фокусируется на криминалистике и расследованиях в реальном времени. Это позволяет аналитикам безопасности удаленно исследовать, атаковать и выполнять анализ.

GRR развернут в архитектуре сервер-клиент. Сервер GRR предоставляет пользовательский веб-интерфейс, который позволяет аналитикам анализировать данные, полученные от клиентов. Клиент GRR с другой стороны развертывается на хосте, подлежащем исследованию, и время от времени опрашивает сервер GRR для различных действий, таких как перечисление каталога, загрузка файлов.

Также используется IBM Security QRadar XDR – это решение для обнаружения угроз и реагирования на них, которое работает для более быстрого устранения угроз.

IBM Security QRadar помогает службам безопасности обнаруживать, понимать и определять приоритеты наиболее важных для бизнеса угроз. Решение собирает данные об активах, облаке, сети, конечных точках и пользователях, сопоставляет их с информацией об уязвимостях и сведениями об угрозах и применяет расширенную аналитику для выявления и отслеживания наиболее серьезных угроз по мере их продвижения по цепочке уничтожения.

Как только реальная угроза выявлена, расследования с помощью ИИ

обеспечивают быстрое и интеллектуальное понимание первопричины и масштаба угрозы, с целью предоставления организациям возможности поддерживать своих первоклассных аналитиков безопасности, ускорять процессы операций по обеспечению безопасности и снижать влияние угроз. инциденты. Открытый объединенный подход помогает организациям управлять растущим числом облачных приложений.

С помощью QRadar пользователь может интегрировать EDR, SIEM, NDR, SOAR и Threat Intelligence, оставляя данные там, где они есть, для комплексного подхода XDR, подключая существующие инструменты и автоматизируя SOC с помощью IBM и открытых сторонних интеграций.

Информация об угрозах поступает с платформы IBM X-Force Threat Intelligence, которая позволяет обмениваться исследованиями угроз безопасности, собирать аналитику и сотрудничать с коллегами.

QRadar XDR - это набор продуктов для обнаружения и реагирования на угрозы, который включает:

- IBM QRadar XDR Connect объединяет инструменты, автоматизирует SOC и оптимизирует рабочие процессы;
- IBM QRadar SIEM - это интеллектуальная аналитика безопасности, позволяющая получить действенное представление о наиболее серьезных угрозах;
- IBM QRadar NDR обнаруживает скрытые угрозы в сети;
- IBM QRadar SOAR уверенно, последовательно и совместно реагирует на инциденты безопасности.

Преимущества:

- простой и понятный интерфейс;
- горизонтальная масштабируемость;
- функции анализа сетевых потоков;
- возможность интеграции с множеством дополнительных модулей от IBM.

Недостатки:

– возможности тонкой отладки и кастомизации ограничены;
– корреляционные возможности ограничены.

Как видно из анализа имеющихся инструментов расследования инцидентов, в корпорации имеется набор утилит, но он довольно беден и для обеспечения информационной безопасности такой крупной организации их явно недостаточно. На выявление и расследование инцидентов сотрудники по безопасности тратят много времени и не всегда добиваются результата. До недавнего времени в корпорации использовалась система IBM Security QRadar XDR, но после ухода фирмы IBM с рынка России, система перестала обновляться и поддерживаться производителем. Все это приводит у тому, что корпорация «Росатом» подвергается дополнительным угрозам, так как специалисты по информационной безопасности не могут всецело обеспечивать защиту информации.

2.3 Обзор и сравнительный анализ SIEM-систем

Далее нужно провести обзор продуктов SIEM.

Arcsight Enterprise Security Manager (ранее HP Arcsight) - это программное обеспечение для управления информацией и событиями безопасности (SIEM), приобретенное у Hewlett-Packard Enterprise компанией Micro Focus и предлагаемое подразделением CyberRes компании.

Внедряемая система расследования инцидентов должна решать задачи, представленные на рисунке 20.

Рисунок 20 – Задачи системы расследования инцидентов

Преимущества продукта:

- нормализация на высоком уровне;
- тонкая отладка;
- кастомизация;
- мощный корреляционный функционал;
- интеграция с интеллектуальным регистратором и ESM для создания правил и простого управления ими;
- простая интеграция со всеми инструментами управления безопасностью конечных точек (IPS/IDS, брандмауэр, антивирус) и их консолидированные выходные данные в одном месте для эффективного устранения истинных и ложных срабатываний.
- Недостатки:
- существует проблема с хранилищем, которую следует решить для лучшего управления;
- сложность;
- необходимо улучшить механизм поиска;
- высокая стоимость;

– мало российских специалистов, которые могут работать с приложением.

Splunk Enterprise Security – это решение SIEM, которое помогает организациям обнаруживать, исследовать и реагировать на угрозы безопасности. Splunk Enterprise Security работает путем сбора и анализа данных из различных источников, включая сетевые устройства, серверы, приложения и устройства безопасности.

Затем он использует расширенную аналитику для выявления потенциальных угроз безопасности и создания предупреждений для специалистов по безопасности. Splunk Enterprise Security также интегрируется с внешними источниками информации об угрозах для расширения возможностей обнаружения угроз (рисунок 21).

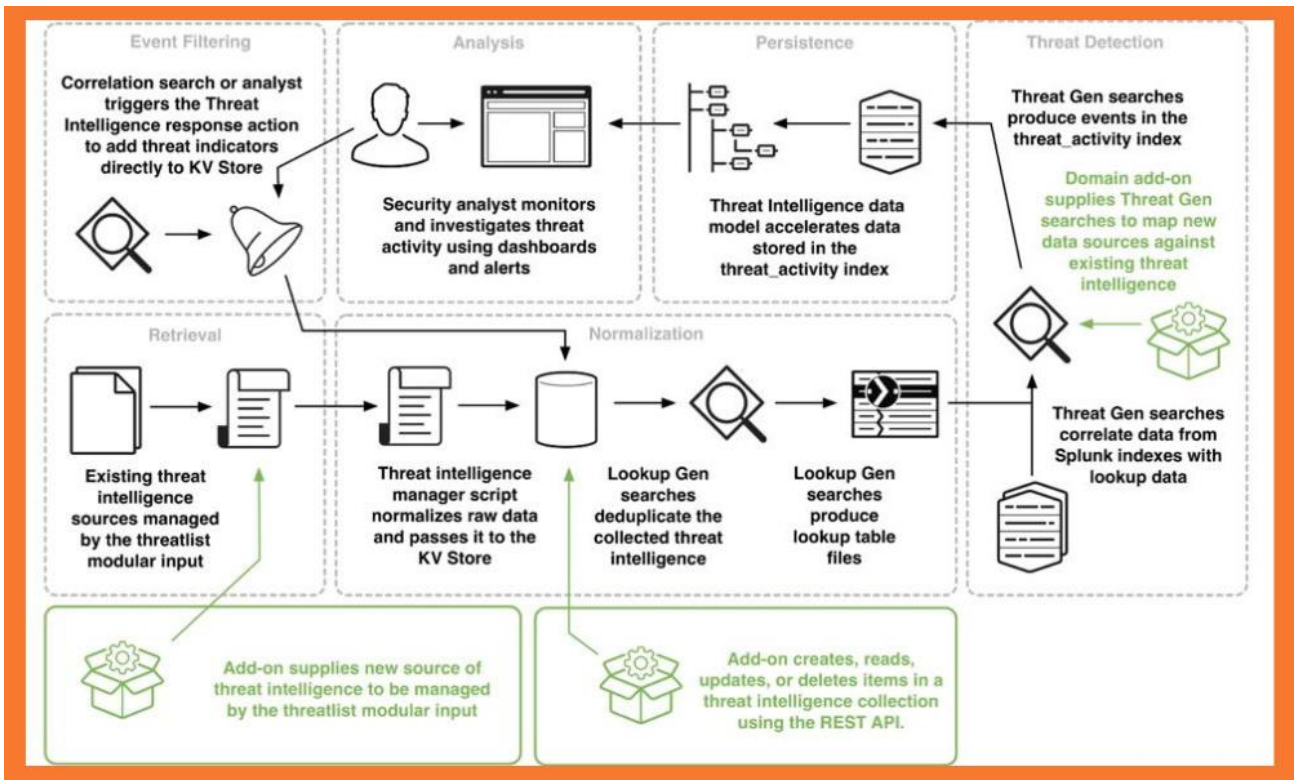

Рисунок 21 – Принцип работы Splunk Enterprise Security

Splunk Enterprise Security – это продукт премиум-класса, который может быть дорогим для небольших организаций. Модель ценообразования основана

на объеме данных, поступающих в день, и количестве пользователей. Цены начинаются от 150 долларов за гигабайт в день, и за премиум-функции и поддержку взимается дополнительная плата.

Преимущества:

- Splunk Enterprise Security предоставляет расширенные аналитические возможности, включая машинное обучение и поведенческую аналитику, которые помогают организациям быстро и эффективно обнаруживать угрозы безопасности и реагировать на них;
- Splunk Enterprise Security можно настроить в соответствии с конкретными потребностями организации в области безопасности. Он также интегрируется с широким спектром сторонних инструментов и платформ безопасности;
- Splunk может обрабатывать большие объемы данных безопасности, что делает его подходящим для организаций любого размера;
- Splunk имеет удобный интерфейс, который позволяет командам безопасности легко расследовать инциденты безопасности и принимать меры по исправлению положения.
- Недостатки:
- Splunk Enterprise Security – это продукт премиум-класса, который может быть дорогим для небольших организаций;
- у него крутая кривая обучения, и для его эффективного использования может потребоваться обучение сотрудников службы безопасности;
- Splunk Enterprise Security может быть ресурсоемким, требуя значительной вычислительной мощности и емкости хранилища для обработки больших объемов данных безопасности.

Российские вендоры только начинают свой путь на рынке систем расследования инцидентов, и продукты Security Capsule и MaxPatrol имеют все шансы прочно закрепиться на внутреннем рынке благодаря позициям вендора и тенденциям к импортозамещению.

«СёрчИнформ SIEM» - разработка российской компании

«СёрчИнформ». Первый релиз системы вышел в свет в ноябре 2016 года. Разработчик позиционирует продукт как «принципиально новую систему для выявления угроз и нарушений политик информационной безопасности с помощью анализа событий корпоративных систем». «СёрчИнформ SIEM» - система для сбора, мониторинга и анализа событий безопасности из корпоративных систем в режиме реального времени. Программа аккумулирует информацию из различных источников, анализирует ее, фиксирует инциденты и оповещает о них заинтересованных лиц» [13].

«СёрчИнформ SIEM» предоставляется только в виде программного обеспечения. Сервер комплекса работает на платформе Windows. Работа с комплексом также возможна только через приложение для Windows (рисунок 22)» [13].

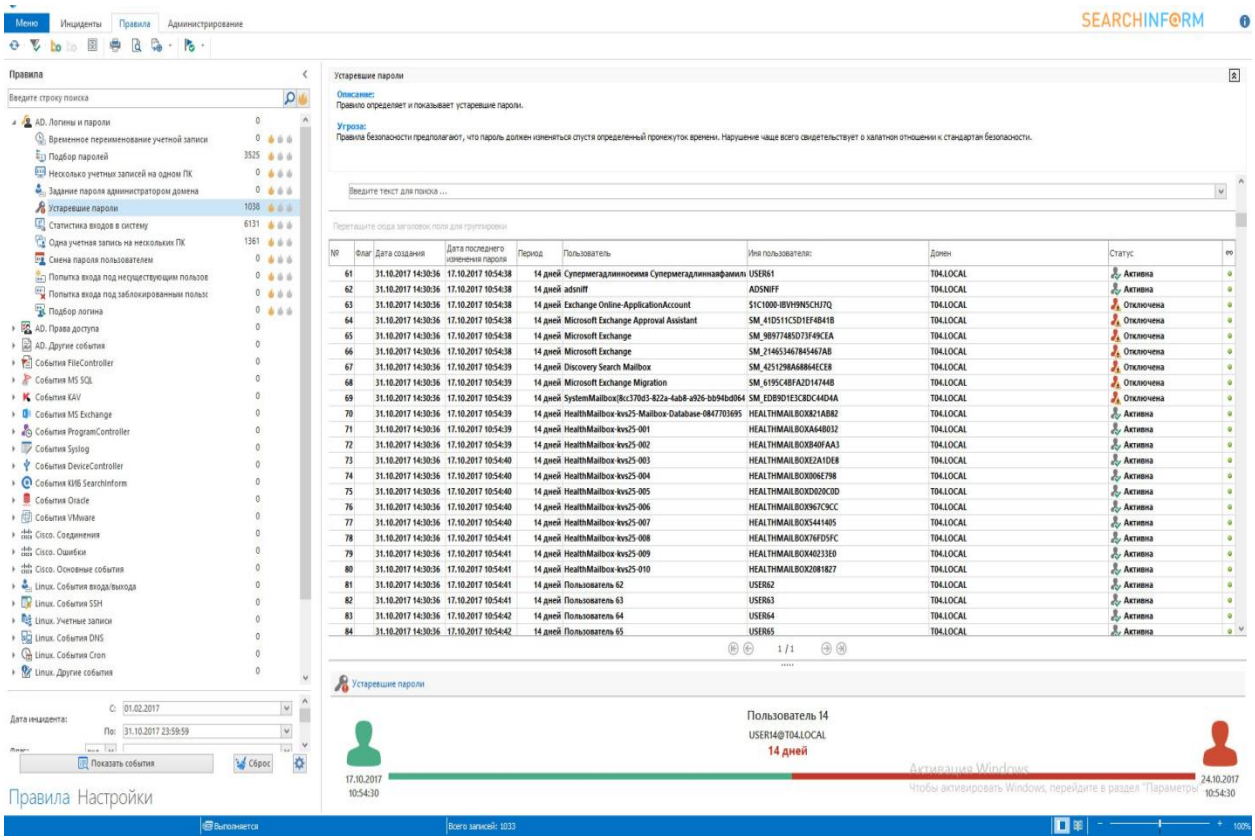

Рисунок 22 – Интерфейс системы «СёрчИнформ SIEM»

СёрчИнформ SIEM» имеет встроенные возможности, показанные на

рисунке.

