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

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой _к.п.н. Бердибаев Рат Шындалиевич_
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Комплексное, масштабируемое средство управления безопасностью, производительностью с принменением “FotiSIEM”_____

Специальность Системы Информационной Безопасности_____

Выполнил(а) Анарбекұлы Алишер_____ Группа СИБ-16-2___
(Ф.И.О.)

Научный руководитель к.т.н., профессор Маргаров Г.И._____
(ученая степень, звание, Ф.И.О.)
Консультанты: _____
по специальной части:
старший преподаватель Дмитриева Маргарита Валерьевна_____

_____ «_____» _____20____г.
(подпись)

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

_____ «_____» _____20____г.
(подпись)

Нормоконтролер: старший преподаватель Дмитриева Маргарита Валерьевна_
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

Рецензент: Айтхожаева Евгения Жамалхановна_____
(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 Технологий

Кафедра «Системы информационной безопасности»

Специальность «Системы информационной безопасности»

ЗАДАНИЕ

на выполнение дипломного проекта

Студенту Анарбекұлы Алишеру

(Ф.И.О.)

Тема проекта «Комплексное, масштабируемое средство управления безопасностью, производительностью с принменением “FotiSIEM”»

Утверждена приказом по университету № 147 от «11» 11 2019 г.

Срок сдачи законченного проекта « 01 » 06 2020 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): Исходные материалы для выполнения дипломного проекта – Облачная система FortiSIEM, VPN-сервер, OS Linux Debian 9.5, strongSwan Хостер для VPN Amazon Web Service

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Цель работы – изучение SIEM-систем, демонстрация работы с FortiSIEM и настройка VPN-сервера.

Перечень графического материала (с точным указанием обязательных чертежей): 70 изображений, 9 таблиц

Основная рекомендуемая литература: Официальный сайт компании Forti // Fortinet.com: FortiSIEM - мощная технология управления информационной безопасностью и событиями. URL: https://www.fortinet.com/ru/products/siem/fortisiem

Консультации по проекту с указанием относящихся к ним разделов проекта

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

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Изучение SIEM	17.02.2020 – 20.02.2020	
Внедрение FortiSIEM	21.02.2020- 28.02.2020	
Неавторизованный вход	01.03.2020 - 08.03.2020	
Работа с инцидентами внутри SIEM	09.03.2020 – 08.04.2020	
Настройка VPN-сервера	09.04.2020 – 09.05.2020	

Дата выдачи задания «_23_»___10___2019_г.

Заведующий кафедрой _____ (_Бердибаев Рат Шындалиевич__)
(подпись) (ФИО)

Научный руководитель
проекта _____ (_____)
(подпись) (ФИО)

Задание принял к
исполнению студент _____ (_Анарбекұлы Алишер__)
(подпись) (ФИО)

Аннотация

Применение *SIEM*-технологии (технологии управления информацией и событиями безопасности) является перспективным направлением в области защиты информации, особенно для критически важных инфраструктур. Тема дипломного проекта «Комплексное, масштабируемое средство управления безопасностью, производительностью с применением “FortiSIEM”». SIEM система позволяет получить максимально полное представление о том, что происходит в системе. Также она дает возможность строить подробные отчеты о инцидентах ИБ и реагировать на них быстрее.

Была произведена попытка несанкционированного входа в SIEM. Для масштабируемого решения проблем связанных с инцидентом использовался VPN-сервер на Debian. Т.е. привлечение сотрудников с различных регионов посредством защищенного подключения VPN.

Проведен анализ условий труда с расчетом системы кондиционирования и пожарной безопасности.

Аңдатпа

SYSTEM (information and security event management technology) технологиясын пайдалану ақпараттық қауіпсіздік саласындағы, әсіресе сыни инфрақұрылымдар үшін перспективалы бағыт болып табылады. Дипломдық жобаның тақырыбы - " FortiSIEM "қолдану арқылы қауіпсіздікті және өнімділікті басқарудың кешенді, масштабты құралы". SIEM жүйесі жүйеде болып жатқан ең толық суретті алуға мүмкіндік береді. Бұл сондай-ақ IB оқиғалары туралы егжей-тегжейлі есептерді жасауға және оларға жылдам жауап беруге мүмкіндік береді.

SIEM жүйесіне кіруге рұқсат етілмеген әрекет жасалды. Инциденттің ауқымды шешімін қамтамасыз ету үшін Debian базасында VPN-сервері пайдаланылды, яғни қорғалған VPN-қосылым арқылы әр аймақтан қызметкерлерді тарту.

Ауа баптау және өрт қауіпсіздігі жүйелерін есептеумен еңбек жағдайларына талдау жүргізілді.

Abstract

The use of SYSTEM technology (information and security event management technology) is a promising direction in the field of information security, especially for critical infrastructures. The topic of the diploma project is "a Comprehensive, scalable security and performance management tool using "FortiSIEM"". The SIEM system allows you to get the most complete picture of what is happening in the system. This also allows you to create detailed reports about IB incidents and respond to them faster.

An unauthorized attempt was made to log in to the SIEM system. To provide a scalable solution to the incident, a Debian-based VPN server was used, i.e.

attracting employees from different regions via a secure VPN connection.

The analysis of working conditions with the calculation of air conditioning and fire safety systems is carried out.

Содержание

Введение

В наше время количество и разнообразие угроз, связанных с нарушением целостности и конфиденциальности информации ежегодно растет. И системы безопасности должны успевать добавлять новые компоненты, тем самым расширяя инфраструктуру информационной безопасности. В случае, когда имеется несколько систем информационной безопасности, становится трудно продуктивно их администрировать и понимать, что происходит в инфраструктуре. Ведущие специалисты в данной области считают, что необходимо создать комплексный подход в сфере реагирования и расследования инцидентов информационной безопасности в виде единого централизованного решения. Поэтому многие компании интегрируют в свои системы SIEM (Security Information Event Management). SIEM система позволяет получить максимально полное представление о том, что происходит в системе. Также она дает возможность строить подробные отчеты о инцидентах ИБ и реагировать на них быстрее.

Управление информацией о безопасности и событиями, или определение SIEM – это подход к управлению безопасностью, объединяющий функции SIM (управление информацией о безопасности) и SEM (управление событиями безопасности) в единую систему управления безопасностью. Решения для обеспечения безопасности информации и управления событиями собирают журналы и анализируют события безопасности вместе с другими данными для ускорения обнаружения угроз и поддержки управления инцидентами и событиями безопасности, а также соблюдения требований. По сути, система технологий SIEM собирает данные из нескольких источников, что позволяет быстрее реагировать на угрозы. Если обнаружена аномалия, она может собрать больше информации, вызвать предупреждение или изолировать актив.

SIEM-система поддерживает интеграцию со сторонними устройствами, взаимодействуя с инфраструктурой, опрашивая ее о возникающих событиях безопасности, логах и производительности. При этом система позволяет обмениваться данными с внешними системами управления уязвимостей и оповещения об обнаруженных уязвимостях и тем самым расширять возможности по противодействию и защите от них.

1 SIEM

До момента обнаружения злоумышленника в сети или какой-нибудь уязвимости могут проходить многие месяцы. Все было хорошо, пока не возник реальный инцидент информационной безопасности. Допустим, нужен лог некого приложения за длительный промежуток времени. Найдя этот лог выясняется, что в нем нет необходимой информации для расследования. Все это ведет к большим потерям для компании. Площадь атак стремительно растет с высокой динамикой. Чем выше площадь атаки, тем ниже возможность управления поведением атаки. Для того чтобы, нивелировать негативную ситуацию предлагается решение класса SIEM. Для того, чтобы быстро расследовать инциденты безопасности и внедрять меры противодействия [1].

SIEM – Security Information & Event Management складывается из двух систем. SIM – Security Information Management. Система отвечающая за сбор, хранение, индексацию и исторический поиск по событиям поступающие от отслеживающих систем инфраструктуры, такие как межсетевые экраны, маршрутизаторы, серверы. SEM – Security Event Management. В этой системе происходит идентификация событий, корреляция между различными системами, построение отчетности и автоматизация выводов. В 2018 году 51% организаций сообщили о проблемной нехватке навыков кибербезопасности по сравнению с 45% в 2017 году. Организации стремятся повысить эффективность и действенность и обращаются к автоматизированным или автоматизированным инструментам, чтобы облегчить бремя ручного или повторяющегося задания [1].

FortiSIEM собирает данные из разнородных хост-систем, сетевых устройств и платформ безопасности в организации и добавляет контекст в реальном времени, аналитику и оповещения для более полного понимания среды, чем это можно сделать с помощью традиционной системы SIEM. FortiSIEM позволяет быстро и эффективно анализировать и идентифицировать инциденты с использованием данных из нескольких доменов с высокой степенью достоверности. ESG Lab подтвердила, что FortiSIEM смогла собирать, индексировать и анализировать реальный сетевой трафик, состоящий из сотен миллионов ежедневных событий от тысяч устройств и систем, и предоставлять краткий, оперативный, действенный интеллект [1].

FortiSIEM может автоматизировать как мониторинг, так и реагирование на угрозы и инциденты, чтобы свести к минимуму воздействие и время простоя, позволяя ИТ-отделам и командам безопасности сосредоточиться на более активных действиях [1].

Рисунок 1 – Сценарий работы SIEM

Подобные системы помогут решить нам следующие задачи:

- консолидация и хранение журналов событий от различных источников – сетевых устройств, журналов ОС, приложений и СЗИ. Посмотрев любой стандарт ИБ, мы увидим технические требования по сбору и анализу событий. Они нужны не только для того, чтобы выполнить требования стандарта, ведь бывают ситуации, когда инцидент увидели поздно, а события уже давно удалены или журналы событий почему-то недоступны и причины произошедшего выявить практически невозможно;

- предоставление инструментов для анализа событий и разбора инцидентов. Создает читабельный ответ. В том числе непосредственно с нужной Вам фильтрацией. Например, ежедневный отчет об инцидентах, отчет о работоспособности и т.д.;

- корреляция и обработка по правилам. Простейший пример — «login failed»: один случай ничего не значит, но три и более таких события с одной учетной записью уже могут свидетельствовать о попытках подбора. В простейшем случае в SIEM правила представлены в формате RBR (Rule Based Reasoning) и содержат набор условий, триггеры, счетчики, сценарий действий;

- автоматические оповещение и инцидент-менеджмент. Основная задача таких систем – не простой сбор событий, но и автоматизация процесса обнаружения инцидентов со сбором в журнале, а также своевременное информирование о событии;

- при наличии сканера уязвимостей, система частично поможет оценить риски [1].

Рассмотрим последовательность разбора событий в SIEM. На первом этапе происходит сбор информации, затем система производит ее анализ, далее сортировка, т.е. отбрасывание лишнего и нормализация событий, на следующем этапе корреляция между событиями различных направленностей. После корреляции происходит сохранение с одной стороны и оповещение с другой т.е. формируются отчеты и инциденты безопасности. На последнем

этапе происходит автоматическое принятие действие на основе анализа отчетности [2]. Алгоритм работы SIEM-системы представлен на рисунке 2.

Рисунок 2 – Разбор событий в SIEM

1.1 Архитектура SIEM системы

В основном, SIEM-система разворачивается над информационной системой находящейся под защитой и имеет архитектуру «источники данных» — «сервер приложений» — «хранилище данных» . SIEM-решения представляются как интегрированные устройства (all-in-one) или двух-трехкомпонентные комплексы. Распределенная архитектура обычно предполагает высокую производительность и наиболее подходящие возможности по масштабированию, а также позволяет развернуть SIEM-решение в IT-инфраструктурах с несколькими площадками. [2]

Агенты выполняют первоначальную обработку, фильтрацию и сбор событий безопасности. Передача информации от источников данных может осуществляться несколькими способами:

- источник сам инициирует передачу событий (например, отправляет по syslog-протоколу);
- события с источника забираются пассивно [2].

Архитектура классической SIEM-системы представлена на рисунке 3.

Рисунок 3 – Архитектура типовой SIEM системы

Собранная и отфильтрованная информация о событиях безопасности поступает в хранилище данных, где она хранится во внутреннем формате представления с целью последующего использования и анализа сервером приложений [2].

Сервер приложений реализует основные функции защиты информации. Он анализирует информацию, хранимую в репозитории, и преобразует ее для выработки предупреждений или управленческих решений по защите информации [2].

1.2 Задачи и функции SIEM-системы

Перед системой SIEM ставятся следующие задачи:

- консолидация и хранение журналов событий от различных источников — сетевых устройств, приложений, журналов ОС, средств защиты. Заглянув в любой стандарт ИБ, можно увидите технические требования по сбору и анализу событий. Они нужны не только для того, чтобы выполнить требование стандарта. Бывают ситуации, когда инцидент увидели поздно, а события уже давно затерты или журналы событий почему-либо недоступны, и причины инцидента выявить фактически невозможно. Кроме того, соединение с каждым источником и просмотр событий займет уйму времени. В противном случае, без анализа событий, есть риск узнать об инциденте в вашей компании из новостных лент;

- предоставление инструментов для анализа событий и разбора инцидентов. Форматы событий в различных источниках различаются. Текстовый формат при больших объемах сильно утомляет, снижает вероятность выявления инцидента. Часть продуктов класса SIEM унифицирует события и делает их более читабельными, а интерфейс визуализирует только важные информационные события, акцентирует на них внимание, позволяет отфильтровывать некритические события;

- корреляция и обработка по правилам. По одному событию не всегда можно судить об инциденте. Простейший пример — «login failed»: один случай ничего не значит, но три и более таких события с одной учетной записью уже могут свидетельствовать о попытках подбора. В простейшем случае в SIEM правила представлены в формате RBR (Rule Based Reasoning) и содержат набор условий, триггеры, счетчики, сценарий действий;

- автоматическое оповещение и инцидент-менеджмент.

Основная задача SIEM — не просто собрать события, но автоматизировать процесс обнаружения инцидентов с документированием в собственном журнале или внешней системе HelpDesk, а также своевременно информировать о событии [4].

SIEM способна выявлять:

- сетевые атаки во внутреннем и внешнем периметрах;

- вирусные эпидемии или отдельные вирусные заражения, неудаленные вирусы, бэкдоры и трояны;

- попытки несанкционированного доступа к конфиденциальной информации;

- фрод и мошенничество;

- ошибки и сбои в работе информационных систем;

- уязвимости;

- ошибки конфигураций в средствах защиты и информационных системах.

Система SIEM универсальна за счет своей логики. Но для того чтобы возложенные на нее задачи решались — необходимы полезные источники и правила корреляции. Любое событие (например, если в определенной комнате открылась дверь) может быть подано на вход SIEM и использовано [2].

Источники выбираются на основании следующих факторов:

- критичность системы (ценность, риски) и информации (обрабатываемой и хранимой);

- достоверность и информативность источника событий;

- покрытие каналов передачи информации (должны учитываться не только внешний, но и внутренний периметр сети);

- решение спектра задач ИТ и ИБ (обеспечение непрерывности, расследование инцидентов, соблюдение политик, предотвращение утечек информации [4].

1.3 Корреляция и аналитика

Корреляция и аналитика являются ядром технологии SIEM, и она включает в себя связывание воедино различных событий, о которых сообщается в журналах, для выявления признаков компромисса. Один пример: сканирование порта с последующим доступом пользователей к определенным типам данных. Важно, чтобы функциональность аналитики была представлена таким образом, чтобы иметь возможность эффективно ее использовать [5].

