МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт Систем Управления и Информационных Технологии
Кафедра «Системы информационной безопасности»

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой _____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Разработка и реализация концепции «Умный офис»
_____

Специальность Системы Информационной Безопасности_____

Выполнил(а) Хамраева Зумрад Тургановна_____ Группа СИБ-16-2___
(Ф.И.О.)

Научный руководитель д.т.н. профессор Маркосян Мгер Вардгесович
(ученая степень, звание, Ф.И.О.)

Консультанты:
по специальной части:
старший преподаватель Дмитриева Маргарита Валерьевна_____

_____ «_____» _____20____г.
(подпись)

по безопасности жизнедеятельности:
к.т.н. доцент Приходько Николай Георгиевич_____

_____ «_____» _____20____г.
(подпись)

Нормоконтролер: _____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

Рецензент: _Бегимбаева Енлик Ериковна_____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

Алматы 2020

Задание на выполнение дипломного проекта

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Институт Систем Управления и Информационных

Кафедра «Системы Информационной Безопасности»

Специальность «Системы Информационной Безопасности»

ЗАДАНИЕ

на выполнение дипломного проекта

Студенту Хамраевой Зумрад Тургановне
(Ф.И.О.)

Тема проекта «Разработка и реализация концепции «Умный офис»»

Утверждена приказом по университету № _____ от «___» _____2020 г.

Срок сдачи законченного проекта «____» _____ 2020 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): Исходные материалы для выполнения задания дипломного проекта –SIEM система IBM QRadar, сервер с Linux RED HAD, локальная вычислительная сеть, гипервизор, персональный компьютер с достаточными мощностями.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Цель работы –разработка и реализация концепции «Умный офис» ее внедрение, полная настройка правил. Создание скриптов для автоматизации действий сотрудников отдела по реагированию на инциденты. Также организация отдела по реагированию на особо тяжкие инциденты, описание основных действий и роле в данном отделе. Создание «одной» единой платформы для управления и реагированием на инциденты информационной безопасности. Задачами данной работы являются исследование существующих программных решений, посредством которых будет реализована данная концепция. Разработка средств администрирования.

Перечень графического материала (с точным указанием обязательных

чертежей): и архитектура подключения SIEM системы, организационная схема ролей отдела по реагированию на инциденты.

Основная рекомендуемая литература: _____

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Анализ рисков информационной безопасности	старший преподаватель Дмитриева Маргарита Валерьевна	17.02.2020 – 09.05.2020	
Безопасность жизнедеятельности	к.т.н. доцент Приходько Николай Георгиевич	17.02.2020 – 09.05.2020	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Установка ОС Linux Red Had	17.02.2020 – 20.02.2020	
Установка SIEM IBM QRadar	21.02.2020 – 28.02.2020	
Настройка SIEM системы и подключение источников	01.03.2020 – 08.03.2020	
Создание правил для автоматизации работы	09.03.2020 - 18.03.2020	
Создание скриптов для автоматизации работы	19.03.2020 – 27.03.2020	
Установка SOAR системы Resilient	28.03.2020 - 07.04.2020	
Настройка соединение между SOAR и SIEM	08.04.2020 - 18.04.2020	
Написание скриптов для SOAR системы	19.04.2020 - 30.04.2020	
Анализ рисков ИБ. БЖД	01.05.2020 - 09.05.2020	

Аннотация

Реализация концепции «Умный офис» позволит сотрудникам информационной безопасности тратить меньше времени на выполнение рутинных задач, так как данная концепция направленна на автоматизацию, действий по мониторингу и реагированию на инциденты информационной безопасности. В данном проекте описывается архитектура концепции, которая защищает сетевой и корпоративный бизнес-трафик, описывается работа и действия команды по реагированию на инцидента также разработана и внедрена программно-техническая структура.

Abstract

The implementation of the "Smart office" concept will allow information security employees to spend less time performing routine tasks, since this concept is aimed at automating, monitoring and responding to information security incidents. This project describes the architecture of the concept that protects network and corporate business traffic, describes the work and actions of the incident response team, and developed a software and technical structure.

Аңдатпа

"Ақылды кеңсе" тұжырымдамасын іске асыру ақпараттық қауіпсіздік қызметкерлеріне рутиндік міндеттерді орындауға аз уақыт жұмсауға мүмкіндік береді, өйткені бұл тұжырымдама автоматтандыруға, мониторинг бойынша іс-қимылдарға және ақпараттық қауіпсіздік инциденттеріне ден қоюға бағытталған. Бұл жобада желілік және корпоративтік бизнес-трафикті қорғайтын тұжырымдама архитектурасы сипатталады, инциденттерге әрекет ету бойынша команданың жұмысы мен әрекеттері сипатталады және бағдарламалық-техникалық құрылым әзірленді.

Содержание

Введение

Согласно лабораторией Pandalabs за последнее время количество инцидентов ИБ возросло десятки раз, при этом это уже не простые вирусы, а более опасные атаки, приводящие к остановке работы всего предприятия, таким образом получаем огромное множество параметров, которые необходимо отслеживать

Для автоматизации управления процесса управления инцидентами, я предлагаю разработать концепцию «Умный офис» которая в последующем будет внедрена в Компанию и будет использоваться для анализа инцидентов ИБ.

Умный офис – это глубоко интегрированная с другими процессами система. Разумеется, большинство этапов можно сделать локальными, но тогда серьезно снизится эффективность автоматизации. Данная концепция поможет защитить вашу сеть, сети клиентов и трафик, связанный с деловой активностью. Организуя разумный баланс технологий, процессов и людских ресурсов «Умный офис» предоставляет возможность непрерывного мониторинга сетей с отслеживанием инцидентов в сфере безопасности и быстрого принятия ответных мер при возникновении угроз.

Основным преимуществом использования концепции «Умный офис» является время реагирования. Вирусы в сети способны распространяться в течение минут или даже секунд, выводят их из строя или замедляют передачу трафика до минимальных скоростей. Для выявления таких атак и их отражения еще до того, как они смогут причинить существенный ущерб, важна каждая секунда.

На практике выполняется постоянный мониторинг состояния безопасности сети и мгновенно реагирует на возникновение критических ситуаций в сфере безопасности проблемы и появление новых уязвимостей.

В этом дипломной работе обосновывается необходимость создания методики «Умный офис», описана его роль, функции и преимущества. Рассмотрены этапы построения архитектуры и меры по обработке инцидентов в сфере безопасности.

1 Теоретическая часть

1.1 Концепция «Умный офис»

1.1.1 Необходимость создания «Умного офиса»

Многие области управления центрами обработки данных уже используют автоматизацию, что позволяет ИТ-отделам значительно расширить свои возможности. К сожалению, управление инцидентами в ИТ - это один из аспектов управления центрами обработки данных, который остался позади. По мере роста и сложности центров обработки данных растет число ежедневных ИТ-предупреждений, требующих внимания. Тем не менее, способы, которыми ИТ-команды управляют и реагируют на эти предупреждения, не поддерживаются. Управление оповещениями по-прежнему очень ручная, медленная и повторяющаяся работа.

Суть в том, что инцидент должен быть решен быстро. В противном случае может быть нанесен долгосрочный ущерб доходам компании, ее инфраструктуре и так далее.

От момента свершения атаки до реагирования на нее и устранения последствий (Атака -> Компрометация -> Утечка данных -> Обнаружение инцидента -> Реагирование и Устранение) могут пройти дни, недели и даже месяцы. Чаще всего это происходит уже после того, как злоумышленник получил доступ к нужным ему данным. На рисунке 1 показана в процентном отношении, стадии реагирования на инциденты информационной безопасности.

Рисунок 1 – Статистика по расследования инцидентов

Для ускорения работы реагирования на инциденты ИБ я предлагаю концепцию «Умный офис». Она представляет собой интеллектуальную

экосистему, которая опирается на ряд подключенных устройств, которые, в общем, отслеживают, контролируют и управляют различными операциями и условиями труда.

Благодаря данной концепции, возможно в полном объеме удовлетворить потребности клиентов в сфере обеспечения безопасности и внедрить архитектуры и процессы, защищающие их организации. Одним словом, при активном участии клиентов вводятся программы, процедуры и инструменты обеспечения безопасности и применяются профессиональные навыки специалистов, которые необходимы сегодня для надлежащего контроля за состоянием сетей.

1.1.2 Общие задачи и функции «Умного офиса»

Концепция «Умного офиса» обеспечивает точное выявление, анализ, защиту, расследование и распространение информации о возможных инцидентах безопасности. На рисунке 2 продемонстрированы основные функции, «Умного офиса» при реагировании на инциденты.

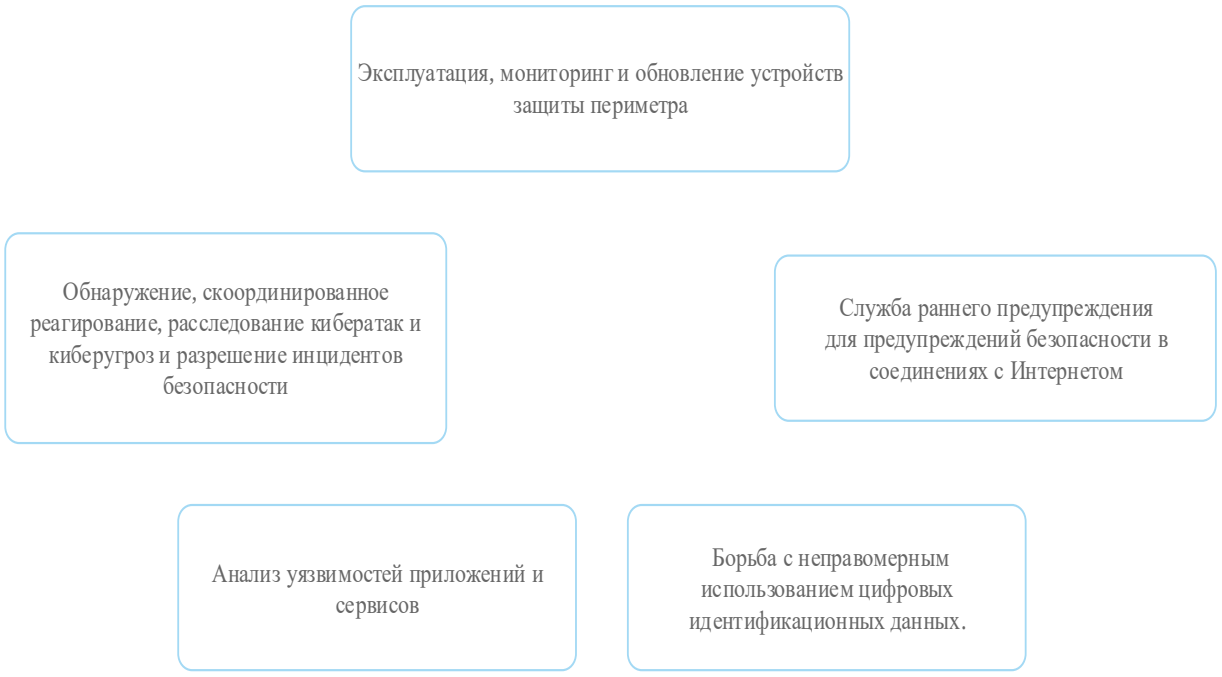

Рисунок 2 – Функции «Умный офис»

Для обеспечения высокого уровня защиты концепция выполняет решение следующих задач [2]:

а) обнаружение активов и управление – это включает в себя получение высокой осведомленности обо всех инструментах, программном обеспечении, оборудовании и технологиях, используемых в «Умном офисе». Он также направлен на то, чтобы все активы работали правильно и регулярно обновлялись;

б) непрерывный поведенческий мониторинг – все системы исследуются

24/7. Это позволяет «Умному офису» придавать равный вес профилактическим и реактивным мерам, поскольку любые нарушения в работе обнаруживаются мгновенно. Поведенческие модели используются для обучения систем сбора данных тому, что считается подозрительной деятельностью, и могут использоваться для корректировки информации, которая может регистрироваться как срабатывания;

в) ведение журналов активности. Все коммуникации и действия в рамках организации должны регистрироваться. Это позволяет членам команды отследить или точно определить предыдущие действия, которые могли привести к нарушению;

г) ранжирование по степени серьезности оповещения. Одним из элементов управления уязвимостями является обеспечение того, чтобы в первую очередь обрабатывались самые серьезные или неотложные оповещения. Это является частью работы «Умного офиса» по ранжированию угроз кибербезопасности с точки зрения потенциального ущерба;

д) развитие обороны. Команда «Умного офиса» должна создать план реагирования на инциденты (IRP), чтобы помочь защитить системы от атак. Кроме того, они несут ответственность за корректировку плана по мере необходимости при получении новой информации;

е) восстановление после инцидента. Помимо предотвращения и предотвращения возникновения утечек данных, «Умный офис» также отвечает за восстановление данных, которые были скомпрометированы. Это может включать перенастройку, обновление или резервное копирование систем;

ж) поддержание соответствия – все члены команды в «Умном офисе» должны соблюдать нормативные стандарты соответствия при выполнении бизнес-планов. Как правило, один член команды отвечает за обучение и обеспечение соблюдения.

1.1.3 Преимущества «Умного офиса»

Задачи и функции, решаемые «Умным офисом», обеспечивают целый ряд преимуществ:

а) **эффективная реакция на инциденты в сфере информационной безопасности.** В течение использования концепции «Умного офиса» осуществляется переход от реактивного подхода к профилактическим мерам. Вместо акцента на ответных мерах, реализуемых при угрозе безопасности, вводится продуманный процесс, который предоставляет возможность быстро и эффективно перейти к обнаружению, локализации и уничтожению угрозы. Помимо этого, достигается возможность ориентировать экспертов по безопасности не на поиск решений при каждой возникающей угрозе, а на разработку сетевых стратегий. А также, появляется возможность предлагать защиту от злоумышленников, атакующих сети или web-сайты клиентов;

б) **экономия энергии.** Автоматически регулируя освещение и отопление в вашем офисе, вы сможете более эффективно использовать свои энергоресурсы и сократить потери;

в) **снижение риска для клиентов.** С помощью «Умного офиса» можно свести к минимуму перерывы в работе сети, которые связаны с событиями в сфере информационной безопасности. «Шагая в ногу» с эволюционирующими глобальными угрозами, можно эффективнее защищать трафик клиентов от потерь и манипулирования данными и устанавливать более эффективный контроль над сервисами обеспечения безопасности;

г) **сокращение затрат.** Поскольку данная концепция в значительной мере опирается на технологии, инструменты и процедуры обеспечения безопасности, которые обеспечивают «первый уровень защиты», можно эффективно использовать всегда недостаточные ресурсы обеспечения безопасности без ущерба для качества результатов работы. Другими словами, «Умный офис» позволяет опереться на процессы и технологии, которые станут весомым подспорьем в работе, выполняемой, как правило, специалистами по безопасности. Это поможет обслуживать большее количество клиентов, не раздувая штат организации;

д) **помощь клиентам в соблюдении нормативных требований.** Во многих случаях клиенты должны соблюдать требования нормативных документов и политик, которые регламентируют использование, защиту и конфиденциальность информации. Клиенты могут использовать отчеты, генерируемые командой «Умным офисом», для помощи в соблюдении таких требований и правил таких, как Закон о прибылях и отчетности в сфере здравоохранения (HIPAA) и требования к безопасному хранению данных, действующих в сфере обращения платежных карт (PCIDSS).

1.1.4 Построение архитектуры «Умного офиса»

«Умный офис» может иметь разную архитектуру в зависимости от требований, технических навыков сотрудников, физических ресурсов и организационных моделей. Поэтому построение «Умного офиса» и его команды – это индивидуальный подход. Основные моменты, которые необходимо рассомтреть при организации концепции «Умного офиса»:

а) первым шагом в создании «Умного офиса» организации является четкое определение стратегии, которая включает в себя конкретные для бизнеса цели из различных отделов, а также вклад и поддержку со стороны руководителей. Как только стратегия будет разработана, должна быть реализована инфраструктура, необходимая для поддержки этой стратегии. Должна существовать технология сбора данных с помощью потоков данных, телеметрии, захвата пакетов, системного журнала и других методов, чтобы сотрудники могли сопоставлять и анализировать активность данных. «Умный офис» также контролирует сети и конечные точки на наличие уязвимостей, чтобы защитить конфиденциальные данные и соответствовать отраслевым или правительственным нормам;

б) определить, какие данные о безопасности следует собирать;

в) исходя из политики безопасности и условий договоров SLA нужно получать от клиентов определенные данные. Как правило, чем шире масштабы мониторинга безопасности, тем более подробны эти данные. Иными словами, возможны большие различия в характере и объеме собираемых данных, которые зависят от каждого клиента;

г) определить, по каким данным следует проводить анализ и определять корреляцию. Нецелесообразно разбираться во всем трафике, что поступает от клиента. Средства анализа и механизмы корреляции мгновенно идентифицируют потенциальные инциденты в сфере ИБ, и эти функции исключительно важны для обеспечения надлежащего качества сервисов. Можно гарантировать клиентам, что никакая конфиденциальная информация, т.е. информация, связанная с их текущей деловой активностью, не попадает в центр «Умного офиса». Это послужит дополнительным аргументом для представителей руководства организаций;

д) проанализировать соответствующие события в сфере безопасности. Когда проведен анализ и определена корреляция трафика клиента, нужно выделить инциденты в сфере безопасности из корректного трафика и обратить все свое внимание на них. Нужно выделять только инциденты, являющиеся фактическим нарушением политики безопасности каждого клиента. Например, нереально выполнить проверку каждой строки из двух миллионов syslog-сообщений, которые созданы межсетевым экраном клиента. Выделив только те строки, которые соответствуют угрозе безопасности, можно эффективно использовать дефицитные ресурсы в сфере информационных технологий;

е) привлечь экспертов по безопасности. Когда команда «Умного офиса» выделит потенциальный инцидент в сфере безопасности, в работу включаются эксперты по безопасности. В команду «Умного офиса» входят следующие роли, должности и обязанности [1]:

1) **Менеджер** – этот сотрудник отвечает за управление повседневной деятельностью его команды. Это также является частью их роли в обмене обновлениями с исполнительным персоналом организации.

2) **Ответственный за инциденты** – Этот сотрудник обрабатывает атаки или нарушения, которые успешно произошли, применяя любые методы, необходимые для уменьшения и устранения угрозы.

3) **Аналитик безопасности** – этот сотрудник просматривает предупреждения безопасности, чтобы систематизировать их по срочности или серьезности, и регулярно проводит уязвимостей.

4) **Инженер по безопасности** – Этот сотрудник разрабатывает и проектирует системы или инструменты, необходимые для эффективного обнаружения вторжений и управления уязвимостями.

ж) последний этап в построении архитектуры «Умного офиса» – формирование процесса, помогающего клиентам получать информацию о каждом инциденте в сфере безопасности и контролировать процесс его

устранения. При возникновении инцидента необходимо сгенерировать учетную карточку (Trouble Ticket) и предоставить клиентам, которых затронул этот инцидент, доступ к этой карточке в соответствии с условиями договора SLA или политикой безопасности. А также, можно составлять подробные еженедельные, ежемесячные и годовые отчеты, что позволяет дополнительно укрепить взаимоотношения с клиентами.

1.2 Реагирование на события Информационной Безопасности

Непрерывный мониторинг и анализ событий ИБ, позволяют эффективно реагировать на инциденты ИБ. И, как следствие, позволяют снижать потери и оперативно восстанавливать работоспособность ИКТ [6].

На схеме 1 ниже описан основной процесс реагирования на инцидент ИБ:

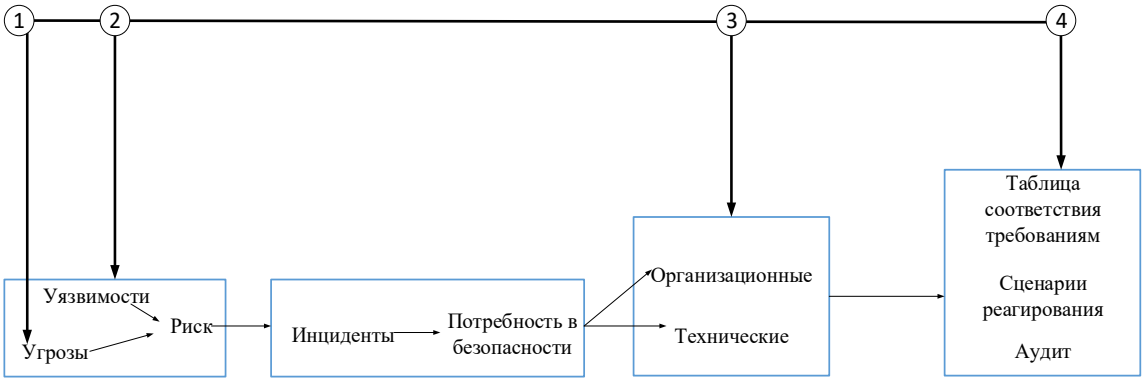

Схема 1 – Реагирование на инциденты ИБ

По схеме 1 выстраивается следующий план реагирования на инциденты:

а) обработка угроз (в реальном времени или с задержкой);

б) обработка уязвимостей и/или несоответствий (в реальном времени или с задержкой);

в) улучшение процессов и правил безопасности, осведомленность пользователей;

г) составление показателей информационной безопасности.

Реагирования 1-го и 2-го типов могут быть достигнуты в рамках имеющихся планов реагирования, запускаемых в режиме реального или отложенного времени в случае значительных или критических событий безопасности.

Третий тип реагирования направлен на улучшение СМИБ (модель PDCA, в частности, описанная в ISO/IEC 27002), которое становится возможным благодаря обратной связи на основе опыта, полученного в результате постоянного отслеживания инцидентов ИБ (измерение эффективности СМИБ).

Четвертый тип реагирования (на уровнях ГРИИБ или управления) заключается в выявлении несоответствий, которые могут перерасти в инциденты ИБ.

1.3 Действия, связанные с управлением инцидентами

На основе пост-инцидентного анализа, результатов анализа событий, пересмотра методики оценки рисков и угроз ИБ производится непрерывное совершенствование всех процессов [6].

Команда «Умного офиса» учитывает перечень инцидентов ИБ, приведенные в отчетах полученные с источников.

Разрабатывается и внедряется стратегия анализа инцидентов ИБ, позволяющая выявлять все инциденты, которые отражены в перечне критичных инцидентов ИБ.

Стратегия анализа включает в себя правила обнаружения инцидентов ИБ на основе собранных событий. Правила обнаружения создаются на основе [6]:

а) перечня и типизации инцидентов ИБ;

б) готовых правил, имеющиеся в IBM Security QRadar SIEM;

в) дополнительная установка специализированных пользовательских скриптов;

г) внутренних баз знаний, полученные из опыта пост-инцидентного анализа инцидентов ИБ;

д) инциденты ИБ, обнаруженные другими средствами обеспечивающие ИБ.

Обнаруженные инциденты ИБ категорируются, чтобы оценить их достоверность (истинный/ложноположительный, доказанный инцидент или нет) и критичность (функциональные воздействия, информационные воздействия и т.д.).

Компания устанавливает уровни критичности, связанные с критичными инцидентами ИБ, принимая во внимание оценку риска, угрозы, активы, потенциальное воздействие и их уровни критичности.

Информация об анализе всех событий и инцидентов ИБ сохраняются в течение периода времени, определенного Компанией.

1.4 Использование инструмента SIEM при построении «Умного офиса»

Основным ядром «Умного офиса» является специализированное программное обеспечение – IBM Security QRadar SIEM – система мониторинга и анализа событий ИБ (далее - SIEM).

SIEM позволяет осуществлять централизованный сбор, хранение и обработку сетевых потоков с ключевого сетевого оборудования и событий системных журналов (логов) с различных источников, позволяет осуществлять корреляцию между событиями из разных систем для выявления аномалий и наиболее важных инцидентов ИБ в общей массе событий, что позволяет специалистам концентрироваться на наиболее серьезных инцидентах и реагировать на них своевременно.

Ниже предоставлена более подробную информацию о наиболее важных функциях, которые выполняет SIEM [5]:

а) сканирование уязвимостей и инструменты тестирования на проникновение;

б) системы управления журналами (обычно как часть SIEM);

в) информационные каналы и базы данных о киберугрозах;

г) машинное обучение и расширенную поведенческую аналитику;

д) взаимодействие с инструменты анализа сетевого трафика (NTA) и мониторинга производительности приложений (APM);

е) обнаружение и реагирование на конечные точки, которое помогает обнаруживать и смягчать подозрительные действия на хостах и пользовательских устройствах;

ж) аналитика поведения пользователя и сущности (UEBA), которая использует машинное обучение для выявления подозрительных поведенческих моделей.

Управление инцидентами и событиями безопасности (SIEM) идентифицирует, отслеживает, записывает и анализирует события безопасности в ИТ-среде в реальном времени.

«Умный офис» использует программное обеспечение SIEM в качестве основного компонента. Это набор инструментов, который предоставляет комбинацию SIM (управление информацией о безопасности), также известную как управление журналом, и SEM (управление событиями безопасности), также известную как механизм корреляции. С SIM и SEM SIEM предлагает действенный интеллект. Эта информация собирается из большого количества разнообразных данных журналов, собираемых вашими компьютерами и серверами, а также устройствами безопасности, такими как брандмауэры, службы обнаружения / предотвращения вторжений, базы данных, приложения, коммутаторы и маршрутизаторы.

Процессы «Умного офиса», поддерживаемые SIEM, ключевые примеры:

а) расследование вредоносных программ. SIEM может помочь сотрудникам службы безопасности объединить данные о вредоносных программах, обнаруженных в организации, сопоставить их с информацией об угрозах и помочь понять системы и данные, на которые влияют. SIEM следующего поколения обеспечивают возможности управления безопасностью, визуализации сроков инцидентов и даже могут автоматически «детонировать» вредоносное ПО в песочнице разведки угрозы;

б) предотвращение и обнаружение фишинга. SIEM может использовать корреляции и анализ поведения, чтобы определить, что пользователь нажал на фишинговую ссылку, распространяемую по электронной почте или другими способами. Когда выдается предупреждение, аналитики могут искать похожие шаблоны в организации и по срокам, чтобы определить весь масштаб атаки;

в) расследование отдела кадров, когда сотрудник подозревается в непосредственном участии в инциденте безопасности, SIEM может помочь, собирая все данные о взаимодействии сотрудника с ИТ-системами в течение длительных периодов времени. SIEM может обнаруживать аномалии, такие как входы в корпоративные системы в необычные часы, повышение

привилегий или перемещение больших объемов данных.

Таким образом SIEM ищет и фильтрует данные и может сказать, кто что сделал, когда и откуда. Он использует предопределенные правила корреляции из ранее обнаруженных векторов атак. Затем он предоставляет отчеты о качестве аудита, которые можно использовать в целях обеспечения соответствия [5].

Основные функции SIEM системы:

а) хранит данные, для принятий решения;

б) использует информационные панели для анализа данных, чтобы обнаружить паттерны или действия, которые не являются нормальными;

в) коррелирует данные и сортирует их в пакеты, чтобы превратить их в полезную информацию;

г) агрегирует данные с ряда сайтов, таких как серверы, сети, базы данных, системы электронной почты и приложения, для дальнейшего анализа;

д) оповещения о возможных проблемах безопасности.

Что SIEM не может сделать

а) обнаружьте атаки нулевого дня (неизвестные атаки), потому что у него не будет правил, необходимых для этого;

б) используйте человеческий интеллект для определения приоритетов атак;

в) запустите самостоятельно без команды экспертов по безопасности.

1.4.1 Функции SIEM

Функционирование SIEM-системы обеспечивают отдельные компоненты [9]:

а) **агрегация данных:** управление журналами данных; данные собираются из различных источников: сетевые устройства и сервисы, датчики систем безопасности, серверы, базы данных, приложения; обеспечивается консолидация данных с целью поиска критических событий;

б) **корреляция:** поиск общих атрибутов, связывание событий в значимые кластеры. Технология обеспечивает применение различных технических приемов для интеграции данных из различных источников для превращения исходных данных в значащую информацию. Корреляция является типичной функцией подмножества Security Event Management;

в) **оповещение:** автоматизированный анализ коррелирующих событий и генерация оповещений (тревог) о текущих проблемах. Оповещение может выводиться на «приборную» панель самого приложения, так и быть направлено в прочие сторонние каналы: e-mail, GSM-шлюз;

г) **средства отображения (информационные панели):** отображение диаграмм, помогающих идентифицировать паттерны отличные от стандартного поведения;

д) **совместимость (трансформируемость):** применение приложений для автоматизации сбора данных, формированию отчетности для адаптации агрегируемых данных к существующим процессам управления информационной безопасностью и аудита;

е) **хранение данных:** применение долговременного хранилища данных в историческом порядке для корреляции данных по времени и для обеспечения трансформируемости. Долговременное хранение данных критично для проведения компьютерно-технических экспертиз, поскольку расследование сетевого инцидента вряд ли будет проводиться в сам момент нарушения;

ж) **экспертный анализ:** возможность поиска по множеству журналов на различных узлах; может выполняться в рамках программно-технической экспертизы.

Источниками данных для SIEM служат разнообразные корпоративные системы, представленные в таблице 1.

Таблица 1 – Источники данных

Источники информации	Описание
Системы контроля доступа и аутентификации	Предназначены для наблюдения за получением доступа к информационному потоку
DLP-системы	Передают данные о несанкционированном выходе информации за пределы корпоративной сети и о нарушении в использовании привилегий
Ресурсы IDS/IPS	Передают данные о сетевых атаках, изменении прав доступа
Антивирусные платформы	Уведомляют об угрозах в виде вредоносного кода, замене конфигураций или политик конфиденциальности, сообщают о работе баз данных и ПО
Журналы событий серверов и тонких клиентов	Контролируют соблюдение прав доступа и политики ИБ
Межсетевые экраны	Передают данные об опасных инцидентах, вредоносном ПО
Оборудование сети	Учитывает трафик сети, контролирует доступ пользователей к информационным потокам
Системы веб-фильтрации	Обобщают и направляют данные о том, какие запрещенные или вредоносные сайты в интернете посещают пользователи
Системы инвентаризации и assetmanagement	Поставляют данные для контроля активов в инфраструктуре и выявления новых

Сканеры уязвимостей	Данные об инвентаризации активов, сервисов, программного обеспечения, уязвимостей, поставка инвентаризационных данных и топологической структуры

1.4.2 Основные компоненты, входящие в состав SIEM систем

Состав и реализация существенно зависят от архитектуры решения, размера внедрения, географического распределения системы, параметров производительности [9].

Как правило, для реализации всех базовых функций в SIEM должны присутствовать несколько основных компонентов, на рисунке 3 они продемонстрированы:

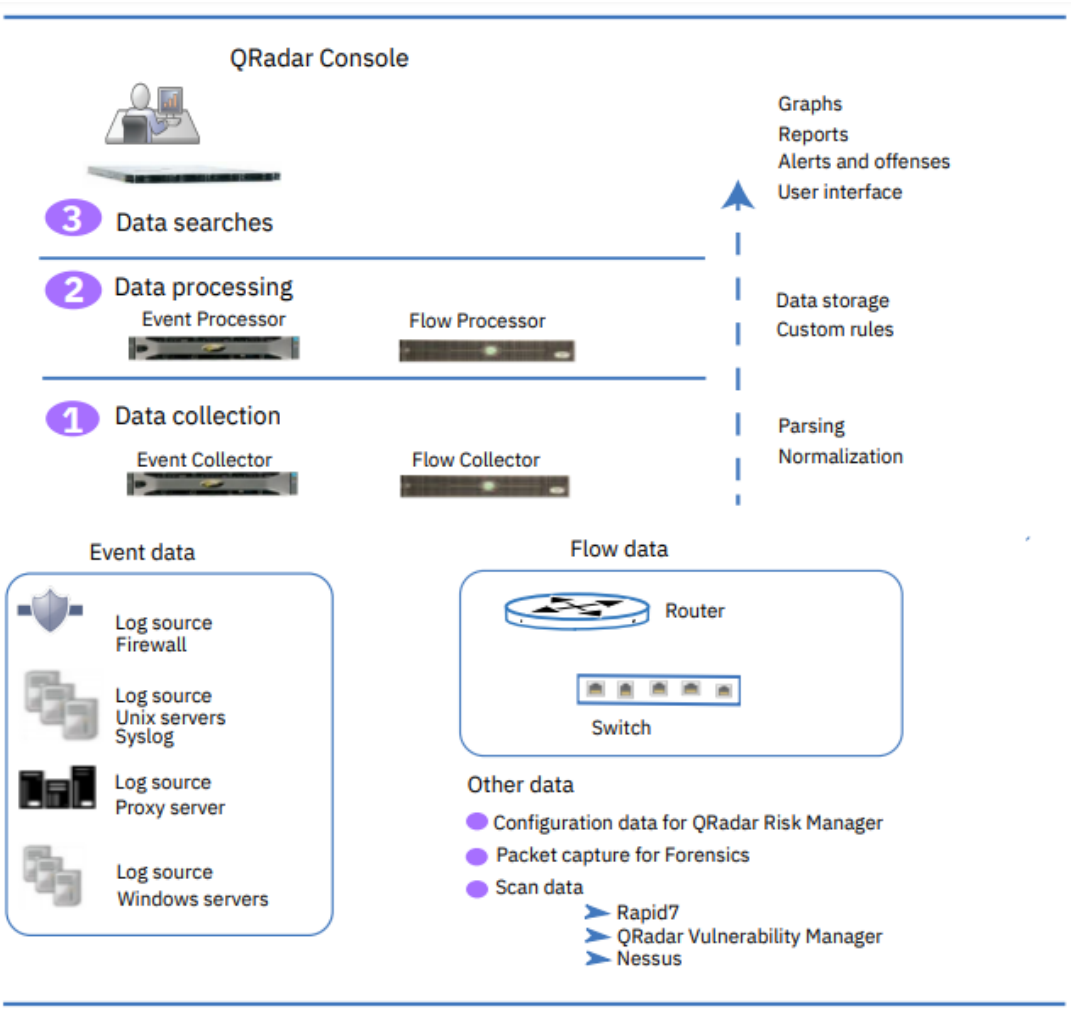

Рисунок 3 – Общая архитектура SIEM

а) **коллекторы:** отвечают за сбор сырых событий. Могут поддерживать массу различных протоколов и сервисов: Syslog, Windows Event Forwarding, SDEE, SNMP Trap, клиентов баз данных (MSSQL, Oracle и т.д.) и другие специфичные сервисы от разных производителей.

Сам сбор событий может происходить как в пассивном режиме отправляет нормализованные события в коррелятор, а сырые события отправляются в хранилище данных. В различных реализациях от разных производителей схема взаимодействия коллектора с другими компонентами может отличатся;

б) **хранилище данных**: отвечает за хранение сырых событий. Возможны реализации с хранением нормализованных событий;

в) **коррелятор**: обеспечивает функции обработки и корреляции нормализованных событий. Возможна реализация контекстного поиска сырых событий, находящихся в хранилище;

г) **консоль управления:** отвечает за управление, настройку и визуализацию. При этом, в ряде случаев, функция визуализации может выполняться отдельной компонентой.

Как было сказано выше, на практике архитектура внедрения главным образом влияет на количество компонент и их реализацию. Например, в малых реализациях почти все функции могут быть выполнены на одном аппаратном устройстве, тогда как масштабирование предполагает максимальное разделение.

1.4.3 Структурная схема архитектура SIEM для Компании

Структурная схема SIEM представлена на рисунке 3 является оптимальным вариантом при построении архитектуры SIEM, так как данная архитектура подразумевает, использование системы «all-in-one» позволяющая сократить затраты на покупку отдельных устройства, а так централизованную систему администрирования, так как все устройства можно содержать в одном помещении.