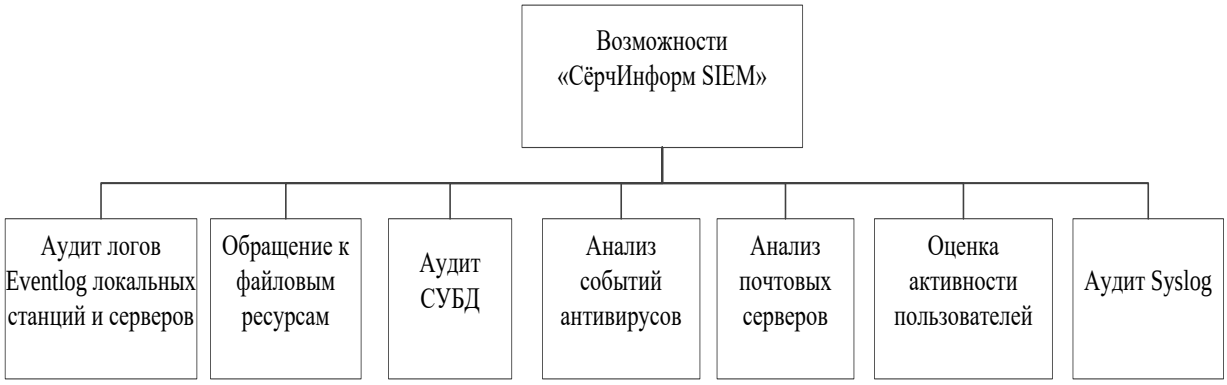

Рисунок 23 – Встроенные возможности «СёрчИнформ SIEM

«Преимущества «СёрчИнформ SIEM»:

- решение готово к работе «из коробки». Система не нуждается в настройке;
- продукт решает прикладные задачи и не требует привлечения дорогостоящих специалистов для настройки и работы с системой;
- тесная интеграция с DLP-системой «КИБ Серчинформ». Симбиоз решений дает доступ к уникальным источникам данных, например, к информации об активности пользователей (Time Tracking), о подключаемых устройствах хранения и т.д.;
- российский продукт. Это позволяет напрямую взаимодействовать с разработчиком, без привлечения интегратора;
- простая и понятная система лицензирования» [30].

Архитектура MaxPatrol SIEM является гибкой: ее можно масштабировать и развертывать в компаниях любого размера. Следует сопоставить MaxPatrol SIEM с инфраструктурой, выбрав количество серверов, сканеров и режимов сканирования.

Ядром системы является MP Server. Этот модуль управления является отправной точкой для настройки системы. Он включает MP Scanner, который

сканирует, собирает и обрабатывает данные. При необходимости подключите к MP Server дополнительные модули сканирования. Добавление модулей повышает скорость сканирования и чувствительность к топологии сети.

MaxPatrol SIEM предназначен для управления уязвимостями и соответствия корпоративным информационным системам. Тестирование на проникновение, системные проверки и мониторинг соответствия требованиям лежат в основе MaxPatrol SIEM . Вместе эти механизмы дают объективную картину состояния безопасности ИТ-инфраструктуры, а также детализированную информацию на уровне отдела, хоста и приложения - именно та информация, которая необходима для быстрого обнаружения уязвимостей и предотвращения атак (рисунок 24).

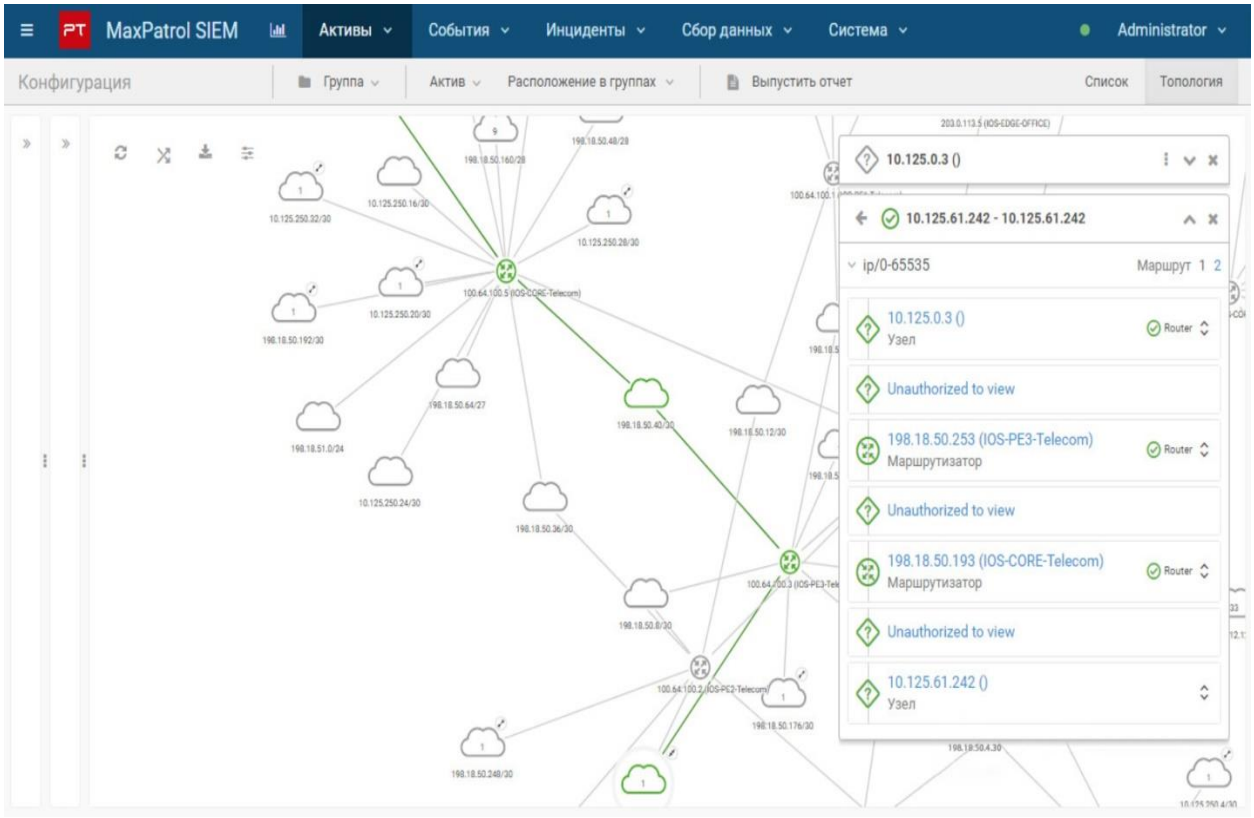

Рисунок 24 – Рабочая область MaxPatrol SIEM

На рисунках 25, 26 представлены отчет по возможным инцидентам, выявленным данной программой.

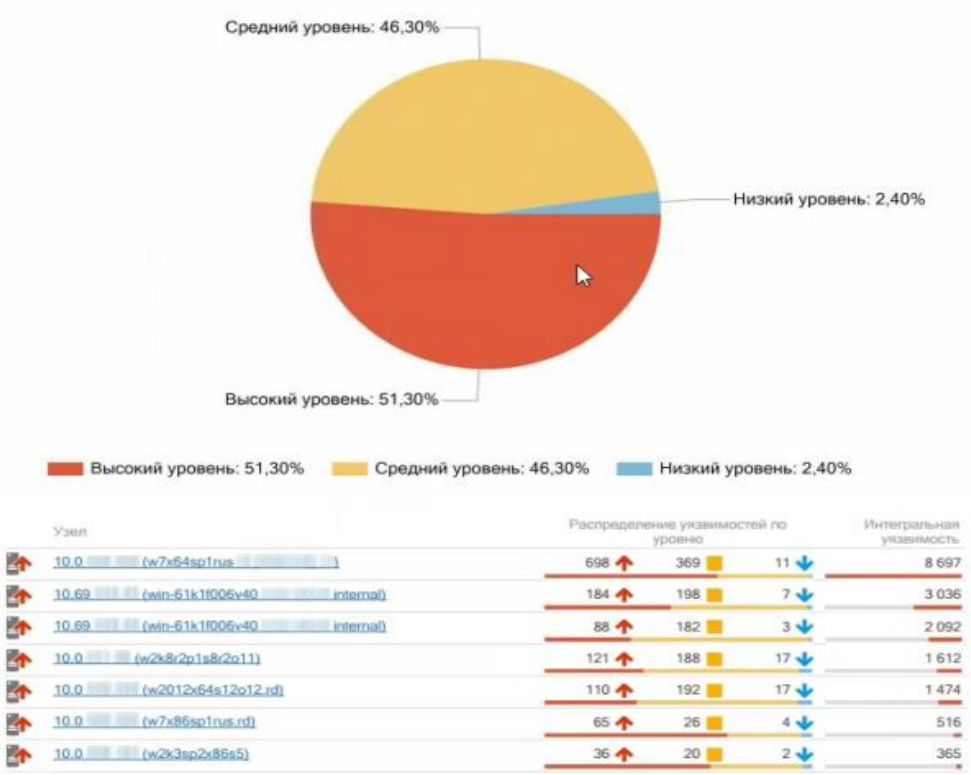

Рисунок 25 – Пример отчета по уязвимым узлам сети в MaxPatrol

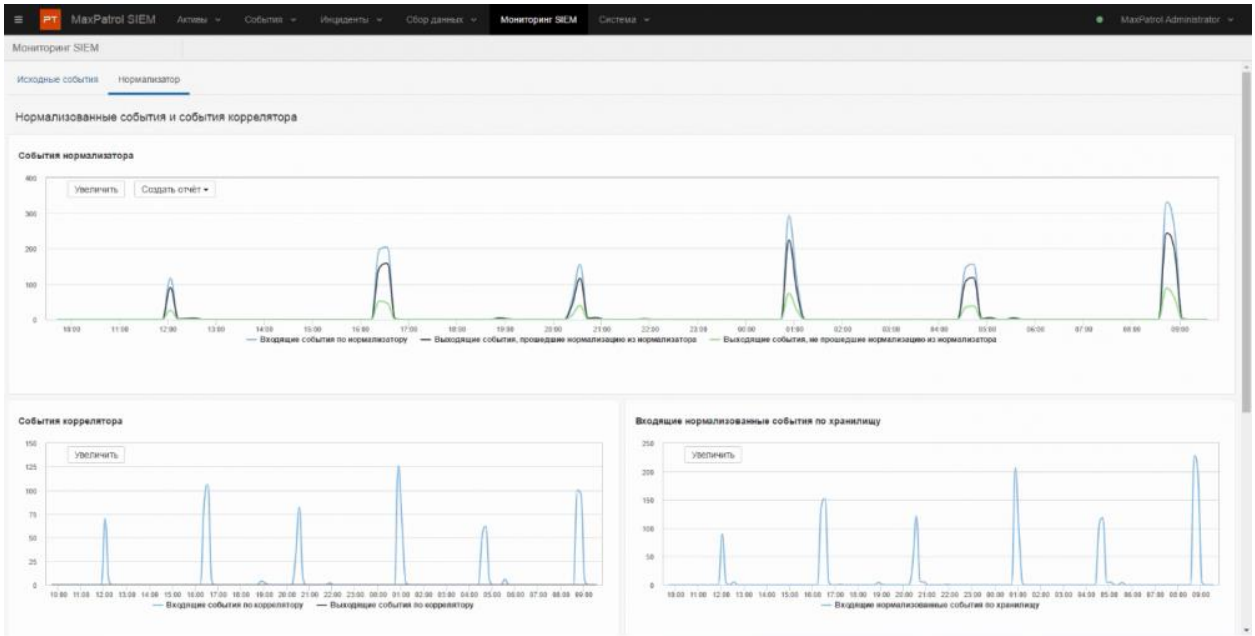

Рисунок 26 – Мониторинг получения событий в MaxPatrol

КОМРАД представляет собой гибкую и масштабируемую систему

централизованного управления событиями информационной безопасности, которая поддерживает широкий спектр отечественных средств защиты информации (рисунок 27).

Рисунок 27 – Анализ событий в «Комрад»

Функциональные возможности системы:

- высокопроизводительный сбор событий ИБ в инфраструктуре масштаба предприятия;
- нормализация - приведение событий к внутренней структуре события;
- автоматическая индексация событий;
- визуальный конструктор правил фильтрации событий;
- визуальный конструктор директив корреляции;
- агрегация инцидентов;
- уведомление о факте регистрации инцидента как в интерфейсе пользователя, так и через по электронной почте;
- отображение данных событий в виде графиков и диаграмм: линейные,

столбчатые, круговые, радиальные и др.;

- создание дашбордов для управления активами;
- формирование отчётов.

Методика проведения исследования включает следующие этапы:

- анализ инфраструктуры, в которую будет интегрирована система расследования инцидентов;
- проведение опроса специалистов для составления политики мониторинга;
- сборка и монтаж оборудования системы расследования инцидентов;
- установка и настройка программных средств системы расследования инцидентов;
- инсталляция политики мониторинга.

Проведение интеграции системы расследования инцидентов с сервисами Заказчика заключаются в следующем:

- подключение документов и материалов, касающихся организационной структуры, списка сотрудников;
- внутренний почтовый трафик пользователей должен быть автоматически записан с почтового сервера Microsoft Exchange;
- интеграция системы расследования инцидентов в почтовую инфраструктуру Заказчика для обеспечения работы системы в разрыв;
- установка агентов системы расследования инцидентов на компьютеры персонала.

В рамках опытной эксплуатации Исполнитель обязан проводить консультации специалистов по вопросам работы системы расследования инцидентов.