Ключом к этой способности обнаруживать угрозы является использование правил корреляции, основной набор которых может быть предоставлен системой SIEM, но к которым администраторы могут добавить. Например, одно правило корреляции может заключаться в том, что, если четыре или более неудачных попыток входа в систему происходят с одного и того же IP-адреса с использованием разных имен пользователей в течение 15 минут, и за этим следует успешный вход с этого IP-адреса на любое устройство в сети. Затем должно быть выдано предупреждение. В этом случае механизм корреляции системы SIEM начинает работать для обнаружения модели поведения (неудачные попытки входа в систему, сопровождаемые успешной), которые могут указывать на то, что атака методом перебора была успешной [5].

Корреляция является одним из ключевых компонентов любого эффективного инструмента SIEM. Поскольку информация из вашей цифровой среды поступает на платформу SIEM, эта платформа использует корреляцию для выявления любых возможных проблем. Это достигается путем сравнения последовательности действий с предустановленными правилами, которые могут быть установлены поставщиком SIEM или пользовательскими настройками, созданными вами и вашей командой [5].

Приведенный выше пример повторных неудачных попыток входа в систему является типичным случаем, в котором корреляция оказывается полезной. Хотя эта информация может не выглядеть угрожающей для невооруженного глаза, читающей множество данных, инструменты SIEM с необходимыми правилами корреляции смогут определить потенциальную угрозу и выдать предупреждение. Для новичков в платформе настройка правил корреляции SIEM может показаться сложной. В конце концов, инструменты SIEM, как правило, будут искать только то, что вы им скажете, поэтому создание правил, предвидящих реальные угрозы, является обязательным. К счастью, многие продукты SIEM поставляются с уже подготовленными правилами корреляции. Вам нужно будет выполнить их, чтобы определить, какие из них имеют смысл для бизнеса, и у вас также будет возможность включить собственные правила корреляции по своему усмотрению [5].

Следует также отметить, что инструменты мониторинга SIEM могут выявлять ложные срабатывания, поэтому здесь важно найти правильный

баланс. Если вы настроите свои правила корреляции таким образом, чтобы они вызывали слишком много ложных срабатываний, вы, возможно, теряете время, спускаясь в кроличьи норы. Однако если вы зайдете слишком далеко в другом направлении, вы рискуете позволить злонамеренной деятельности продолжаться без адекватного и своевременного ответа. Таким образом, правила корреляции SIEM позволяют профессионалам в области кибербезопасности расширять эти инструменты, чтобы они работали для конкретных потребностей каждого бизнеса. Конкретный продукт SIEM может предлагать клиентам тот же тип защиты и те же функции, но это зависит от MSP, чтобы развернуть эти инструменты, чтобы они были максимально эффективными для каждого бизнеса. Схема, демонстрирующая роль корреляции, представлена на рисунке 4.

Рисунок 4 – Роль корреляции

Аналитика SIEM основывается на функциях поиска, выполнении правил и формировании отчетов. Функция поиска SIEM состоит из поиска в реальном времени и исторического поиска информации [4], которая была собрана на основании ИТ-инфраструктуры. В режиме поиска в реальном времени выводятся события уже возникшие, тогда как исторический поиск базируется на информации из баз данных событий. Простой поиск по ключевым словам и структурированные поисковые запросы, позволяющие выполнять поиск основываясь на конкретных атрибутах и значениях событий, затем группирование результатов по атрибутам могут быть включены в оба типа поиска. SIEM непрерывно наблюдает за инфраструктурой и формирует информацию, которую можно использовать для анализа безопасности, производительности и доступности. Для быстрого

реагирования на события безопасности нужно вовремя получать предупреждения о том, что могли возникнуть исключительные, подозрительные или потенциальные неисправности и нарушения. С этой целью используются правила, определяющие условия, на которые необходимо обратить внимание и которые инициируют инцидент [5].

1.4 Принцип работы

Принцип работы SIEM сводится к последовательному алгоритму действий. Система собирает информацию из разных источников, анализирует её в режиме реального времени, при надобности предпринимает превентивные меры, систематизирует базы данных, анализирует действия пользователей на основе результатов предыдущего мониторинга, создает предупреждения и оповещения о критических событиях [4].

Источниками данных для SIEM служат разнообразные корпоративные системы:

- системы контроля доступа и аутентификации. Предназначены для наблюдения за получением доступа к информационному потоку;
- DLP-системы. Передают данные о несанкционированном выходе информации за пределы корпоративной сети и о нарушении в использовании привилегий;
- ресурсы IDS/IPS. Передают данные о сетевых атаках, изменении прав доступа;
- антивирусные платформы. Уведомляют об угрозах в виде вредоносного кода, замене конфигураций или политик конфиденциальности, сообщают о работе баз данных и ПО;
- журналы событий серверов и тонких клиентов. Контролируют соблюдение прав доступа и политики ИБ;
- межсетевые экраны. Передают данные об опасных инцидентах, вредоносном ПО;
- оборудование сети. Учитывает трафик сети, контролирует доступ пользователей к информационным потокам;
- системы веб-фильтрации. Обобщают и направляют данные о том, какие запрещенные или вредоносные сайты в интернете посещают пользователи.

Система SIEM - это, по сути, специализированная система анализа больших данных, которая стремится получить полезную информацию о массе событий и других данных, которые она принимает и хранит. Основным источником данных являются журналы, сгенерированные системами, включая ваши серверы и устройства безопасности, но SIEM могут принимать различные другие типы данных, включая сетевые пакеты, а также контекстную информацию о пользователях [4], ресурсах, угрозах и уязвимостях. это можно найти внутри или за пределами вашей организации. Затем эти данные из разных источников должны быть «нормализованы» или

переформатированы, чтобы SIEM могла их понять. На рисунке 5 показан алгоритм работы SIEM [4].

Рисунок 5 – Алгоритм работы SIEM

SIEM-система обрабатывает и анализирует полученные данные на основе математических вычислений и сравнения статистических данных. Правила анализа в традиционных решениях чаще всего задаются вручную. Например, во время настройки создается скрипт, по которому однократный инцидент не представляет угрозы, а повторяющийся под одной учетной записью – означает попытку подобрать код доступа [4].

SIEM-решение позволяет обнаружить:

- внешние и внутренние кибератаки;
- отдельные заражения и вирусные эпидемии;
- попытки получить несанкционированный доступ к защищенным информационным потокам;
- факты корпоративного мошенничества;
- погрешности и нарушения в работе информационных систем;
- слабые точки защиты;
- нарушение структуры средств защиты;
- целевые хищения.

1.5 Преимущества SIEM системы

Оценить преимущества SIEM-решения поможет анализ по основным характеристикам.

Некоторые из преимуществ SIEM включают следующее:

- сокращает время, необходимое для выявления угроз, сводя к минимуму ущерб от этих угроз;
- предлагает целостное представление о среде информационной безопасности организации, облегчая сбор и анализ информации о безопасности для обеспечения безопасности систем - все данные организации поступают в централизованное хранилище, где они хранятся и легко доступны;
- могут использоваться компаниями для различных вариантов использования, которые вращаются вокруг данных или журналов, включая программы безопасности, аудит и отчеты о соответствии, службу поддержки и устранение неполадок в сети;

- поддерживает большие объемы данных, чтобы организации могли продолжать масштабирование и увеличение своих данных;

- обеспечивает обнаружение угроз и оповещения о безопасности; а также;

- может выполнить детальный судебный анализ в случае серьезных нарушений безопасности [4].

Комплексное средство анализа состояния сети в режиме реального времени. Высокая производительность и скорость анализа событий в режиме реального времени. Большое число правил корреляции и генерируемых отчетов, доступных при внедрении продукта из коробки. Большое число протоколов интеграции со сторонними устройствами и системами. Взаимная корреляция данных анализа SOC и NOC. Реализация практически любого сценария реагирования на инцидент безопасности, проведение расследования за счет возможности определения цепочки последовательных действий. Автоматизация процессов обнаружения угроз и аномалий. Автоматизация процессов регистрации и контроля инцидентов, с последующей возможностью их расследования. Контроль за состоянием инфраструктуры. Наличие агентов сбора данных и мониторинга для Microsoft Windows и агентов контроля целостности файлов для Linux. Поддержка нескольких сценариев развертывания. Поддержка горизонтального масштабирования и виртуализированной архитектуры. Гибридная архитектура базы данных. Распределенная корреляция событий в режиме реального времени. Оперативная настраиваемая обработка журналов. Предусмотрено несколько сценариев развертывания в зависимости от нужд и инфраструктуры заказчика [4].

Важный маркер удобства работы с SIEM – возможность централизованно координировать компоненты платформы из единой консоли, а также автоматически обновлять предустановленные политики и шаблоны отчетности. Все это облегчит труд специалиста по информационной безопасности. Еще один плюс в пользу решения – оперативность и качество технической поддержки. По этому параметру в большинстве случаев выигрывают отечественные производители, главным образом, из-за невысокой стоимости [4].

1.6 Обзор и сравнение SIEM решений

На этапе выбора критериев сравнения в данной рабочей группе возникают разногласия насчет корректности сравнения существующих решений или недостаточного раскрытия ряда функциональных возможностей. Потребности сервисного SOC разительно отличаются от потребностей инфраструктурного внутреннего SOC. И если для первого важно подключить из коробки максимальное количество источников и иметь возможность гибкого управления данными, поступающими от них, то для второго большим приоритетом может стать удобный пользовательский интерфейс. В зависимости от потребностей функциональность продуктов

определяет их возможности. Это ориентировка на интеграцию внутри собственной экосистемы, как у Positive Technologies и IBM, или направленность на интеграцию со сторонними решениями, как у FortiSIEM, RuSIEM и Micro Focus Security. Кроме того, подходы к визуализации и навигации в консоли каждого из решений соответствуют определенной логике, которую не всегда можно оценить четкими критериями, но зато можно эмпирически принять при живой демонстрации. Группировка критериев осуществлялась на основе базовых влияющих на компании-потребители направлений, диктуемых временем: степень автоматизации, стратегия развития (в том числе устойчивость на рынке), эластичность архитектуры. Возможность компании-потребителя учитывать риски при таких условиях в дальнейшем определяет ее выбор. К примеру, стоит присмотреться к комплексному моновендорному решению. Далее проводилась детализация направлений в группы, которые раскладывались, в свою очередь, на подгруппы. По возможности и экспертно оцененному весу влияния критерия на оценку подгруппы разбивались оценочные параметры [6].

Архитектура решения SIEM-системы —масштабируемость, методы управления событиями и схема лицензирования — важный параметр для Enterprise-установок, где необходимо подсчитать и эффективность реализации в распределенных сетях. Интеграционные возможности — наличие развитых встроенных и интегрируемых подсистем управления уязвимостями, инцидентами и активами позволит в начальном периоде эксплуатации ограничиться использованием одного продукта, без увеличения количества используемых администратором и аналитиком консолей. А интеграция со сторонними решениями в целях обогащения информации о событиях ИБ, сведения об API и поддерживаемых источниках событий указывают на открытую позицию компании на рынке, умение находить общий язык с другими игроками, говорит о направлениях развития продукта.

Дополнительные критерии — параметры, которые подвержены влиянию внешней среды. Это и отчетность, удобство, это и глубина погружения при навигации в рамках интерфейса системы. Все это влияет на оперативность при обработке событий ИБ и выявлении инцидентов ИБ и позволяет примериться к существующим внутри компании KPI. Ниже будут рассмотрены некоторые системы в качестве примера и сравним их:

- RUSIEM;
- RSA NetWitness;
- IBM QRadar SIEM;
- Splunk.

RuSIEM — российская разработка отечественной компании РУСИЕМ, резидента Сколково. Разработка ведется с 2014 года. Решение позволяет организовать централизованный и распределенный сбор событий с систем любого класса (включая СКУД), автоматическое обнаружение инцидентов ИТ, ИБ и бизнес-процессов по правилам корреляции и с применением

механизмов искусственного интеллекта (ИИ). Развертывание решения возможно как в виртуальной среде на гипервизорах, так и на физической платформе [6].

Решение состоит из нескольких модулей и включает в себя:

- RuSIEM — коммерческое решение класса SIEM;
- RuSIEM free — полнофункциональное свободно распространяемое готовое решение класса LM (log management);
- RuSIEM Analytics — модуль аналитики, работающий в режиме реального времени;
- RuSIEM Network Sensor — сетевой сенсор для анализа трафика;
- RuSIEM Analytics — модуль, опционально устанавливаемый на RuSIEM, предназначен для обнаружения атак и аномалий в режиме реального времени без необходимости создания правил корреляции.

Модуль позволяет:

- выявлять инциденты с помощью ИИ и симптоматической модели;
- обнаруживать инциденты на основе статистического Baseline, управляемого пользовательскими правилами;
- уведомлять о совпадениях по фид-листам, содержащим IP и URL-адреса, хэши файлов malware, управляющих серверов ботнетов, выходные ноды tor и прочие угрозы;
- автоматически строить ИТ-активы по данным из событий и трафика;
- оценивать Standard Compliance и Policy Compliance по техническим контролям, в том числе и по пользовательским стандартам;
- строить сложные аналитические отчеты с большим количеством расчетов [6].

RuSIEM имеет широкий набор визуализаций данных: дашборды, карта взаимосвязей, выборка по событиям, аналитика, отчеты, инциденты. Решение позволяет отслеживать входы и доступы персонала с новых мест и приложений — из других браузеров, IP–адресов и операционных систем. Симптоматическая модель помогает классифицировать и приоритизировать события, находить их без знания текста, строить комплексные отчеты. Интеграция с системами СКУД позволяет решать такие кейсы, как «интерактивный вход без прохода в офис», «отобразить сотрудников, присутствующих в офисе», «построить отчет о входах/выходах в офис». Схема принципа работы RuSIEM представлена на рисунке 6.

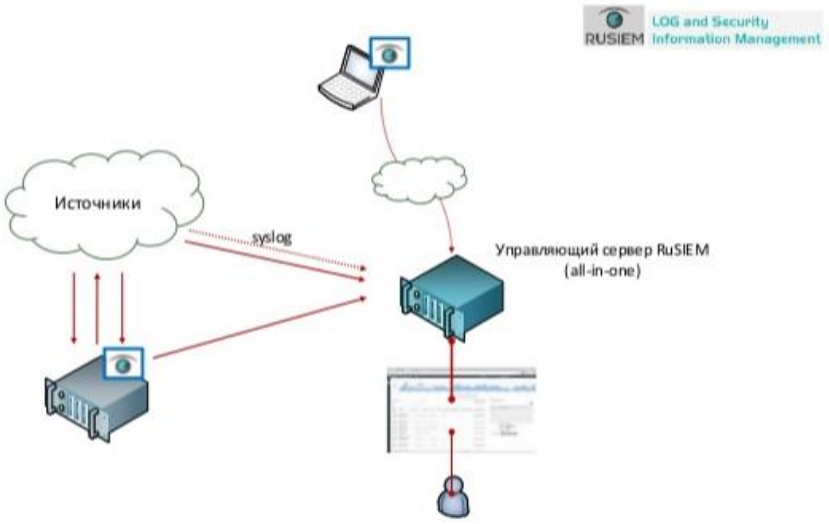

Рисунок 6 – Принцип работы

Преимущества RuSIEM:

- применение современных аналитических подходов без облачных сервисов, на стороне заказчика, позволяет обнаруживать угрозы и аномалии даже без созданных для этих случаев правил корреляции;
- универсальные коннекторы позволяют подключать новые источники в кратчайшие сроки;
- гибкие правила корреляции позволяют описать любой сложный кейс;
- модульные варианты развертывания позволяют применять систему даже с минимальным бюджетом;
- не имеющее лимита горизонтальное и вертикальное масштабирование;
- управляемая пользователем критичность событий и аналитика;
- распределенная корреляция без необходимости сбора событий в центральный офис;
- встроенный инцидент–менеджмент по itil, включая постановку задач, ограничение видимости инцидентов, эскалацию инцидентов.

Интерфейс RuSIEM представлен на рисунке 7.

