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: Расследование инцидентов безопасности с помощью системы комплексной защиты «SIEM»

Специальность Системы Информационной Безопасности_____

Выполнил(а) Сапиев Алишер Галимович_____ Группа СИБ-16-2___
(Ф.И.О.)

Научный руководитель к.т.н., профессор Тынымбаев С.Т._____
(ученая степень, звание, Ф.И.О.)

Консультанты:
по специальной части:
старший преподаватель Тергеусизова Алия Советжанова_____

_____ «_____» _____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: _____
(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 Сапиеву Алишеру Галимовичу
(Ф.И.О.)

Тема проекта «Расследование инцидентов безопасностис помощью системы комплексной защиты «SIEM»

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 –топология сети предприятия, тестовая лицензия ESXi, тестовая лицензия IBM QRadar, физический сервер HP.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Цель работы - проектировка и организация системы комплексной защиты для предприятия. Акцент делается на организации расследования инцидента и описания использования всех требуемых для этого средств. Задача – организация мер по реагированию на инцидент и разработка правил обработки новых источников.

Перечень графического материала (с точным указанием обязательных чертежей): топология сети компании

Основная рекомендуемая литература: Дэвид Миллер Security Information and Event Management (Siem) Implementation, веб-сайт www.ibm.com, Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Анали 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 гипервизора	17.02.2020 – 20.02.2020	
Установка SIEM системы	21.02.2020 – 28.02.2020	
Первоначальная настройка SIEM	01.03.2020 – 08.03.2020	
Установка модуля Resilient	09.03.2020 - 18.03.2020	
Разработка регулярных выражений	19.03.2020 – 27.03.2020	
Построение плана расследования инцидента	28.03.2020 - 07.04.2020	
Расследование инцидента	08.04.2020 - 18.04.2020	
Составление вывода и отчета по иниденту	19.04.2020 - 30.04.2020	
Анализ рисков ИБ. БЖД	01.05.2020 - 09.05.2020	

Аннотация

В рамках данной дипломной работы была рассмотрена тема управления событиями информационной безопасности с помощью системы мониторинга и анализа событий IBM QRadar SIEM.

В результате проведенных работ сформулированы следующие результаты:

а) представлен обзор SIEM системы и краткие характеристики данного продукта;

б) согласовано размещение сервера, установлен гипервизор, собран RAID – массив и настроен удаленный доступ;

в) была определена топология сети и выделены IP-адреса, а также сделана начальная конфигурация IBM QRadar;

г) разработаны и настроены дополнительные правила, настроен парсинг журналов событий, а также расследован инцидент информационной безопасности.

Annotation

As part of this thesis, the topic of information security event management using the IBM QRadar SIEM event monitoring and analysis system was considered.

As a result of the work, the following results are formulated:

а) provides an overview of the SIEM system and brief characteristics of this product;

б) the server location was agreed, a hypervisor was installed, a RAID array was assembled, and remote access was configured;

в) the network topology was determined and IP addresses allocated, and the initial configuration of IBM QRadar was made;

г) additional rules were developed and configured, parsing of event logs was configured, and an information security incident was investigated.

Аңдатпа

Дипломдық жұмыстың бөлігі ретінде IBM QRadar SIEM оқиғаларын бақылау және талдау жүйесін қолдана отырып, ақпараттық қауіпсіздік оқиғаларын басқару тақырыбы қарастырылды.

Жұмыстың нәтижесінде келесі нәтижелер тұжырымдалады:

а) SIEM жүйесі мен осы өнімнің қысқаша сипаттамаларын ұсынады;

б) сервердің орналасуы келісілді, гипервизор орнатылды, RAID массиві жиналды және қашықтан қол жетімділік конфигурацияланды;

в) желінің топологиясы анықталып, IP мекенжайлары бөлінді және IBM QRadar бастапқы конфигурациясы жасалды;

г) қосымша ережелер жасалды және конфигурацияланды, оқиғалар журналын талдау жасалды, ақпараттық қауіпсіздік оқиғасы зерттелді.

Содержание

Введение

В последнее время в Казахстане, как и в других странах стали актуальны проблемы автоматизации процессов информационной безопасности.

Каждый день внедряются десятки и сотни средств защиты информации и каждое из этих средств отличается своей сложностью и неоднородностью. Службами информационной безопасности, имеющих на вооружении различные программно-технические средства, такие как антивирусное программное обеспечение, системы предотвращения утечек данных, системы предотвращения и обнаружения вторжений, журналы событий, а также различные сканеры безопасности ежедневно анализируются десятки инцидентов и событий.

В связи с этим требуется высококачественный продукт, который централизует активность систем информационной безопасности в зависимости от поставленных целей и задач. Ведущие специалисты в области информационной безопасности доказывают на основе статистик инцидентов, предоставленных крупными организациями, что для обеспечения комплексного подхода на реагирование и расследование событий информационной безопасности необходимы централизованные системы. Некачественный мониторинг событий может отрицательно повлиять на выявление инцидента, что может обернуться для организации крупными потерями.

Системы мониторинга событий в современном мире отличаются своей постоянной актуальностью в связи с возрастанием количества угроз и нарушений, а также для постоянного анализа событий безопасности.

Целью работы является внедрение системы мониторинга и анализа событий информационной безопасности QRadar на предприятии и расследование инцидента информационной безопасности.

Для достижения цели необходимо:

а) изучить архитектуру системы;

б) обозначить методы и последовательность рефлекторного обнаружения и анализа свежих данных событий информационной безопасности;

в) внедрить систему мониторинга событий безопасности;

г) определить событие информационной безопасности;

д) провести расследование инцидента.

1 Теоритическая часть

1.1 Описание IBM QRadar SIEM

Безопасность информации и защита объектов от текущих угроз.

IBM QRadar SIEM определяет события с тысячи устройств находящихся в сети компании и анализирует, нормализует события и отделяет потенциальные угрозы от ошибочных срабатываний. Также к системе прилагается IBM Security X-Force Threat Intelligence. X-Force обладает списком потенциально опасных IP-адресов, найденные угрозы, источники спама и другие угрозы [1].

В IBM QRadar SIEM применяется следующие функции:

а) отображение событий в режиме реального времени с целью определения угроз и установке приоритета для главных задач. Выявление ошибочных и незначительных угроз;

б) сбор событий с операционных систем, программ, баз данных и систем безопасности. Сбор данных с маршрутизаторов и коммутаторов о сетевых потоках;

в) сбор данных с систем управления, серверов DHCP, сканеров уязвимостей. Назначение приоритетов и снижение тревожных сигналов;

г) быстрая нормализация и взаимодействие с остальной информацией. Снижение количества потоков и выявления действительных нарушений;

д) поиск отклонений в поведении пользователей, клиентов и сетевых устройств. Использование IBM X-Force для действий связанными с подозрительными IP-адресами;

е) эффективное управление угрозами и настройка детальных отчетов. Поиск информации в реальном времени и в сохраненных данных потока информации;

ж) дополнительные устройства QRadar QFlow и QRadar VFlow для углубленного анализа. Использование централизованного интерфейса, совмещающего управление, регулирование инцидентов, отчетность и другим функциям.

1.2 Системные требования

Для правильной работы IBM QRadar SIEM необходимо знать минимальные требования к виртуальным устройствам. Минимальные требования расчитаны на использование QRadar только с минимальным набором данных, использованием приложений по умолчанию и на минимальной производительности.

Конфигурация «All-in-one» предоставляет 200000 событий в минуту и до 5000 событий в секунду и минимально для данной конфигурации необходимо 32 ГБ памяти и рекомендовано 48 ГБ. Для дополнительных модулей таких как: сервера для приложений (App Host), резервного сервера (HA), сервера Risk Manager, Vulnerability Manager также необходимы дополнительные ресурсы памяти. Данные приведены в таблице 1.1.

Таблица 1.1 – Системные требование к оперативной памяти

Ресурс	Минимально	Рекомендовано
QRadar App Host	12 GB	64 GB
QRadar Risk Manager	24 GB	48 GB
QRadar High-Availability	32 GB	48 GB
QRadar Vulnerability Manager	32 GB	32 GB

Также при конфигурации «All-in-one» производитель рекомендует использование 24 ядер процессора и минимально 4 ядра.

Для дополнительных модулей также необходимы дополнительные ресурсы процессора. Данные приведены в таблице 1.2

Таблица 1.2 – Системные требования к процессору

Ресурс	Минимально	Рекомендовано
QRadar App Host	4	12
QRadar Risk Manager	8	8
QRadar High-Availability	4	24
QRadar Vulnerability Manager	4	4

Любая конфигурация IBM QRadar требует минимум 256 ГБ памяти хранилища.

1.3 Обзор панелей и веб-интерфейса

С помощью пользовательского интерфейса мы получаем возможность полного управления нашей системой, а также возможность анализа событий информационной безопасности.

Доступ к консоли предоставляется с помощью безопасного протокола HTTPS с наличием шифрования.

В консоли IBM QRadar основными вкладкам являются: Dashboard, Offences, Log Activity, Network Activity, Assets, Reports, Pulse и Admin [1].

Вкладка Dashboard предоставляет нам панели с различной информацией из различных источников, что дает нам возможность анализа всей поступающей информации на QRadar (рисунок 1.1).

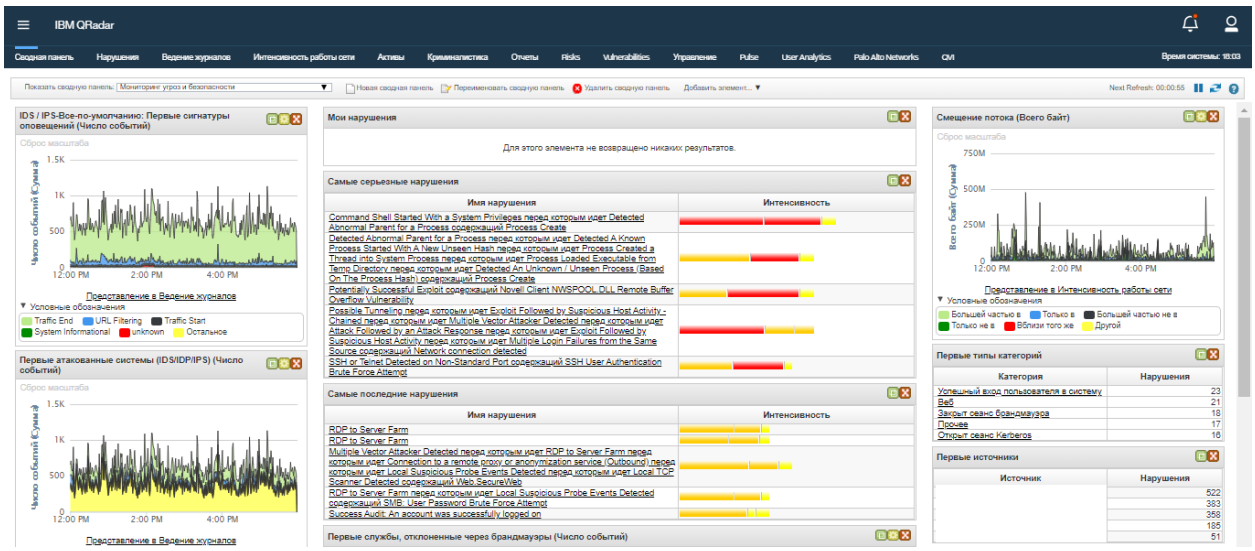


Рисунок 1.1 - Вкладка Dashboard

Вкладка Offences отображает все нарушения, зарегистрированные системой. Также в Offences производится настройка правил (рисунок 1.2).

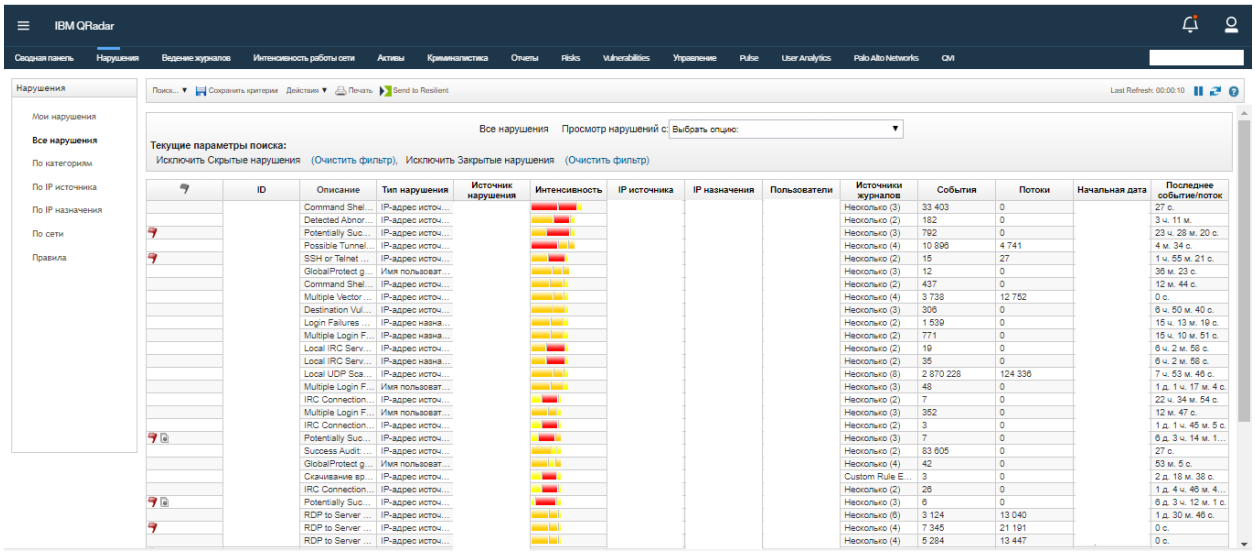


Рисунок 1.2 - Вкладка Offences

Во вкладке Log Activity система отображает нам все события безопасности, нормализованные системой (рисунок 1.3).

Во вкладке Network Activity система отображает нам все сетевые потоки, нормализованные системой (рисунок 1.4).

Вкладка Assets предоставляет обзор на профили устройств, обнаруженные сервера и сканеры (рисунок 1.5).

Во вкладке Reports администраторы системы могут выводить данные в отчеты (рисунок 1.6).

Вкладка Pulse предоставляет офицерам безопасности доступ к данным о нарушениях информационной безопасности по всему миру (рисунок 1.7).

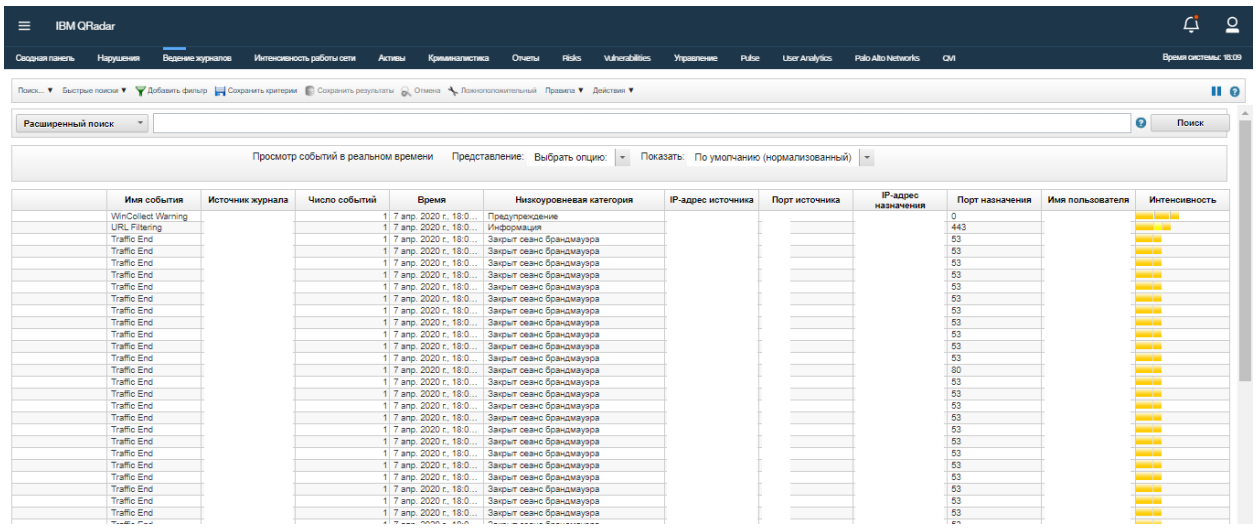


Рисунок 1.3 - Вкладка Log Activity

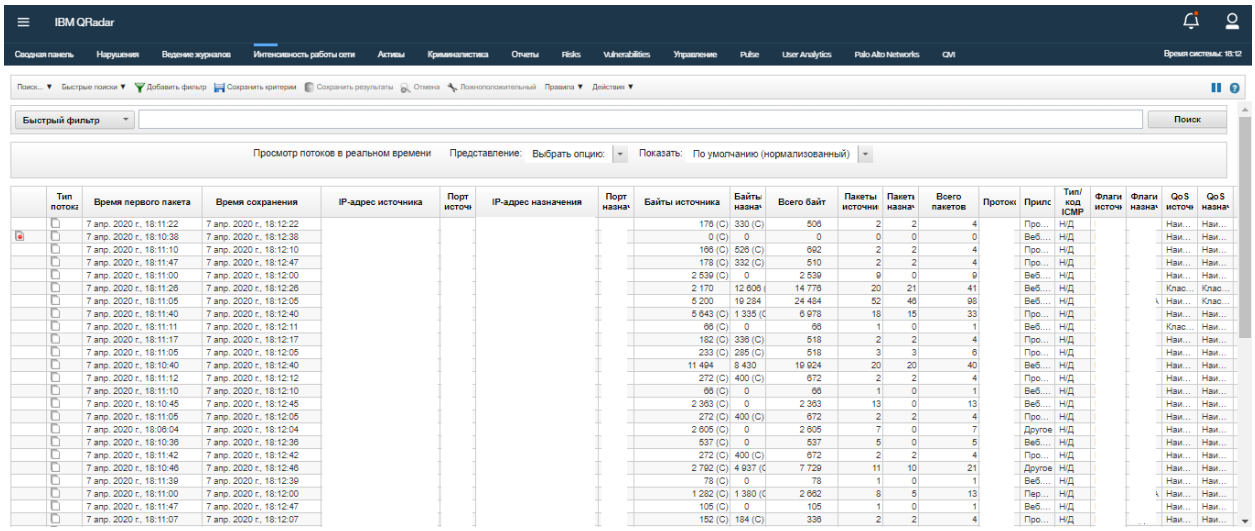


Рисунок 1.4 - Network Activity

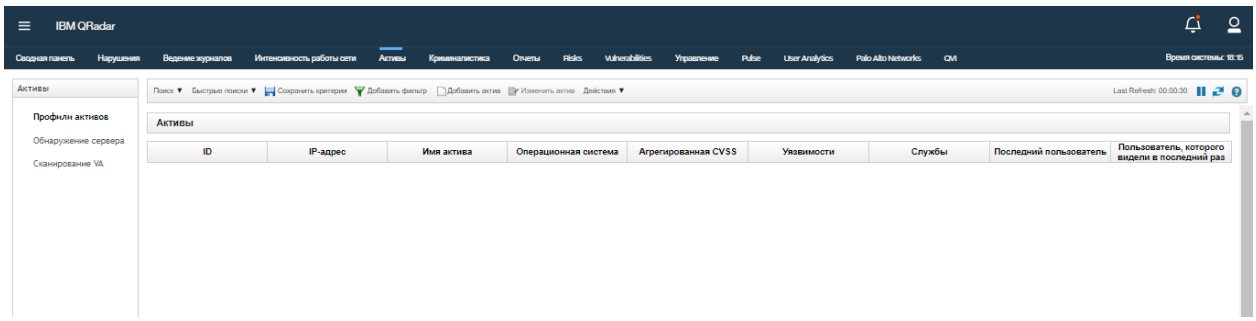


Рисунок 1.5 - Вкладка Assets

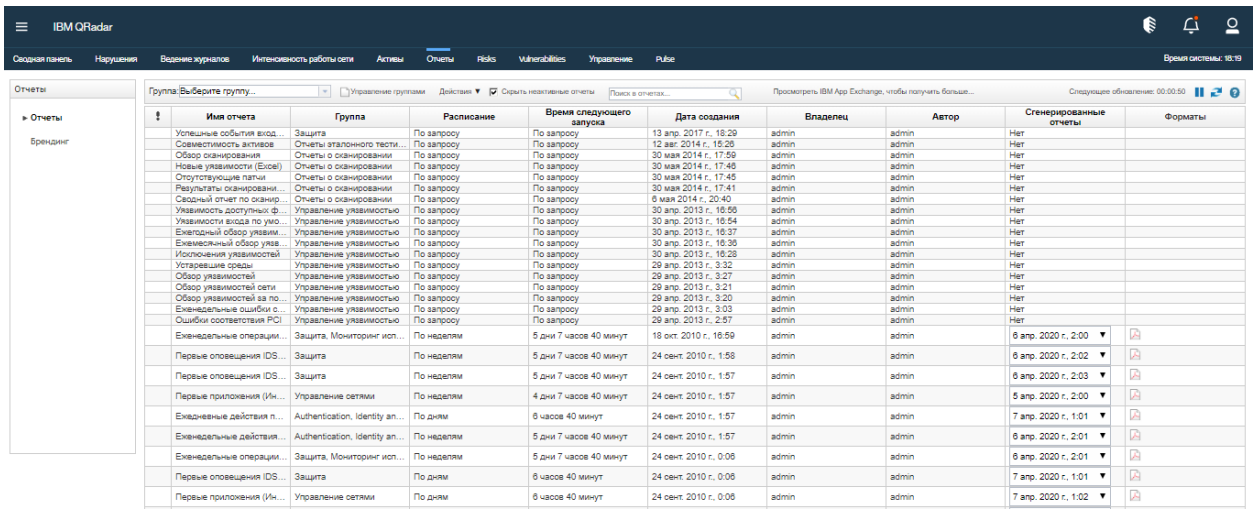


Рисунок 1.6 – Вкладка Reports

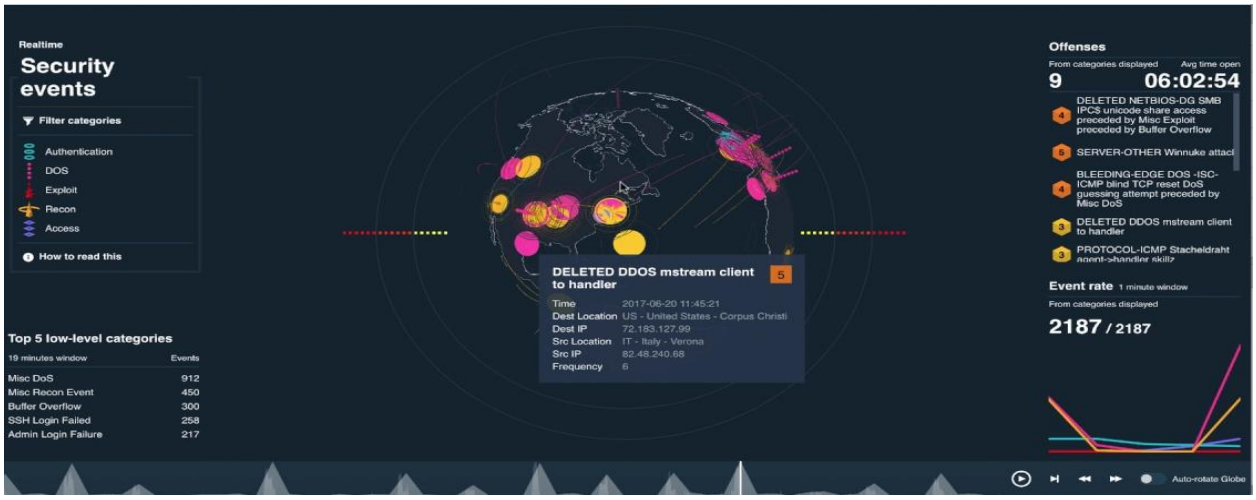


Рисунок 1.7 – Вкладка Pulse

Во вкладке Admin осуществляется основное управление и настройка системы, пользователей и источников событий (рисунок 1.8).

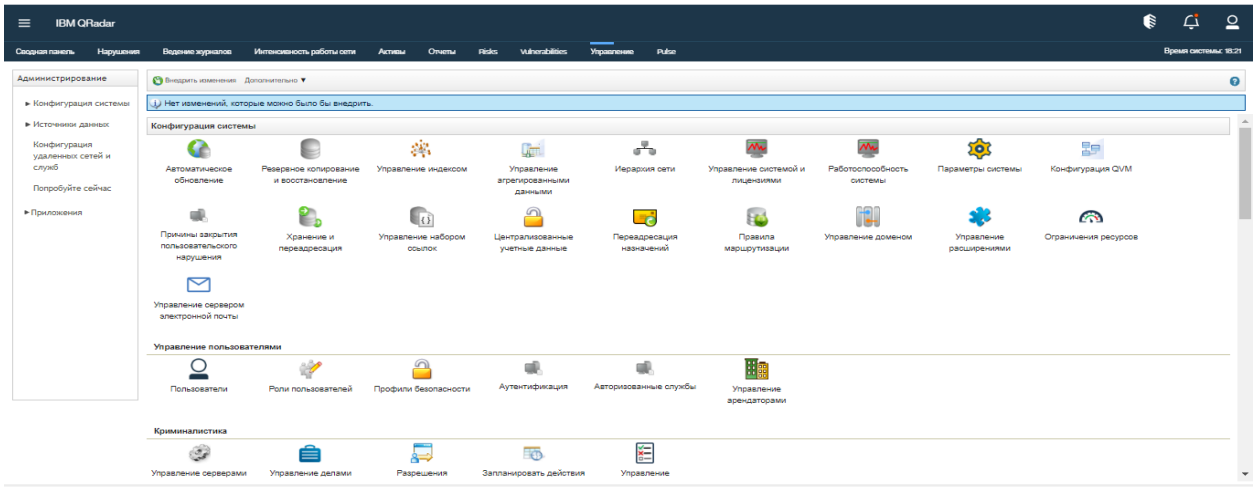


Рисунок 1.8 – Вкладка Admin

1.4 Архитектура

При создании архитектуры для IBM QRadar, важно понимать как компоненты QRadar будут функционировать в сети компании, для последующего планирования и развертывания.

IBM QRadar SIEM представляет собой модульную архитектуру, которая показывает IT-инфраструктуру компании в настоящем времени, что дает офицерам безопасности своевременно обнаруживать угрозы и определять приоритетные задачи. В IBM QRadar можно добавить модули по управлению рисками, уязвимостями и компьютерной криминалистике [2].

Процесс работы платформы, независимо от структуры развертывания, состоит из трех уровней (рисунок 1.9).

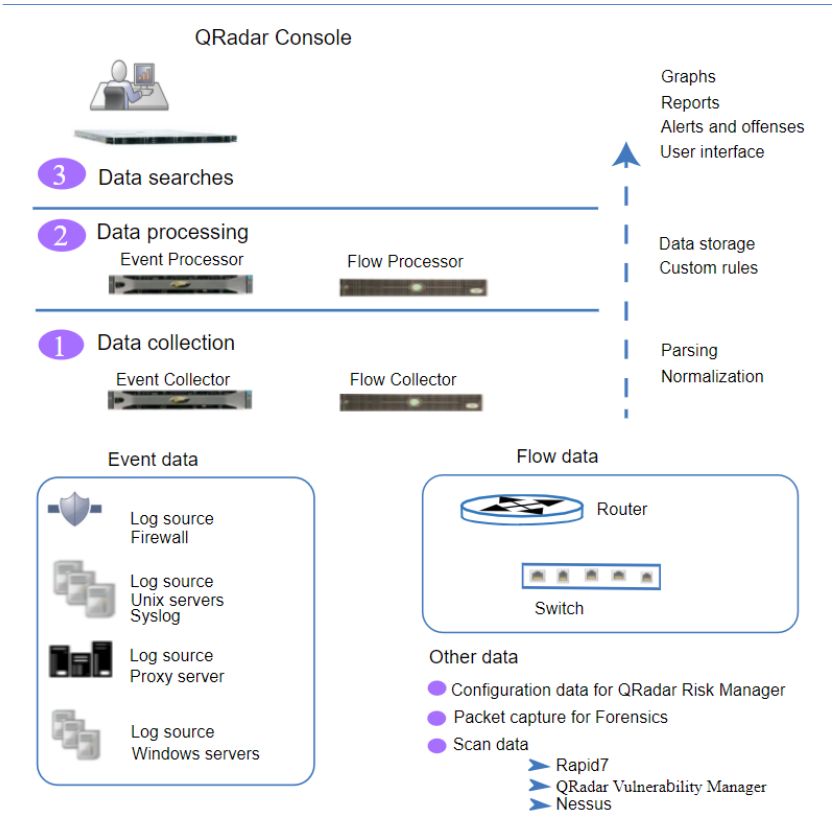


Рисунок 1.9 – Модульная архитектура

Сбор данных – это первый уровень, в котором ведется сбор данных и потоков со всей сети компании. Сбор данных является одной из самых важных функций в QRadar. Идет сбор таких данных как: авторизация пользователя в систему, VPN-подключения, данные межсетевого экрана, электронная почта, прокси-подключения и любые другие события. Данные анализируются и нормализуются перед передачей на вышестоящий уровень обработки.

Далее данные попадают на уровень обработки и проходят через алгоритмы пользовательских правил, которые в свою очередь создают нарушения или предупреждения.

На третьем уровне данные доступны пользователям для поиска, анализа, составления отчета и расследований.

Компоненты QRadar:

а) QFlow Collector – является пассивным сборщиком транспортных потоков с помощью зеркалированных портов сетевых устройств;

б) Event Collector – занимается сбором событий с локальных и удаленных устройств, а также их нормализацией;

в) Event Processor – получает события с Event Collector, коррелирует информацию и отправляет ее в соответствующую область в зависимости от типа события. Также обладает информацией об изменении поведенческих моделей или нарушении политик. После завершения обработки процессор пересылает событие в Magistrate;

г) Magistrate является одним из основных компонентом для обработки событий информационной безопасности. Magistrate нужен для обзора, отчетности, оповещений и анализа сетевого трафика и событий безопасности;

д) Data Node используется для добавления дополнительных ресурсов хранения и обработки информации;

е) QRadar App Host – управляемый узел, используемый для запуска приложений, требующих дополнительных вычислительных ресурсов и памяти;

ж) Console – это пользовательский интерфейс для QRadar. Консоль дает нам возможность администрирования, просмотра всей информации по потокам и событиям в реальном времени, проходящих через QRadar. Доступ осуществляется с помощью браузера.

Под топологией понимают взаимное расположение узлов сети в зависимости друг от друга. К узлам сети относятся: маршрутизаторы, коммутаторы, точки доступа, сервера и конечные точки. Топология помогает понять где и какой узел с чем связан и где в случае сбоя искать неисправность. Схема сети компании обозначена на рисунке 1.10.

Данная построенная топология отображает нахождение сервера ESXi, где расположена консоль QRadar, относительно других узлов сети заказчика.

Также к серверу ESXi протянут SPAN (Switch Port Analyzer) предназначенный для дублирования трафика. Это применяется для мониторинга трафика в целях безопасности и оценки производительности сетевого оборудования.

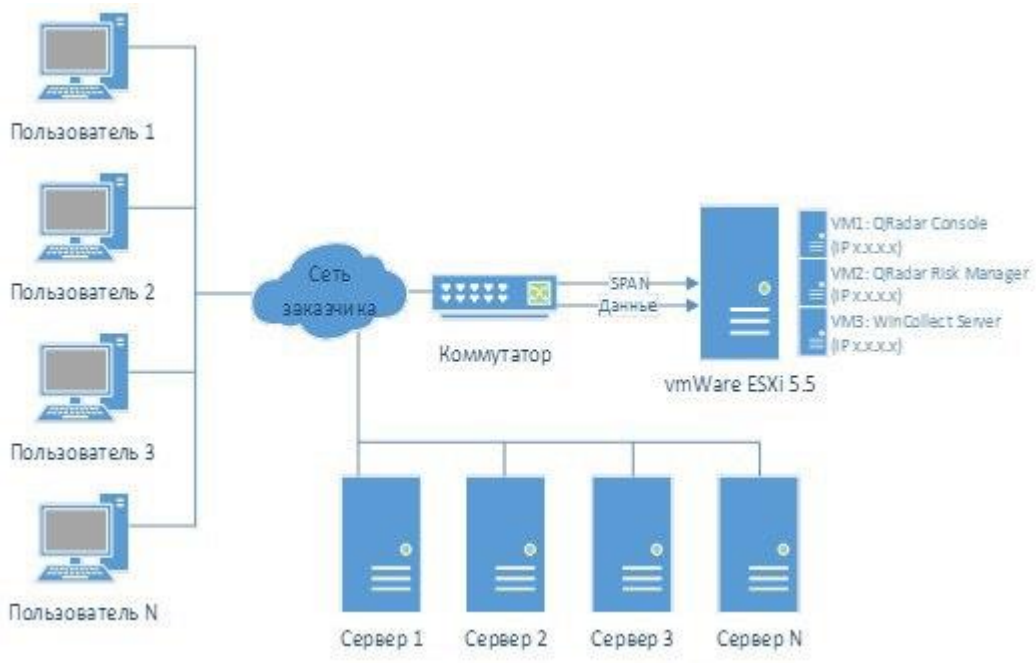


Рисунок 1.10 – Топология сети предприятия

1.5 Достоинства и недостатки

Как и любая другая SIEM система IBM QRadar обладает своими преимуществами и недостатками.

Минусы:

а) потеря событий при превышении лицензионных метрик;

б) слабая система визуализации при построение отчетов, нет возможности редактировать уже примененные фильтры при поиске, неудобный поиск событий.

Плюсы:

а) передовые технологии для построения SOC;

б) машинное обучение, анализ поведения пользователей, управления уязвимостями, базы Threat Intelligence;

в) эффективность реагирования на новые инциденты;

г) легкая масштабируемость и многофункциональность;

д) поддержка продуктов более чем 200 производителей;

е) поддержка дополнительных бесплатных модулей.

1.6 IBM Resilient

IBM Resilient IRP - это специально созданный инструмент для уникальных требований последовательного и эффективного управления инцидентами безопасности, связанными с компьютером, или нарушением личной информации. IBM Resilient IRP является центральным узлом реагирования на инциденты. Ключевой особенностью IBM Resilient является настройка под конкретные нужды каждой компании. Поэтому, взаимодействие с платформой Resilient, напрямую зависит от этих настроек [10].

Организация разрабатывает и реализует набор правил, условий, бизнес-логики и задач, используемых для реагирования на инцидент. Этот набор упоминается как динамический сценарий. Эти сценарии предоставляют платформе Resilient средство автоматического обновления ответа на инцидент по мере изменения входных данных или прохождения инцидента.

Управление пользователями и их ролями находится во вкладке Пользователи. Во вкладке «Пользователи» можно создавать новые учетные записи, назначать группы, назначать рабочие пространства, назначать роли, переназначать инциденты и задачи, деактивировать и удалять пользователей.

Группы пользователей необходимы для решения инцидента определенной командой специалистов. Могут быть созданы разные команды, которые добавляются к инциденту в зависимости от типа инцидента, местоположения или наличия в инциденте компонента нарушения конфиденциальности. Группы могут быть созданы на вкладке Группы.