Проведение приемо-сдаточных испытаний осуществляется на основании согласованной с заказчиком программе и методике испытаний.

В заключение осуществляется перевод системы расследования инцидентов в промышленную эксплуатацию.

В итоге выполнения работ по проектированию и внедрению системы

расследования инцидентов система должна работать в штатном режиме. Процесс управления событиями и инцидентами должен быть автоматизирован.

2.4 Характеристика выявленных проблем при внедрении SIEM-системы в конкретную ИТ-инфраструктуру

При внедрении SIEM-системы выявилось, что развертывания SIEM недостаточно для полной защиты организации.

Решения SIEM имеют ограничения, которые делают их неэффективными без правильной поддержки и сторонних решений. В отличие от Firewall Security или IDS, SIEM не отслеживает события безопасности, а использует хранящиеся в них данные журналов. Поэтому важно не пренебрегать реализацией этих решений.

SIEM - это сложный продукт, который требует поддержки для обеспечения успешной интеграции с элементами управления безопасностью компании и множеством хостов в ее инфраструктуре.

Важно не просто установить SIEM с конфигурациями производителя и/или по умолчанию, так как их часто бывает недостаточно. Конфигурации должны быть настроены и адаптированы к потребностям пользователей. Точно так же для отчетов лучше создавать свои аналитические отчеты, адаптированные к различным выявленным угрозам. В противном случае есть реальный риск того, что воспользоваться преимуществами SIEM-решения не получится.

Для анализа, настройки и интеграции отчетов требуется опыт экспертов. По этой причине большинство SIEM управляются непосредственно внутри SOC (Security Operations Center), который часто отдается на аутсорсинг. Неправильно настроенная SIEM может принести немало разочарований.

Процесс управления инцидентами SOC (Security Operations Center) является важным компонентом стратегии безопасности организации. Это

помогает команде SOC быстро обнаруживать, реагировать и восстанавливаться после инцидентов безопасности, которые могут нанести ущерб системам, данным и репутации организации [12].

Типичный процесс управления инцидентами SOC состоит из нескольких этапов, в том числе:

- обнаружение инцидента. Первым шагом является обнаружение и классификация инцидента. Это может включать выявление необычных шаблонов действий или предупреждений системы безопасности, инициируемых инструментами безопасности, такими как системы обнаружения вторжений (IDS) и системы управления информацией и событиями безопасности (SIEM);
- сортировка инцидента: после обнаружения и классификации инцидента группа SOC проводит процесс сортировки, чтобы определить масштаб, серьезность и влияние инцидента. Это помогает расставить приоритеты в ответных действиях в зависимости от риска для организации;
- сдерживание инцидента. Следующим шагом является сдерживание инцидента путем изоляции затронутых систем или сетей для предотвращения дальнейшего ущерба. Это может включать в себя отключение затронутых систем или отключение сетевых подключений;
- расследование инцидента. На этом этапе команда SOC проводит тщательное расследование, чтобы определить первопричину инцидента, степень ущерба и любые потенциальные индикаторы компрометации (IOC), которые могут указывать на нарушение;
- смягчение последствий инцидента: после завершения расследования команда SOC реализует план смягчения последствий, чтобы свести к минимуму последствия инцидента. Обычно это включает удаление вредоносного ПО, восстановление данных из резервной копии и исправление уязвимостей;

– отчетность об инцидентах. Наконец, команда SOC документирует инцидент, описывая детали инцидента, меры реагирования и любые извлеченные уроки. Это помогает информировать будущие процессы управления инцидентами и улучшать состояние безопасности организации.

В целом процесс управления инцидентами SOC является важнейшим компонентом любой стратегии кибербезопасности, помогая организациям быстро реагировать на инциденты безопасности и предотвращать дальнейший ущерб.

Обслуживание и настройка оказались сложны.

После покупки SIEM потребовалось около 90 дней только для установки, прежде чем она начнет работать.

Решения SIEM обычно полагаются на правила для анализа всех записанных данных. Однако сеть компании генерирует очень большое количество предупреждений (в среднем 10 000 в день), которые могут быть положительными или нет. В результате выявление потенциальных атак осложняется объемом нерелевантных журналов.

Решение состоит в том, чтобы определить точные правила, которые обычно пишет SOC, и контролируемый периметр: что следует отслеживать в первую очередь? Периметр? Сеть/система/приложение? Какой технологии отдать предпочтение и т. д.

Бюджет на персонал оказался выше ожидаемого.

Решения SIEM получают журналы безопасности из самых разных систем: компьютеров, серверов, систем аутентификации, брандмауэров и т. д.

В эти журналы записываются все события, происходящие в системах и сетях. Их обзор может помочь отслеживать действия, реагировать на события и защищать системы. Поскольку журналы компании ежедневно отслеживают миллионы событий, функция решения SIEM заключается в хранении и анализе в режиме реального времени всех этих предупреждений системы безопасности, генерируемых сетевыми приложениями и устройствами.

Кроме того, для корректной работы SIEM-решениям требуется круглосуточный мониторинг предупреждений и журналов. Для просмотра событий, проведения регулярных обзоров и извлечения соответствующих отчетов требуется обученный персонал или специальная группа.

Многие предприятия предполагают, что установить SIEM довольно просто, но на самом деле они не понимают, что SIEM потребует создания специально обученного и квалифицированного персонала, чтобы максимально использовать данные SIEM и отвечать на его отчеты. Таким образом, кадровый бюджет оказывается выше ожидаемого.

Информированный кибер-злоумышленник знает, что журналы событий обычно отправляются пакетами, а не в режиме реального времени, чтобы ограничить влияние их передачи на пропускную способность сети.

Таким образом, у хакера есть окно доступа к операционной системе, включая базовую систему регистрации. Если он может очистить доступ к журналу с правами администратора перед его отправкой, у компании не будет никаких доказательств нарушения безопасности.

С другой стороны, если злоумышленнику удастся выполнить аутентификацию системы, не вызвав предупреждение об аномалии или используя вредоносное ПО, системы сетевого мониторинга не будут генерировать никаких событий [15].

Решение этих проблем SIEM заключается в том, чтобы найти лучший инструмент, который лучше всего подходит для ИТ-команды.

Выводы по главе 2

В данной главе проблемы внедрения SIEM-систем рассмотрены на примере крупнейшей государственной корпорации «Росатом». Предприятие является субъектом КИИ, так как занимается производством электроэнергии.

Был проведен анализ ИТ-инфраструктуры организации. Компания не только имеет развитую инфраструктуры, но и сама разрабатывает цифровые продукты. Корпорация используется множество инструментов для

обнаружения угроз – это различные утилиты, журналы. Так как субъекты КИИ обязаны использовать SIEM-системы, в корпорации использовалась система IBM Security QRadar XDR. Но из-за санкций фирма IBM ушла с рынка России, система перестала обновляться и поддерживаться производителем. Поэтому встал вопрос о внедрении другой SIEM-системы. Для этого был проведен обзор распространенных SIEM-систем, преимущественно российского производства. В результате анализа и сравнения была выбрана система «СёрчИнформ SIEM».

При внедрении системы возникли проблемы различного характера. Первая проблема заключается в необходимости автоматизации процесса мониторинга событий безопасности в локальной сети организации. Вторая – сложность настройки и обслуживания системы. Третья – сложность эксплуатации – экспертозависимость. Хотя в компании имеется штат сотрудников, все равно работе с новой системой необходимо обучиться. четвертая проблема – планирование бюджета, он в итоге превысил ожидаемый лимит.

Варианты решения данных проблем будут рассмотрены в следующей главе.

Глава 3 Разработка принципов эффективного управления информационной безопасностью в организации на основе SIEM-технологии

По результатам проведенной научно-исследовательской работы удалось сформировать следующие тезисы (положения) по теме проводимого исследования.

3.1 Необходимость автоматизации процесса мониторинга событий информационной безопасности

На сегодняшний день разнообразие типов и количество различных средств защиты информации, внедренных в инфраструктуре даже компании среднего размера, не позволяют человеку эффективно отслеживать и контролировать их работу, по причине ограниченности человеческих возможностей. Необходимы средства автоматизации процесса мониторинга событий информационной безопасности.

«Весь перечень используемых в организации средств защиты информации можно объединить по характеру своего назначения в несколько подсистем:

– Подсистема защиты от угроз несанкционированного доступа обеспечивает разграничение доступа к ресурсам автоматизированных рабочих мест и серверов локальной сети, регистрацию и учет событий безопасности, целостность программно-аппаратной среды применяемых программных и программно-технических средств;

– Подсистема антивирусной защиты представляет собой комплекс программно-технических и организационных решений, обеспечивающий обнаружение фактов воздействия вредоносного кода на объекты защиты в процессе их функционирования, а также при выполнении периодических проверок оперативной памяти, сменных и локальных носителей информации,

файлов, в том числе получаемых по каналам связи, по запросам пользователей и/или администраторов;

– Подсистема межсетевого экранирования и защиты каналов связи, обеспечивающая требования по разграничению доступа к сетевым ресурсам, а также защите от сетевых атак и криптозащите сетевого трафика, выходящего за границу сетевого периметра локальной вычислительной сети организации» [8].

Кроме этого информационная инфраструктура компании по требованию государственных регуляторов может быть дополнена подсистемами анализа защищенности и обнаружения вторжений [11]. Обязательность выполнения данных требований зависит от основного рода деятельности организации и закреплена в действующих нормативных актах Российской Федерации. Для наглядности примерная схема взаимодействия источников событий безопасности представлена на рисунке 28.

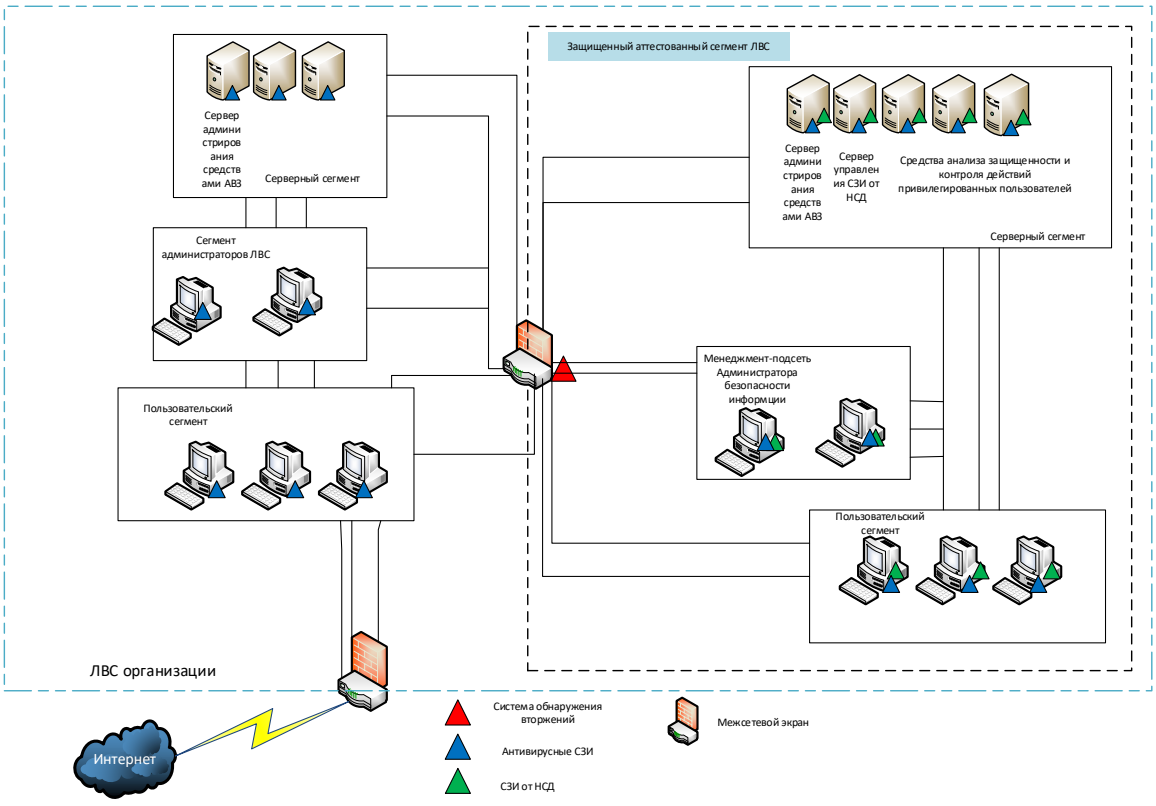

Рисунок 28 – Схема взаимодействия источников событий безопасности

Как видно из вышеизложенного, разнообразие используемых средств защиты в пределах одной организации сегодня не позволяет одному или нескольким специалистам эффективно обрабатывать в реальном времени поток сообщений о событиях информационной безопасности со всех перечисленных технических средств и грамотно на них реагировать, необходима автоматизированная система централизованного мониторинга.

Диаграммы процесса обеспечения информационной безопасности (ИБ) в организации без внедренной SIEM-системы представлены на рисунках 29 и 30.