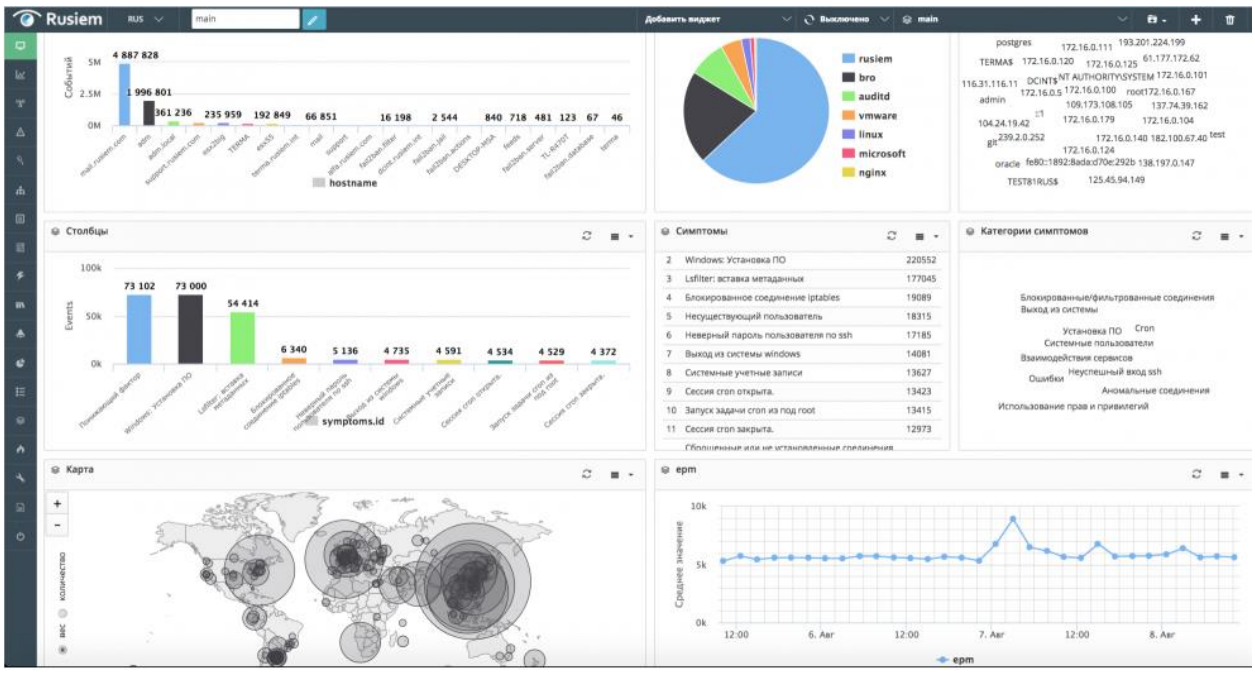

Рисунок 7 – Консоль RuSIEM

Следующая рассматриваемая SIEM-система - QRadar SIEM.

QRadar SIEM обеспечивает тотальную видимость внутри сети, осуществляя сбор и анализ данных, которые позволяют оперативно получать всю необходимую информацию о событиях безопасности и работе сетевых устройств, независимо от сложности сетевой конфигурации. Максимальная прозрачность сети позволяет с наибольшей эффективностью управлять ее безопасностью и обнаруживать все существующие и потенциальные угрозы задолго до их реализации [6].

QRadar SIEM - это интегрированное средство, прекрасно справляющееся с задачами управления политиками по соответствию требованиям и стандартам, сбора и анализа логов и предоставляющее самый современный инструментарий для выявления угроз. Решение основано на гибкой платформе QRadar Security Intelligence Platform, которая может развиваться параллельно с предприятием и подстраиваться под его расширяющуюся инфраструктуру, легко и оперативно обеспечивая мониторинг корпоративной безопасности [6].

QRadar SIEM собирает информацию из следующих источников:

- события системы безопасности - события от брандмауэров, VPNs, IDS/IPS, и т.д.;

- сетевые события - события от свитчей, роутеров, серверов, хостов и т.д.;

- монитор активности сети - контекстные идентификаторы протоколов 7-го уровня от сетевого трафика и приложений;

- монитор активности пользователей - данные продуктов типа IAM и сканеров уязвимостей;

- журналы событий приложений – ERP (Enterprise Resource Planning), документооборот, базы данных приложений, административные платформы и т.д.;

- контроль угроз, логов и соответствия политикам в режиме реального времени [6].

Объединяя разрозненную информацию, QRadar SIEM делает более эффективным обнаружение всех современных угроз. Данные нормируются и коррелируются для своевременного выявления, уведомления и реагирования на угрозы, которые не в состоянии определить другие средства защиты с ограниченной видимостью. Мониторинг, осуществляемый QRadar SIEM, позволит предприятиям обнаружить сложные угрозы, среди которых инсайдерское мошенничество, нецелевое использование приложений и многие другие [6].

Особенно эффективно применение QRadar SIEM для предприятий с крупномасштабными сетями, в которых регистрируются миллионы и более событий в день. QRadar SIEM осуществляет сбор, анализ и хранение данных и предоставляет корреляцию событий в режиме реального времени. Это позволяет среди огромного количества данных распознать те, которые могут привести к инцидентам безопасности. Миллиарды сетевых событий и потоков могут быть упрощены, что, соответственно, упростит процессы выявления угроз, аудита и 13 создания отчетности, соответствующей требованиям и стандартам. В целях аудита и защиты сетевой инфраструктуры QRadar SIEM обеспечит долгосрочный сбор событий и прикладных данных, их архивирование, поиск необходимых данных и отчетность [6].

QRadar SIEM контролирует все серьезные инциденты и угрозы, предоставляя хронологию обслуживания и всю необходимую сопутствующую информацию. Благодаря этому решению службы безопасности смогут всегда узнать ответы на такие вопросы, как: кто нарушает безопасность, какой объект подвергается нападению, в каком месте проводить расследование, каковы последствия для бизнеса? QRadar SIEM предоставит полную информацию о факторах, нарушающих нормальный режим работы, пользователях, моделях нарушителей, важности ресурсов, характеристиках уязвимостей, уровне активности угроз и отчетах о предыдущих нарушениях и т.д. Таким образом, служба безопасности сможет получить все необходимые сведения для своевременного реагирования на любые инциденты безопасности [6].

При помощи QRadar SIEM можно обнаружить любые отклонения и изменения в работе приложений, серверов, хостов и сегментов сети. Возможность идентификации трафика на прикладном уровне позволяет QRadar SIEM достаточно точно анализировать и понимать политики и угрозы корпоративной сети предприятия, а также проводить общий мониторинг сетевой активности. Функция контроля работы с таким приложением, как Skype, и социальными сетями (включая Twitter, LinkedIn и т.д.), также

позволяет улучшить видимости сети. Поддерживая обнаружение большого количества отклонений и поведенческих правил, QRadar SIEM может детально ответить на вопрос о том, какой пользователь и что использует. Контентный анализ и оповещения при передаче контента, корреляция с прочей сетевой активностью и журналами событий позволяют выявить нецелевую передачу данных. Возможности фильтрации и выбор любого временного промежутка для анализа позволяют пользователю настроить вариант вывода результатов по собственному усмотрению. [6]

Теперь IT-специалистам доступна улучшенная видимость активности широкого спектра бизнес-приложений в виртуальных сетях. Виртуальные сервера, как и физические, имеют уязвимости в системе безопасности, поэтому прозрачность виртуальной среды обработки данных требуется для точного определения необходимых мероприятий по защите приложений и данных.

Централизованная интуитивно понятная консоль управления обеспечивает ролевой доступ, предоставляя глобальный обзор управления инцидентами и отчетности. Панели управления QRadar SIEM предлагаются как функционал, и пользователи могут сами создать и настроить свое рабочее пространство в соответствии с решаемыми задачами. Такая детализация предоставит возможность гораздо проще выявлять и выбирать всплески событий и сетевые потоки, связанные с нарушениями. QRadar SIEM предлагает около 3 500 шаблонов отчетов, связанных с конкретными устройствами, ролями и требованиями регуляторов. [7]

Решение QRadar SIEM в первую очередь предназначено для малого и среднего бизнеса, но может быть с успехом развернуто в компании любого масштаба за счет своей легкой масштабируемости. QRadar SIEM делает возможным автоматический переход с другого решения и полную синхронизацию между системами. Внедрять дополнительные решения сторонних производителей нет необходимости, так как QRadar SIEM обеспечивает высокий уровень анализа и хранения данных благодаря plug-andplay устройствам, входящим в семейство продуктов QRadar. Графический интерфейс QRadar SIEM показан на рисунке 8.

Рисунок 8 – Графический интерфейс QRadar SIEM

В июле 2016 года RSA, подразделение безопасности EMC, повторно представило свою SIEM-систему как платформу RSA NetWitness Suite, которая включает в себя: управление журналами RSA NetWitness Logs & Packets (ранее RSA Security Analytics); средство обнаружения угроз на рабочих станциях RSA NetWitness Endpoint (ранее RSA Enterprise Compromise Assessment Tool); менеджер центра оперативного управления RSA NetWitness SecOps Manager (ранее RSA SecOps). RSA NetWitness Suite обеспечивает видимость угроз с использованием данных из событий безопасности и других источников журналов, полного захвата пакетов, NetFlow и конечных точек (через RSA NetWitness Endpoint). Система RSA NetWitness ориентирована на мониторинг, анализ и оповещение в режиме реального времени в дополнение к поддержке упреждающей угрозы, а также реагированию на инциденты и судебному расследованию. Алгоритм работы RSA NetWitness Suite показан на рисунке 9.

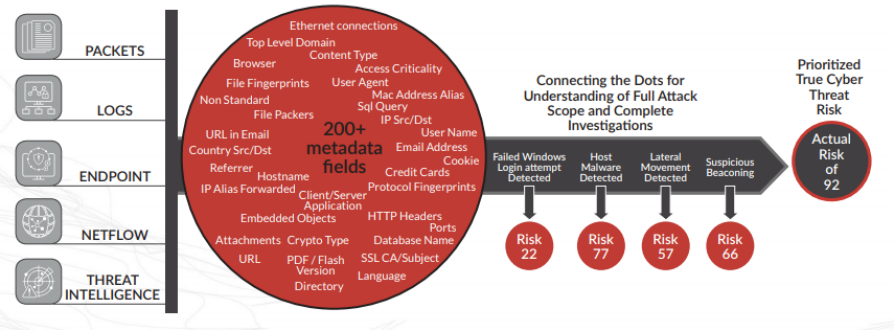

Рисунок 9 – Алгоритм работы RSA NetWitness Suite

Платформа использует комбинацию одного или нескольких физических или виртуальных устройств для регистрации журналов и пакетов (декодер), запросов и поиска необработанных данных (концентраторы), аналитики в реальном времени (Event Stream Analysis) и долговременного хранения журналов и отчетов (Archiver). Гибридные устройства, объединяющие декодеры и концентраторы в одну систему, доступны для небольших сред. Декодеры и концентраторы доступны для поддержки крупных и региональных распределенных архитектур. Сервер NetWitness предоставляет унифицированный интерфейс для администрирования и анализа. Он также предоставляет интерфейс для отчетов и аналитики вредоносных программ. [8]

RSA Live Connect — это облачная служба, которая обеспечивает автоматическое обновление контента, включая правила обнаружения, парсеры пакетов и журналов, отчеты и источники угроз. Пользователи RSA NetWitness Suite также могут использовать RSA NetWitness SecOps Management (модуль в решении RSA Archer Governance, Risk and Compliance), который добавляет расширенный процесс управления инцидентами, панели управления и отчеты. Преимущества RSA NetWitness Suite: Платформа RSA NetWitness объединяет аналитику обнаружения угроз и мониторинг событий, расследование и анализ угроз в сетевом трафике, конечных точках и других источниках событий безопасности и журналов. Модульные варианты развертывания позволяют клиентам выбирать мониторинг сетевого трафика, а также возможности мониторинга и анализа событий и журналов по мере необходимости. RSA Live обеспечивает простой и автоматизированный подход для обеспечения бесперебойной доставки информации об угрозах, контента и других обновлений. Интеграция с RSA NetWitness SecOps Manager обеспечивает унифицированные возможности SOC. Визуализация RSA NetWitness Suite представлена на рисунке 10.

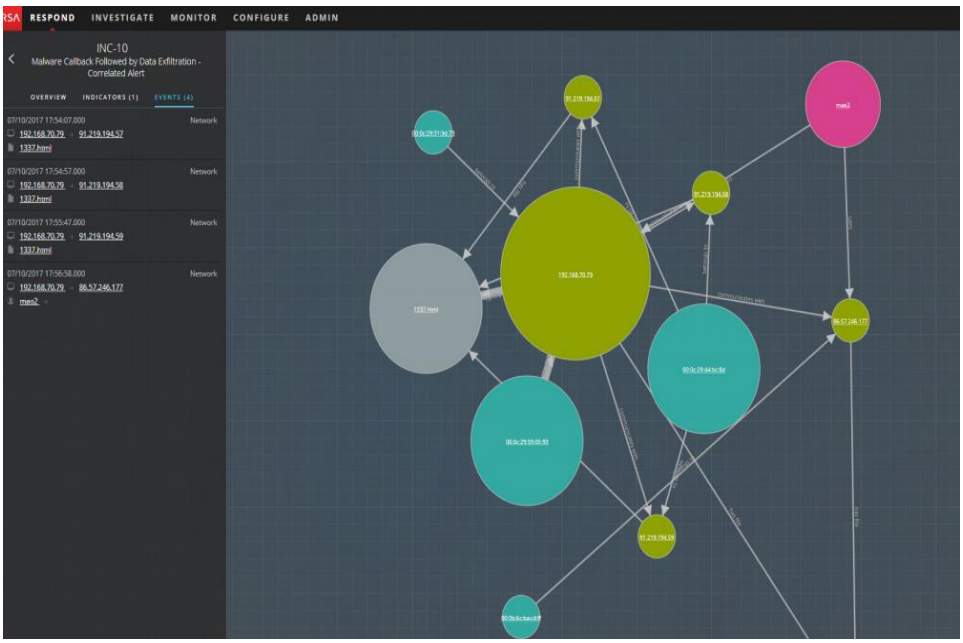

Рисунок 10 – Визуализация RSA NetWitness Suite

Следующая рассматриваемая SIEM – Splunk Enterprise Security.

Splunk — это многофункциональная платформа для сбора, хранения, обработки и анализа машинных данных. На сегодняшний день она является крайне популярной в США и в Европе и постепенно выходит на другие рынки, включая Россию. Одной из главных особенностей платформы является то, что она может работать с данными практически из любых источников, что позволяет широко применять платформу в разных отраслях. Одним из ключевых направлений развития является SIEM-система Splunk Enterprise Security [8].

В состав Splunk Enterprise Security входят следующие функциональные решения:

- Incident Review — гибкий инструмент обзора и управления инцидентами, обогащенный информацией из внешних источников;
- Investigator — визуальный инструмент выявления;
- Kill Chain- таки и создания новых корреляционных поисков на базе собранного опыта;
- Glass Tables — наглядное построение логических схем защищаемых ресурсов со встроенным редактором. Возможность создания индивидуально настроенных визуализаций с ключевыми показателями работы SOC, изменяемыми в масштабе реального времени;
- Security Intelligence — обширный набор преднастроенных интеграций с внешними источниками информации об угрозах, включая интеграцию с Facebook Threat Exchange.