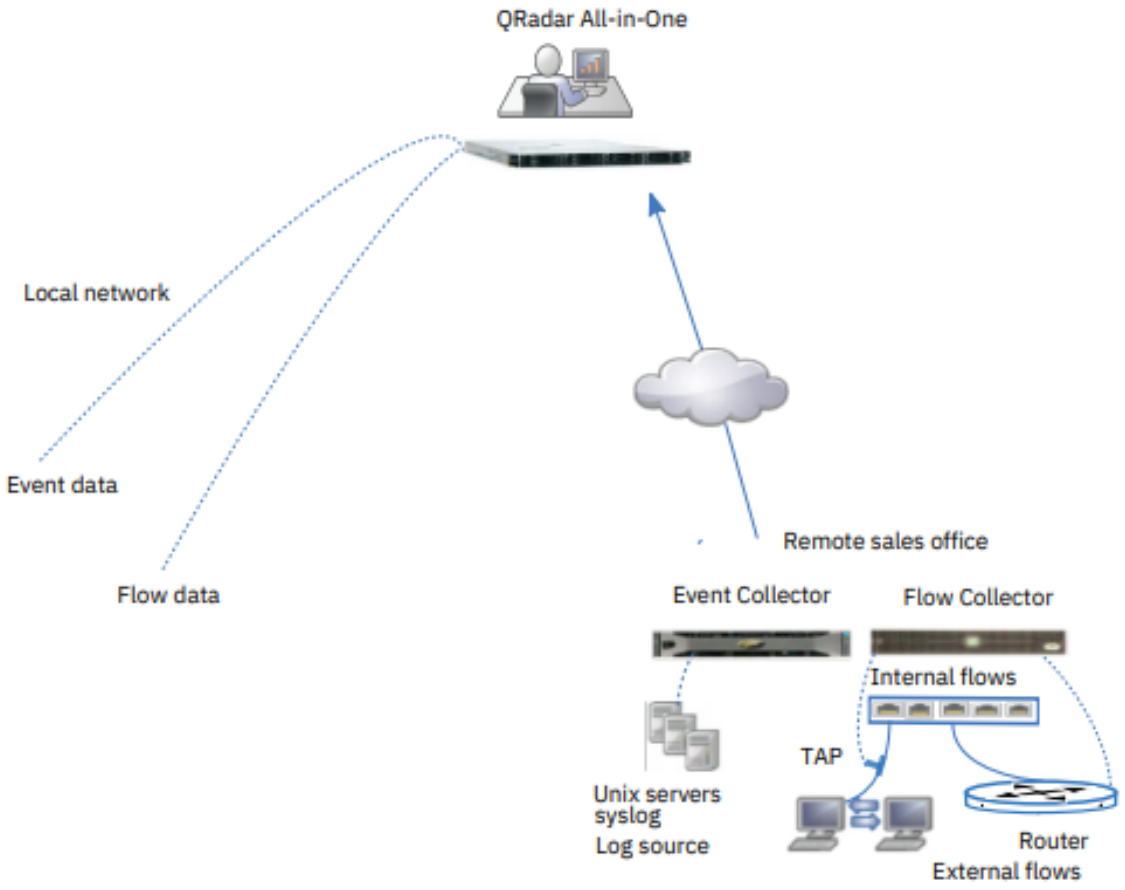

Рисунок 4 – Структурная схема развёртывания SIEM

Ниже описаны как компоненты системы взаимодействуют между собой и какие выполняются процессы [4]:

а) в удаленном офисе сборщик событий собирает данные из источников журналов, а сборщик потоков-из источников журналов, данные с маршрутизаторов и коммутаторов. Коллекторы объединяют и нормализуют данные;

б) сборщики сжимают и передают данные к Неразъемному прибору через глобальную сеть;

в) устройство «all-in-one» обрабатывает и хранит данные. Компания отслеживает сетевую активность с помощью веб-приложения QRadar для поиска и анализа, отчетность, а также для управления предупреждениями и правонарушениями;

г) система «all-in-one» собирает и обрабатывает события из локальной сети.

При возникновении событий ИБ на конечных устройствах или системах данные об этом записываются в журналы состояния соответствующих объектов ИТ-инфраструктуры и в режиме времени, близком к реальному, отправляются на сервер агентами, собственными средствами конечных устройств и систем или по запросу от сенсора (SQL, WMI, и т.д.).

Сервер принимает данные, агрегирует и записывает их в журналы в соответствии с типом источника событий с помощью утилиты rsyslog. Сенсор

обрабатывает журналы в соответствии с логикой плагинов, обеспечивающих поддержку работы с конечными устройствами и системами различных типов, после чего нормализованные данные поступают в БД, где каждому событию ИБ присваивается персональный идентификатор. После этого выполняется обработка данных модулем корреляции в соответствии с заранее определенными правилами корреляции и политиками, на основании которых выявляются инциденты ИБ.

Уведомление о выявленных инцидентах ИБ передается средствами веб-интерфейса администратору безопасности. Нормализованные события ИБ, данные об инцидентах ИБ и информация о настройках системы хранятся в реляционной базе данных.

Взаимодействие администратора безопасности с ядром осуществляется с использованием веб-интерфейса и интерфейса командной строки.

1.5 Использование инструмента SOAR при построении «Умного офиса»

Для более быстрого и практичного решения при управлении инцидентами ИБ, используется также система SOAR, а именно IBM Resilient SOAR Platform.

Платформа Resilient координирует и автоматизирует людей, процессы и технологии, связанные с реагированием на инциденты. Созданные специально для облачных или локальных сред, основанных на потребностях бизнеса, эти решения для платформ оптимизируют управление реагированием на инциденты и конфиденциальностью, предоставляя организациям быстрый, быстрый и гибкий способ реагировать на события и инциденты.

Платформа Resilient настраивается таким образом, чтобы ее можно было адаптировать к следующим базовым сценариям использования [10]:

а) **мониторинг и эскалация.** Платформа Resilient позволяет вводить инциденты, включая соответствующие данные, пользователям или системам, интегрированным с платформой Resilient. Затем можно отслеживать статус от начала до разрешения инцидента. Данные могут включать артефакты, такие как IP-адреса, хэши файлов, URL-адреса, имена пользователей и имена компьютеров. Все данные связаны с инцидентом;

б) **идентификация и обогащение.** Автоматический поиск угроз, рабочие процессы и действия на основе меню предоставляют ценный контекст, сокращают время на определение масштаба и воздействия, обеспечивая быстрый и решительный ответ;

в) **сдерживание, ответ и восстановление.** На основе условий триггера или действий, выполняемых вручную, система может отправлять уведомления или инициировать внешние действия, чтобы содержать и настраивать ваше состояние безопасности как часть вашей книги ответов;

г) **связь и координация.** Включает в себя использование пользовательских действий, функций и API REST для двунаправленной интеграции с вашей средой, включая управление билетами и услугами,

коммуникационные платформы и другие бизнес-приложения. Благодаря интеграции за пределы SOC пользователи могут координировать быстрое и эффективное разрешение инцидентов с платформы.

1.5.1 Преимущество Resilient

Данная систем позволяет разделить роли сотрудников, по их должностным обязанностям, например, сотрудники могут просматривать данные об инцидентах, но не изменять их, тогда как роль создателя инцидентов может вводить инциденты и управлять ими.

Кроме того, челны команды могут получить доступ ко всем инцидентам или только к конкретным инцидентам.

При первом входе в систему панель инструментов деятельности предоставляет новостную ленту, которая предоставляет самые свежие обновления для тех инцидентов, в которых вы участвуете, и список задач, которые должны быть выполнены в течение следующих 7 дней.

В следующих разделах описаны действия, которые может выполнять участники команды:

а) **выполнение поставленных задач.** Задача – это инструкция. Задачи определяются командой реагирования. После выполнения задачи ее можно пометить как завершенную, чтобы план реагирования мог перейти к следующему набору задач. К заданию можно добавить пояснительные примечания и соответствующие приложения.

Можно выполнить инструкцию внутри экрана задачи, выбрав действие из меню. Например, можно отправить инцидент в билетную систему.

Сотрудник может просматривать задачи, которые должны быть выполнены в ближайшее время, с панели управления активностями.

Можно просмотреть задания, назначенные на конкретный инцидент, щелкнув Инциденты в строке меню, а затем выбрав инцидент;

б) **наблюдение за инцидентами и генерация отчетов.** Каждый инцидент упорядочивает данные по различным вкладкам, таким как задачи, сведения, заметки и артефакты. Страница задачи позволяет легко увидеть текущую фазу инцидента, какие фазы и задачи были завершены, а какие еще предстоит выполнить. Аналитик определяет и настраивает эти вкладки. Некоторые вкладки могут быть условными и появляться только при выполнении одного или нескольких заданных условий.

Создание отчета по одному или нескольким инцидентам, используя стандартный шаблон или свой собственный шаблон. Шаблон определяет, какую информацию следует включить. Отчет можно сохранить в виде электронной таблицы Excel или в печатном формате, например, PDF;

в) **панель мониторинга Analytics** отображает диаграммы и графики для просмотра статистической информации. Существует ряд предопределенных виджетов для различных типов информации, таких как открытые задачи по владельцу, открытые инциденты по степени серьезности и инциденты с течением времени по типу;

г) **управление инцидентом**. По мере развития инцидента в системе можно добавить или обновить детали инцидента, заметки, вложения, артефакты и так далее. Эти изменения вносятся путем редактирования соответствующих вкладок в инциденте.

Также при расследовании инцидента может потребоваться обновить информацию в таблицах данных, которую можно найти на различных вкладках инцидента. При интеграции платформы Resilient с другими системами безопасности, можно выполнять действия с этой системой непосредственно из таблицы данных.

Платформа Resilient поддерживает базу данных о нормативных актах, касающихся уведомлений о нарушениях, и руководящих документах. Это позволяет платформе предоставлять сводку требований к отчетам и уведомлениям, автоматически генерировать задачи и обновлять инцидент.

Таки образом данные функции намного упрощают расследование инцидентов ИБ.

1.5.2 Основные функции Resilient для Qradar

Интеграция обеспечивает мощь и гибкость функций рабочего процесса, которые подключаются к QRadar, для автоматизации плана реагирования на инциденты.

При реагировании на все типы предупреждений и инцидентов безопасности очень часто в журнале QRadar SIEM появляются журналы с соответствующей информацией об активности пользователя, сетевом трафике или другом поведении.

Основными функции, которые выполняет Resilient при интеграции с Qradar [10]:

а) **автоматизация поиска.** Автоматизируя эти поиски, при правильных условиях вы можете значительно сократить время и усилия, необходимые для расследования оповещения. Автоматизация может предоставить ответы в течение нескольких секунд на такие вопросы, как: Какие другие пользователи загрузили с этого подозрительного URL? Что еще связано с этой машиной во время этого события? И многое другое

Эта интеграция предоставляет функцию поиска QRadar, которая позволяет пользователям вручную или автоматически запускать произвольные запросы QRadar Ariel непосредственно из устойчивых рабочих процессов в любое время после создания инцидента. Результаты поиска могут быть добавлены к инциденту как артефакты, как заметки, помещены непосредственно в пользовательскую таблицу данных или использованы любым другим способом.

Функция поиска имеет широкие параметры и может выполнять поиск по имени пользователя, IP-адресу или идентификатору нарушения, сгенерированному в QRadar;

б) **справочные данные.** Дополнительные функции включают управление и соединение справочных данных QRadar с Resilient. Эти функции

позволяют рабочим процессам читать и записывать элементы набора ссылок, а затем соответствующим образом обновлять устойчивые артефакты или задачи. Наборы ссылок QRadar могут затем управлять поведением правила SIEM, основываясь на активности в рамках процесса Resilient Response.

Простой пример использования этой интеграции - когда группа безопасности имеет два набора ссылок «Подозрительные IP-адреса» и «Заблокированные IP-адреса», чтобы различать уровни опасности;

в) **эскалация инцидентов.** Эта функция Resilient позволяет эскалации инцидентов из QRadar в платформу реагирования на инциденты Resilient (IRP) и создает подробный план реагирования на инциденты.

1.6 Настройка интеграции Resilient и Qradar

Для интеграции требуется установка параметров конфигурации на вкладке администратор и зайти на вкладку плагины в меню панель навигации слева. Щелкнуть на значок IBM Resilient, конфигурации, в нижней части экрана на рисунке 5.

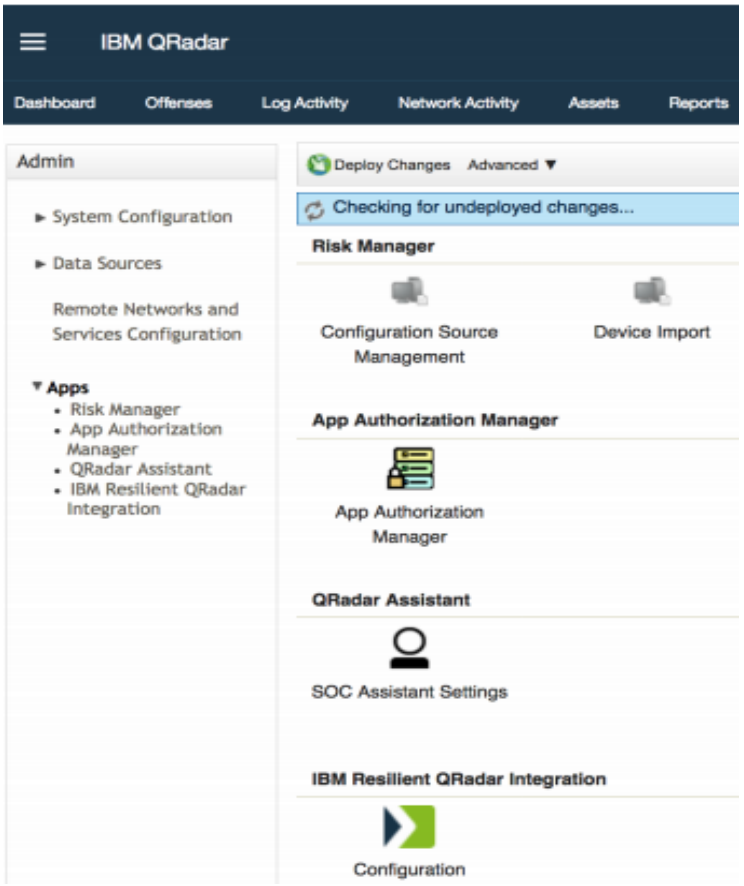

Рисунок 5 – Настройка системы SIEM

Далее открывает всплывающее окно для настройки интеграции на рисунке 5. Вкладка доступ содержит настройки для настройки соединения между QRadar и устойчивой платформой.

Ниже приводится описание каждого поля на рисунке 6:

а) авторизованный сервисный токен: авторизованный сервисный токен, используемый для доступа к API;

б) URL-адрес Resilient Server: URL-адрес вашего сервера Resilient platform, строка URL-адреса должна начинаться с “http: / / ” или “протокол https://”;

в) пользователь API (адрес электронной почты): адрес электронной почты устойчивой учетной записи, используемой для этой интеграции;

г) пароль пользователя API: пароль для пользователя API;

д) поддержка нескольких организаций: Проверьте, поддерживается ли сопоставление между доменами QRadar;

е) название организации: Название организации. При подключении к Resilient настроенная с помощью надстройки MSSP, это должна быть организация конфигурации;

ж) безопасное подключение: если этот флажок установлен, SSL-сертификаты проверяются. Для локальных развертываний, использующих самозаверяющие SSL-сертификаты или имеющие проблемы с SSL-сертификатами, возможно, вам придется снять флажок подключаться

надежно, чтобы позволить интеграции успешно установить соединение;

з) автоматическая настройка Resilient: если флажок установлен, приложение создает в платформе Resilient все обязательные поля, действия и адресаты сообщений, необходимые для работы интеграции;

и) параметры прокси-сервера: установив этот флажок, в случае если конфигурация требует подключения через прокси-сервер, через имя хоста в виде URL-адреса и номера порта. Если схема не предусмотрена для прокси хоста, https:// используется по умолчанию. Если ваше прокси-соединение требует аутентификации, введите имя пользователя и пароль. Функции прокси-сервера используют основной метод аутентификации для поддержки аутентификации.

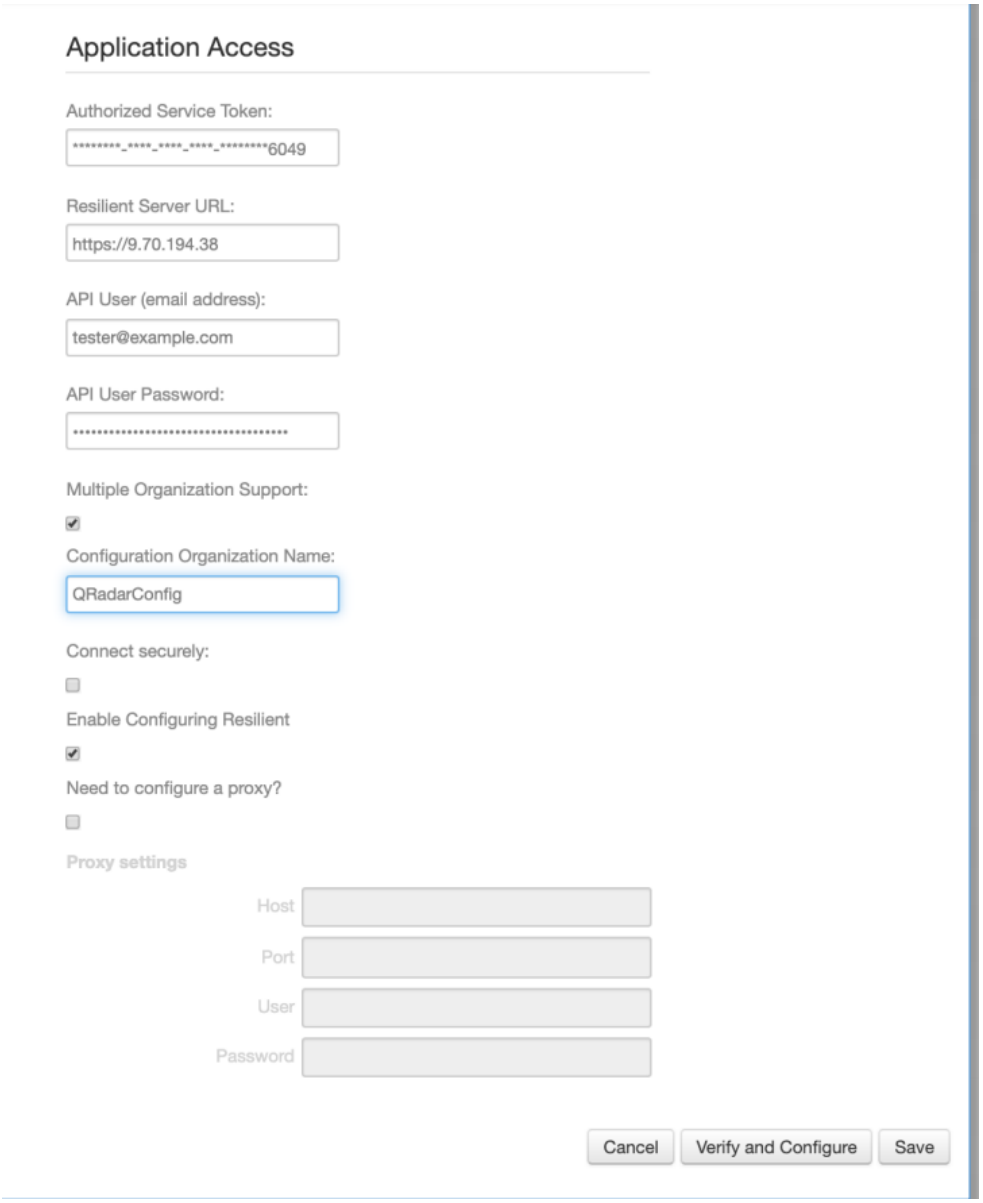

Рисунок 6 – Параметры подключения

к) Далее нажимаем проверить и настроить, чтобы проверить возможность подключения к URL-адресу сервера. Это также проверяет,

присутствует ли поле идентификатора QRadar в платформе, действителен ли авторизованный сервисный токен, а при использовании прокси-сервера-прокси-соединение. Если включена поддержка нескольких организаций, она также извлекает все домены QRadar и дочерние организации. Затем они отображаются на вкладке, где пользователь может выбрать одну из платформ Qradar.

1.7 Построение организационно-технической структуры «Умного офиса»

1.7.1 Командная структура «Умного офиса»

В качестве основного программного средства используется IBM Security QRadar SIEM в вязки с IBM Resilient Security Orchestration, Automation and Response (SOAR).

Также кроме программного комплекса, необходимо создать отдел, в котором, специалисты будут расследовать тяжелые либо инциденты «Zero day», кроме того они будут автоматизировать системы и администрировать ее в непредвиденны случаях.

Отдел реагирования на инциденты - это команда опытных людей в которой они полностью посвящают себя высококачественным операциям в области безопасности ИТ. Они стремятся предотвратить угрозы кибербезопасности, а также обнаруживает и реагирует на любые инциденты на компьютерах, серверах и в сетях, которые он контролирует. Уникальность данного отдела заключается в возможности постоянного мониторинга всех систем, так как сотрудники работают посменно, чередуются и ведут журналы круглосуточно[2].

В отличие от традиционного ИТ-отдела, персонал отдела реагирования на инциденты в основном состоит из команды высококвалифицированных аналитиков кибербезопасности и обученных инженеров. Эти люди используют целый ряд компьютерных программ и специализированных процессов безопасности, которые могут выявить слабые места в виртуальной инфраструктуре компании и не допустить, чтобы эти уязвимости привели к вторжению или краже.

Отдел по реагированию на инциденты опережает потенциальные угрозы, анализируя активные каналы, устанавливая правила, выявляя исключения, усиливая отклики и следя за возможными уязвимостями в уже созданной защите. На таблице 2 ниже описаны основные обязанности, функции, которые должен выполнять сотрудник [1]:

Таблица 2 – Функции отдела реагирования на инциденты

№	Роль	Квалификация	Обязанности
1	Аналитик Оповещение Следователь	Навыки системного администрирования, языки веб-программирования, такие как Python, Ruby, PHP, языки сценариев, сертификаты безопасности, такие как CISSP или SANS SEC401	Мониторинг оповещений SIEM, управление и настройка средств мониторинга безопасности. Расставляет приоритеты предупреждений или проблем и выполняет сортировку.
2	Ответственный за инциденты аналитика уровня 2	Подобно аналитику уровня 1, но с большим опытом, включая реакцию на инциденты. Расширенная криминалистика, оценка вредоносных программ, анализ угроз. Сертификация или обучение хакеров в белой шляпе - главное преимущество.	Получает инциденты и выполняет глубокий анализ, соотносится с информацией об угрозах, чтобы определить действующего лица, характер атаки, а также системы или данные, на которые влияют. Определяет стратегию сдерживания, восстановления и восстановления и принимает меры по ней.
3	Специалист по вопросам анал итики уровня 3	Подобно аналитику уровня 2, но с еще большим опытом, включая инциденты высокого уровня. Опыт работы с инструментами тестирования на проникновение и визуализацией данных между организациями. Обратный инжиниринг вредоносных программ, опыт выявления и разработки ответов на новые угрозы и шаблоны атак.	Ежедневно проводит оценки уязвимостей и тесты на проникновение, а также анализирует оповещения, отраслевые новости, сведения об угрозах и данные о безопасности. Когда происходит серьезный инцидент, присоединяется к аналитику уровня 2, который отвечает и содержит его.
4	Менеджер управления	Подобно аналитику уровня 3, включая навыки управления проектами, обучение управлению реагированием на инциденты, сильные коммуникативные навыки.	Функции наема и обучение персонала SOC, отвечающего за оборонительную и наступательную стратегию, управляет ресурсами, приоритетами и проектами, а также руководит командой непосредственно при реагировании на критически важные для бизнеса инциденты безопасности.

Продолжение таблицы 2

5	Поддержка инженера по безопасности и инфраструктура	Степень в области компьютерных наук, вычислительной техники или обеспечения информации, как правило, в сочетании с такими сертификатами, как CISSP	Специалист по программному или аппаратному обеспечению, который фокусируется на аспектах безопасности при проектировании информационных систем. Создает решения и инструменты, которые помогают организациям надежно справляться с перебоями в работе или злонамеренными атаками.

Обеспечение соответствия этих программ нормативным актам компании, отрасли и правительства также является важной частью работы.

На рисунке 6 показана схема работы концепции «Умного офиса». На данном рисунке 6 описываются следующие шаги [6]:

а) все устройства, подключённые к SIEM системе, отправляют свои данные;

б) данные, которые попали в систему начинают коррелироваться и распределяться по степени важности, риска, степени вероятности, уровня опасности и.т.д;

в) далее SIEM система сама решает, как распорядится событием, которые отправляются в Resilient или же в случае если происходят событие решение которых требует дополнительного рассмотрения оповещает Аналитиков;

г) после Аналитик, рассматривает событие создает карточку инцидента и делает свободный отчет, в котором описывает свои действия, которые он проделал для закрытия инцидента;

д) и в конце старший Аналитик составляет свободный отчет по событию и отправляет его Руководителю.

После того, как выстроена схема работы команды «Умного офиса» выстраиваем соединение работы SIEM. На рисунке 7 показана схема работы SIEM.

Это обуславливается тем, что класс SIEM, который используется полностью подлежит автоматизации и имеет полную совместимость с классами SOAR.

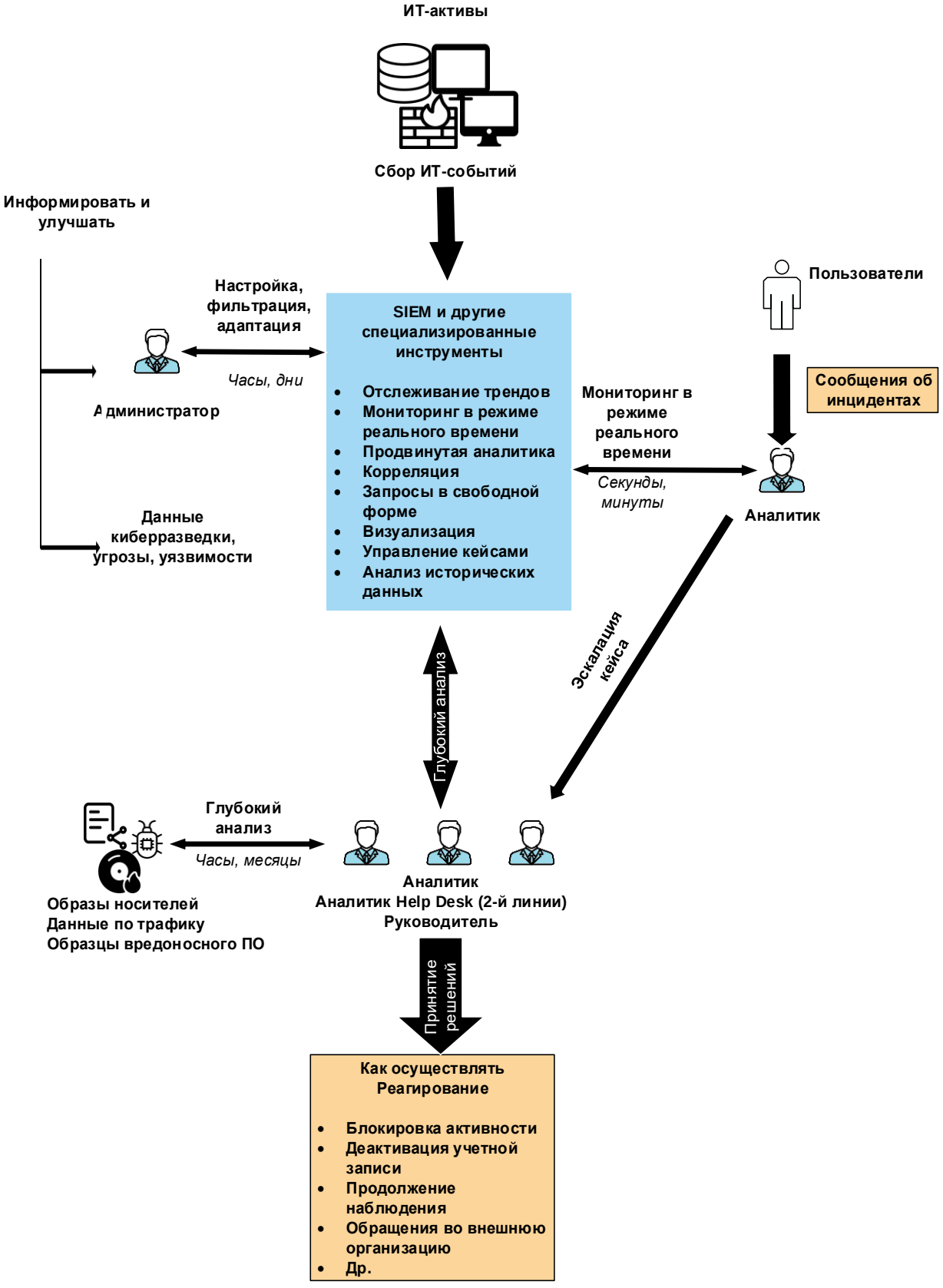

Рисунок 7 – Архитектура команды «Умного офиса»

1.7.2 Техническая структура подключения SIEM

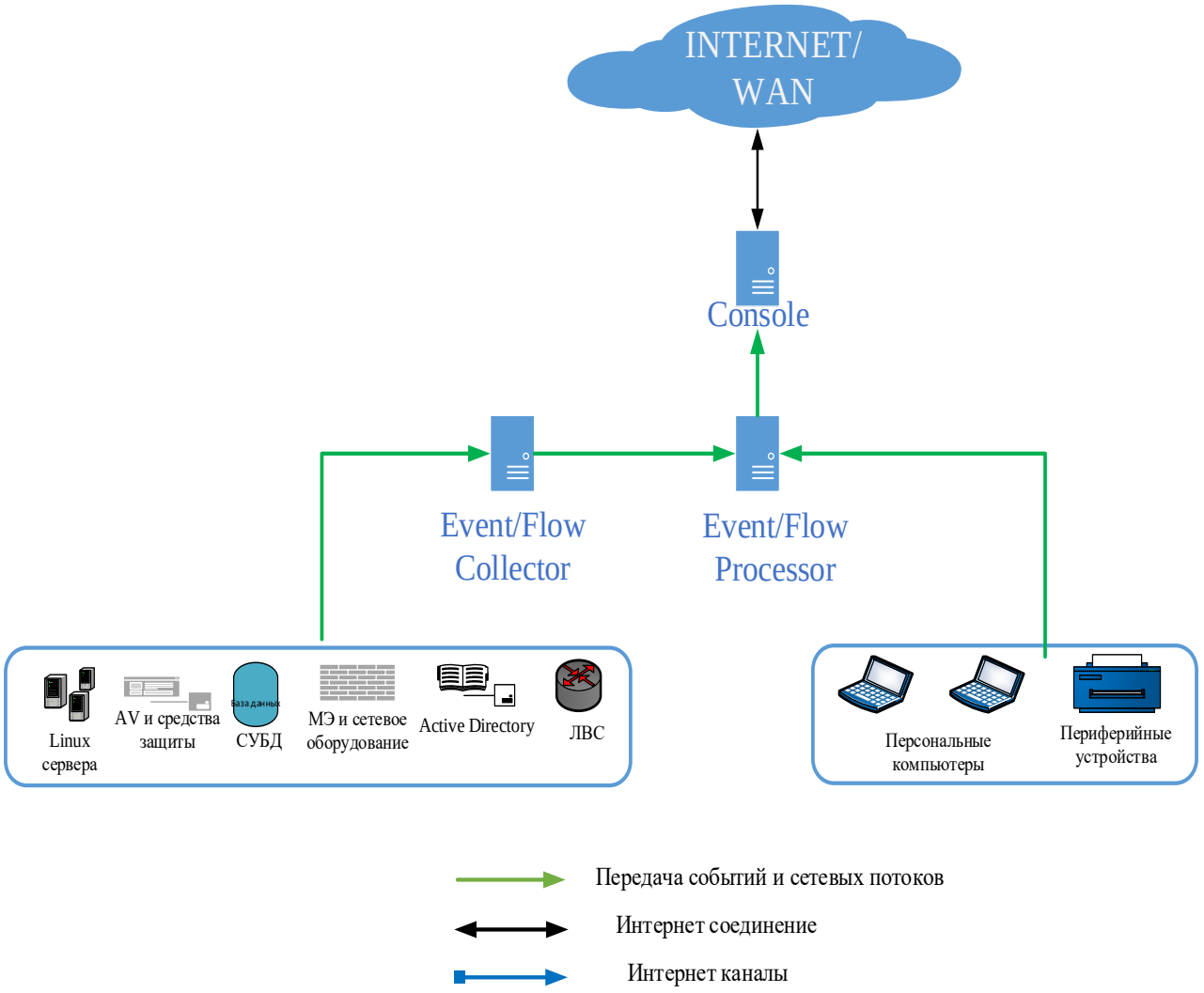

Рисунок 8– Схема подключения устройств

На рисунке 8 показана архитектура “All-in-One”. Сервер планируется установить в офисе компании. Все удаленные источники подключить с использованием существующих VPN подключений.

IBM Security QRadar SIEM имеет в своем составе следующие компоненты [8]:

а) **event collector** – коллектор для сбора событий с источников. Осуществляет первичную обработку полученных событий (парсинг, категоризация) и отправку для анализа и хранения на Event Processor. Данные не хранит;

б) **qflow collector** – коллектор для сбора информации о сетевых потоках. Осуществляет первичную обработку и отправку на Flow Processor. Поддерживает следующие протоколы для передачи статистики о сетевом трафике: NetFlow, JFlow, SFlow, Packeteer. Имеет возможность анализа

трафика до уровня приложений (L7) при условии наличия полной копии трафика (SPAN порт). Данные не хранит;

в) **event processor** – осуществляет хранение и анализ полученных событий. Обработка событий на соответствие правилам корреляции также производится на процессорах;

г) **flow processor** - осуществляет хранение и анализ полученных данных о сетевых потоках. Производит анализ полученных данных на предмет соответствия правилам корреляции;

д) **console** – единая консоль управления всей системой и визуализации полученных данных. Осуществляет генерацию отчетов, хранит всю информация о инцидентах. Позволяет осуществлять корреляцию между данными, хранящимися на разных процессорах.

В таблице 3 приведенные основные технические характеристики для компонентов системы.

Таблица 3 – Технические характеристики

Компоненты	Жесткий диск	Оперативная память	Процессор
Qradar core	2x600 gb	64 gb	3.0 Ггц, 8 ядер
Сервер	2x600 gb	64 gb	3.0 Ггц, 16 ядер
БД	1 tb	16 gb	3.0 Ггц, 8 ядер
Secret Net 7 сервер безопасности	1 tb	16 gb	3.0 Ггц 8 ядер
Resilient	2tb	64 gb	2x Intel I7 E5-2620v3
1 ПК	4 tb	16 gb	Intel I7- 2620v3

Следующая таблица 4 описывает общие требования, которые будут решены с помощью концепции «Умного офиса»

Таблица 4 – Соответствующие требованиям программные и аппаратные средства

№	Наименование оборудования	Технические и (или) функциональные характеристики	Программные и аппаратные средства
1	Средства (системы) контроля (анализа) защищенности информационных систем	Автоматизированная инвентаризация ресурсов информационных систем (сбор информации об узлах информационных систем и об используемом в них программном обеспечении), выявление уязвимостей.	SIEM

Продолжение таблицы 4

2	Средства управления информацией об угрозах безопасности информации	Автоматизированный сбор и анализ информации, поступающей из различных источников, об угрозах безопасности информации. Должны иметь формуляры, оформленные разработчиками (производителями) данных средств.	SIEM
3	Средства управления событиями безопасности информации	Автоматизированный сбор, анализ и корреляция данных о событиях безопасности информации, регистрируемых компонентами информационных систем, идентификация по заданным индикаторам типовых инцидентов информационной безопасности и их локализация.	SIEM, Resilient
4	Средства управления инцидентами информационной безопасности	Автоматизированная регистрация информации об инцидентах информационной безопасности информационных систем, предоставление рекомендаций по реагированию на них, формирование и модификация шаблонов инцидента информационной безопасности, в том числе рекомендаций по реагированию на них. Должны иметь формуляры, оформленные разработчиками (производителями) данных средств. Лицензиатами (соискателями лицензии)	SIEM, Resilient
5	Системы защиты информации информационных систем, используемых для мониторинга информационной безопасности	Системы защиты информации информационных, используемых для оказания услуг по мониторингу информационной безопасности информационных систем, должны соответствовать Требованиям о защите информации, составляющей корпоративную тайну, содержащейся в государственных информационных системах	SIEM, Resilient

2 Практическая часть

2.1 Реализация концепции «Умный офис»

2.1.1 Настройка системы SIEM IBM QRadar

SIEM QRadar имеет множество настроек управления, на рисунке 9 ниже видно, что для каждого действия в системе имеется определенная вкладка.