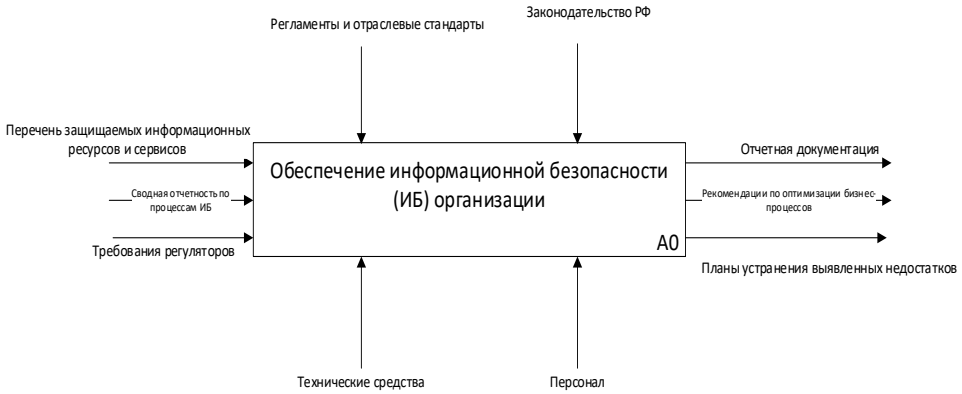

Рисунок 29 – Контекстная диаграмма обеспечения ИБ в организации

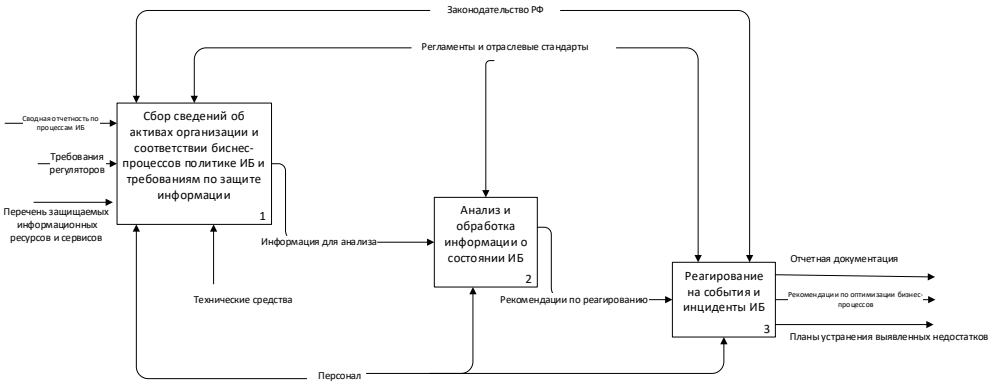

Рисунок 30 – Диаграмма обеспечения ИБ без SIEM

Диаграмма процесса обеспечения ИБ с эксплуатируемой в её

информационной инфраструктуре SIEM представлена на рисунке 31.

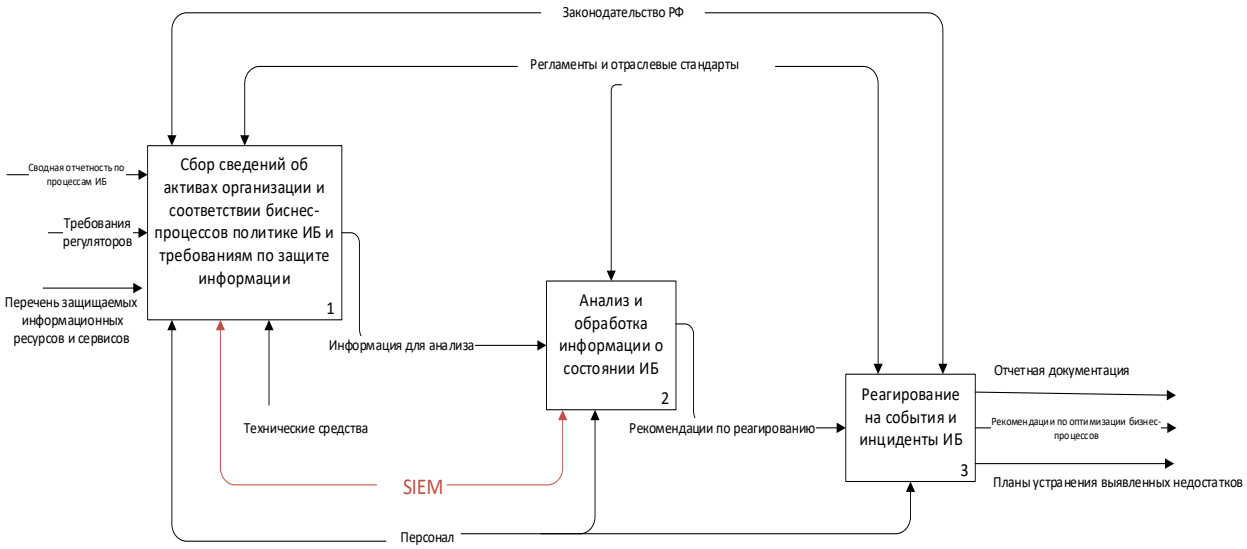

Рисунок 31 – Диаграмма обеспечения ИБ после внедрения SIEM

SIEM осуществляет автоматизированный сбор, хранение и анализ событий, происходящих в ИТ-инфраструктуре с целью выявления аномальной активности и преднамеренных и непреднамеренных вредоносных действий.

SIEM позволяет в автоматическом режиме сканировать ИТ-инфраструктуру с целью инвентаризации подключенных к сети активов и сбора информации о них. Дополнительно сведения об активах могут быть получены при обработке событий и анализе сетевого трафика ИТ-инфраструктуры.

При определенных условиях выявление события ИБ может приводить к необходимости создания инцидента ИБ. SIEM автоматически или пользователь в ручном режиме создает запись об инциденте ИБ (карточку инцидента). Помимо оперативного мониторинга ИБ ИТ-инфраструктуры система позволяет осуществлять поддержку расследования инцидентов, выявленных SIEM или импортированных из других систем. SIEM обеспечивает высокую скорость оповещения персонала через веб-интерфейс и/или электронную почту, а также сторонние сервисы. Система в целом

обеспечивает автоматизацию процессов управление активами, событиями и инцидентами. SIEM-система позволяет получать сведения о событиях и инцидентах ИБ, происходящих в информационной инфраструктуре организации, из единой консоли управления без необходимости подключаться ко множеству средств защиты и мониторинга. Централизованное средство управления процессами ИБ в организации позволит сэкономить время на сбор информации и значительно увеличит скорость принятия решений и реагирования на инциденты и/или события ИБ.

Наглядно данные различия показаны на рисунках 32 и 33.

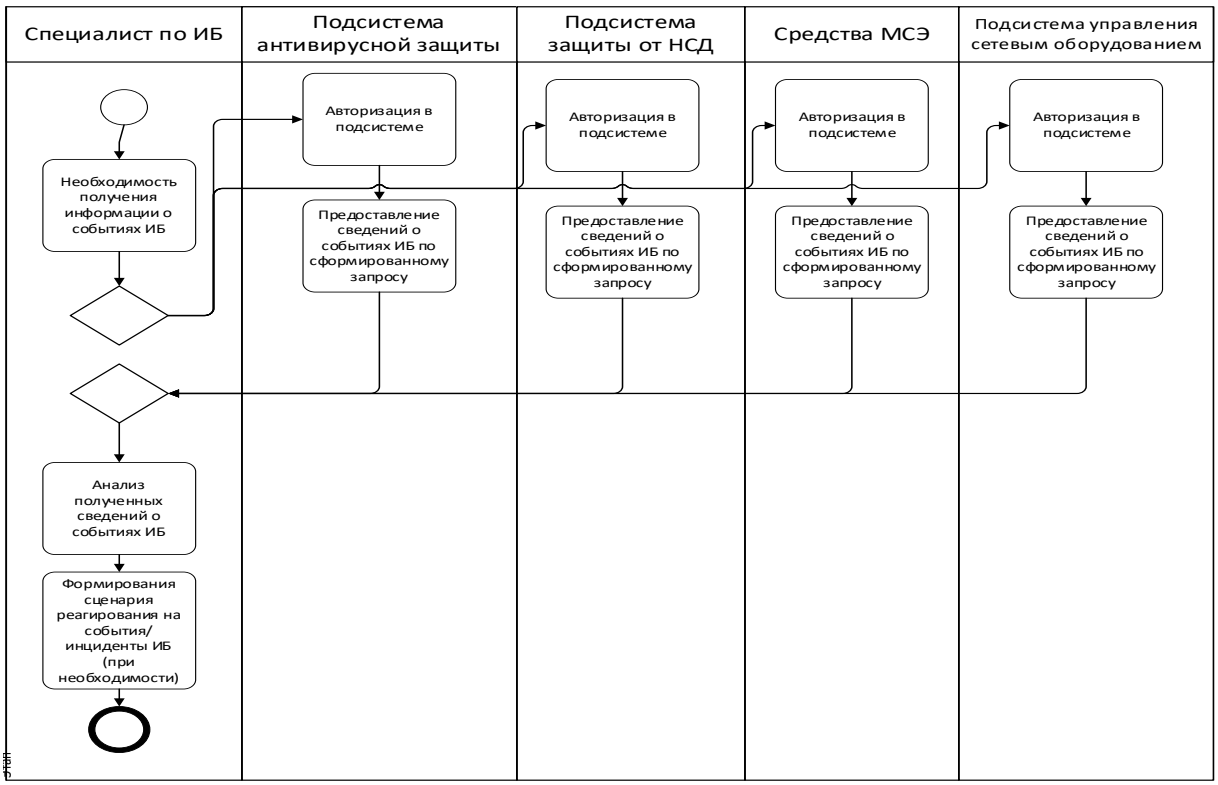

Рисунок 32 – Схема мониторинга событий ИБ без SIEM

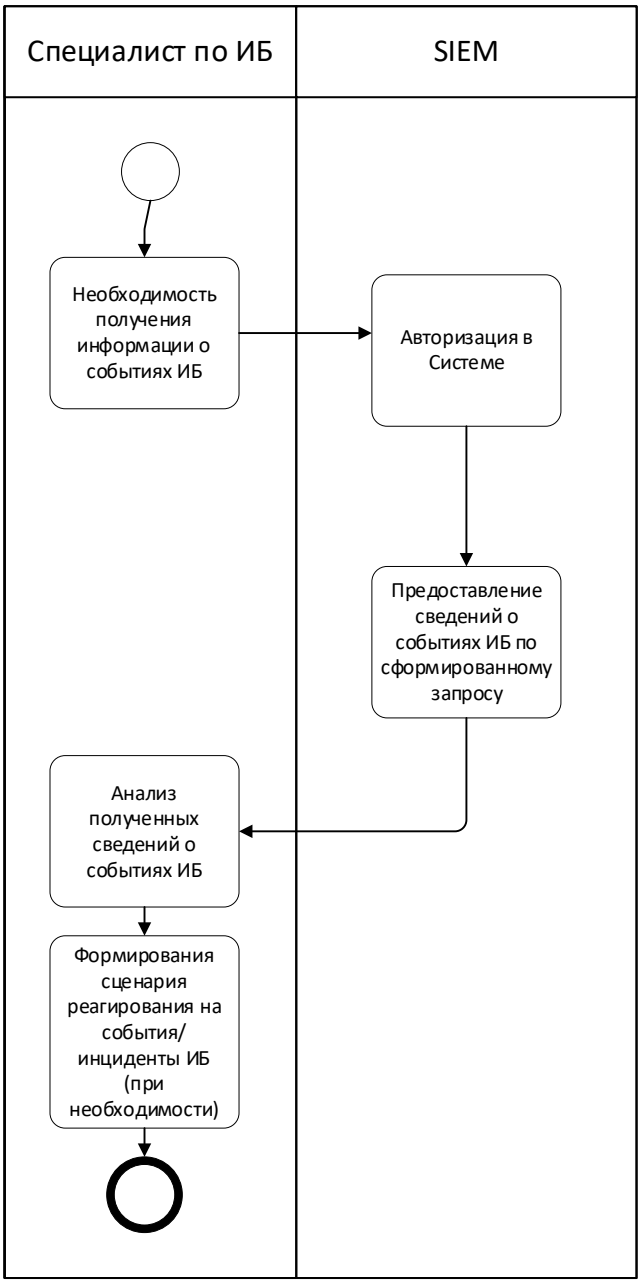

Рисунок 33 – Схема мониторинга событий ИБ с внедренной SIEM

Преимущество от внедрения и применения SIEM-системы заключается в том, что она значительно ускоряет процесс обработки инцидентов ИБ и получения требуемой информации о событиях ИБ: аналитику не нужно подключаться к каждому средству защиты информации, он видит все данные в едином, консолидированном виде в одном удобном интерфейсе.

3.2 SIEM-система – основа корпоративной системы обеспечения ИБ

SIEM-система может стать той самой основой корпоративной системы обеспечения информационной безопасности, развивая и дополняя которую различными компонентами (источниками событий), можно выстроить эффективную систему защиты информации в рамках организации [25].

SIEM работает по непрерывному циклу сбора, анализа и реагирования на информацию в реальном времени. При обнаружении потенциальной угрозы система срабатывает, отправляет уведомления и принимает необходимые меры для предотвращения инцидентов безопасности. Затем проводится анализ произошедших событий и составляются отчеты, которые помогают лучше понять текущую ситуацию и принять меры для улучшения стратегии безопасности. Схематично SIEM-процесс представлен на рисунке 34.

Рисунок 34 – Схема SIEM-процесса

Диаграмма развертывания компонентов SIEM-системы в информационной инфраструктуре организации представлена на рисунке 35.