Платформа Splunk может быть развернута как на физических, так и на виртуальных серверах, также пользователям доступна облачная версия решения. Splunk предлагает два вида лицензий: постоянную и годовую подписку, стоимость которых прямо пропорциональна объему обработанных данных в день, в гигабайтах. За последние годы в связи с сильным развитием

направлений Machine Learning и Artificial Intelligence Splunk разработал и интегрировал в свой продукт отдельный модуль – Splunk Machine Learning Toolkit, позволяющий строить расширенную аналитику в области прогнозирования, выявления аномалий, кластеризации и др. Этот модуль повышает аналитические возможности SIEM-системы Splunk Enterprise Security. В середине 2015 года Splunk добавил собственную функциональность UEBA с приобретением Caspida, которая была переименована в Splunk UBA (Splunk также работает с рядом других продуктов UEBA). Более жесткая интеграция между продуктами Enterprise Security и UBA была введена в начале 2016 года. Преимущества Splunk: Splunk осуществляет сбор, поиск, мониторинг и анализ по различным и достаточно большим объемам данных как в режиме исторического поиска, так и в реальном времени, выдавая быстрый результат и высокую интерактивность поисковых запросов на чрезвычайно больших объемах данных. Splunk является полноценной Big Data платформой. Splunk является универсальной системой для машинных данных, которая обеспечивает комплексный сбор данных, их обработку и анализ. Таким образом система способна объединить в себе машинные данные, бизнес данные, пользовательские данные и строить аналитику в различных разрезах, что делает ее крайне универсальным. Splunk использует технологию MapReduce [9], что обеспечивает распределение нагрузок и быструю горизонтальную масштабируемость системы. Также благодаря технологии MapReduce возрастает ее производительность. На рисунке приведена панель мониторинга [8].

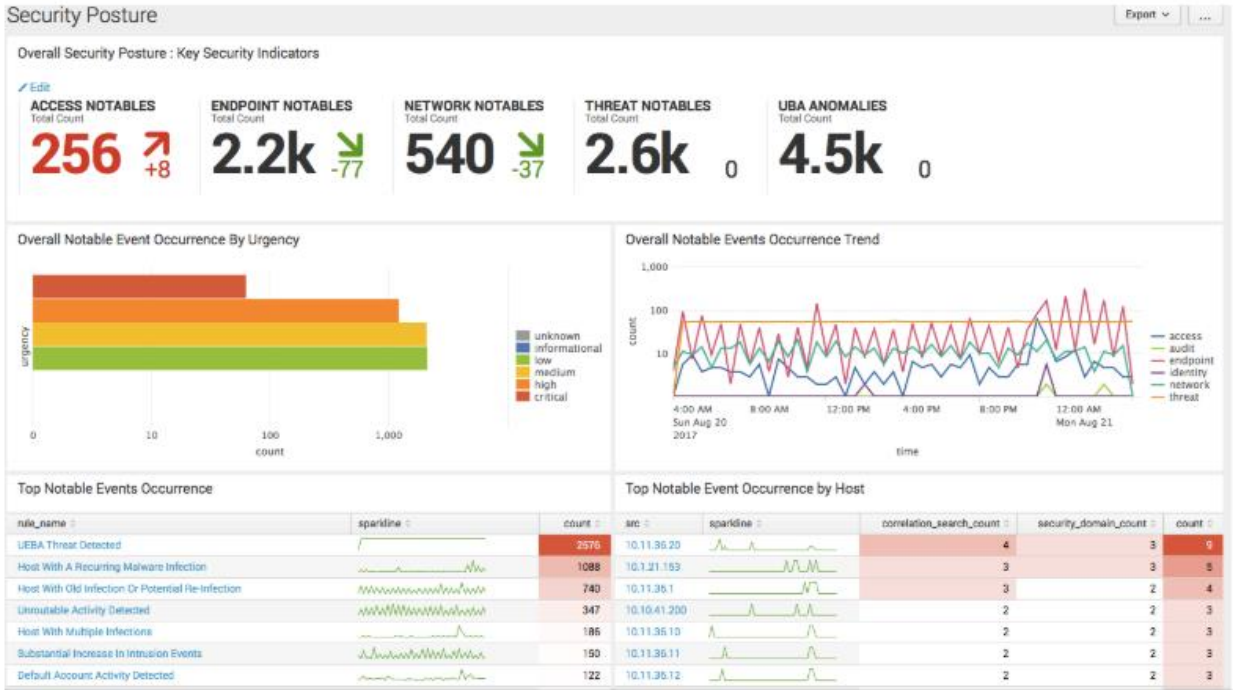

Рисунок 11 – Панель мониторинга Splunk Enterprise Security

Таблица 1 – Сравнение различных SIEM систем

Критерий оценки / Вендор	IBM Qradar	RSA NetWitness	Splunk	RuSIEM
Авторегистрация уязвимостей (интеграция со сканерами)	Интеграция со всеми популярными сканерами крупных вендоров, возможности по интеграции через API и отчеты различных форматов	Нет	Интеграция со сканерами по открытым протоколам. Для популярных сканеров есть модули разбора событий (Qualys, Netxpose Rapid7 и др.)	Интеграция с некоторыми сканерами через API, файловые логи и syslog

Продолжение таблицы 1

Риск-корреляция, учет риск-корреляции в правилах	Риск-корреляция с учетом составляющих показателя Magnitude (Relevance, Credibility и Severity)	Нет	Скоринговая модель, учитывающая данные об активах и учетных записях пользователей	Через симптомы, определяющие вес события. Через правила корреляции. Через AI с уточнением в правилах
Пред настроенные панели визуализации и отчеты по соответствию стандартам (Compliance)	COBIT, FISMA, GLBA, GSX-Memo22, HIPAA, NERC, PCI DSS, SOX	FISMA, ISO27002, FERPA, GLBA, FFIEC, NERC-CIP, BILL 198, BASEL II, GPG-13, HIPAA, NISPOM, PCI DSS, SOX, SSAE 16	GDPR, HIPAA, FISMA, PCI DSS (платные и бесплатные дополнения к платформе SPLUNK ENTERPRISE и SPLUNK ES)	PCI DSS
Произвольные формулы расчета рисков	Нет	Нет	Встроено в язык SPL, на который опираются правила корреляции, а	Формул нет, но есть возможность. Определяется суммой из

			также в Risk Analysis Framework	одного или нескольких симптомов с весами и правилами корреляции
Наличие возможности задания или импорта информации об активах (assets)	От сканеров безопасности, CSV-файлов, API	Нет	Штатно описана интеграция с 13 типами и вендорами (AD, CMDB, SCOM, Cisco ISE, Symatec Endpoint Protection и др.)	Импорт в режиме реального времени по событиям и поступающей информации из источников. Правка на уровне удаления элемента актива и шаблона актива

Продолжение таблицы 1

Определение критичности актива	На уровне сетевого объекта (группировка в модели системы), критичность источника (выставляется при заве), учет в правилах корреляции	Нет	Система встроеных справочников (порты, процессы, виды трафика и др.) с возможностью проставления степени критичности	Нет
Управление правилами корреляции	Объектный конструтор, язык AQL	Объектный конструктор, язык Esper	Конструктор, язык поисковых запросов	Графический конструктор
Возможности управления ИТ-активами	Возможность создания и редактирования после заведения вручную	Нет	Автоматическое и ручное создание, редактирование и удаление элементов	Только ручное удаление актива и изменение шаблона
Интеграция со службами каталогов	Для аутентификации — да. Для расширения возможности выгрузки из каталога —	Аутентификация	Для выгрузки пользователей и устройств, для прозрачной аутентификации	Аутентификация, интеграция со СКУД

	через приложение			
Использование технологий искусственного интеллекта, автоматизации аналитики верхнего уровня	QRadar Advisor With Watson	Нет	Встроенный в Splunk ES 5.0.+ функциональность Workbench Investigator	DL, ML на базе RuSIEM Analitics (включение после закупки лицензии на компонент)
Использование алгоритмов машинного обучения	QRadar Advisor With Watson	Нет	Splunk UBA, Splunk ML Toolkit, Splunk Extreme Search	PMML, AI, DL
Подключение репутационных баз по IP	Да (свои от IBM X-Force и сторонние)	Да (свои (RSA Live) и сторонние)	Да	Да (фиды в модуле аналитики)
Другие интеграции и виды коннекторов	Через магазин приложений (IBM App Exchange)	Через плагины	REST API, SDK, SplunkJS, ODBC и др.	Через file, syslog, API

2 Практическая часть

2.1 Описание системы FortiSIEM

FortiSIEM — это комплексное, масштабируемое средство управления безопасностью, производительностью и обеспечением соответствия требованиям всех компонентов инфраструктуры, способное работать как с облаками [10], так и с интернетом вещей (IoT). Решение FortiSIEM направлено на снижение сложности обнаружения угроз при повышении эффективности системы безопасности. SIEM-система такого уровня направлена на защиту не только информации, но и репутации клиентов, снижая негативные последствия от угроз и противодействуя возникновению новых атак. FortiSIEM является развитием известной и зарекомендовавшей себя на рынке SIEM-системы компании AccelOps, которую Fortinet приобрела в 2016 году. Fortinet добавила к классической SIEM-системе ряд своих запатентованных технологий: распределенной корреляции событий в режиме реального времени; автоматизированного обнаружения инфраструктуры и приложений (CMDB); настраиваемой обработки журналов. FortiSIEM поддерживает интеграцию со сторонними устройствами, опрашивая инфраструктуру о возникающих событиях безопасности, логах, производительности и т. д. При этом FortiSIEM позволяет общаться с внешними системами управления уязвимостями и оповещения об обнаруженных уязвимостях и таким образом расширять возможности по противодействию и защите от них. FortiSIEM является частью фабрики безопасности Fortinet Security Fabric, то есть другие средства защиты Fortinet могут быть интегрированы с FortiSIEM и обмениваться с продуктом информацией, в том числе и об обнаруженных уязвимостях [9].

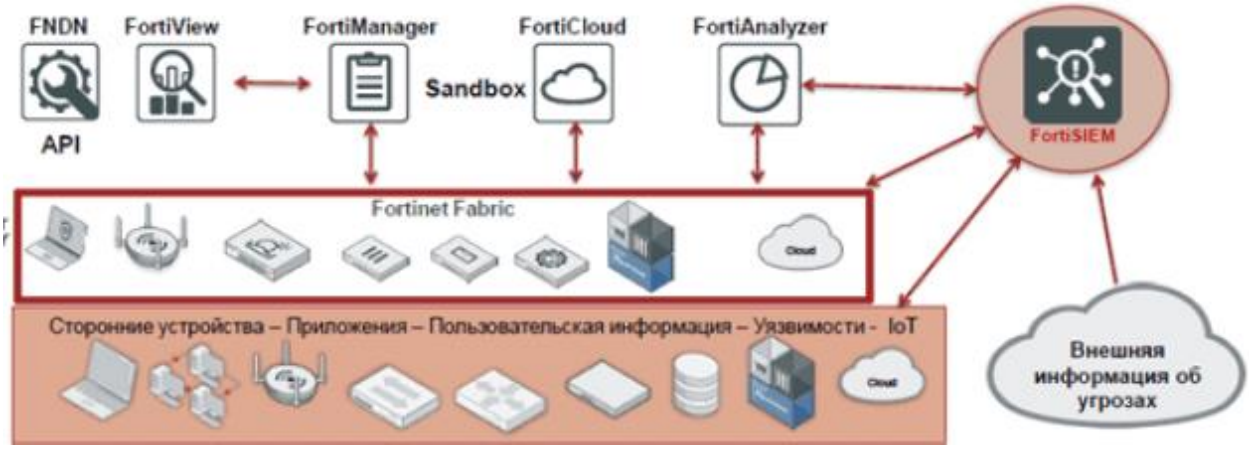

Рисунок 12 – FortiSIEM в концепции

Система FortiSIEM располагается на границе отдельных технологий SOC (Security Operations Center) и NOC (Network Operations Center), позволяя использовать кросс-корреляцию информации от одного и от другого и

повысить эффективность взаимодействия между SOC и NOC, снижая время на расследование инцидентов информационной безопасности [9].

FortiSIEM представляет собой комплексное и масштабируемое корпоративное решение, обеспечивающее охват сети от IoT до облака и включающее в себя запатентованные аналитические инструменты, которые обеспечивают эффективное управление сетевой безопасностью и производительностью в режиме реального времени.

Рассмотрим основные возможности FortiSIEM.

Масштабируемый и гибкий сбор журналов:

- сбор, обработка, хранение, нормализация, индексирование и корреляция событий безопасности с поддержкой десятков тысяч событий в секунду (один супервизор — в едином исполнении до 20000 EPS, с возможностью масштабирования до необходимого объема);
- поддержка большого количества систем безопасности и API поставщиков (локальных и облачных);
- сбор событий при помощи агентов Windows, мониторинг целостности файлов, изменений установленных программ и изменений реестра; мониторинг целостности файлов при помощи агентов Linux;
- создание и изменение средств синтаксического анализа (шаблонов XML) в рамках графического интерфейса и предоставление доступа другим пользователям при помощи функции экспорта/импорта.

Уведомление и управление инцидентами:

- построение инфраструктуры уведомления об инцидентах на основе политик; возможность запуска сценария обновления в случае возникновения указанного инцидента;
- интеграция на основе API с внешними системами отправки запросов — ServiceNow, ConnectWise и Remedy;
- встроенная система отправки запросов. Предоставление пользователю полнофункциональных настраиваемых панелей мониторинга: настраиваемые в режиме реального времени панели мониторинга с функцией прокрутки слайд-шоу для демонстрации ключевых показателей эффективности;
- генерация отчетов и аналитических данных, доступных для коллективного использования сотрудниками организаций и пользователями;
- цветовая маркировка для оперативного выявления критических проблем;
- специализированные многоуровневые панели мониторинга для бизнес-служб, виртуализированных инфраструктур и специальных приложений.

Интеграция внешних данных об угрозах:

- предоставление API для интеграции внешних источников данных об угрозах — доменах с вредоносными программами, IP-адресах, URL-адресах, хэшах, узлах Tor;
- интеграция популярных источников данных об угрозах — ThreatStream, CyberArk, SANS, Zeus;

- технология обработки больших объемов данных об угрозах — добавочная загрузка и распространение в рамках кластера, сопоставление шаблонов с сетевым трафиком в режиме реального времени.

Предоставление масштабируемой функции анализа:

- поиск событий в режиме реального времени;

- поиск по ключевому слову и обработанным атрибутам события; поиск исторических событий — запросы по типу SQL с булевыми условиями фильтрации, группировка по соответствующим агрегированиям, фильтрация в зависимости от времени суток, сопоставление регулярных выражений, вычисляемые выражения — графический интерфейс и API;

- триггер для шаблонов сложных событий в режиме реального времени; использование обнаруженных объектов CMDB, данных пользователя/удостоверения и сведений о расположении в процессе поиска и создания правил;

- планирование составления отчетов и доставка результатов ключевым сотрудникам с помощью электронной почты; поиск событий в рамках всей корпоративной сети либо физического или логического домена составления отчетов;

- динамически изменяющиеся списки отслеживания, предназначенные для выявления критических нарушений — поддерживается использование списков отслеживания для создания правил составления отчетов; масштабирование каналов аналитических данных за счет добавления рабочих узлов без простоя;

- возможность развертывания функции определения приоритета в процессе составления отчетов об инцидентах с помощью критических бизнес-служб.

Архитектура FortiSIEM (показана на рисунке 13) представляет собой иерархическую структуру, которая строится на базе различных элементов в зависимости от местоположения системы (собственная инфраструктура, облако, ЦОД) и объема обрабатываемых данных [9].