Ниже описаны вкладки, которые будут настраиваться:

a) Сводная панель;

b) Нарушения –> Правила;

c) Управление –> Иерархия сети;

d) Управление –> Конфигурация системы;

e) Управление –> Управление Пользователями.

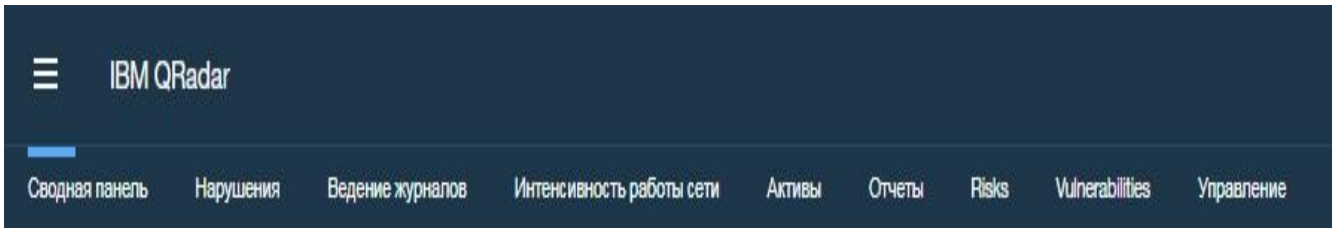

Рисунок 9 – Вкладки SIEM системы

Для начала необходимо настроить иерархию сети в которой укажем какие устройства будут подключены и откуда будут поступать события.

Построение сетевой иерархии в IBM QRadar – это важный шаг в настройке развертывания. Без правильно настроенной сетевой иерархии QRadar не может определять направления потока, создавать надежную базу данных активов или использовать полезные строительные блоки в правилах [9].

Организация системы и сети по ролям или аналогичным моделям трафика на рисунке 10. Сеть организована следующим образом:

а) она включает группы для почтовых серверов, пользователей отделов, групп разработчиков. Используя эту организацию, можно различить поведение сети и применять политики безопасности управления сетью на основе поведения. Размещен только один уникальный сервер, что обеспечивает лучшую видимость сервера в QRadar и упрощает создание определенных политик безопасности для сервера;

б) помещены серверы с большим объемом трафика, такие как почтовые серверы, в верхней части группы. Эта иерархия предоставляет визуальное представление при возникновении расхождений;

в) сетевая группа настроена с 9 объектами;

г) для экономии дискового пространства путем объединения нескольких бесклассовых междоменных маршрутов (CIDR) или подсетей в одну сетевую группу.

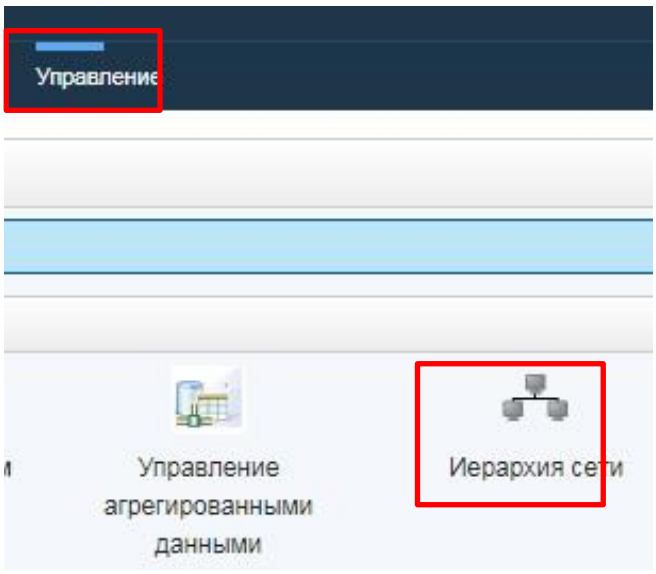

Рисунок 10 – Настройка сетевой иерархи

Продемонстрировать, то как добавляются устройства, для создания иерархии, на примере создания группы демилитаризированной зоны.

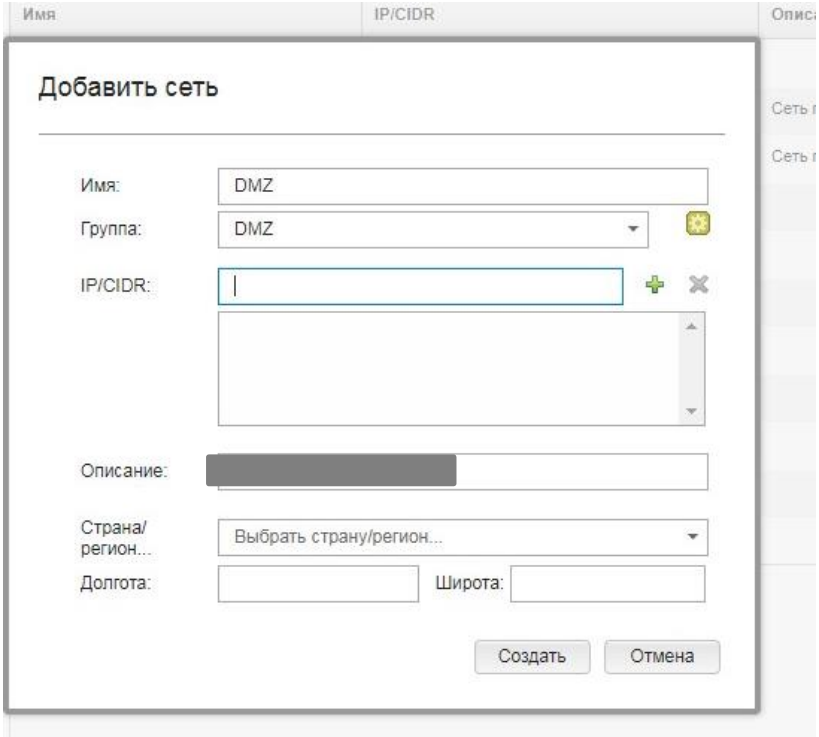

Рисунок 11 – Создание группы

Во вкладке CIDR введите IP-адрес или диапазон CIDR для сетевого объекта. Имеется возможность добавить несколько IP-адресов и диапазонов CIDR как видно на рисунке 11.

Далее настроем вкладку «Сводная панель» [9], для того, чтобы Аналитику было легче сориентироваться, какие инциденты являются новыми и какие требуют немедленного расследования и т.д.

Сводная панель – предоставляет рабочую среду, поддерживающую несколько панелей мониторинга, на которых можно отобразить свои представления о сетевой безопасности, активности или собираемых данных.

Сводная панель позволяют организовать элементы панели мониторинга в функциональные представления, которые позволяют сосредоточиться на определенных областях вашей сети.

Используйте вкладку Сводная панель для отслеживания поведения событий безопасности.

Вы можете настроить свою панель мониторинга. Содержимое, отображаемое на вкладке Сводная панель, зависит от конкретного пользователя.

Вкладка панель мониторинга будет содержать пять панелей мониторинга, ориентированных на безопасность, сетевую активность, активность приложений, мониторинг системы и соответствие требованиям.

Каждая панель мониторинга отображает набор элементов панели мониторинга. Элементы панели мониторинга служат отправной точкой для перехода к более подробным данным. В следующей таблице 5 определены панели мониторинга.

Для создания данных панелей необходимо:

а) нажать на вкладку «Сводная панель»;

б) нажать на иконку «Создание новой панели»;

в) далее дать название панели;

г) после этого выбираются данные которые панель будет отражать;

д) нажимаю ОК.

QRadar анализирует следующую информацию:

а) входящие события и потоки;

б) информация об активах;

в) известные уязвимости.

Правило, создавшее правонарушение, определяет тип правонарушения.

Магистрат определяет приоритетность правонарушений и назначает величину ущерба, основываясь на нескольких факторах, включая количество событий, серьезность, актуальность и достоверность.

На таблице 5 показаны панели, которые создавались их название, для чего она необходим и настройка, которую необходимо произвести для создания панели.

Таблица 5– Создание Панелей мониторинга

Сводная панель	Описание
Нарушение правил брандмауэра	Данная панель отражает случаи, когда пользователи или же программно были нарушены правила настройки брандмауэра, тем самым можно увидеть на какие сайты хотел попасть пользователь или же были ли совершенны попытки отключения либо изменение настроек брандмауэра. Данная вкладка отображает следующие поля: ICMP Type/Code (Total Packets) Top Networks by Traffic Volume (Total Bytes) Firewall Deny by DST Port (Event Count) Firewall Deny by DST IP (Event Count) Firewall Deny by SRC IP (Event Count) Top Applications (Total Bytes) Link Utilization (real-time) DSCP - Precedence (Total Bytes)

Рисунок 12 – Пример данных нарушений

Продолжение таблицы 5

Источники событий	В это вкладке по часам и минутам отражаются события и источники откуда приходят данные события: Top Log Sources (Event Count) Link Utilization (real-time) System Notifications Event Processor Distribution (Event Count) Event Rate (Events per Second Coalesced - Average 1 Min) Flow Rate (Flows per Second - Peak 1 Min)

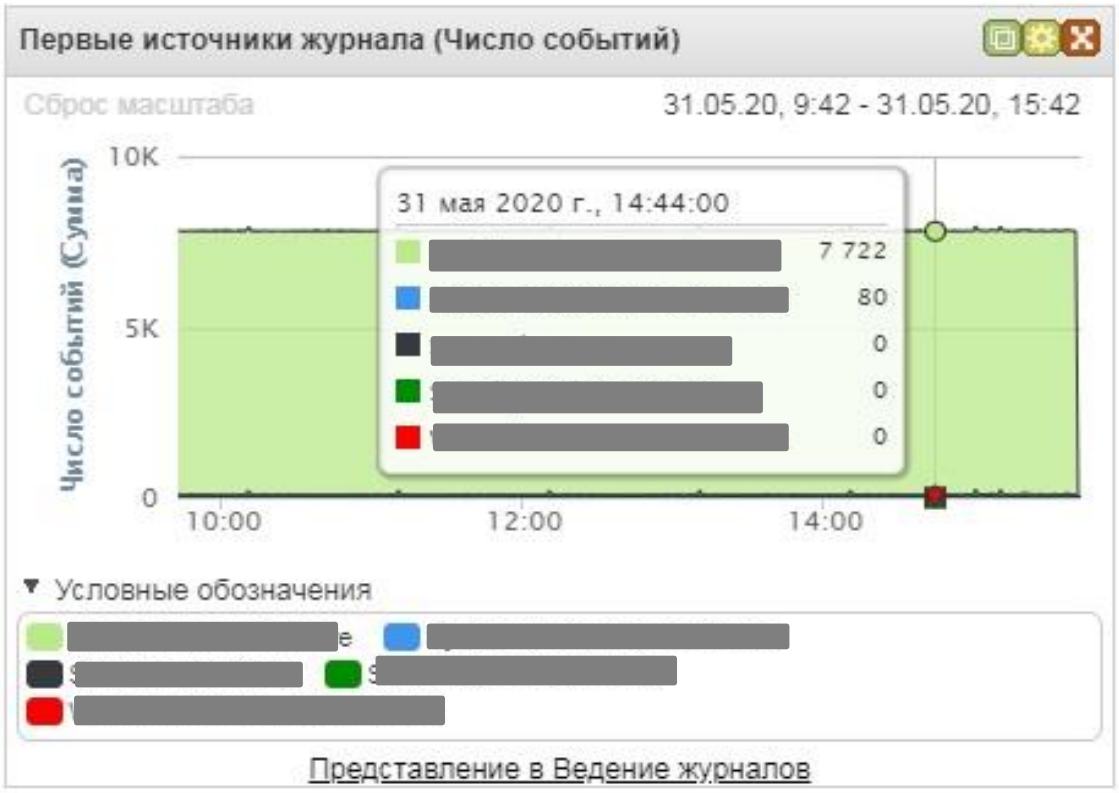

Рисунок 13 – Пример данных событий

Продолжение таблицы 5

Самые последние нарушения	Данная вкладка является, основной так как в ней отражаются серьезные инциденты, которые произошли в течении недели, дня либо же часов требуют немедленного расследования Default-IDS/IPS-All: Top Alarm Signatures (real-time) Top Systems Attacked (Event Count) Top Systems Sourcing Attacks (Event Count) My Offenses Most Severe Offenses Most Recent Offenses Top Services Denied through Firewalls (Event Count) Internet Threat Information Center Flow Bias (Total Bytes) Top Category Types Top Sources Top Local Destinations

Рисунок 14 – Пример данных последних нарушений

Серезные нарушения	В данной вкладке отображаются серьезные нраушения, которые не были закрыты вовремя или дейтсвия по реагирвоанию на рисунке 15 виднл какие нарушения серьезные.

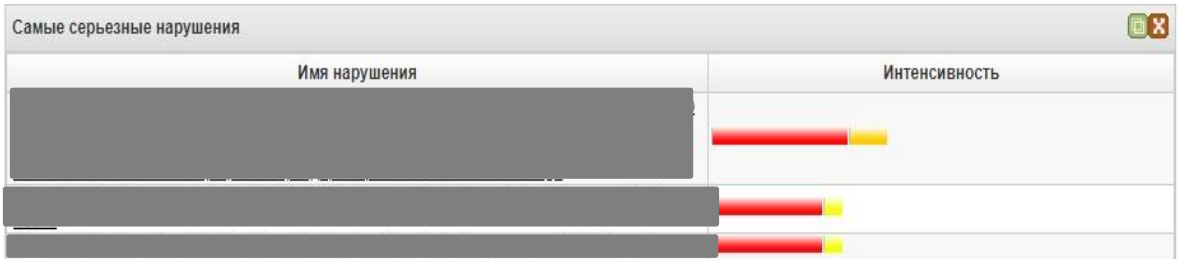

Рисунок 15 – Пример данных серьезных нарушений

После, того как были созданы основные Панели вывода информации по инцидентам создадим Правила с помощью, которых Аналитик сможет видеть, на панелях основные события и инциденты, происходящие в информационной системе.

Настраиваемые правила проверяют события, потоки и нарушения, чтобы обнаружить необычную активность в информационной системе. Правила обнаружения аномалий проверяют результаты поиска сохраненных потоков или событий, чтобы определить, когда в сети возникают необычные шаблоны трафика. Правила обнаружения аномалий требуют сохраненного поиска, сгруппированного вокруг общего параметра.

Правила, связанные с событиями и потоками, группируют обычно используемые тесты для построения сложной логики, чтобы ее можно было повторно использовать в правилах. Такие правила часто проверяет наличие IP-адресов, привилегированных имен пользователей или коллекций имен событий. Например, правило может включать в себя IP-адреса всех DNS-серверов. Затем правила могут использовать этот строительный блок.

Правила работают следующим образом: Сборщики событий QRadar собирают события из локальных и удаленных источников, нормализуют эти события и классифицируют их на низкоуровневые и высокоуровневые категории. Для потоков сборщики QRadar QFlow считывают пакеты с провода или принимают потоки с других устройств, а затем преобразуют сетевые данные в записи потоков. Каждый обработчик событий обрабатывает события или потока данных с помощью QRadar коллекционеров событие. Процессоры потока изучают и коррелируют информацию, чтобы указать на поведенческие изменения или нарушения политики. Механизм пользовательских правил (CRE) обрабатывает события и сравнивает их с определенными правилами для поиска аномалий. При выполнении условия правила обработчик событий генерирует действие, определенное в ответе правила. CRE отслеживает системы, участвующие в инцидентах, вносит свой вклад в события, связанные с правонарушениями, и генерирует уведомления.

Перед созданием правил необходимо понять, что необходимо обнаружить и каковы критерии срабатывания правил.

Правила будут разделены на пять категорий:

а) правила, основанные на событиях;

б) правила, основанные на потоках;

в) правила, основанные на событиях и потоках данных;

г) нахождение отклонений от нормального поведения.

Создание правил на основе событий

Такие правила позволяют QRadar соотносить поля с различными типами источников данных, соотносить события с другими событиями и выявлять определенные закономерности.

Чтобы создать правило, нужно сделать следующее:

Перейти на вкладку правонарушения-Правила-действия-новое правило события, как на рисунке 16.

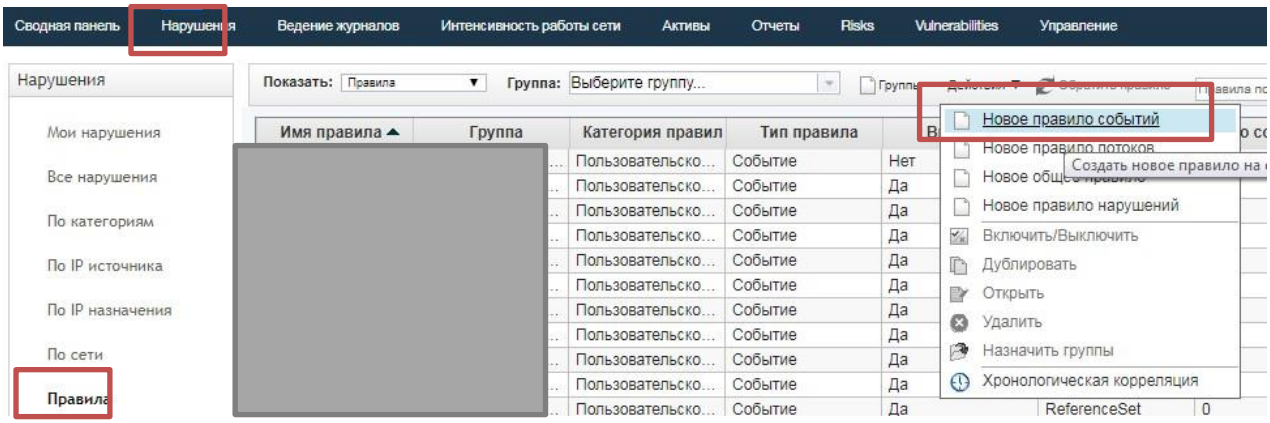

Рисунок 16 – Создание правила

Далее заполняем поле Имя правила. Добавление условия, как на рисунке 17. Установка значения условий. Выбор групп для этого правила, жмем Далее.

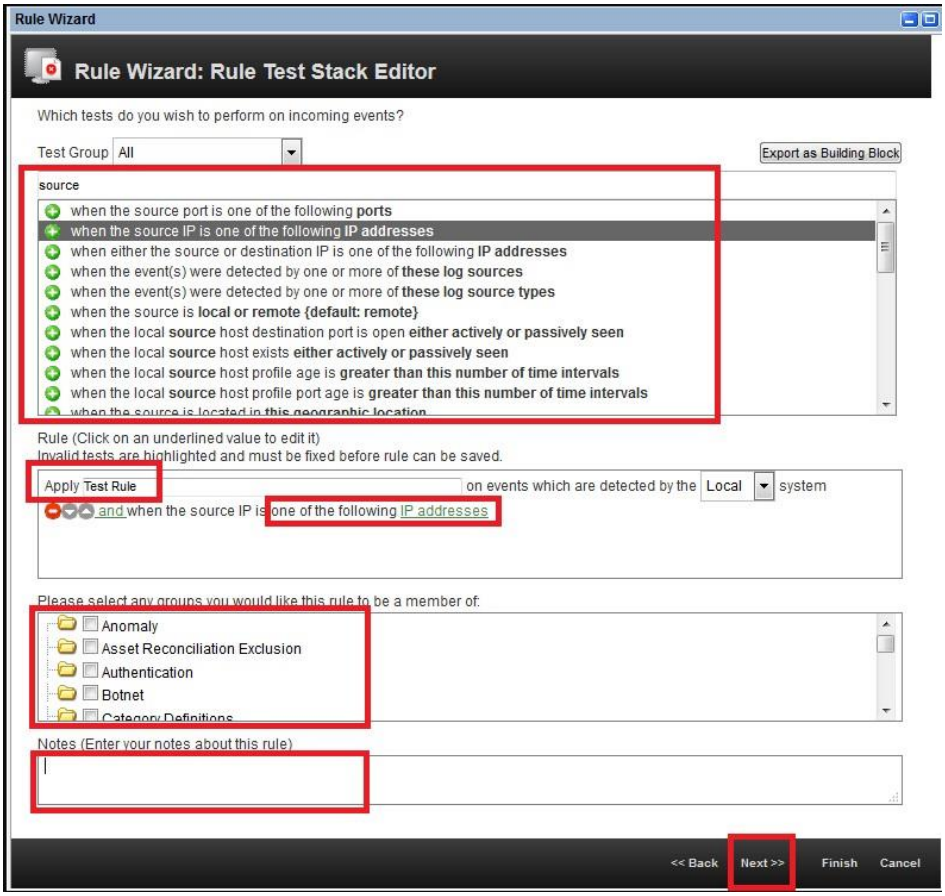

Рисунок 17 – Настройка правила для событий

После этого нужно указать действие правила, ответ правила, ограничитель правила и включить правило, как на рисунке 18 нажать далее.

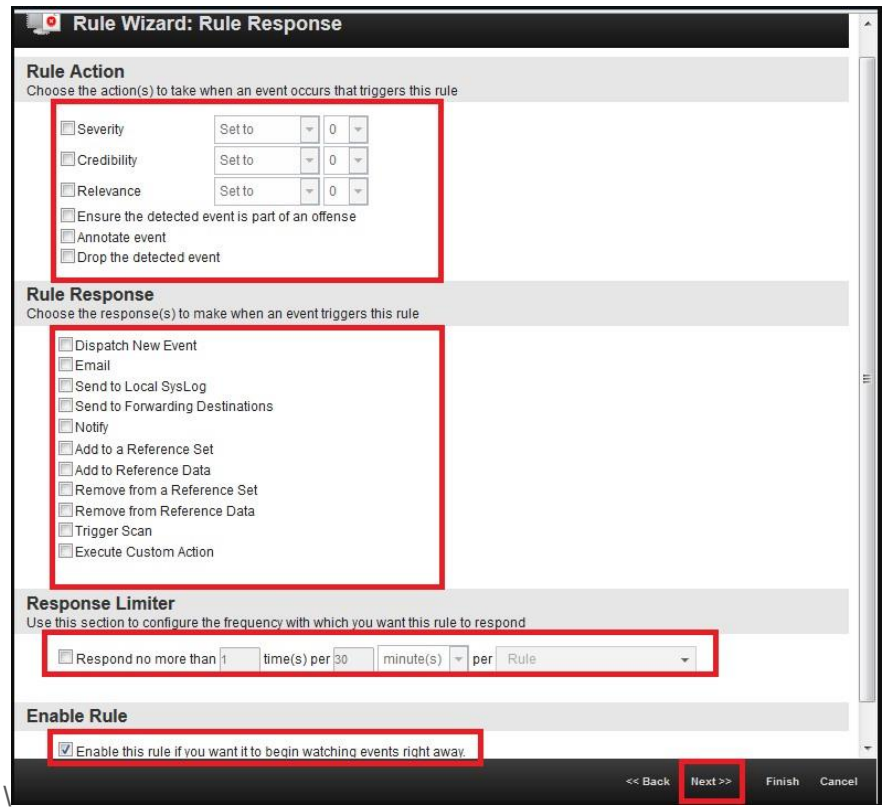

Рисунок 18 – Настройка правила для событий

В открывшемся окне отображаются все параметры и условия, которые применяются к правилу как на рисунке 19. Если все правильно, нажмите кнопку Готово.

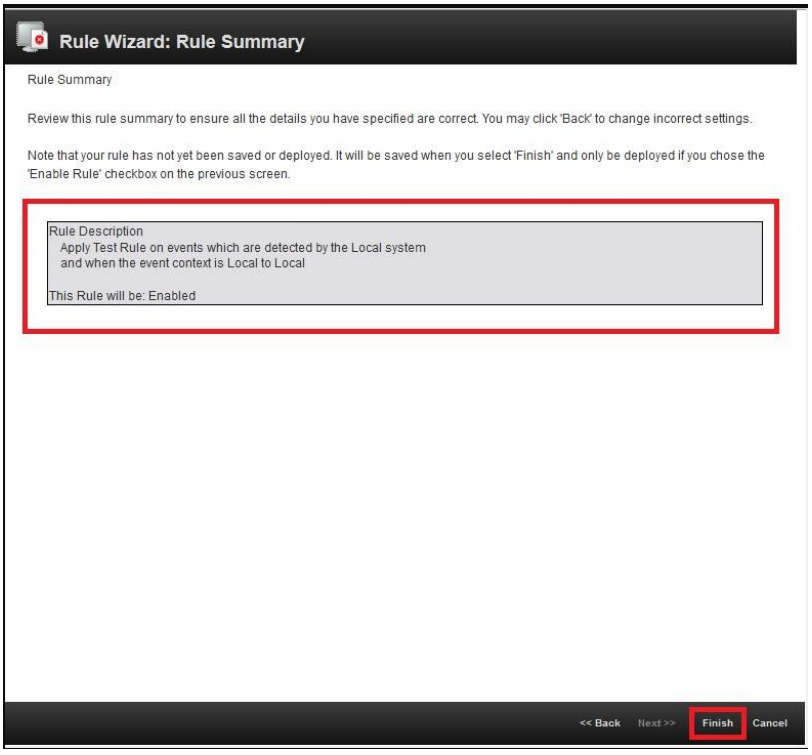

Рисунок 19 – Созданное правило

Создание правил на основе потоков данных

Этот вид правил позволяет анализировать и коррелировать сетевые события.

Чтобы создать такое правило, необходимо:

Перейдите на вкладку правонарушения, как на рисунке 20-Правила-действия-новое правило потока.

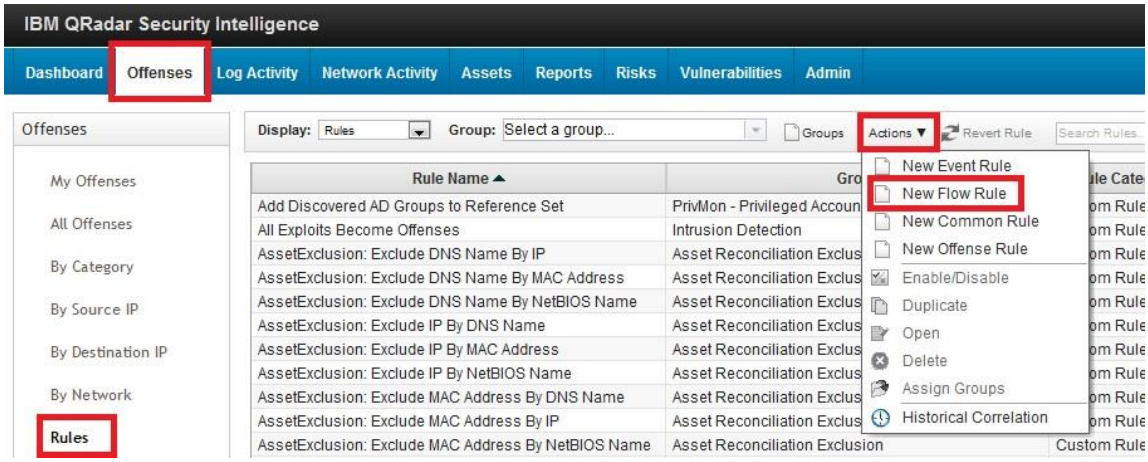

Рисунок 20 – Создание потока

Все остальные шаги такие же, как и для Правил событий, описанные выше.

Создание правил на основе событий и потоков данных.

Правила, основанные на событиях и сетевых потоках данных, позволяют соотносить поля из различных типов источников данных с аналогичными полями в потоках данных рисунок 21 и 22.

Чтобы создать такое правило, необходимо:

Перейти на вкладку правонарушения-Правила-действия-новое общее правило.

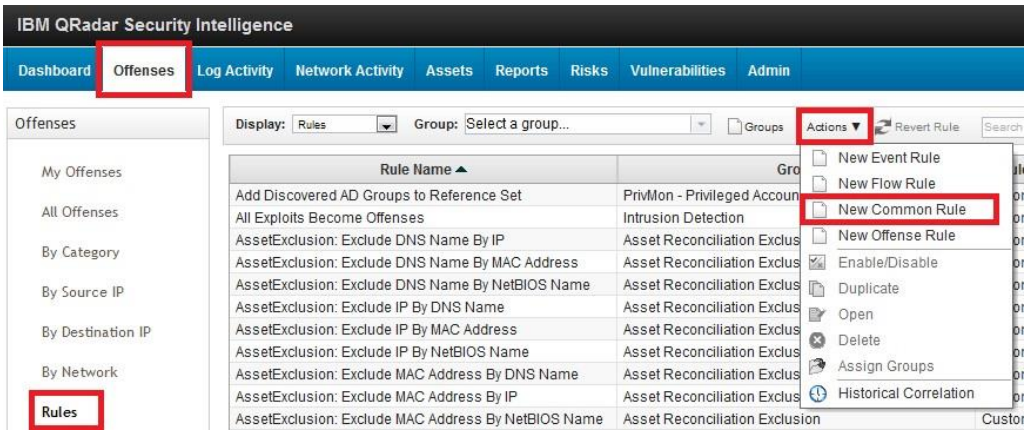

Рисунок 21 – Создание правил на потоки

Далее необходимо настроить следующее

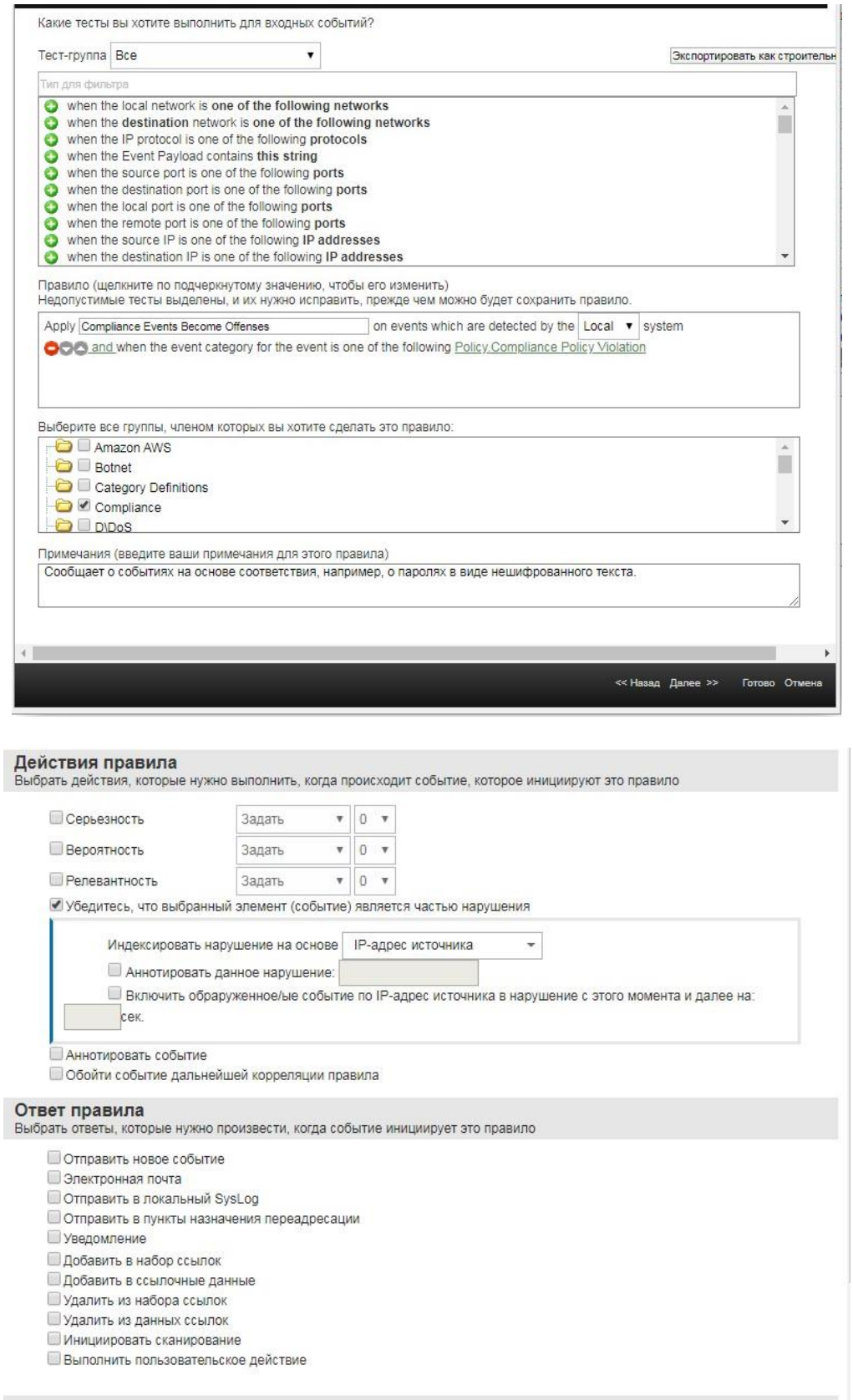

Рисунок 22 – Настройка правила

Обнаружение отклонений от нормального поведения

Правила обнаружения отклонений от нормального поведения основаны на поисковых запросах. Запрос должен соответствовать определенному формату и должен описывать, что такое нормальное поведение.

Чтобы создать такое правило, необходимо создать Поиск, описывающий нормальное поведение. Обязательным критерием для создания поиска является агрегирование по одному или нескольким полям.

Тогда вам нужно запустить его. После этого перейдите на вкладку правило и выберите один из типов правил, как показано на рисунке 23 ниже.

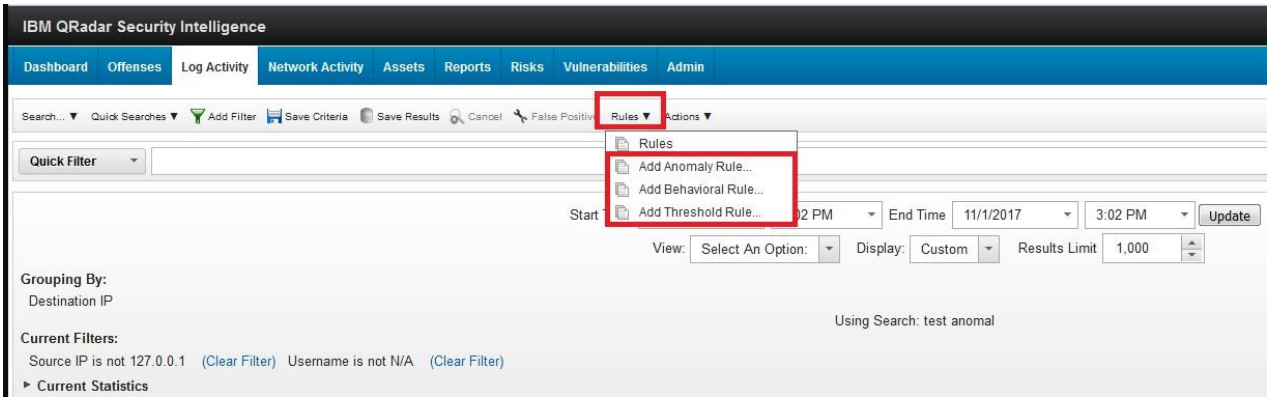

Рисунок 23 –Создание фильтр правила

Наконец, необходимо указать условия запуска правила, как это было в разделе Создание правил на основе событий.