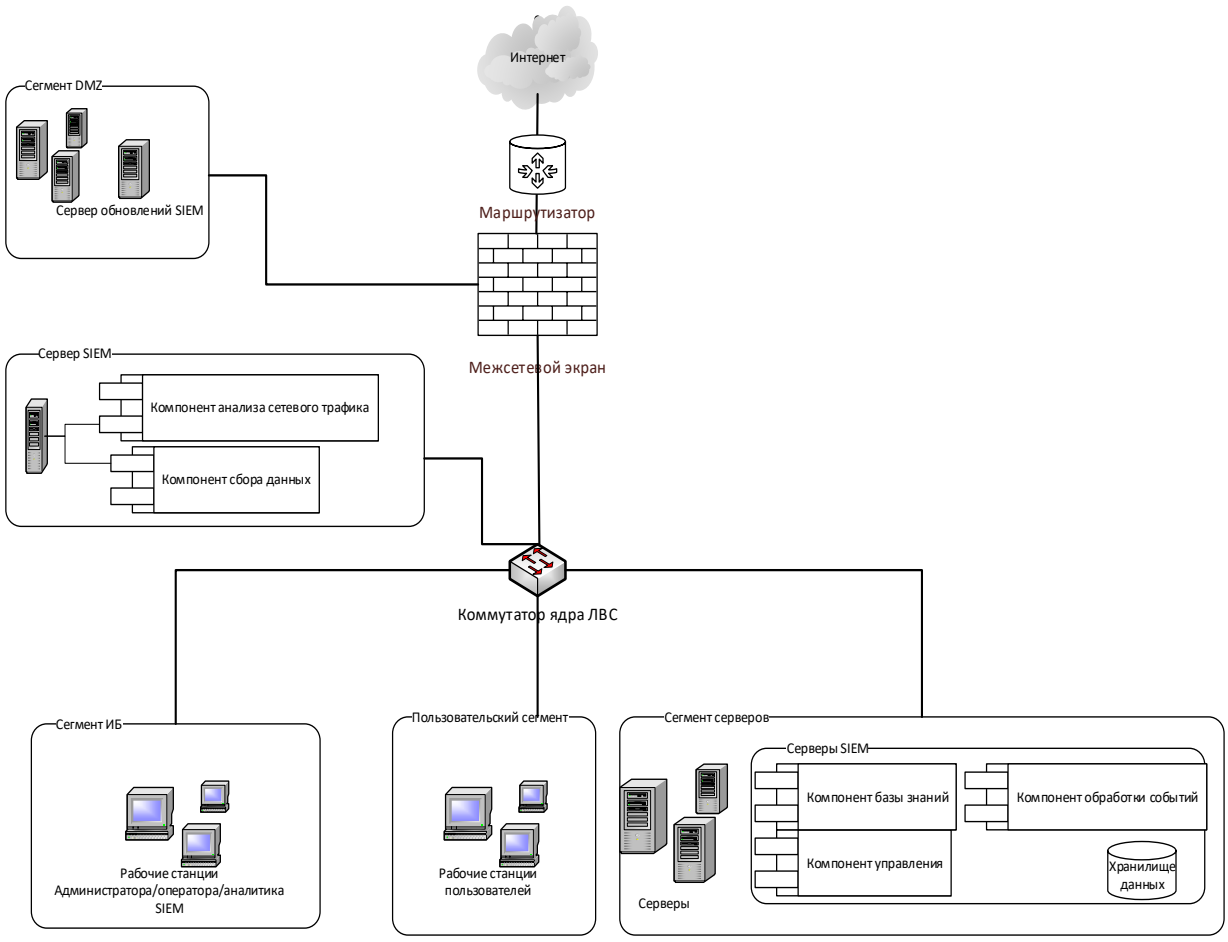

Рисунок 35 – Диаграмма развертывания компонентов SIEM-систем

Рассмотрим алгоритм разработки универсальных правил корреляции.

3.3 Алгоритм разработки универсальных правил корреляции

Принимая решение о внедрении SIEM-системы в собственную инфраструктуру, необходимо помнить, что вышеуказанные преимущества от наличия системы подобного класса возможно получить только при правильной настройке и эксплуатации SIEM-системы.

Данные аспекты неразрывно связаны с разработкой унифицированных правил нормализации и корреляции событий безопасности, поступающих в SIEM, которые значительно сократят время на внедрение и настройку системы, и так называемой «экспертозависимостью» при эксплуатации SIEM-

системы.

Предустановленные производителем SIEM правила корреляции не адаптированы под особенности инфраструктуры конкретного заказчика. У данной проблемы есть несколько причин:

- потеря данных, характеризующих событие, при их распределении по полям таксономии в соответствии с настроенной схемой внутри SIEM-системы на этапе нормализации;
- отсутствие четко определенной методологии нормализации событий;
- постоянное изменение объекта защиты (его свойств и характеристик) под воздействием людей и процессов;
- отсутствие методологии написания правил корреляции.

Проанализировав возможные варианты взаимодействия сущностей (субъектов и объектов) внутри любой инфраструктуры, можно сформулировать определенные принципы, которых необходимо придерживаться при создании правил нормализации событий:

- на этапе нормализации событий необходимо явно выделить сущности, присутствующие в рамках каждого события: субъект, объект, ресурс (например, файлы или директории), источник (например, нода межсетевого экрана или сервера) и передатчик (в случае наличия промежуточного сервера – syslog-сервер, Kaspersky Security Center и т.д.);
- при нормализации потока событий, поступающих в SIEM, необходимо учитывать, что в описании одного события могут быть одновременно отражены взаимодействия и уровня сети и уровня приложений;
- описания взаимодействия сущностей между собой содержат не только информацию об образованных каналах передачи данных, но и о самих данных, передаваемых по данным каналам.

Таким образом, перечень полей для нормализации событий в SIEM-системе, на уровне сети выглядит следующим образом:

– субъект;

– объект;

– источник;

– передатчик;

– канал взаимодействия (канал передачи данных);

– данные, передаваемые по каналу передачи данных.

Для уровня приложений перечень полей включает субъект, объект (группу объектов), ресурс (группу ресурсов).

Вариант распределения данных по полям таксономии (нормализации) представлен на рисунке 36.

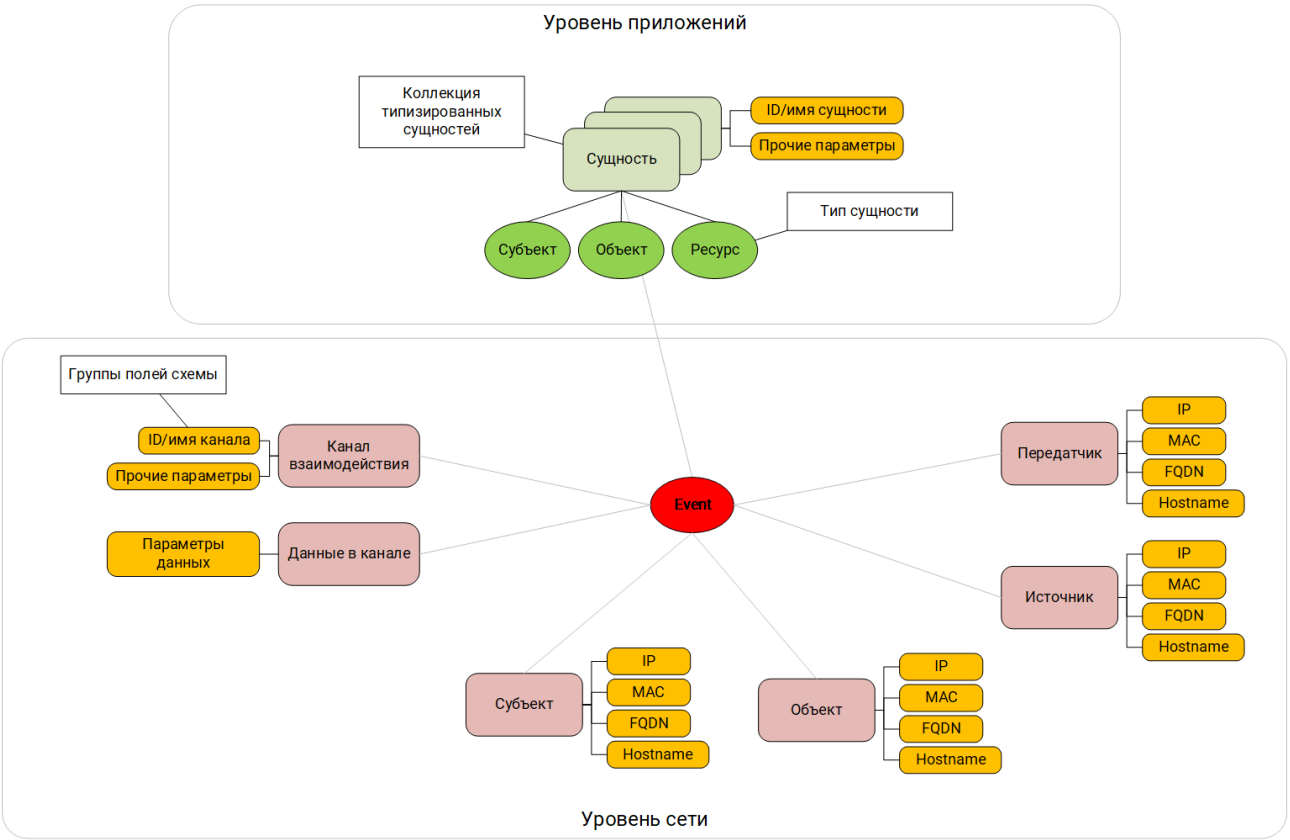

Рисунок 36 – Разделение сущностей по полям нормализации

Описываемая сущность содержит определенный индивидуальный набор свойств, который помогает ее однозначно идентифицировать (IP- или MAC-

адреса, FQDN). Для уровня приложений — это имена и\или идентификаторы. Также существуют схемы взаимодействия, при которых одна сущность может сочетать в себе сразу несколько ролей. При нормализации событий, описывающих взаимодействие сущностей, сочетающих в себе сразу несколько ролей, необходимо явно определить правило заполнения всех полей схемы нормализации, отвечающих за весь набор сущностей, чтобы не пропустить часть взаимодействий.

Далее для корректного создания правил корреляции и проведения расследований инцидентов информационной безопасности необходимо сформировать систему категоризации событий.

Система категоризации событий должна соответствовать определенным требованиям:

- однозначность: одно событие должно быть отнесено только к одной категории;
- компактность: эксперт должен иметь возможность запомнить перечень имеющихся в наличии категорий;
- иерархичность: на первом уровне располагаются более «общие» категории, на следующих – узкоспециализированные;
- расширяемость: система категоризации должна позволить вносить в неё изменения при появлении новых типов событий, требующих отдельных категорий, при этом не меняя основного подхода.

Целесообразно разделить всю систему категоризации на два крупных направления: категоризации событий от IT-источников и категоризации событий от ИБ-источников.

Система категоризации событий от ИТ-источников формируется, в соответствии со следующими правилами:

- IT-события отражают этапы или детали IT-процессов, которые поддерживаются или реализуются источниками событий;
- система категоризации состоит из 3-х основных уровней и одного дополнительного, определяющего успешность или не успешность

действия, описанного в событии;

– на первом уровне выделяются IT-процессы, в рамках которых работает источник событий (управление сетевыми взаимодействиями, управление базами данных, управление доступом и т.д.);
– второй уровень описывает основные сущности, участвующие в данном процессе (профиль пользователя, приложения, правила и политики, сетевые адреса, базы данных и т.д.);
– третий уровень определяет действия, выполняющиеся определенной или с определенной сущностью в рамках рассматриваемого процесса (взаимодействие, влияющее на функционирование сущности; изменение состояния; взаимодействие, в результате которого происходит добавление новой сущности в контекст, либо удаление сущности из контекста).

Система категоризации ИТ-событий наглядно представлена на рисунке 37.

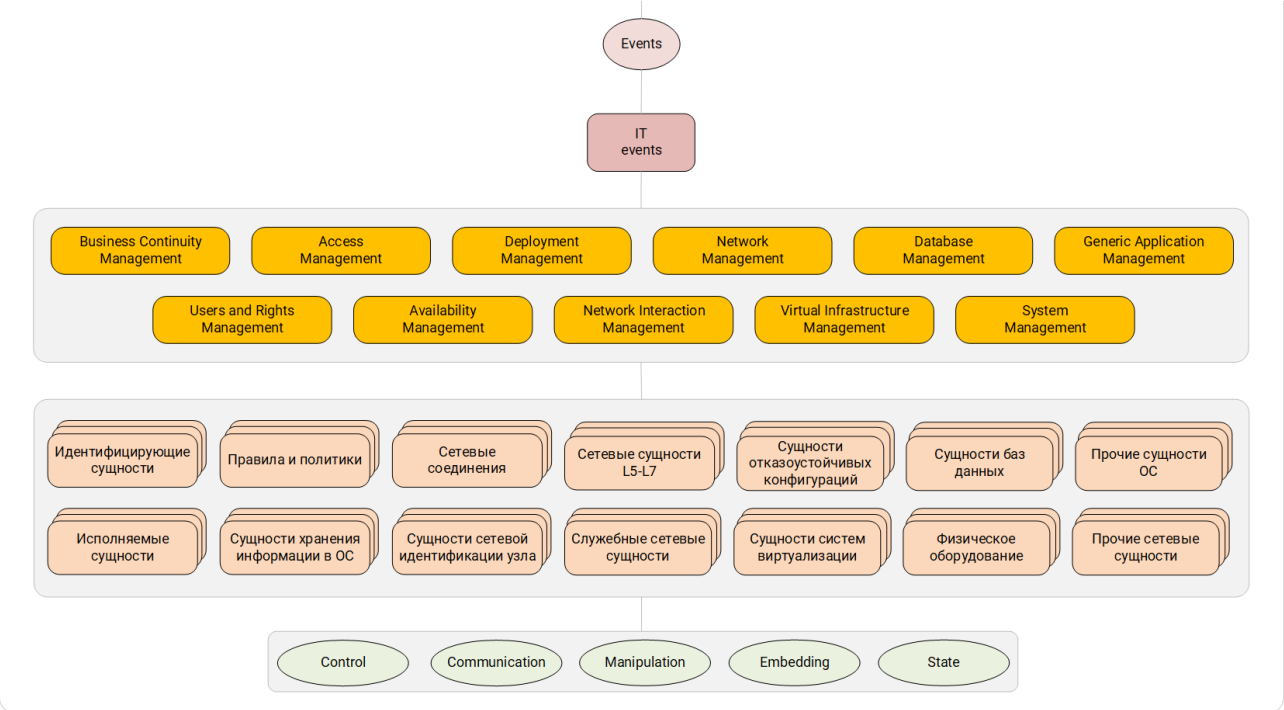

Рисунок 37 – Система категоризации ИТ-событий

Система категоризации ИБ-событий, наглядно показана на рисунке 38 и применяется исключительно к событиям, собираемым с различных средств защиты информации. Сама система категоризации состоит из 3-х уровней;

– на первом уровне выделяются домены, в которых могут быть зафиксированы нарушения ИБ (нарушения уровня хоста, сети и физической среды);
– второй уровень образуют определенные классы нарушений (зловредный контент, нарушение доступности, выявление использования вредоносного кода и т.д.);
– третий уровень образуют типы нарушений, определяемые в рамках заданного класса (спам, фишинг, DDoS, TOR client и т.д.).