Рабочие пространства служат контейнерами или разделами для группировки различных инцидентов и позволяют вам более эффективно управлять инцидентами в нескольких группах, а также внутри групп. Они предоставляют возможность назначать конкретные инциденты конкретным командам, ограничивая доступ и контроль только для команд и пользователей, которым это необходимо. Можно создать и настроить рабочее пространство для группы безопасности и второе рабочее пространство для группы ИТ-операций. В этих двух рабочих пространствах каждая команда управляет своими инцидентами безопасности или ИТ-операциями отдельно и независимо.

1.7 Сравнение с аналогами

В последнее время SIEM системы получили широкое применение на рынке обеспечения защиты информации. На ровне с зарубежными производителями выступили на рынок и российские разработки. Проанализировав динамику развития SIEM компания SIEM Analytics предоставила график доли рынка SIEM для Российской Федерации в котором большую часть рынка занимают IBM QRadar SIEM и HP ArcSight SIEM (22% и 25% соответственно).

HP ArcSight – программно-аппаратное устройство компании Hewlett Packard. Данное решение является одним из лидирующих в сфере контроля и мониторинга информации. Система HP ArcSight может обрабатывать большое количество событий и автоматизировать систему безопасности.

Основной функционал платформы состоит из сбора журналов, управления и генерации отчетов. Система Arcsight Enterprise Security Management рассчитана на широкомасштабную полосу развертывания и мониторинга безопасности. Комплекс имеет тип установки «All in one». Система разворачивается как виртуальный образ или программное-обеспечение.

Помимо основного функционал как SIEM системы, ArcSight предлагает систему выявления аномалий пользователей, анализ DNS трафика, дает доступ

к интерактивной базе знаний. Также на портале вендора в Marketplace можно дополнительно получить доступ к дополнительным правилам и приложениям.

К особенностям HP ArcSight можно отнести то, что вендор внедрил как сложные и функциональные правила корелляции, так и упрощенный для простых ситуаций. Минимальные требования к системе описаны в таблице 1.3.

Таблица 1.3 - Минимальные требования к оборудованию HP ArcSight

CPU	1 или 2x Intel Xeon Quad Core или аналогичный
RAM	4 – 12 Gb
Disk space	4 – 12 Gb

Российская разработка «СёрчИнформ SIEM» является одним из современных решений систем мониторинга и анализа событий для малого и среднего бизнеса. Также, как и другие SIEM системы, она постовляется с готовым набором правил, которые анализируют и автоматизируют поиск необычной активности в инфраструктуре компании.

На сегодняшний день разработчики дополнили арсенал SIEM картой инцидентов, которая в реальном времени отображает состояние текущих задач и инцидентов.

Достоинствами данной системы являются: простота внедрения и обучения пользователей, дополнительное обнаружение системных, программных и аппаратных сбоев, низкие минимальные требования, а также приемлемая цена.

К недостаткам систем можно отнести отсутствие системы анализа поведения пользователей, небольшое количество коннекторов, а также небольшое разнообразие визуализации. Но все эти недостатки можно отнести к новизне решения и система развивается и дополняется с каждым новым релизом. Минимальные требования к оборудованию описаны в таблице 1.4.

Таблица 1.4 - Минимальные требования к оборудованию СёрчИнформ

CPU	4-ядерный, частотой 2,1 ГГц
RAM	4 Gb
Disk space	200 Gb

Решение FortiSIEM – комплексное средство управления безопасностью, целью которого является уменьшение сложность обнаружения угроз и увеличению эффективности системы безопасности в целом. Сбор журналов представляет собой сбор событий с помощью агентов Windows, агентов Linux, а также поддержки большого количество систем безопасности от партнеров. Уведомление и управление инцидентами строится на основе политик безопасности. Также система предоставляет администратору доступ к многофункциональным панелям мониторинга с функциям и демонстрации для демонстрации основных показателей.

Преимуществами данной системы являются: очень развитая система анализа событий, основанная на различных типах поиска событий, реализации триггеров для нетипичных событий зарегистрированных в системе и динамические списки отслеживания.

К недостаткам FortiSIEM можно отнести отсутствие локализации на русский язык и поддержки аналитики поведения пользователей системы. Минимальные требования к оборудованию FortiSIEM описаны в таблице 1.5.

Таблица 1.5 - Минимальные требования к оборудованию FortiSIEM

CPU	Intel Xeon E3-1225V3 4 ядра / 4 потока 3,20 ГГц
RAM	DDR3 16 Gb (2x 8 Gb)
Disk space	3 Tb(1x 3 Tb)

На сегодняшний день в мире существует много решений для анализа и мониторинга событий системы. Все решения позволяют собирать журналы и контролировать события. В связи с этим нынешние SIEM системы можно оценить по параметрам дополнительных средств и опций, уровню кастомизации, дополнительным модулям и мощностью самой системы. Исходя из этого можно сделать вывод, что IBM QRadar SIEM является одним из самых полноценных и многофункциональных решений на рынке, имея все дополнительные функции, например аналитика поведения пользователей.

1.8 Вывод по разделу «Обзор QRadar SIEM»

В данном разделе было описано про основные функции и возможности IBM QRadar. К ним относятся: отображение событий в режиме реального времени, сбор событий со всех возможных источников, быстрая нормализация информации и анализ поведения пользователей. Также были описаны минимальные системные требования. Было проанализировано что для оптимальной работы системы, без дополнительных модулей, необходимо 32 ГБ оперативной памяти и минимальной 16 ядер процессора. IBM QRadar SIEM обладает широким функционалом, которым можно управлять с помощью web-интерфейса системы. Были описаны все панели web-интерфейса и описана модульная трехуровневая архитектура системы. Из преимуществ IBM QRadar можно отметить машинное обучение, управление уязвимостями, поддержку дополнительных модулей и множества продуктов других производителей. В результате можно оценить IBM QRadar как готовый, зрелый продукт для использования в любой IT-инфраструктуре для сбора событий и управлением безопасностью [2].

2 Практическая часть

2.1 Установка гипервизора ESXi

Для установки SIEM системы IBM QRadar нам потребуется гипервизор. Гипервизор позволит нам расположить всеми требуемые для нас виртуальные машины на одном аппаратном устройстве. Что даст возможность управления всеми виртуальными машины с одной консоли.

Для осуществления данной концепции требуется производительный сервер. Мощность и производительность сервера подбирается под каждую компанию отдельно, в зависимости от требуемых параметров. В данном случае я остановил свой выбор на сборном сервере от INTEL на серверной платформе S2600WFR, так как это является надежным, гибким и зарекомендовавшим себя решением для построения инфраструктуры виртуализации. Процессоры были выбраны INTEL XEON GOLD 6130, что даст хорошую производительность. Шасси для сервера выбираем R2224WFTZSR с одним USB и VGA портом. Так как при установке будет собираться RAID массив требуемая кэш память будет составлять не менее 2 GB. На данной платформе нам доступны варианты RAID 0, 1, 10 и 5. Хранилищем будут выступать SSD накопители общей емкостью 750 GB.

В качестве гипервизора был выбран ESXi от компании VMware. Это небольшая операционная система позволит управлять и настраивать все виртуальные машины. Дистрибутив ESXi можно бесплатно скачать с официального сайта и при необходимости докупить к нему лицензию, для расширенных возможностей. ESXi ставится на «голое» железо и не требует заранее установленной операционной системы [2].

Загружаем дистрибутив на флешку с помощью программы Rufus (рисунок 2.1). Далее подключаем накопитель с образом к серверу и устанавливаем гипервизор (рисунок 2.2). Затем принимаем лицензионное соглашение и выбираем язык раскладки (рисунок 2.3). Выбираем язык интерфейса (рисунок 2.4). Набираем пароль (не меньше 7 символов) для привилегированного пользователя (root) (рисунок 2.5). Завершение процесса установки (рисунок 2.6). После перезагрузки сервера, нажимаем клавишу F2 и переходим во вкладку настроек и задаем статический IP-адрес (рисунок 2.7). Доступ к консоли управления ESXi можно получить через клиентское приложение VMware vSphere Client или с помощью браузера, перейдя по https://<ESXi _ip_address> (рисунок 2.8) [4].

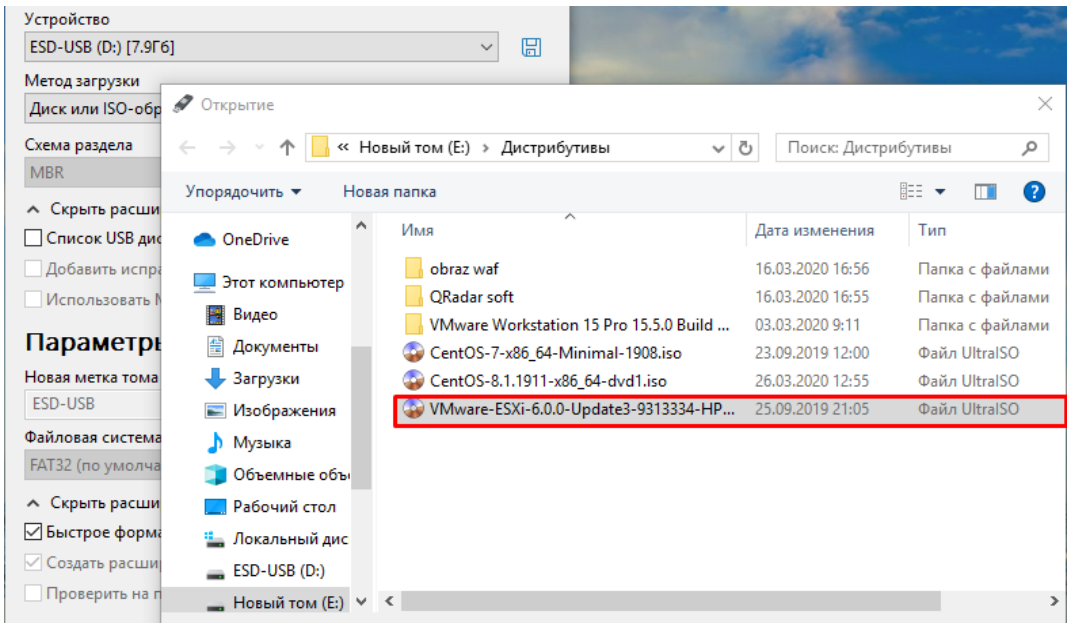


Рисунок 2.1 – Загрузка дистрибутива

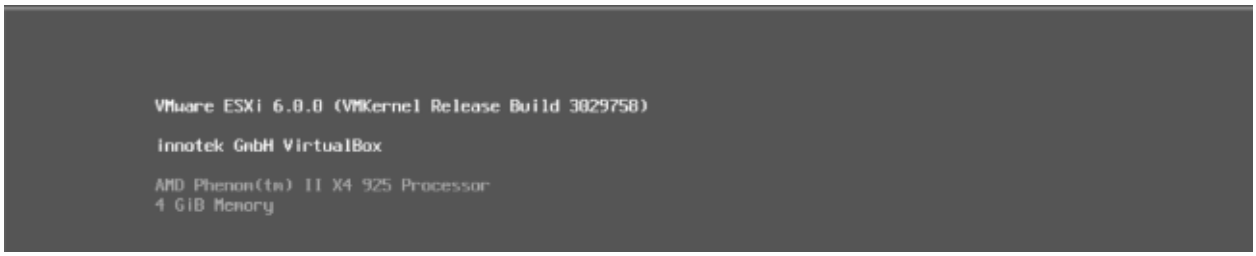


Рисунок 2.2 – Установка ESXi

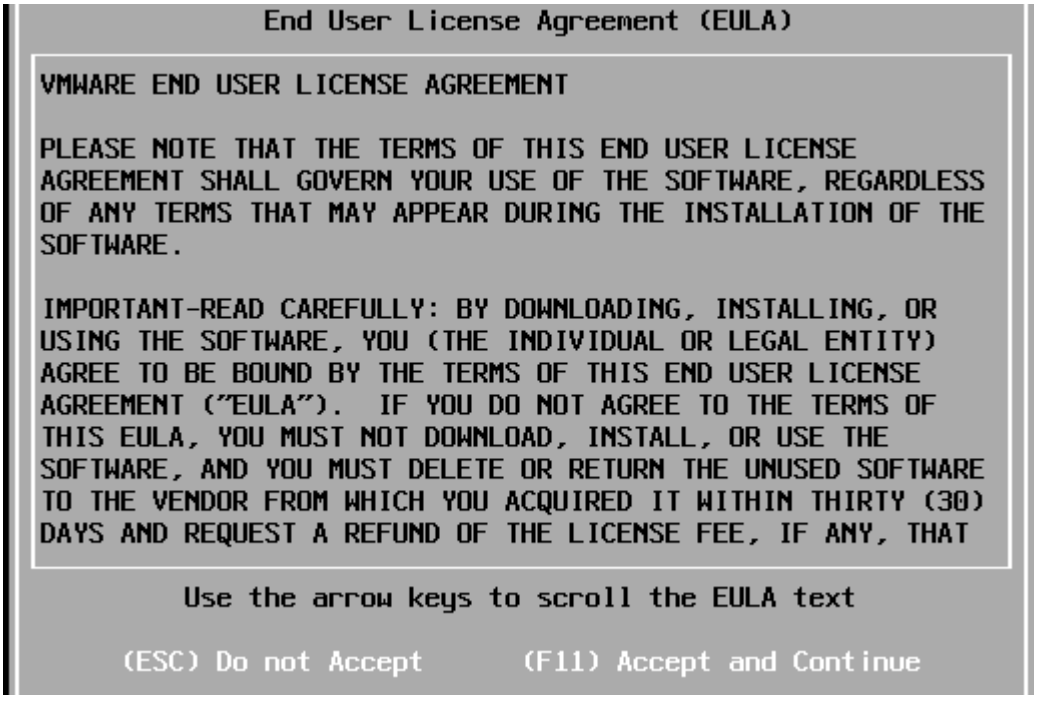


Рисунок 2.3 – Лицензионное соглашение

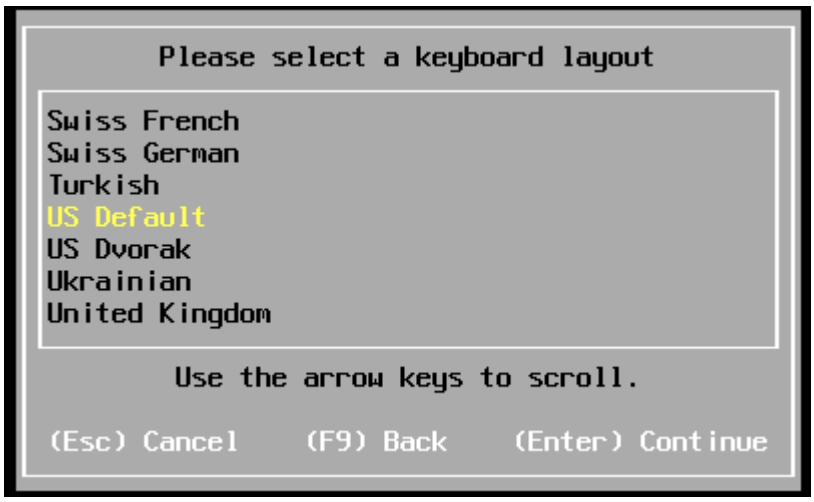


Рисунок 2.4 – Выбор раскладки клавиатуры

Рисунок 2.5 – Установка пароля суперпользователя

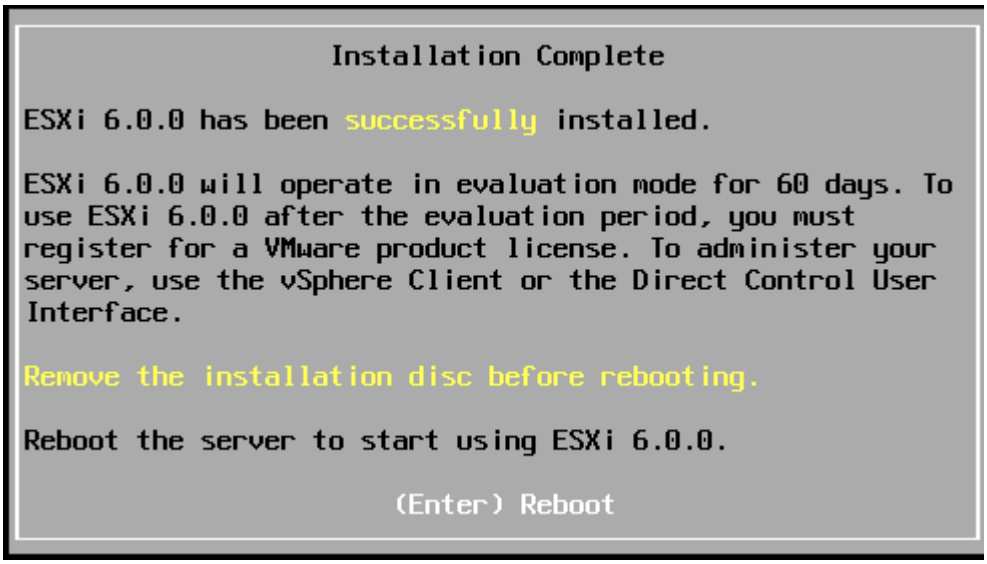


Рисунок 2.6 – Завершение установки

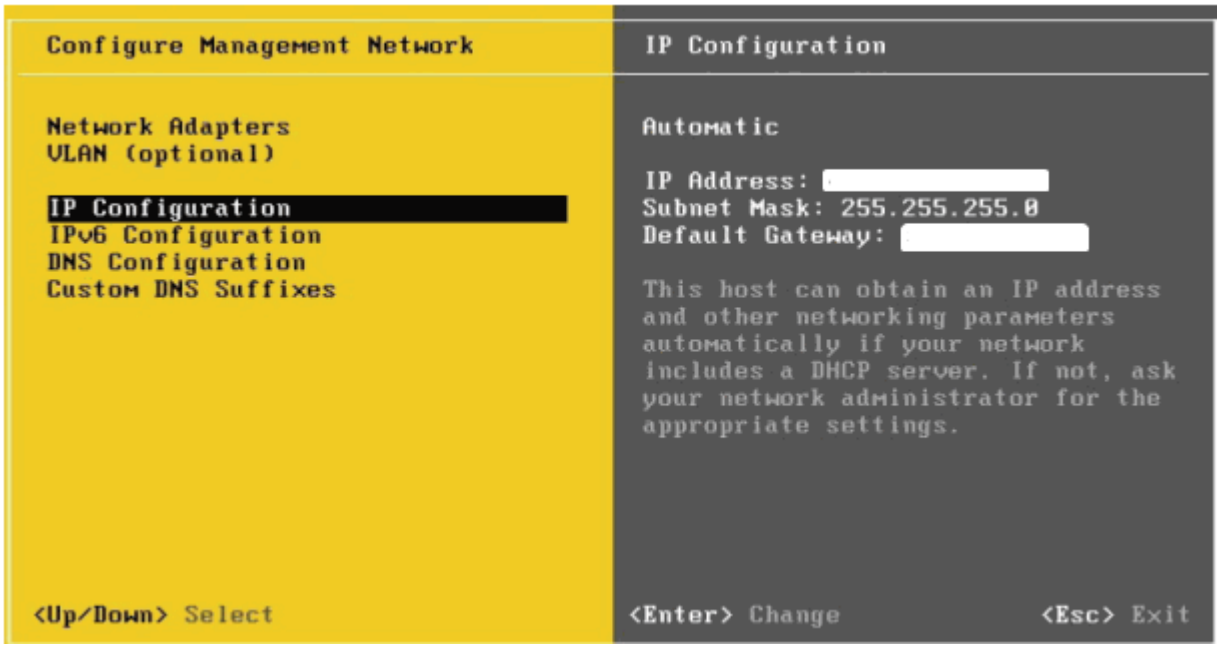


Рисунок 2.7 – Конфигурация сети

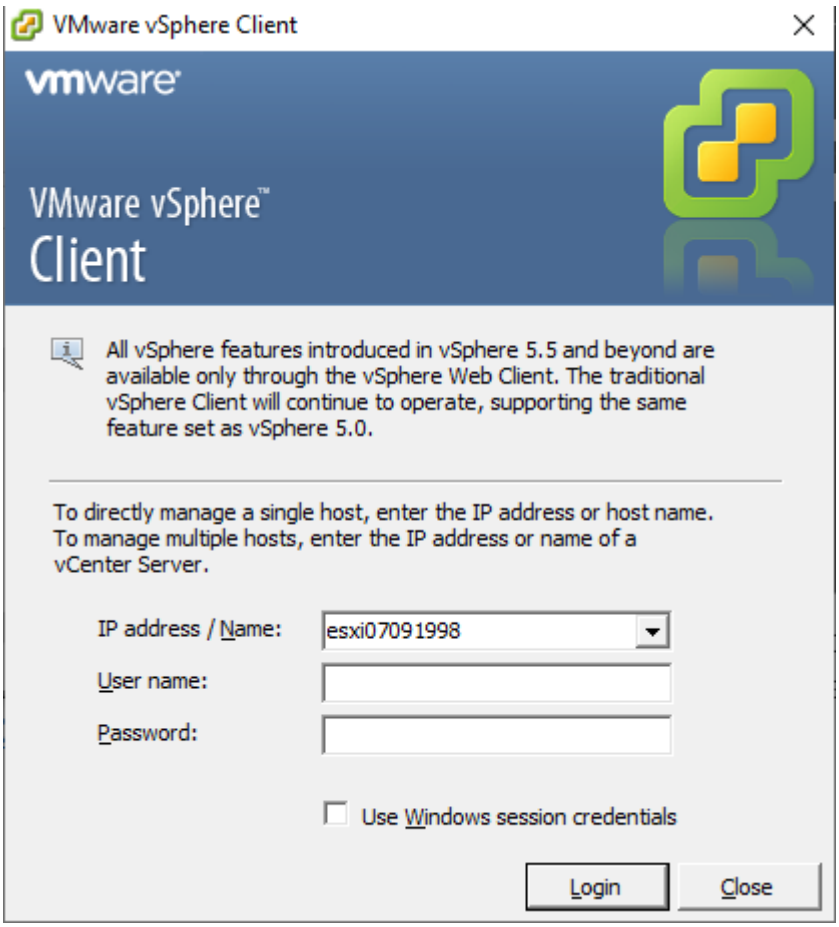


Рисунок 2.8 – Запуск клиента

2.2 Установка IBM QRadar SIEM

Создание новой виртуальной машины (рисунок 2.9).

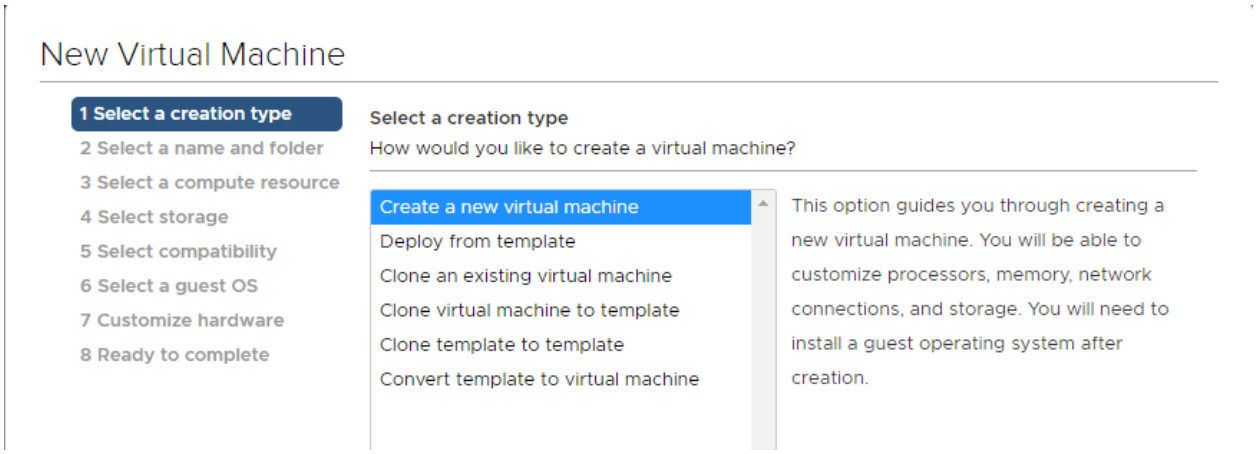


Рисунок 2.9 – Создание новой виртуальной машины

При выборе операционной системы выбираем Red Hat Enterprise Linux 7 (рисунок 2.10).

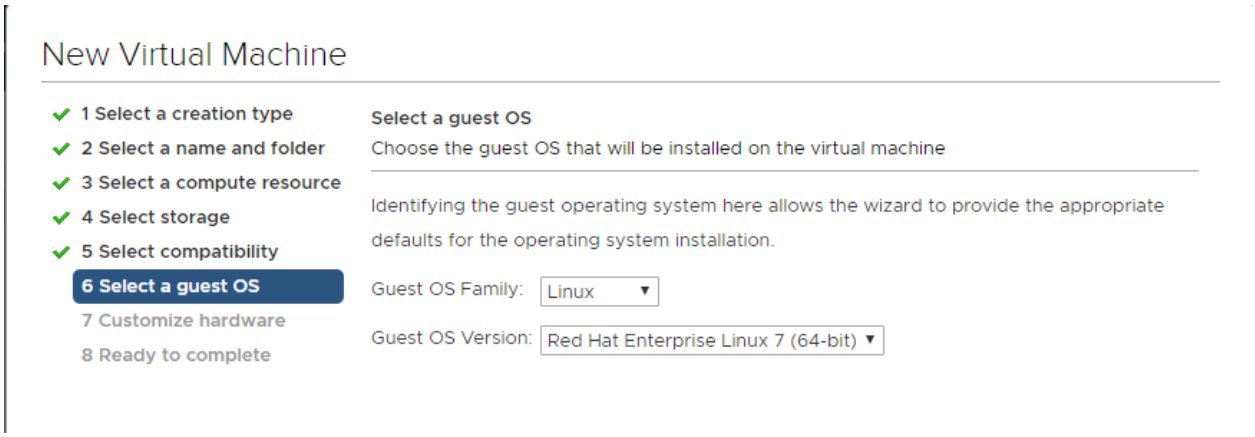


Рисунок 2.10 – Выбор операционной системы

Для работы QRadar нам потребуется минимум 2 центральных процессора, 8 Гб ОЗУ и 250 Гб места на жестком диске (рисунок 2.11). В первую очередь устанавливается дистрибутив Red Hat Enterprise (рисунок 2.12), далее на установленный Red Hat устанавливается IBM QRadar SIEM (рисунок 2.13). Выбираем заводскую установку QRadar (рисунок 2.14). Прочитав лицензионное сообщение, соглашаемся введя «YES» (рисунок 2.15).

IBM QRadar SIEM предлагает несколько вариантов установки (рисунок 2.16). Выбираем первый вариант (Appliance Install) установки, который включает установку QRadar вместе с Red Hat Enterprise 7.

Вариант Software Install предполагает установку на уже предустановленный Red Hat Enterprise Linux [3].

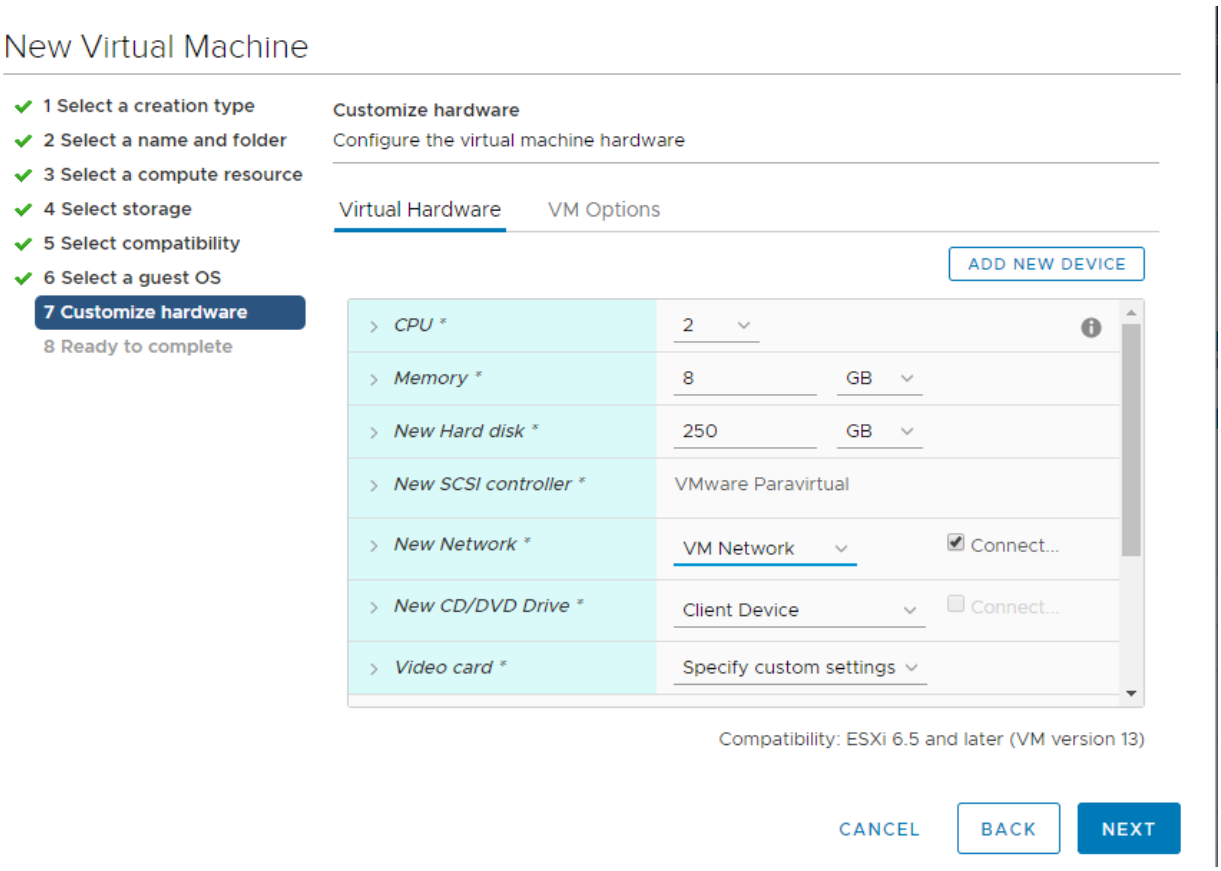


Рисунок 2.11 – Системные требования системы

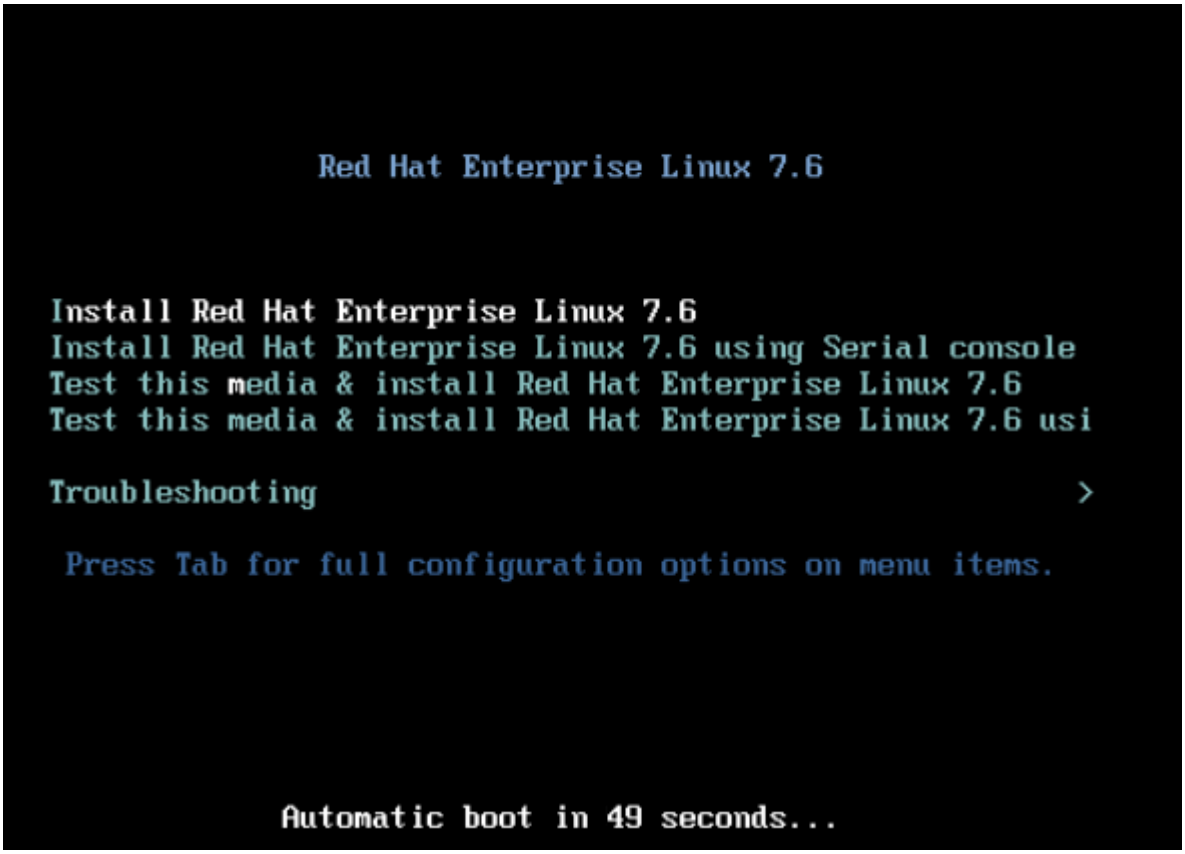


Рисунок 2.12 – Установка Red Hat Enterprise 7.6

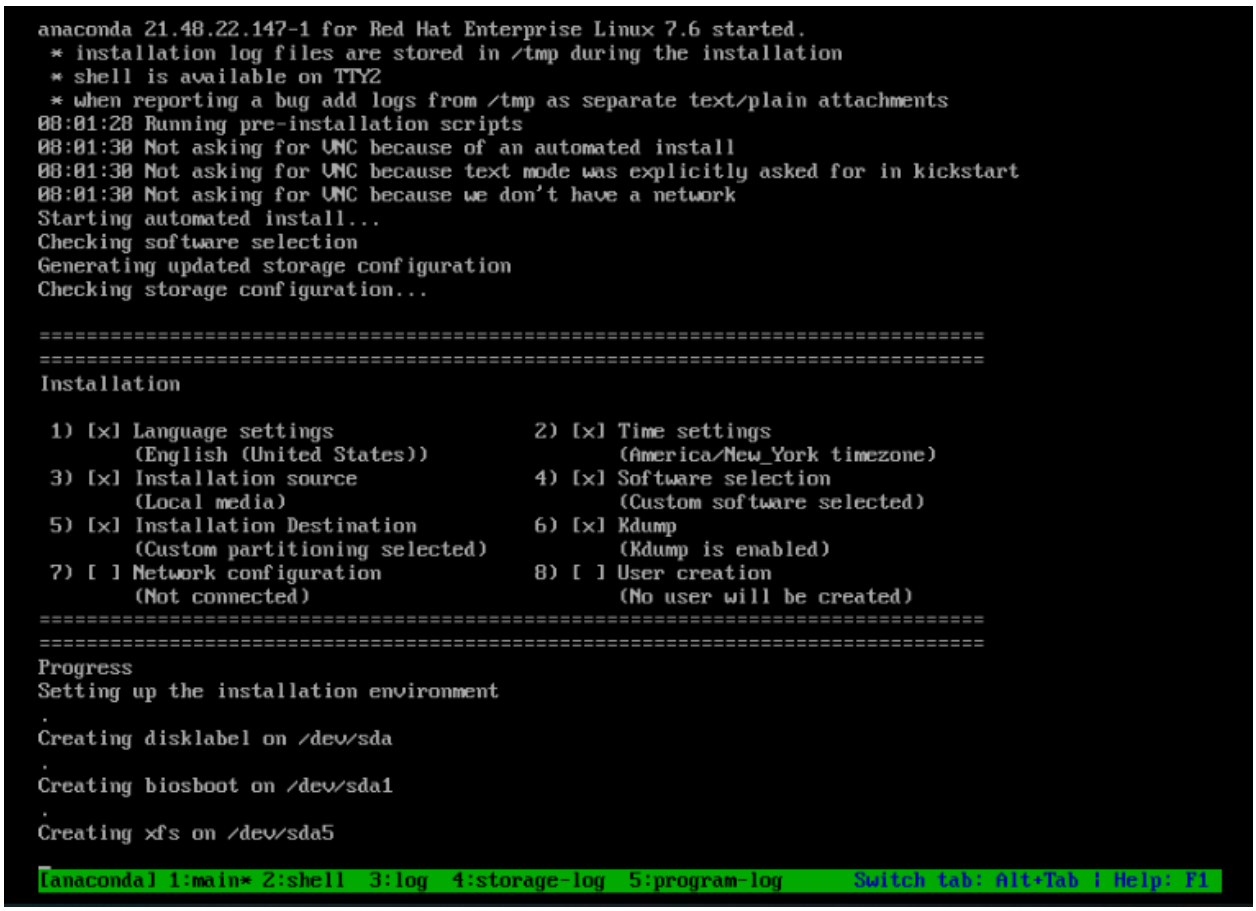


Рисунок 2.13 – Процесс установки

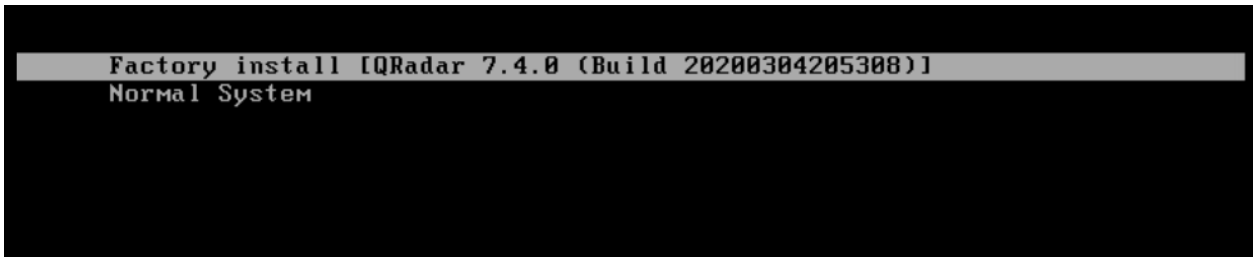


Рисунок 2.14 – Заводская установка QRadar

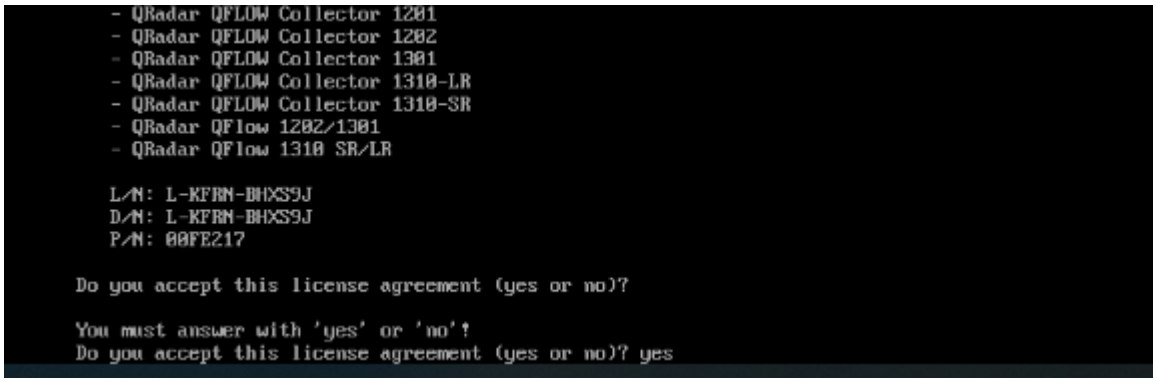


Рисунок 2.15 – Лицензионное соглашение

High Availability Appliance это установка вторичного сервера для основного QRadar, который предназначен для использования в случае выхода из строя основного и полностью копирует основной сервер [3].