Таким образом использование правил позволяет SIEM автоматически выявлять аномалии в поведении пользователей и выявлять конкретные инциденты безопасности. Обработка результатов запуска правил снижает нагрузку на администратора SIEM и позволяет повысить уровень безопасности внутри организации.

Добавляем пользователей, которые будут иметь доступ к системе на рисунке 24. Для этого, необходимо определить роли, которые будут включать пользователи. Для своей системы я создала следующие роли пользователей.

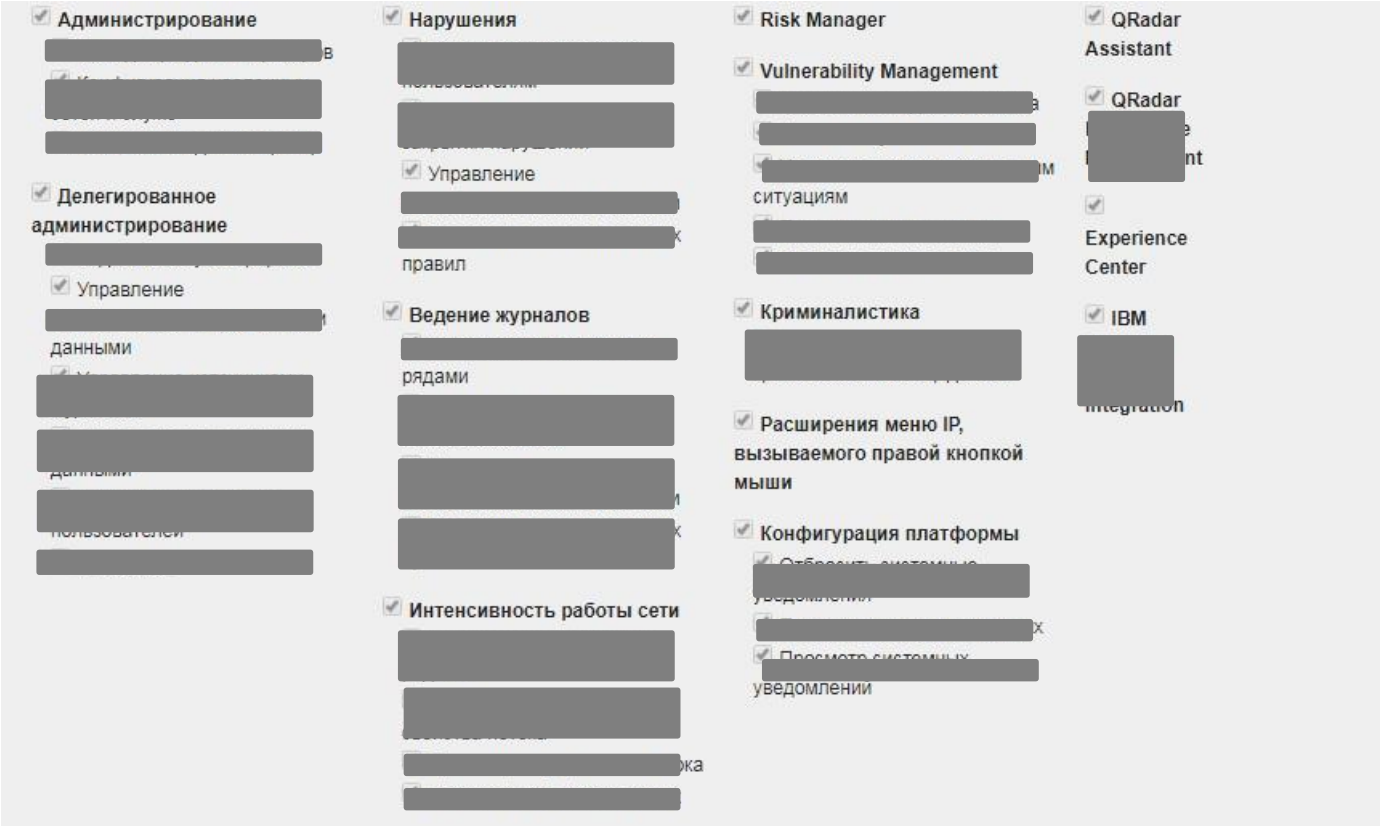

Рисунок 24 – Роли пользователей и их разрешения

Также устанавливаем политику для аутентификации пользователей на рисунке 25.

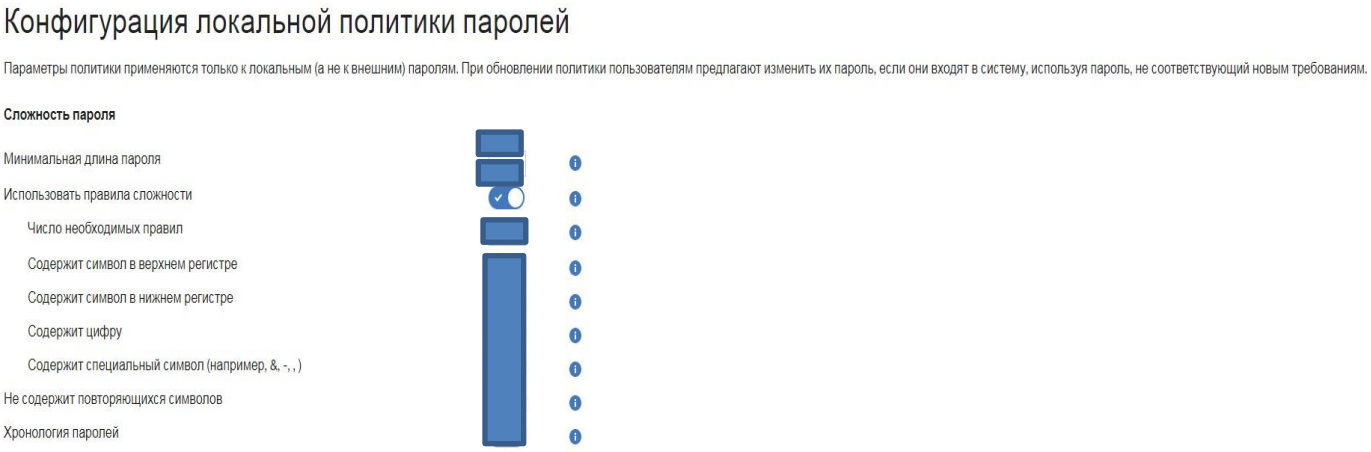

Рисунок 25 – Политика аутентификации пользователей

2.1.2 Расширенные возможности поиска Qradar

Для того, чтобы администратору не искать определенный события или же инциденты, применяются запросы Ariel Query Language (AQL), который определяет поля, которые необходимы и то как нужно сгруппировать их для выполнения запроса.

Чтобы настроить расширенный поиск необходимо:

а) в параметрах Advanced Search на панели инструментов поиска, которая находится на вкладках Network Activity и Log Activity, чтобы ввести запрос AQL;

б) выбрать Advanced Search в списке на панели инструментов поиска. Развернуть поле расширенного поиска, выполнив следующие действия:

1) перетащить значок расширения, который находится справа от поля;
2) нажать Shift + Enter, чтобы перейти к следующей строке;
3) нажать Enter;
4) можно щелкнуть правой кнопкой мыши любое значение в результате поиска и отфильтровать это значение;
5) все поиски, включая поиски AQL, включаются в журнал аудита.

В таблице 6 ниже представлены примеры простых запросов поиска AQL

Таблица 6 – Примеры поиска AQL

Описание	**Пример**
Выбор определенных столбцов	SELECT sourceip, destinationip FROM events
Выбор определенных столбцов и упорядочьте результаты.	SELECT sourceip, destinationip FROM events ORDER BY destinationip
Выполнение агрегированный поисковый запрос.	SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip
Выполнение вызова функции в предложении SELECT.	SELECT CATEGORYNAME(category) AS namedCategory FROM events
Отфильтровать результаты поиска с помощью предложения WHERE.	SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1
Поиск событий, вызвавших определенное правило, основанное на имени правила или частичном тексте в имени правила.	SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'
Ссылки на имена полей, содержащие специальные символы, такие как арифметические символы или пробелы, путем заключения имени Поля в двойные кавычки.	SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'

Использование Ariel Query Language (AQL) для извлечения определенных полей из событий, потоков и таблиц 6 simarc в базе данных Ariel.

Активы и конфигурация.

Индикаторы угрозы и использования зависят от типа ресурса, операционной системы, состояния уязвимости, типа сервера, классификации и других параметров.

В этом запросе расширенный поиск и модель активов обеспечивают оперативное понимание местоположения.

Функция Assetproperty извлекает значения свойств из активов, что позволяет включать данные в результаты.

```
SELECT
ASSETPROPERTY('Location',sourc
eip) as location, COUNT(*) as 'event count'
FROM events
GROUP BY
location LAST 1
days
```

Следующий запрос показывает, как вы можете использовать расширенный поиск и отслеживание идентификаторов пользователей в модели активов.

Функция Network LOOKUP.

Использовать функцию Network LOOKUP для получения сетевого имени, связанного с IP-адресом.

```
SELECT
NETWORKNAME(sourceip) as
srcnet,
NETWORKNAME(destinationip)
as dstnet FROM events
```

Функция Rule LOOKUP.

Использовать функцию Rule LOOKUP, чтобы получить имя правила по его идентификатору.

```
SELECT RULENAME(123) FROM events
```

Следующий запрос возвращает события, которые вызвали определенное имя правила.

```
SELECT * FROM events
WHERE RULENAME(creEventList) ILIKE '%my rule name%'
```

Полный поиск по тексту.

Использовать оператор TEXT SEARCH для выполнения полного поиска с помощью опции расширенного поиска.

В этом примере есть ряд событий, которые содержат слово «межсетевой экран» в полезной нагрузке. Вы можете искать эти события, используя параметр Quick filter и Advanced search на вкладке Log Activity.

Чтобы использовать параметр Quick filter введите следующий текст в поле Quick filter box: 'firewall'

Чтобы использовать параметр Advanced search, введите следующий запрос.

SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'

2.1.3 Написание пользовательских скриптов

Основным инструментом для автоматизации действий SIEM системы — это написание пользовательских скриптов (Custom action scripts). Использование таких скриптов очень структурировано. Существует три варианта сценариев:

а) Bash;
б) Perl;
в) Python.

Сценарий должен быть загружен в QRadar с помощью значка «Определить действия» на вкладке администратора. Сценарий сначала создается с помощью стандартного редактора и сохраняется на ПК, который используется для доступа к QRadar.

Затем на вкладке «Определить действия», который отображает список существующих сценариев и разрешает добавление нового сценария.

QRadar загружает скрипт и предоставляет опции для применения параметров к скрипту. Например, свойство сетевого события, такое как IP-адрес источника, может быть взято из полезной нагрузки события и передано в сценарий для дальнейшей обработки. Теперь скрипт хранится в QRadar в определенной директории / opt / qradar / bin / ca_jail. Использование этого каталога позволяет QRadar контролировать обработку и предотвращать повреждение системы плохо сформированными сценариями. Обратите внимание, что при выполнении сценария, если в течение 15 секунд не было никаких действий, сценарий сбрасывается.

Если сценарию требуется произвести вывод, он будет сохранен в каталоге / opt / qradar / bin / ca_jail / home / customactionuser.

В данной концепции SIEM будет использована как система сбора событий, и передача их SOAR систему Resilient. В качестве скриптов написанных для SIEM я выбрала следующие наиболее значимые и требующие автоматизации:

Скрипт для проверки работоспособности системы.

Данный скрипт разработан в первую очередь в связи с необходимостью проверки работы системы после каждого обновления или внесения изменений. Для того, чтобы администратор системы мог одним скриптом проверить работоспособность системы.

Для запуска скрипта необходимо выполнить следующее:

1. **Сделать скрипт исполняемым:** chmod +x ./health-check.sh
2. **Запуск:** ./health-check.sh

Устанавливаем соединение с SIEM через по защищённому SSH соединению и в качестве приложения по отправки скрипта использовала WinSCP на рисунке 26 и 27.

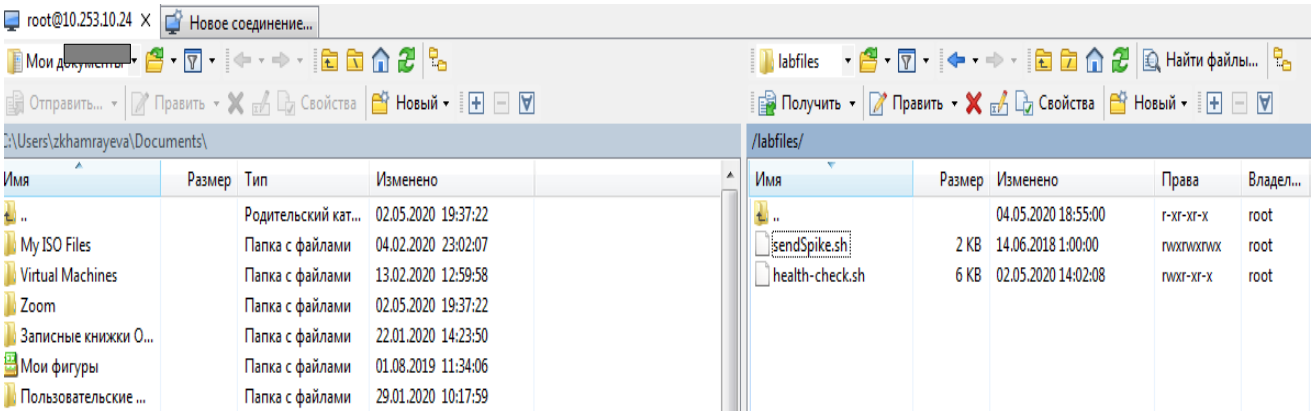

Рисунок 26 – Соединение с сервером

```
[root@icore /]# cd labfiles/
[root@icore labfiles]# ls
sendSpike.sh
[root@icore labfiles]# ls
health-check.sh  sendSpike.sh
[root@icore labfiles]# chmod +x ./health-check.sh
[root@icore labfiles]# ls
health-check.sh  sendSpike.sh
[root@icore labfiles]# ./health-check.sh
```

Рисунок 27 – Создании директории и запуск скрипта

На следующих рисунках 28 показан результат выполнения скрипта

```
[root@icore labfiles]# ./health-check.sh
************************************
        System Health Status
************************************

Print Operating System Details
------------------------------------
Hostname : icore.kz
Operating System : Red Hat Enterprise Linux Server release 7.5 (Maipo)
Kernel Version :  3.10.0-1062.1.1.el7.x86_64
OS Architecture :  64 Bit OS
System Uptime :  up by 4 days 22:14 hours
Current System Date & Time : Mon 04 May 2020 07:43:26 PM +06

Checking For Read-only File System[s]
------------------------------------
.....No read-only file system[s] found.


Checking For Currently Mounted File System[s]
------------------------------------------------------------------------
/dev/mapper/rootrhel-home         on  /home          type  xfs  (rw,noatime,attr2,nobarrier,inode64,logbsize=256k,noquota)
/dev/mapper/rootrhel-opt          on  /opt           type  xfs  (rw,noatime,attr2,nobarrier,inode64,logbsize=256k,noquota)
/dev/mapper/rootrhel-root         on  /              type  xfs  (rw,noatime,attr2,inode64,noquota)
/dev/mapper/rootrhel-storetmp     on  /storetmp      type  xfs  (rw,noatime,attr2,nobarrier,inode64,logbsize=256k,noquota)
/dev/mapper/rootrhel-tmp          on  /tmp           type  xfs  (rw,noatime,attr2,nobarrier,inode64,logbsize=256k,noquota)
/dev/mapper/rootrhel-varlogaudit  on  /var/log/audit type  xfs  (rw,noatime,attr2,nobarrier,inode64,logbsize=256k,noquota)
/dev/mapper/rootrhel-varlog       on  /var/log       type  xfs  (rw,noatime,attr2,nobarrier,inode64,logbsize=256k,noquota)
/dev/mapper/rootrhel-var          on  /var           type  xfs  (rw,noatime,attr2,nobarrier,inode64,logbsize=256k,noquota)
/dev/mapper/storerhel-store       on  /store         type  xfs  (rw,noatime,attr2,nobarrier,inode64,logbsize=256k,noquota)
/dev/mapper/storerhel-transient   on  /transient     type  xfs  (rw,noatime,attr2,nobarrier,inode64,logbsize=256k,noquota)
/dev/sda2                         on  /boot          type  xfs  (rw,relatime,attr2,inode64,noquota)


Checking For Disk Usage On Mounted File System[s]
------------------------------------------------------------------------
( 0-90% = OK/HEALTHY, 90-95% = WARNING, 95-100% = CRITICAL )
------------------------------------------------------------------------
Mounted File System[s] Utilization (Percentage Used):

/dev/mapper/rootrhel-storetmp     /storetmp       2%      ------  OK/HEALTHY
```

Продолжение рисунка 28

```
Checking For Disk Usage On Mounted File System[s]
--------------------------------------------------------------------------------
( 0-90% = OK/HEALTHY, 90-95% = WARNING, 95-100% = CRITICAL )
--------------------------------------------------------------------------------
Mounted File System[s] Utilization (Percentage Used):

/dev/mapper/rootrhel-storetmp     /storetmp       2%      ------  OK/HEALTHY
/dev/mapper/rootrhel-tmp          /tmp            2%      ------  OK/HEALTHY
/dev/mapper/rootrhel-varlog       /var/log        2%      ------  OK/HEALTHY
/dev/mapper/rootrhel-varlogaudit  /var/log/audit  3%      ------  OK/HEALTHY
/dev/mapper/rootrhel-home         /home           4%      ------  OK/HEALTHY
/dev/mapper/rootrhel-var          /var            4%      ------  OK/HEALTHY
/dev/mapper/storerhel-transient   /transient      4%      ------  OK/HEALTHY
/dev/mapper/storerhel-store       /store          17%     ------  OK/HEALTHY
/dev/mapper/rootrhel-root         /               22%     ------  OK/HEALTHY
/dev/sda2                         /boot           23%     ------  OK/HEALTHY
/dev/mapper/rootrhel-opt          /opt            39%     ------  OK/HEALTHY


Checking For Zombie Processes
-------------------------------------
Number of zombie process on the system are : 5

  Details of each zombie processes found
  --------------------------------------
  PID  PPID USER     STAT COMMAND
  438 17338 root     Z    [python] <defunct>
  PID  PPID USER     STAT COMMAND
10321 17338 root     Z    [python] <defunct>
  PID  PPID USER     STAT COMMAND
12018 17338 root     Z    [python] <defunct>
  PID  PPID USER     STAT COMMAND
16194 17338 root     Z    [python] <defunct>
  PID  PPID USER     STAT COMMAND
23400 17338 root     Z    [python] <defunct>
```

```
 id  |             name              | status  | task_status
-----+-------------------------------+---------+-------------
 1001 | QRadar Assistant              | RUNNING | COMPLETED
 1051 | QRadar Log Source Management  | RUNNING | COMPLETED
 1052 | Experience Center             | RUNNING | COMPLETED
 1053 | IBM Resilient QRadar Integration | RUNNING | COMPLETED
(4 rows)

--------------------------------------------------------------------------
App-ID  Name                          Managed Host ID Workload ID          Service Name    AB      Container Name  CDEGH   Port    IJKL
1001    QRadar Assistant              53              apps                 qapp-1001       ++      qapp-1001       +++++   5000    ++++
1051    QRadar Log Source Management  53              apps                 qapp-1051       ++      qapp-1051       +++++   5000    ++++
1052    Experience Center             53              apps                 qapp-1052       ++      qapp-1052       +++++   5000    ++++
1053    IBM Resilient QRadar Integration 53           apps                 qapp-1053       ++      qapp-1053       +++++   5000    ++++

Legend:

Symbols:
n - Not Applicable
- - Failure
* - Warning
+ - Success

Checks:
Service:
A - Service exists in the workload file
B - Service is set to started

Container:
C - Container is in ConMan workload file
D - Container environment file exists
E - Container image is in si-registry
G - Container Systemd Units are started
H - Container exists and is running in Docker

Port:
I - Container IP are in firewall main filter rules
J - Container IP and port is in iptables NAT filter rules
K - Container port has routes through Traefik
L - Container port is responsive on debug path
```

Рисунок 28 – Результат состояния системы

Скрипт на проверку работы firewall.

Частыми инцидентами являются те, что связанные с защитой по сети, одним из защитных методов является правильно настроенный firewall, но существуют атаки, направленные на откаченные правил firewall, или же сотрудники, которые незаконным путём хотят совершать неправомерные действия. Для таких типов инцидентов скрипт выполняет проверку работы firewall на устройстве. В случае если firewall включен, то система выдаст какие порты открыты на рисунке 29.

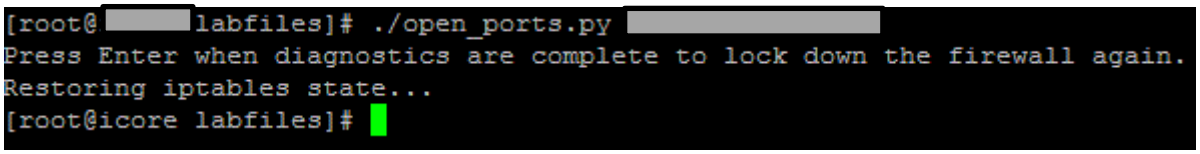

Рисунок 29 – Состояние работы брандмауэра

Скрипт на запись логов.

Обновления SIEM системы не всегда заканчиваются успешно, особенно если пользователь производивший обновление не компетентен, а также в случае расследования инцидентов, связанные с «Zero day». В таком случае используется скрипт, который записывает логи в архив, волнение скрипта на рисунке 32

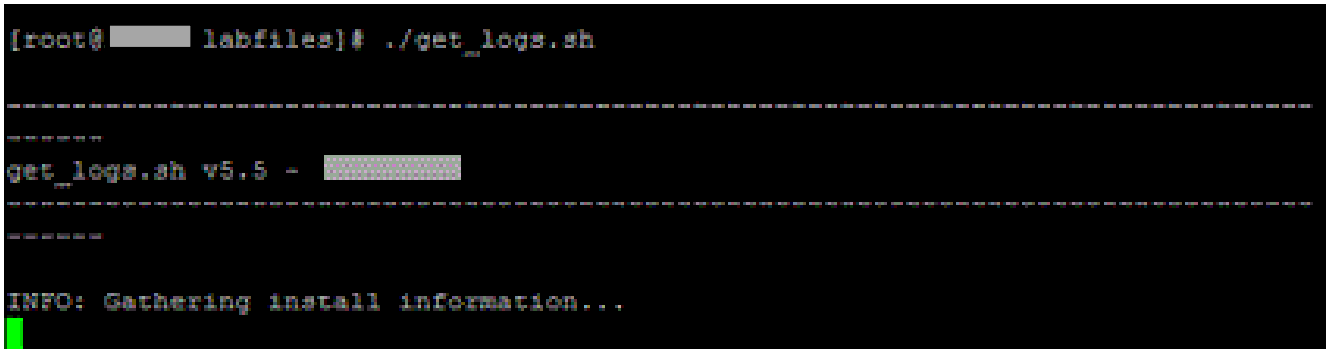

Рисунок 30 – Выполнение скрипта

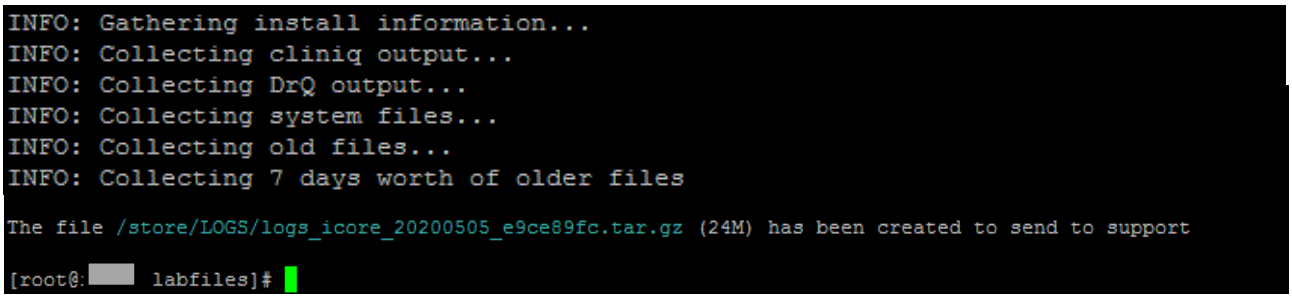

Рисунок 31 – Завершение скрипта

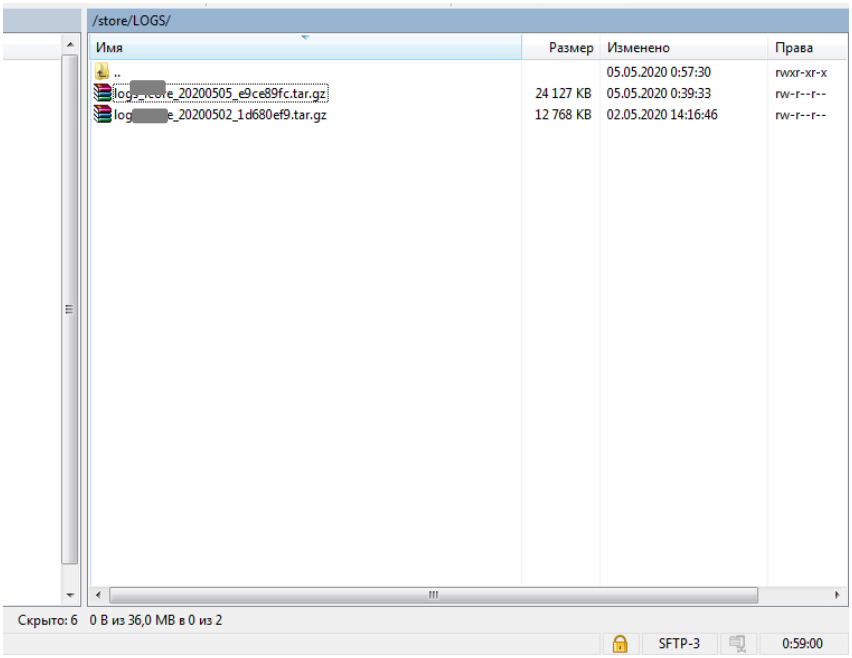

Рисунок 32 – Результат, создание архива с логами

Скрипт для проверки процессов запущенные в системе.

Данный скрипт на риуснке 33 позволяет вывести список пакетов, которые запущенны в системе, дополнением к этому скрипту, возможность того что процессы, которые запущены даже в том случае, когда системно они отключены.

```
[root@ labfiles]# ./wait_for_start.sh
Tue May  5 01:35:14 +06 2020: Waiting for processes 'reporting_executor historic
al_correlation_server qflow.qflow0 accumulator.accumulator assetprofiler.assetpr
ofiler vis.vis0 ariel_proxy_server.ariel_proxy qvmprocessor.IBMVulnerabilityProc
essor ecs-ep ecs-ec ecs-ec-ingress arc_builder offline_forwarder hostcontext ' t
o be running...
+----------------------------+-------+-------+
|Process                     |Seconds|Status |
+----------------------------+-------+-------+
|reporting_executor          |0      |running|
|historical_correlation_server|0      |running|
|qflow0                      |0      |running|
|accumulator                 |0      |running|
|assetprofiler               |0      |running|
|vis0                        |0      |running|
|ariel_proxy                 |0      |running|
|IBMVulnerabilityProcessor   |1      |running|
|ecs-ep                      |1      |running|
|ecs-ec                      |1      |running|
|ecs-ec-ingress              |1      |running|
|arc_builder                 |1      |running|
|offline_forwarder           |1      |running|
|hostcontext                 |1      |running|
+----------------------------+-------+-------+
All 14 managed processes are running.

OK: All processes started after 1 seconds on icore.
[root@ labfiles]#
```

Рисунок 33 – Результат количества процессов

Скрипт, проверяющий правила, которые не используются системой.

В связи с тем, что написанием сценариев могут заниматься несколько человек, то может возникнуть такое, что создаваться множество правил, которые могут либо нагружать систему, либо же которые не работают.

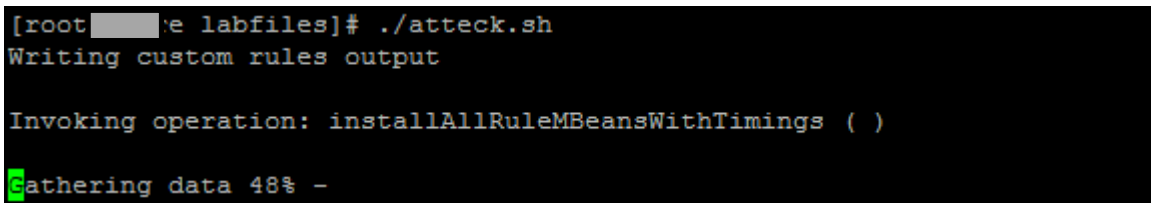

Рисунок 34 – Выполнение скрипта

Скрипт смены пароля для пользователей и администратора.

Данный скрипт необходимо при удаленной работе с сервером, а также для того, чтобы можно было через одну команду заменить пароль и для пользователя, и для администратора, как на рисунке 35.

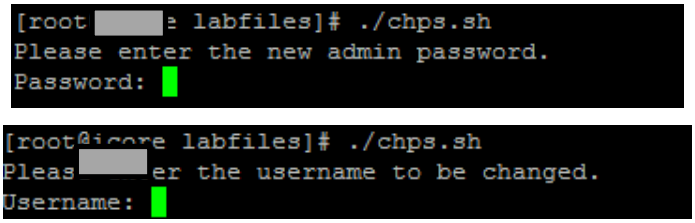

Рисунок 35 – Результат

Скрипт проверки состояния сети.

Данный скрипт совмещает в себе действия, связанные с управлением сетью, работа этого скрипта заключается в том, что берет значения с скриптов системы. Этот скрипт, на рисунке 36 удобен тем, что администратору не нужно, проделывать отдельные действия, связанные с управлением сетью и тем что, происходит внутри нее, то позволяет сократить время проверки.

Рисунок 36 – Скрипт на управление сетью

При выборе первого пункта выводится информации о айпи адресе системы, домен в котором находится система, если система не актива, то ее

статус выводится как неактивным или активным, как на риснуке 37, количество устройств, подключенных к SIEM.

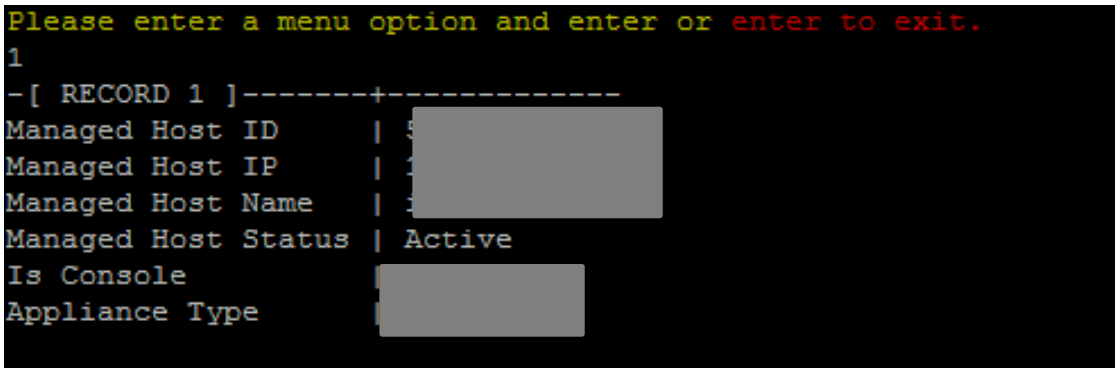

Рисунок 37 – Вывод информации о сети

Следующий пункт дает информацию о состоянии сети системы, а также настройку сети ОС Linux. Пункты скрипта описаны на рисунке 38

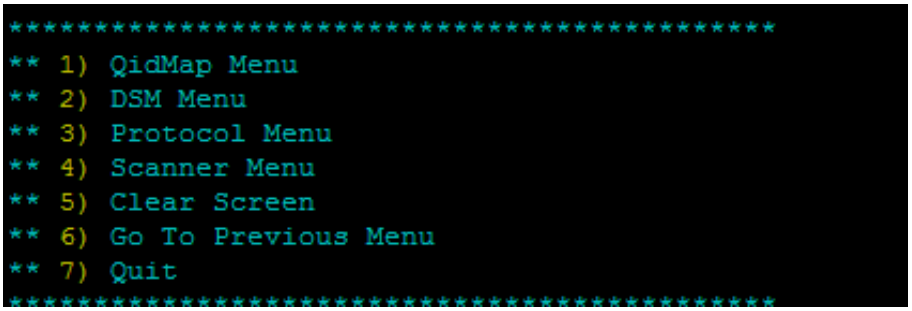

Рисунок 38 – Меню выбора настроек сети

Первый пункт используется в том случае если SIEM подключена с Palo Alto, так как в моём случае нет интеграции с Palo Alto, просмотрим вкладку номер два.

Вторая вкладка дает информации об инцидентах, событиях и сопоставление инцидентов с устройствами, которые подключены к системе. Первым пункт, показывает всю информацию про инцидент, которые имеются в системе. Указывается номер инцидента, который необходимо просмотреть и выдается вся информация по инциденту, что показано на рисунке 39.

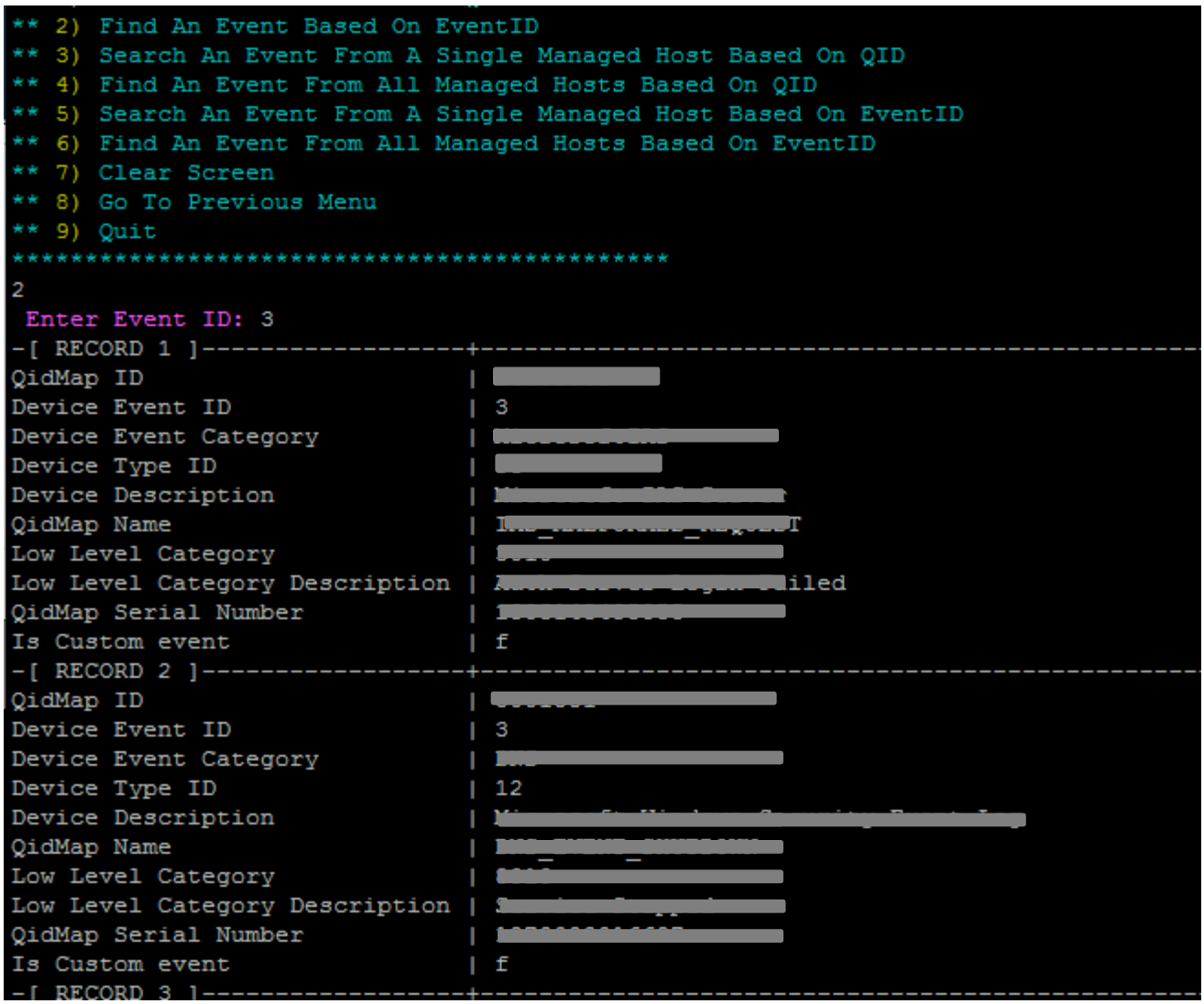

Рисунок 39 – Информация по инциденту

Далее выбираем пункт сопоставления инцидент с устройством, откуда поступил инцидент, айпи адрес и номер иниудента на риснуке 40.