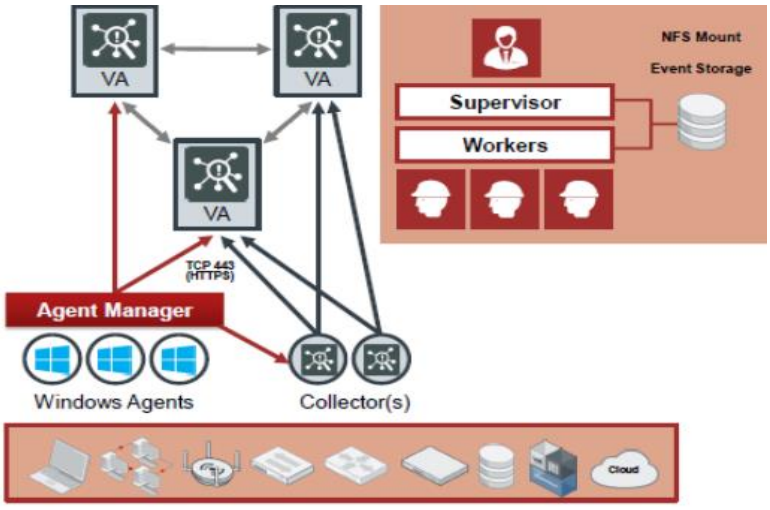

Рисунок 13 – Архитектуры FortiSIEM

Основным элементом FortiSIEM является супервизор (Supervisor), на котором располагаются все службы по обработке, веб-сервер, сервер приложений, сервер баз данных, интерфейс решения. Далее идут обработчики (Workers), занимающиеся аналитикой и отвечающие за часть событий безопасности, снимая нагрузку с супервизора. Следующим элементом архитектуры являются коллекторы (Collectors), собирающие и нормализующие события на удаленных узлах для дальнейшей передачи данных с инфраструктуры на обработчики и супервизор [9].

2.2 Внедрение SIEM системы

В настоящее время существует множество систем мониторинга сети. Конкуренция среди вендоров систем на фоне роста в казахстане информационных атак на информационные системы , привели к масштабному внедрению такой системы как “SIEM” [10].

Сценарии внедрения FortiSIEM Архитектура FortiSIEM предполагает ряд вариантов внедрения для предприятий любого масштаба и поставщиков услуг. Внедрение автономного супервизора — «Все-в-одном» Это самый простой вариант развертывания, в котором один супервизор осуществляет всю работу по сбору, мониторингу, обработке и анализу данных и отслеживанию возникающих инцидентов безопасности. Супервизор может использовать локальное или NFS-хранилища в зависимости от требований к хранилищу данных событий. Для повышения точности мониторинга на рабочих станциях и серверах могут использоваться Windows Agents и Agent Manager. Схема сценария внедрения супервизора представлена на рисунке 14.

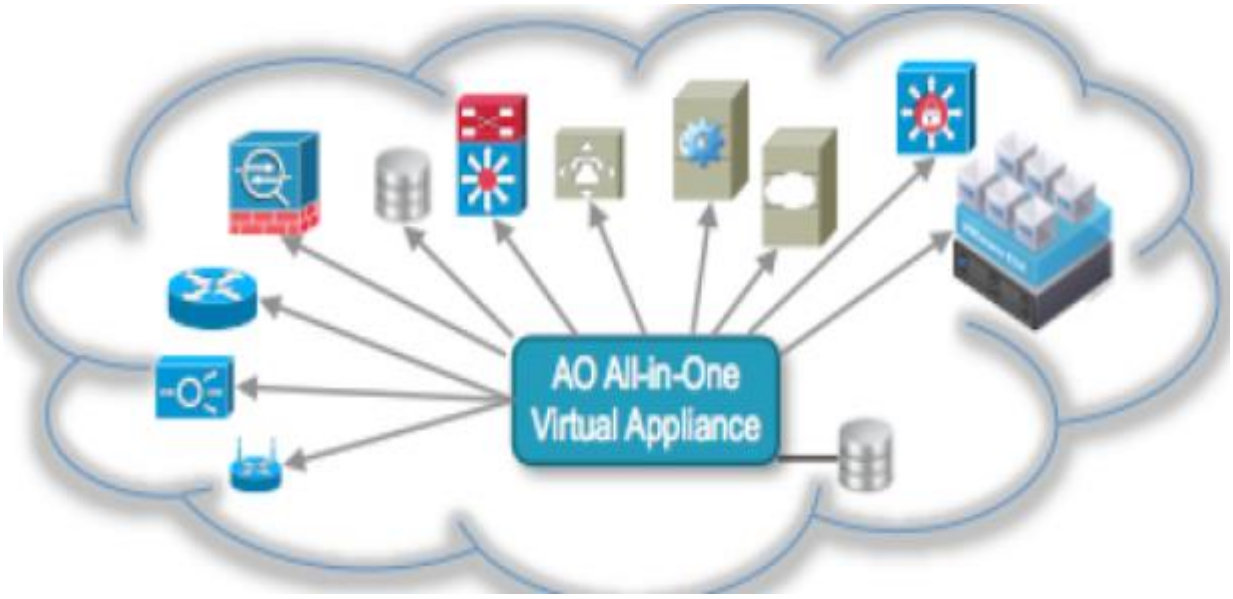

Рисунок 14 – Сценарий внедрения супервизора все в одном

Так как продукт Forti является коммерческим, для получения лицензии необходимо сделать запрос на получение лицензии SIEM-системы. В данном случае был сделан запрос на облачный сервис all-in-all. Процесс получения

доступа показан на рисунке 15. Главная страница облачного сервиса представлена на рисунке 16 [10].

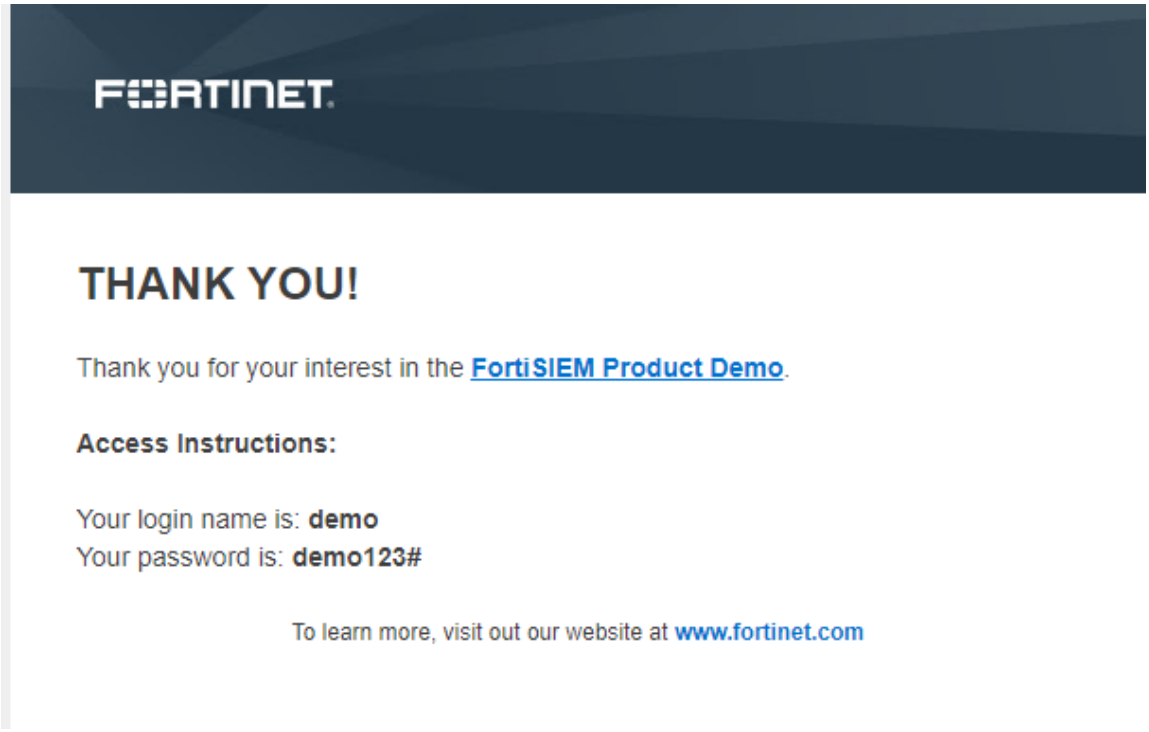

Рисунок 15 – Получение доступа к SIEM

Рисунок 16 – Облачный сервис

2.3 Веб интерфейс системы

Интерфейс позволяет осуществлять текущий мониторинг событий на любом устройстве, на крупных экранах и плазменных панелях. Отображение выполняется по панелям (Dashboard) или инцидентам (Incidents) и различным критериям. Этот раздел показывает полное представление обо всех компонентах, таких как серьезность угрозы, уязвимости в сетевом узле,

состояние развертывания, карты рисков и статистика OTX. Подменю дашборда показаны на рисунках 17 и 18.

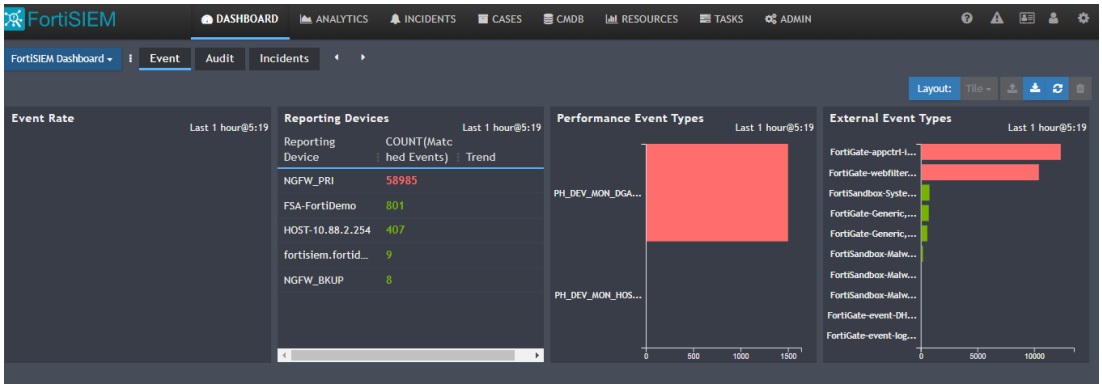

Рисунок 17 – Dashboard

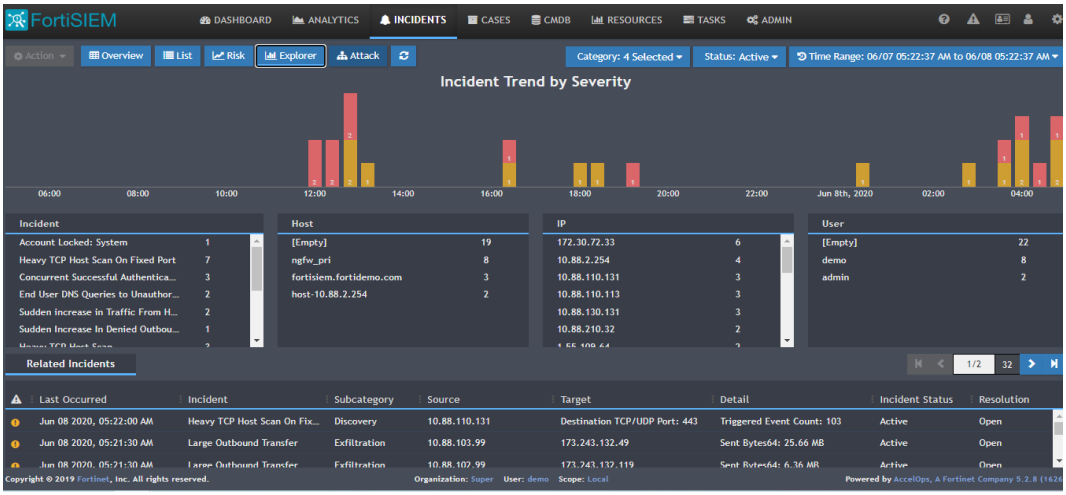

Рисунок 18 – Инциденты

Следующее окно появится в настройках личных данных. Сменим пароль и имя пользователя и заполним контактные данные для оповещения о событиях ИБ на рисунках 19-20.

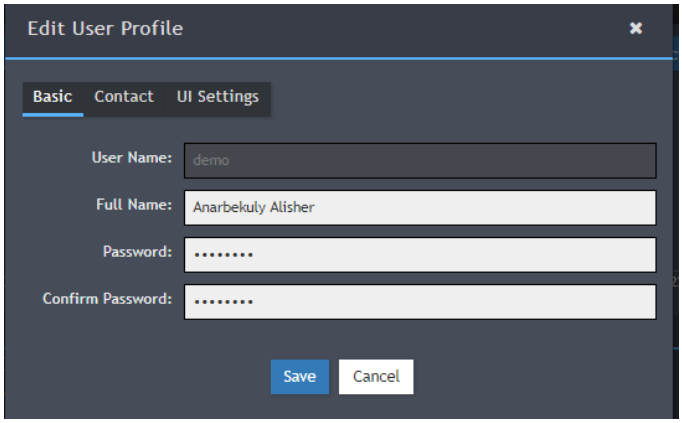

Рисунок 19– Смена пароля

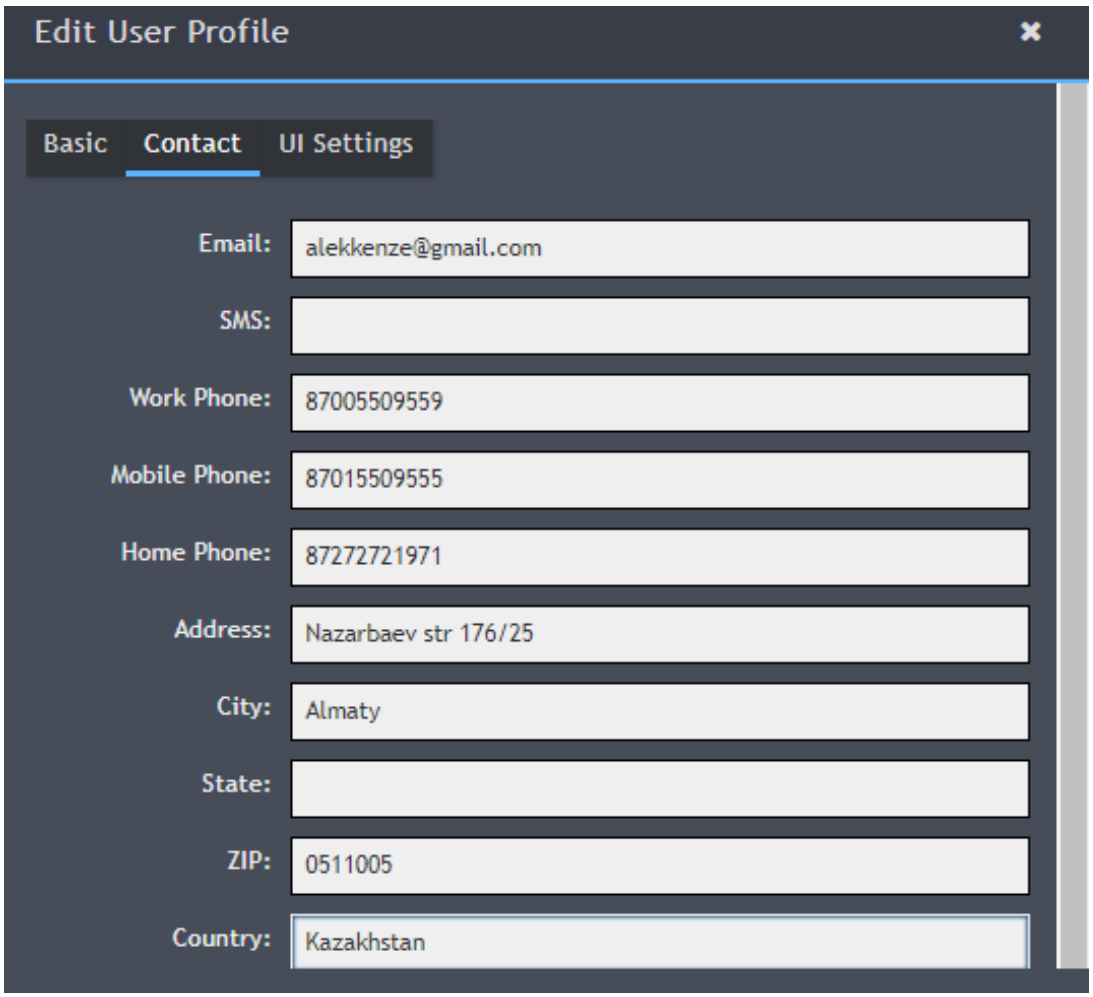

Рисунок 20 – Заполнение данных

Панель инструментов виджетов отображает графическое представление отчетов FortiSIEM. Отчеты могут быть из данных CMDB или данных событий. Отчеты могут быть агрегированными отчетами типа Top N или неагрегированными, вероятно, с необработанными сообщениями. Агрегированные отчеты могут отображаться в различных формах: гаджеты, столбики, пончики, таблицы, линии, составные линии, точечные диаграммы, тепловые карты, древовидные карты и геокарты [11].