App Host Appliance это установка дополнительного сервера для установки на нем приложений QRadar, чтобы не занимать вычислительные ресурсы основного сервера.

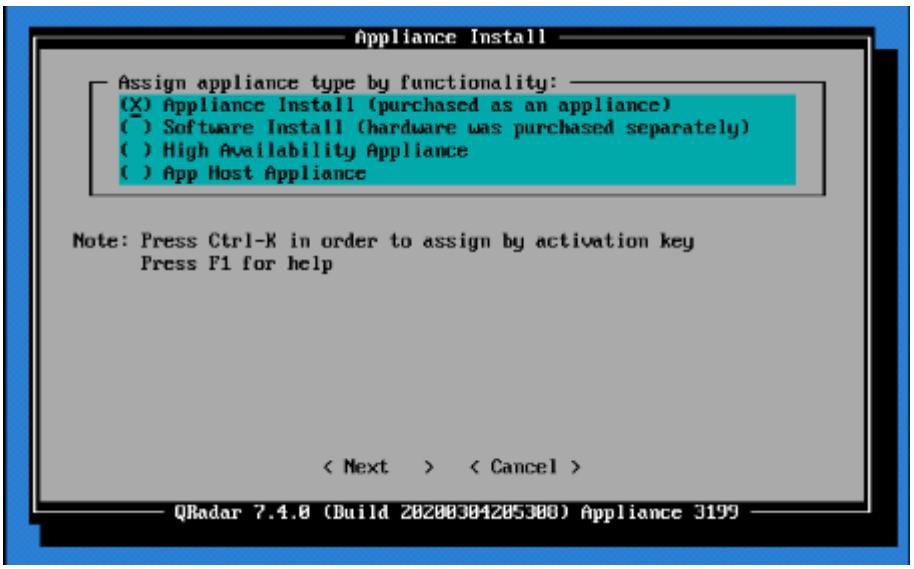


Рисунок 2.16 – Выбор варианта установки

Выбираем Flow Collector (рисунок 2.17).

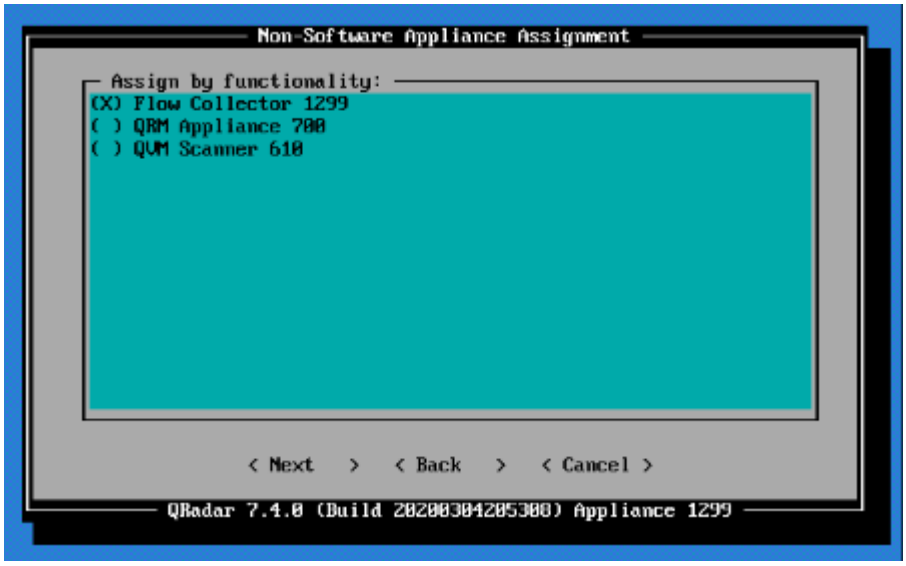


Рисунок 2.17 – Выбор функционала

QRadar предлагает 2 типа установки Normal и Recovery. Recovery режим нужен на случай восстановления с помощью вторичного сервера (рисунок 2.18)

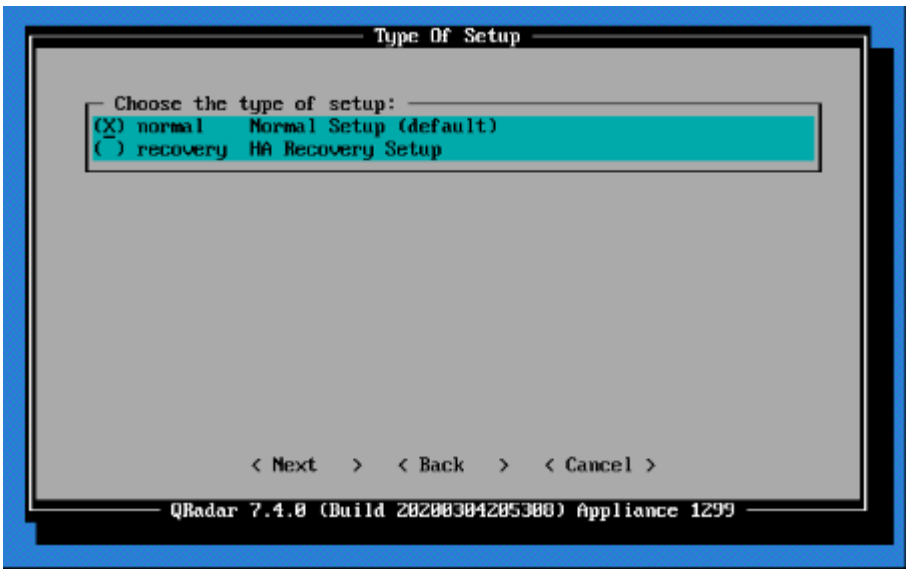


Рисунок 2.18 – Тип установки

Выбор региона Азия (рисунок 2.19)

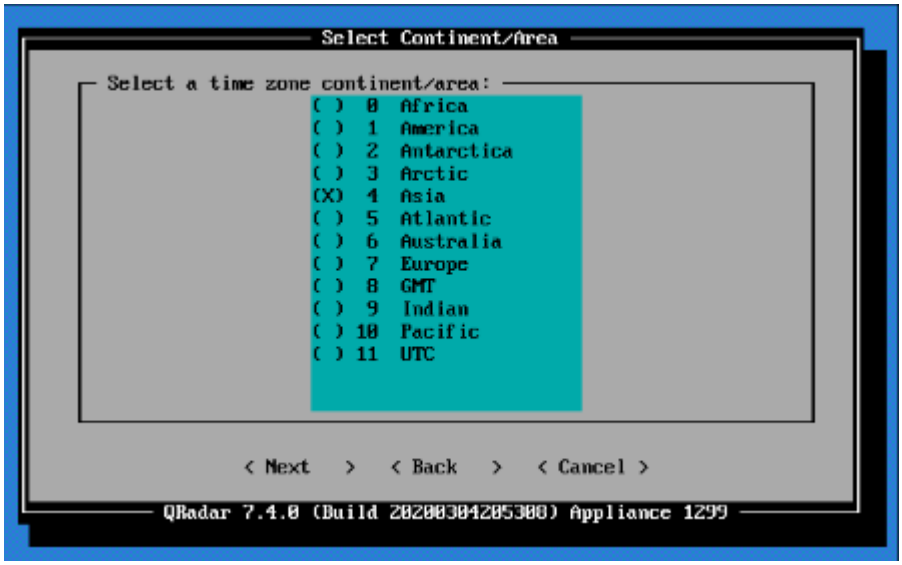


Рисунок 2.19 – Выбор региона

Выбор временной зоны Almaty (Kazakhstan) (рисунок 2.20)

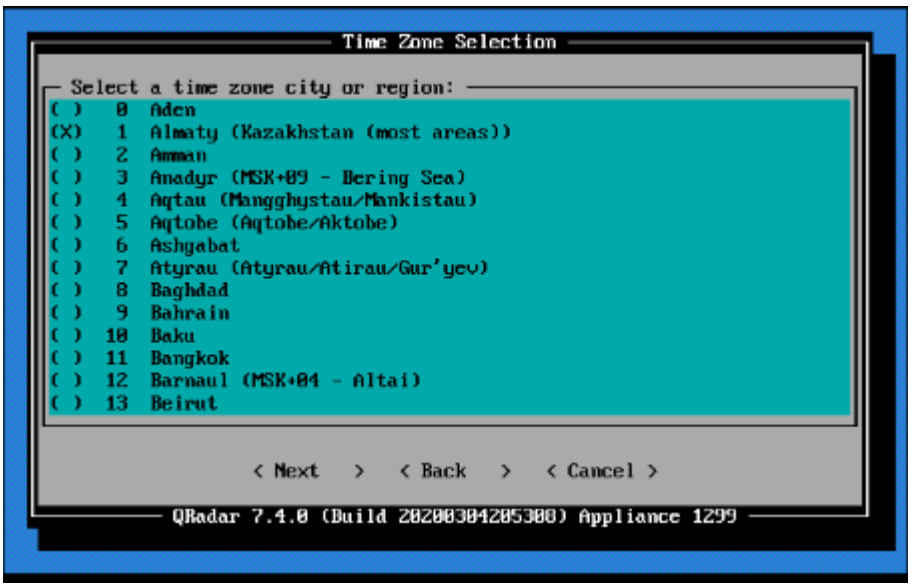


Рисунок 2.20 – Выбор временной зоны

Выбираем Интернет протокол ipv4 (рисунок 2.21).

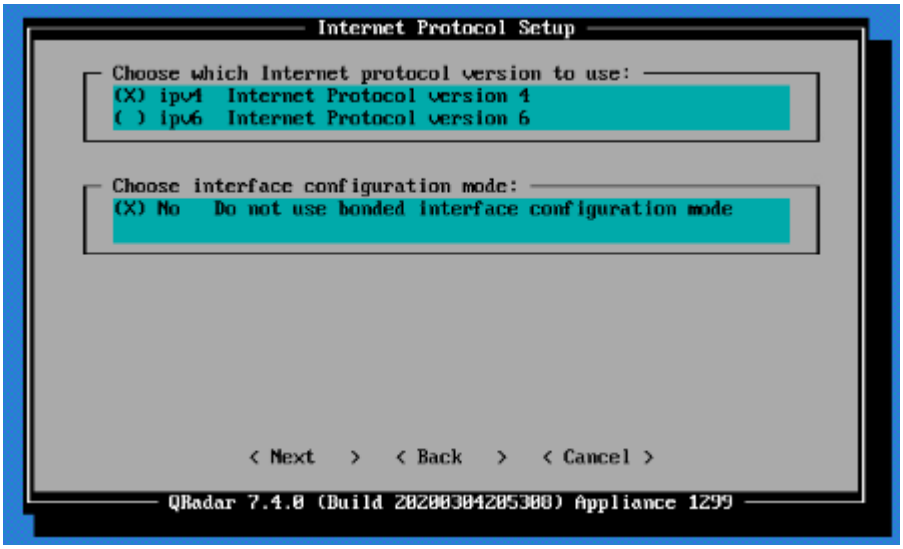


Рисунок 2.21 – Выбор протокола ipv4

Выбор сетевого интерфейса (рисунок 2.22).

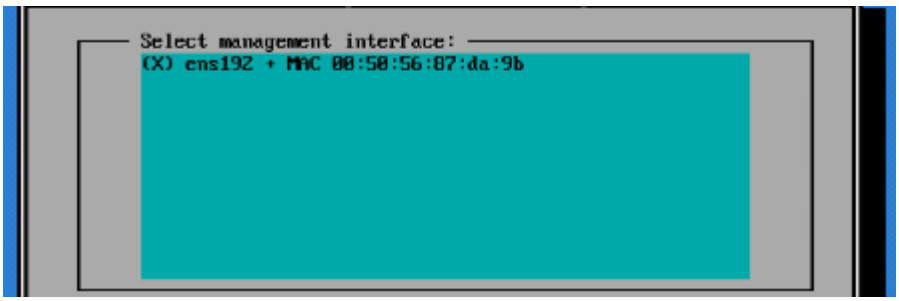


Рисунок 2.22 – выбор сетевого интерфейса

Ввод IP-адреса, маски подсети, шлюза сети и адреса DNS.

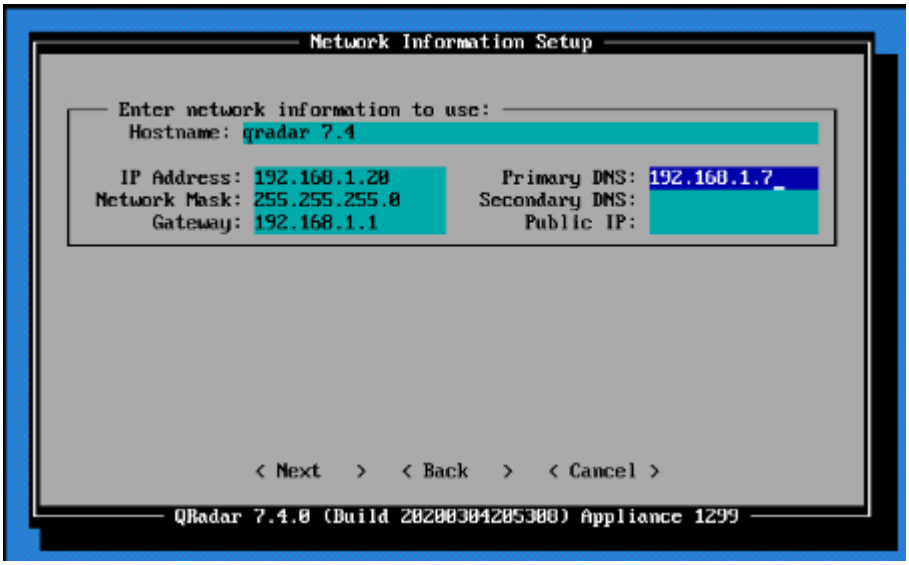


Рисунок 2.23 – Настройки сети

Применение сетевых настроек (рисунок 2.24).

Рисунок 2.24 – применение настроек

Установка пароля на привилегированный режим (рисунок 2.25).

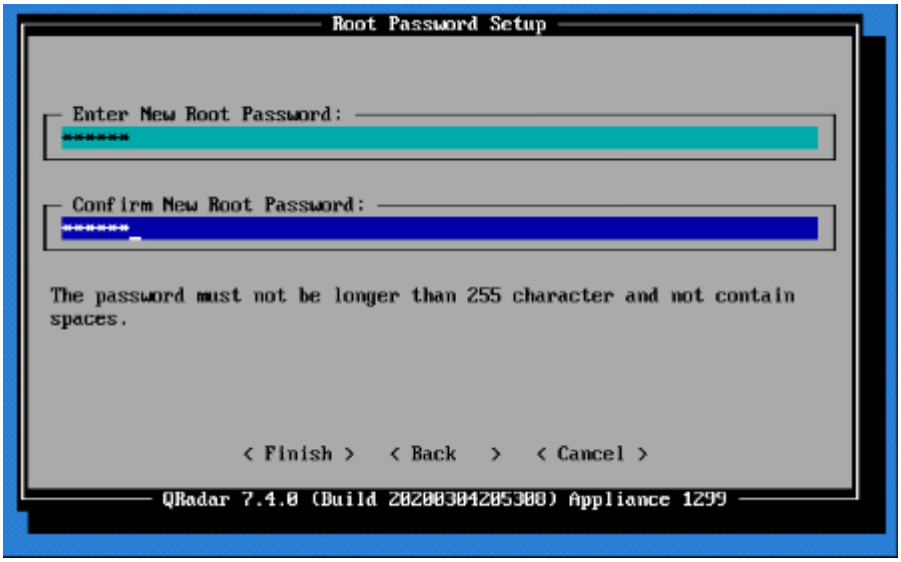


Рисунок 2.25 – Установка пароля на root

Завершения установки IBM QRadar SIEM (рисунок 2.26)

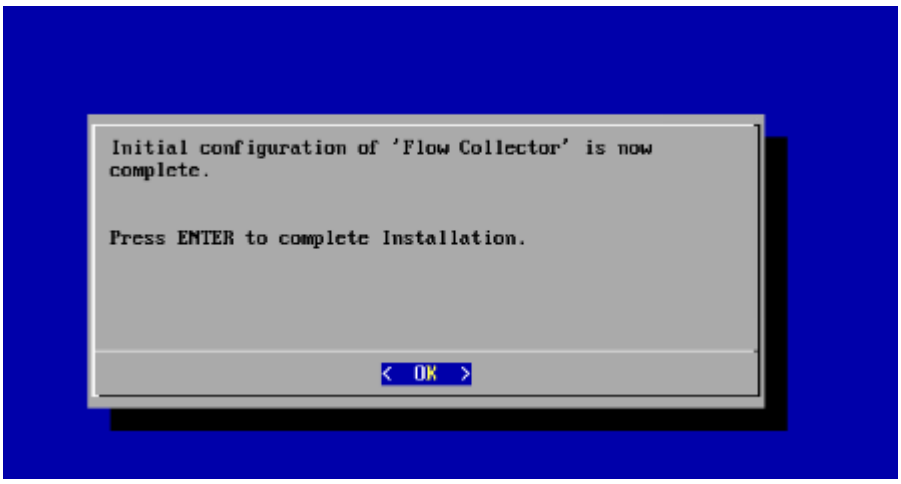


Рисунок 2.26 – Завершение установки

Командная строка IBM QRadar SIEM (рисунок 2.27).

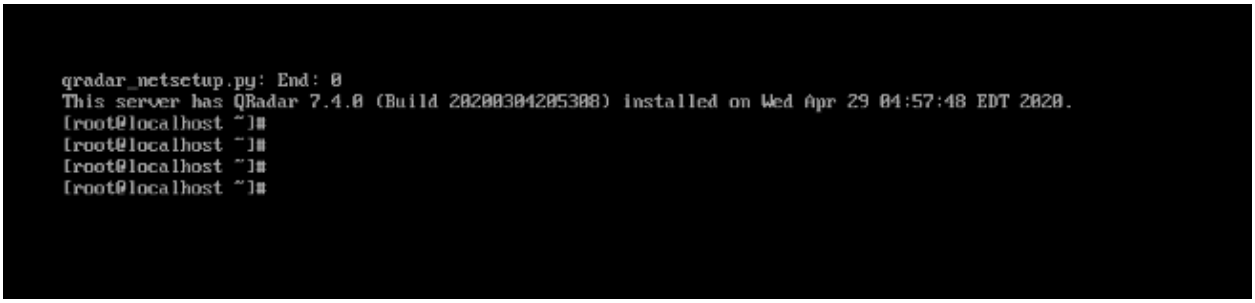


Рисунок 2.27 – Командная строка QRadar

2.3 Добавление источника событий в IBM QRadar SIEM

Как источник событий используется CentOS 7. В терминале линукса нужно добавить строки в файл конфигурации rsyslog.conf [6].

После авторизации под root – пользователем редактируем файл командой nano/etc/rsyslog.conf (рисунок 2.28)

Рисунок 2.28 – Конфигурация файла rsyslog.conf

Добавляем строку *.* @*.*.10.24:514 , где *.* - означает об отправки всех событий на QRadar, @*.*.10.24 – IP-адрес в данном случае * скрывают настоящие цифры, 514 – порт передачи данных (рисунок 2.29).

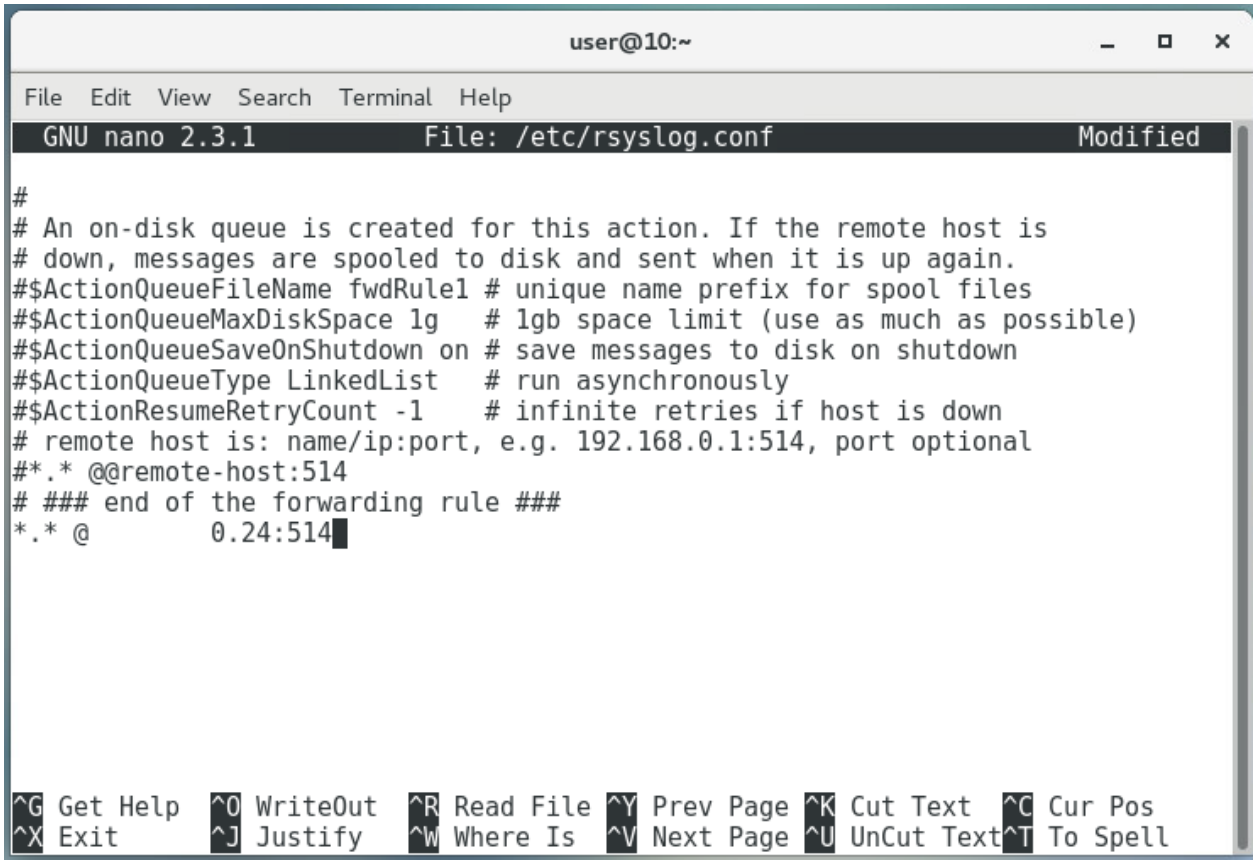


Рисунок 2.29 - Конфигурация файла rsyslog.conf

Сохраняем конфигурацию с помощью Ctrl+O. Перейдя в интерфейс управления QRadar, нужно перейти в Log Source Management и создать новый источник (рисунок 2.30).

Рисунок 2.30 – Создание источника событий в QRadar

Используя поиск найти подходящий источник (рисунок 2.31).

Рисунок 2.31 – Выбор типа источника

Выбор протокола Syslog, который является стандартным и используется для отправки журналов и сведений, происходящих в системе, на сервер (рисунок 2.32) [7].

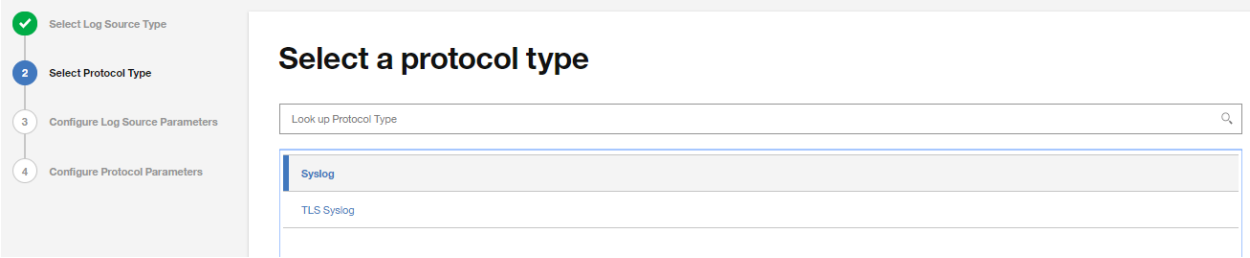


Рисунок 2.32 – Выбор протокола SYSLOG

Далее настраиваются параметры источника (рисунок 2.33).

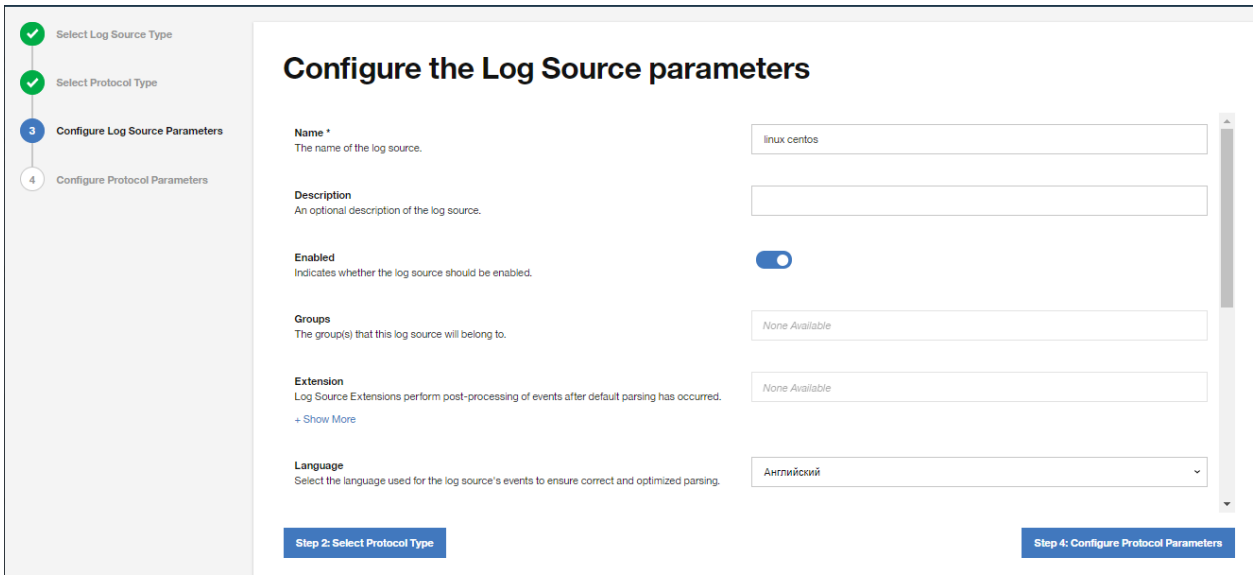


Рисунок 2.33 – Настройка параметров источника

Завершаем конфигурацию записав IP-адрес источника и выбором кодировки UFT-8 (рисунок 2.34).

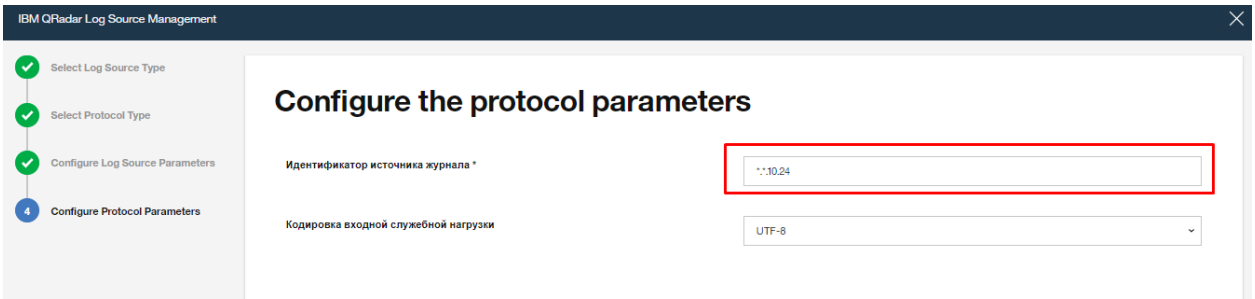


Рисунок 2.34 – Завершение конфигурации

Завершив конфигурацию видно, что добавлен новый источник событий для Cent OS (рисунок 2.35).

Рисунок 2.35 – Обновленный журнал источников

После добавления источника можно визуально увидеть в консоли QRadar как начали приходить логи с CentOS (рисунок 2.36, рисунок 2.37).