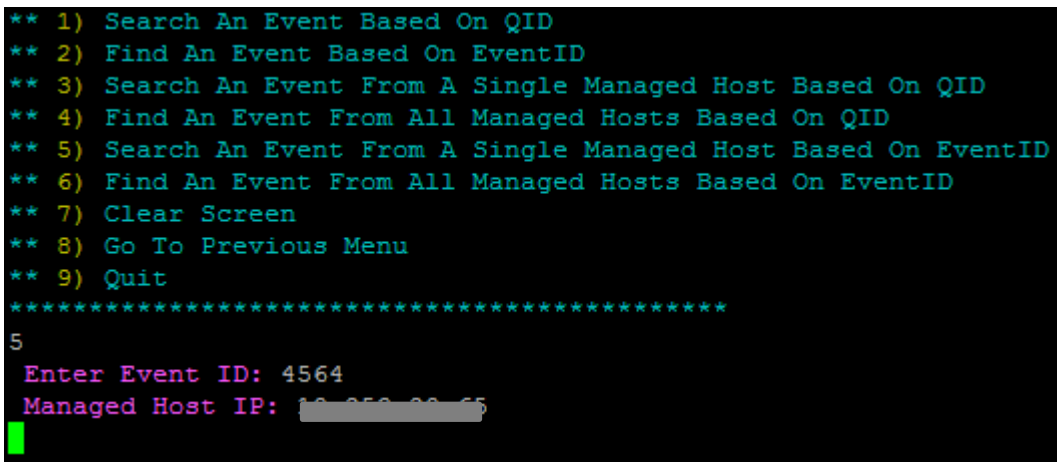

Рисунок 40 – Сопоставление инцидента с устройством

На рисунке 41 показан результат выполнения данного скрипта, как видно из рисунка выводится информация обо всех инцидентах, которые предоставило устройство.

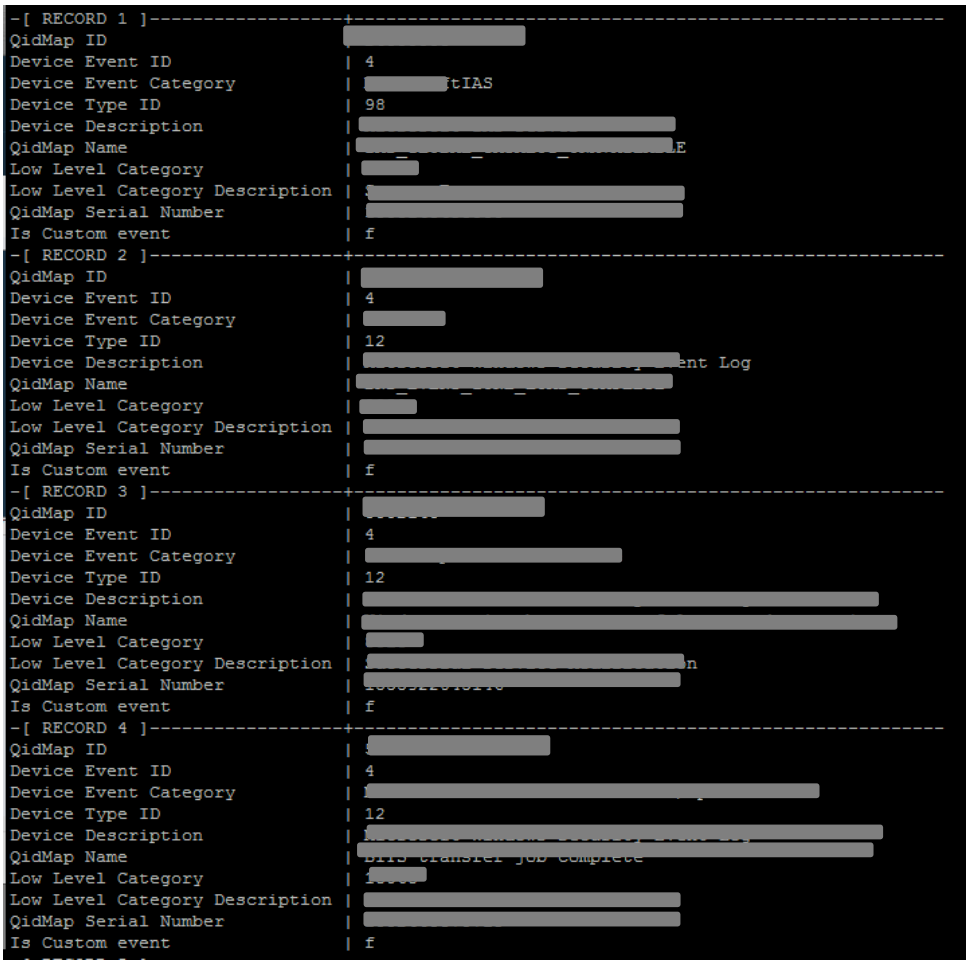

Рисунок 41 – Информация об инцидентах

Далее просмотрим вкладку на рисунке 42, которая сканирует состояние системы, в данной вкладке необходимо только знать, что вы хотите просканировать, например, можно просмотреть состояние ip сетки.

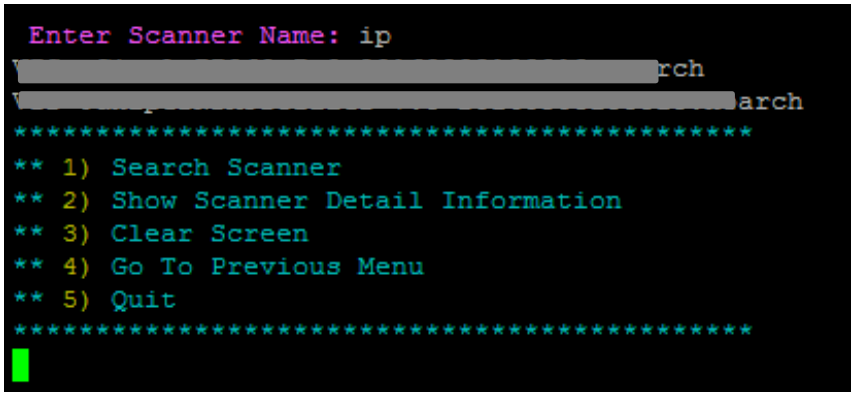

Рисунок 42 – Получение информации от сканера

2.2 Настройка системы SOAR Resilient

После того, как инцидент был зафиксирован в SIEM системе, он перенаправляется в систему Resilient с помощью, которой расследование инцидента происходит намного быстрее и эффективнее.

Также как в QRadar система Resilient имеется множество настроек для управления инцидентами.

Для начала создадим роли и группы пользователей, для того, чтобы разграничь их права пользования системой.

Роль – это определенный набор разрешений, который можно назначать пользователям и группам. Вкладка «Роли» позволяет определять роли и управлять ими.

Роли и их разрешения будут сгруппированы по следующим категориям:

а) **разрешения на администрирование и настройку.** Эти разрешения применяются только к глобальным ролям. За исключением двух разрешений, эти разрешения представляют собой вкладки, доступные из пунктов меню «Настройки администратора» или «Настройки». Пользователи, у которых нет этих разрешений, не видят Настройки администратора или Настройки меню Настройки. Исключениями являются общие панели мониторинга и фильтры, которые позволяют пользователям совместно использовать свои собственные аналитические панели мониторинга и поисковые фильтры, а также разрешение на управление страницами вики, которые позволяют пользователям создавать, редактировать и удалять вики-страницы;

б) **разрешения на инциденты.** Эти разрешения применяются как к глобальным, так и к рабочим ролям. Они определяют, как пользователи взаимодействуют с различными функциями инцидентов во всех инцидентах. Вы должны предоставить эти разрешения роли, в которой пользователю необходимо получить доступ к инцидентам или управлять ими, если пользователь не обязательно является владельцем инцидента или участником. По умолчанию пользователям, которым не назначена роль, могут быть назначены инциденты, и они могут управлять этими инцидентами, когда участник или владелец инцидента;

в) **разрешения на симуляцию.** Это разрешение применяется только к глобальным ролям. Он определяет, могут ли пользователи создавать симуляции. Он может работать с разрешениями инцидентов или независимо от них. Пользователи с этим разрешением имеют возможность создавать моделирования в рабочем пространстве по умолчанию или выбирать другое рабочее пространство, если у них есть разрешения Создать инциденты для этого рабочего пространства и если поле рабочего пространства добавлено в новый макет инцидента. Пользователи без этого разрешения не видят меню Create> Simulation. Если у роли есть разрешения «Создать симуляции», но нет разрешений «Создать инцидент», если они нажимают «Создать» в меню, они видят экран «Создать симуляцию». Если у пользователя есть разрешение создать инцидент и Создать симуляции. Можно выбрать, создавать ли новый инцидент

или симуляцию с помощью кнопки «Создать» в главном меню. Только пользователи с разрешением Удалить инциденты могут удалять симуляции;

г) **входящие разрешения.** Эти разрешения применяются только к глобальным ролям. Они определяют, могут ли пользователи получать доступ к почтовым ящикам и электронным письмам во входящих. Предоставьте эти разрешения роли, где пользователям необходимо просматривать и сортировать электронные письма из входящих подключений электронной почты. Пользователи без этих разрешений не видят Входящие или электронные письма в Входящие Проверьте разрешение Входящие Входящие, чтобы предоставить разрешения для роли, чтобы позволить пользователю просматривать содержимое почтового ящика. Установите флажки «Загрузить электронную почту» и «Удалить электронную почту», чтобы предоставить разрешения ролям для загрузки содержимого электронной почты и удаления сообщений электронной почты из папки «Входящие».

На рисунке 43 ниже показаны пользователи, входящие в систему всего их будет 9.

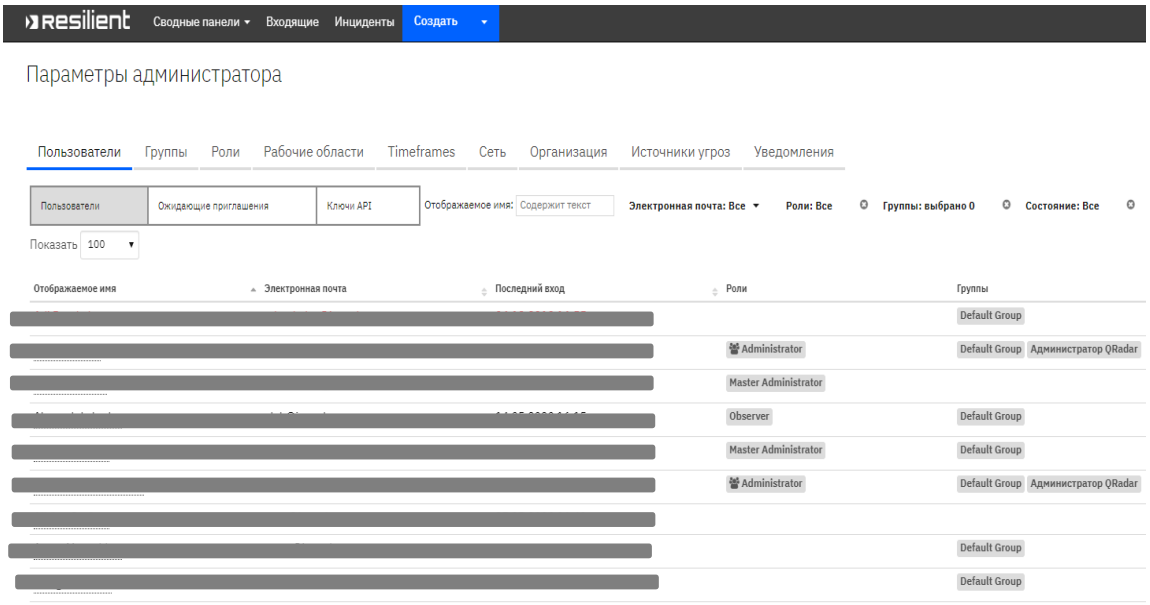

Рисунок 43 – Группы пользователей

Пользователей Admininstrator – имеет право настраивать систему, создавать скрипты, вносить изменения в саму систему, делать ее бэкап, и обновлять. Но не имеет права на создание инцидента его редактирование и расследования.

Пользователь Master Administrator – обычно такие права дают менеджеру группы реагирования, так как пользователь с такими права может полностью настраивать систему, взаимодействовать с инцидентами.

Пользователь Observer/Owner – данные пользователи имеют права на работу с инцидентами и только, то есть настраивать систему или менять какие-то ее параметры они не имеют права.

Далее настроим Сводные панели, на которых будет отражаться вся текущая информация об системе и инцидентах, которые имеются.

Первым виджетом, который добавляется на панели сводки, будет количество инцидентов на рисунке 44, которые имеются в систему, а также пользователи, которые активны на данный момент времени.

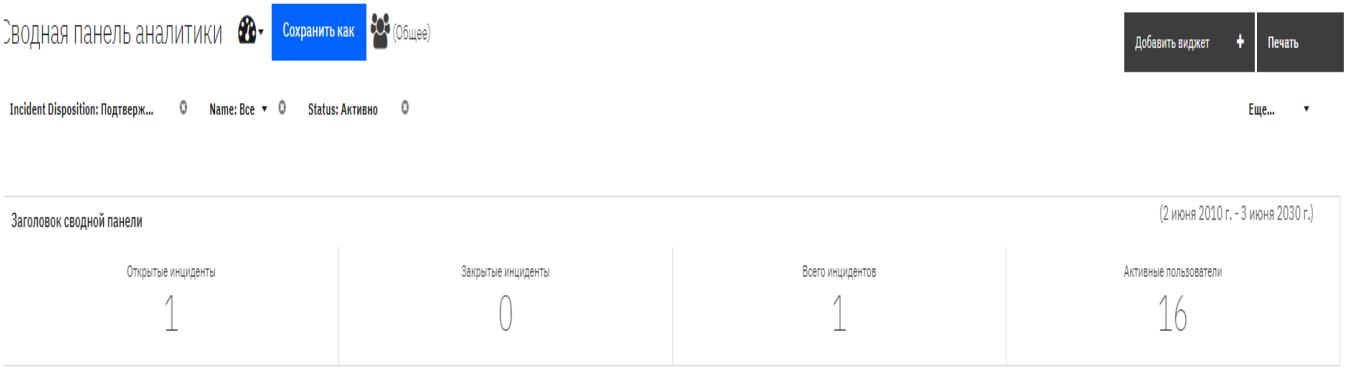

Рисунок 44 –Сводная панели аналитики

Ниже виджеты отвечающие за показ всей информации касающиеся инцидентов, то есть количество открытых и закрытых, временные рамки для инцидентов, а также показ инцидентов по степени серьезности на рисунке 45. И в продолжении виджетов об инцидентах добавляется еще виджет временной диаграммы и информацию об пользователях и какие инциденты за ними закреплённые на рисунках 46 и 47.

Открытые инциденты по этапу

Приоритетность	Начало	Начало расследования инцидента	Определение угрозы и Анализ	Реагирование	Выводы и отчётность	Final Phase	Завершение	Всего
Zero	0	0	0	0	0	0	0	0
Низкий	0	1	0	0	0	0	0	1
Средний	0	0	0	0	0	0	0	0
Высокий	0	0	0	0	0	0	0	0
Catastrophic	0	0	0	0	0	0	0	0
Нарушение	0	0	0	0	0	0	0	0
Преступные действия	0	0	0	0	0	0	0	0

Рисунок 45 – Количество открытых инцидентов

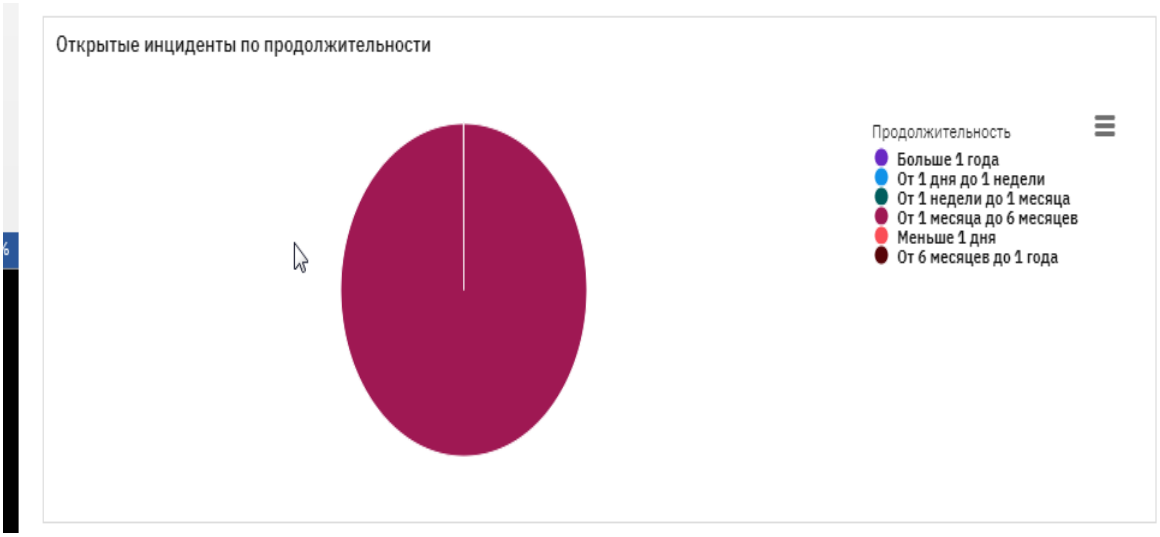

Рисунок 46 – Диаграмма окружности открытых инцидентов с временными рамками

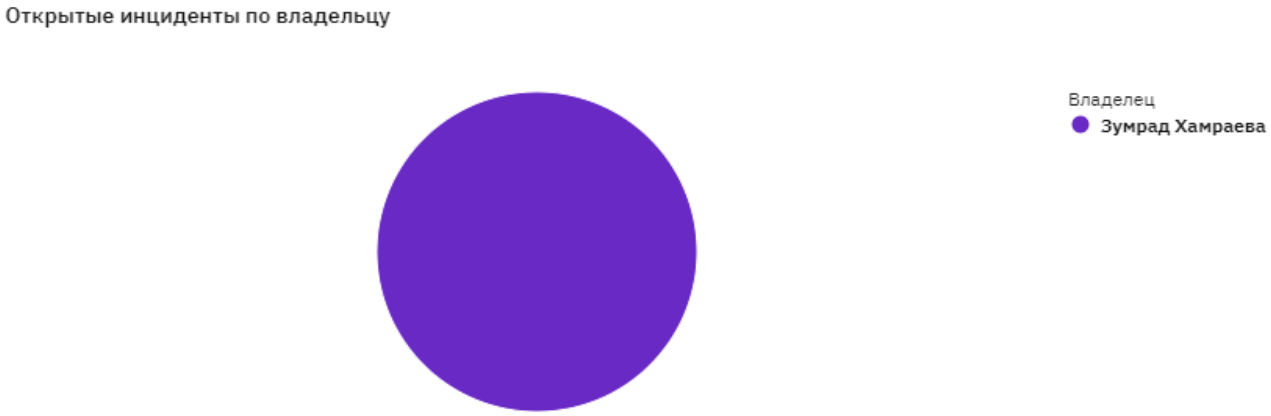

Рисунок 47 – Панель информации об инцидентах

После настройки, части помогающая визуально увидеть инциденты и всю информацию, настраиваем часть автоматизации действий сотрудников команды реагирования.

2.2.1 Написание скриптов для управления инцидентами

Написание и редактирование скриптов, позволяют настраивать инциденты и получать информацию об инцидентах и других типах объектов. Затем можно вызвать скрипт из правила или рабочего процесса.

Вкладка «Сценарии» позволяет просматривать, редактировать и создавать сценарии. На вкладке представлена следующая информация:

а) имя. Нажав на название скрипта, можно просмотреть его детали или отредактировать скрипт. При редактировании или создании сценария необходимо ввести имя, которое описывает назначение сценария;

б) описание. Текст для описания сценария;

в) тип объекта. При назначении сценарий для одного типа объекта, например, инцидента, заметки, вехи, задачи, вложения, артефакта, таблицы

данных или сообщения электронной почты. Тип объекта определяет контекст данных, предоставляемых сценарию;

г) правила. Список правил, которые вызывают скрипт. Любые отключенные правила показаны красным;

д) значок корзины. Для удаления срипта. Если на скрипт ссылаются в правиле, нужно удалить его из правила, прежде чем сможете его удалить.

Функция сценариев поддерживает только Python 2.7 и имеет следующие языковые функции и ограничения безопасности для предотвращения нежелательных действий.

Получая доступ к различным данным об инцидентах, используете сценарии для добавления объектов, таких как задачи, заметки и строки в таблицу данных. Сценарий только изменяет или действует на объект, который вызвал правило или его родительский объект. Для объекта сообщения электронной почты он также может изменить связанный с ним инцидент (если он есть).

Доступ к объектам Resilient при написании скрипта. Эти объекты отражают данные объекта действия, а некоторые содержат вспомогательные методы. Обратите внимание, что функция скрипта может получить доступ ко всем объектам, доступным в виде типов объектов, а также к дополнительным объектам.

При написании сценария необходимо ввести объект, например, «инцидент». или «задача», чтобы отобразить доступные значения поля. Чтобы увидеть настраиваемые поля «ident.properties. ».

Чтобы написать скрипт, перейдите на вкладку «Сценарии» проделываются следующие действия:

а) выбор кнопки «Новый скрипт»;

б) ввод описательное имя для сценария;

в) описание цели сценария;

г) выбор тип объекта. При выборе таблицы данных, также выбрать конкретную таблицу данных.

Скрипт для вывода информации об инциденте.

Данный скрипт необходим в связи с тем, что в систему поступает множество инцидентов и для того, чтобы аналитику было проще найти инциденты, владельцами которых они являются в временном промежутке. Пример выполнения скрипта показан на рисунке 48, а вывод информации 49.

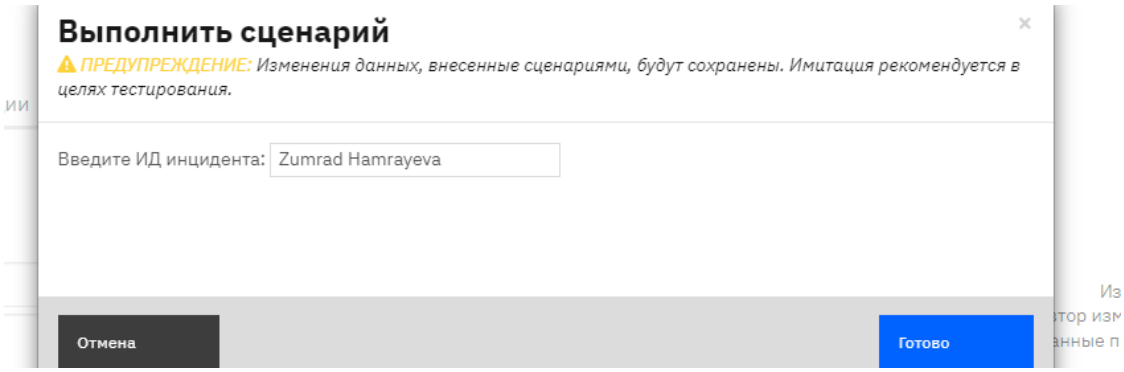

Рисунок 48 – Написание имени аналитика

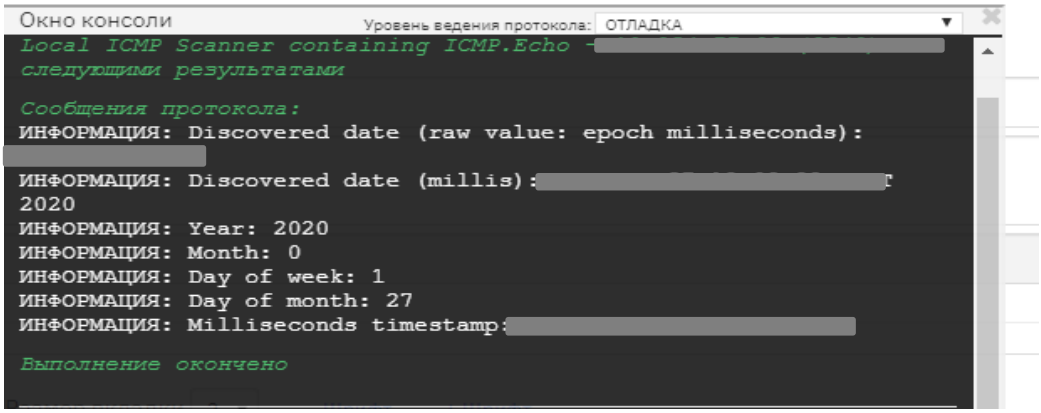

Рисунок 49 – Вывод временной информации связанных инцидентов

Скрипт на вывод информации об инциденте.

Если первый скрипт выводил данные временных промежутков инцидента, то этот выводит полностью всю информацию об инциденте на рисунке 50 и 51.

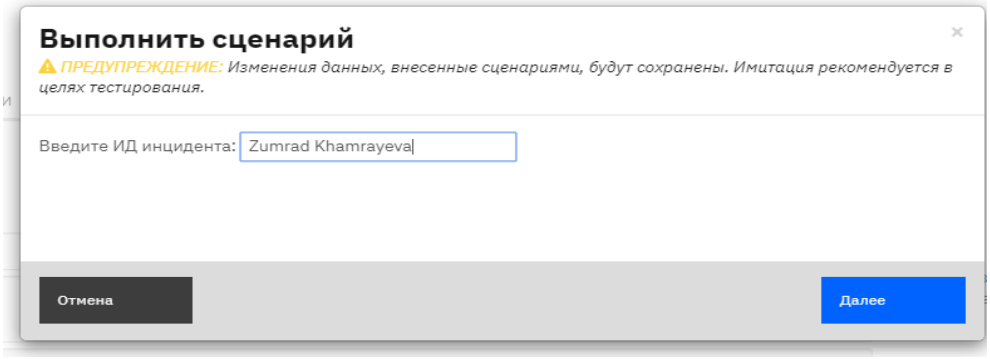

Рисунок 50 – Введение имя аналитика

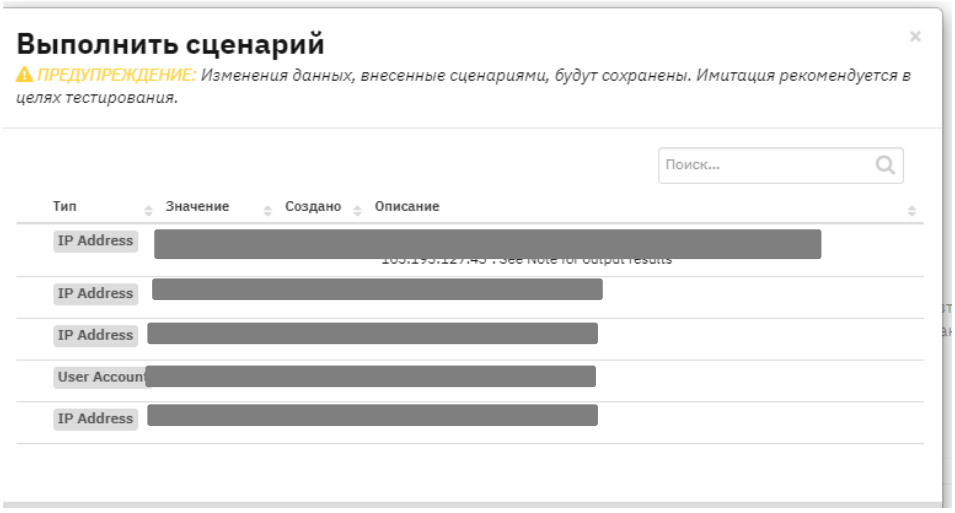

Рисунок 51 – Вывод информации об инцидентах аналитика

Скрипт на изменение владельца инцидента.

В случае, когда аналитик не может решить какой-либо инцидент, для того, чтобы перенаправить этот инцидент другому специалисту в системе придется заново создать инцидент, но с помощью данного скрипта на рисунке 52, можно поменять владельца инцидента на рисунке 54 при этом аналитик переназначавший инцидент остается как наблюдатель и может также вносить правки при расследовании.

Рисунок 52 – Владелец инцидента

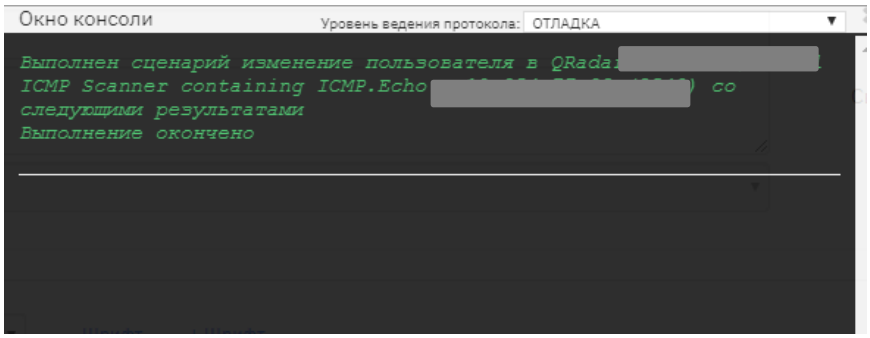

Рисунок 53 – Выполнение скрипта

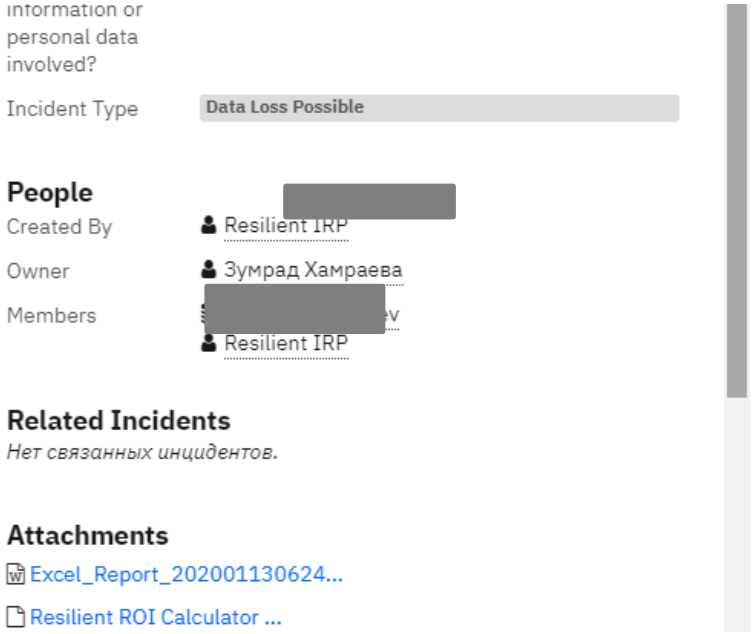

Рисунок 54 – Изменение владельца инцидента

Скрипт, определяющий заметки и артефакты, принадлежащие инциденту.

При создании инцидента ему присваиваются артефакт и пишутся заметки, есть случаи, когда артефакт может принадлежать нескольким инцидентам и также заметки могут ссылаться на другие инциденты, для того чтобы аналитику было проще просматривать все артефакты на рисунке 55, связанные с инцидентами.

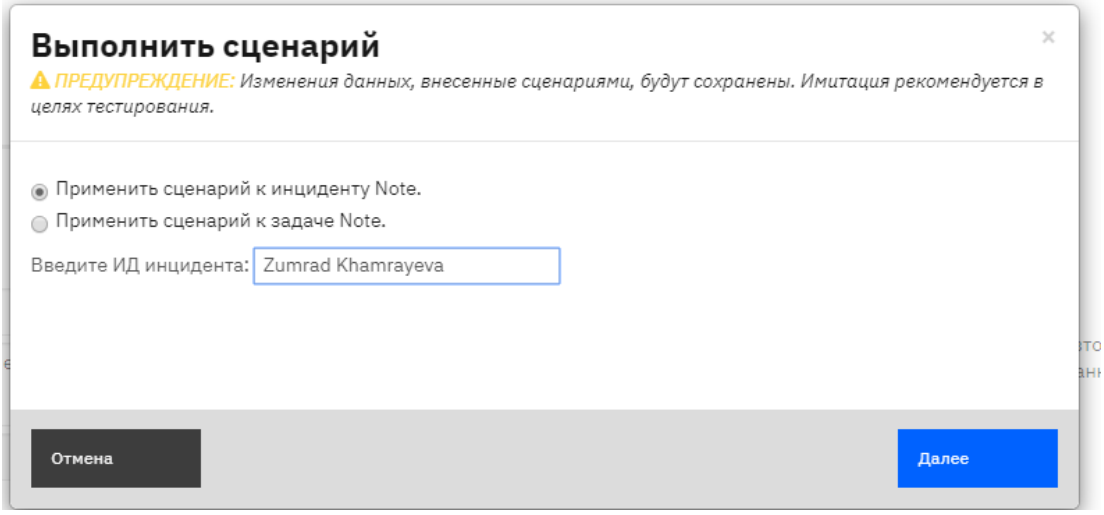

Рисунок 55 – Вписываем либо владельца, либо айди инцидента

После этого выводится полная информация с артефактами и заметки связанных инцидентов на рисунке 56.

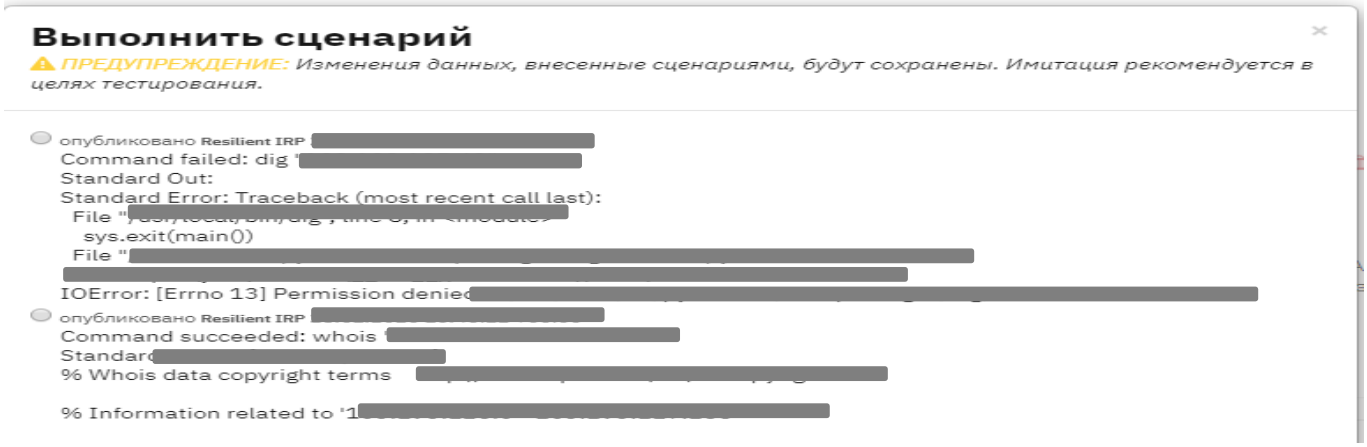

Рисунок 56 – Артефакты по инцидентам

Скрипт, определяющий действия, связанные с инцидентом.