На данном этапе выполняется автоматическое обнаружение сетевых устройств во вкладке CMDB, представленной на рисунке 21. Оно поддерживает автоматическое и ручное обнаружение устройств.

Есть три типа хостов в системе:

- Windows;
- Linux;
- сетевое устройство.

Обнаружены устройства.: брэндмауэры и машины с ОС Линукс.

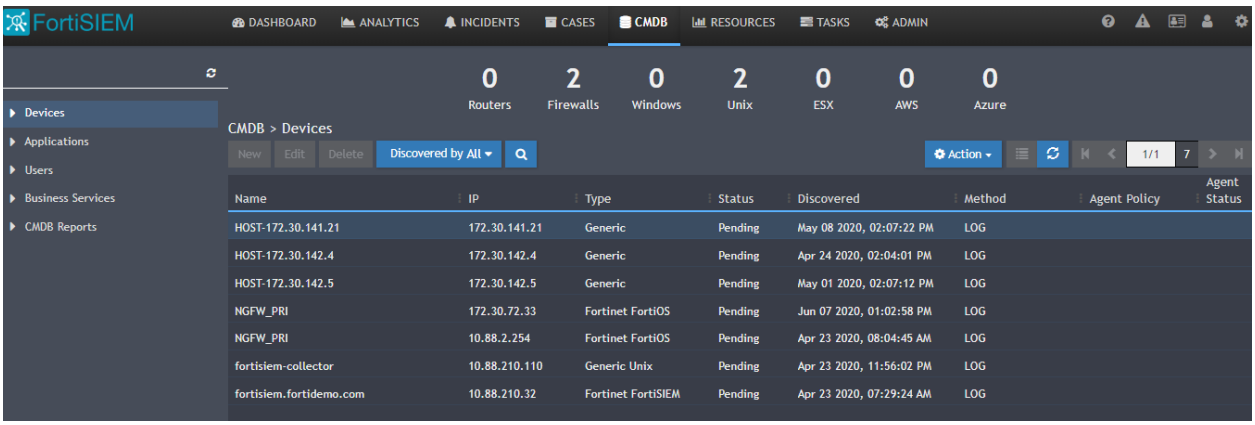

Рисунок 21 – CMDB

Все инциденты разделены по категориям. Приведен ряд возможных инцидентов и составлен топ обнаруженных угроз. По каждой выявленной угрозе создается отчет, один из них представлен на рисунках 22 и 23.

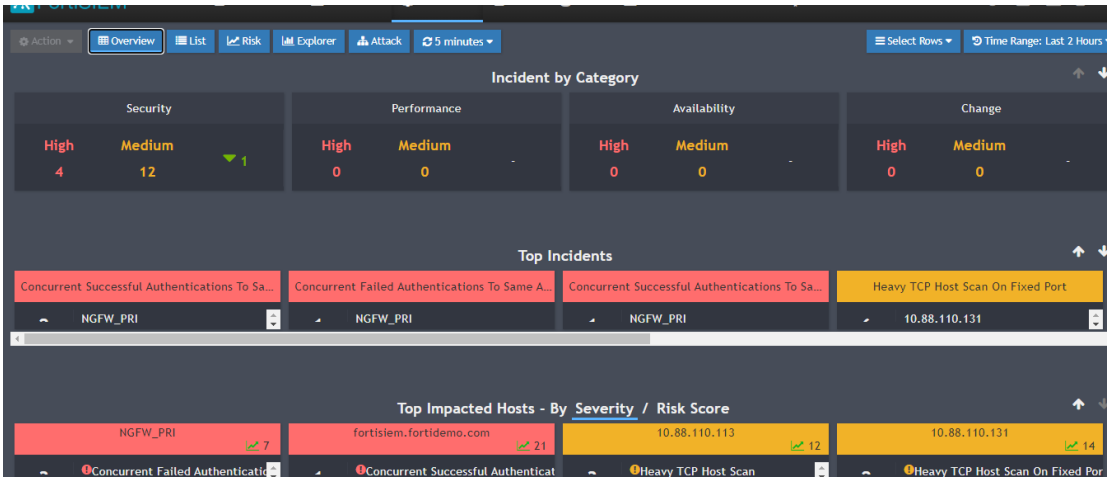

Рисунок 22 – Категории инцидентов

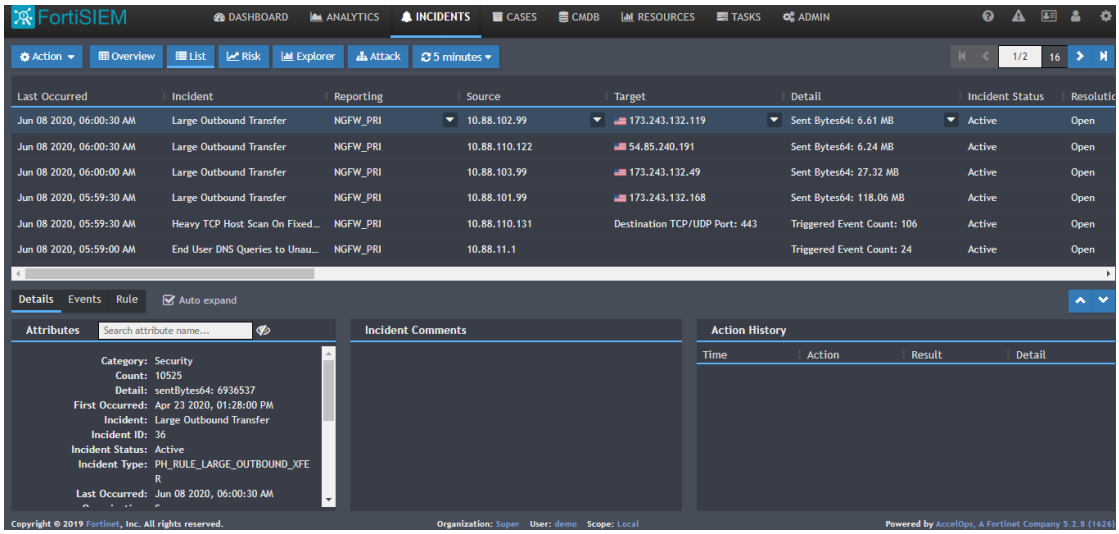

Рисунок 23 – Детали инцидентов

Аналитика является очень важной составляющей любого устройства SIEM. SIEM проанализирует хосты на основе их логов. Это меню показывает сигналы тревоги, SIEM (события безопасности), тикеты и необработанные логи. Меню анализа далее разделено на следующие подменю (показано на рисунке 24).

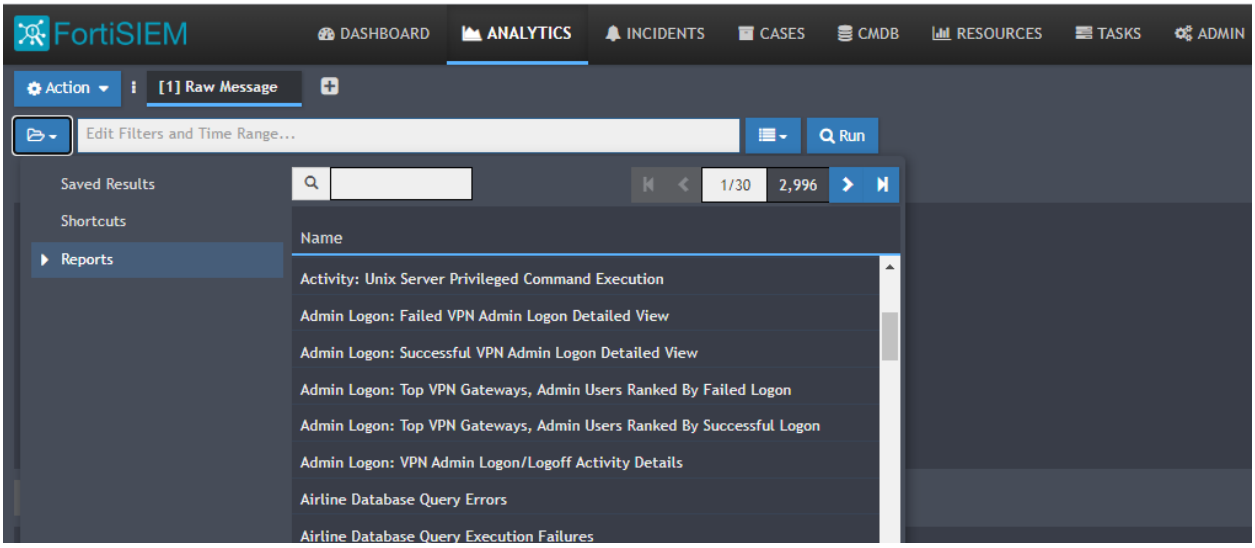

Рисунок 24–Раздел аналитики

2.4 Неавторизованный вход

Осуществим попытку неавторизованного входа в SIEM. Для этого вводится неправильный пароль. Как можно увидеть, через несколько попыток неудачного входа SIEM блокирует аккаунт (приведено на рисунках 25и 26) [11].

Рисунок 25 – Попытка входа

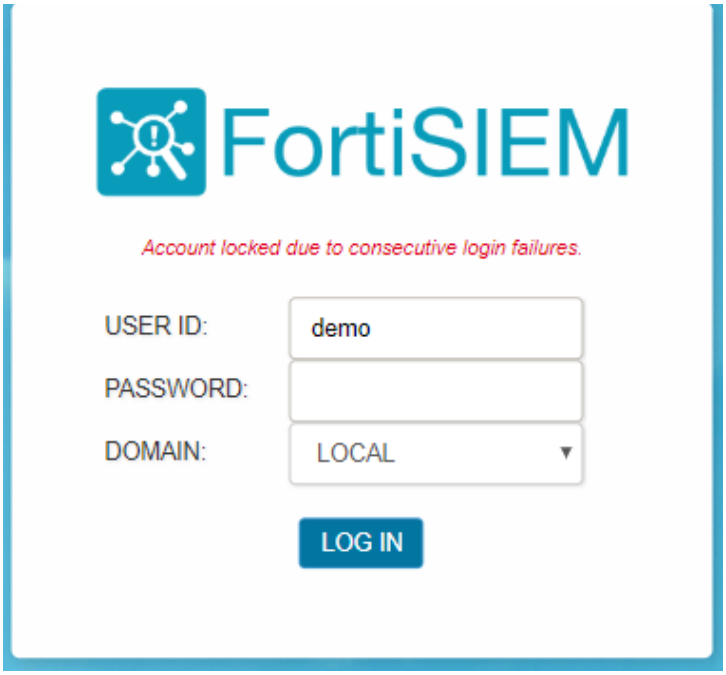

Рисунок 26 – Блокировка аккаунта

Чтобы разблокировать аккаунт необходимо написать письмо в службу поддержки компании Forti. После чего был восстановлен аккаунт и удалось войти в систему. Далее будет разбор инцидента. Во вкладке Dashboard видно, что были осуществлены попытки неудачного входа в систему (рисунок 27). Далее переходим во вкладку инцидентов, для получения подробностей. Детали отчета представлены на рисунках 27 – 32 [11].