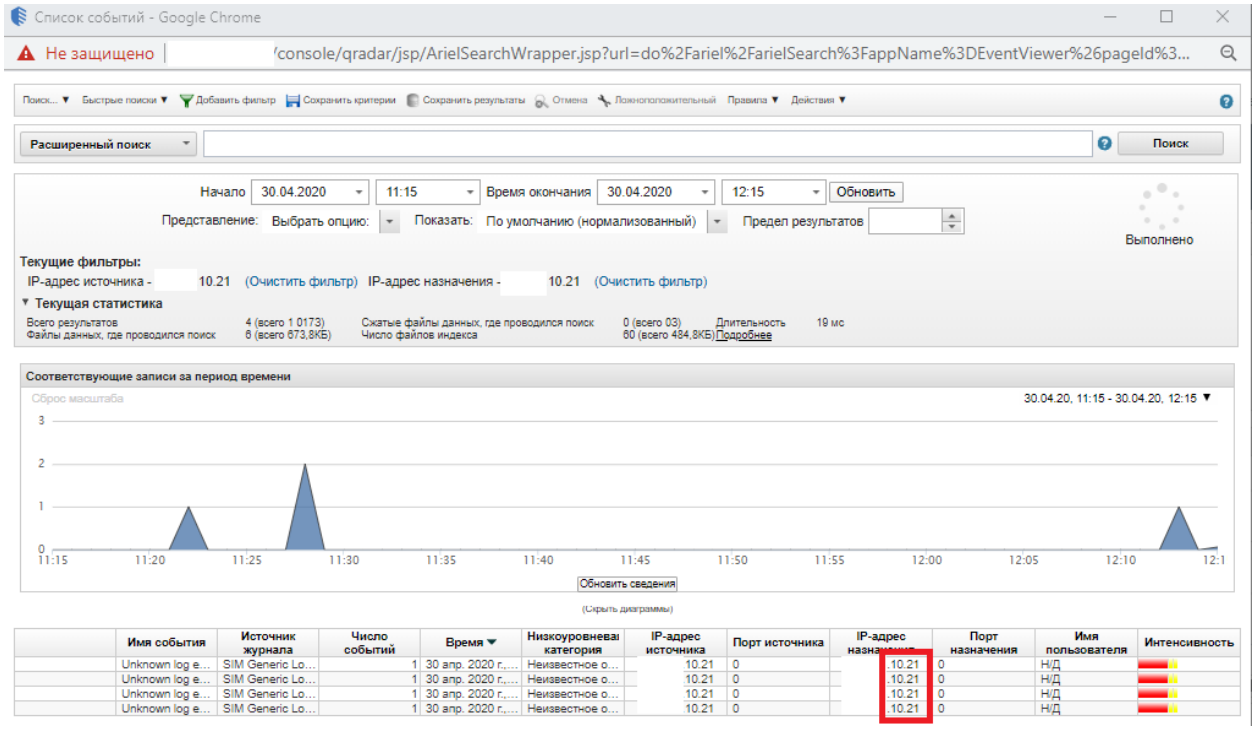


Рисунок 2.36 – Логи источника Cent OS

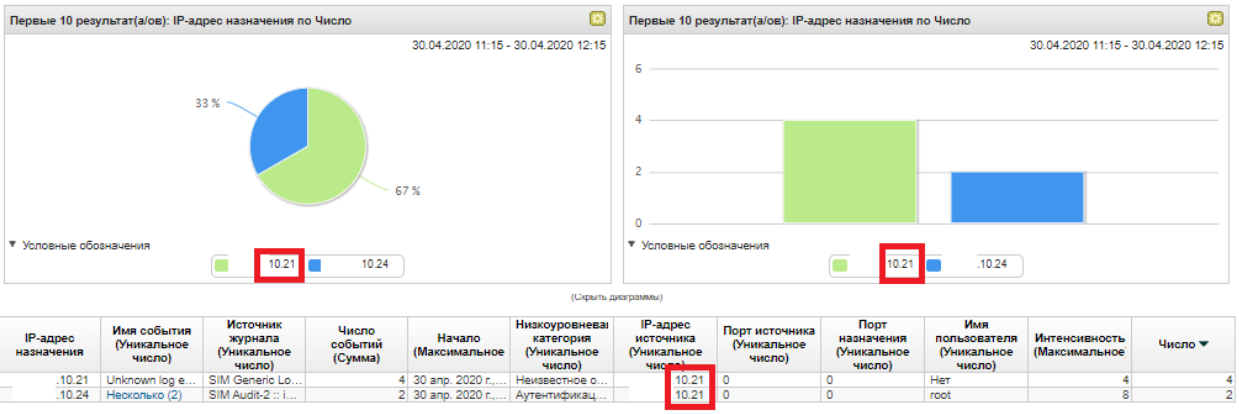


Рисунок 2.37 - Логи источника Cent OS

2.4. Расследование инцидента

2.4.1 Обработка неизвестных источников событий

IBM QRadar SIEM может собирать события безопасности с различных продуктов защиты информации.

Используется стандартный протокол Syslog, а также поддерживаются множество различных протоколов с других устройств. Количество источников, распознаваемых IBM QRadar SIEM автоматически, исчисляется 1000 источниками, но количество устройств с каждым днем растет и появляются источники не распознаваемые системой. В таком случае есть необходимость написать вручную правила по которым источник будет определен и события были упорядочены, доступны и легко читаемы. Это позволит создать более гибкую и комфортную систему, которая будет отвечать требованиям под конкретного заказчика[8].

Также во многих ситуациях система устанавливается на предприятия, где уже находятся различные предустановленные системы, не поддерживаемые QRadar. И в данном вопросе сбор данных с уже установленных в компании решений становится критическим, так как потенциал этих систем не будет раскрыт полностью. Парсинг событий ускорит процесс реагирования на инциденты, увеличит эффективность работы служб безопасности, а также поможет собрать все события в нормализованном и доступном визуальном отображении. Оптимизация данного процесса помогает службе информационной безопасности в экономии средств и времени.

Для решении данной проблемы было решено использовать регулярные выражения. Регулярные выражения представляют собой небольшой язык программирования, предназначенный для поиска необходимых данных в массиве. Регулярные выражения - это мощный инструмент заточенный под реализацию поиска строк. Выражение пишется с помощью метасимволов (таблица 2.1) и ключевых слов, по которым и находится совпадение в массиве строк. К метасимволам относятся: \ | ( ) ? { [ ] . ^ $ * + [9].

Таблица 2.1 – Таблица метасимволов

\	Экранирование используемых символов
|	ИЛИ
( )	Создание группы символов
?	Один или ноль
{}	Количество повторения символов
[ ]	Любые символы, диапазон
.	Любой символ
^	Начало строки
$	Конец строки
*	Неограниченное количество предыдущих символов
+	Один или более символов

В качестве примера был взят NG Firewall Huawei USG 6620, а также система видеонаблюдения Hikvision. Так как журналы с данных источников являются нестандартными, требуется проведение анализа источника и разработки формул регулярного выражения для каждого события.

Для анализа и тестирования регулярных выражений были взяты образцы журналов Huawei USG 6620 и системы видеонаблюдения Hikvision.

Образец журнала межсетевого экрана Huawei:

#2020/1/3 10:38:42+05:00 h-fw-01 ATK/4/FIREWALLATCK:AttackType="ICMP unreachable attack", slot=" ", cpu="0", receive interface="GE1/0/5 ", proto="ICMP", src="11.22.33.44 ", dst="11.22.33.44 ", begin time="2020-1-31 10:38:27", end time="2020-1-31 10:38:27", total packets="1", max speed="0", User="", Action="alert".

#2020/1/3 10:38:42+05:00 h-fw-01 ATK/4/FIREWALLATCK:AttackType="Fraggle attack", slot=" ", cpu="0", receive interface="GE1/0/9 ", proto="UDP", src="11.22.33.44", dst="11.22.33.44 ", begin time="2020-1-3 10:38:37", end time="2020-1-1 10:38:37", total packets="1", max speed="0", User="", Action="alert".

#2020/1/3 10:38:12+05:00 h-fw-01 ATK/4/FIREWALLATCK:AttackType="Trace route attack", slot=" ", cpu="0", receive interface="GE1/0/9 ", proto="ICMP", src="11.22.33.44 ", dst="11.22.33.44 ", begin time="2020-1-3 10:38:3", end time="2020-1-3 10:38:3", total packets="1", max speed="0", User="", Action="alert".

Образец журнала системы видеонаблюдения Hikvision:

2019-06-15 09:27:30,Operation,Remote Operation: Login,Nick,,106.126.18.92,,

2019-06-14 19:00:00,Operation,Remote Operation: Login,admin,,106.126.18.26,,

В результате выполнения анализа журнала межсетевого экрана и использования регулярных выражений нужно получить такие данные как: тип атаки, время атаки, интерфейс, адрес источника, адрес назначения и действие.

В результате выполнения анализа журнала системы видеонаблюдения и использования регулярных выражений нужно получить такие данные как: дату и время операции, тип операции, имя пользователя и IP-адрес.

Для первичного анализа журнала можно воспользоваться ресурсами по сравнению текста доступными в Интернете (рисунок 2.38, рисунок 2.39). Для этого необходимо взять разные строки журнала и сравнить их.

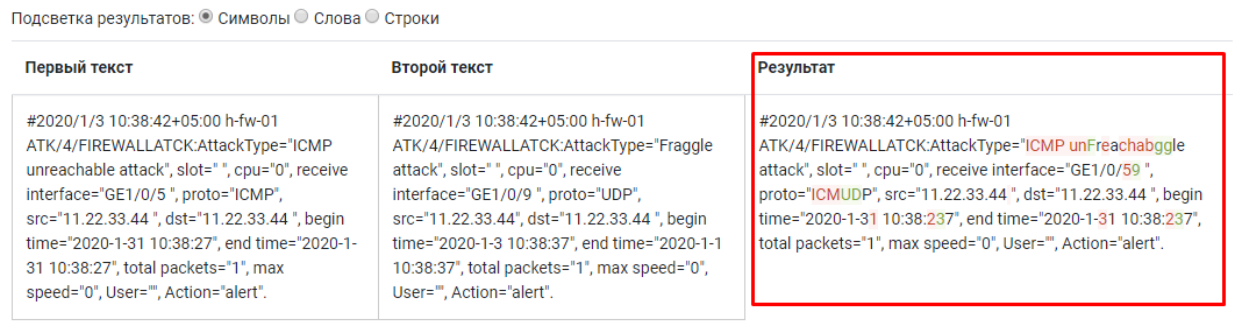


Рисунок 2.38 – Сравнение текста

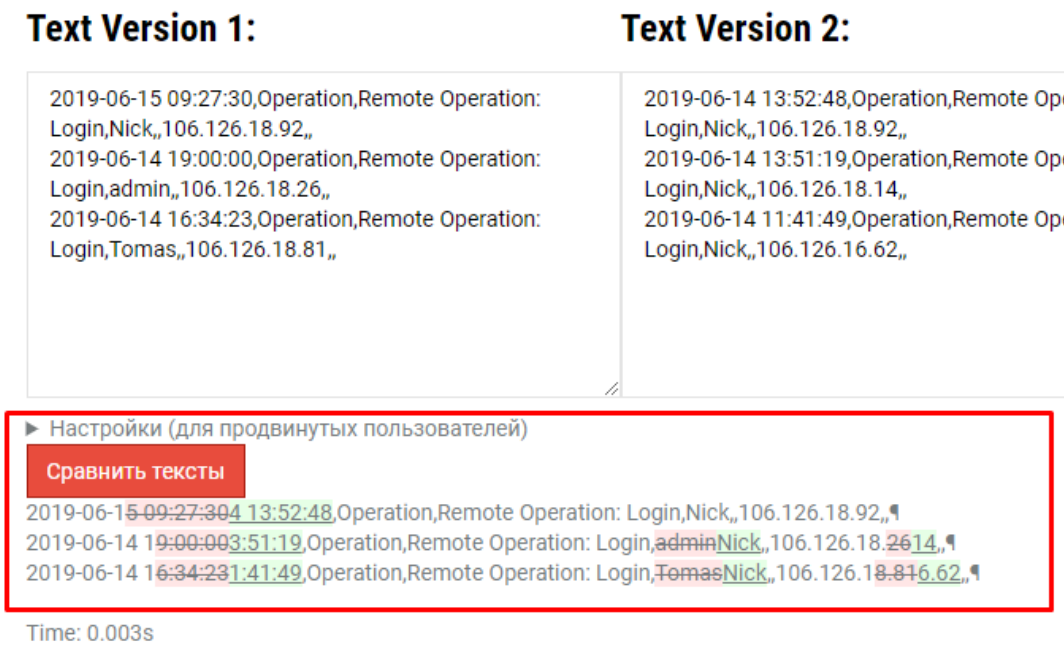


Рисунок 2.39 – Сравнение текста

Сравнение текстов поможет выделить одинаковые и различные части лога, что поможет при разработке регулярных выражений.

Следующим этапом необходимо перейти в консоль QRadar во вкладку «Управление – Редактор DSM» (рисунок 2.40).

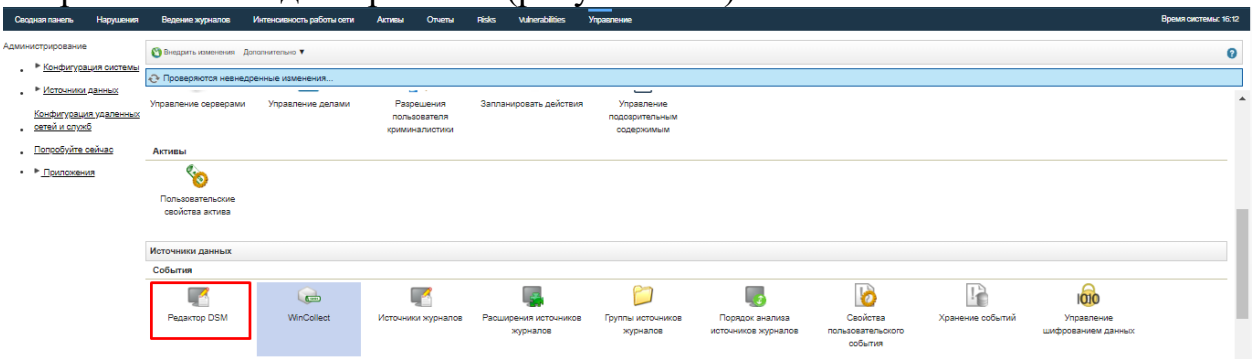


Рисунок 2.40 – DSM Редактор

Интерфейс Редактора DSM состоит из вкладки Конфигурации, Рабочего пространства и Панели предварительного просмотра (рисунок 2.41).

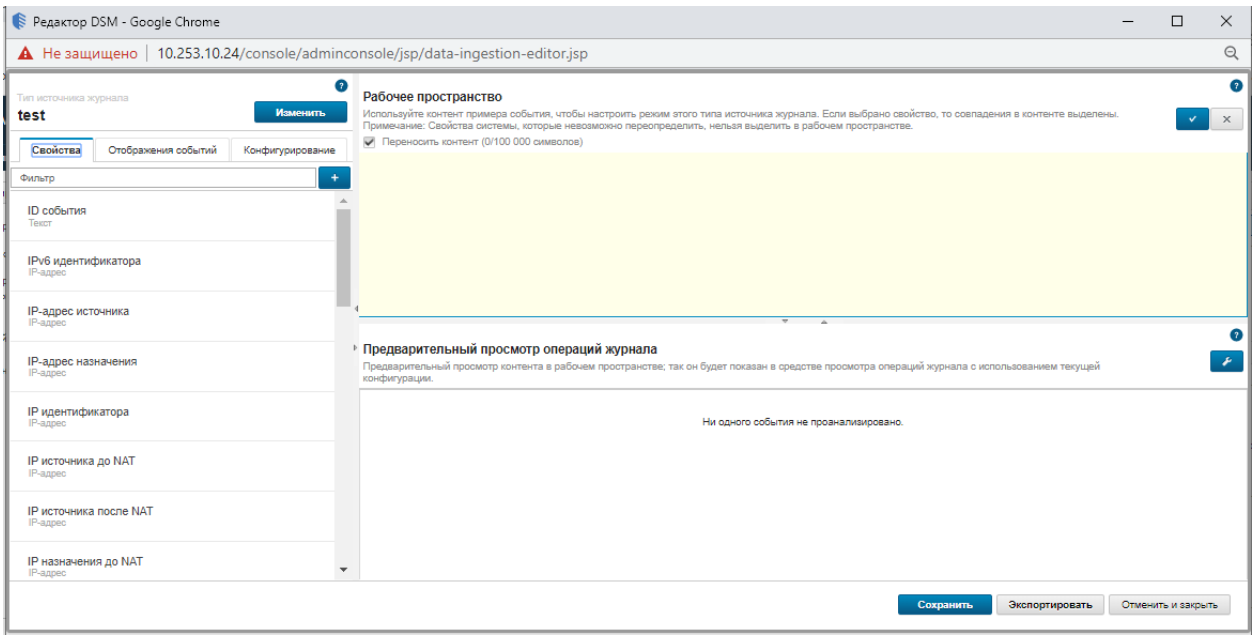


Рисунок 2.41 – Интерфейс Редактора DSM

Рабочее пространство нужно для того, чтобы поместить туда пример события для настройки соответствующего режима для него. При парсинге событий в этой области будет отображено, какую именно информацию мы фильтруем (рисунок 2.42).

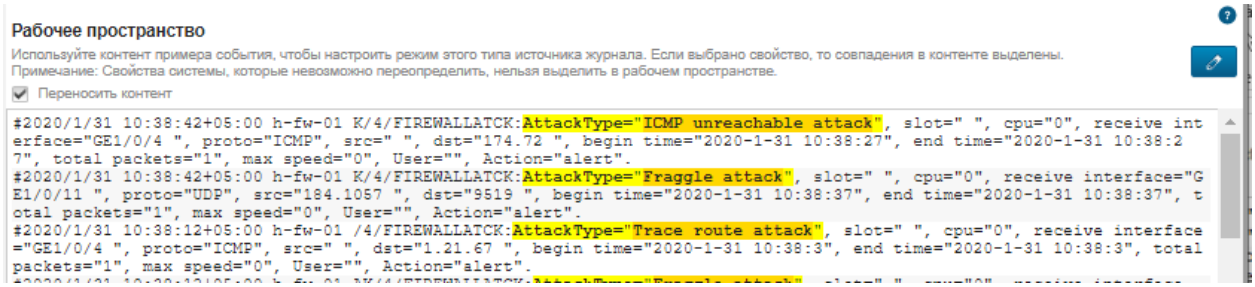


Рисунок 2.42 – Рабочее пространство

Во вкладке свойства содержаться системные и добавленные пользовательские свойства. Можно настроить оба типа свойств перераспределив регулярное выражение (рисунок 2.43).

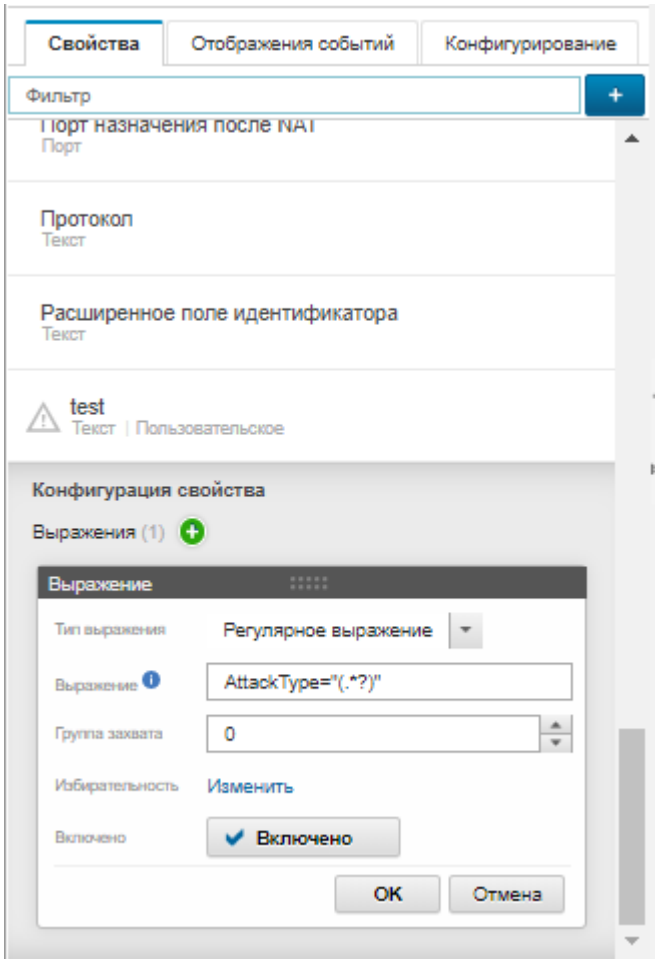


Рисунок 2.43 – Вкладка Свойства

Панель предварительного просмотра отображает нам результат парсинга и нормализации событий (рисунок 2.44).

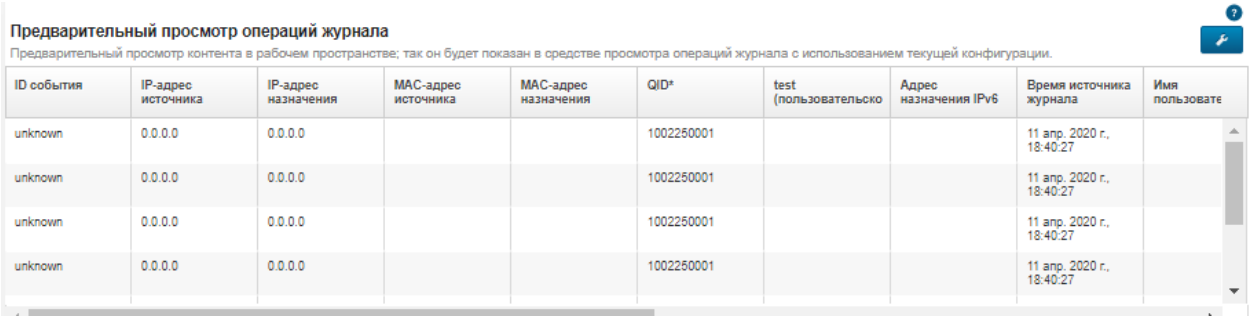


Рисунок 2.44 - Панель предварительного просмотра

Разработка формул регулярных выражений начинается с создания нового типа источника. В Редакторе DSM создаем новый тип источника журнала для NG Firewall Huawei USG 6620 (рисунок 2.45).

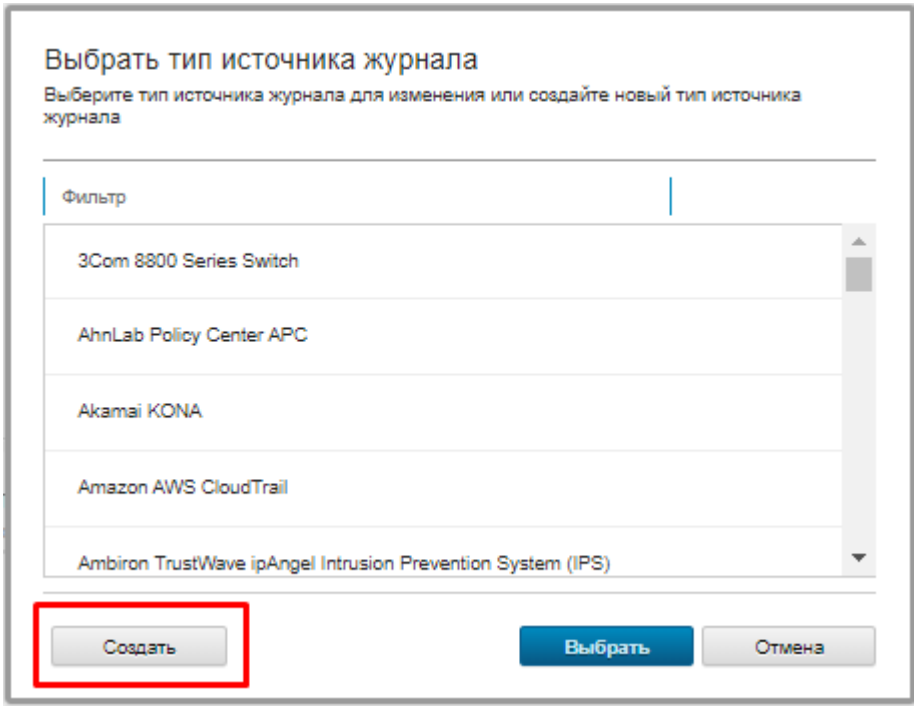


Рисунок 2.45 – Создание нового источника

Задаем имя нового источника (рисунок 2.46).

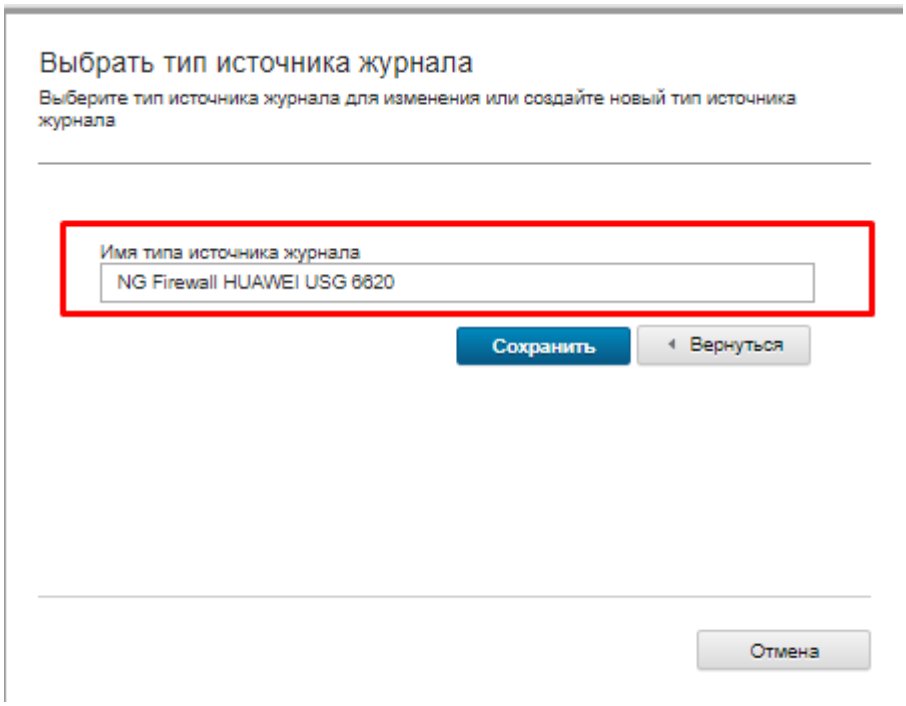


Рисунок 2.46 – Имя источника событий

Создав новый тип источника появляется рабочее пространство и вкладка свойств. Добавляем образец журнала в рабочее пространство (рисунок 2.47).

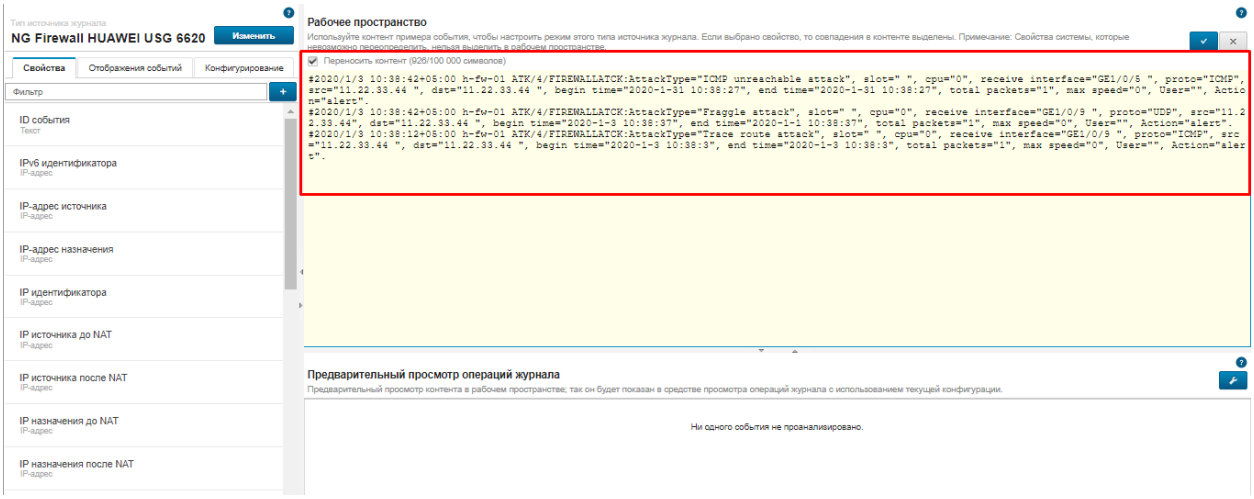


Рисунок 2.47 – Образец журнала

В данном варианте журнала необходимо выделить события по типу атаки.

Формула регулярного выражения: AttackType="(.*?)" (рисунок 2.48).

Разбор регулярного выражения.

Поле Attacktype=”” – Ограничения выражения в рамках которого находится тип атаки.

(.*?) – В рамках данного сгруппированного выражения будут определяться все символы до символа «”».

Альтернативный вариант: Attacktype=”.*”,\sslot.

Рисунок 2.48 – Проверка формулы

Вывод категорий атаки (рисунок 2.49)

Рисунок 2.49 – Результат вывода регулярного выражения

Поле begin time=""– Ограничения выражения в рамках которого находится время события.

(.*?) – В рамках данного сгруппированного выражения будут определяться все символы до символа «”».

Формула регулярного выражения: begin time="(.*?)".

В случаях выполнения поиска даты, необходимо проанализировать формат даты в журнале и указать его в соответствующем поле для последующего вывода.

Формат вывода даты: yyyy-d-m hh:mm:ss.

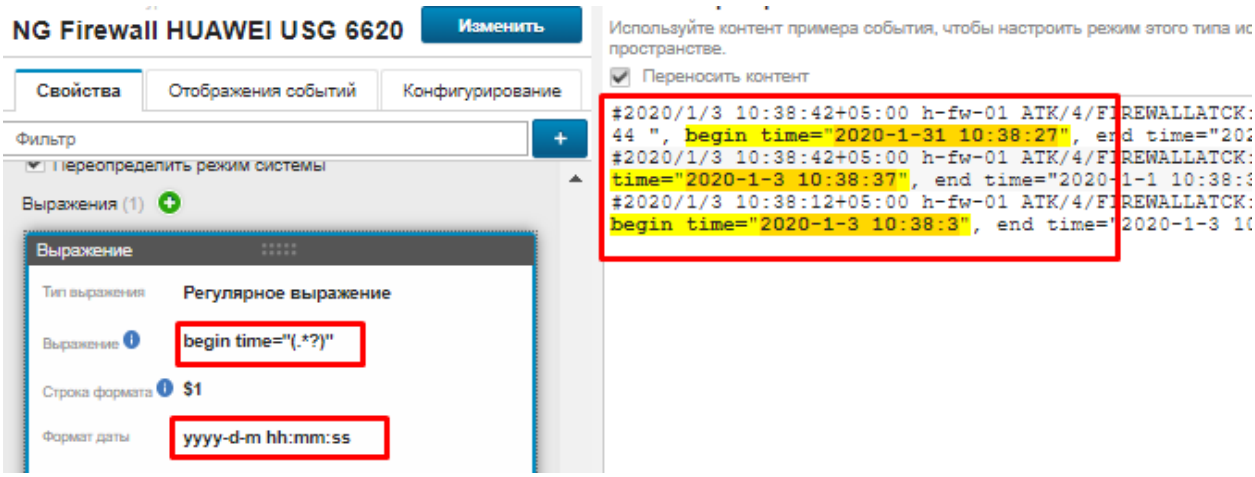


Рисунок 2.50 – Формула даты и времени события

Вывод времени события (рисунок 2.51).

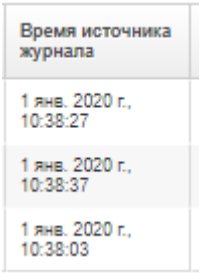


Рисунок 2.51 – Вывод даты и времени события

Вывод интерфейса события. Стандартными средствами в IBM QRadar SIEM не предусмотрено свойство интерфейса события. Добавляем свойство «Interface» вручную, выбрав вкладку «Создание свойства» (рисунок 2.52) и выбрав тип поля «Текст» (рисунок 2.53). Далее выбираем новое пользовательское свойство и добавляем регулярное выражение (рисунок 2.54).

Формула регулярного выражения: interface="(.*?)"

Поле interface=""– Ограничения выражения в рамках которого находится интерфейс события.

(.*?) – В рамках данного сгруппированного выражения будут определяться все символы до символа «”».

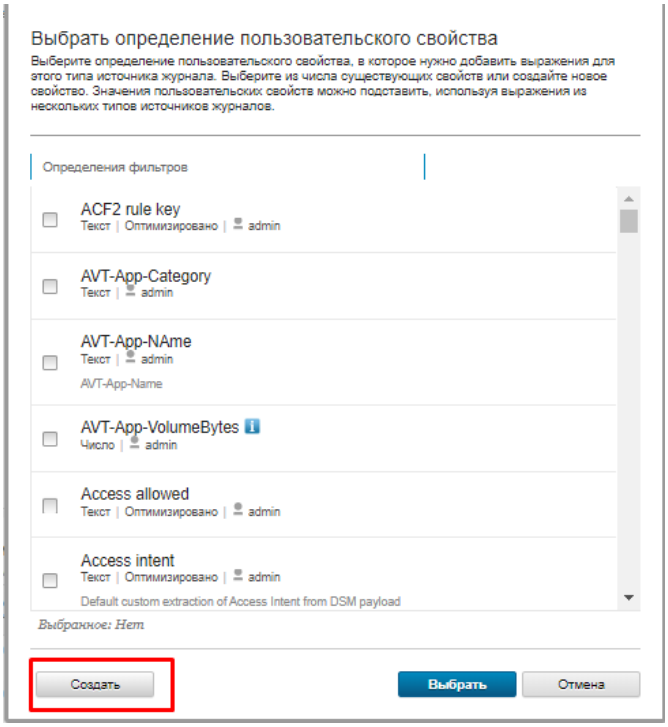


Рисунок 2.52 – Создание нового поля свойства

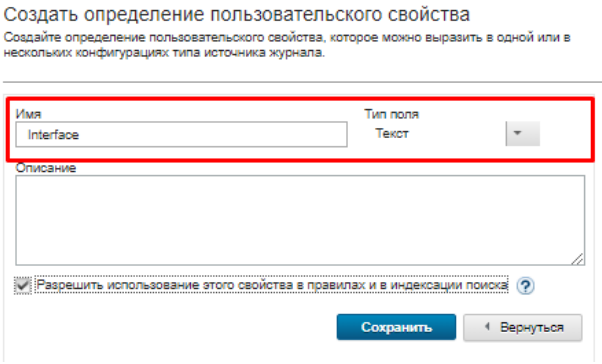


Рисунок 2.53 – Тип нового свойства

Рисунок 2.54 – Регулярное выражение

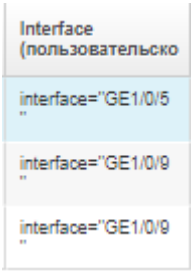


Рисунок 2.55 – Вывод интерфейса

Вывод IP-адреса источника.

Формула регулярного выражения: src="(.*?)\s (рисунок 2.56)

Поле src="– Начиная с данного выражения будет происходить фильтрация строки.

(.*?) – В рамках данного сгруппированного выражения будут определяться все символы до символа «\s».

\s – Ограничение выражения пробельным символом.

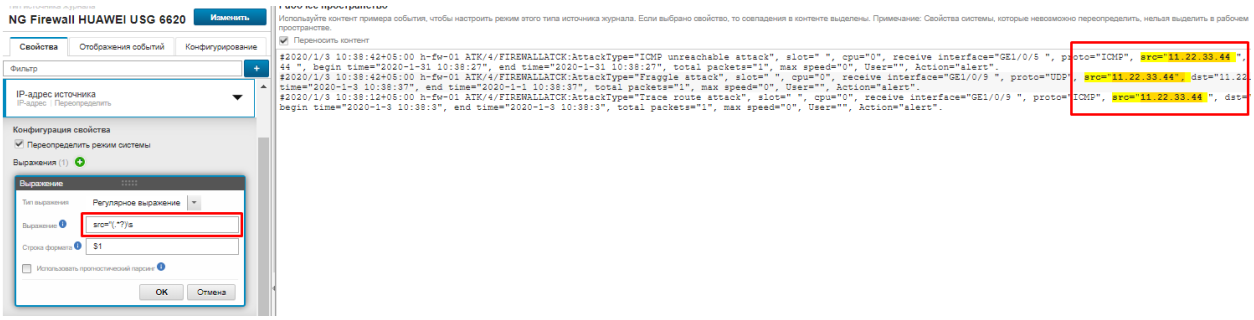


Рисунок 2.56 – Регулярное выражение

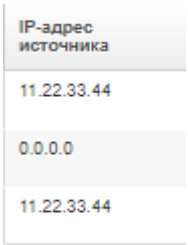


Рисунок 2.57 – Вывод IP – адресов источника

Вывод IP-адреса назначения.

Формула регулярного выражения: dst="(.*?)\s (рисунок 2.58)

Поле dst ="– Начиная с данного выражения будет происходить фильтрация строки.

(.*?) – В рамках данного сгруппированного выражения будут определяться все символы до символа «\s».

\s – Ограничение выражения пробельным символом.