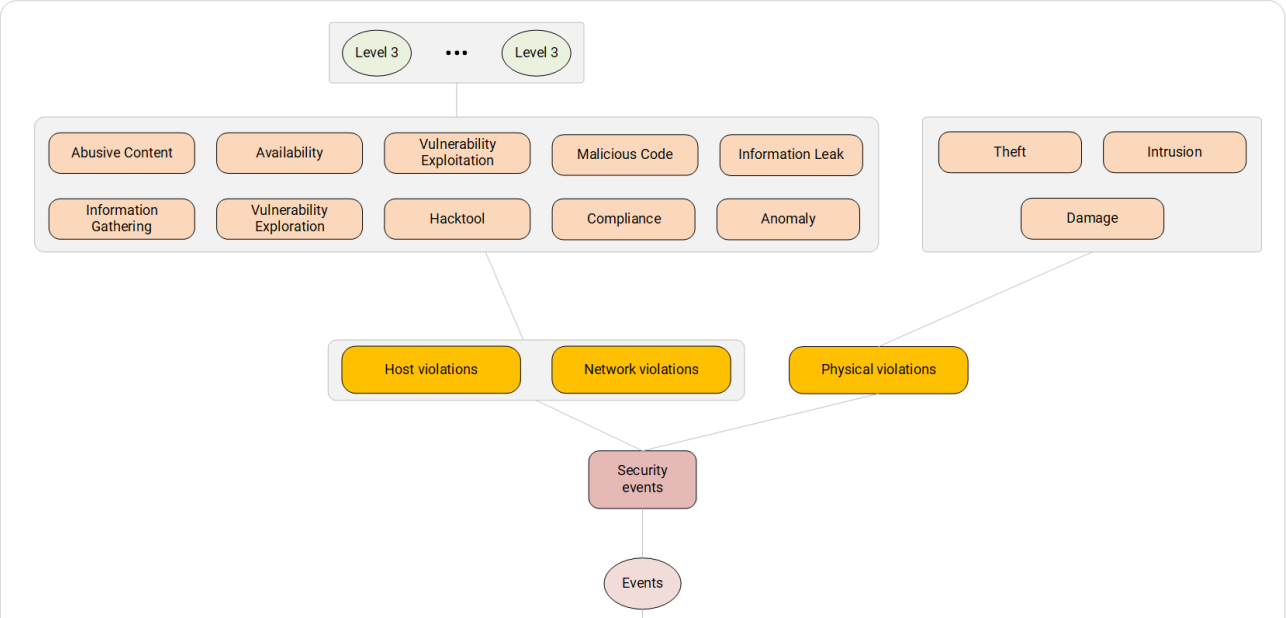

Рисунок 38 – Система категоризации ИБ-событий

Теперь на основании вышеприведенного анализа возможно сделать вывод, что вся методология нормализации событий по сути состоит из следующих этапов:

– оценка события экспертом;
– определение схемы взаимодействия;

– определение категории события.

Определение четкой методологии нормализации событий необходима для формирования в дальнейшем корректных правил корреляции.

Для того чтобы правила корреляции функционировали с минимальным количеством ложных срабатываний, они должны учитывать контекст, в котором работают, т. е. учитывать постоянное изменение объекта защиты в котором функционирует SIEM-система.

Информационная инфраструктура любой компании не статичный объект – она подвержена постоянным изменениям: вводятся новые рабочие места пользователей, выводятся из эксплуатации сервера и иное оборудование, меняется адресация и маршрутизация в сетевой инфраструктуре и т.д.

Для того, чтобы своевременно получать информацию об изменениях, вносимых в защищаемый объект (инфраструктуру компании) необходимо использовать активные и пассивные способы сбора данных об объектах информатизации.

Активный сбор данных реализуется встроенными в SIEM механизмами интеграции со сканерами безопасности и выгрузкой данных из различных источников, например, баз данных.

Пассивный сбор предполагает анализ событий, проходящих через SIEM, путем создания отдельных правил, в рамках которых при появлении нужных событий (создание пользователя, удаление софта, передача файла и т.д.) данные из этих событий учитываются при формировании новых правил корреляции.

Схематично изменение модели активов с течением времени представлено на рисунке 39.

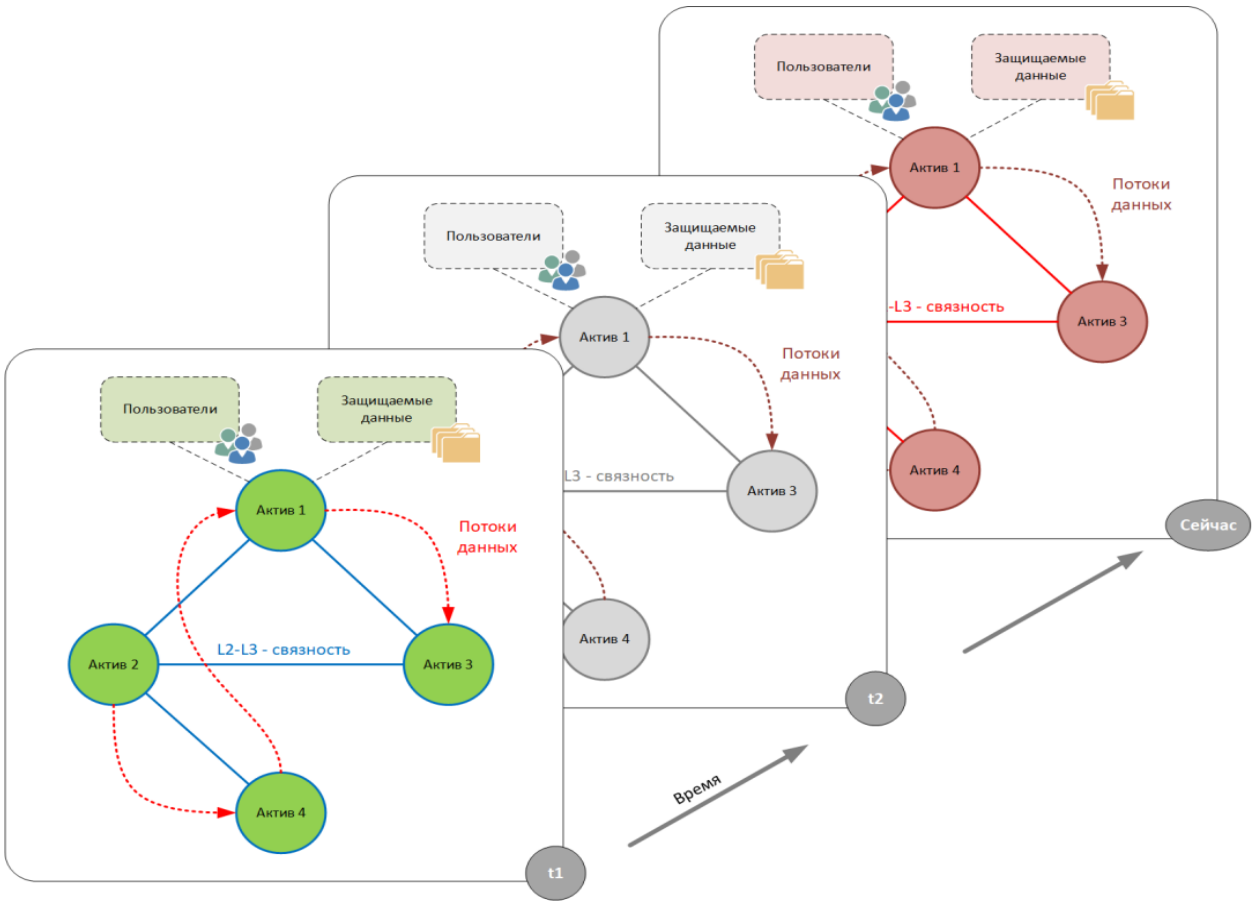

Рисунок 39 – Изменение модели активов локальной сети во времени

На заключительном этапе разработки предустановленных и корректно работающих правил корреляции необходимо в процессе подготовки к внедрению сформировать своего рода соглашение о срабатываниях – определиться, какой набор, соотношение или периодичность событий в инфраструктуре можно считать инцидентом информационной безопасности.

Для начала необходимо определить «условия агрегации инцидентов и отключения правила в случае большого количества ложноположительных срабатываний.

Механизм агрегации инцидентов позволит не создавать миллионы одинаковых инцидентов, а добавлять новые инциденты к уже существующему, при условии их идентичности.

В крайних случаях, когда даже агрегация инцидентов дает значительную нагрузку, рекомендуется настроить автоматическое отключение правила

корреляции при превышении заданного количества срабатываний в единицу времени (минута, час, сутки)» [13].

Далее необходимо определить правила формирования степени важности и значимости инцидента.

Для этого рекомендуется выработать формулу расчета, учитывающую критичность области, в которой работает правило, важность активов и учетных записей пользователей, участвующих в инциденте, повторяемость определенного инцидента.

Процедура разработки правил реагирования SIEM-системы на события и инциденты ИБ в локальной сети организации представляет собой следующую последовательность действий:

- воспроизведение действий в локальной сети, квалифицируемых как инцидент ИБ, с целью имитации действий злоумышленника;
- поиск в логах событий сведений об указанных действиях;
- определение уникальных атрибутов в программном коде, позволяющих однозначно идентифицировать данное событие безопасности;
- создание соответствующего правила корреляции в редакторе правил SIEM-системы на основе уникальных атрибутов события;
- повторение имитации рассматриваемых действий с целью проверки работоспособности правила корреляции.

Схема алгоритма создания правила представлена на рисунке 40.

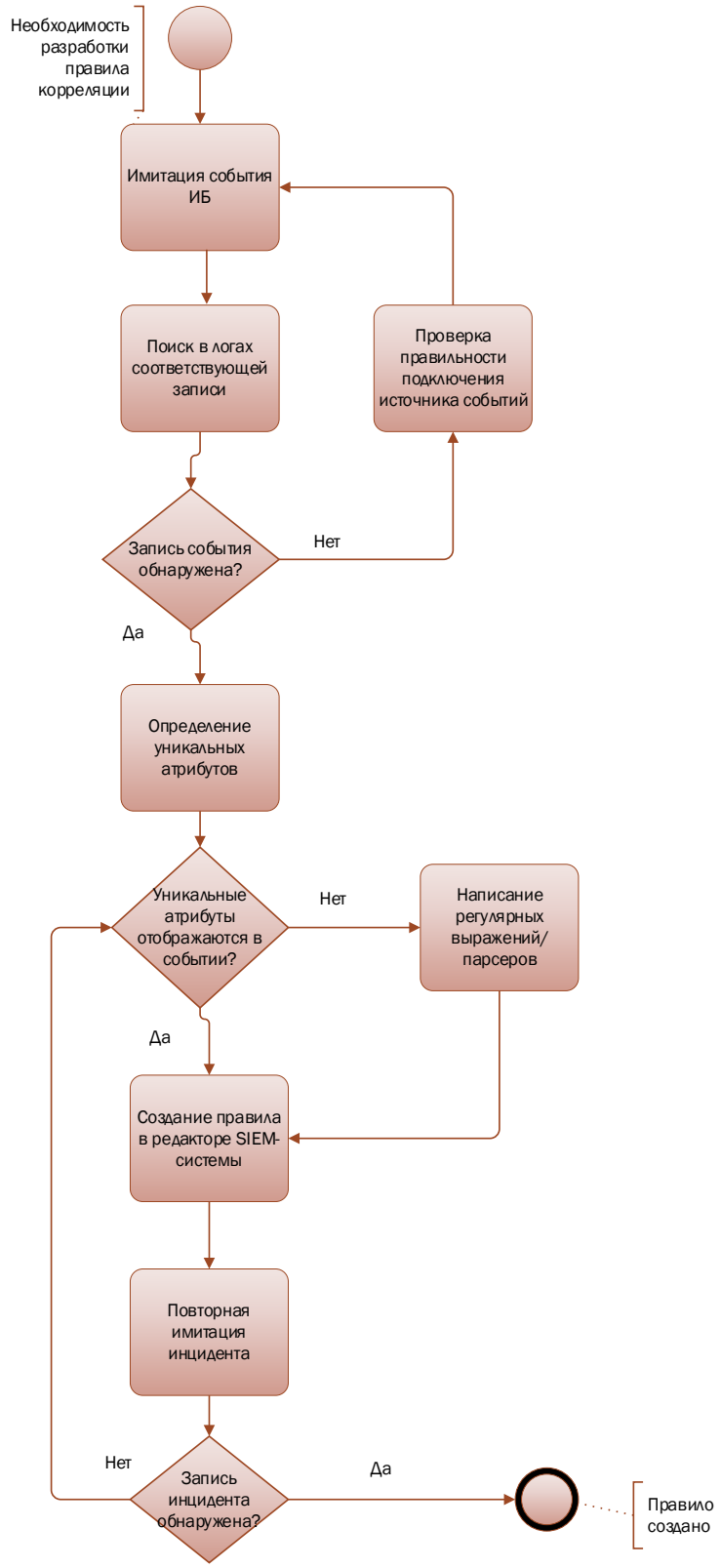

Рисунок 40 – Алгоритм разработки правила корреляции

Соблюдение вышеописанных правил позволит приблизиться к формированию правил корреляции «из коробки», что, в свою очередь,

сократит время на внедрение SIEM-системы и обеспечит её минимальное функционирование в кратчайший срок.