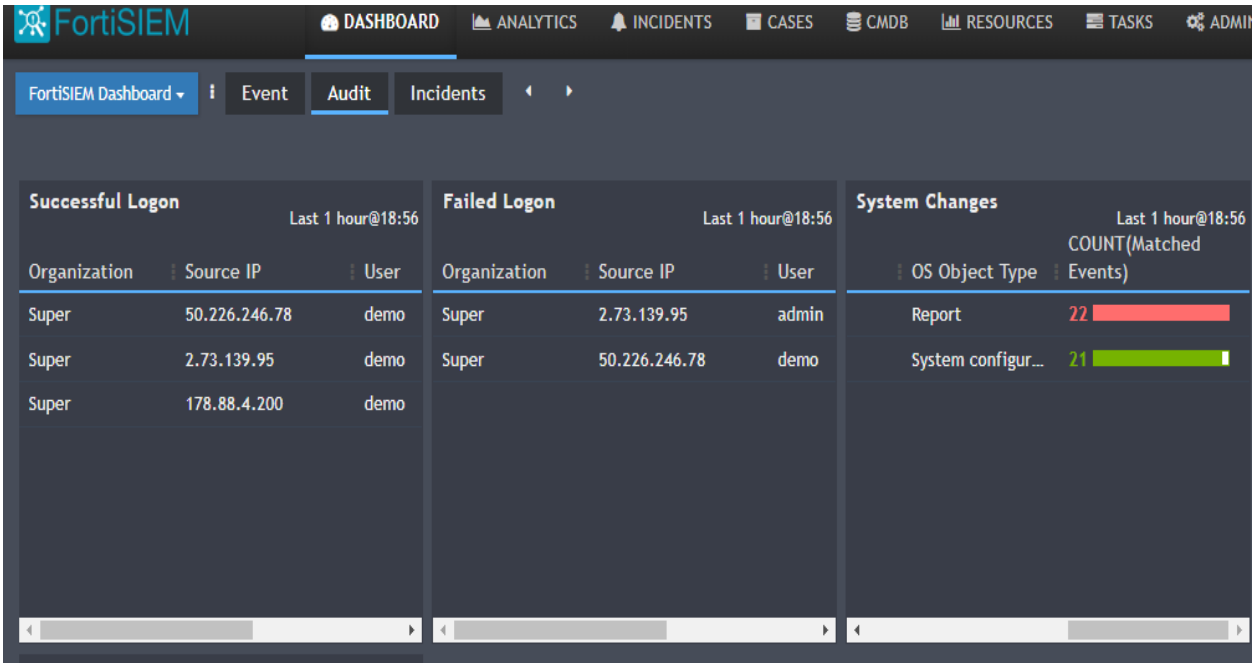

Рисунок 27 – Аудит системы

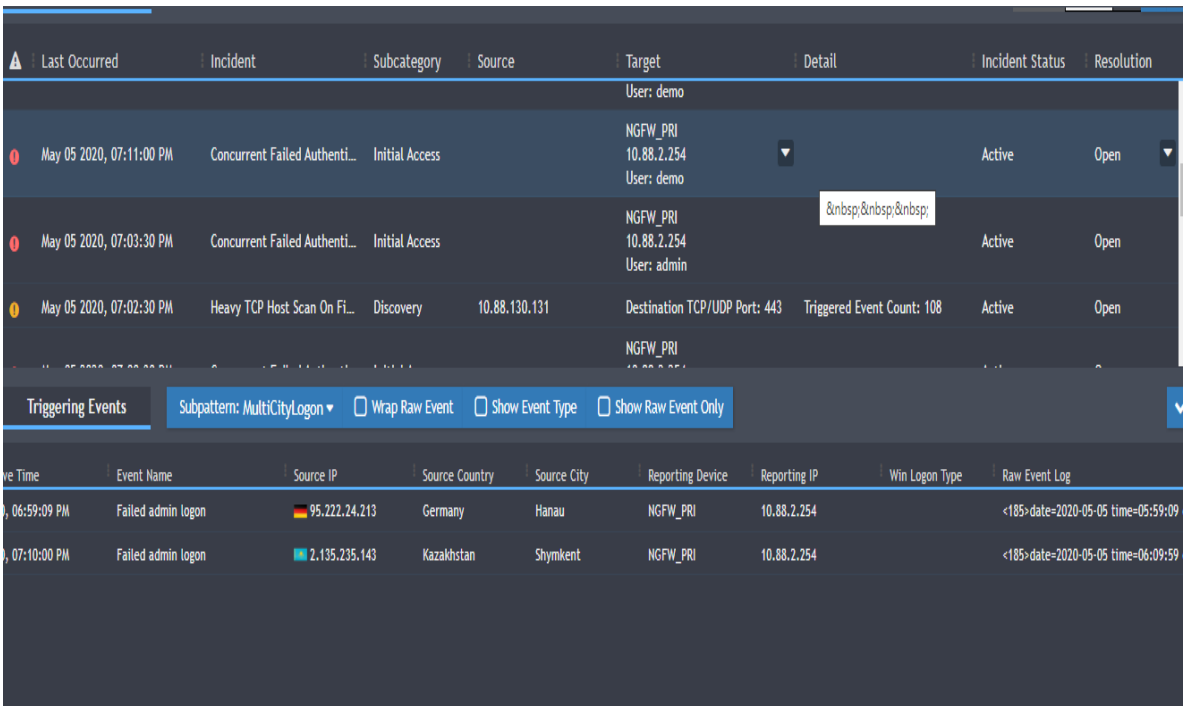

Рисунок 28 – Предупреждение об инциденте

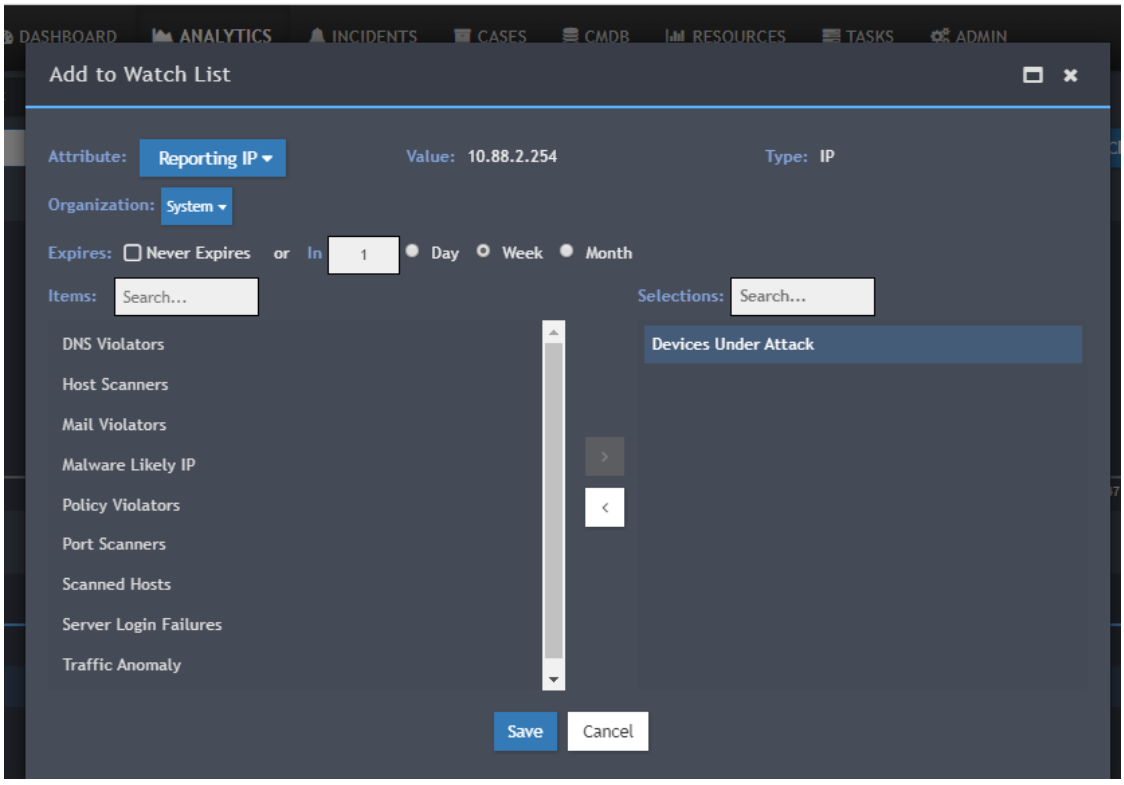

Рисунок 29 – Устройство под атакой

Для выявления нарушителя необходимо создать отчет. Во вкладке аналитики создаем отчет. В отчете указано, что была попытка неудачного входа и предпринятые меры в виде блокировки аккаунта. Создадим логи для подробного просмотра [11].

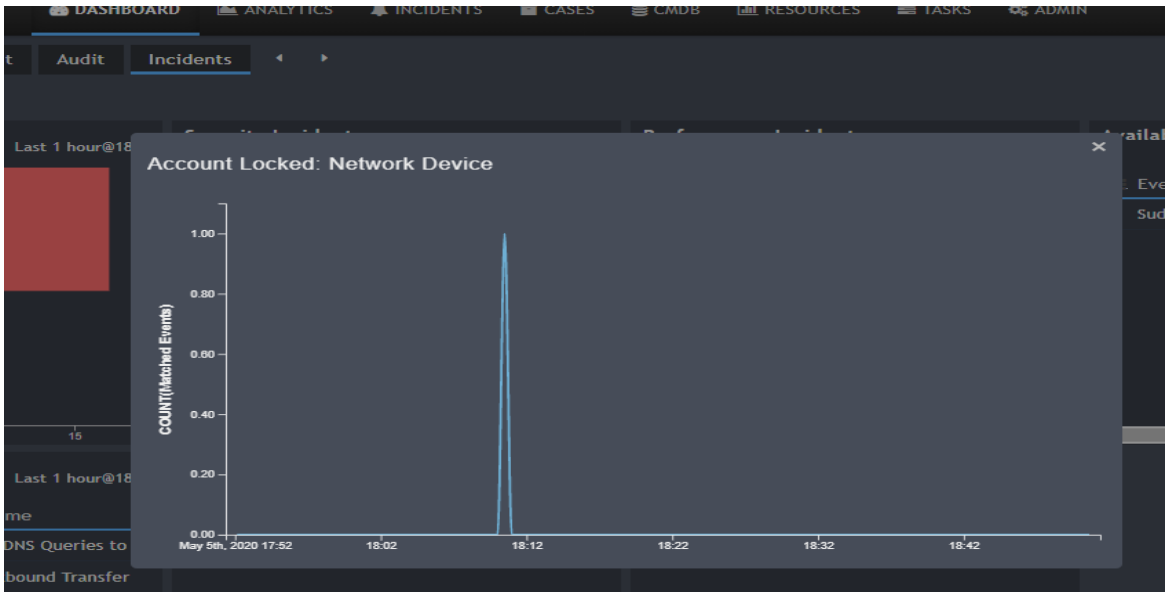

Рисунок 30 – Блокировка аккаунта

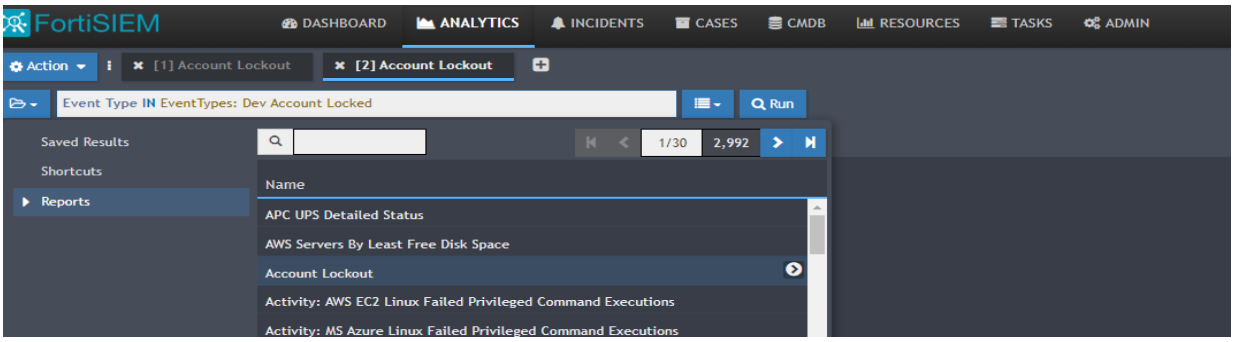

Рисунок 31 – Создание отчета

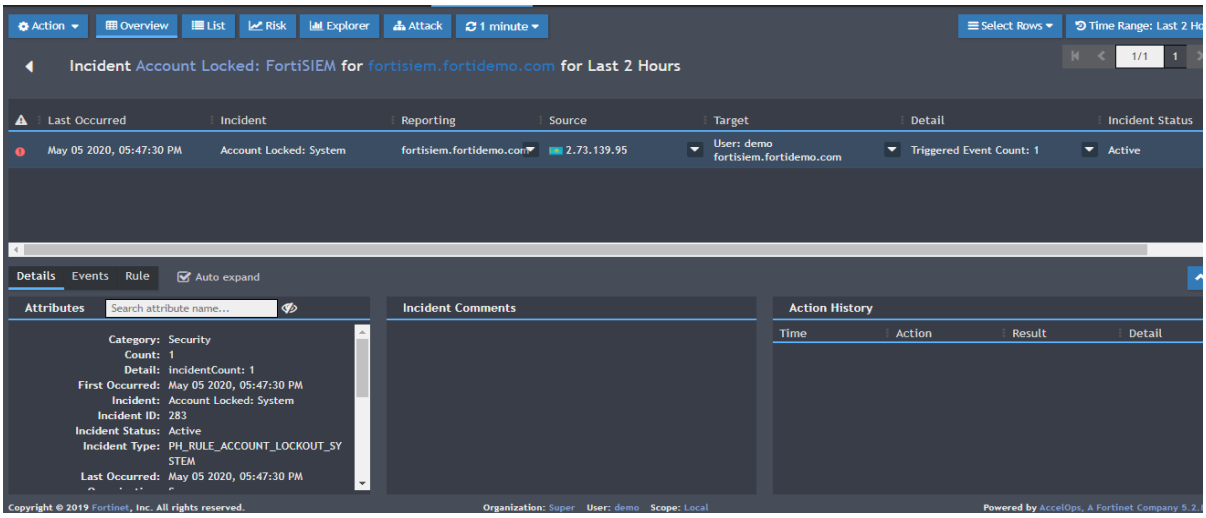

Рисунок 32 – Отчет

В отчете можно увидеть IP-адрес нарушителя. Далее по IP у SIEM есть возможность узнать более подробные данные о нарушителе, что представлено на рисунках 33 и 34.

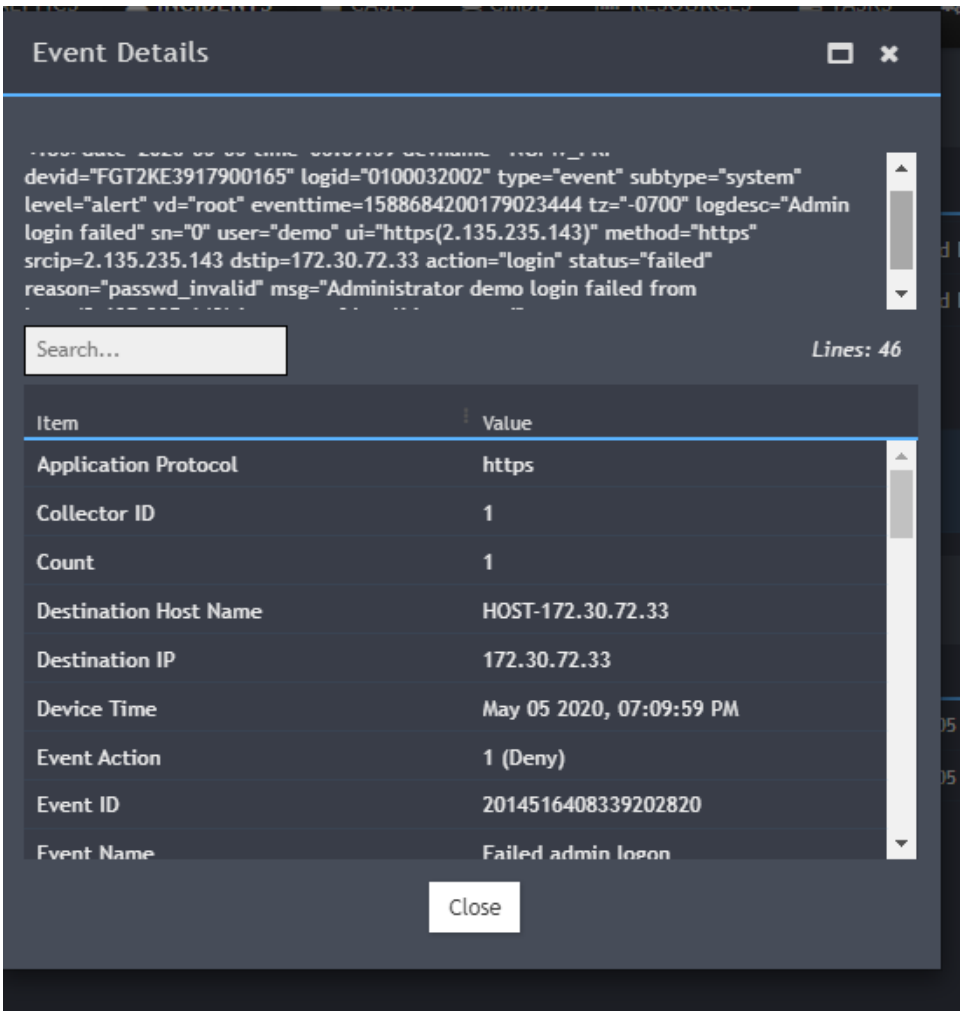

Рисунок 33 – IP нарушителя

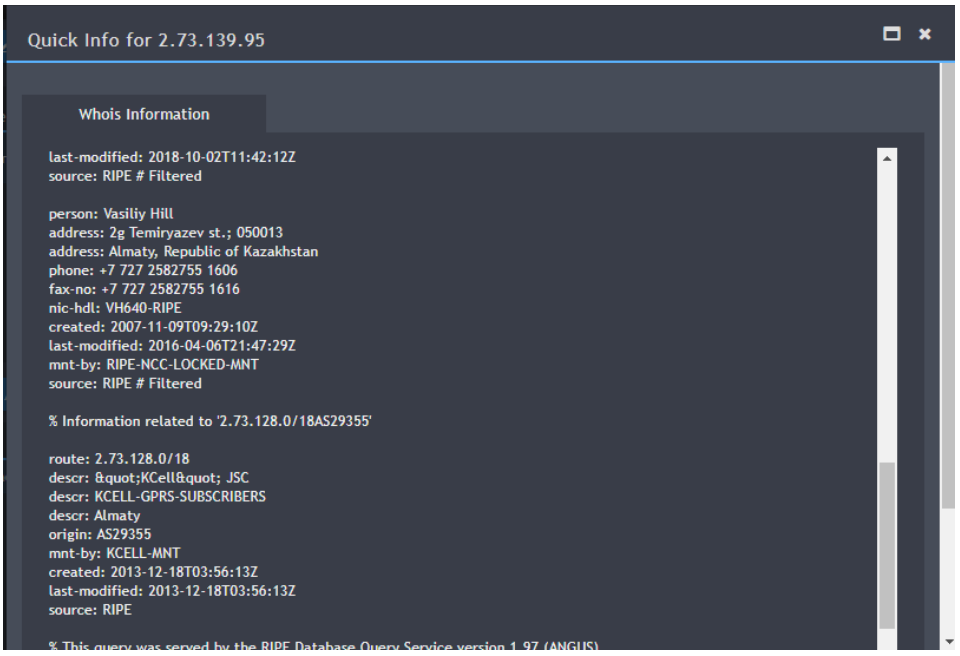

Рисунок 34 – Данные о нарушителе

SIEM система предприняла меры в виде блокировки аккаунта, далее получилось узнать данные о нарушителе. Чтобы избежать последующих блокировок аккаунта, нужно разрешить вход в SIEM только конкретной подсети. Для этого необходимо поднять VPN-сервер. Это даст возможность масштабируемого решения проблем связанных с инцидентом. То есть привлечения сотрудников с различных регионов посредством защищенного подключения VPN.