Рисунок 2.58 – Регулярное выражение

IP-адрес назначения
11.22.33.44
11.22.33.44
11.22.33.44

Рисунок 2.59 – вывод IP-адресов назначения

Вывод действия «Action».

Формула регулярного выражения: Action="(.*?)" (рисунок 2.60).

Поле Action ="" – Ограничения выражения в рамках которого находится действие события.

(.*?) – В рамках данного сгруппированного выражения будут определяться все символы до символа «”».

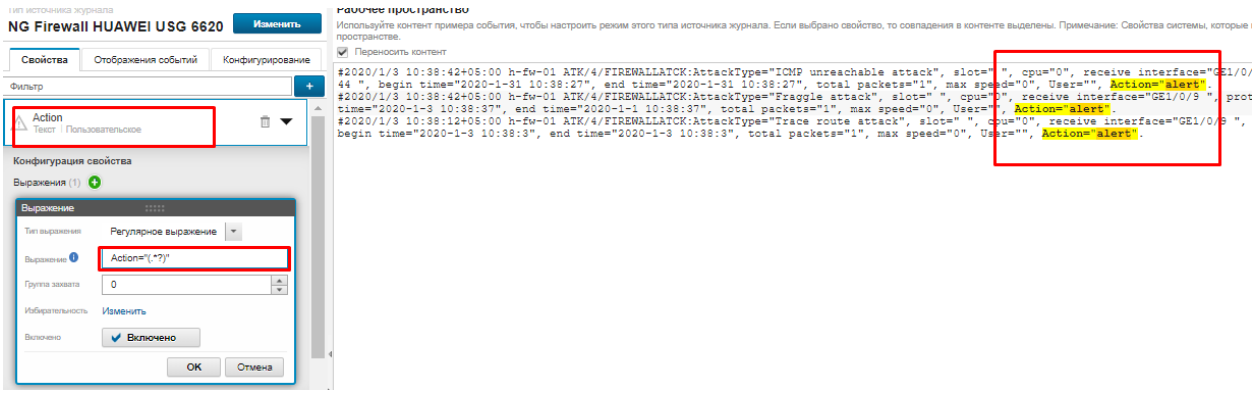


Рисунок 2.60 – Регулярное выражение

Action (пользовательско
Action="alert"
Action="alert"
Action="alert"

Рисунок 2.61 – Вывод поля события

Далее необходимо сконфигурировать просмотр операций журнала, чтобы убрать лишние поля, которые не нужны в данных критериях поиска (рисунок 2.62).

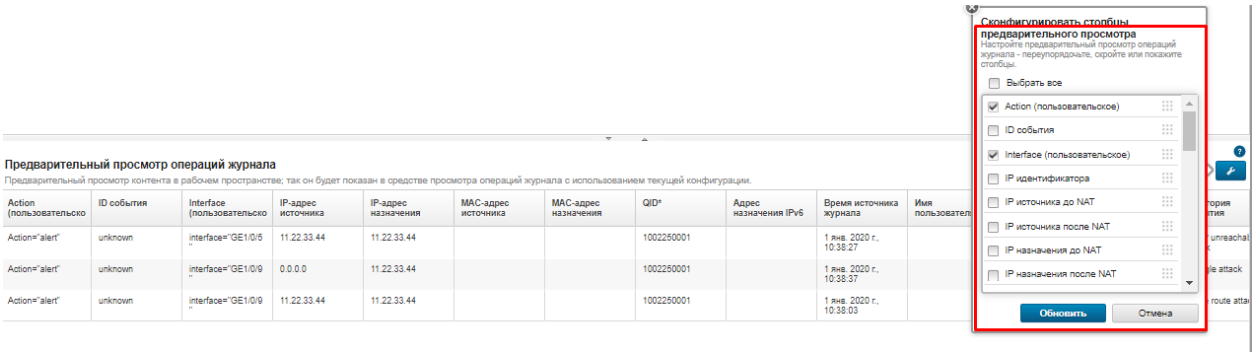


Рисунок 2.62 – Конфигурация отображаемых полей

Нормализовав вид журнала, можно увидеть его окончательную версию, в котором будет представлен готовый источник журнала для NG Firewall Huawei USG 6620 (рисунок 2.63).

Редактор DSM предоставляем возможность экспорта (рисунок 2.64) созданной конфигурации, что очень полезно при переустановке системы, использовании данной конфигурации на другом устройстве или восстановлении при сбое.

Action (пользовательско	Interface (пользовательско	IP-адрес источника	IP-адрес назначения	Время источника журнала	Категория события
Action="alert"	interface="GE1/0/5 "	11.22.33.44	11.22.33.44	1 янв. 2020 г., 10:38:27	ICMP unreachable attack
Action="alert"	interface="GE1/0/9 "	0.0.0.0	11.22.33.44	1 янв. 2020 г., 10:38:37	Fraggle attack
Action="alert"	interface="GE1/0/9 "	11.22.33.44	11.22.33.44	1 янв. 2020 г., 10:38:03	Trace route attack

Рисунок 2.63 – Окончательный вид журнала

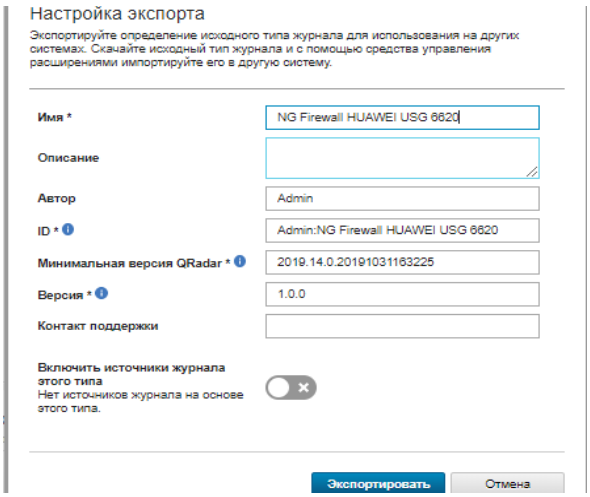


Рисунок 2.64 – Экспорт конфигурации

Экспорт конфигурации DSM в формате .zip (рисунок 2.65).

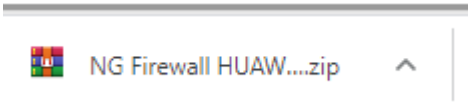


Рисунок 2.65 - Экспорт конфигурации DSM в формате .zip

В Редакторе DSM создаем новый тип источника журнала для Hikvision. Задаем имя нового источника (рисунок 2.66). Создав новый тип источника появляется рабочее пространство и вкладка свойств. Добавляем образец журнала в рабочее пространство (рисунок 2.67).

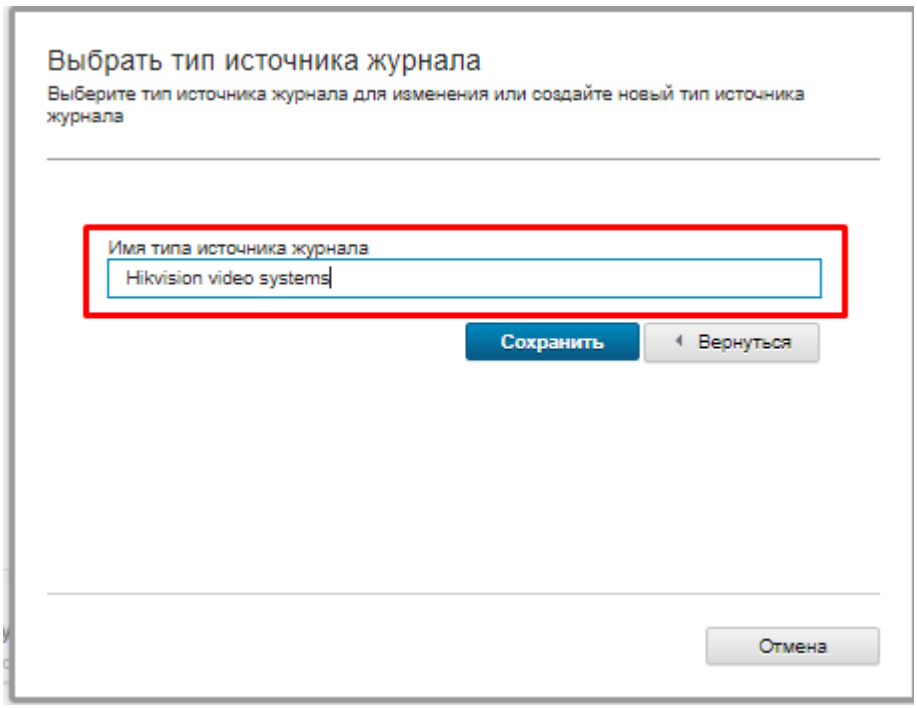


Рисунок 2.66 – Создание нового типа источника

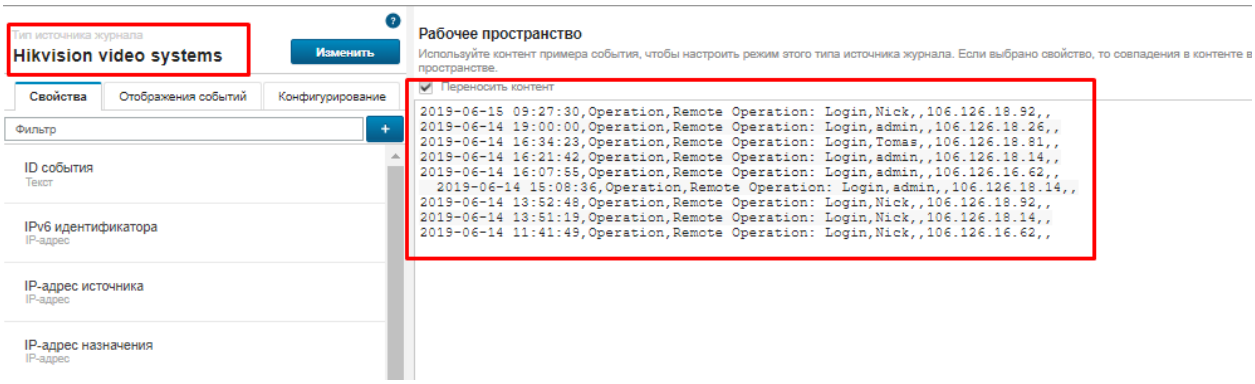


Рисунок 2.67 – Образец журнала нового источника

Вывод даты события.

Формула регулярного выражения: (\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2}) (рисунок 2.68).

Поля \d{} – Определяют цифровые символы и в их количество в фигурных скобках.

Конец сгруппированного выражения определяется первым символом «,», так как дата и время находятся в начале строки данного журнала.

В случаях выполнения поиска даты, необходимо проанализировать формат даты в журнале и указать его в соответствующем поле для последующего вывода.

Формат вывода даты: yyyy-MM-dd hh:mm:ss

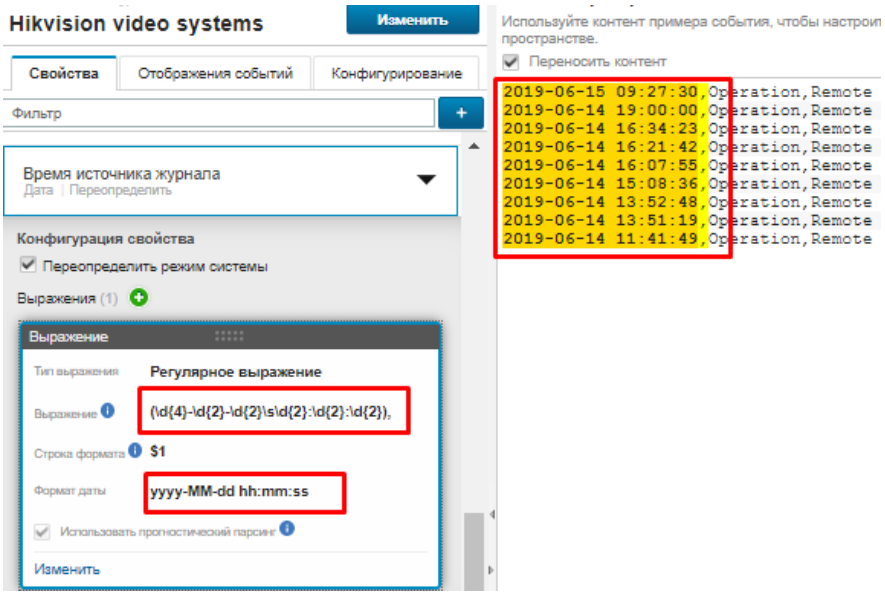


Рисунок 2.68 – Формула регулярного выражения

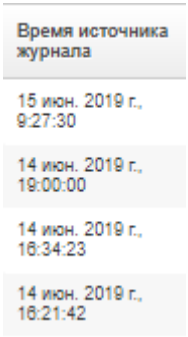


Рисунок 2.69 – Вывод времени источника журнала

Вывод события входа, выхода в систему и имени пользователя.

Так как данное свойство не предусмотрено стандартными средствами, добавляем его как новое пользовательское свойство «Operation and User» (рисунок 2.70).

Формула регулярного выражения: Operation:\s(Log(in|out),[a-zA-Z0-9]*),,

\s – Экранирование пробелом начала поиска строки.

Operation:\s ,, - Рамки экранирования поиска по операции и имени пользователя.

(Log(in|out),[a-zA-Z0-9]*) – Данная строка группирует свойства по которым будет произведен поиск

Log(in|out) – События входа и выхода в зависимости от значения, «|» означает операцию «ИЛИ».

[a-zA-Z0-9]* - Группа имени пользователя, разрешает использование неограниченного количества цифр и букв в разном регистре.

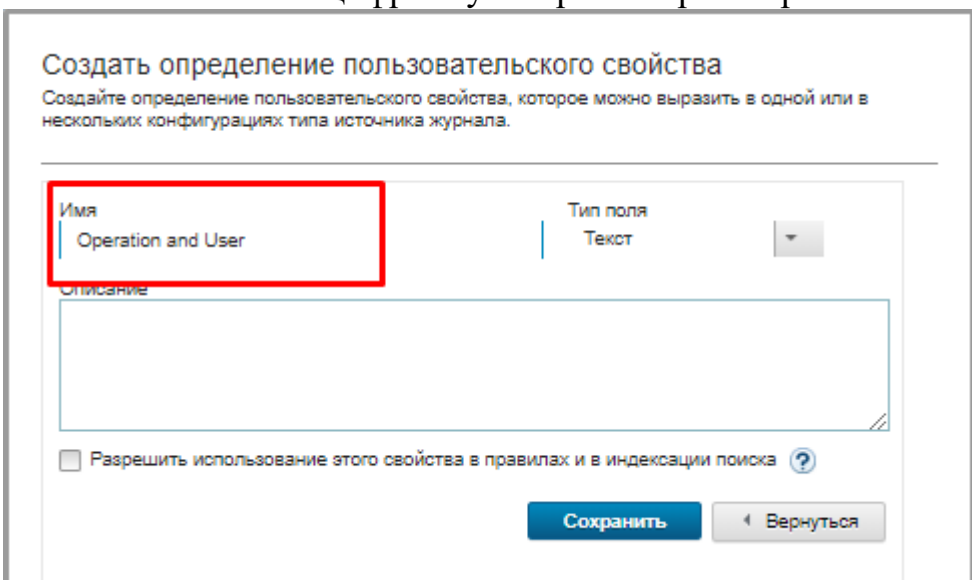


Рисунок 2.70 – Создание пользовательского свойства

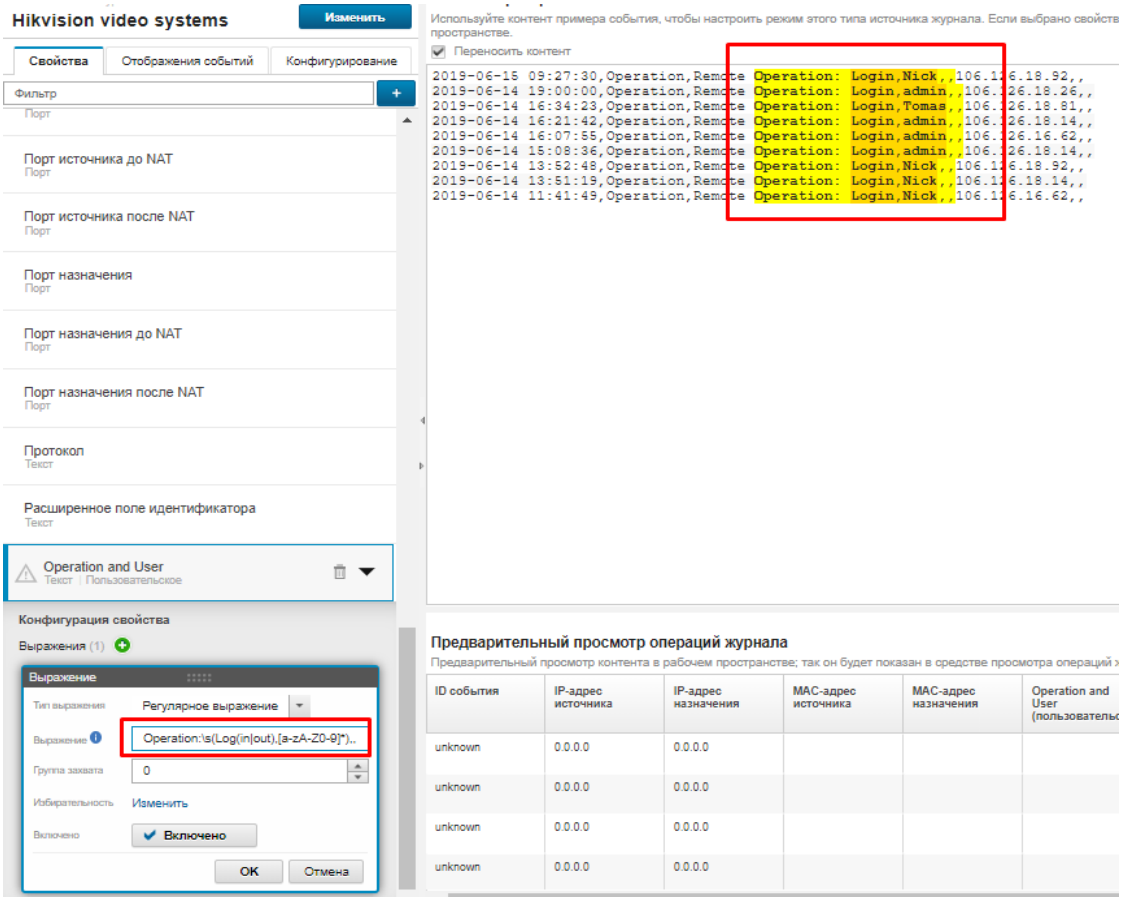


Рисунок 2.71 – Формула регулярного выражения

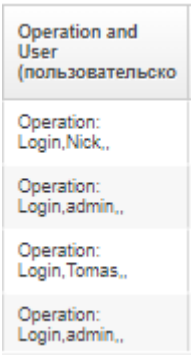


Рисунок 2.72 – Вывод пользователей

Вывод IP- адреса пользователя.

Формула регулярного выражения: ,(.*?),, (рисунок 2.73)

(.*?) – В рамках данного сгруппированного выражения будут определяться все символы начиная и заканчивая символами «,,» в рамках которых и находится IP – адрес пользователя.

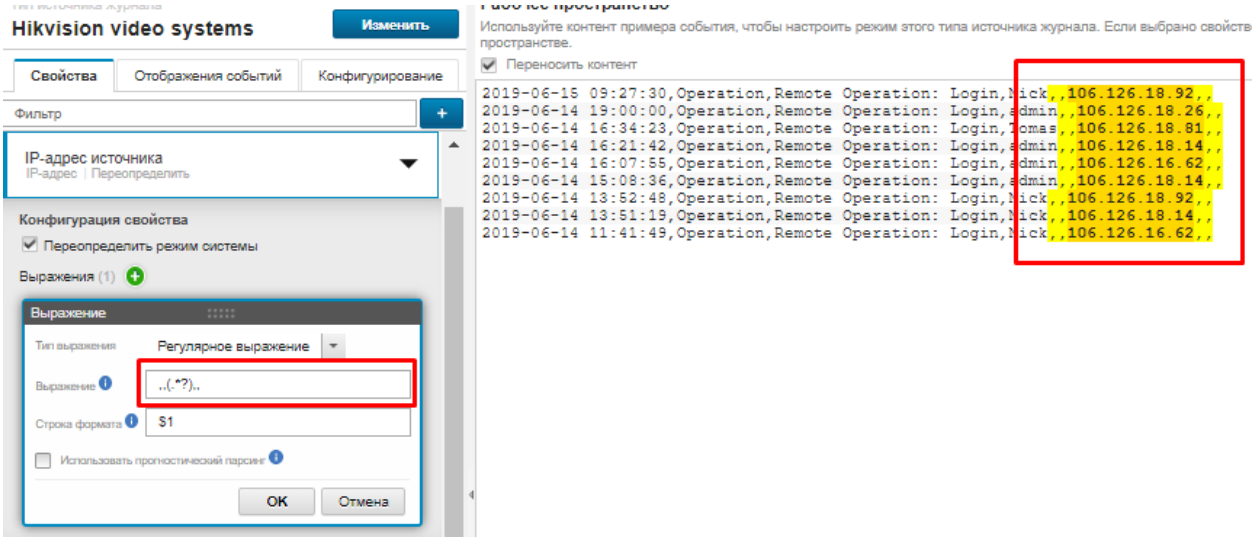


Рисунок 2.73 – Формула регулярного выражения

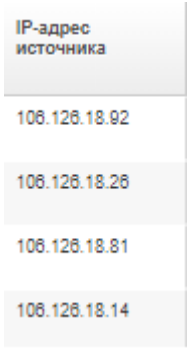


Рисунок 2.74 – Вывод IP – адресов источника

Далее необходимо сконфигурировать просмотр операций журнала, чтобы убрать лишние поля, которые не нужны в данных критериях поиска.

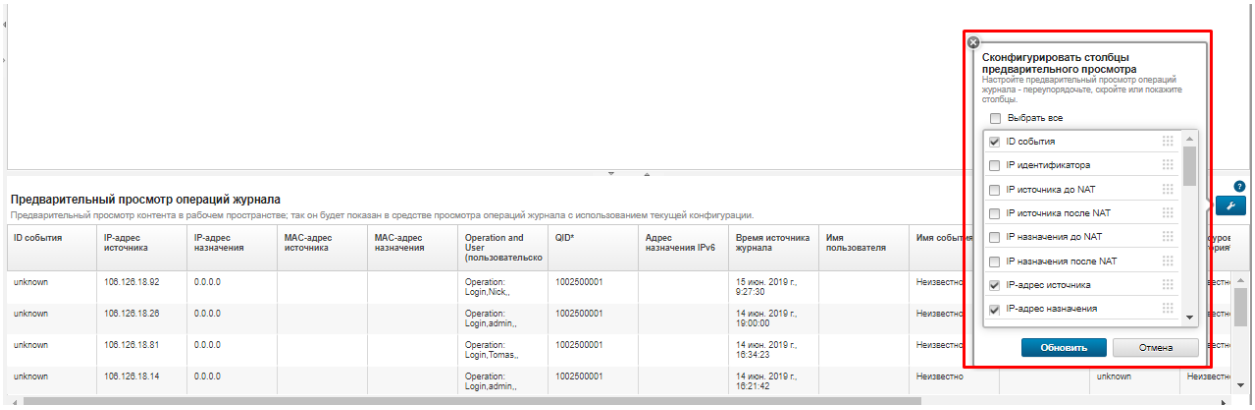


Рисунок 2.75 - Конфигурация отображаемых полей

Нормализовав вид журнала, можно увидеть его окончательную версию, в котором будет представлен готовый источник журнала для системы видеонаблюдения Hikvision.

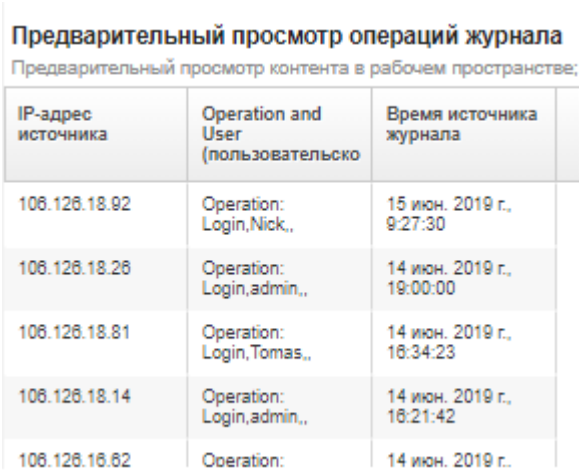


Рисунок 2.76 – Окончательный вид журнала

2.4.2. Расследование Resilient

В рамках расследования было выбрано событие из журнала межсетевого экрана зафиксированное в IBM QRadar “Fraggle attack”[10] (рисунок 2.77).

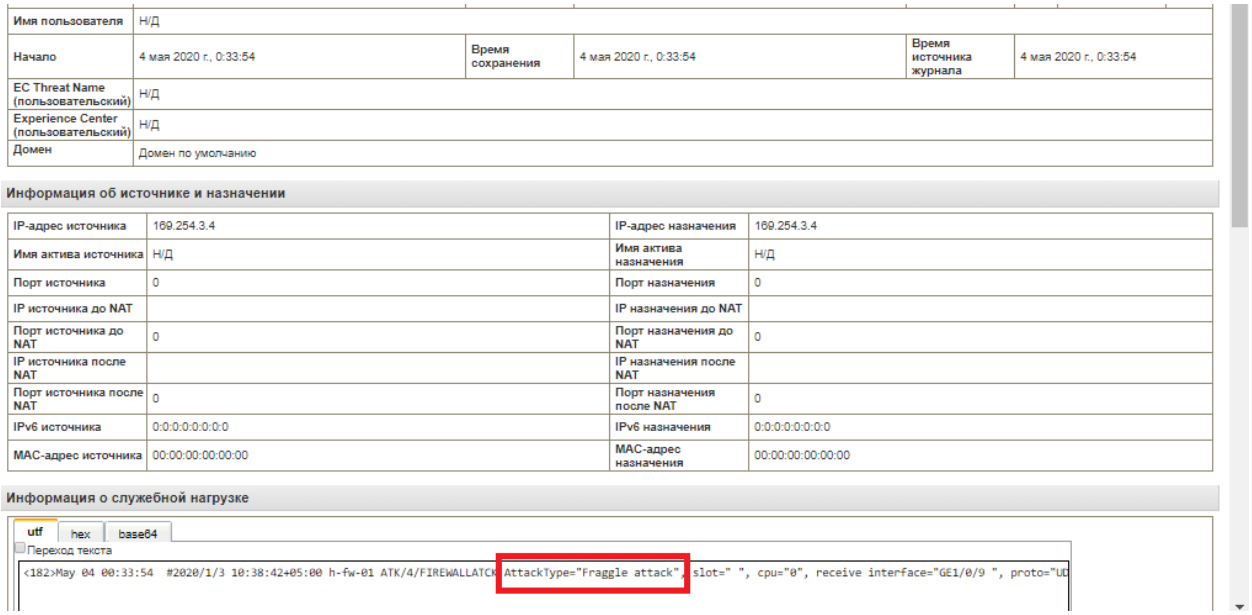


Рисунок 2.77 – Событие Fraggle attack

Нормализованное событие с помощью Редактора DSM и регулярных выражений (рисунок 2.77) [11].

Action (пользовательско	Interface (пользовательско	IP-адрес источника	IP-адрес назначения	Время источника журнала	Категория события
Action="alert"	interface="GE1/0/9 "	0.0.0.0	11.22.33.44	1 янв. 2020 г., 10:38:37	Fraggle attack

Рисунок 2.78 – Нормализованное событие

Созданный инцидент в IBM Resilient (рисунок 2.79)

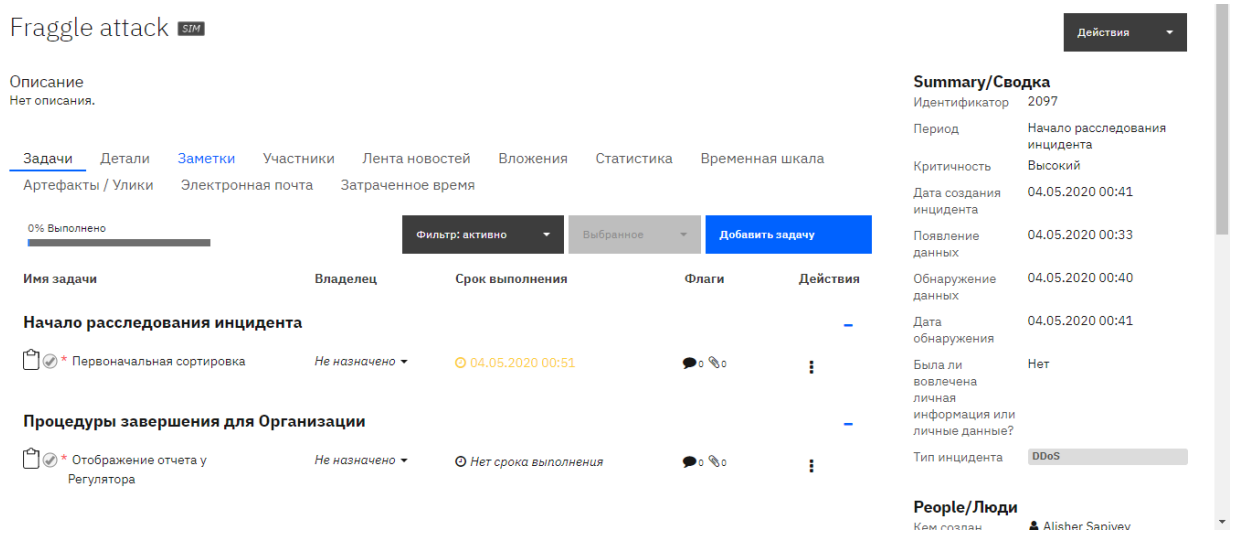


Рисунок 2.79 – Созданный инцидент

Назначение исполнителя ответственного за расследование (рисунок 2.80).

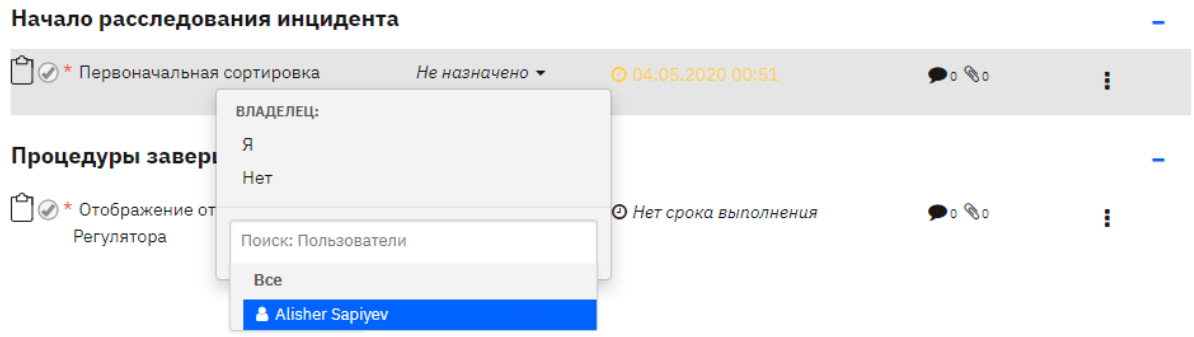


Рисунок 2.80 – Назначение исполнителя

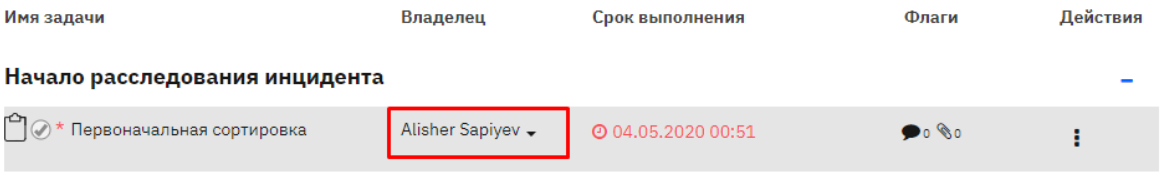


Рисунок 2.81 - Назначение исполнителя

Определение срока выполнения начала расследования инцидента (рисунок 2.82).

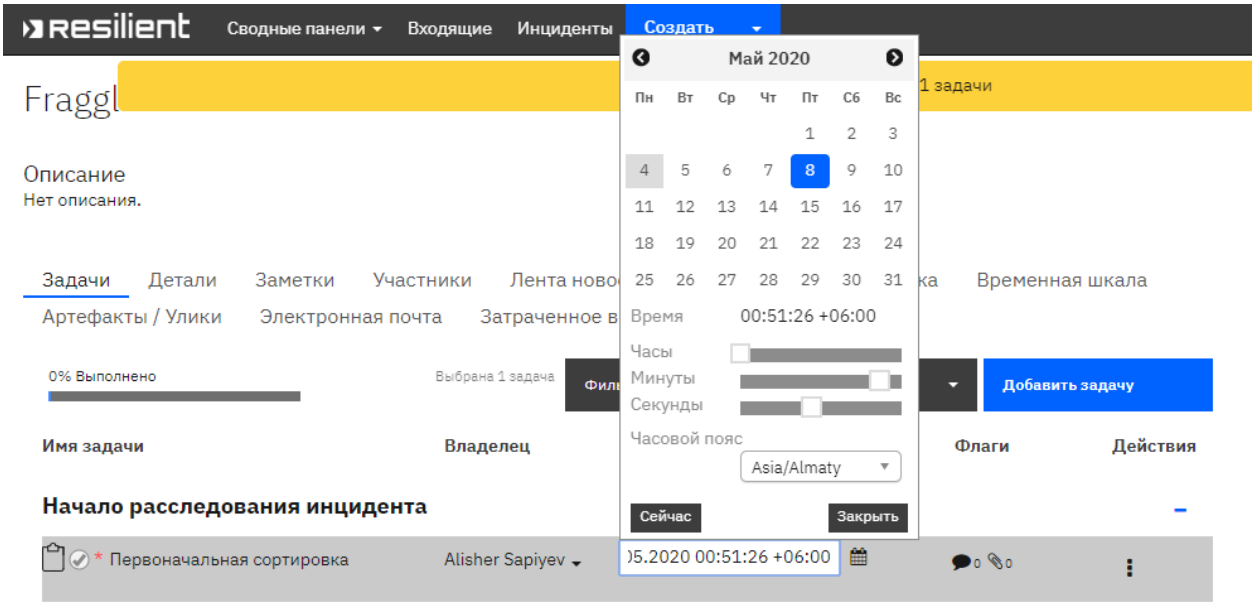


Рисунок 2.82 – Назначение сроков

Вложение оригинального лога [12] (рисунок 2.83).