3.4 Сложности при эксплуатации SIEM-систем

SIEM-система сложна в эксплуатации. Необходимо заранее еще на этапе планирования предусмотреть бюджет на обучение специалистов работе в указанной системе или даже создание целого структурного подразделения, которое будет заниматься техническим сопровождением. Недопустимо привлекать работников указанных подразделений (групп/отделов) к решению других задач, пусть даже лежащих в плоскости обеспечения информационной безопасности.

В настоящее время сложилась неприемлемая тенденция включать в обязанности единственного штатного системного администратора или «безопасника» дополнительно к их должностному функционалу еще и вопросы обеспечения технического сопровождения внедренной SIEM-системы.

Данной проблеме при внедрении SIEM-систем посвящена статья автора настоящего исследования, опубликованная в научном издании «Тенденции развития науки и образования» в 2023 году.

Для успешной и правильной эксплуатации SIEM-системы выделяются следующие функциональные роли персонала:

- администратор;
- оператор;
- аналитик.

Диаграмма вариантов использования приведена на рисунке 41.

Рисунок 41 – Диаграмма вариантов использования

«Как показывает практический опыт, при эксплуатации SIEM-систем существуют два основных направления деятельности:

– Непосредственно эксплуатация и развитие;

– Мониторинг и работа в консоли управления системой.

Первое направление включает в себя поддержание в работоспособном состоянии самой SIEM, общение с техподдержкой, создание и развитие существующих инструментов для сбора логов и правил корреляции, их тестирование и ввод в эксплуатацию, написание документации по работе с данными правилами и сценариями.

Второе направление подразумевает добавление в задачи мониторинга новых активов, реагирование на события, анализ логов через средства визуализации, настройку новых средств визуализации и формирование запросов на написание новых правил корреляции.

Важно понимать, что заниматься данными направлениями должны разные специалисты, совмещение может снизить результативность работы

сотрудников. Совмещение обеих ролей одним человеком может привести к потере эффективности использования всей SIEM-системы в целом» [9].

3.5 Требования государственных регуляторов к SIEM

Если организация является субъектом КИИ, согласно Федерального закона № 187 от 26.07.2017 «Об обеспечении безопасности критической информационной инфраструктуры Российской Федерации», то для выполнения требований действующего законодательства необходимо, чтобы внедряемая SIEM-система была не только разработана отечественным производителем, но еще и была сертифицирована ФСТЭК России по требованиям безопасности информации [19]. В настоящее время не все SIEM-системы отечественных вендоров, а также не все версии ранее сертифицированных продуктов имеют действующие сертификаты соответствия ФСТЭК России. Еще одним требованием для субъектов КИИ при внедрении SIEM-систем является возможность подключения к инфраструктуре Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) в автоматическом режиме для передачи сведений об инцидентах информационной безопасности и результатах их расследований в Национальный координационный центр по компьютерным инцидентам (НКЦКИ) с минимальным участием человека.

Схема взаимодействия субъекта КИИ с Ведомственным центром ГосСОПКА представлена на рисунке 42.

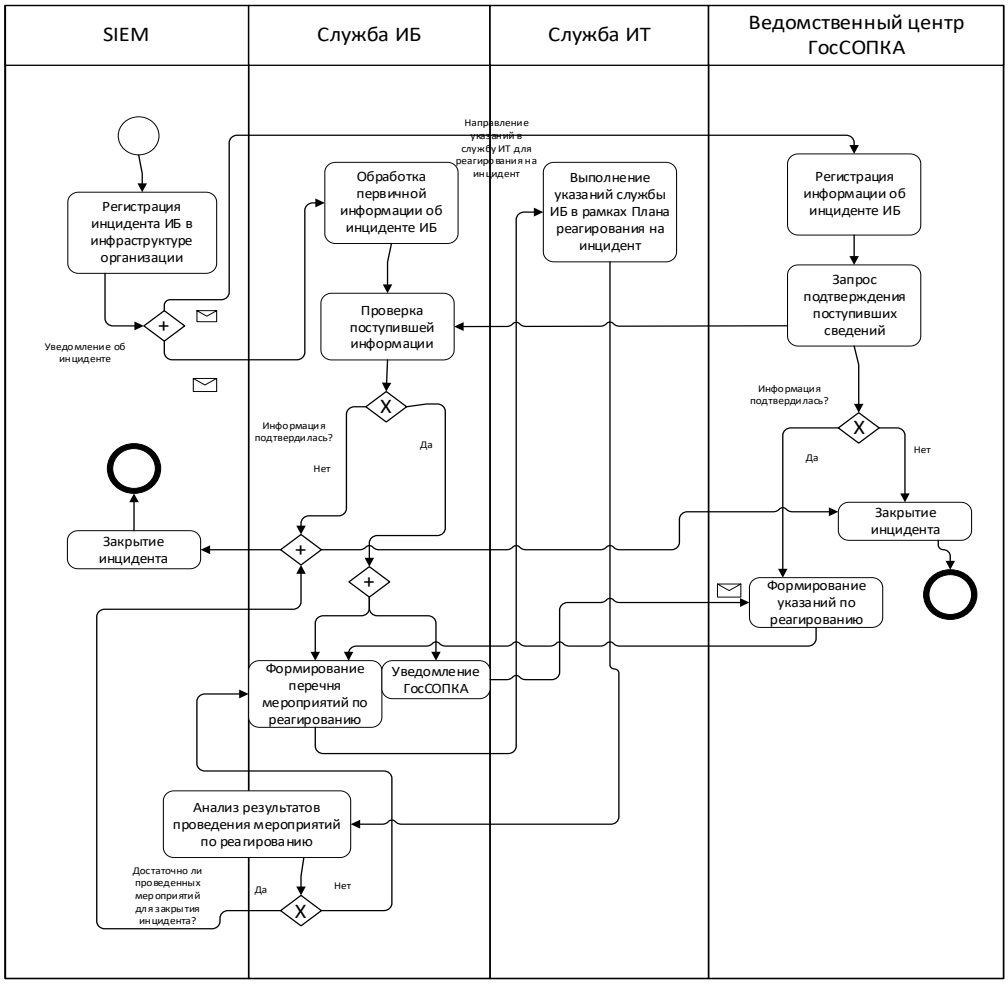

Рисунок 42 – Схема взаимодействия субъекта КИИ
с Ведомственным центром ГосСОПКА

Данный сервис также позволяет увеличить скорость реагирования на зафиксированные инциденты ИБ, и как следствие – повысить общий уровень защищенности информационных ресурсов организации [22].

3.6 Оценка эффективности результатов внедрения SIEM

В целях проверки гипотезы исследования, заключающейся в повышении уровня защищенности информационных ресурсов и уровня ИБ в компании в целом после внедрения в её инфраструктуру SIEM-системы, произведена оценка рисков ИБ в информационной инфраструктуре до и после внедрения SIEM. Проведен сравнительный анализ полученных результатов.

Оценка рисков ИБ производится с использованием качественного

метода оценки. «Результативный показатель «уровень риска» вычисляется с учетом нескольких факторных показателей: ценности (значимости) информационного актива, вероятности реализации угрозы и степени уязвимости информационного актива, в которую включен ряд факторов.

Расчет осуществляется по следующей формуле (1):

$$УР = Ц_а * В_у * К_{уп} + \left(\frac{К_{тс}+К_{пас}+К_{орг}}{3}\right), \quad (1)$$

где УР – уровень риска информационным активам;

$Ц_а$ – ценность информационного актива;

$В_у$ - вероятность реализации угрозы;

$К_{уп}$ – коэффициент уязвимости персонала;

$К_{тс}$ – коэффициент уязвимости технических средств;

$К_{пас}$ – коэффициент уязвимости программно-аппаратных средств;

$К_{орг}$ – коэффициент уязвимости организационных мер.

Уязвимость технических, программно-аппаратных средств обработки информации определяется уровнем их защищенности. При качественном подходе не используются количественные или денежные выражения для объекта оценки. Вместо этого объекту оценки присваивается показатель, проранжированный по трехбалльной системе оценки (низкий, средний, высокий). Для сбора данных при качественной оценке рисков применяются опросы целевых групп, интервьюирование, анкетирование.

Вероятность реализации каждого вида угрозы предлагается определять методом экспертных оценок с учетом имеющейся некоторой статистики по видам угроз, затем необходимо преобразовать вероятности угроз к ежегодной частоте. Показатель вероятной частоты наступления угрозы в дальнейшем используется для расчета уровня рисков. Шкалу вероятности наступления угроз предлагается разделить на пять уровней – очень низкий, низкий, средний, высокий, очень высокий (таблица 4)» [32].

Таблица 4 – Таблица вероятности возникновения угрозы

Часто-та (Ву)	Вероятность возникновения угрозы за определенный период	Уровень вероятности
0,5	реже 1 раза в год	очень низкий уровень
1	примерно 1 раз в год	низкий уровень
2	примерно 1 раз в полгода	низкий уровень
4	примерно 1 раз в 3 месяца	средний уровень
12	примерно 1 раз в месяц	высокий уровень
52	примерно 1 раз в неделю	высокий уровень
365	ежедневно	очень высокий уровень

Предполагаем, что вероятность реализации угрозы в выбранной организации имеет средний уровень, то есть вероятность возникновения угрозы (например, утечки информации) примерно 1 раз в 3 месяца.

«Для определения ценности информационного актива каждой категории имеющихся в наличии активов присваивается определенное весовое значение для определения уровня значимости с точки зрения участия в деятельности компании. Таким способом можно, например, определить коэффициент ценности различных активов в зависимости от обрабатываемых ими категорий информации (таблица 5)» [8].

Таблица 5 – Таблица ценности информационных активов

Категория информации	Открытая информация	Конфиденциальная информация			
		Управленческая	Техническая	Финансовая	Персональные данные
Коэффициент критичности	1	1,3	1,3	1,2	1,4

Оценка уровня уязвимости персонала, уязвимости технических средств обработки информации, уязвимости программно-аппаратных средств обработки информации и уязвимости организационно-режимных мер

осуществляется по результатам анкетирования.

С помощью балльной системы оценки определяется, по мнению экспертов, уровень защищенности анализируемых средств обработки информации (низкий, средний, высокий). Каждому уровню соответствует определенный коэффициент риска (таблицы 6, 7, 8, 9).

Таблица 6 – Уровень надежности и коэффициент уязвимости персонала

Уровень защищенности	Коэффициент уязвимости
Высокий (надежный)	0,2
Средний (не совсем надежный)	0,4
Низкий (не надежный)	0,6

Таблица 7 – Уровень защищенности и коэффициент уязвимости технических средств обработки информации

Уровень защищенности	Коэффициент уязвимости
Высокий	0,1
Средний	0,25
Низкий	0,4

Таблица 8 – Уровень защищенности и коэффициент уязвимости программно-аппаратных средств обработки информации

Уровень защищенности	Коэффициент уязвимости
Высокий	0,1
Средний	0,25
Низкий	0,4

Таблица 9 – Уровень защищенности и коэффициент уязвимости организационно-режимных мер

Уровень защищенности	Коэффициент уязвимости
Высокий	0,1
Средний	0,25
Низкий	0,4

По результатам проведения качественного метода оценки рисков информационной безопасности без использования SIEM-системы выявлено, что вероятность реализации угрозы безопасности информации имеет средний уровень, показатель надежности персонала имеет средний уровень, организационно-режимные меры имеют высокий уровень надежности, технические средства обработки информации и программно-аппаратных средств обработки информации имеют низкий и средний уровень защищённости соответственно.

Таким образом, для расчета уровня риска информационным ресурсам организации без SIEM-системы определены следующие коэффициенты (таблица 10):

Таблица 10 – Коэффициенты уязвимости

	$Ц_а$	$В_у$	$К_{уп}$	$К_{тс}$	$К_{пас}$	$К_{орг}$
Показатель	1,2	4	0,4	0,4	0,25	0,1

Уровень риска информационным активам предприятия без SIEM-системы ($УР_{без\ SIEM}$) будет равен (2):

$$УР_{без\ SIEM} = Ц_а * В_у * К_{уп} + \left(\frac{К_{тс}+К_{пас}+К_{орг}}{3}\right) \quad (2)$$

$$УР_{без\ SIEM} = 1{,}2 * 4 * 0{,}4 + \left(\frac{0{,}4 + 0{,}25 + 0{,}1}{3}\right) = 2{,}17$$

Главной проблемой организации была низкая скорость обработки поступающей информации и возможные риски пропустить эксплуатацию уязвимости из-за низкого уровня защищенности технических средств, среднего уровня программно-аппаратных средств обработки информации, а также низкого уровня надежности персонала.

После внедрения SIEM-системы в информационную инфраструктуру предприятия данные показатели изменились в соответствии со значениями, указанными в таблице 11.

Таблица 11 – Коэффициенты уязвимости

	$Ц_а$	$В_у$	$К_{уп}$	$К_{тс}$	$К_{пас}$	$К_{орг}$
Показатель	1,2	4	0,2	0,25	0,1	0,1

Уровень риска информационным активам предприятия при использовании SIEM-системы ($УР_{с\ SIEM}$) стал равен:

$$УР_{с\ SIEM} = Ц_а * В_у * К_{уп} + \left(\frac{К_{тс} + К_{пас} + К_{орг}}{3}\right) \quad (3)$$

$$УР_{с\ SIEM} = 1{,}2 * 4 * 0{,}2 + \left(\frac{0{,}25 + 0{,}1 + 0{,}1}{3}\right) = 1{,}11$$

По результатам проведенной оценки уровень риска информационным активам в инфраструктуре рассматриваемой организации при использовании SIEM-системы составляет 1,11. Полученное значение почти в 2 раза ниже уровня рисков без использования SIEM-системы. Внедрение программно-аппаратных средств SIEM-системы увеличивает скорость и точность

обработки информации, снижает риск утечки информации, позволяет ИТ-персоналу в кратчайшие сроки реагировать на возникающие инциденты ИБ. SIEM-система существенно облегчает работу по администрированию и управлению безопасностью организации за счет сохранения информации об инциденте, возможности определения ответственного за обработку конкретного инцидента, а также сроков обработки инцидента. В свою очередь, собранные и обработанные статистические данные позволяют оценить эффективность функционирования как отдельных средств защиты информации, так и системы безопасности в целом.