Для, того чтобы было легче отслеживать действия на рисунке 57 происходящие с инцидентом, и информацию об последних изменениях.

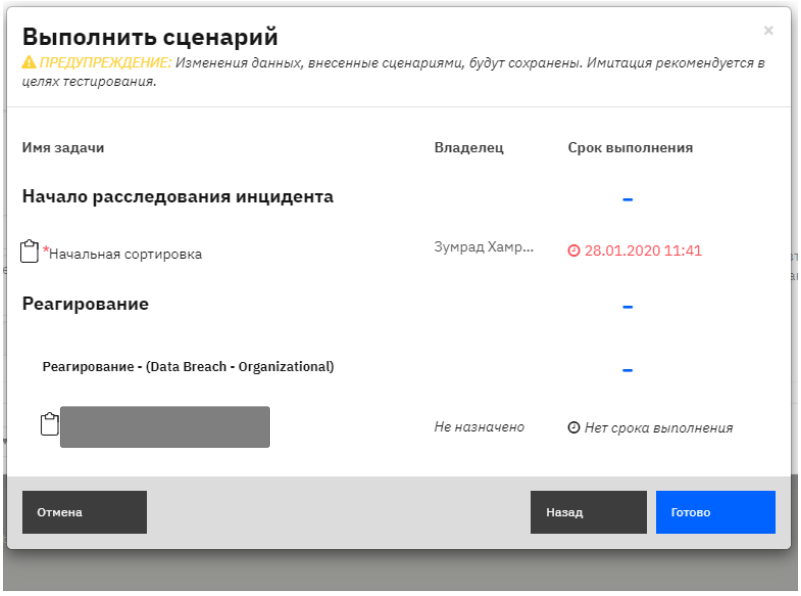

Рисунок 57 – Информация об инциденте

Скрипт для автоматического создания инцидента.

Этот скрипт на рисунке 58 обрабатывает входящие сообщения электронной почты. Сценарий создает инцидент из сообщения электронной почты, добавляет артефакты к инциденту на основе информации в теле сообщения и добавляет любые вложения электронной почты к инциденту.

```
# The new incident owner - the email address of a user or the name of a group and cannot be blank.
# Change this value to reflect who will be the owner of the incident before running the script.
newIncidentOwner = "

# Whitelist for IP V4 addresses
ipV4WhiteList = [
```

Рисунок 58 –Запись электронной почты пользователя

После запуска скрипта владельцу приходит уведомлении о добавлении инцидента на рисунке 59.

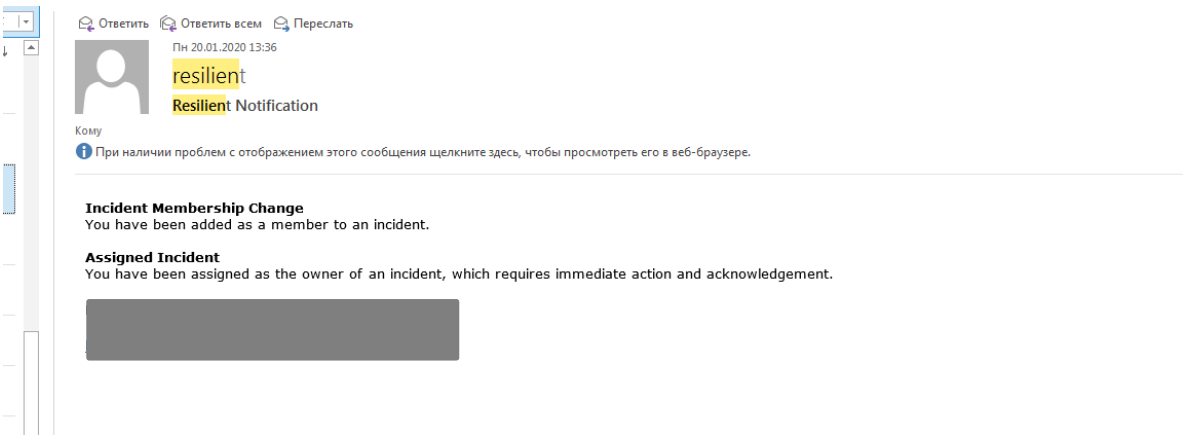

Рисунок 59– Уведомление системы

Выводы: При выполнении практической части, были реализованные поставленные задачи по реализации концепции «Умный офис». Основной идеей данной концепции является быстрое реагирование на инциденты ИБ, а также сокращение времени на выполнение стандарты задача при расследовании инцидентов командной реагирования на инциденты. Полностью была описана архитектура, с помощью которой должна работать SIEM система и как ее компоненты взаимосвязаны, а также подключение SIEM системы с SOAR. С помощью написания скриптов и настройкой правил в системе SIEM, были выполнены задачи по автоматизации стандартах действий по реагированию, а также помощь администраторам при настройке самой системы, также была полностью интегрирована система SOAR с помощью, которой, команда реагирования может работать более эффективно. Данная система была полностью настроена, созданы пользователи и обозначены их роли, также созданы специальные сводные панели, которые показывают всю необходимую информацию по инцидентам для аналитика. Кроме этого были написаны скрипты с помощью которых аналитик, может просматривать всю информацию по инцидентам, менять их и добавлять тем самым действия по управления сокращается к минимуму.

3 Расчет проектных рисков

Проектирование означает создавать, моделировать, выполнять или конструировать в соответствии с планом.

Проектирование бизнес-системы – это набор проектных документов и вспомогательных материалов, которые определяют функциональные возможности системы, которые поддерживают один или несколько бизнес-процессов и в процессе, создают, извлекают, обновляют и удаляют данные.

При успешном проектировании систем необходимо учитывать и эффективно управлять тремя основными компонентами. Это качество, своевременность и экономическая эффективность. Этот трехсторонний подход помогает как командам разработчиков, которые становятся более осведомленными о приоритетах руководства, так и руководителям проектов, которые вынуждены принимать более реалистичный взгляд на процесс проектирования системы с точки зрения качества, стоимости и значимых сроков.

Существует целый ряд проблем и неопределенностей, с которыми сталкиваются те, кто работает над проектами. Стратегия управления рисками является ключом к прогнозированию и решению широкого спектра проектных рисков. Таким образом, проектирование рисков должна осуществляться не изолированно, а как неотъемлемая часть общего процесса управления рисками проекта. Конечно, сам дизайн также может представлять риск для проекта; например, ошибки в расчетах, имеющих решающее значение для безопасности информационной системы, должны быть устранены, например, путем использования режимов проверки и предоставления соответствующего уровня контроля менее опытному персоналу.

Неспособность управлять проектным риском может иметь следующие последствия:

а) потеря или неспособность достичь интересов потребителей и клиентов (системы, обращенные вовне);

б) при использовании бизнес-системы из-за отсутствия интереса;

в) неэффективное представление бренда, возможно нанесение ущерба деловой репутации;

г) невозможность компенсировать затраты, связанные с развитием бизнес-системы;

д) неспособность компенсировать затраты на поддержание бизнес-системы.

Спроектированная в дипломном проекте концепция «Умный офис» создавалась с «нуля» и в этом случае необходимо провести анализа всех рисков, которые могут возникнуть при внедрении данного проекта.

При проведении анализа проектных рисков сначала определяются вероятные пределы изменения всех его «рисковых» факторов (или критических переменных), а затем проводятся последовательные проверочные расчеты при допущении, что переменные случайно изменяются

в области своих допустимых значений.

На основании расчетов результатов проекта при большом количестве различных обстоятельств анализ риска позволяет оценить распределение вероятности различных вариантов проекта и его ожидаемую ценность (стоимость).

Риск, связанный с проектом, характеризуется тремя факторами: событие, связанное с риском; вероятность риска; сумма, подвергаемая риску.

3.1.1 Идентификация основных активов информационной системы

Основными активами, которые будут использованы для реализации данной концепции являются:

1. Сервер, на котором будет разворачиваться система.
2. SIEM система IBM QRadar.
3. Конечные точки, которые будут подключены.
4. Все компоненты входящие в ЛВС Компании.
5. Сотрудники использующие данную систему.

3.1.2 Оценка проектного риска

Одним из первых шагов, чтобы определить потенциальные риски, связанные с любым аспектом проекта, то есть определить вероятность возникновения какое-либо риска. Для определения вероятность воспользуемся качественным методом определения вероятности для оцифровки вероятности составим таблицу 7, в которой будем использовать числовую оценку от 1 до 3 [9].

Таблица 7 – Шкала вероятности рисков

Шкала вероятности рисков			
Вероятность реализации риска %	Сценарий	Числовая оценка	Потери
от 1 до 45	низкая	1	стоимость свыше 1500 000 тг
от 46 до 67	средняя	2	стоимость до 1000 000 тг
от 68 до 99	высокая	3	стоимость до 100 000 тг

Следующим шагом определяем уязвимости и угрозы, которые могут возникнуть в ходе выполнения проектирования. Ниже описаны основные уязвимости и угрозы:

1. Угроза – Не понимание заказчиком функционирование системы – На стадии написания технического здания заказчик может требовать от системы того функционала, который она не выполняет в связи с чем создаются проблемы с отсутствием понимания, дублированием задач и выполнение взаимоисключающих задач и т.д.

2. Угроза – Увеличение сроков выполнения работ. Тратиться много времени на сборку и проектирование системы в связи с тем, что сотрудники ответственные за конфигурацию системы опаздывают либо возникли угрозы человеческого фактора, что может привести к остановке проекта.

3. Угроза – Потеря первоначальных инвестиций. Некорректно сформированный бюджет проекта при планировании финансовых затрат.

4. Угроза – Сложность приема результатов работ. В процессе проектирование заказчик может потребовать выполнения несогласованных работ, что может привести к рассогласованию мнений заказчика с исполнителем.

5. Угроза – Несоответствие результатов проекта ожиданиям заказчика. Неполнота исходной информации о работе бизнес процессов и отсутствие полной информации о работе информационной системы заказчика.

6. Угроза – Плохая коммуникация с заказчиком. Заказчик пропадает на несколько дней, что привод к тому что, заверить какой-либо этап работы может сдвинуться.

7. Угроза – Нестабильность технических мощностей заказчика. Сервера, компании заказчик могут работать нестабильно, что может привести к тому что систему придется переконфигурировать заново систему, либо же при сдаче конечного результата сервер может упасть.

8. Угроза – Неквалифицированные сотрудники со стороны заказчика – Такие сотрудники могут вносить изменения в архитектуру или код проекта, не предупреждая исполнителя и тратиться время на откаты и разбирательства.

9. Угроза – Атаки на проект вовремя его администрирования. Возможно возникновение атак на систему как внешними та и внутренними злоумышленниками, что приводит к потери данных, которые находились в системе на этапе ее поддержки.

10. Угроза – Проблемы при интеграции с уже существующими технологиями. Заказчик может не дать полную информацию об информационно системе, что может привести к трудностям интегрирования двух систем.

11. Угроза – Неисправность SVN сервера. ЫМТ находит на стороне заказчика, может возникнуть, что данный сервер упадет, и поднять его займет время, что приводит к задержке работы

После того, как были определены основные угрозы и уязвимости для активов, необходимо определить степень влияния рисков возникшие в результате данных угроз. Определение степени влияния по 4 аспектам: цели, срок, бюджет и качество. Для их описания можно использовать вот такую матрицу влияния на таблице 8.

Таблица 8 – Шкала влияния рисков

Шкала влияние риска на проект					
Кол.оценка	**Кач.оценка**	**Перерасход средств (стоимость)**	**Сроки**	**Содержание проекта**	**Качество**
1	очень низкая	до 5%	незначительное увеличение времени (Сдвиг на 1 месяц)	Едва заметное уменьшение содержания	Едва заметное понижение качества
2	низкая	от 5 до 20%	увеличение времени на <10% (Сдвиг на 1-3 месяца)	Затронуты второстепенные области содержания	Затронуты только самые трудоемкие приложения
3	умеренная	от 20 до 40%	увеличение времени от 10-20% (Сдвиг на 3-5 месяца)	Затронуты основные области содержания	Для понижения качества требуется одобрение заказчика
4	высокая	от 40 до 60%	увеличение времени 20-40% (Сдвиг на 6 месяцев)	Уменьшение содержания не приемлемо для заказчика	Понижение качества не приемлемо для заказчика
5	очень высокая	свыше 60%	увеличение времени> 40% (Сдвиг более чем на 6 месяца)	Конечный проект фактически бесполезен	Конечный проект фактически бесполезен

Для расчета общего влияния риска на проект будем использовать формулу [9]:

$$\text{Влияние} = \frac{(\text{Срок}+\text{Бюджет}+\text{Содержание}+\text{Качество})}{4} \quad (1)$$

Построим таблицу 9, где будут все указаны все угрозы на уязвимости активов, также степень влияния этих угроз и уязвимостей на актив.

По данной таблице 9 уже можно сделать выводы каике угрозы и уязвимости являются критичными, а какие являются менее критичными

Таблица 9 – Угрозы, уязвимости и риск проекта

№	Угроза	Описание уязвимость	Оценка	Перерасход средств	Сроки	Содержание проекта	Качество проекта	Меры по обработке	Итог Влияния риска на проект
1	Не понимание заказчиком функционирование системы	Выбор системы заказчиком был без понимания требований к нему и его функционирования	5	4	4	4	4	При проведении тендера, подробно описать функционал системе, а также провести коуч для заказчика, чтобы он понимал, как работает система	4
2	Увеличение сроков выполнения работ	Тратиться много времени для сборки и проектирования системы в связи с недооценкой сложности работ	5	3	3	3	2	Определение высококвалифицированных сотрудников, а также детализация задач для проектировщиков	2
3	Потеря первоначальных инвестиций	Некорректно сформированный бюджет	4	4	3	3	3	Корректное формирование бюджета проекта, планирование финансового резерва.	2

Продолжение таблицы 9

4	Сложность при приеме результатов работ	В процессе проектирование заказчик может потребовать выполнения несогласованных работ.	5	3	4	5	5	Отправка отчетов со стороны исполнителя о проделанных работах	1
5	Несоответствие результатов проекта ожиданиям заказчика	Неполнота исходной информации о работе бизнес процессов и отсутствие полной информации о работе информационной системы заказчика.	3	2	3	3	2	Составление чётких условий выполнения работ	3
6	Плохая коммуникация с заказчиком	Заказчик пропадает на несколько дней	4	4	3	3	2	Назначение ответственного лица за сроки проекта	3
7	Нестабильность технических мощностей заказчика	Сервера, компании заказчик могут работать нестабильно, что может привести к тому что систему придется переконфигурировать заново систему.	5	3	3	2	2	Установка заказчику технологий поддерживающие мощности для системы	1

Продолжение таблицы 9

8	Неквалифицированные сотрудники со стороны заказчика	Сотрудники со стороны заказчика вносят изменения в архитектуру или код проекта, не предупреждая исполнителя.	5	3	3	2	2	Оговаривание условий внесения изменений в архитектуру проекта	3
9	Атаки на проект вовремя его администрирования	Возможно возникновение атак на систему	3	1	2	2	1	Создание дампа системы, проверка логов и т.д.	2
10	Проблемы при интеграции	Заказчик может не дать полную информацию об информационно системе	4	4	3	3	2	Проверка аудитом все информационные системы, находящиеся в компании заказчика	2
11	Неисправность SVN сервера	SVN находит на стороне заказчика, может возникнуть падение сервера	3	2	3	2	2	Назначение администратора SVN сервера, со стороны заказчика	3

Используя заполненную выше таблицу 9, можно определить последствия влияние на проект рисков определим, на какую величину они могут возрасти. Риски, связанные с персоналом их квалификацией и коммуникации с заказчиком может привести к увеличению объёмов работ в среднем более чем на 50% от запланированного. Это означает, что оценка влияния на содержание проекта будет от 4 до 5 балла. Если проект продолжается около 1 года, а содержание изменится более чем на 60%, то (если не увеличится объем ресурсов) можно спрогнозировать увеличение сроков примерно на тот же процент, что и содержание проекта. Поэтому для календарного графика поставим оценку в 5 баллов. В связи с ростом объемов работ более чем на 50% бюджет проекта, очень вероятно, также изменится более чем на 50%. Присваиваем такому аспекту, как перерасход средств оценку в 4 балла. На качество продуктов проекта рост объемов работ оказывает влияние, так как поломка сервера приведет к полной настройке системы заново. Аспекту качество проекта присваивается оценка в 4 баллов. Последствием такого, риска является увеличение объемов работ.

Риски, вязанные с календарным графиком проекта. Установка жестких графиков проекта и несвоевременная сдача этапов проекта приводит к дополнительным штрафам, свыше чем на 60% от запланированного. Это означает, что оценка влияния на содержание проекта будет 5 баллов. Если поддержка проекта продолжается около 1 года, а содержание не изменится, то (если не увеличится объем ресурсов) можно спрогнозировать увеличение техподдержке примерно на тот же процент, что и содержание проекта. Поэтому для календарного графика поставим оценку в 4 баллов. В связи с тем, что графики работы проекта сбиты, это принес вред бюджету проекта, на суммы более чем на 30%. Присваиваем такому аспекту, как перерасход средств оценку в 4 балла**.** На качество продуктов проекта рост объемов работ оказывает большое влияние, так как установка может привести к дополнительным работам, но на качество повлияйте в умеренных цифрах. Аспекту качество проекта присваивается оценка в 4 балла. Последствием такого, риска является увеличение времени на проектировку проекта.

Используя данные формулировки можно оценить какие риски являются важными и объяснить руководству, наглядно показывая проценты увлечения работа в случае возникновения рисков.

3.1.3 Сопоставление рисков

После расчетов вероятности и влияния используем формулу расчета важности риска [9].

$$\text{Важность риска} = \text{Вероятность} \times \text{Влияние} \qquad (2)$$

Таблица 10 – Расчет важности риска

№	Угроза	Описание уязвимость	Влияние риска на проект	Вероятность возникновения риска	Важность риска
1	Не понимание заказчиком функционирование системы	Выбор системы заказчиком был без понимания требований к нему и его функционирования	4	2	8
2	Увеличение сроков выполнения работ	Тратиться много времени для сборки и проектирования системы в связи с недооценкой сложности работ	2	3	6
3	Потеря первоначальных инвестиций	Некорректно сформированный бюджет	2	2	4
4	Сложность при приеме результатов работ	В процессе проектирование заказчик может потребовать выполнения несогласованных работ.	2	2	5
5	Несоответствие результатов проекта ожиданиям заказчика	Неполнота исходной информации о работе бизнес процессов и отсутствие полной информации о работе информационной системы заказчика.	3	3	9

Продолжение таблицы 10

6	Плохая коммуникация с заказчиком	Заказчик пропадает на несколько дней	1	2	2
7	Нестабильность технических мощностей заказчика	Сервера, компании заказчик могут работать нестабильно, что может привести к тому что систему придется переконфигурировать заново систему.	3	2	6
8	Неквалифицированные сотрудники со стороны заказчика	Сотрудники со стороны заказчика вносят изменения в архитектуру или код проекта, не предупреждая исполнителя.	1	2	2
9	Атаки на проект вовремя его администрирования	Возможно возникновение атак на систему	1	3	3
10	Проблемы при интеграции	Заказчик может не дать полную информацию об информационно системе	3	2	6
11	Неисправность SVN сервера	SVN находит на стороне заказчика, может возникнуть падение сервера	3	1	3

По данной таблице 10 можно проследить, рейтинг важности рисков, следовательно, какие риски являются критичными для проекта. В данном случае критичными рисками являются относящие к правильному составление технического задания, где будут описаны основной функционал системы, а также объяснение заказчику, функционал системы, для того чтобы он понимал с чем он работает.

После того, как потенциальные риски были определены, начинает стадия внесений изменений, пересмотра или пересмотра проекта, чтобы устранить или минимизировать идентифицированные риски, гарантируя, что любые такие конструктивные изменения сами по себе не приводят к новым опасностям.

3.1.4 Анализ рисков с инструментом CORAS

В качестве инструмента графического представления угроз, уязвимостей и степени влияния риска используется CORAS.

Основными элементами, входящими в данный метод, являются: анализ древа событий, цепи Маркова, анализ опасности и работоспособности и анализ видов, последствий и критичности отказов, которые выполняют адаптацию, уточнение и комбинирование информации в рамках проведения анализа рисков.

На рисунке 60 представлены основные активы, которые задействуются в проекте.

На рисунке 61 представлена диаграмма модели угроз. С помощью данной диаграммы можно проследить реализацию угроз, последствия, которые они приносят и как эти угрозы влияет на активы проекта.

На рисунке 62 представлена диаграмма модели угроз с учетом вероятности возникновения инцидента. В данной диаграмме наглядно показано какие инциденты появляются в результате возникновения тех или иных угроз, влияющие на активы, а также добавлен параметр вероятности возникновения инцидентов (высокая, средняя, низкая).

На рисунке 63 представлена диаграмма рисков с влиянием угроз. В данной диаграмме описываются угрозы и риски, которые влияют на активы проекта, а также их степень влияния.

На рисунке 64 представлена диаграмма модели угроз с учетом защитных мер. Здесь наглядно показано, какие меры защиты расставлены для предотвращения рисков возникшие в результате проектирования. Эти защитные меры направлены на снижение рисков.

На рисунке 65 представлена диаграмма недопустимых рисков. Эта диаграмма показывает основные риски, которые описанные на рисунке 64 выше, но данные риски являются высокими и тем самым на рисунке 65 видно на какие риски стоит обратить внимание и немедленно их предотвратить.