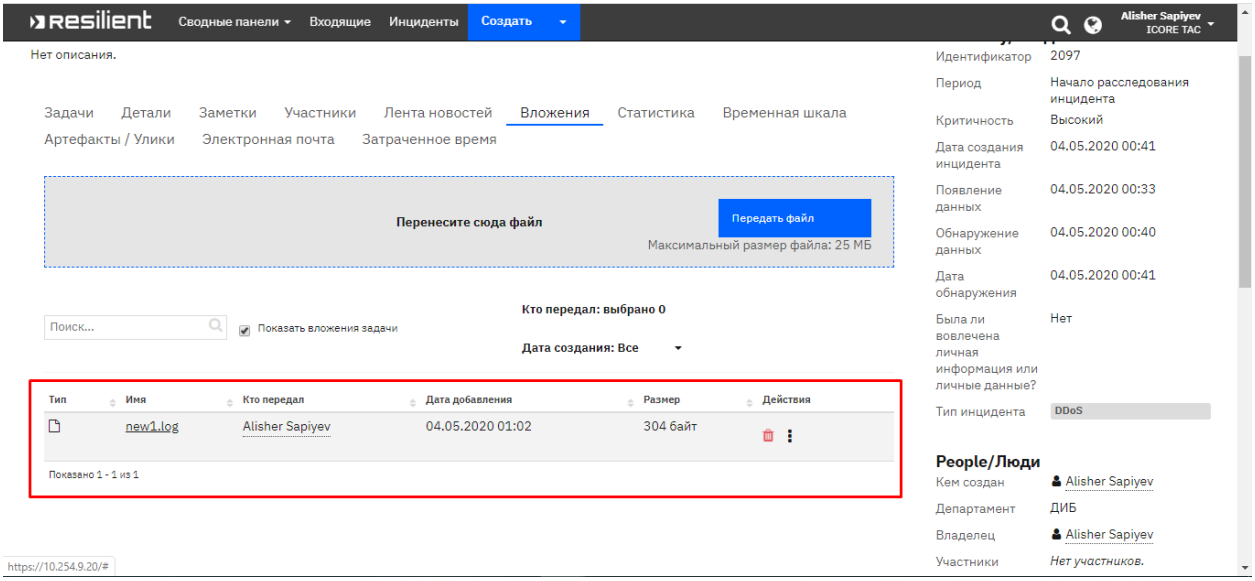


Рисунок 2.83 – Вложение оригинального лога

Определение артефактов для данного инцидента [13]. За артефакты приняли такие значения как: название атаки, источник лога, IP-адрес источника и получателя (рисунок 2.84).

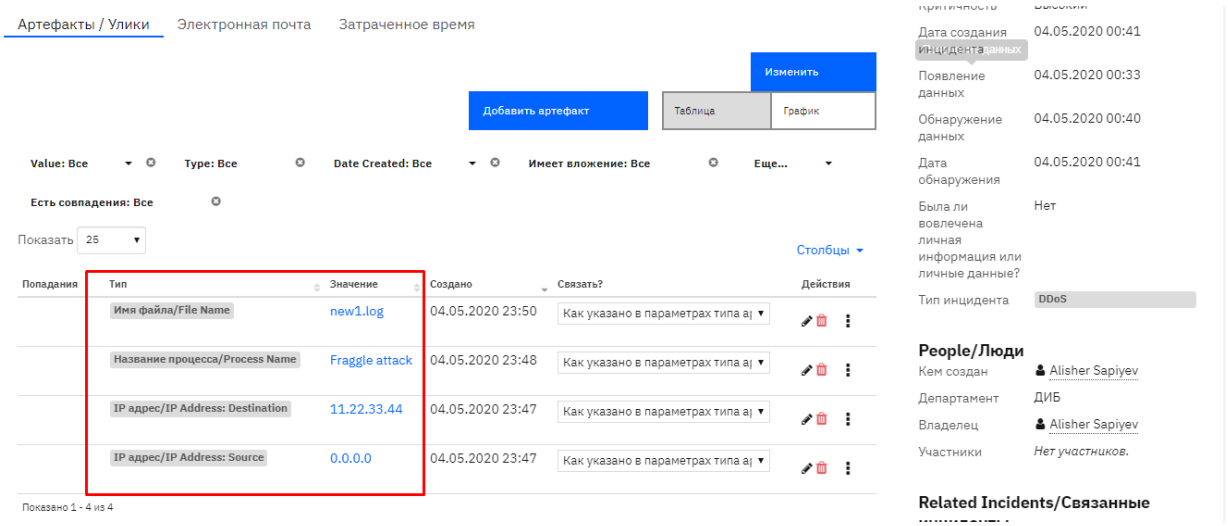


Рисунок 2.84 – Определение артефактов инцидента

Завершение выполнения данного этапа «Начало расследования инцидента» (рисунок 2.85).

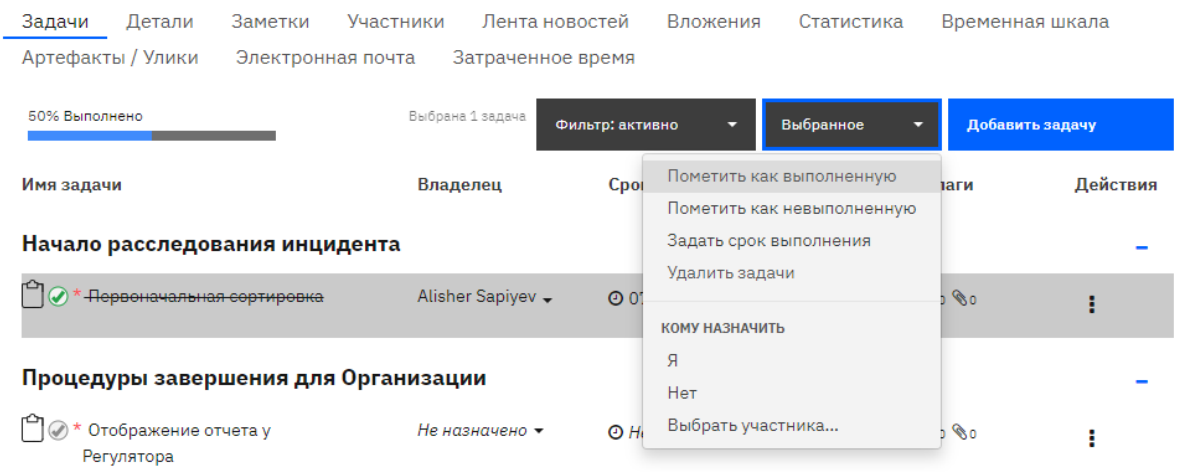


Рисунок 2.85 – Завершение этапа «Начало расследования»

Постановка последующей задачи «Анализ инцидента» (рисунок 2.86).

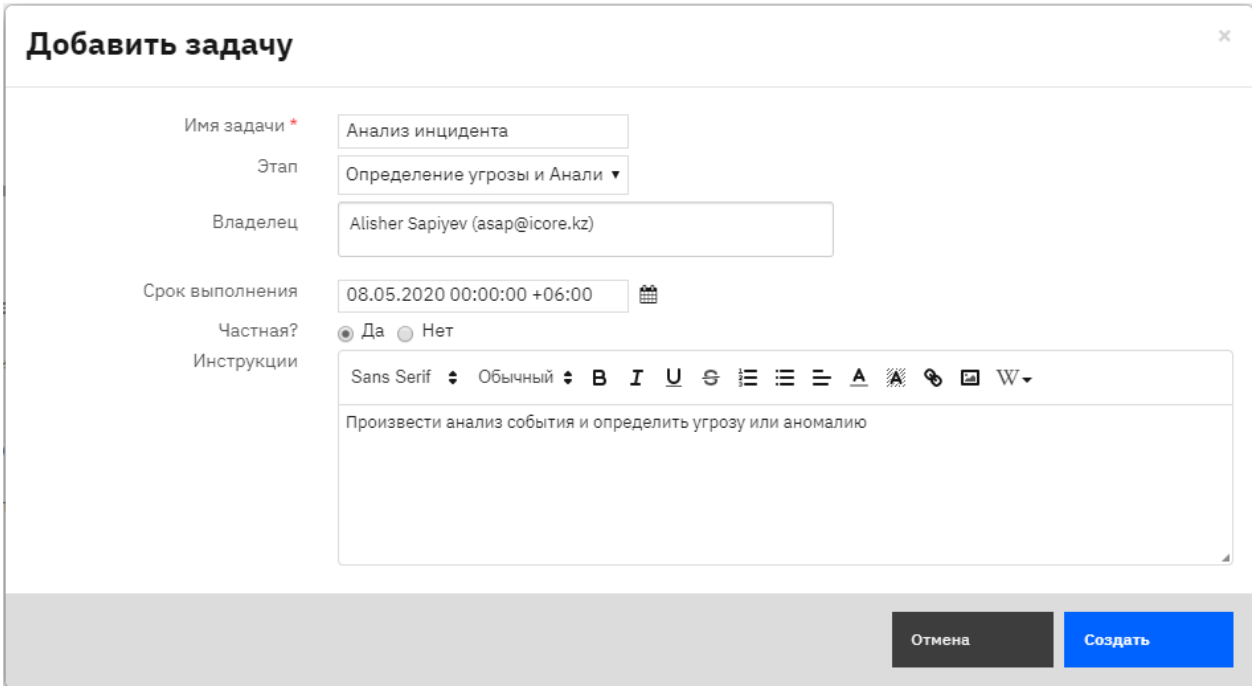


Рисунок 2.86 – Создание задачи «Анализ инцидента»

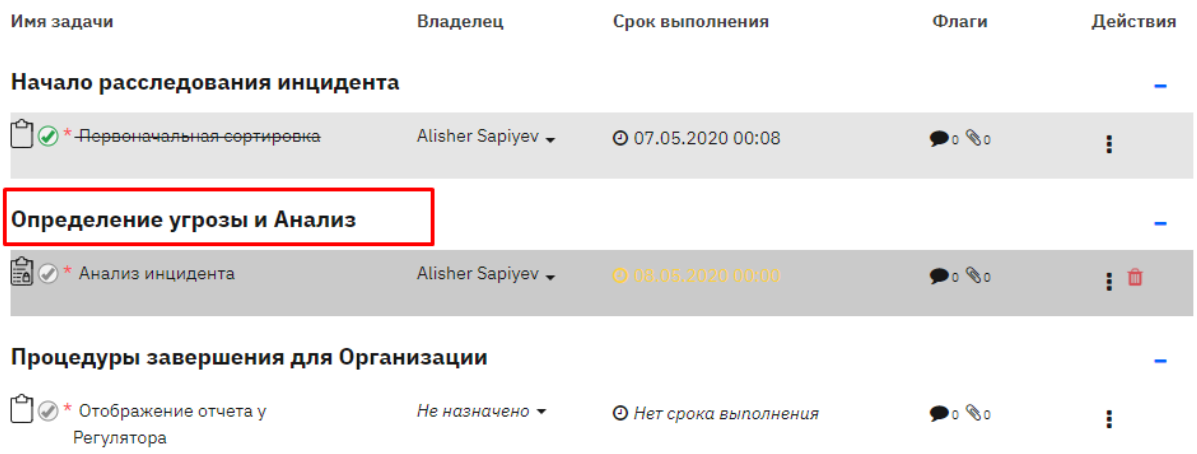


Рисунок 2.87 - Создание задачи «Анализ инцидента»

Добавление примечаний о ходе выполнения этапа анализа расследования (рисунок 2.88).

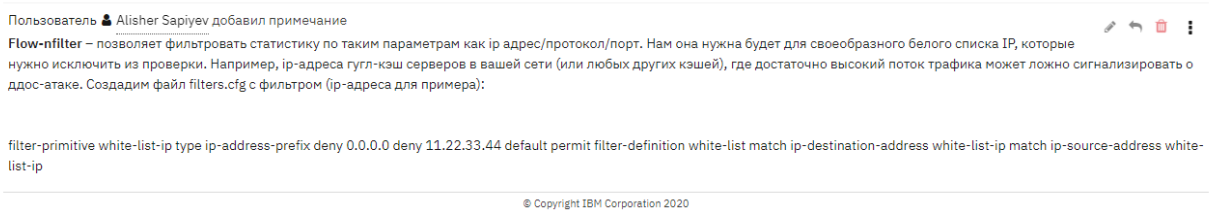


Рисунок 2.88 – Ход расследования

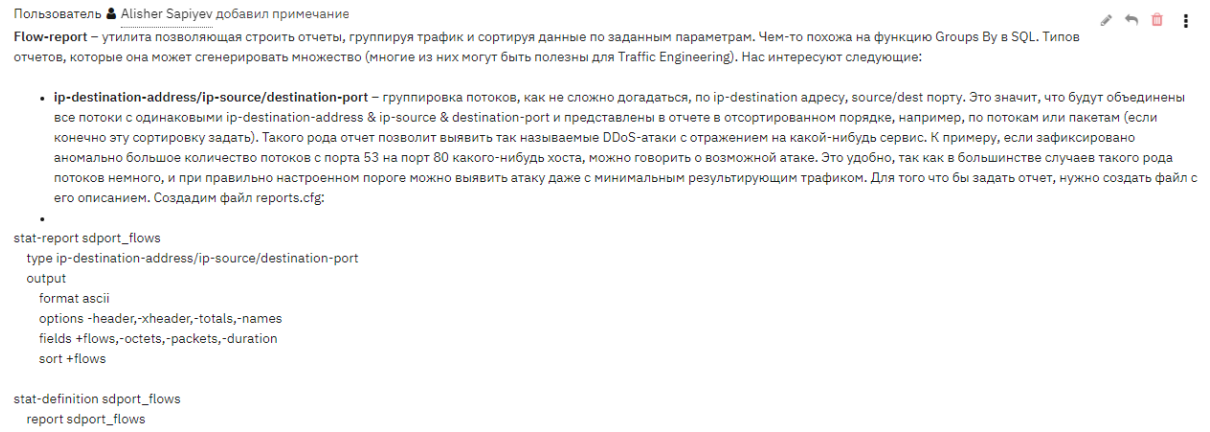


Рисунок 2.89 - Ход расследования

Завершение этапа расследования «Определение угрозы и анализа инцидента» (рисунок 2.90).

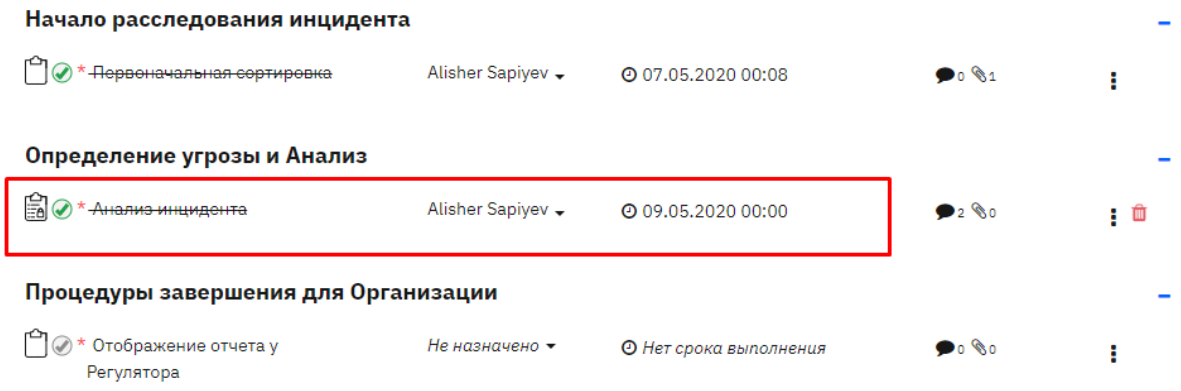


Рисунок 2.90 – Завершение этапа «Анализ инцидента».

Постановка следующей задачи «Реагирование на инцидент» (рисунок 2.91).

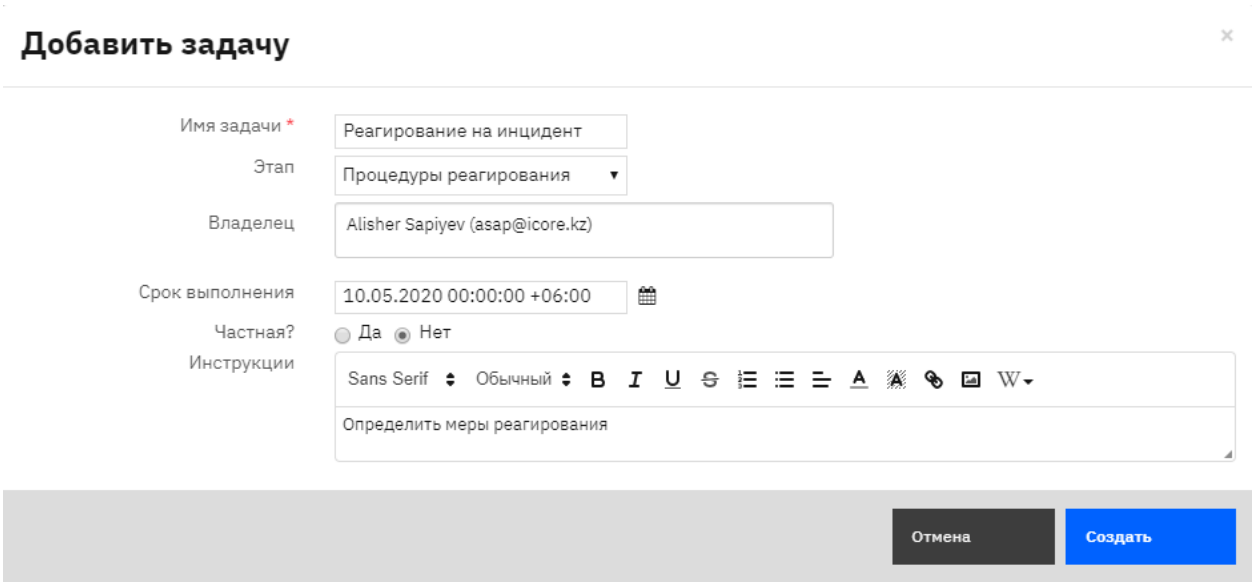


Рисунок 2.91 – Создание задачи реагирование на инцидент

Примечания о ходе выполнения этапа «Реагирование на инцидент» (рисунок 2.92).

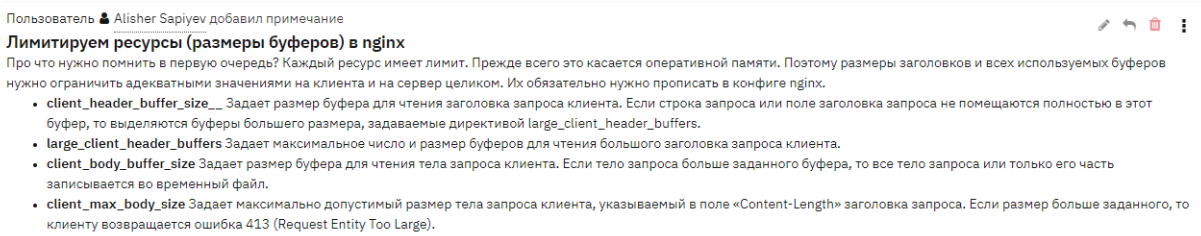
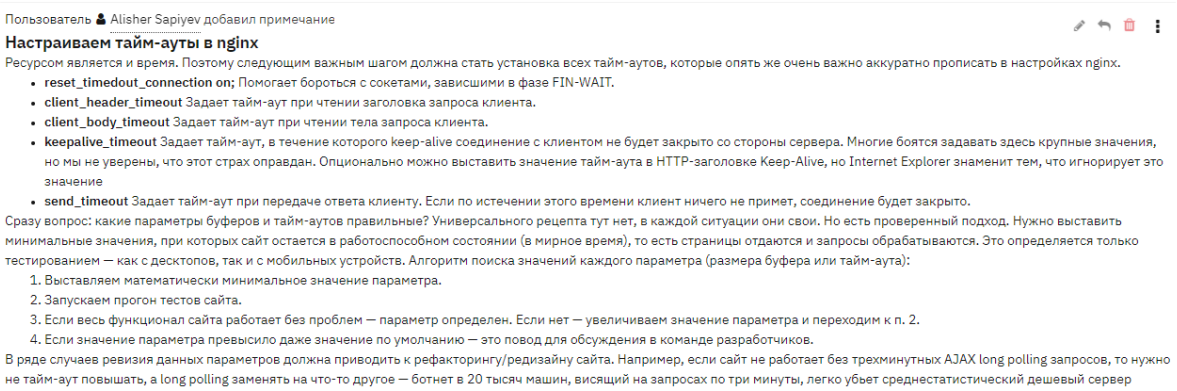


Рисунок 2.92 – Реагирование на инцидент



Пользователь Alisher Sapiyev добавил примечание

Настраиваем тайм-ауты в nginx

Ресурсом является и время. Поэтому следующим важным шагом должна стать установка всех тайм-аутов, которые опять же очень важно аккуратно прописать в настройках nginx.

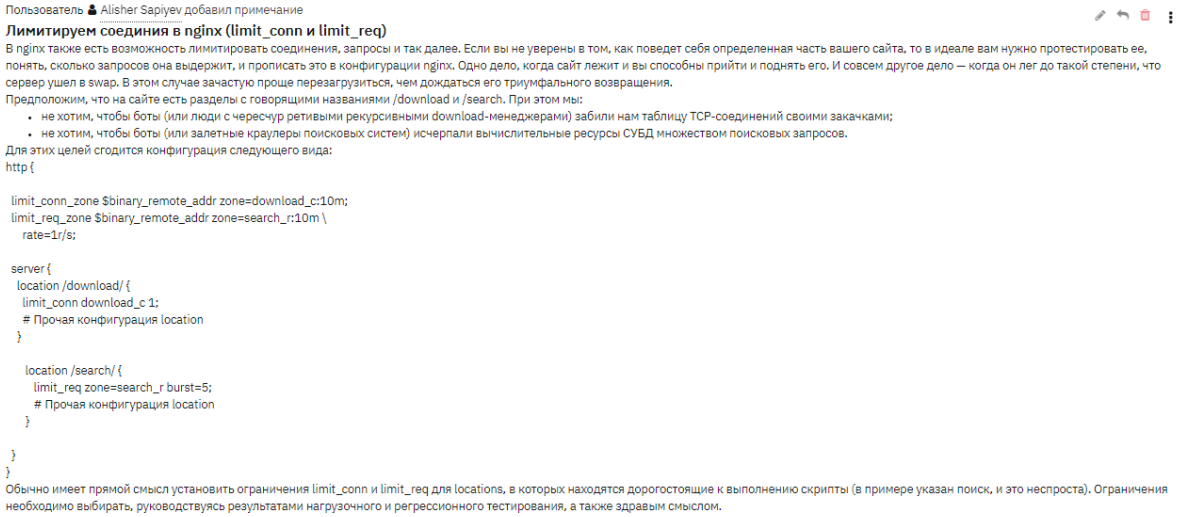
- **reset_timedout_connection on;** Помогает бороться с сокетами, зависшими в фазе FIN-WAIT.
- **client_header_timeout** Задает тайм-аут при чтении заголовка запроса клиента.
- **client_body_timeout** Задает тайм-аут при чтении тела запроса клиента.
- **keepalive_timeout** Задает тайм-аут, в течение которого keep-alive соединение с клиентом не будет закрыто со стороны сервера. Многие боятся задавать здесь крупные значения, но мы не уверены, что этот страх оправдан. Опционально можно выставить значение тайм-аута в HTTP-заголовке Keep-Alive, но Internet Explorer знаменит тем, что игнорирует это значение
- **send_timeout** Задает тайм-аут при передаче ответа клиенту. Если по истечении этого времени клиент ничего не примет, соединение будет закрыто.

Сразу вопрос: какие параметры буферов и тайм-аутов правильные? Универсального рецепта тут нет, в каждой ситуации они свои. Но есть проверенный подход. Нужно выставить минимальные значения, при которых сайт остается в работоспособном состоянии (в мирное время), то есть страницы отдаются и запросы обрабатываются. Это определяется только тестированием — как с десктопов, так и с мобильных устройств. Алгоритм поиска значений каждого параметра (размера буфера или тайм-аута):

1. Выставляем математически минимальное значение параметра.
2. Запускаем прогон тестов сайта.
3. Если весь функционал сайта работает без проблем — параметр определен. Если нет — увеличиваем значение параметра и переходим к п. 2.
4. Если значение параметра превысило даже значение по умолчанию — это повод для обсуждения в команде разработчиков.

В ряде случаев ревизия данных параметров должна приводить к рефакторингу/редизайну сайта. Например, если сайт не работает без трехминутных AJAX long polling запросов, то нужно не тайм-аут повышать, а long polling заменять на что-то другое — ботнет в 20 тысяч машин, висящий на запросах по три минуты, легко убьет среднестатистический дешевый сервер

Рисунок 2.93 - Реагирование на инцидент



Пользователь Alisher Sapiyev добавил примечание

Лимитируем соединия в nginx (limit_conn и limit_req)

В nginx также есть возможность лимитировать соединения, запросы и так далее. Если вы не уверены в том, как поведет себя определенная часть вашего сайта, то в идеале вам нужно протестировать ее, понять, сколько запросов она выдержит, и прописать это в конфигурации nginx. Одно дело, когда сайт лежит и вы способны прийти и поднять его. И совсем другое дело — когда он лег до такой степени, что сервер ушел в swap. В этом случае зачастую проще перезагрузиться, чем дождаться его триумфального возвращения.

Предположим, что на сайте есть разделы с говорящими названиями /download и /search. При этом мы:

- не хотим, чтобы боты (или люди с чересчур ретивыми рекурсивными download-менеджерами) забили нам таблицу TCP-соединений своими закачками;
- не хотим, чтобы боты (или залетные краулеры поисковых систем) исчерпали вычислительные ресурсы СУБД множеством поисковых запросов.

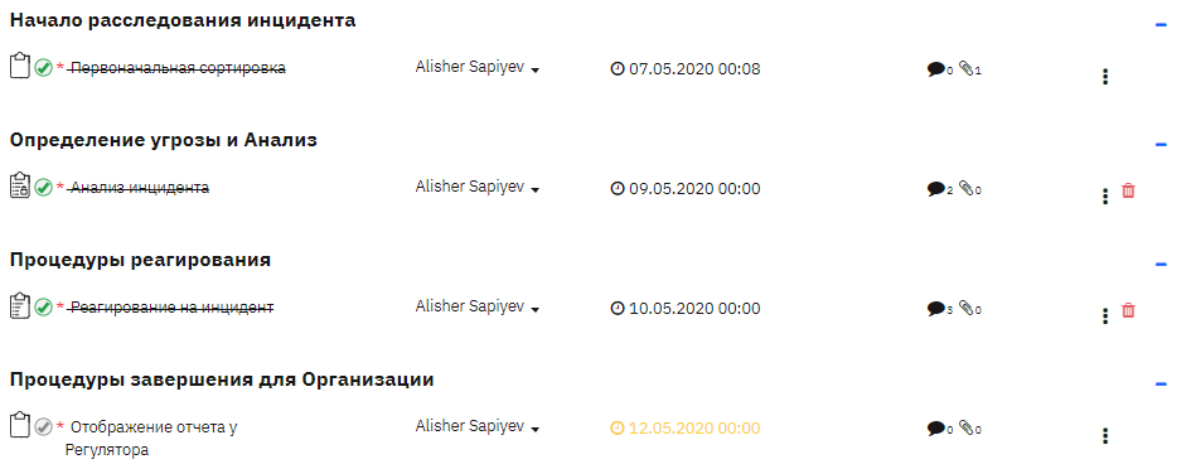
Для этих целей сгодится конфигурация следующего вида:

```
http {

 limit_conn_zone $binary_remote_addr zone=download_c:10m;
 limit_req_zone $binary_remote_addr zone=search_r:10m \
    rate=1r/s;

 server {
  location /download/ {
   limit_conn download_c 1;
   # Прочая конфигурация location
  }

    location /search/ {
     limit_req zone=search_r burst=5;
     # Прочая конфигурация location
    }

 }
}
```

Обычно имеет прямой смысл установить ограничения limit_conn и limit_req для locations, в которых находятся дорогостоящие к выполнению скрипты (в примере указан поиск, и это неспроста). Ограничения необходимо выбирать, руководствуясь результатами нагрузочного и регрессионного тестирования, а также здравым смыслом.

Рисунок 2.94 - Реагирование на инцидент

Завершение этапа «Реагирование на инцидент» (рисунок 2.95).



Начало расследования инцидента

~~* Первоначальная сортировка~~ Alisher Sapiyev 07.05.2020 00:08 0 1

Определение угрозы и Анализ

~~* Анализ инцидента~~ Alisher Sapiyev 09.05.2020 00:00 2 0

Процедуры реагирования

~~* Реагирование на инцидент~~ Alisher Sapiyev 10.05.2020 00:00 3 0

Процедуры завершения для Организации

* Отображение отчета у Регулятора Alisher Sapiyev 12.05.2020 00:00 0 0

Рисунок 2.95 – Завершение этапа «Реагирование на инцидент»

Завершение выполнения поставленной задачи с предоставление отчета о проделанной работе (рисунок 2.96).

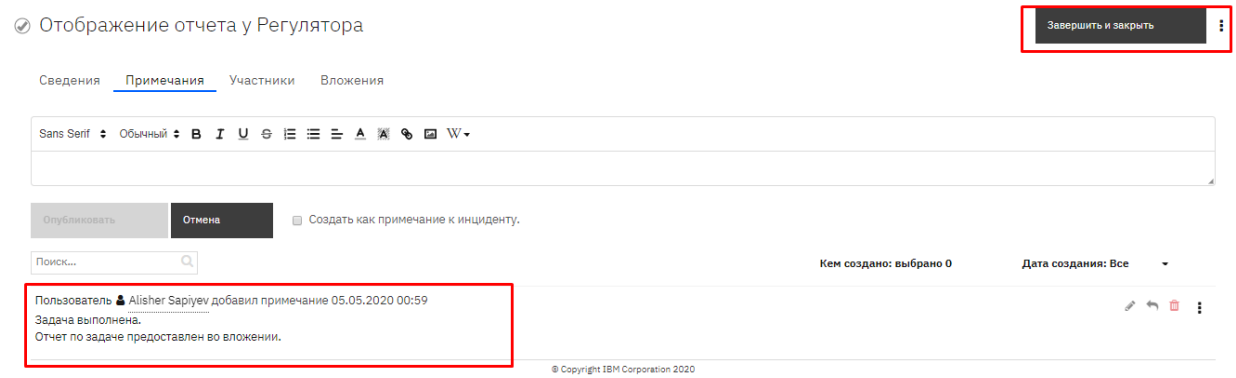


Рисунок 2.96 – Закрытие задачи

Вложение отчета о проделанной работе (рисунок 2.97).

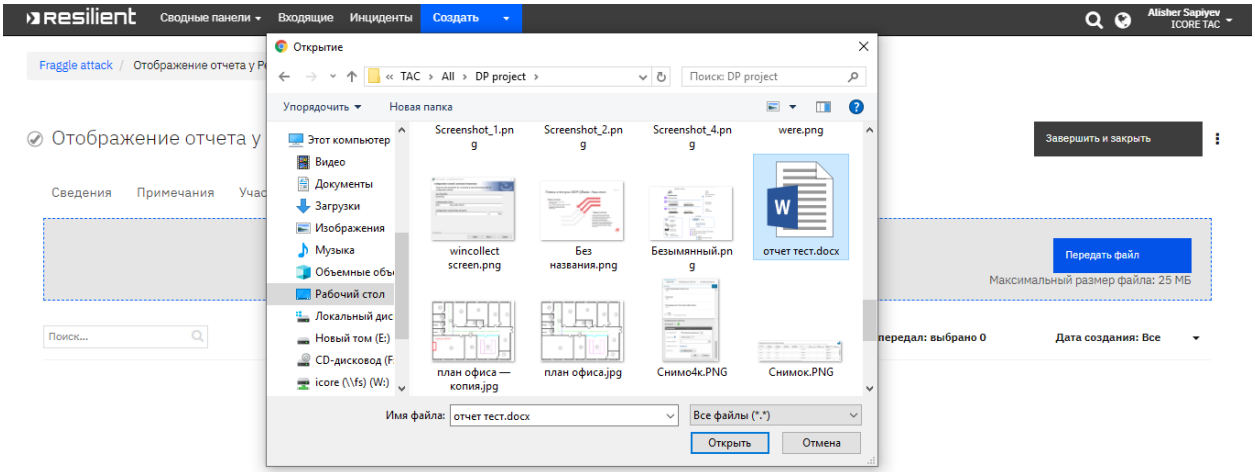


Рисунок 2.97 – Отчет о проделанной работе

Окончательная процедура закрытия инцидента (рисунок 2.98).

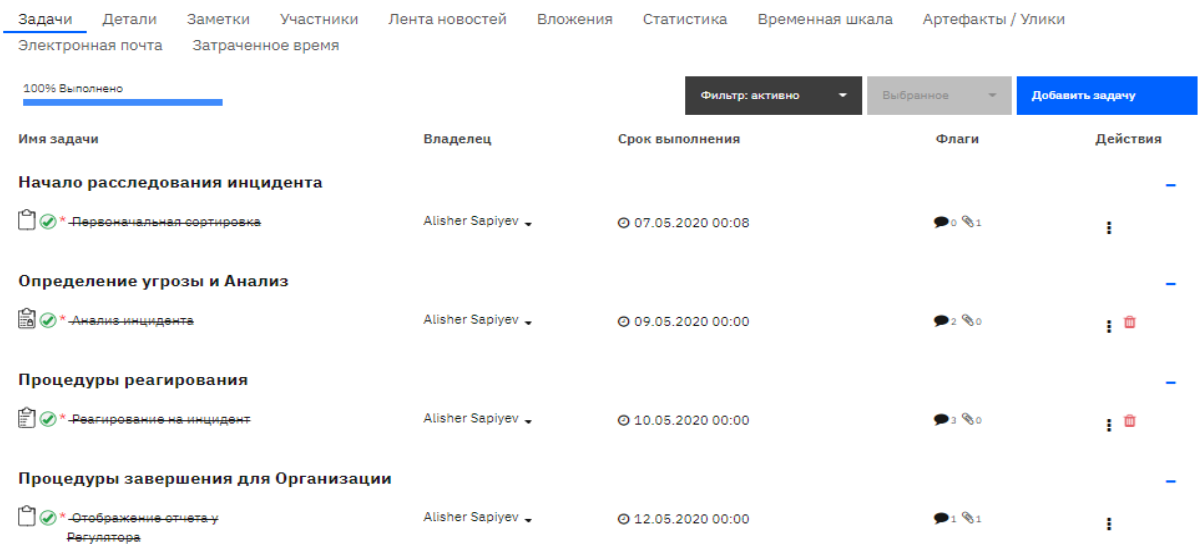


Рисунок 2.98 – Закрытие инцидента

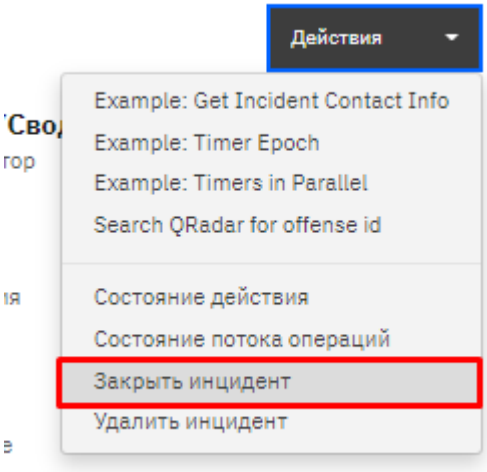


Рисунок 2.99 - Закрытие инцидента

Установка статуса решения на «Resolved/Решен» (рисунок 2.100).