Регулярное повышение квалификации ИТ-персонала способствует эффективному использованию SIEM-системы в инфраструктуре предприятия, одновременно снижая риски информационным активам.

Выводы по главе 3

В данной главе по результатам экспериментальной апробации были определены подходы для эффективного использования SIEM-системы в качестве инструмента управления информационной безопасностью организации.

С помощью качественного метода оценки рисков сделаны выводы об эффективности использования SIEM-технологии для совершенствования методов и средств управления информационной безопасностью и повышения общего уровня защищенности информационных ресурсов.

Заключение

В последнее время процессы глобализации информационного пространства оказываются столь значительными, что захватывают разнообразные ответственные сферы современной цивилизации, и это ставит острые вопросы по обеспечению безопасности инфраструктуры компьютерных сетей. При этом темпы экспансии диктуются по большей части соображениями мировой конкурентной борьбы, захвата мировых рынков и достижения выгодного положения на конкурентном пространстве для извлечения максимальной прибыли. В то же время недостаточно внимания уделяется проблемам уязвимости инфраструктуры компьютерной сети [4].

Упомянутая проблема уязвимости инфраструктуры компьютерной сети для нашей страны приобретает особое значение в силу того, что со стороны западных стран в отношении нашей страны вводятся немотивированные ограничения и, более того, сохраняются риски блокирования глобальных информационных ресурсов.

Несанкционированный доступ к информационным ресурсам становится все более распространенным, а сектор по обеспечению безопасности компьютерных сетей по многим позициям не соответствует уровню задач безопасности.

В связи с этим актуализируются вопросы широкого круга задач безопасности компьютерных сетей, в том числе изучения тенденций проведения атак на компьютерные системы, включая вопросы анализа характера основных угроз, методов их выявления и защиты объектов сетевой инфраструктуры от сетевых атак.

В настоящем проекте были исследованы методы и средства обеспечения информационной безопасности на основе SIEM-технологии в действующей ИТ-инфраструктуре компании.

Рост удаленной работы по всему миру предоставляет злоумышленникам новые ресурсы для проведения атак на различные отрасли. Это делает

правильно настроенные решения SIEM, обеспечивающие полную видимость сети, более важными, чем когда-либо. Тем не менее, это также означает, что система SIEM будет заполнена большим количеством информации, большим количеством ложных предупреждений и большим количеством потенциальных угроз. Для многих компаний способность идти в ногу с потоком информации, собираемой SIEM каждый день, означала бы наем дополнительных аналитиков безопасности, которые ежедневно просматривали бы тысячи записей в журнале событий. Использование инструментов, которые работают вместе с программным обеспечением SIEM, является лучшим решением.

Как и многие бизнес-затраты, безопасность - это инвестиции, которые со временем приносят дополнительную пользу. В то время как некоторые инструменты и продукты, используемые в ИТ и безопасности, быстро устаревают, SIEM - это решение, которое растет вместе с организацией и часто приобретает дополнительную ценность с течением времени. Качественная SIEM-система предназначена для масштабирования для растущих компаний. Он также может использовать ИИ и продолжать улучшать процессы по мере возникновения новых угроз.

SIEM со временем повышает свою ценность благодаря возможности непрерывной автоматизации задач. Хотя автоматизированные задачи позволяют организациям инвестировать в SIEM без первоначальных затрат на наем дополнительных аналитиков по безопасности, они также способствуют будущему росту без затрат на привлечение дополнительного персонала по безопасности.

Обычно основная причина, по которой компании инвестируют в SIEM, заключается в том, чтобы избежать затрат, связанных с нарушением безопасности. Поскольку системы SIEM предназначены для непрерывного приема и обработки данных, инвестиции продолжают окупаться. По мере развития технологий растут и решения SIEM, которые обеспечивают непрерывное решение, обеспечивающее одинаковый уровень безопасности.

Проблемы в основном могут быть подразделены на следующие категории:

- организационные - недостатки в планировании проекта, бюджета, времени;
- технические - системы SIEM очень сложны в построении, соответственно, во внедрении. Приходится иногда менять аппаратное обеспечение, чтобы технические характеристики соответствовали минимальным требованиям.
- кадровые - мало квалифицированных специалистов;
- финансовые - внедрение обходится дорого.

Внедрение системы было рассмотрено на примере корпорации «Росатом». В рамках проведенного исследования были сформированы правила для оптимизации бизнес-процессов в части внедрения в информационную инфраструктуру рассматриваемой организации программного обеспечения, позволяющего в обозримом будущем уменьшить затраты на обеспечение информационной безопасности, снизить риски реализации угроз безопасности информации и подготовить высококвалифицированный персонал, способный решать задачи по защите информации от актуальных угроз в соответствии с современными тенденциями. Разработанные предложения по оптимизации бизнес-процессов были проверены на практике и доказали свою эффективность.

Гипотеза исследования была подтверждена.

Настоящая работа может представлять практический интерес для руководителей организаций, а также руководителей ИТ- и ИБ-служб, стремящихся оптимизировать бизнес-процессы организации и построить эффективную систему защиты критически важных информационных активов своих организаций и предприятий.

Список используемой литературы и используемых источников

1. Актуальные киберугрозы: итоги 2021 года. [Электронный ресурс]. URL: http://ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021(дата обращения: 25.03.2023).

2. Арламов Е.А., Панасюк Г.О. Анализ состояния информационной безопасности в современной России // Экономика и менеджмент инновационных технологий. 2020. № 12 [Электронный ресурс]. URL: http://ekonomika.snauka.ru/2016/12/13291 (дата обращения: 25.03.2023).

3. Гуфан К.Ю, Проскурин Д.Ю. Анализ возможностей создания скрытых каналов передачи информации из защищаемых сетей// Технические науки. 2019. №1.

4. Доктрина информационной безопасности [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения: 20.02.2024).

5. Домарев В.В. Защита информации и безопасность компьютерных систем. К.: изд-во «Диа-Софт». 2020. 480 с.

6. Дудкина И. А. Технологии и методы обеспечения комплексной защиты информации / И. А. Дудкина// Молодой ученый. 2020. № 16 (120). С. 37-39. [Электронный ресурс]. URL: https://moluch.ru/archive/120/33148/ (дата обращения: 25.06.2023).

7. Жук А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. 2-е изд. М.: ИЦ РИОР: НИЦ ИНФРА-М, 2019. 392 с.

8. Казыханов А.А., Попов К.Г. Обеспечение безопасности информационных систем / В сборнике: Актуальные проблемы социального, экономического и информационного развития современного общества Всероссийская научно-практическая конференция, Башкирский государственный университет. 2019. с. 71-74.

9. Казьмин Д.А. Проблемы внедрения SIEM-систем // Тенденции

развития науки и образования. 2023. № 102-5. С. 19-22. URL: https://www.elibrary.ru/item.asp?id=54811197 (дата обращения: 10.02.2024).

10. Любохинец С. Ответ компании Cisco на современные угрозы безопасности // VIII-й Международный Security Innovation Forum 2018. СпБ: 27 ноября 2018. с. 29-33.

11. Макеенко Н.И., Новожилов И.О., Корабейников Д.Н. Система обнаружения вторжений // Современные научные исследования и инновации. 2017. № 5 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2017/05/82889 (дата обращения: 03.07.2023).

12. Михеева О.И., Гатчин Ю.А., Савков С.В., Хамматова Р.М., Ныркова А.П. Методы поиска аномальных активностей веб-приложений // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 2. С. 233–242.

13. Обзор мирового и российского рынка SIEM-систем [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem (дата обращения: 20.02.2024).

14. Ортыков А. У. Обеспечение информационной безопасности предприятия от несанкционированного доступа // Технические науки: традиции и инновации: материалы III Междунар. науч. конф. (г. Казань, март 2018 г.). Казань. Молодой ученый. 2018. С. 22-24.

15. Пинженин В. Безопасность сети на основе 802.1 x и SFlow, «идеальная и недостижимая» / / Сетевые решения. 2019. №1. С. 38-42.

16. Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений» [Электронный ресурс]. URL: https://ivo.garant.ru/#/document/71876120/paragraph/1/doclist/3045/1/0/0/Об%20утверждении%20Правил%20категорирования%20объектов%20КИИ%20РФ,%20а%20также%20перечня%20показателей%20критериев%20значимости%20объектов%20КИИ%20РФ%20и%20их%20значений:9 (дата обращения: 20.02.2024).

17. Постановление Правительства РФ №162 от 17.02.2018 «Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ» [Электронный ресурс]. URL: https://ivo.garant.ru/#/document/71876120/paragraph/1/doclist/3045/1/0/0/Об%20утверждении%20Правил%20категорирования%20объектов%20КИИ%20РФ,%20а%20также%20перечня%20показателей%20критериев%20значимости%20объектов%20КИИ%20РФ%20и%20их%20значений:9 (дата обращения: 20.02.2024).

18. Приказ ФСТЭК от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных[Электронный ресурс]. URL: https://ivo.garant.ru/#/document/70380924/paragraph/1/doclist/3248/1/0/0/Об%20утверждении%20состава%20и%20содержания%20организационных%20и%20технических%20мер%20по%20обеспечению%20безопасности%20персональных%20данных%20при%20их%20обработке%20в%20информационных%20системах%20персональных:19 (дата обращения: 20.02.2024).

19. Приказ ФСТЭК России №229 от 11.12.2017 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ» [Электронный ресурс]. URL: https://ivo.garant.ru/#/document/71848406/paragraph/1/doclist/3145/1/0/0/6.%20Приказ%20ФСТЭК%20России%20№229%20от%2011.12.2017%20Об%20утверждении%20формы%20акта%20проверки,%20составляемого%20по%20итогам%20проведения%20госконтроля%20в%20области%20обеспечения%20безопасности%20значимых%20объектов%20КИИ%20РФ.:11 (дата обращения: 20.02.2024).

20. Приказ ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования» [Электронный ресурс]. URL: https://ivo.garant.ru/#/document/71886248/paragraph/1/doclist/3191/1/0/0/O

б%20утверждении%20Требований%20к%20созданию%20систем%20безопасности%20значимых%20объектов%20КИИ%20РФ%20и%20обеспечению%20их%20функционирования:13 (дата обращения: 20.02.2024).

21. Приказ ФСТЭК России №236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» [Электронный ресурс]. URL: https://ivo.garant.ru/#/document/71924214/paragraph/1/doclist/3211/1/0/0/Об%20утверждении%20формы%20направления%20сведений%20о%20результатах%20присвоения%20объекту%20КИИ%20одной%20из%20категорий%20значимости%20либо%20об%20отсутствии%20необходимости%20присвоения%20ему%20одной%20из%20таких%20категорий:15 (дата обращения: 20.02.2024).

22. Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ» [Электронный ресурс]. URL: https://ivo.garant.ru/#/document/71901880/paragraph/1/doclist/3234/1/0/0/Об%20утверждении%20Требований%20по%20обеспечению%20безопасности%20значимых%20объектов%20КИИ%20РФ:17 (дата обращения: 20.02.2024).

23. Саяркин Л. А., Зайцева А.А., Лапин С. П., Домбровский Я. А. Программно-аппаратные средства защиты автоматизированных систем от несанкционированного доступа // Молодой ученый. 2017. № 13 (147). С. 19-22.

24. Сила цифры. Как российская атомная отрасль прокладывает курс на цифровизацию [Электронный ресурс]. URL: https://ria.ru/20221216/nuclear-digit-1836689061.html (дата обращения: 20.02.2024).

25. Фахрутдинова И.Р., Трофимова Н.О. Информационная безопасность на предприятии // Современные научные исследования и инновации. 2016. № 2 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2016/02/64549 (дата обращения: 20.02.2024).

26. Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности

критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. URL: https://ivo.garant.ru/#/document/71730198/paragraph/1/doclist/2838/1/0/0/187%20ap:1 (дата обращения: 20.02.2024).

27. Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации». [Электронный ресурс]. URL: https://ivo.garant.ru/#/document/12148555/paragraph/3471/doclist/3018/1/0/0/от%2027%20июля%202006%20г.%20№149-ФЗ%20Об%20информации,%20информационных%20технологиях%20и%20о%20защите%20информации.:7 (дата обращения: 20.02.2024).

28. Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» [Электронный ресурс]. URL: https://ivo.garant.ru/#/document/12148567/paragraph/24880/doclist/2993/1/0/0/152%20фз:5 (дата обращения: 20.02.2024).

29. Arbanas, K., Hrustek, N.Z. Key success factors of information systems security// Journal of Information and Organizational Sciences. 43(2), pp.131-144.

30. CNEWS Исследование «Серчинформ»: средства мониторинга угроз не внедряют из-за кадрового голода [Электронный ресурс]. URL: https://safe.cnews.ru/news/line/2022-09-12_issledovanie_serchinform (дата обращения: 20.02.2024).

31. Koo J., Kang G., Kim Y.G. Security and privacy in big data life cycle: A survey and open challenges// Sustainability (Switzerland).

32. MaxPatrol SIEM Система мониторинга событий ИБ и выявления инцидентов в реальном времени [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/products/mpsiem/ (дата обращения: 10.05.2023)

33. Rabadi, D., Teo, S.G. Advanced Windows Methods on Malware Detection and Classification // ACM International Conference Proceeding Series.

34. Tang, D., Dai, R., Tang, L., Li, X. Low-rate DoS attack detection based on two-step cluster analysis and UTR analysis// Human-centric Computing and Information Sciences.