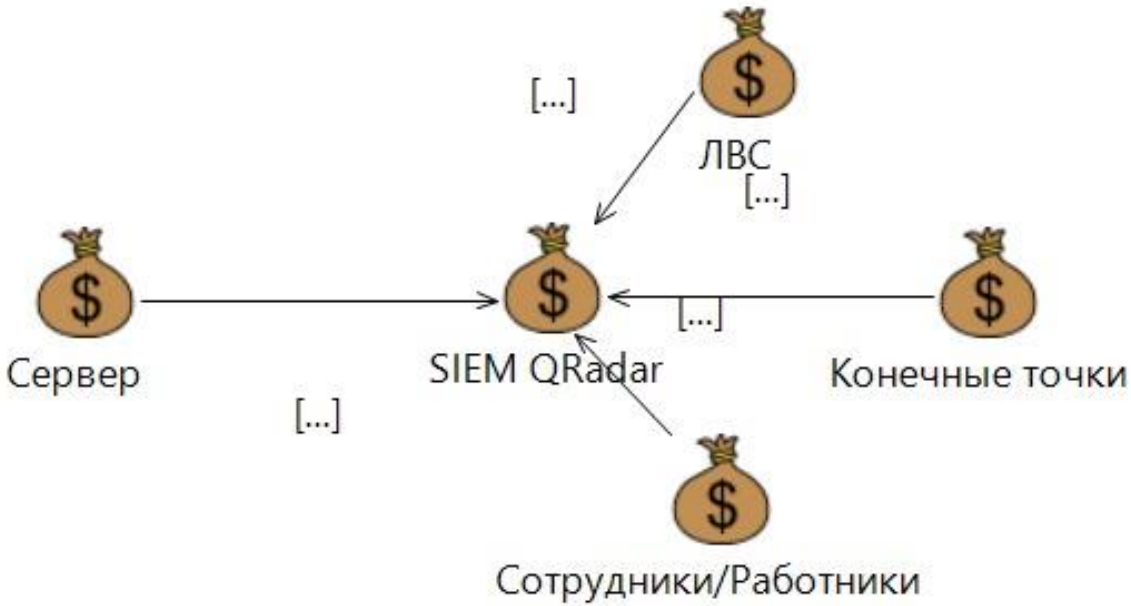

Рисунок 60 –Активы проекта

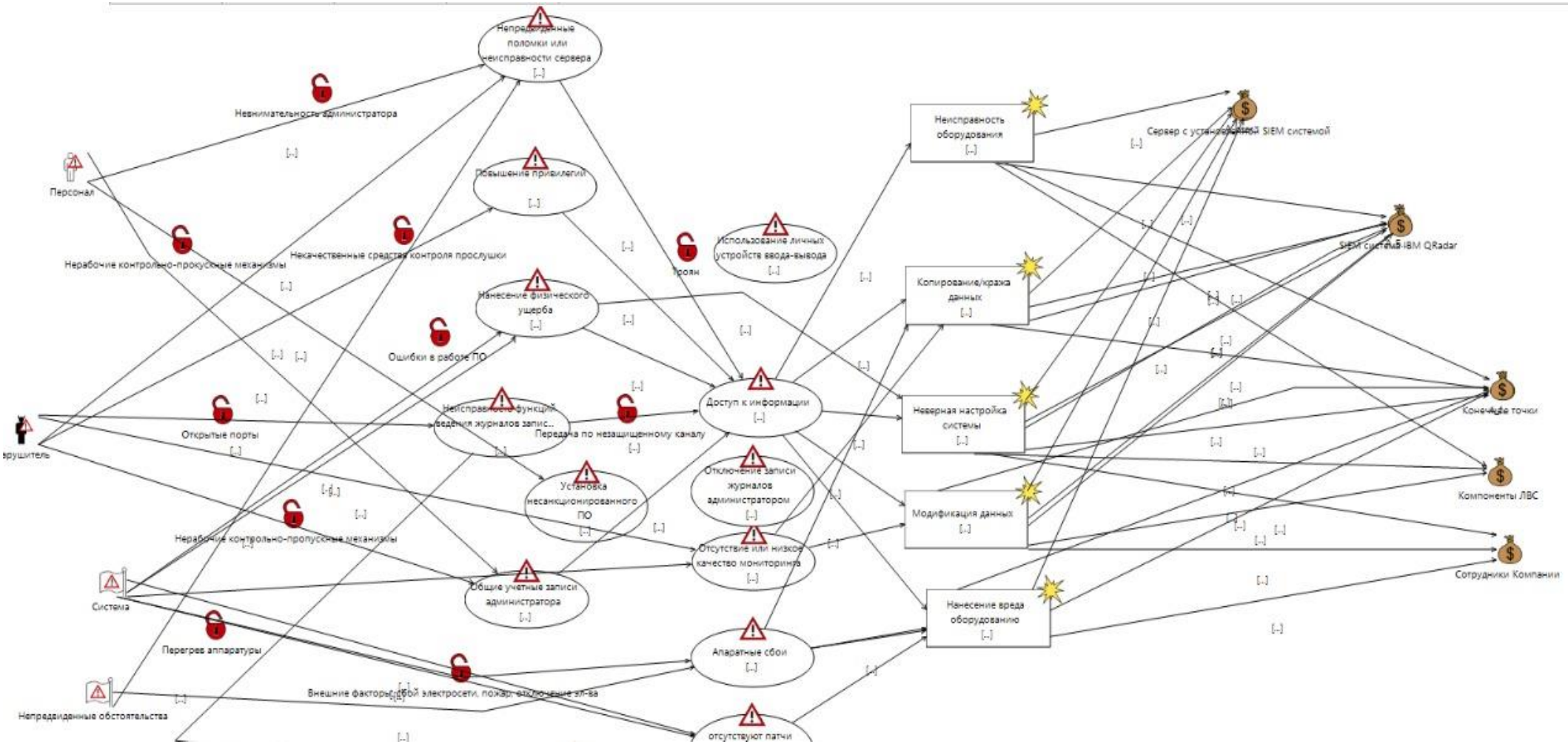

Рисунок 61 – Модель угроз

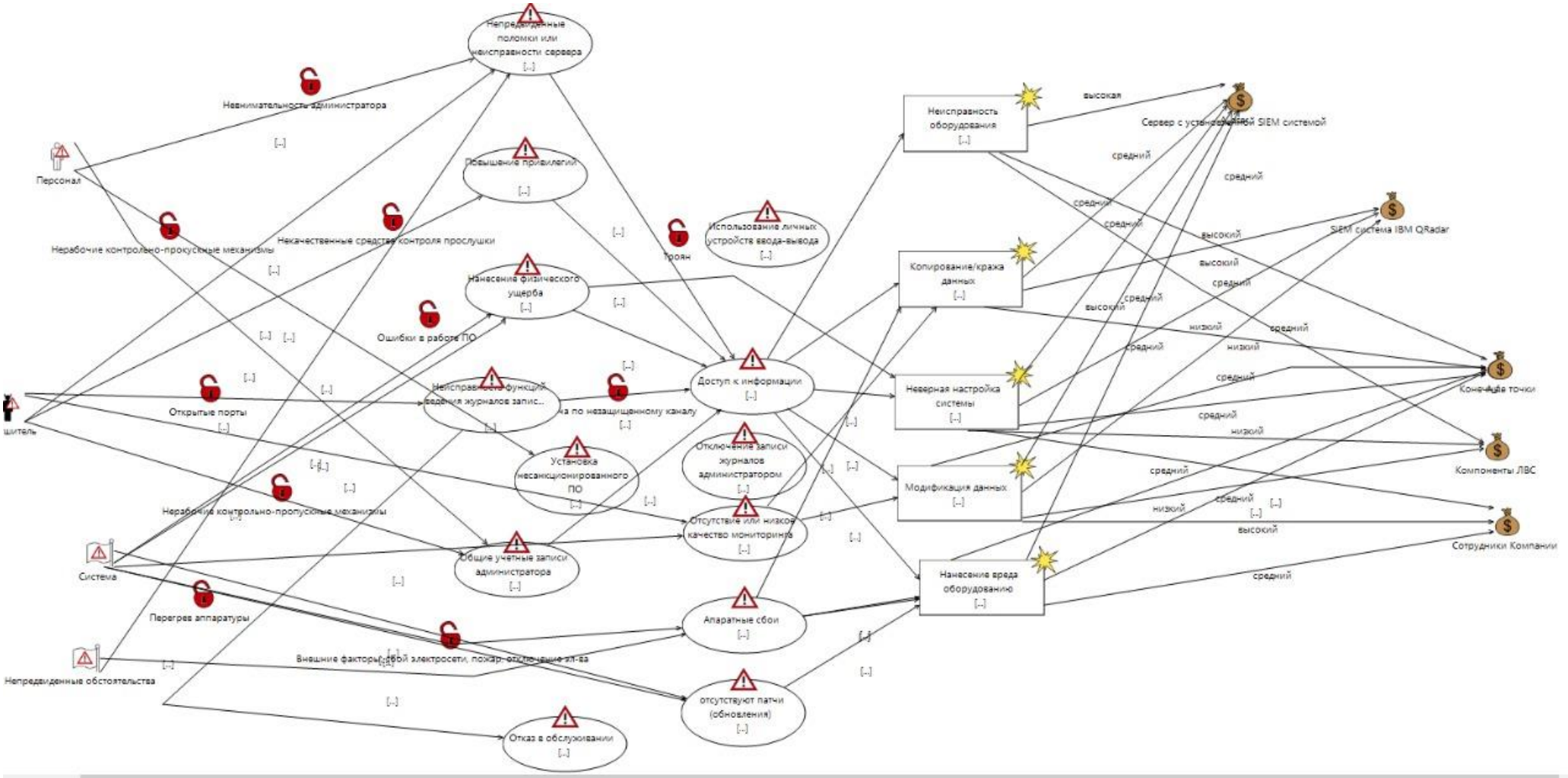

Рисунок 62 – Модель угроз с учетом вероятности инцидентов

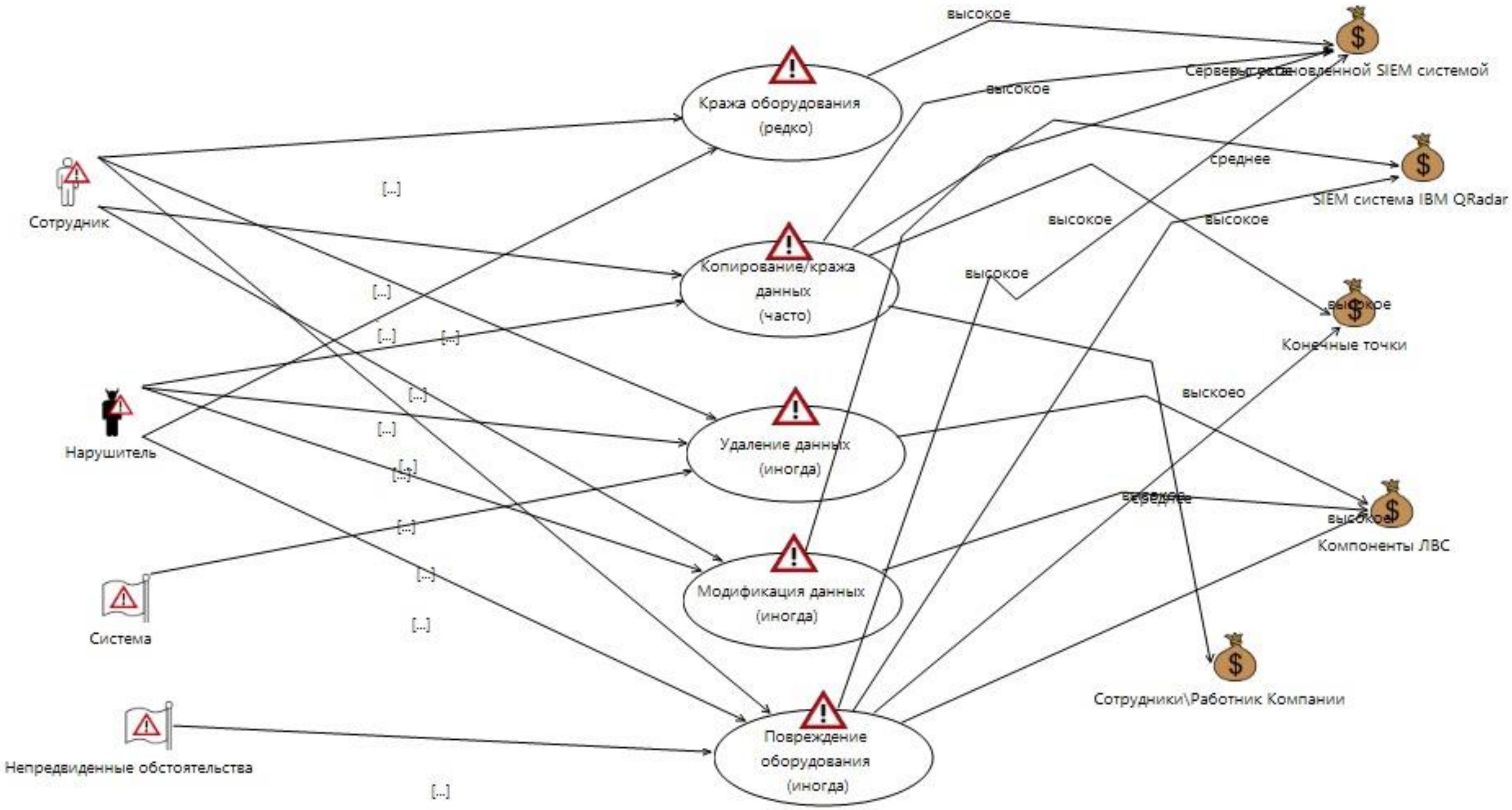

Рисунок 63 – Диаграмма влияния угроз и риски

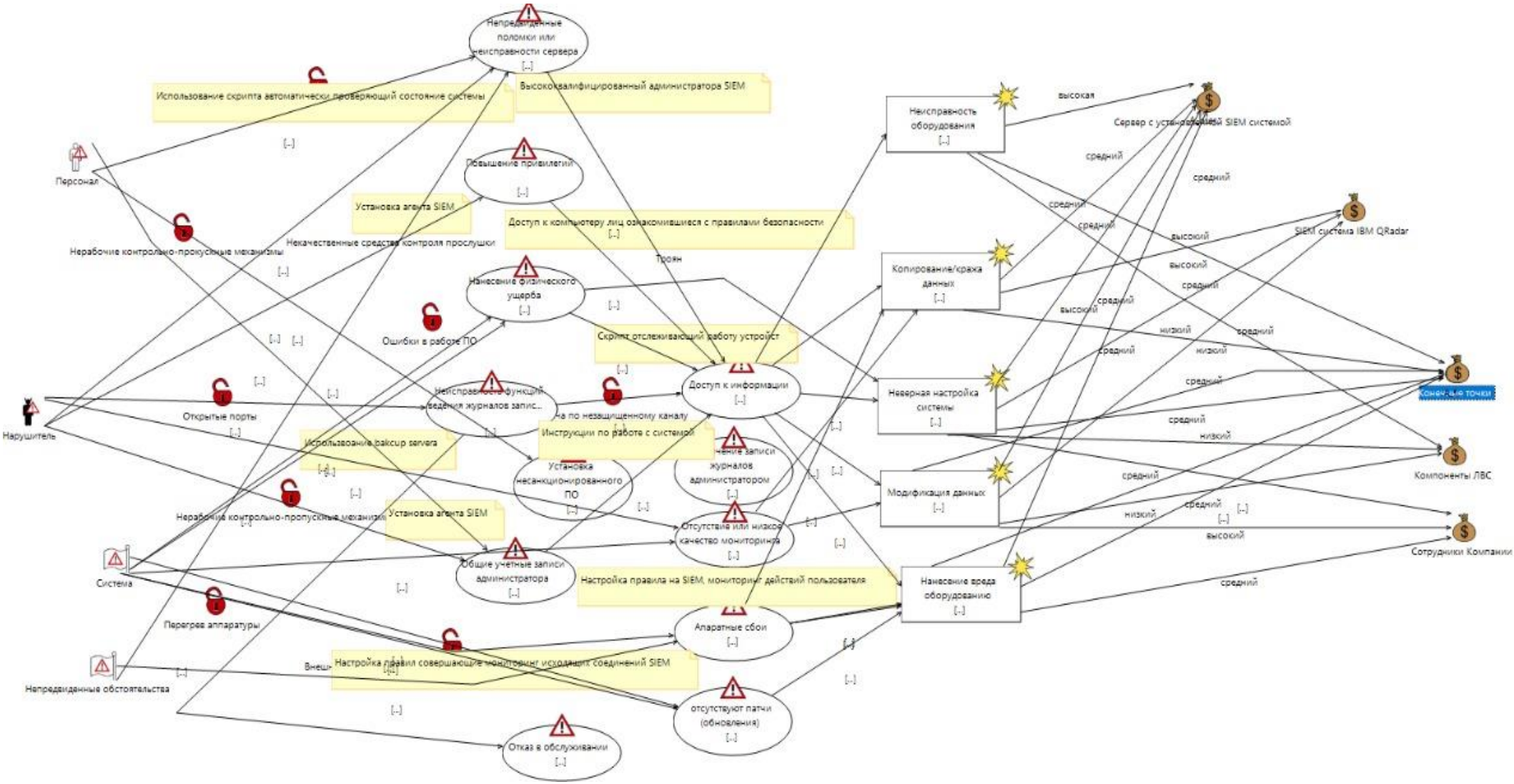

Рисунок 64 – Расстановка защитных мер

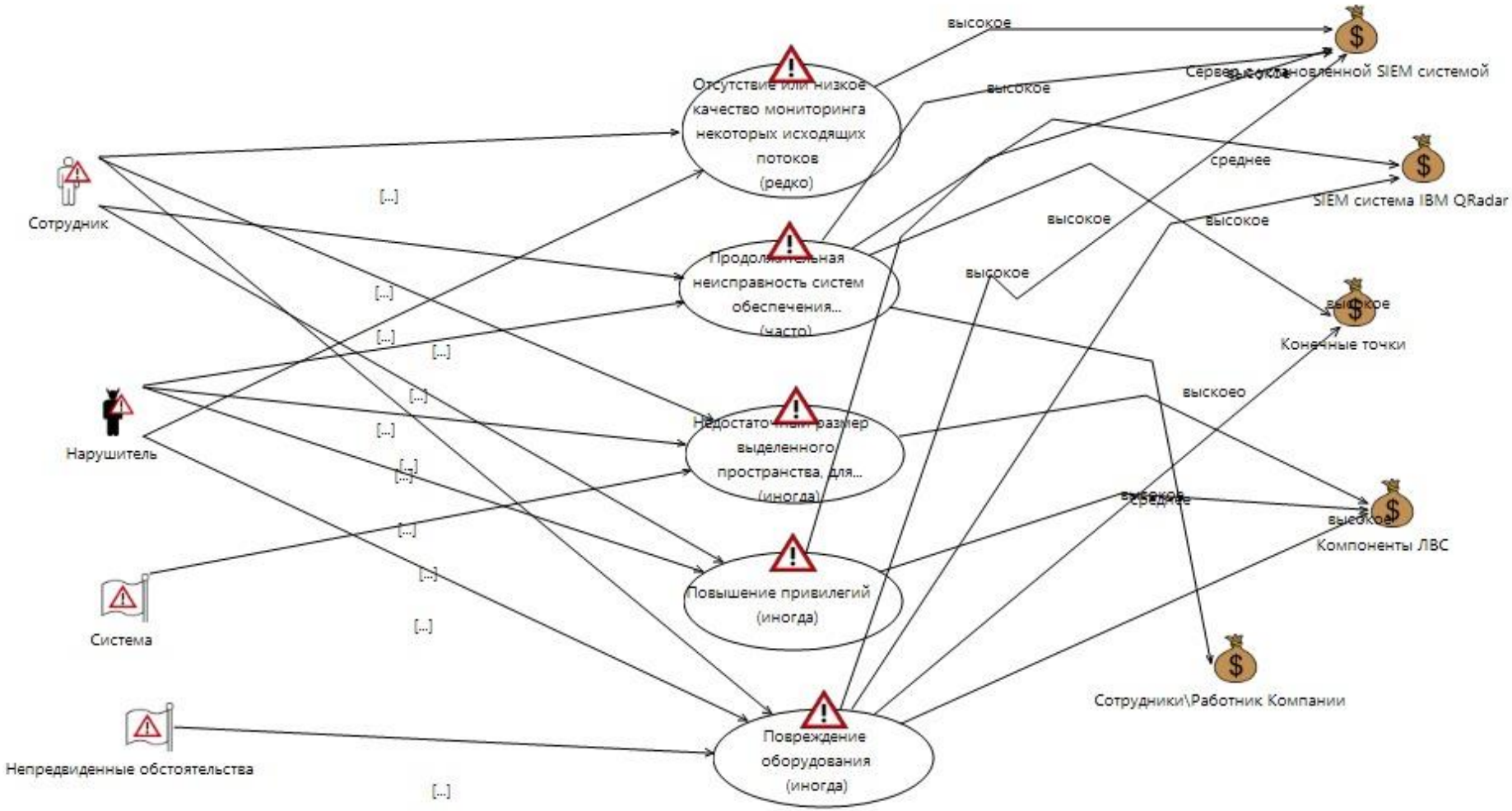

Рисунок 65 – Диаграмма неприемлемых рисков

Выводы: В данном раздел была проведена оценка проектных рисков. При оценивании проектных рисков можно определить потенциальные риски в процессе проектирования либо на стадии его создания. С помощью данной оценки рисков можно устранить всевозможные потенциальные сбои и уменьшить их влияние. Это обеспечивает строгий систематический анализ надежности проекта и позволяет фиксировать риски на уровне системы.

В проекте, который описан в данном дипломном проекты, были выделены основные угрозы, уязвимости и риски, которые могут возникнуть при проектировании и в ходе работы проекта. После того как были определены основные угрозы и уязвимости, была рассчитана их степень влияния на проект были определены основные риски, которые могут возникнуть.

Далее необходимо определить какие риски необходимо рассматривать в первую очередь и для этого использовалась формула важности риска с помощью, которой наглядно было видно какие риски являются наиболее важными. И также стоит отметить, что были учтены меры по снижению рисков.

Для того, чтобы видеть наглядно и было более понятно, как это все взаимодействует между собой и как необходимо расписать план проекта и с какими рисками и какой степени, использовался инструмент CORAS.

Основные диаграммы, которые были построены это:

а) диаграмма активов;

б) диаграмма модели угроз;

в) модель угроз с учетом вероятности возникновения инцидента;

г) диаграмма последствий угроз и степень влияния рисков;

д) диаграмма расстановки защитных мер;

е) диаграмма неприемлемых рисков.

4 Безопасность жизнедеятельности

4.1 Анализ потенциально опасных и вредных факторов в офисе, воздействующих на персонал

Офис имеет важное значение для здоровья из-за множества опасностей, которые существуют во многих производственных средах. Эти опасности могут быть связаны с широким спектром физических, химических и биологических агентов. Многие аспекты регулируются (например, Правила об охране труда и технике безопасности на производстве и правила контроля за веществами, опасными для здоровья, а также ГОСТ 12.0.003-74) [12].

Компания находится на первом этаже многоэтажного здания, в каждом отделе окна выходят на сторону, где постоянно ездят машины, а также находится детская площадка. Отделы разделены перегородками, через которые сотрудники могут слышать, то что происходит в соседнем отделе при повышенном тоне разговоров сотрудников соседнего отдела. Также кроме того, что в Компании «тонкие стены» шум могут вызвать, работаю персональные компьютеры, процессор, монитор, машины на проезжей части, а также различные вспомогательное оборудование (вентиляционные установки, кондиционеры) и т.д.

При таком расположении офиса и отделки, можно сказать, что офис не соответствует допустимым нормам шума, которое составляет 40 дБА по нормам СН 32.23-85 «Санитарные нормы допустимого шума на рабочих местах» [13].

Уровень шума на рабочем месте не должен превышать 50дБА СН 32.23-85 «Санитарные нормы допустимого шума на рабочих местах».

Кроме шума сотрудники также подвергаются вибрации от компьютерной техники с которой взаимодействуют.

В связи с такой ситуацией у сотрудников ухудшается концентрация работы, а также они чаще испытывают раздражительность, головные боли, головокружение, повышенную усталость, боли в ушах и так далее. Данные нарушения могут вызвать негативные изменения в эмоциональном состоянии сотрудников.

В качестве мер по снижению шума, необходимо по СНиП II-12-77 «Защита от шума» [15], установить звукопоглощающие материалы не только на устройства, с которым взаимодействует сотрудник, а также сделать облицовку перегородок. Уровень вибрации в помещениях вычислительных центров может быть снижен путем установки оборудования на специальные виброизоляторы.

В таблице 11 приведены максимальные уровни шума в зависимости от категории тяжести и интенсивности работы, которые являются безопасными с точки зрения поддержания здоровья и работоспособности.

Таблица 11 – Предельные уровни звука, дБ, на рабочих местах.

Категория Напряженности труда	Категория тяжести труда			
I. Легкая	II. Средняя	III. Тяжелая	IV. Очень тяжелая	
I. Мало напряженный	80	80	75	75
II. Умеренно напряженный	70	70	65	65
III. Напряженный	60	60	-	-
IV. Очень напряженный	50	50	-	-

Параметры микроклимата

Сотрудники довольно много часов проводят за работой с вычислительными устройствами, которые является источником значительного тепла, которое может привести к повышению температуры и снижению относительной влажности воздуха в помещении. В помещениях, где установлены компьютеры, необходимо соблюдать определенные параметры микроклимата. Санитарные нормы СН-245-71 устанавливают значения параметров микроклимата, которые создают комфортные условия [14]. Эти нормативы устанавливаются в зависимости от времени года, характера трудового процесса и характера производственных помещений приведены в таблице 12.

Объем помещений, в которых размещаются сотрудники вычислительных центров, должен быть не менее 19,5 м3 / чел. с учетом максимального количества одновременных работников в смену. Температура в таких помещениях не должна превышать 21-25 °С летом, а зимой не превышать 23 °С, так как высокая температура неблагоприятно сказывается на работоспособность человека.

Атмосферное давление должно быть в пределах 105 кПа. В случае повышенного давления человеку требуется время на акклиматизацию.

Нормы подачи свежего воздуха в помещения, где расположены компьютеры, приведены в таблицах 12 и 13.

Таблица 12 – Параметры микроклимата для помещений

Период года	Параметр микроклимата	Величина
Холодный	Температура воздуха в помещении Относительная влажность Скорость движения воздуха	22…24°С 40…60% до 0,1м/с
Теплый	Температура воздуха в помещении Относительная влажность Скорость движения воздуха	23…25°С 40…60% 0,1…0,2м/с

Таблица 13 – Нормы подачи свежего воздуха в помещения

Характеристика помещения	Объемный расход подаваемого в помещение свежего воздуха, м3 /на одного человека в час
Объем до 20м3 на человека 20…40м3 на человека Более 40м3 на человека	Не менее 30 Не менее 20 Естественная вентиляция

4.2 Расчетная часть

4.2.1 Видеонаблюдение

Перед тем как обустроить свой офис камерами видеонаблюдения необходимо следовать правовым аспектам видео и аудио контроля, а именно:

а) не размещать камеры в таких местах как: туалетные комнаты, раздевалки, душевые, процедурные кабинеты и в других подобных местах. См. статью 23 Конституции РК [16];

б) создать локально нормативный акт предприятия о введении видеофиксации. В нем четко прописать цели видеосъемки. В зависимости от специфики деятельности организации они могут быть разными, главное, чтобы они удовлетворяли требованиям соблюдения законности;

в) необходимо письменно ознакомить персонал с регламентом "о введении видеофиксации", который нужно подписать, дав свое согласие;

г) разместить информационную табличку: "ведется видеонаблюдение";

д) камеры не должны быть скрытыми или замаскированными под предметы;

е) запись с камер не должна быть в свободном доступе, работодатель может указать ответственного, который получит доступ и будет за это отвечать. Учтите, есть учреждения, где использование видеонаблюдения является обязанностью работодателя: сфера образования и здравоохранения с целью безопасности и противодействию терроризму пункт 2, статья 11 N 152-ФЗ (редакция от 29.07.2017) [14].

4.2.1.1 Технические меры при построении системы видеонаблюдения

Теперь необходимо рассмотреть техническую строну размещения видеокамер.

В основном в офисах выставляют камеры с AHD разрешением, то это – это схожая система с аналоговой, только обладает более высоким разрешением. При этом установка проводится точно так же как у цифровых. При организации установки в офисе следует учитывать определенный ряд особенностей:

а) поиск места;

б) поиск помех;

в) создание плана по размещению;

г) подключение;

д) проверка.

Внутренний периметр офиса. Внутри здания располагается четырнадцать помещений. Четыре видеокамеры расположены в ключевых помещениях офиса.

Две камеры находятся в зоне ресепшена, а также около первой переговорной комнаты, так как именно через эту зону проходят все сотрудники, клиенты и посетители офиса. Именно в ней, чаще всего,

возникают споры между клиентами и сотрудниками офиса. Данную зону принято защищать, как минимум, двумя видеокамерами. Первая видеокамера с широким углом обзора должна захватить максимальную площадь помещения. Ее задачи фиксировать перемещение людей в зоне и их действия. Устанавливать камеру следует таким образом, чтобы в кадре одновременно находились и клиенты офиса, и собственные сотрудники на рисунке 66.

Камера 2 будет ответственная за угол обзора всего ресепшна, а камера 3 с более узким углом обзора фиксации посетителей и сотрудников офиса.

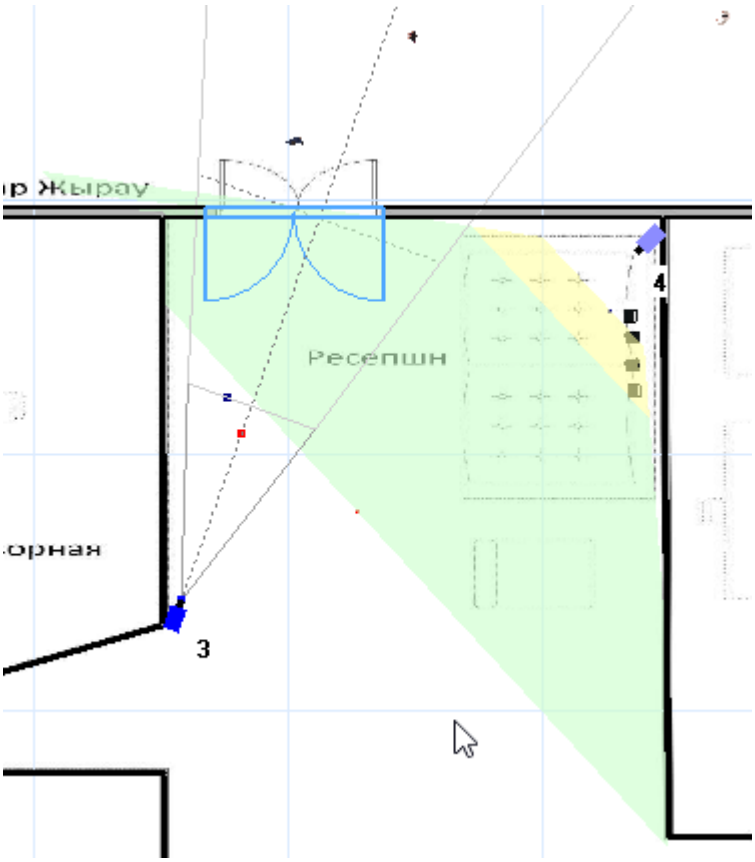

Рисунок 66 – Камеры в зоне ресепшна

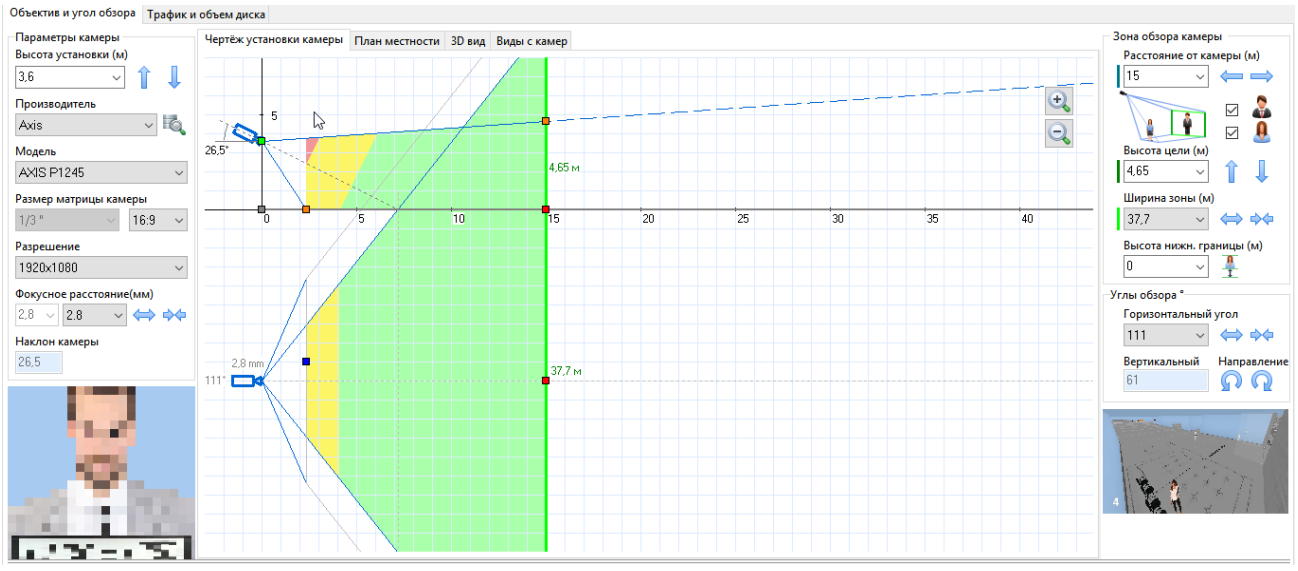

Рисунок 67 – Настройки камеры 4

Далее идет длинные коридор, который является зоной с активным перемещением людей рисунок 68. Для контроля этих зон наилучшим образом подходят камеры с широкоугольным объективом. Контроль зон с высокой активностью позволяет отследить перемещение любого сотрудника, посетителя или злоумышленника по офису. Если все-таки случилось страшное и со стола сотрудника пропал новый дорогой телефон и известно, что это случилось, например, в четверг с между 14.00 и 15.30, вы всегда сможете просмотреть заданную часть видеоархива и определить входящих и выходящих из кабинета людей, тем самым либо сузить круг подозреваемых, либо даже найти виновного.

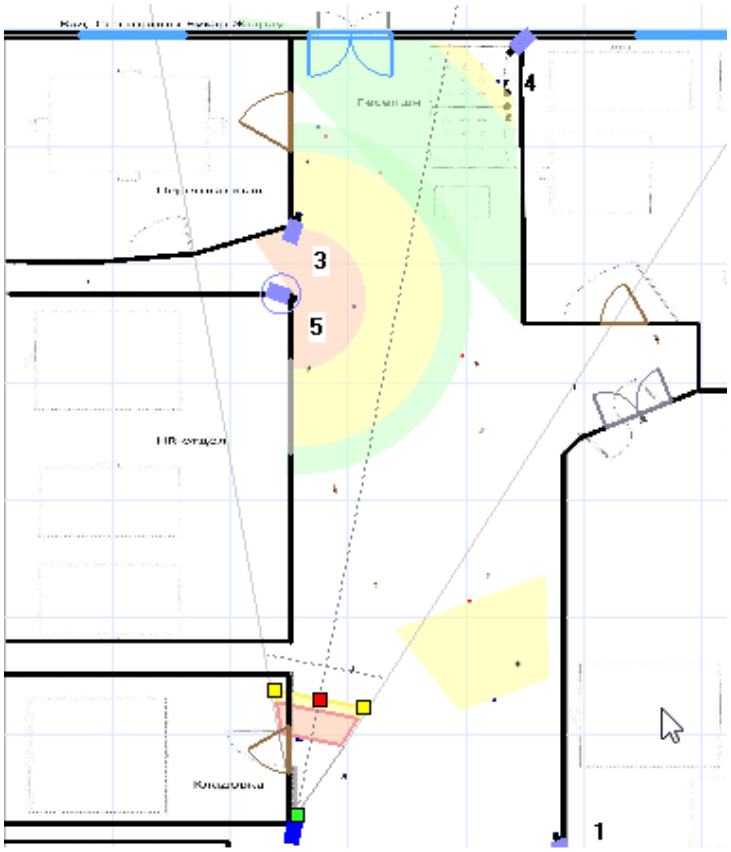

Рисунок 68 – Общий план коридора

Камера следит за перемещением между офисами продаж и отделом разработки рисунок 69.

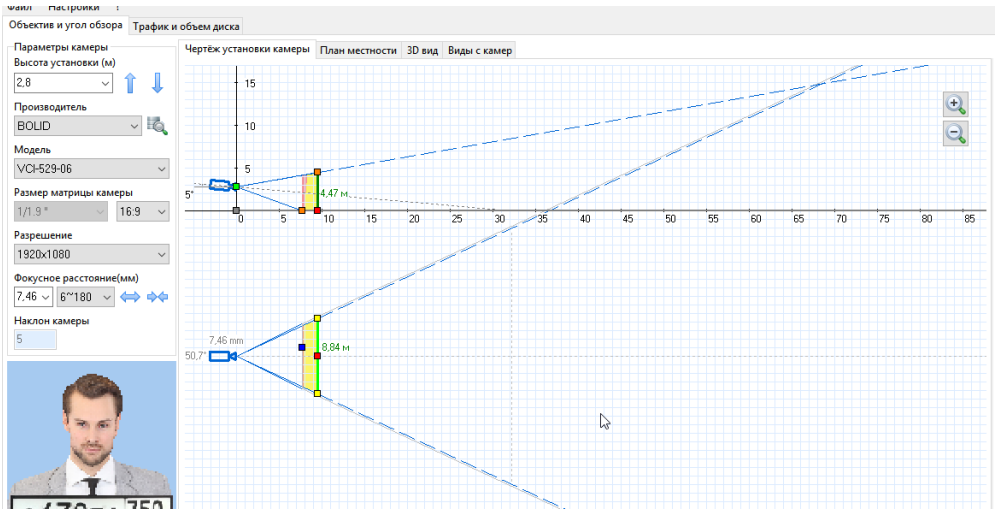

Рисунок 69– Настройки камеры 5

Камера 1 имеет широкий угол просмотра тем самым охватывает весь коридор, но при это качество теряется рисунок 70. Также видно, что у камеры 1 есть мертвая зона, которую перекрывает камер 6

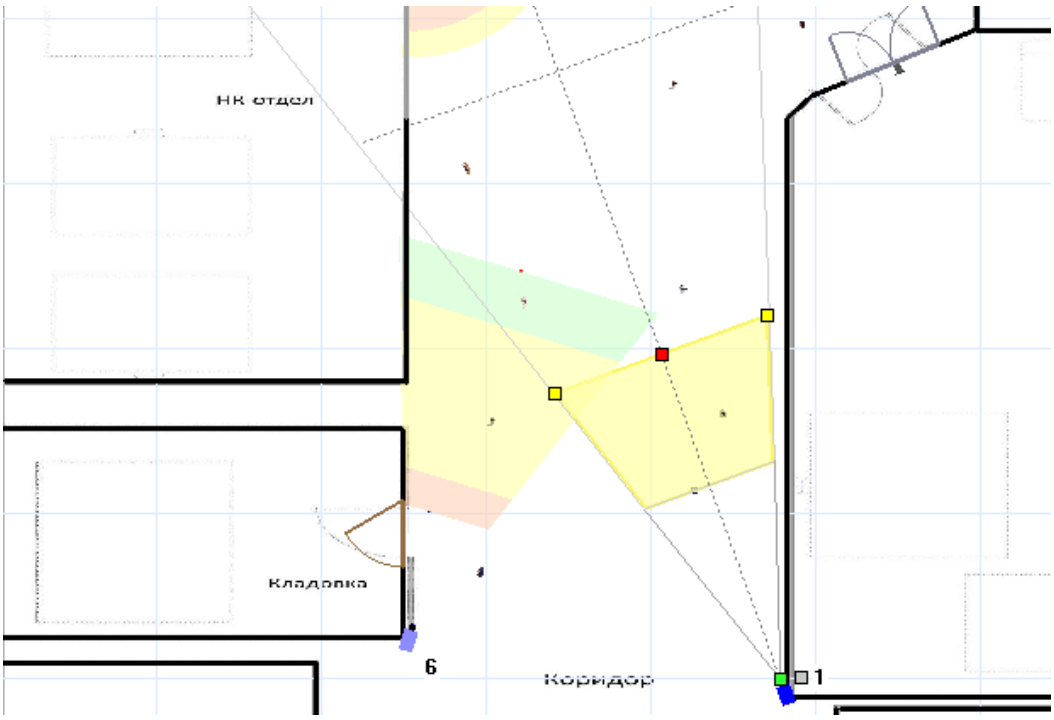

Рисунок 70 – Вид с камер 1 и 6

Устанавливаем камеры на входе серверной на рисунке 71 и 72.

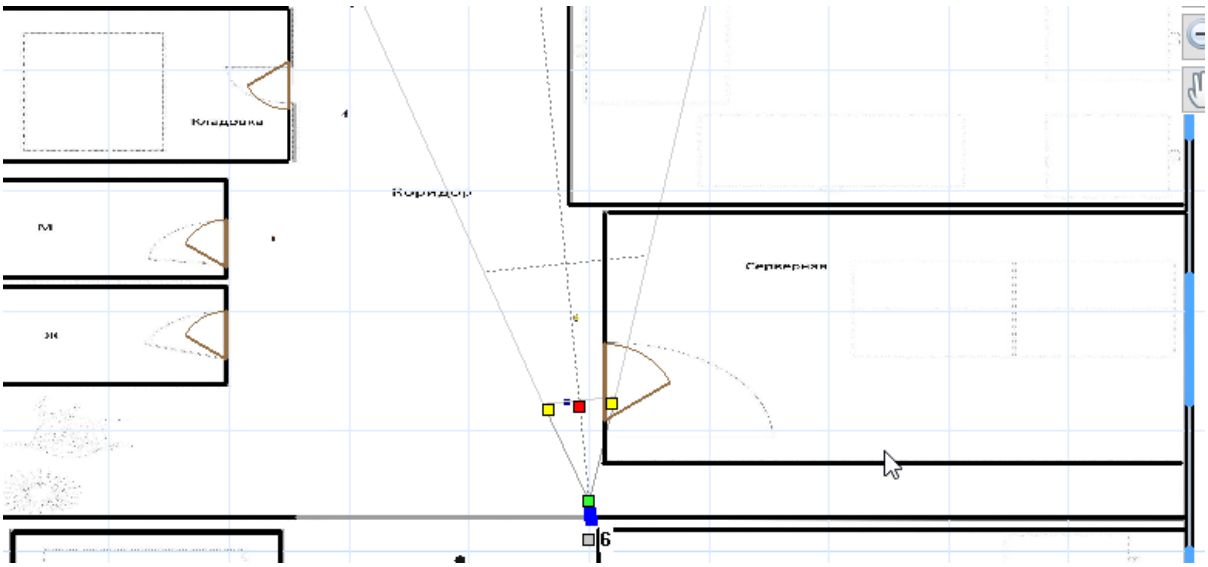

Рисунок 71 – Камера на входе серверной

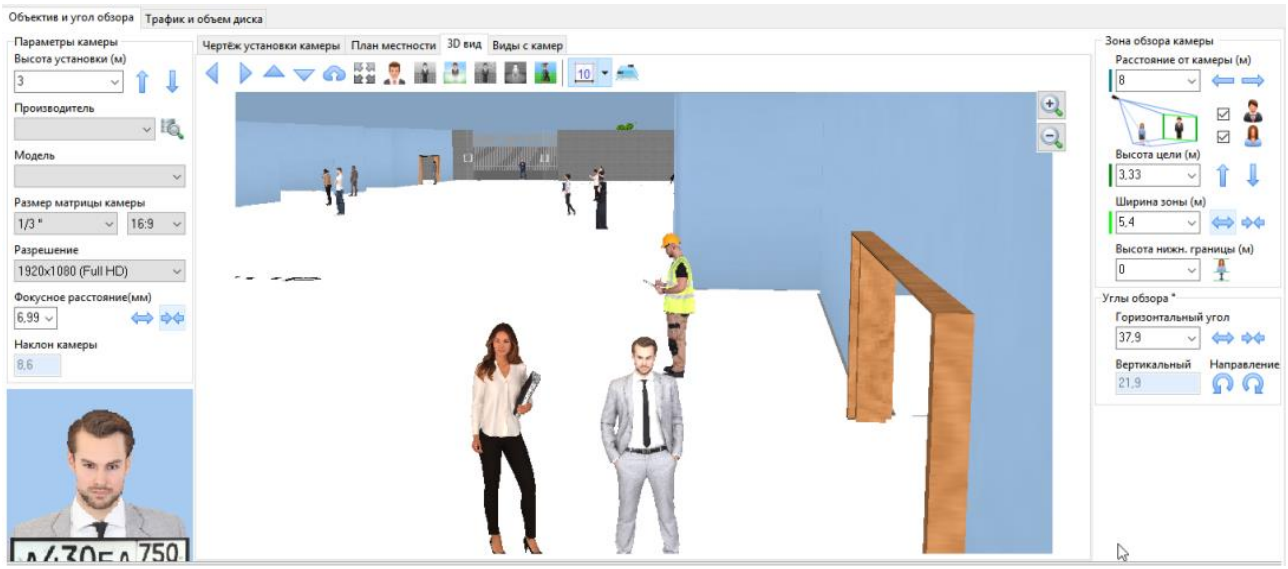

Рисунок 72 – Настройка и вид на вход в серверную через камеру

Чтобы закрыть мертвые зоны камеры 1 устанавливаем камеру 7 на рисунке 73 для того, чтобы видеть кто заходит в кабинет бухгалтерии.

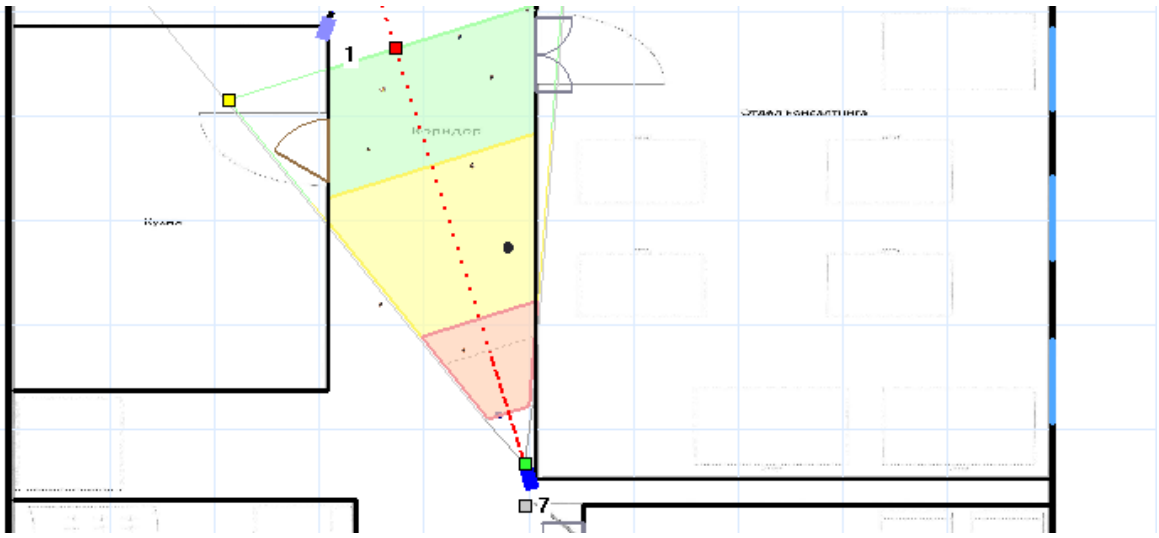

Рисунок 73 – Вид камеры 7

И наконец установим камеру около входа во вторую переговорную рисунок 74

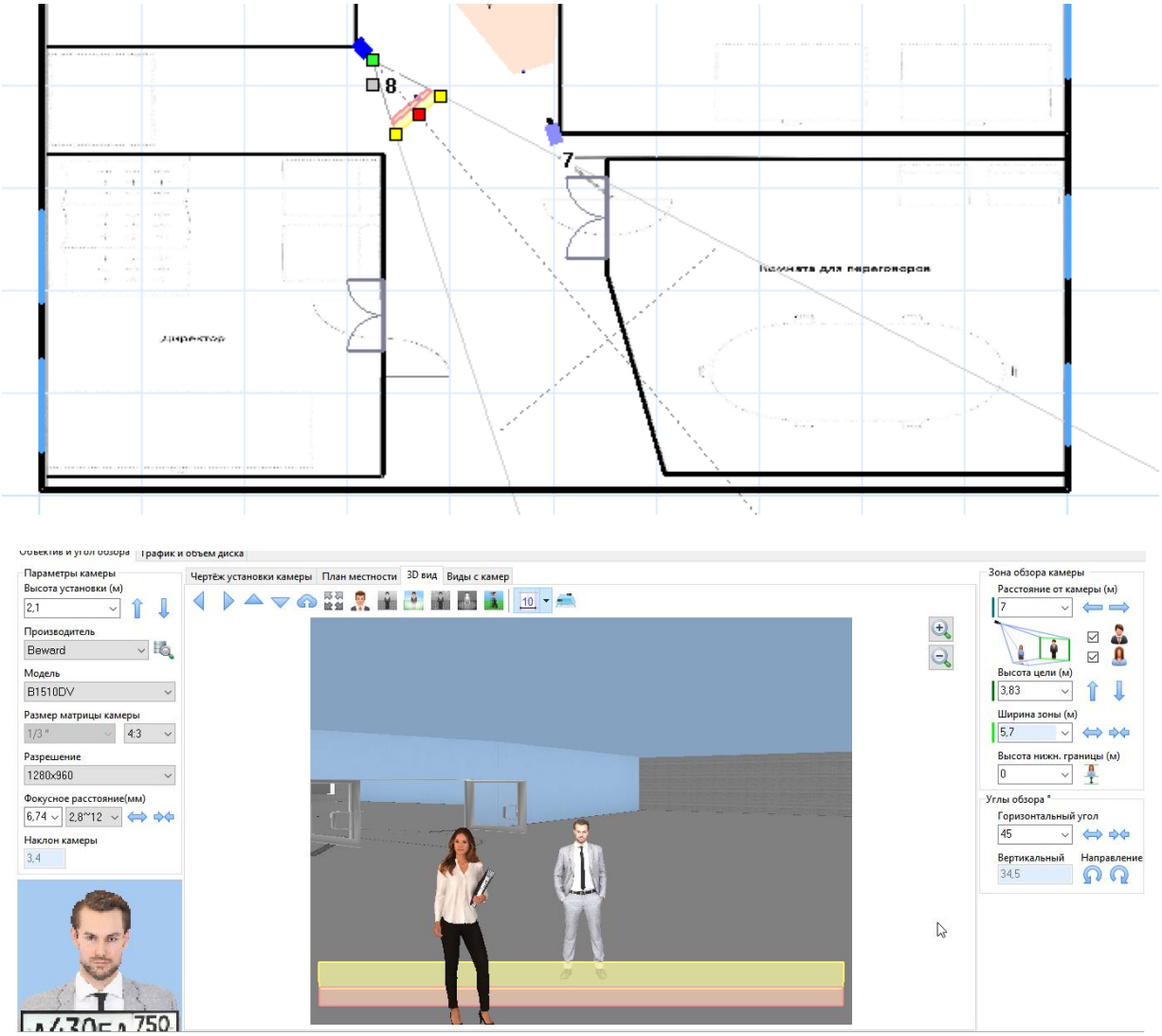

Рисунок 74 – Вид и настройка камеры 8

4.2.1.2 Проводка видеокамер

Подключение камеры видеонаблюдения состоит из нескольких этапов монтажных работ:

а) сначала осуществляется монтаж крепления в указанном на предварительно начерченной схеме месте;

б) далее устанавливается сама камера и надежно закрепляется;

в) потом к ней подключаются провод, подающий электропитание, и видеокабель, через который будет поступать сигнал на регистратора.