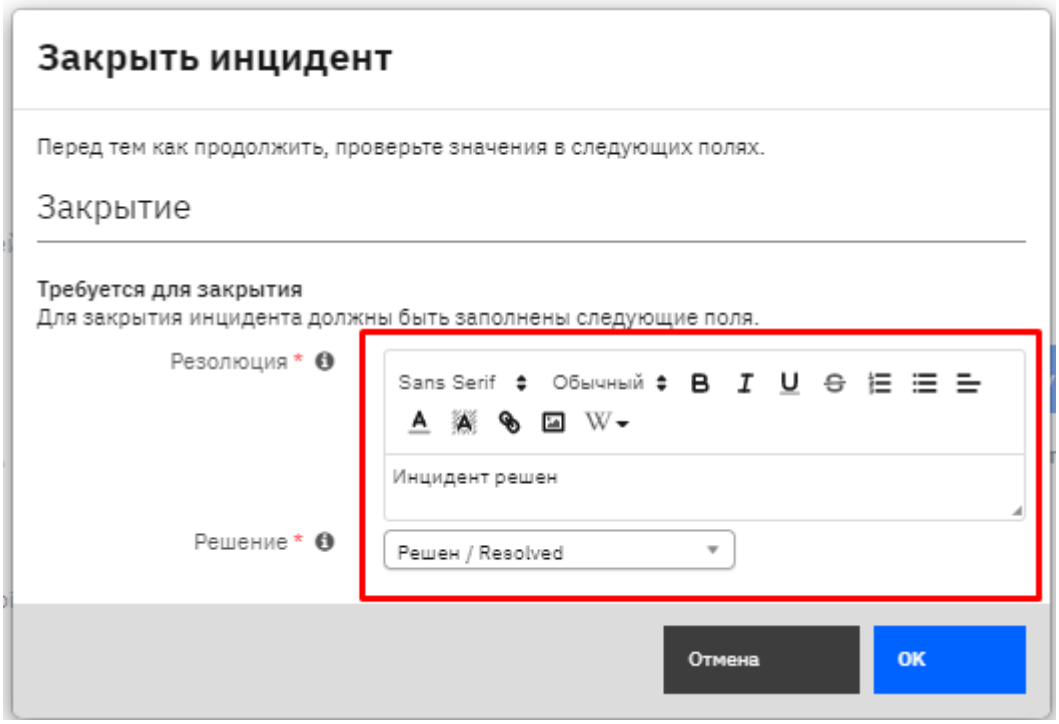


Рисунок 2.100 – Установка статуса «Решено»

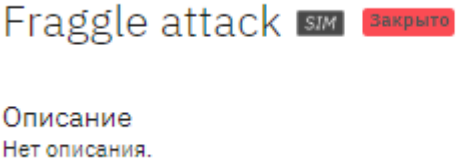


Рисунок 101 – Закрытый инцидент

Временная шкала расследования инцидента (рисунок 2.102).

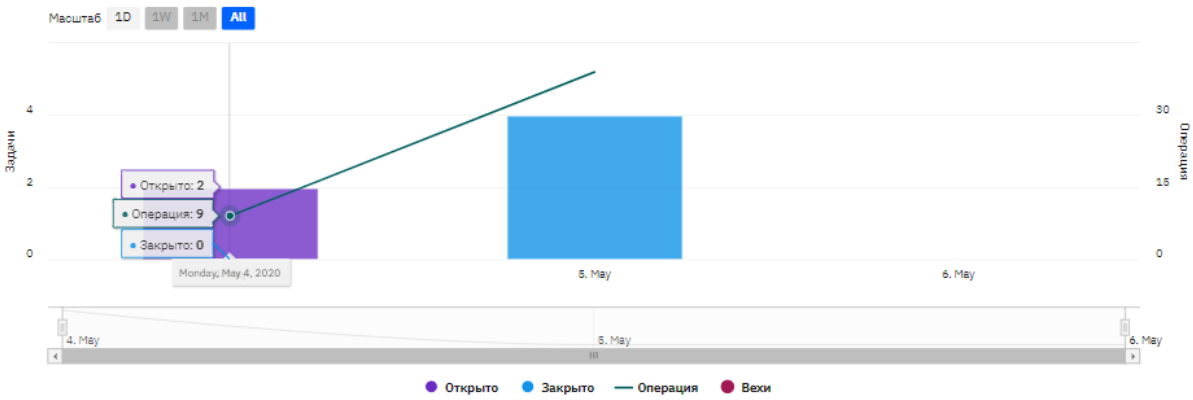


Рисунок 2.102 – Временная шкала

Статистика закрытых задач владельца инцидента (рисунок 2.103).

Рисунок 2.103 - Статистика закрытых задач владельца инцидента

Просмотр ленты новостей, отображающей всю последовательность действий по данному инциденту (рисунок 2.104).

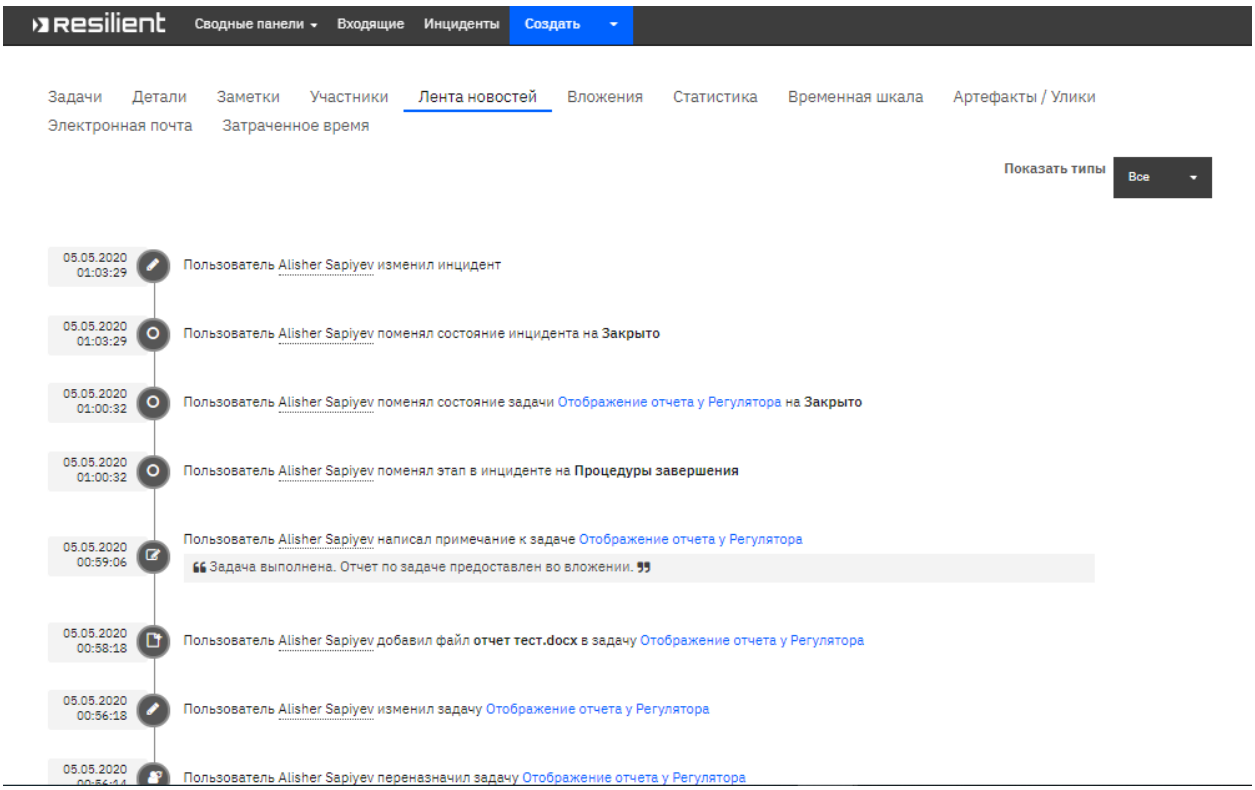


Рисунок 2.104 – Лента событий

2.5 Вывод по главе «Практическая часть»

В данной главе были проведены такие работы как: установка и начальная настройка гипервизора ESXi, установка и настройка QRadar, добавление источника событий в QRadar, определение новых источников событий, расследование инцидента с помощью модуля Resilient.

Для размещение QRadar SIEM необходим сервер производительный физический сервер с установленным на него гипервизором ESXi.Установка ESXi не занимает много времени и трудозатрат, далее производится установка QRadar на данный сервер. При установке QRadar необходимо заранее продумать сколько ресурсов потребуется нашей системе. В данном случае использовалось 2 ядра процессора, 8 ГБ оперативной памяти и 250 ГБ дискового пространства. После установки QRadar, на SEIM систему было добавлено несколько источников на базе CENT OS и Windows 10. Также были разработаны регулярные выражения для определения неизвестных для SIEM системы источников. После разработки формул было получено событие для расследования инцидента в модуле Resilient. В ходе расследования были назначены ответственные лица, установлены сроки, проанализированы этапы, получены и собраны в отчет результаты расследования.

3 Безопасность жизнедеятельности

3.1 Анализ потенциально опасных и вредных факторов

Анализ потенциально опасных и вредных факторов в офисе воздействующих на персонал

Рабочее место - это среда, в которой большинство сотрудников проводят значительную часть своего времени. Оно может оказывать как положительное, так и отрицательное влияние на здоровье персонала. Рабочее место имеет важное значение для здоровья из-за множества потенциальных опасностей, которые существуют в различных рабочих условиях. Эти опасности могут относиться к большому спектру физических, химических и биологических аспектов. Обеспечение и поддержка оптимальных и хороших условий для деятельности человека и отдыха способствует его повышенной эффективности и продуктивности [1].

Компания располагается на первом этаже многоэтажного здания и представляет собой офис состоящий из кабинетов для каждого отдела. Каждый отдел находится в помещении размером от 20 до 25 квадратных метров. Расстояние между рабочими местами сотрудников отдела составляет от 2 до 3 метров. У каждого сотрудника имеется рабочий стол, ноутбук, мышь и монитор. План офиса приведен на рисунке 3.1

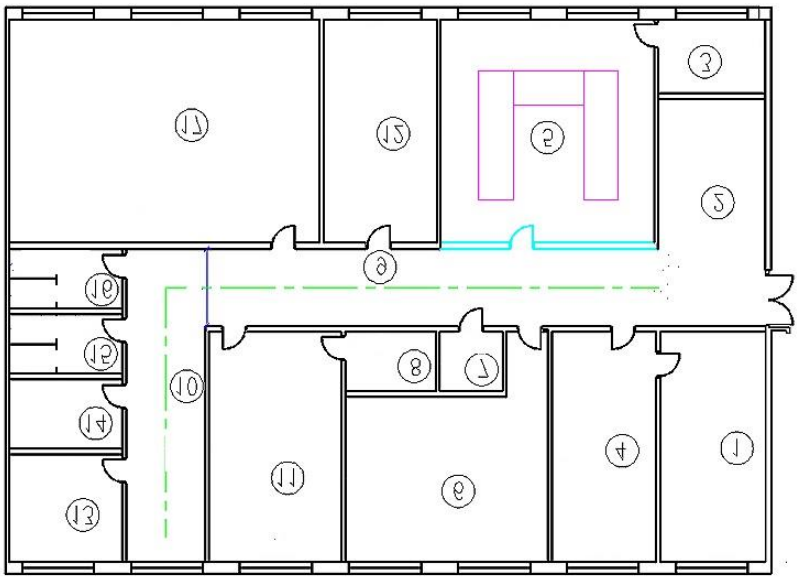


Рисунок 3.1 – Схема здания

В компании электромагнитное излучение от персональных компьютеров оказывает негативное влияние на здоровье сотрудников. В среднем работа на персональном компьютере составляет от пяти до семи часов. В связи с повышенной работой за компьютером у сотрудников наблюдаются расстройства центральной нервной системы, увеличивается риск болезней сердечно-сосудистой системы и болезней верхних дыхательных путей, а также присутствуют болезни опорно-двигательного аппарата [2].

В данный момент в компании все больше и больше процессов автоматизируется, и вся основная работа происходит в офисе. В связи с этим время работы в сидячей позе у сотрудников увеличилось, что негативно влияет на весь организм. В основном вред на организм повышается при неправильном положении тела при сидячей работе. В первую очередь проявляются заболевания позвоночника, которое определяется изменениями в положении позвоночных дисков и хрящах.

В связи с этим предлагается ввести перерывы по 10-15 минут для снятия напряжения глаз от ноутбука и физическую разминку каждый час. Также сотрудники не соблюдают безопасное расстояние до монитора, которое должно быть не менее 50 сантиметров, а оптимально 60-70 сантиметров. В связи с этим предполагается использование жидкокристаллических мониторов вместо мониторов с электроннолучевой трубкой и расположить мониторы в углах кабинета для увеличения площади поглощения излучения стенами, что снизит электромагнитное излучение на человека.

`Предельно-допустимые нормы напряженности и плотности электрического поля приведены в таблице 3.1 [3].

Таблица 3.1 - Предельно-допустимые нормы напряженности и плотности электрического поля

Напряженность электрического поля	
Диапазон частот 5 Гц – 2 кГц, Е1	25 В/м
Диапазон частот 2 кГц – 400 кГц, Е2	2,5 В/м
Плотность магнитного потока	
Диапазон частот 5 Гц — 2 кГц, В1	250 нТл
Диапазон частот 2 кГц — 400 кГц, В2	25 нТл

При проектировании рабочей области пользователей ПК необходимо учитывать и контролировать вышеперечисленные пункты, так как в определенных условиях они могут отрицательно повлиять на здоровье сотрудника и снизить эффективность его работы.

В помещениях оборудованных вычислительной техникой должен соблюдаться определенный микроклимат. Микроклимат зависит от таких аспектов как: запыленность, влажность, температура воздуха и т.д. Помещения с вычислительной техникой нуждаются в соблюдении определенных требований вышеперечисленных значений.

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. Она может влиять на количество ошибок, допускаемых сотрудником, уменьшать скорость его реагирования, а также плохо влияет на психологическое состояние работника [14].

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

Уровень излучения в помещениях с вычислительной техникой зависит от влажности воздуха, чем выше влажность, тем меньше воздействие электромагнитного поля на человека. Поэтому уровень влажности является важной характеристикой для соблюдения оптимального микроклимата. Относительная влажность должна быть в средних значениях от 40% до 60%.

Также важный фактор в офисном помещении с компьютером это – пыль. Наш организм не приспособлен к условиям повышенной запыленности. Из-за повышенного уровня излучения от компьютеров пыль не оседает на поверхностях и висит в воздухе, поэтому такой пыли легче попасть в организм человека. Чтобы это предотвратить необходимо хорошо проветриваемое помещение и проводить влажную уборку несколько раз в день, что сократит уровень пыли в помещении.

Свет является одним и важнейших факторов для комфортной работы сотрудника компании. Так как сотрудник проводит большое количество времени на работе, непродуманное освещение отрицательно сказывается на его работоспособности. Неправильно выставленный свет усиливает усталость, снижает трудоспособность персонала. Главная задача освещения - это выстроить оптимальные комфортные условия для глаз и зрительное восприятие в рабочей зоне. Офис состоит из офисных помещений общего назначения, конференц-зала, архива, кладовой и кабинета руководителя. Нормы по освещенности данных помещений приведены в таблице 3.2.

Таблица 3.2 - Нормы по освещенности помещений

Тип помещения	Освещенность (лк) по Международным нормам
Офис общего пространства	500
Конференц-зал	300
Архив	200
Склад	200
Кабинет руководителя	400

3.2 Расчет пожарной безопасности

Пожар – это неконтролируемое горение, которое может нанести большой материальный ущерб, а в некоторых случаях и унести жизнь людей. В связи с этим одной из главных обязанностей каждого члена общества является защита от пожаров. Пожарная безопасность обеспечивается мерами профилактики и мерами активной защиты.

Пожарная безопасность объекта в первую очередь направленна на предотвращение опасности причинения вреда сотрудникам здания в результате возгораний.

По техническому регламенту «Общие требования к пожарной безопасности» утвержденному от 11 апреля 2014 года здание по взрывопожарной и пожарной опасности, определяющейся по наличию в

помещениях горючих веществ и материалов, их количества и свойств, а также по внутренним технологическим процессам, относится к категории Д (пониженная пожароопасность) [4].

К основным причинам пожара в офисных помещениях относятся:

а) невыполнение правил пожарной безопасности;

б) короткие замыкания;

в) использование неисправного электрооборудования.

Согласно требованиям к системам обеспечения пожарной безопасности объектов расстояние между возможным очагом возгорания и местом расположения огнетушителей не должно превышать 70 метров.

Также на каждом этаже здания должно быть не менее 2 ручных огнетушителей. Так как помещения оборудованы дорогим электронным оборудованием, то допускается оснащать кабинеты хладоновыми или углекислотными огнетушителями. Огнетушители имеют свой порядковый номер, а также паспорт установленной формы [14].

Совокупная площадь помещения составляет 45м2. В качестве огнетушащего вещества применяется комбинированный углекислотно-хладоновый состав. Расчетная масса комбинированного углекислотно-хладонового состава md, для объемного пожаротушения определяется по формуле:

$$m_d = kg_n v, \tag{4.1}$$

где k = l,2 – коэффициент компенсации не учитываемых потерь углекислотно-хладонового состава, gn = 0,04 – нормативная массовая концентрация углекислотно-хладонового состава, V – объем помещения, который можно вычислить по следующей формуле:

$$V = X \times Y \times Z. \tag{4.2}$$

где X = 9 м - длина помещения, Y = 5 м - ширина помещения, Z = 4м - высота помещения.

Тогда:

$$V = 9 \times 5 \times 4 = 96 \text{ м3}$$

Следовательно,:

$$m_d = 1{,}2 \times 0{,}04 \times 96 \approx 4.6 \text{ кг}$$

Расчетное число баллонов x определяется из расчета вместимости в 20-литровый баллон 12 кг углекислотно - хладонового состава.

Внутренний диаметр магистрального трубопровода di (мм), определяется по формуле:

$$d_i = 12 \times \sqrt{2} \approx 17 \text{ мм.}$$

Эквивалентная длина магистрального трубопровода l2 определяется по формуле:

$$l_2 = k_1 \times l. \quad (4.3)$$

где k1=1,2 - коэффициент увеличения длины трубопровода для компенсации не учитывающих местных потерь, l=3м - длина трубопровода по проекту тогда:

$$l_2 = 1{,}2 \times 3 = 3{,}6 \text{ м,}$$

Расход углекислотно-хладонового состава Q, в зависимости от эквивалентной длины и диаметра трубопровода равна 1,4 кг/с.

Расчетное время подачи углекислотно-хладонового состава t, определяется по формуле:

$$t = \frac{m_d}{60Q}. \quad (4.4)$$

Тогда:

$$t = \frac{4{,}6}{96 \times 1{,}4} = 0{,}034 \text{ мин.}$$

Масса основного запаса углекислотно-хладонового состава m определяется по формуле:

$$m = 1{,}1 \times m_d \times (1 + \frac{k_2}{k_1}). \quad (4.5)$$

где $k2 = 0{,}2$ – коэффициент учитывающий остаток углекислотно-хладонового состава в баллонах и трубопроводах. Тогда:

$$m = 1{,}1 \times 4.6 \times \left(1 + \frac{0{,}2}{1{,}2}\right) = 5{,}903 \text{ кг.}$$

Получив данные результаты, мы можем сделать вывод, что для полноценной работы автоматической системы пожаротушения нам нужен один баллон углекисло-хладонового огнетушителя с вместимостью 20 литров и массой смеси в 4,6 кг. Для системы автоматического пожаротушения предусмотрены устройства автоматического пуска. Такой огнетушитель

ставится непосредственно в кабинете офицера информационной безопасности (Департамент информационной безопасности), также на этаже находятся 2 общих ручных огнетушителя [4].

Расчет системы кондиционирования кабинета специалиста по информационной безопасности.

В таблице описаны параметры микроклимата с учетом года для сотрудников офиса.

Небольшое выделение тепла аппаратуры не оказывается серьезного влияния на микроклимат рабочего помещения. Поэтому оборудование и аппаратура не расцениваются как источник тепла.

Состояние микроклимата помещения соответствует нормам для рабочего персонала [4].

Таблица 3.3 − Нормы температуры, относительная влажность и скорость движения воздуха в помещениях [5]

Время года	Категория работ	Температура воздуха, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Зимнее	Легкая - 1а	23-25	40-60	0,1
	Легкая – 1б	22-24	40-60	0,1
Летнее	Легкая - 1а	22-24	40-60	0,1
	Легкая – 1б	21-23	40-60	0,2

Для вентиляции офисного помещения используются каналы естественной вентиляции, прокладываемые при строительстве здания и открытые окна летом.

Каналы вентиляции используются для вентиляции помещения. Каналы прокладываются при строительстве здания. В теплое время года при достижении повышенных температур, для обеспечения качественной и комфортной работы сотрудников, используется кондиционер и открытые окна.

Далее произведен расчет системы кондиционирования в помещении. Кондиционирование позволит обеспечит соответствие климата нормам в рабочем помещении.

Определяем по формуле $L_{\text{пр}}, \frac{\text{м}^3}{\text{ч}}$: количество приточного воздуха

$$L_{\text{пр}} = \frac{Q_{\text{изб}}}{\text{с}p_{\text{пв}}(t_{\text{выт}} - t_{\text{пв}})}. \quad (4.6)$$

где $Q_{\text{изб}}$ - избыточное выделение теплоты, кДЖ/ч; c - удельная теплоемкость воздуха при постоянном давлении, равная $c = 1$кДж/кг°С; $p_{\text{пв}}$ - плотность поступающего в помещение воздуха, равная 1,2 кг/м3; $t_{\text{выт}}$ -

температура удаляемого из помещения воздуха за пределы рабочей или обслуживаемой зоны,℃; $t_{пв}$ - температура приточного воздуха,℃.

Определяем по формуле температуру удаляемого из помещения воздуха $t_{выт}$ ℃, о:

$$t_{выт} = t_{рз} + \Delta t(h_{вп} - z). \quad (4.7)$$

где: $t_{рз}$ - температура в рабочей зоне, которая не должна превышать допустимую по нормам ($t_{рз} \leq t_{доп}$),℃; $h_{вп}$ - расстояние от пола до центра вытяжных проемов (кондиционера),м.

Поскольку расчет производится для теплого периода года, то примем $t_{рз} = 22$℃. Внутренняя часть кондиционера расположена на высоте $h_{вп} = 2{,}8$м.

$$t_{выт} = 22 + 1{,}2(2{,}8 - 3) = 21{,}76\ ℃$$

Температура приточного воздуха $t_{пр}$ при наличии избытка явной теплоты должна быть на $5-7$ ℃ ниже температуры воздуха в рабочей зоне:

$$t_{пр} = 22 - 7 = 15\ ℃$$

Величину избыточного выделения явной теплоты $Q_{изб}$ находят на основании баланса теплоты в помещении по формуле:

$$Q_{изб} = \sum Q - \sum Q_{ух}. \quad (4.8)$$

где $\sum Q$ - суммарное количество поступающей в помещение явной теплоты; $\sum Q_{ух}$ - суммарное количество уходящей из помещения теплоты (за счет теплопотерь ограждениями, нагрева поступающего в помещение воздуха).

Световое освещение, люди и солнечная радиация относятся к основным источникам превышения норм температуры. В этом случае тепловыделением от аппаратуры мы пренебрегаем, так как оно очень мало и аппаратура оснащается воздушными кулерами охлаждения. В связи с этим учитываем тепло искусственного освещения, от людей и тепло поступающее через окна от солнечной радиации [3].

Тепловыделения от искусственного освещения Q_2, рассчитывают, предполагая, что практически вся затрачиваемая энергия, в конечном счете, преобразуется в тепло, по формуле:

$$Q_2 = 1000N \quad (4.9)$$

где N – расходуемая мощность светильников, кВТ.

$$Q_2 = 1000 \times 0{,}28 \times 4 = 1120 \text{ кВТ}$$

Тепловыделения от людей Q_3, определяют по формуле:

$$Q_3 = nq_ч. \quad (4.10)$$

где n - число работающих; $q_ч$ - количество тепла, выделяемое одним человеком, представлено в таблице 4.2.

Таблица 4.2 – Количество тепла, выделяемое одним человеком в зависимости от категории работ и температуры окружающей среды

Категория работ	Количество тепла, Вт (мужч.) при температуре воздуха в помещении, °С			
	Полное		Явное	
	при 10°С	При 20°С	при 10°С	При 20°С
Легкая	180Вт	145Вт	150Вт	100Вт

$$Q_3 = 1 \times 145 = 145\text{Вт}$$

Количество тепла, поступающего в помещение от солнечной радиации $Q_{\text{солн.рад.}}$, определяют по формуле:

$$Q_{\text{солн.рад.}} = F_{\text{ост}} q_{\text{ост}} A_{\text{ост}}, \quad (4.11)$$

для покрытий:

$$Q_{\text{п.рад.}} = F_n q_n k_n. \quad (4.12)$$

Где $F_{\text{ост}}$ и F_n - площадь поверхности и покрытия, м2; $q_{\text{ост}}$ и q_n - теплопоступления через 1м2 поверхности остекления и поверхности покрытия, при коэффициенте теплопередачи, равном 1Вт/м2°С; $A_{\text{ост}}$ - коэффициент остекления; k_n- коэффициент теплопередачи покрытия, 1Вт/м2°С.

Значение $q_{\text{ост}}$ в зависимости от географической ориентации поверхности и характеристики окон или фонарей принимается в пределах $70-210$, а коэффициента $A_{\text{ост}}$ в зависимости от вида остекления и его солнцезащитных свойств - в пределах $0{,}25-1{,}25$, средние значения теплопоступления от солнечной радиации через покрытие в зависимости от географической широты и вида покрытия принимают в пределах 6 - 24.

$$F_{\text{ост}} = 1{,}5 \times 1{,}2 \times 2 = 3{,}6 \text{ м2}$$

Окна рабочего помещения направлены на север, поэтому примем значение $q_{\text{ост}}$ равным 140Вт/м2°С. Примем $A_{\text{ост}} = 0{,}35$.

$$Q_{\text{ост.рад.}} = 3{,}6 \times 140 \times 0{,}35 = 176{,}4\text{Вт}$$

Среднее значение теплопоступления для покрытия с учетом географической широты примем равным $Q_{\text{п.рад.}} = 18\text{Вт}$.

Потери тепла из помещения Q_{yx} кВТ, через стены двери, окна оценивают ориентировочно по формуле:

$$Q_{yx} = \frac{\lambda S(t_{\text{выт}} - t_{\text{пр}})}{\delta}. \quad (4.13)$$

Где λ - теплопроводность стен, Вт/м°С; S - площадь, м2; δ - толщина стен,м.

Стены рабочего помещения изготовлены из тяжелого бетона М600, теплопроводность которого равна 12Вт/м°С. Толщина стен δ = 0,5м.

$$Q_{yx} = \frac{1{,}2 \times 24(21{,}76 - 15)}{0{,}5} = 389{,}376 \text{ Вт}$$

Вычислим суммарное количество поступающей в помещение явной теплоты:

$$\sum Q = Q_2 + Q_3 + Q_{\text{ост.рад.}} + Q_{\text{п.рад}}. \quad (4.14)$$

$$\sum Q = 1120 + 145 + 176{,}4 + 18 = 1120{,}3 \text{ кВТ}$$

Так как расчет производится для летнего периода величина избыточного выделения явной теплоты равна:

$$Q_{\text{изб}} = 1120{,}3\text{кВт}$$

Вычислим количество приточного воздуха:

$$L_{\text{пр}} = \frac{1120{,}3}{1 \times 1{,}2(21{,}76 - 15)} = 138{,}1\text{м3/ч}$$

Чтобы обеспечивать расход воздуха, $L = 138{,}1$ м3/ч, можно использовать 1 кондиционер фирмы Samsung AR5500 (рисунок 3.2) с функцией ускоренного охлаждения:

Мощность охлаждения – 6,8 кВт;
Мощность обогрева – 8 кВт;
Максимальная длина/высота трубопровода – 20/12м.;
Уровень шума внутреннего блока - 44/28 дБ:;
Уровень шума наружного блока – 54 Дб.

Что является сверх достаточным для обеспечения комфортного микроклимата.

Рисунок 3.2 - Кондиционер фирмы Samsung AR5500

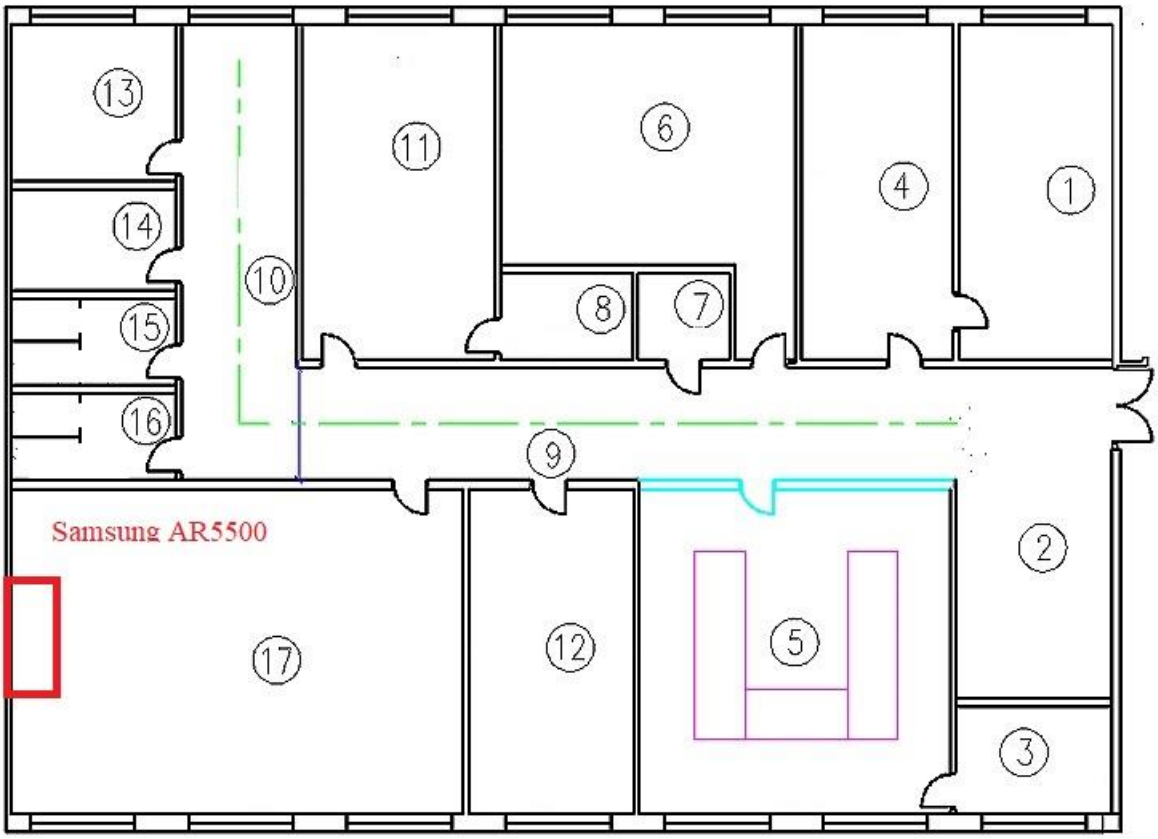


Рисунок 3.3 – Размещение кондиционера в офисе

3.3 Вывод

В рамках данной дипломной работы был совершен анализ потенциально опасных и вредных факторов в офисе воздействующих на персонал, произведены расчеты по пожарной безопасности, а также по кондиционированию кабинета специалиста информационной безопасности. Проанализированы такие факторы как электромагнитное излучение от персональных компьютеров, микроклимат, влажность и запыленность. В ходе анализа были определены меры по минимизации влияния опасных факторов. По данным полученным из расчетов пожаробезопасности было определено, что для работы автоматической системы пожаротушения необходим один баллон огнетушителя вместимостью 20 литров и массой смеси 4,6 кг, а также 2 ручных огнетушителя. Для обеспечения системы кондиционирования было определено использовать один кондиционер марки Samsung AR5500, что обеспечить.

4 Анализ рисков информационной безопасности

Ежедневное использование информационных систем приводит к образованию рисков и возникновению угроз и уязвимостей. Оценка рисков необходима для оценки эффективности использования информационных систем, определению контрмер безопасности и экономически правильному обоснованию используемых систем защиты. Оценка рисков является одной из самых важных и первостепенных задач при внедрении любой информационной системы.

Риски требуют периодической переоценки и постоянного контроля. Качественная первичная оценка позволит заложить надежный фундамент для дальнейшей работы по оценке рисков. Оценка рисков в довольно больших размерах помогает снизить убытки компании, путем предотвращения возможных атак на информационную инфраструктуру компании.

Потенциально возможные события и разные действия, наносящие ущерб или вред IT-инфраструктуре являются угрозами компьютерной безопасности. Понятие риска — это потенциальная возможность нарушения информационной безопасности путем использования уязвимости или определенной угрозы к активам компании для нанесения ущерба.

Оценка угроз и рисков, включая все возможные методы и способы нарушения основных принципов информационной безопасности: целостности, конфиденциальности и доступности, является основной целью анализа и оценки рисков, а также определение мер защиты для снижения риска и повышению уровня защиты систем. Основные факторы, используемые для оценки рисков: уровни угроз и уязвимостей, влияние используемых мер защиты, стоимость активов и другое [15].

Целью компании является обеспечение достижения контроля по допустимому уровню рисков, на что и направлен процесс определения уязвимостей, которые потенциально могут повлиять на организацию. При определении стратегии и курса компании на всех уровнях и каждом подразделении происходит процесс управления рисками, затрагивающий всю организацию.

Обеспечение физической безопасности, безопасности информационной системы, разграничение уровня доступ к сетевым ресурсам, разработка нормативных документов, мониторинг и контроль состояния информационных систем – эти перечисленные процессы относятся к мерам по управлению рисками информационных систем. Изначально должны быть определены объекты защиты путем инвентаризации информационных активов компании и оценивается их важность для процессов организации. Далее определяются возможные уязвимости систем, их критичность и вероятность их реализации.

4.1 Идентификация угроз и уязвимостей

Существует множество угроз, которым может подвергнуться информационная система Компании и для возникновения любой угрозы

необходимо существования уязвимости. Ниже перечислены защищаемые активы:

а) SIEM система IBM QRadar;

б) межсетевой экран, подключенный к SIEM системе;

в) event collector (устройство для сбора событий) SIEM;

г) файловый сервер;

д) персональные данные.

Ниже описаны основные угрозы благодаря которым, могут возникнуть угязвимости информационной безопасности:

1. Угроза – Незаконное подключение. Отсутствие корреляции и контроля данных от сетевых устройств, посредством чего, злоумышленники могут подключиться к ЛВС Компании.

2. Угроза – Искажение данных. Отсутствие контроля входных и выходных данных, которые пользователи отправляют в внешнюю сеть либо же получают из вне.

3. Угроза – Несанкционированное удаленное подключение. Отсутствие проверка авторизации пользователей при удаленном подключении, через ВПН, который не контролирует, какие учетные записи являются внутренними, а какие нет.

4. Угроз – Нарушение Политики ИБ. Обход пользователями политик брандмауэра для доступа на незащищенные ресурсы.

5. Угроза – DDos атаки. Атака на ресурс с целью выведения его из строя отправляя большого количества запросов

6. Угроза – Незаконное использование серверных ресурсов работниками Компании. Незаконное присвоение сетевых и серверных ИТ-ресурсов для собственного использования.

7. Угроза – Несанкционированные попытки вход в учетную запись. Перебор пароля пользователя с помощью брутфорса или же других способ с помощью которых можно узнать пароль пользователя.

8. Угроза – Внедрение SQL-инъекций. Отсутствие проверки логов с БД, что может привести к атаке по типу SQL-инъекций.

9. Угроза – Некорректная работа системы мониторинга. Мониторинг за подозрительными событиями ИБ, которые происходят внутри и вне сети Компании. Для постоянного мониторинга за угрозами, которые могут возникнуть.

10. Уязвимая настройка сетевых соединений – Настройка сетевых соединений без дополнительной защиты шифрованием, может быть использовано злоумышленниками для подключения к системам.

4.2 Анализ рисков качественным методом

Существует два основных метода анализа рисков:

– Качественный анализ рисков;

– Количественный анализ рисков.

Основное различие между этими двумя методами анализа риска состоит в том, что качественный анализ риска использует относительную или описательную шкалу для измерения вероятности возникновения, тогда как количественный анализ риска использует числовую шкалу.

Качественный анализ рисков позволяет определить, что повлияло к появлению риска, выявить, какова степень угрозы ее возникновения. Таким образом, можно установить возможные области риска, и провести работу по выявлению возможных прибылей и убытков возникновения рисков [15].

Используя рейтинговые шкалы, можно проанализировать вероятность каждой уязвимости и угрозы и их влияние, чтобы определить, на каком уровне риска оно находится. Это даст информацию, необходимую для определения приоритетности списка рисков проекта.

Ниже приведены таблицы, с помощью которых можно оценить приоритетность риска (таблица 4.1).

Таблица 4.1. Максимальные уровни риска

Количественная оценка	Качественная оценка
1	Маловероятно
2	Редкое
3	Возможное
4	Весьма вероятно
5	Неизбежно

Таблица 4.2. Остаточный уровень риска

Количественная оценка	Качественная оценка
1-3	Низкий
4	Средний
5	Высокий

Таблица 4.3 – Расчет рисков

№	Угроза	Уязвимость	Максимальный уровень риска	Меры по обработке риска	Остаточный уровень риска	Дата	Ответственный
Актив 1: SIEM система IBM QRadar							
1 Незаконное подключение	Отсутствие корреляции и контроля данных от сетевых устройств	**4**	**Настройка правил корреляции SIEM системы**	**3**	**10.05.2020**	**Администратор SIEM**	
2 Искажение данных	Отсутствие контроля входных и выходных данных	**3**	**Настройка и использование модуля сетевой активности SIEM системы**	**2**	**12.05.2020**	**Системный администратор**	
3 Попытки удаленного подключения	Отсутствие проверки авторизации пользователей при удаленном подключении	**2**	**Установка дополнительной двухфакторной аутентификации пользователей с помощью SIEM системы**	**1**	**14.05.2020**	**Системный администратор**	
Актив 2: Межсетевой экран, подключенный к SIEM системе							
4 Нарушение Политики ИБ	Обход пользователями политик брандмауэра для доступа на незащищенные ресурсы.	**4**	**Проверка политик и правил межсетевого экрана с помощью SIEM системы**	**3**	**16.05.2020**	**Инженер**	

Продолжение таблицы 2

Актив 3: Event Collector SIEM						
5 DDos атака	Атака на ресурс с целью выведения его из строя отправляя большое количество запросов	**4**	**Ограничение количества принимаемых запросов с помощью SIEM системы**	**3**	**17.05.2020**	**Инженер**
6 Незаконное использование серверных ресурсов	Незаконное присвоение сетевых и серверных ИТ-ресурсов для собственного использования.	**2**	**Аудит использования серверных ресурсов и анализ журналов устройств с помощью SIEM системы**	**1**	**20.05.2020**	**Глава отдела ИБ**
Актив 4: Файловый сервер						
7 Попытки входа в учетную запись	Перебор пароля пользователя с помощью брутфорса или же других способов	**3**	**Установка сложных паролей пользователей на сервера**	**2**	**22.05.2020**	**Инженер**
8 Внедрение SQL-инъекций	Отсутствие проверки логов с БД, что может привести к атаке по типу SQL-инъекций	**5**	**Добавление Базы Данных как источник событий в SIEM**	**4**	**24.05.2020**	**Администратор SIEM**
9 Некорректная работа системы мониторинга	Мониторинг за подозрительными событиями ИБ, которые происходят внутри и вне сети Компании	**2**	**Установка дополнительного модуля UBA (User Behavior Analytics) на SIEM систему**	**1**	**26.05.2020**	**Администратор SIEM**

Продолжение таблицы 2

Актив 5: Персональные данные						
10 Уязвимая настройка сетевых соединений	Настройка сетевых соединений без дополнительной защиты шифрованием, может быть использовано злоумышленниками для подключения к системам.	**3**	**Аудит и мониторинг использования сетевых соединений с помощью SIEM системы**	**2**	**28.05.2020**	**Системный администратор**

Расчет рисков информационной безопасности – это один из ключевых этапов при исследовании и расчетов рисков. Наглядно показывает эффективно ли были приняты меры, на ту или иную угрозу и остаточный риск, а также сведения об уязвимостях, угроз и показатели максимального риска. Качественная оценка риска позволяет помочь определить, есть ли какие - либо типы конкретных или категории рисков, которые потребуют особого внимания или каких -либо событий риска, которые должны быть обработаны в ближайшее время.

При расчетах основные риски были определены для сервера SIEM системы и подключенных к нему источников данных, таких как файловый сервер, межсетевой экран и другие. К самым критичным уязвимостям относятся уязвимости связанные с базой данных и межсетевым экраном.

После определения угроз и уязвимостей были определены меры по снижению рисков, такие как: настройка правил корреляции SIEM системы, аудит и мониторинг использования сетевых соединений, добавление Базы Данных как источник событий в SIEM, установка дополнительного модуля UBA (User Behavior Analytics) на SIEM систему. До

принятия мер средний уровень риска составлял 3-4(средний - высокий), после принятия мер средний уровень риска снизился до 2-3 (низкий-средний).

4.3 Анализ рисков с инструментом CORAS

Для графического представления влияния угроз и уязвимостей на активы, а также степень влияния рисков и то какие защитные меры необходимо предпринять используется инструмбеет CORAS.

С помощью CORAS можно определить и выбрать нужные и необходимые меры по снижению уровня рисков. CORAS определяет эффективность принятых мер и вложенного бюджета на предотвращение рисков информационной безопасности. Программа CORAS распространяется бесплатно, что делает ее эффективным инструментом для детального анализа рисков информационной безопасности.

При проектировании первым этапом является определение активов (рисунок 4.1). На рисунке 1 представлены активы, для которых необходимо определить их уязвимости и к каким угрозам они могут привести.

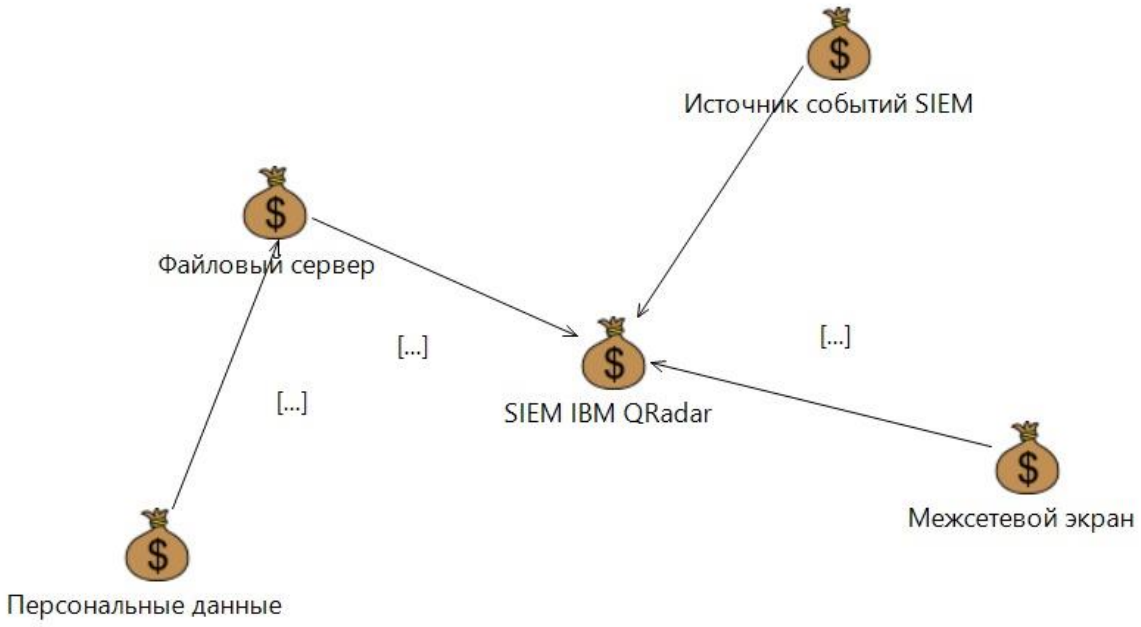


Рисунок 4.1 – Диаграмма активов

После того, как были определены основные активы, строю диаграмму модели угроз (рисунок 4.2). Данная диаграмма на рисунке 2 описывает существующие угрозы информационной безопасности, возможность их реализации и последствия. Модель угроз позволяет выявить существующие угрозы и разработать эффективные меры по защите информационной системы и активов компании. В данной диаграмме описаны следующие элементы: источники угроз, уязвимости, угрозы, понесшие от реализации угрозы ущерб активы.

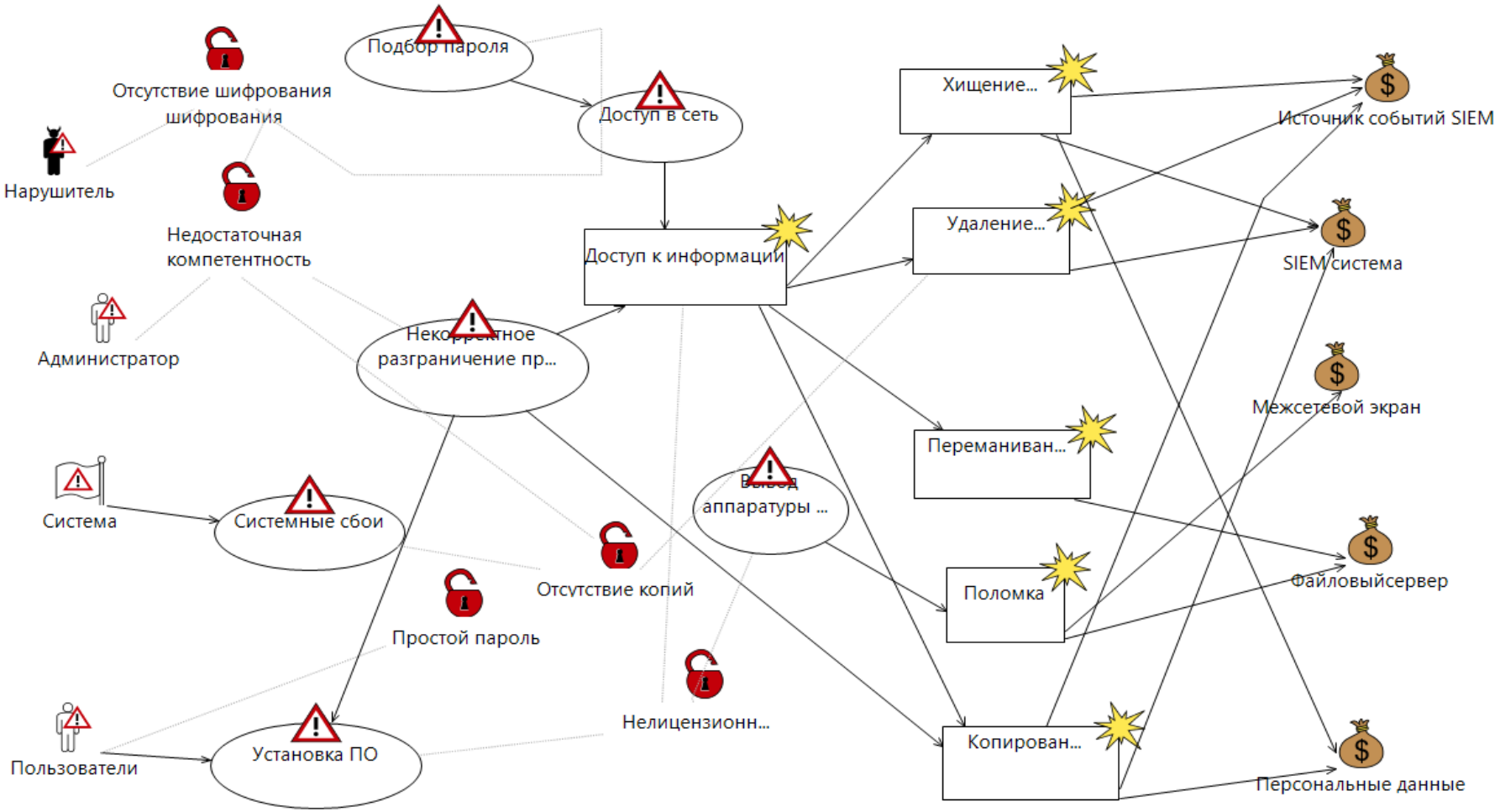


Рисунок 4.2 – Диаграмма модели угроз

После того, как были обнаружены уязвимости и к каким угрозам они могут привести, следующим шагом демонстрирую по средствам чего могут возникнуть те или иные уязвимости и к каким инцидентам могут привести. В данной диаграмме описываются те же угрозы, что и на диаграмме рисунок 4.2, но с учетом вероятности возникновения

инцидента, главное на что в этой диаграмме необходимо обратить внимание какие угрозы могут привести к инциденту (рисунок 4.3).

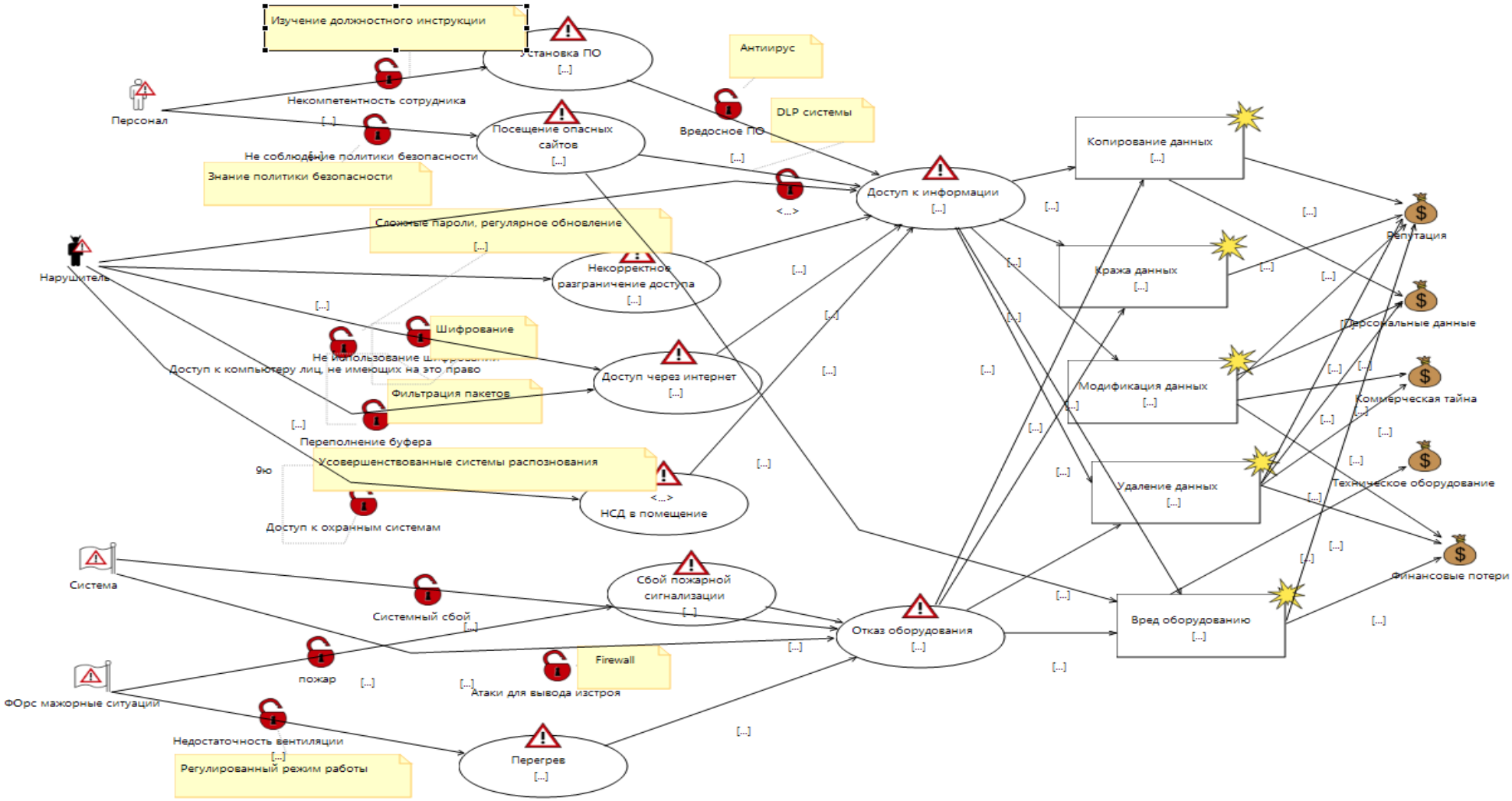


Рисунок 4.3 – Модель угроз с учетом вероятности возникновения инцидента

Теперь, когда возникли инциденты, имеет смысл расставить степень влияния рисков, которые возникли посредством инцидентов (рисунок 4.4). Данная диаграмма демонстрирует элементы, которые позволяют понять степень влияния риска на актив, такие как угрозы, которые возникают, а также посредством чего они переходят в инциденты и какую степень риска представляют

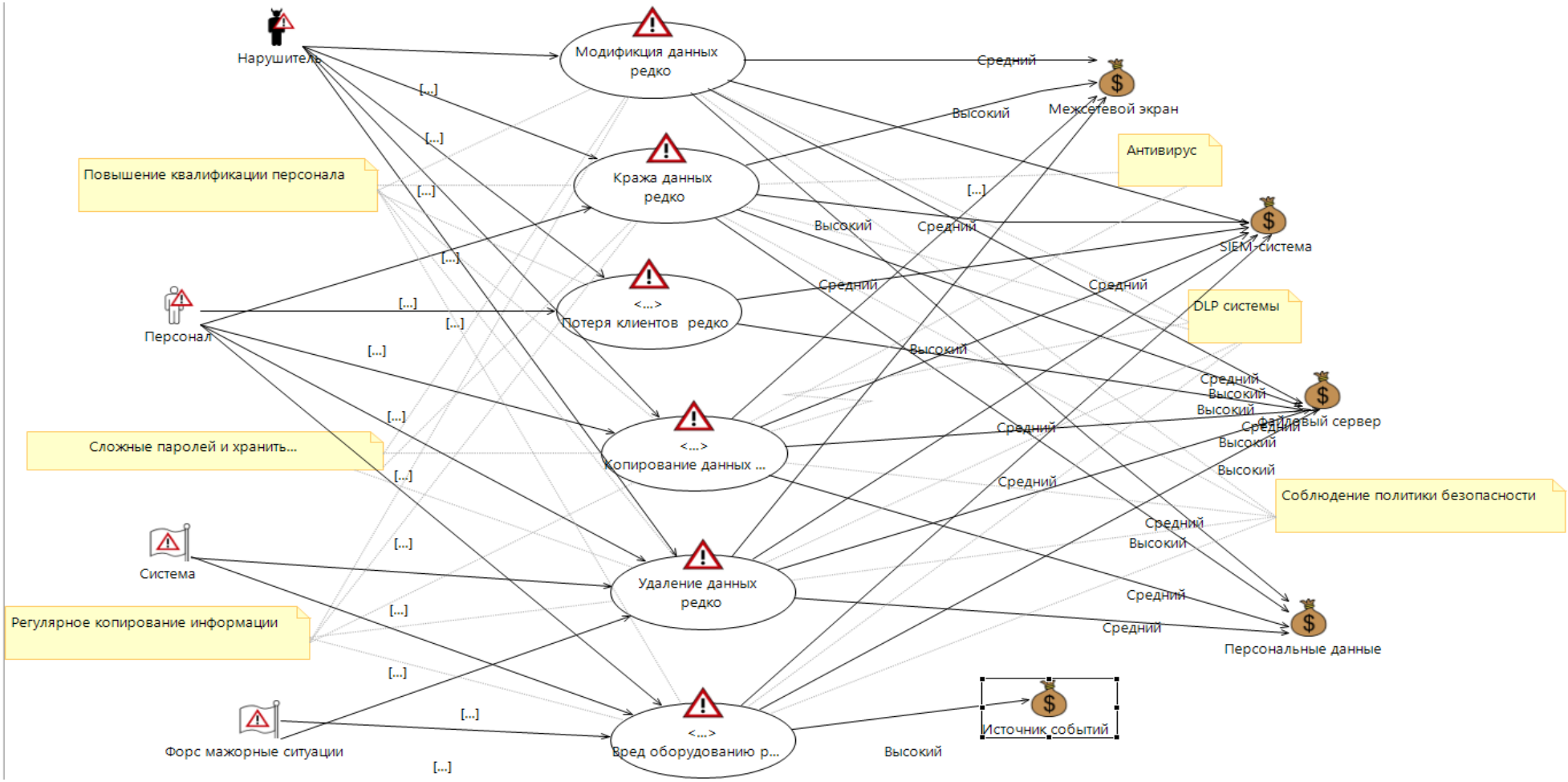


Рисунок 4.4 - Диаграмма последствий угроз и степень влияния рисков

Теперь расставляем защитные меры (рисунок 4.5), с помощью SIEM системы, которая использует в дипломном проекте. Следующая диаграмма описывает защитные меры, которые будут использованы для снижения степени риска. Основными элементами это диаграммы являются защитные расставленные для каждого инцидента.

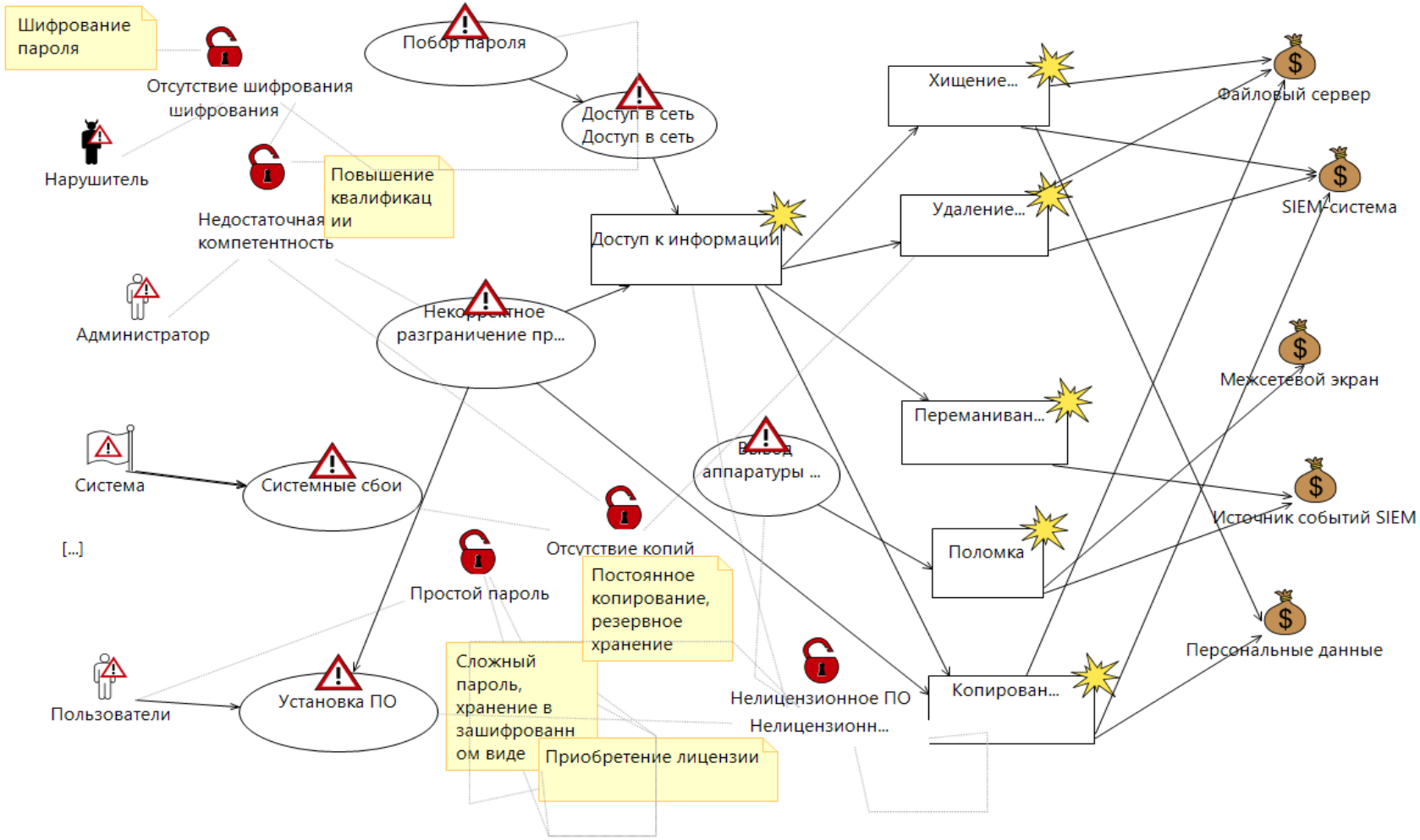


Рисунок 4.5 – Диаграмма расстановки защитных мер

Так как не все риски можно закрыть, существуют так называемые неприемлемые риски, которые возникают в любой информационной системе (рисунок 4.6). Необходимо знать эти риски и снижать их по мере возможности, далее на диаграмме показаны те риски, которые являются неприемлемыми имеющие высокую степень влияния и которые имеют высокий приоритет при расследовании и устранении.

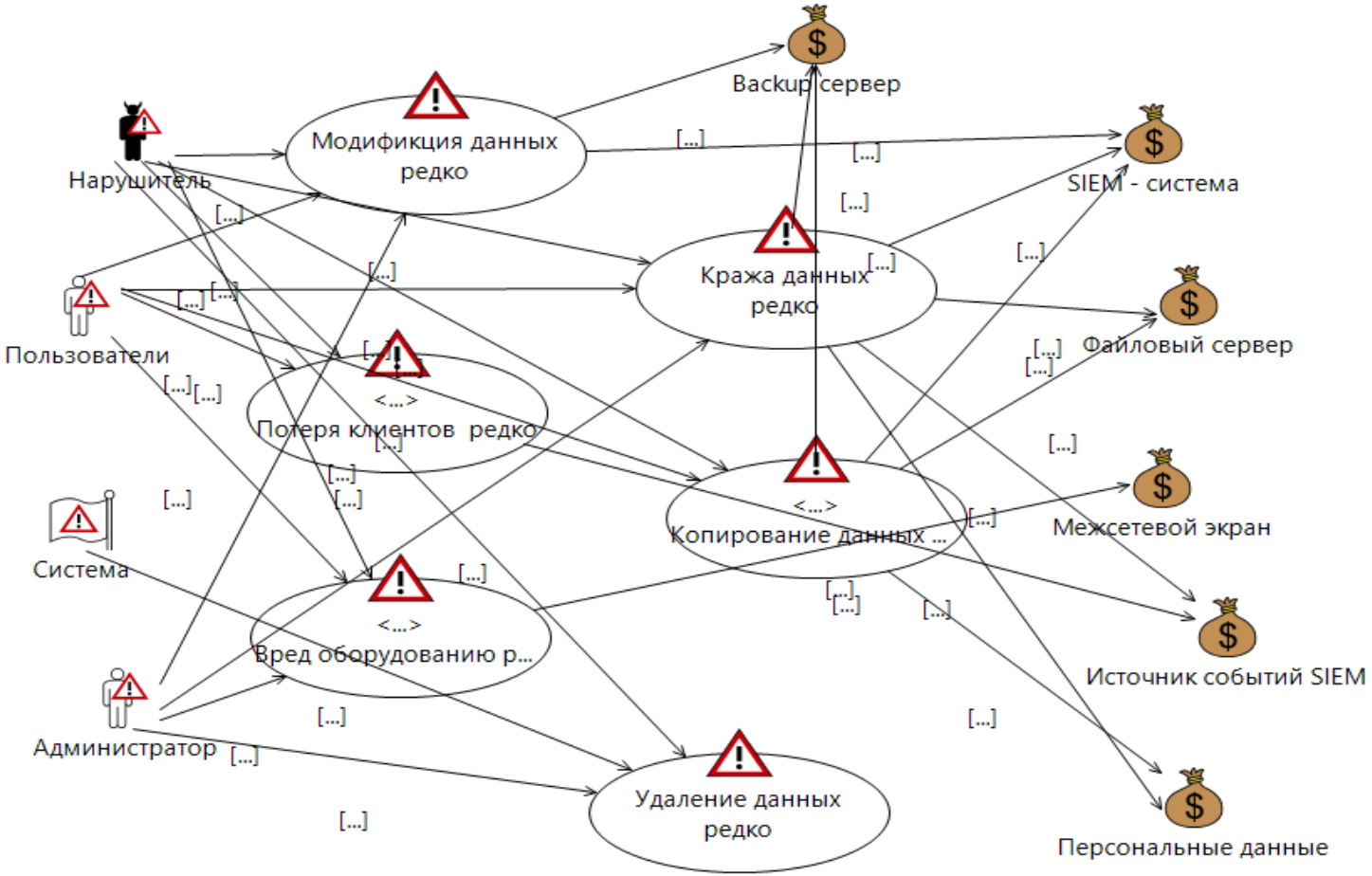


Рисунок 4.6 – Диаграмма неприемлемых рисков

4.4 Вывод по разделу «Анализ и оценка рисков»

В данном разделе произведен расчет рисков. Главной целью было необходимость определения активов, конкретных угроз и уязвимостей, выработка мер противодействия, определение сроков и исполнителей работ по внедрению мер противодействия и расчет остаточных рисков.

Качественная оценка риска позволяет помочь определить, есть ли какие -либо типы конкретных или категории рисков, которые потребуют особого внимания или каких -либо событий риска, которые должны быть обработаны в ближайшее время.

При расчетах основные риски были определены для сервера SIEM системы и подключенных к нему источников данных, таких как файловый сервер, межсетевой экран и другие. К самым критичным уязвимостям относятся уязвимости связанные с базой данных и межсетевым экраном.

После определения угроз и уязвимостей были определены меры по снижению рисков, такие как: настройка правил корреляции SIEM системы, аудит и мониторинг использования сетевых соединений, добавление Базы Данных как источник событий в SIEM, установка дополнительного модуля UBA (User Behavior Analytics) на SIEM систему. До принятия мер средний уровень риска составлял 3-4(средний - высокий), после принятия мер средний уровень риска снизился до 2-3 (низкий-средний).

Использование CORAS позволяет наглядно увидеть все параметры оценки рисков с помощью построенных диаграмм.

Самым главным аспектом проведения качественного анализа рисков было определение рейтинговых шкал. Но после проведения оценки данных параметров, их можно использовать для дальнейших исследований рисков компании.

Заключение

В ходе выполнения данной дипломной работы проведена интеграция системы на сервер. Также было рассмотрено расследование популярного в настоящее время инцидента с применением SIEM системы IBM QRadar. Был определен ход расследования, назначены исполнители, определены сроки и приняты меры в отношении инцидента. Помимо расследования инцидента была продемонстрирована настройка системы, добавлены источники событий и созданы регулярные выражения для неизвестных источников. Были выполнены поставленные цели и задачи. Кроме того, были выполнены расчеты рисков и исследованы оптимальные условия труда в разделе безопасности жизнедеятельности.

Список литературы

1 IBM Knowledge Center: IBM QRadar SIEM documentation // ibm.com: Начальная конфигурация. URL: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_qradar_pdfs.html (дата обращения: 01.02.2020).

2 IBM Knowledge Center: IBM QRadar SIEM documentation // ibm.com: Архитектура и внедрение. URL: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_siem_deployment.pdf?view=kc (дата обращения: 02.02.2020).

3 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).

4 IBM Knowledge Center: IBM QRadar SIEM documentation // ibm.com: Сервер высокой доступности. URL: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_ha_guide.pdf?view=kc (дата обращения: 01.04.2020).

5 IBM Knowledge Center: IBM QRadar SIEM documentation // ibm.com: Настройка DSM. URL: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/com.ibm.dsm.doc/b_dsm_guide.pdf?view=kc&origURL=SS42VS_DSM/b_dsm_guide.pdf (дата обращения: 06.04.2020).

6 IBM Knowledge Center: IBM QRadar SIEM documentation // ibm.com: Инструкция по WinCollect. URL: https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/com.ibm.wincollect.doc/b_wincollect.pdf?view=kc&origURL=SS42VS_7.3.2/com.ibm.wincollect.doc/b_wincollect.pdf (дата обращения: 07.04.2020).

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

8 IBM Knowledge Center: IBM QRadar SIEM documentation // ibm.com: Инструкция пользователя. URL: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_users_guide.pdf?view=kc (дата обращения: 23.03.2020).

9 IBM Knowledge Center: IBM QRadar SIEM documentation // ibm.com: Проблемы системы и их решения. URL: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_system_notifications.pdf?view=kc (дата обращения: 13.03.2020).

10 IBM Knowledge Center: IBM Resilient documentation // ibm.com: Системный администратор. URL: https://www.ibm.com/support/knowledgecenter/SSBRUQ_34.0.0/com.ibm.resilient.doc/admin/resilient_m_admin_intro.htm (дата обращения: 03.03.2020).

11 IBM Knowledge Center: IBM Resilient documentation // ibm.com: Обзор платформы Resilient. URL: https://www.ibm.com/support/knowledgecenter/SSBRUQ_34.0.0/com.ibm.resilient.doc/onboarding/overview.htm (дата обращения: 04.02.2020).

12 IBM Knowledge Center: IBM Resilient documentation // ibm.com: Обзор платформы Resilient. URL: https://www.ibm.com/support/knowledgecenter/SSBRUQ_34.0.0/com.ibm.resilient.doc/onboarding/modules.htm (дата обращения: 03.02.2020).

13 IBM Knowledge Center: IBM Resilient documentation // ibm.com: Playbook designer. URL: https://www.ibm.com/support/knowledgecenter/SSBRUQ_34.0.0/com.ibm.resilient.doc/onboarding/playbook_designer.htm (дата обращения: 01.03.2020).

14 StudFiles – Файловый архив студентов // studfiles.net: Основы расчета сил и средств для тушения пожаров. URL: https://studfile.net/preview/5674672/page:47 (дата обращения: 02.03.2020).

15 Risk24 – Управление рисками // risk24.ru: Качественный анализ рисков. URL: http://www.risk24.ru/analiz2.htm (дата обращения: 03.03.2020).