Коаксиальный. В системе используется для передачи сигнала от камеры к записывающему устройству. Для видеонаблюдения оптимален кабель с медной жилой с 5 мм сечением. Покупать кабель с большим сечением нет смысла;

Комбинированный. Самый простой и оптимальный вариант для соединения камер с записывающим устройством. Он проводится к камере и наиболее часто используется при установке видеонаблюдения в небольших квартирах.

4.2.1.3 Выбор видеорегистратор

Основной параметр видеорегистратора – количество входов (для аудио и видео). Обычно у регистраторов присутствует 16 каналов. Однако, если вам требуется больше, приобретите несколько регистраторов и закольцуйте их в сеть с использованием платы видеозахвата.

В моем офисе подключения камер видеонаблюдения будет происходить - по витой паре и коаксиальному кабелю.

Схема подключения камер видеонаблюдения по витой паре приведена на рисунке 75.

При таком способе организации видеонаблюдения используется преобразование несимметричного сигнала видеокамеры в симметричный, его передача и обратное преобразование при подключении к приемной аппаратуре системы видеонаблюдения.

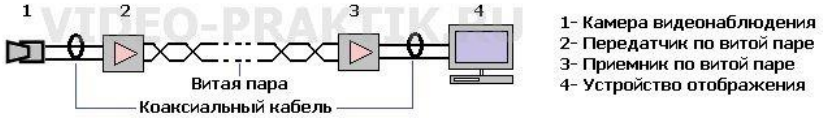

Рисунок 75 – Схема подключения по коаксиальному кабелю

4.2.1.4 Выбор камер по рассчитанным характеристикам

а) BEWARD B1073WB2-K12 ip-камера-наружная.

B1073 - камера, оснащенная ПЗС-сенсором Sony ExView HAD II, который, совместно с процессором Effio-E, а так же благодаря ряду функций улучшения качества, цветности и подавлению шумов, позволяет получать более четкое изображение с повышенной детализацией.

б) Vision Hi-Tech PD4-SE-B3.6IR- внутренняя аналоговая камера.

Основные особенности:

Видеокамера оснащена ПЗС-матрицей 1/3" Sony Super HAD CCD II высокого разрешения 700 ТВЛ и минимальной чувствительностью 0.001 люкс.

Наличие процессора цифровой обработки сигнала Effio-E обеспечивает работу большого числа цифровых функций, таких как, фильтр цифрового шумоподавления 2DNR, двойная система компенсации встречной засветки BLC и HLC.

4.3 Расчет нагрузки сотрудника

Так как работа сотрудника буде связанна с программирование и настройкой системы, в его обязанности входит следующее, общие действия в таблице 14:

Таблица 14 – Должностные обязанности сотрудника

Этап	Содержание	Затрата времени, %
I II	Постановка задачи Изучение материала по поставленной задаче	6.25
III	Определение метода решения задачи	6.25
IV	Составление алгоритма решения задачи	12.5
V	Программирование	25
VI	Отладка программы, составление отчета	50

Для расчета уровня нагрузки сотрудника, необходимо определить, количество повторений действий сотрудника по следующей формуле:

$$p_i = k/n, \quad (1)$$

где k – количество повторений каждого элемента одного типа.

n – суммарное количество повторений от источника информации

Составляем таблицу 15 с количеством алгоритмов и действием которые проделывает сотрудник

Таблица 15 – Действия сотрудника

Члены алгоритма	Количество алгоритмов	Частота повторений pi
Изучение технической	5	1,00

документации и литературы		

Продолжение таблицы 15

Наблюдение полученных результатов	2	0,4
Уточнение и согласование полученных материалов	4	0, 8
Выбор наилучшего варианта из нескольких	6	1,00
Исправление ошибок	3	0,5
Анализ полученных результатов	4	0,7
Выполнение механических действий	1	0,2
Принятие решений на основе изучения технической литературы	5	0,8
Графического материала	0	0
Полученного текста программы	5	0,7

Количественные характеристики алгоритма (Таблица 15) позволяют рассчитать информационную нагрузку программиста. Энтропия информации элементов каждого источника информации рассчитывается по формуле, бит/сигн:

$$H_j = -\sum_{i=1}^{m} p_i \log_2 p, \qquad (2)$$

где m – число однотипных членов алгоритма рассматриваемого источника информации.

H1 = 2 * 1,3 + 4 * 0,3 = 3,8

H2 = 3 * 1 + 4 * 1 + 0 + 5 * 0,33 = 8,65

H3 = 5 * 1 + 2 * 1,7 + 2 * 1,7 = 11,8

Далее определяется поток информационной нагрузки бит/мин:

$$\Phi = \frac{H_{\Sigma} \times N}{t}, \qquad (3)$$

где N – суммарное число всех членов алгоритма;

t – длительность выполнения всей работы, мин.

От каждого источника в информации (члена алгоритма) в среднем поступает 2 информационных сигнала в час, время работы - 225 часов,

$$Ф = \frac{24{,}25*33*2*225}{13500} = 3{,}3 \text{бит/с}$$

Рассчитанная информационная нагрузка сравнивается с допустимой. При необходимости принимается решение об изменениях в трудовом процессе.

Условия нормальной работы выполняются при соблюдении соотношения:

$$\boldsymbol{Ф}_{доп.мин.} \leq \boldsymbol{Ф}_{расч.} \leq \boldsymbol{Ф}_{доп.макс.}$$

где Фдоп.мин. и Фдоп.макс. – минимальный и максимальный допустимые уровни информационных нагрузок (0,8 и 3,2 бит/с соответственно);

Фрасч. – расчетная информационная нагрузка

$$0{,}8 < 3{,}3 < 3{,}2$$

Заключение

В ходе выполнения данной работы были реализованные поставленные задачи по реализации концепции «Умный офис».

Компании, внедрившие данную концепцию могут активно бороться против кибер-злоумышленников. «Умный офис» может оказывать значительное влияние на результаты бизнеса. В результате выполнения данной работы можно выделить основные преимущества «Умного офиса»:

Централизованный подход.

Команда создания в данной концепции начинает реагирование, как только происходит какое-либо нарушение или инцидент. Они предлагают услуги в режиме реального времени, сохраняя все процессы и программное обеспечение в одном месте, таким образом, поддерживая бесперебойную работу.

Поддерживать доверие клиентов и сотрудников.

Клиенты и сотрудники доверяют организациям хранить свои данные в безопасности. Данная концепция помогает предотвратить потерю данных и тем самым сохранить целостность информации и информационных активов.

Максимальная осведомленность и минимальные затраты.

Это повышает возможность снижения потенциальных потерь из-за нарушений безопасности, способствуя высокой рентабельности инвестиций. Благодаря интеграции SIEM и SOAR фирмы могут сэкономить деньги на восстановлении после кражи данных.

В данной концепции основными инструмента является SIEM и SOAR. Программное обеспечение SIEM представляет собой набор инструментов для предоставления информации, необходимой для обнаружения и управления событиями безопасности.

В частности, инструменты SIEM агрегируют и нормализуют данные из различных источников. Эти данные могут поступать из журналов сообщений (syslog), журналов ОС, оконечных устройств, выходных данных брандмауэра / IDS и журналов сетевого потока. Вместо того, чтобы просто регистрировать все данные, инструменты SIEM затем удаляют все несущественное. Это называется нормализацией. Программное обеспечение SIEM затем использует интеллектуальные правила корреляции, чтобы выделить связи между событиями, готовыми для анализа группой поддержки ИТ-специалистов. Затем аналитики могут выполнить анализ с помощью SOAR, чтобы выяснить причины любых аномалий и, при необходимости, принять меры для защиты ИТ-инфраструктуры бизнеса.

С помощью написания скриптов и настройкой правил в системе SIEM, были выполнены задачи по автоматизации стандартах действий по реагированию, а также помощь администраторам при настройке самой системы, также была полностью интегрирована система SOAR с помощью, которой, команда реагирования может работать более эффективно. Данная

система была полностью настроена, созданы пользователи и обозначены их роли, также созданы специальные сводные панели, которые показывают всю необходимую информацию по инцидентам для аналитика. Кроме этого были написаны скрипты с помощью которых аналитик, может просматривать всю информацию по инцидентам, менять их и добавлять тем самым действия по управления сокращается к минимуму.

Приложение А
Код скрипта на проверку состояния системы

```
     #!/bin/bash
     #------variables used------#
     S="**********************************"
     D="----------------------------------"
     COLOR="y"
     MOUNT=$(mount|egrep -iw "ext4|ext3|xfs|gfs|gfs2|btrfs"|grep
-v "loop"|sort -u -t' ' -k1,2)
     FS_USAGE=$(df -PTh|egrep -iw
"ext4|ext3|xfs|gfs|gfs2|btrfs"|grep -v "loop"|sort -k6n|awk
'!seen[$1]++')
     IUSAGE=$(df -PThi|egrep -iw
"ext4|ext3|xfs|gfs|gfs2|btrfs"|grep -v "loop"|sort -k6n|awk
'!seen[$1]++')
     if [ $COLOR == y ]; then
     {
      GCOLOR="\e[47;32m ------ OK/HEALTHY \e[0m"
      WCOLOR="\e[43;31m ------ WARNING \e[0m"
      CCOLOR="\e[47;31m ------ CRITICAL \e[0m"
     }
     else
     {
      GCOLOR=" ------ OK/HEALTHY "
      WCOLOR=" ------ WARNING "
      CCOLOR=" ------ CRITICAL "
     }
     #--------Check for currently mounted file systems--------#
     echo -e "\n\nChecking For Currently Mounted File System[s]"
     echo -e "$D$D"
     echo "$MOUNT"|column -t
     #--------Check disk usage on all mounted file systems-------
-#
     echo -e "\n\nChecking For Disk Usage On Mounted File
System[s]"
     echo -e "$D$D"
     echo -e "( 0-90% = OK/HEALTHY, 90-95% = WARNING, 95-100% =
CRITICAL )"
     echo -e "$D$D"
     echo -e "Mounted File System[s] Utilization (Percentage
Used):\n"

     COL1=$(echo "$FS_USAGE"|awk '{print $1 " "$7}')
     COL2=$(echo "$FS_USAGE"|awk '{print $6}'|sed -e 's/%//g')

     for i in $(echo "$COL2"); do
     {
       if [ $i -ge 95 ]; then
         COL3="$(echo -e $i"% $CCOLOR\n$COL3")"
       elif [[ $i -ge 90 && $i -lt 95 ]]; then
```

Продолжение приложения А

```
        COL3="$(echo -e $i"% $WCOLOR\n$COL3")"
      else
        COL3="$(echo -e $i"% $GCOLOR\n$COL3")"
      fi
    }
    done
    COL3=$(echo "$COL3"|sort -k1n)
    paste  <(echo "$COL1") <(echo "$COL3") -d' '|column -t
    echo -e "\n\nChecking For Processor Utilization"
    echo -e "$D"
    echo -e "\nCurrent Processor Utilization Summary :\n"
    mpstat|tail -2
    #------Print memory usage ------#
    echo -e "\n\nTotal memory information"
    echo -e "$D$D"
    free -h \
    #-----App health status------#
    echo -e "$D$D"
    psql -U qradar -c "select id,name, status, task_status from
installed_application;"
    #-----PS status-------#
    echo -e "$D$D"
    /opt/qradar/support/recon ps
```

Приложение Б
Скрипт на проверку портов

```
#!/usr/bin/python
import sys
import atexit
import os
import argparse
import re
from random import choice
from string import ascii_uppercase

sys.path.append('/usr/local/bin/')

class OpenPorts:
    def __init__(self):
        self.args = []
        self.chainName = "";

    def main(self):
        self.chainName = "TMP_" + self.get_random_postfix()

        # Process arguments
        progName = os.path.basename(sys.argv[0])
        parser = argparse.ArgumentParser(description="Temporarily
open ports")
        parser.add_argument("-i", "--ip", dest='white_list_ips',
action='append', default=[], required=True,
                            help="ipv4 or ipv6 address or cidr to
whitelist")
        parser.add_argument("-p", "--port", dest='ports',
action='append', default=[],
                            help="port to open")
        parser.add_argument("-a", "--all", action='store_true',
help="open all ports")
        parser.set_defaults(a=False)
        args = parser.parse_args()

        if not args.all and len(args.ports) == 0:
            print("No ports defined. Define ports with '-p
<port>' or '-a' to open all ports.")
            exit(1)

        for cidr in args.white_list_ips:
            if not self.validate_ip(cidr):
                print("Invalid ip or cidr provided! " + cidr)
                exit(1)

        self.setup_firewall_iptables(args.white_list_ips,
args.ports, args.all)
        self.prompt_for_completion()
```

Продолжение приложения Б

```
    def setup_firewall_iptables(self, white_list_ips, ports,
open_all_ports):
        """Add new firewall rules to iptables"""

        atexit.register(self.cleanup_firewall_iptables)

        chain_setup_cmd_list = []
        chain_setup_cmd_list.append("iptables -N " +
self.chainName)
        for cidr in white_list_ips:
            chain_setup_cmd_list.append("iptables -I INPUT -s " +
cidr + " -j " + self.chainName)

        if open_all_ports:
            chain_setup_cmd_list.append("iptables -A " +
self.chainName + " -p tcp -j ACCEPT")
        else:
            for port in ports:
                chain_setup_cmd_list.append("iptables -A " +
self.chainName + " -p tcp --dport " + str(port) + " -j ACCEPT")
        setup_cmd = "; ".join(chain_setup_cmd_list)

        setup_rc = os.system(setup_cmd)
        if setup_rc != 0:
            print("An error occurred attempting to register
whitelist cidr with iptables.")
            exit(1)

    def cleanup_firewall_iptables(self):
        print("Restoring iptables state...")
        cmd = "iptables -F " + self.chainName + "; iptables -D
INPUT `iptables -L INPUT --line-numbers | grep '" +
self.chainName + "' | awk '{print $1;}'`; iptables -X " +
self.chainName
        cleanup_rc = os.system(cmd)
        if cleanup_rc != 0:
            print("Unable to restore iptables state. Please
manually execute '" + cmd + "'")


    def prompt_for_completion(self):
        completion_prompt = lambda: (
        raw_input("Press Enter when diagnostics are complete to
lock down the firewall again."))
        completion_prompt()


    def validate_ip(self, ip_address):
        return self.is_valid_ipv4_address(ip_address) or
self.is_valid_ipv6_address(ip_address)
```

```
    def is_valid_ipv4_address(self, ip_address):
        valid_ipv4_regex = re.compile(r"^(([0-9]|[1-9][0-9]|1[0-
9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-
4][0-9]|25[0-5])(\/([0-9]|[1-2][0-9]|3[0-2]))?$")
        return valid_ipv4_regex.match(ip_address) is not None

    def is_valid_ipv6_address(self, ip_address):
        valid_ipv6_regex = re.compile(r"^s*((([0-9A-Fa-
f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-
Fa-f]{1,4}|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(.(25[0-5]|2[0-
4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){5}(((:[0-9A-
Fa-f]{1,4}){1,2})|:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(.(25[0-
5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-
f]{1,4}:){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-
f]{1,4})?:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(.(25[0-5]|2[0-
4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}(((:[0-9A-
Fa-f]{1,4}){1,4})|((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-
4]\d|1\d\d|[1-9]?\d)(.(25[0-5]|2[0-4]\d|1\d\d|[1-
9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}(((:[0-9A-Fa-
f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-
4]\d|1\d\d|[1-9]?\d)(.(25[0-5]|2[0-4]\d|1\d\d|[1-
9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){1}(((:[0-9A-Fa-
f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-
4]\d|1\d\d|[1-9]?\d)(.(25[0-5]|2[0-4]\d|1\d\d|[1-
9]?\d)){3}))|:))|(:(((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-
f]{1,4}){0,5}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(.(25[0-5]|2[0-
4]\d|1\d\d|[1-9]?\d)){3}))|:)))(%.+)?s*(\/(\d|\d\d|1[0-1]\d|12[0-
8]))?$")
        return valid_ipv6_regex.match(ip_address) is not None


    def get_random_postfix(self):
        return ''.join(choice(ascii_uppercase) for i in
range(12))

if __name__ == '__main__':
    openPorts = OpenPorts()
    openPorts.main()
```

Приложение В
Скрипт на запись автоматическую запись логов

```
#!/bin/bash
        SCRIPT=$(echo $0 | awk -F "/" '{print $NF}')
        REV="v5.5"
        SAVE_DIR="/store/LOGS/"
        DEF_SAVE_DIR=$SAVE_DIR
        CUR_DATE=$(date +"%Y%m%d")
        CUR_DATE_DEPLOYMENT_INFO=$(date +"%m-%d-%Y")
        UUIDSHORT=$(cat /proc/sys/kernel/random/uuid | cut -d\- -
   f1)
        GET_LOGS_LOG="get_logs.log"
        GET_DEFECT=""
        GET_REPORTS=""

        # LOG="/dev/null"   #logging off by default, run echo
   /var/log/supportability.log > /opt/qradar/support/.logLocation
   to turn on logging
        LOGCONF=/opt/qradar/support/.logLocation

        # if [ -f "$LOGCONF" ] ; then
        # LOG=$(cat $LOGCONF)
        # fi

        function Log() {
          echo "`date` [getLogs] $@" >> $GET_LOGS_LOG
        }

        function Error() {
          (>&2 echo "[getLogs] [ERROR] $@")
          Log "[ERROR] $@"
        }

        function Run() {
          Log "[RUNNING] $@"
          eval $@ >> $GET_LOGS_LOG 2>&1
          # Log "Running '$@' in '`pwd`'"
          # $@ 2>&1 | tee -a $GET_LOGS_LOG
        }

        CMD="/opt/qradar/support/$SCRIPT"
        IS_CON=$(/opt/qradar/bin/myver -c 2>/dev/null)
        HOST=$(hostname | awk -F. '{print $1}')
        BACKUP_DIR=$(grep                    backup-directory-path
   /opt/qradar/conf/backup-recovery-config.xml     |   perl   -lpe
   's/.*backup-directory-path="(.*?)".*/\1/')
        HA_CONFIG="/opt/qradar/ha/ha.conf"
        HA_STATE=
        IS_HA=
        if [ -f "$HA_CONFIG" ]
```

```
        then
          IS_HA=true
          HA_STATE=$(/opt/qradar/ha/bin/ha state)
        else
          IS_HA=false
fi
```

Приложение Г
Скрипт на провекру запущенных процессов

```
  #!/bin/bash
     LOGDIR=$(cat /etc/qradar_logdir)
     if [ $LOGDIR = "" ] ; then
       LOGFILE=/var/log/wait_for_start.log
       echo "Could not resolve logging directory. Defaulting
to \"$LOGFILE\"."
     else
       # If the log directory doesn't exist (but it should),
create it
       if [ ! -d $LOGDIR ] ; then
            $(mkdir -p $LOGDIR)
       fi
       LOGFILE=$LOGDIR"/wait_for_start.log"
       # If the file doesn't already exist, create it
       if [ ! -f $LOGFILE ] ; then
            $(touch $LOGFILE)
       fi
     fi
     ERROR()
     {
       # Need to make sure the last "ERROR" line is on a line
by it's own
       echo ""
       echo "ERROR: $@"
       if [ -f $LOGFILE ] ; then
            echo ""
            tail -200 /var/log/qradar.log >> $LOGFILE
            echo $(date)" [wait_for_start.sh] [ERROR]: $@" >>
$LOGFILE
            exit 255
       fi
     }
     ECHOINFO()
     {
       echo -e "$@"
       INFO $@
     }
     INFO()
     {
       #If the log file exists, append to it
       if [ -f $LOGFILE ] ; then
            echo -e $(date)" [wait_for_start.sh] [INFO]: "$@
>> $LOGFILE
       fi
     }

     DASHES="----------------------------------------------
------------------------------"
     PrintHeader()
```

```
    {
      PrintDashes

      echo -ne "\r\033[0K"
      printf                                                    "|%-
${PROCESS_COLUMN_WIDTH}.${PROCESS_COLUMN_WIDTH}s" "Process"
      printf   "|%-${TIME_COLUMN_WIDTH}.${TIME_COLUMN_WIDTH}s"
"Seconds"
      printf                                                    "|%-
${STATUS_COLUMN_WIDTH}.${STATUS_COLUMN_WIDTH}s" "Status"
      echo "|"
      LINECOUNT=$(( $LINECOUNT + 1 ))
      PrintDashes
    }

    PrintRow()
    {
      local process="$1"
      local seconds="$2"
      local status="$3"

      echo -ne "\r\033[0K"
      printf                                                    "|%-
${PROCESS_COLUMN_WIDTH}.${PROCESS_COLUMN_WIDTH}s" "${process}"
      printf   "|%-${TIME_COLUMN_WIDTH}.${TIME_COLUMN_WIDTH}s"
"${seconds}"
      printf                                                    "|%-
${STATUS_COLUMN_WIDTH}.${STATUS_COLUMN_WIDTH}s" "${status}"
      echo "|"
      LINECOUNT=$(( $LINECOUNT + 1 ))
    }

    PrintDashes()
    {
      echo -ne "\r\033[0K"
      printf                                                    "+%-
${PROCESS_COLUMN_WIDTH}.${PROCESS_COLUMN_WIDTH}s" "${DASHES}"
      printf   "+%-${TIME_COLUMN_WIDTH}.${TIME_COLUMN_WIDTH}s"
"${DASHES}"
      printf                                                    "+%-
${STATUS_COLUMN_WIDTH}.${STATUS_COLUMN_WIDTH}s" "${DASHES}"
      echo "+"
      LINECOUNT=$(( $LINECOUNT + 1 ))
    }

    MoveCursorBack()
    {
      echo -e "\033[${LINECOUNT}A"
      LINECOUNT=1
  }
```

Приложение Д
Скрипт на соответствие определённым значениям

```
#!/bin/bash
database_type=$1
custom=$2
offense_name=$3
offense_id=$3
auth_header="SEC:$api_token"
output=$(curl -k -H $auth_header
https://$console_ip/console/restapi/api/
asset_model/assets?filter=interfaces%20contains%20%28%20ip_a
ddresses
%20contains%20%28%20value%20%3D%20%22$offense_source_ip
%22%29%29)
# Basic print out of the output of the command echo
$output
```

Приложение Ж
Скрипт смены пароля для пользователей и администратора

```
  #!/bin/bash
     SCRIPT=$(echo $0 | awk -F "/" '{print $NF}')
     REV="v1.8"
     [          -z          $NVA_CONF          ]          &&
NVA_CONF="/opt/qradar/conf/nva.conf"
     NVACONF=`grep "^NVACONF=" $NVA_CONF 2> /dev/null |
cut -d= -f2`
     USERS_CONFIG_FILE="users.conf"
     CONFIGSERVICES_SEARCH_STRING="configuration.services
.password"

     # Changes the hashed passwords in users.conf (no
longer needed after 7.2.8)
     function changeHash()
     {
       local TARGET=$1
       PASSWD=$2
       MYFILE=$3

       if [ ! -e "$MYFILE" ]
       then
            echo "File $MYFILE does not exist!"
            return
       fi
       [ $VERBOSE ] && echo "Backing up original $MYFILE
..." && cp -v $MYFILE /tmp/$(echo $MYFILE | awk -F\/
'{print $NF}').orig || cp $MYFILE /tmp/$(echo $MYFILE |
awk -F\/ '{print $NF}').orig
       [ $VERBOSE ] && echo "Altering $MYFILE ..."
       sed "s@$TARGET:[^:]*:@$TARGET:$PASSWD:@" $MYFILE >
/tmp/$USERS_CONFIG_FILE.$$
       mv /tmp/$USERS_CONFIG_FILE.$$ $MYFILE
       chown "nobody:nobody" $MYFILE
     [ -z $NVACONF ] && NVACONF="/opt/qradar/conf"
     EVERYWHERE=
     TARGET=
     PASSWORD=
     PASSWORDSALT=
     PASSWORDSALTHEX=
  VERBOSE=
```

Приложение И
Скрипт на вывод информации об инциденте

```
    from java.util import Date

    # Built-in date/time fields include: create_date,
discovered_date, start_date, end_date
    dt_raw = incident.discovered_date
    log.info("Discovered date (raw value: epoch
milliseconds): {}".format(dt_raw))

    # Use the Java Date object to work with date and
time values
    dt_date = Date(incident.discovered_date)
    log.info("Discovered date (millis):
{}".format(dt_date))

    year = dt_date.getYear() + 1900
    log.info("Year: {}".format(year))

    month = dt_date.getMonth()
    log.info("Month: {}".format(month))

    weekday = dt_date.getDay()
    log.info("Day of week: {}".format(weekday))

    day = dt_date.getDate()
    log.info("Day of month: {}".format(day))

    millis = dt_date.getTime()
log.info("Milliseconds timestamp: {}".format(millis))
```

Приложение К
Скрипт на вывод информации об инциденте

```
import re
from java.util import Date
now = Date()

# Status mapping similar to ENTRY_TO_DATATABLE_MAP, it
maps the LDAP account status codes to meaningful messages
status_dict = {
   66050: "Disabled, password doesn't expire",
   514: "Disabled account",
   66048: "Enabled"
   }

#=============================================================
=============================================================
====
def convert_when_created_to_EPOCH(PwdLastSet_string):
  """ This function converts the when_created string
value to EPOCH format """

  regex     =     "([0-9]{4})-([0-9]{2})-([0-9]{2})\s([0-
9]{2}):([0-9]{2}):([0-9]{2})+\+([0-9]{2}):([0-9]{2})"
  months = {
  'Jan': "01",
  'Feb': "02",
  'Mar': "03",
  'Apr': "04",
  'May': "05",
  'Jun': "06",
  'Jul': "07",
  'Aug': "08",
  'Sep': "09",
  'Oct': "10",
  'Nov': "11",
  'Dec': "12"
  }
  PwdLastSet_list           =           re.findall(regex,
PwdLastSet_string)[0]

  for key, value in months.items():
    if value == str(PwdLastSet_list[1]):
      PwdLastSet_formatted_string = key

  PwdLastSet_formatted_string                              =
PwdLastSet_formatted_string + ' ' + PwdLastSet_list[2]+', ' +
PwdLastSet_list[0]  +  '  '  +  PwdLastSet_list[3]  +  ':'  +
PwdLastSet_list[4] + ':' + PwdLastSet_list[5]

  PwdLastSet_EPOCH                                         =
Date.parse(PwdLastSet_formatted_string)
```

```
      return PwdLastSet_EPOCH
    #Main part starts here!

    if(results.success):
            row = incident.addRow("ldap_query_results")

      dictionary = results.entries[0]

      for key, value in dictionary.iteritems():
        if key == u'cn' and value is not None:
          row['fullname'] = value
          continue
        if key == u'cn' and value is None:
          row['fullname'] = 'N/A'


        if key == u'sn' and value is not None:
          row['surname'] = value
          continue
        else:
          row['surname'] = 'N/A'

        if key == u'mail' and value is not None:
          row['email_address'] = value
          continue
        if key == u'mail' and value is None:
          row['email_address'] = 'N/A'
    _attribute'] = Epoch_time
          continue

        if key == u'userAccountControl' and value is not
None:
          row['useraccountcontrol_attribute'] = value
          # Check, whether the ldap_status integer can be
found between the status_dict's keys

            # Add the meaningful message to the corresponding
data table column, and if the ldap_status code is not found in
status_dict map we simply write NOPE into that column
            row['account_status']   =   status_dict.get(value,
"NOPE")
            continue
        if key == u'userAccountControl' and value is None:
          row['useraccountcontrol_attribute'] = 'N/A'

 row['timestamp'] = Date()
```

Приложение Л
Скрипт на изменение владельца инцидента

```
     # Set the 'closed_by' field to the current user.
     # Should be called from an automatic rule, when the incident
is closed.

     # Scripts that run from a timer will run as "system", ignore
these
     if principal.type != "user":
       log.error("Cannot run as '{}' {}".format(principal.type,
principal.display_name))

     else:
       # Set closed_by to the current user
       incident.properties.closed_by = principal.display_name
```

Приложение М
Скрипт, определяющий действия, связанные с инцидентом

```
    # Record the user who was first assigned a task in the
incident
    #
    # This script should be run from an Automatic rule on a
Task.
    #
    # If the incident does not yet record a value for custom
field "who_first_edited",
    # and if the task is assigned,
    # record the task's "owner_id" (the email address of the
task assignee).

    if not incident.properties.who_first_edited:
        incident.properties.who_first_edited                    =
```

Приложение Н
Скрипт на создание инцидента

```
#!/usr/bin/env python

"""
Simple script to create a new incident.
"""
from __future__ import print_function
import time
import logging
import resilient


logging.basicConfig()


class ExampleArgumentParser(resilient.ArgumentParser):
    """Arguments for this command-line application,
extending the standard Resilient arguments"""

    def __init__(self, config_file=None):
        super(ExampleArgumentParser,
self).__init__(config_file=config_file)

        self.add_argument('--name', '-n',
                          required=True,
                          help="The incident name.")

        self.add_argument('--description', '-d',
                          required=True,
                          help="The incident description.")

        self.add_argument('--itype', '-t',
                          action='append',
                          help="The    incident    type(s).
Multiple arguments may be supplied.")


def main():
    """
    program main
    """

    parser                                                =
ExampleArgumentParser(config_file=resilient.get_config_file())
    opts = parser.parse_args()

    inc_name = opts["name"]
    inc_desc = opts["description"]
    inc_types = opts["itype"]
```

Продолжение приложения Н

```
        # Create SimpleClient for a REST connection to the
Resilient services
        client = resilient.get_client(opts)

        # Discovered Date will be set to the current time
        time_now = int(time.time() * 1000)

        # Construct the basic incident DTO that will be posted
        new_incident = {"name": inc_name,
                        "description": inc_desc,
                        "incident_type_ids": inc_types,
                        "discovered_date": time_now}

        try:
            uri = '/incidents'

            # Create the incident
            incident = client.post(uri, new_incident)

            inc_id = incident["id"]

            print("Created incident {}".format(inc_id))

        except resilient.SimpleHTTPException as ecode:
            print("create failed : {}".format(ecode))

    if __name__ == "__main__":
    main()
```

Список литературы

1 IBM Knowledge Center: IBM QRadar SIEM documentation // ibm.com: Инструкция администратора. URL: https://www.ibm.com/support/knowledge center/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_admin_guide.pdf?view=kc (дата обращения: 08.03.2020).

2 Cisco OpenSOC — open source решение для создания собственного центра мониторинга киберугроз. [Электронный ресурс]. URL: http://habrahabr.net/thread/1370 (дата обращения 01.03.2020).

3 Автоматизация процессов кибербразведки на основе решений класса Threat Intelligence Platform (TIP). [Электронный ресурс]. URL: https://www.anti-malware.ru/practice/methods/threat-intelligence-platform (дата обращения 15.03.2020).

4 IBM Knowledge Center: IBM QRadar SIEM documentation // ibm.com: Установка. URL: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_siem_inst.pdf?view=kc (дата обращения: 13.04.2020).

5 Цели и методы работы SIEM-системы. URL: https://searchinform.ru/products/siem/sravnenie-siem-sistem/ (дата обращения 19.03.2020).

6 ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. Введ. 01.01.2012. М.: Стандартинформ, 2012. 62 с. (дата обращения 19.03.2020).

7 Программно-аппаратные средства защиты передачи данных по каналам связи. [Электронный ресурс]. URL: https://studbooks.net/2008449/informatika/programmno_apparatnye_s redstva_zaschity_peredachi_dannyh_kanalam_svyazi (дата обращения 23.03.2020).

8 Macaulay T. Upstream intelligence: anatomy, architecture, case studies and use-cases // Information Assurance Newsletter. 2011. V. 14. P. 18–22 (дата обращения 23.03.2020).

9 Catteddu D., Hogben G. Cloud computing: benefits, risks and recommendations for information security. Heraklion: ENISA, 2009 (дата обращения 23.03.2020).

10Knowledge center // IBM QRadar SIEM. URL: https://www.ibm.com/support/knowledgecenter. (дата обращения: 23.03.2020).

11Use ibm resilient // Resilient Incident response platform. URL: https://community.ibm.com/community/user/security/blogs/andysu/2018/11/27/use-ibm-resilient-incident-response-platform (дата обращения: 12.04.2020).

12Ефремова О.С. Документация по охране труда в организации. [Текст] Практическое пособие /О.С. Ефремова 5-е изд. перераб. и доп. -М.: Изд. “Альфа-Пресс”,2015 г. – 152 с (дата обращения 27.04.20202)

13 Об утверждении Санитарных правил // Об утверждении Санитарных правил "Санитарно-эпидемиологические требования к объектам здравоохранения"/ URL: http://adilet.zan.kz/rus/docs/V1700015760 (дата обращения 27.04.20202)

14 СН 32.23-85 «Санитарные нормы допустимого шума на рабочих местах». URL: http://www.normacs.ru/Doclist/doc/1LP.html (дата обращения 27.04.20202)

15 СНиП II-12-77 «Защита от шума». URL: http://gostrf.com/normadata/1/4294854/4294854802.pdf. (дата обращения 27.04.20202)

16 Юрист – Параграф Online // Закон РК от 27 июля 2006 года № 152-ФЗ «О персональных данных» // URL: https://online.zakon.kz/m/document/?doc_id=30464339/ (дата обращения 27.04.20202)