2.5 Создание VPN-сервера

С помощью обычного Интернет-соединения между устройством и VPN-сервером устанавливается специальное соединение — VPN-туннель. Все передаваемые и получаемые данные в этом соединении шифруются. С этого момента вся ваша сетевая активность осуществляется через данный туннель, а не через основной канал провайдера, и появляется возможность для авторизованного входа в SIEM.

Для того, чтобы создать VPN-сервер, необходимо арендовать виртуальный сервер (Virtual Private Server) у одного из хостинг-провайдеров. На него нужно установить Linux и затем настроить его. Из наиболее популярных на сегодняшний день глобальных хостинговых компаний можно выделить следующие:

- Amazon Web Services;
- DigitalOcean;
- Hetzner;
- Vultr;
- Bluehost;
- Arubacloud.

Выбор пал на Amazon Web Services (AWS). В основном, из-за известности бренда, большого количества доступных географических зон для размещения сервера и высокой стабильности. На самом деле, многие популярные интернет-сервисы работают на базе AWS, арендуя там сервера для своих нужд, например, Facebook. Компания AWS была пионером в облачных технологиях и, по сути, открыла эту отрасль. Сегодня AWS предоставляет множество решений для облачных вычислений на любой вкус и цвет, но для дальнейшего выполнения нужна обычная виртуальная машина. Для этого можно воспользоваться одной из разработок AWS: Lightsail.

Lightsail — это упрощенное решение для создания виртуальных серверов, в отличие от своего старшего собрата EC2. Всё завернуто в очень простой интерфейс, в котором разберется даже новичок, поэтому для цели — создания VPN-сервера, AWS Lightsail подходит лучше всего.

Подниматься VPN-сервер будет на основе операционной системы Linux Debian, а не Linux Ubuntu, которую довольно часто используют. Ubuntu изначально создавалась именно как пользовательская система, а не серверная. Debian же надежен и стабилен. Установка показана на рисунке 35 [12]..

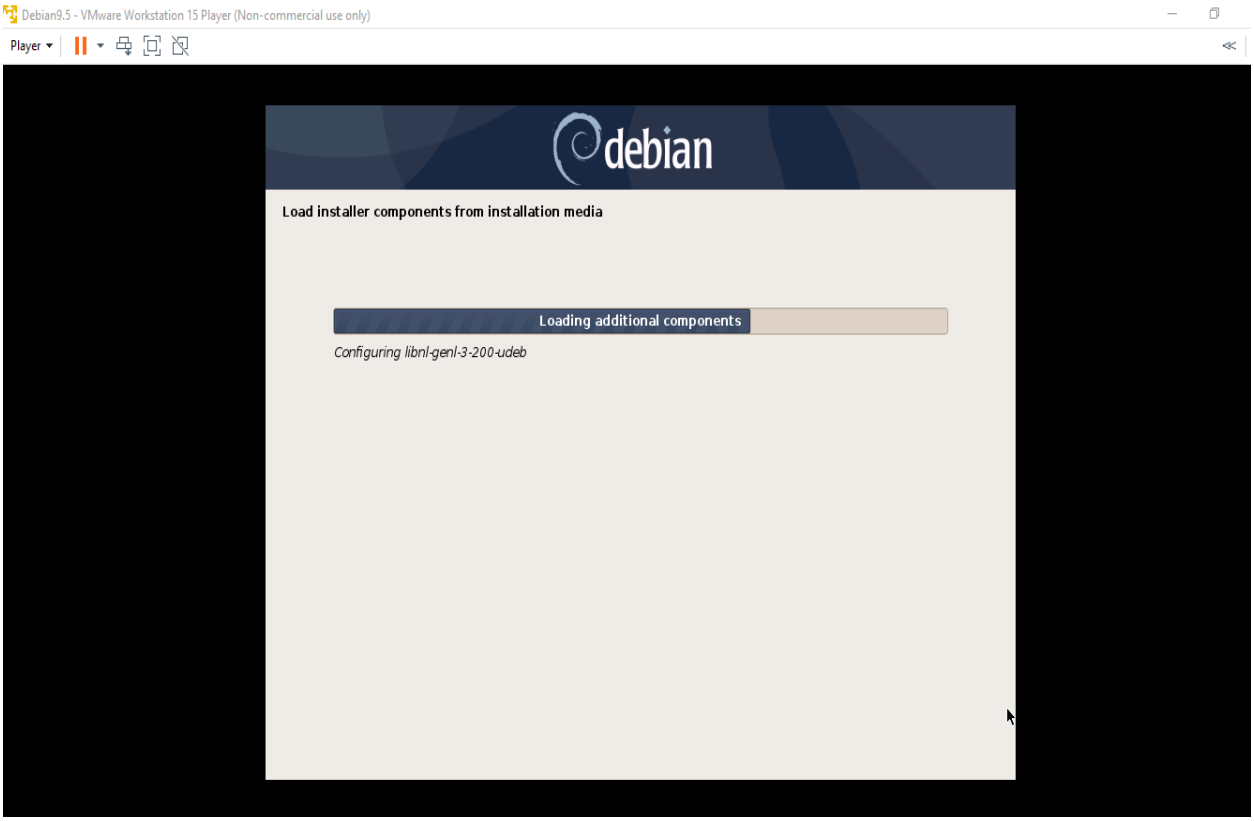

Рисунок 35– Установка Debian 9.5

На сегодняшний день существуют разные протоколы VPN-соединения.. Среди них наиболее популярны IPsec IKEv2 и OpenVPN. Оба протокола хороши и надежны, но будет использоваться IKEv2, поскольку у OpenVPN имеется существенный недостаток, который перекрывает его прочие достоинства. OpenVPN требует установки своего приложения, которое всегда должно быть запущено на устройствах, что, во-первых, неудобно в использовании, а во-вторых, дополнительно расходует батарею iPhone, iPad и, в меньшей степени, Mac. IKEv2 же «вшит» в iOS и macOS и является для них нативным, не требуя установки никакого дополнительного ПО. В качестве серверной части мы будем использовать strongSwan — популярный VPN-сервер для Linux.

Таким образом, VPN-сервер будет подниматься, используя следующие технологии:

- AWS Lightsail в качестве виртуального сервера;
- IKEv2 как протокол VPN;
- Linux Debian в качестве серверной ОС;
- strongSwan в качестве VPN-сервера.

После регистрации необходимо перейти в Lightsail, выберать гео-зону в которой необходимо поднять VPN-сервер. Был создан новый инстанс, и выбран «OS Only» и операционную систему Debian 9.5 (рисунок 36).

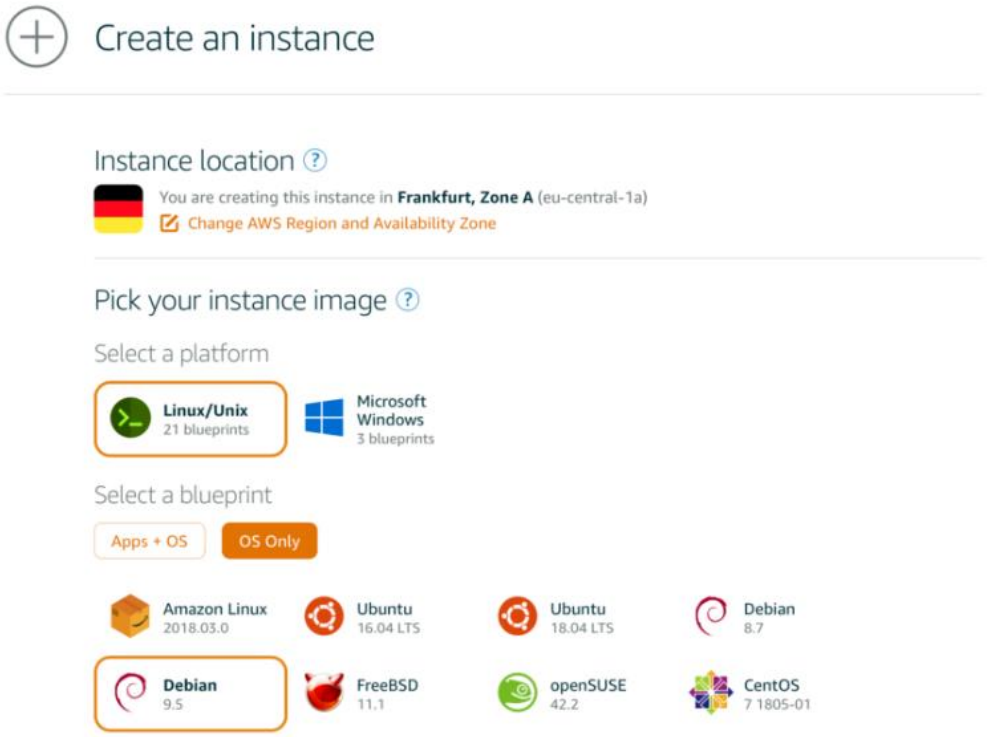

Рисунок 36 – Выбор Debian

Некоторые сайты (например, Авито) необоснованно блокируют визиты с IP-адресов популярных хостеров, считая, что последние часто принимают участие в DDOS-атаках. Чтобы этого не происходило и чтобы не делили один IP-адрес с тысячами других машин AWS, нужно перейти в «Networking» и выделить Static IP. Назначим его на созданный инстанс (рисунок 37).

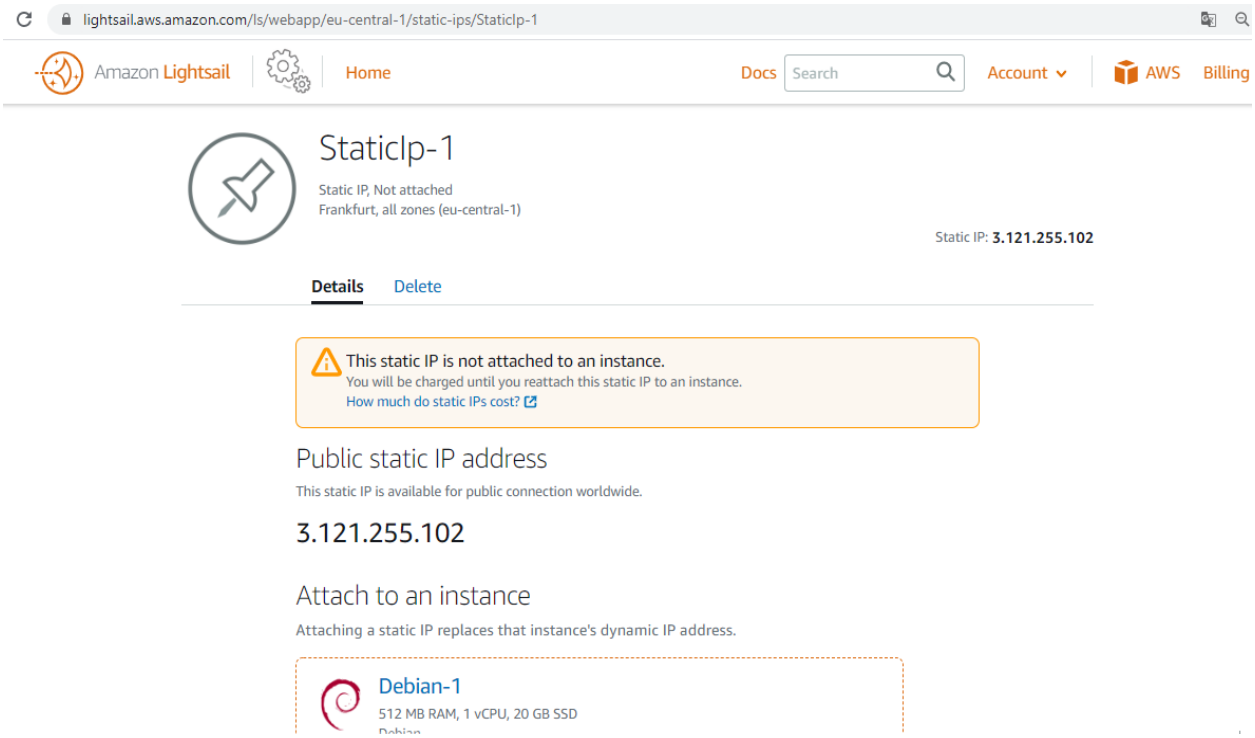

Рисунок 37 – Выделение статического адреса

Далее необходимо скачать SSH key, для клиента сервера. В дальнейшем подключение к серверу без ключа не будет доступна

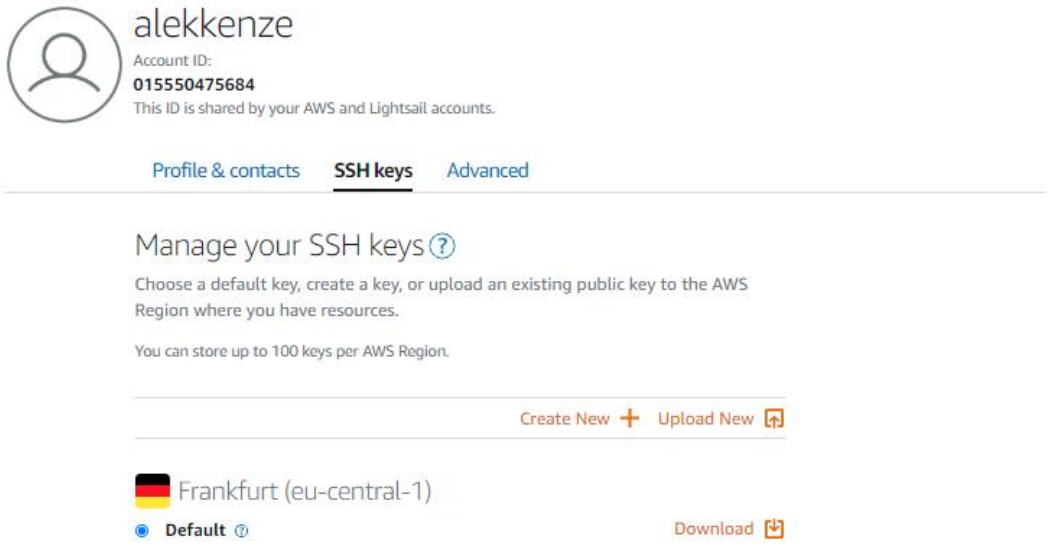

Рисунок 38 – Загрузка ключа SSH

Далее все настройки будут осуществляться в Debian. Переходим ОС Линукс. Необходимо зайти под супер пользователем. Для начала нужно установить StrongSwan (рисунок 39).

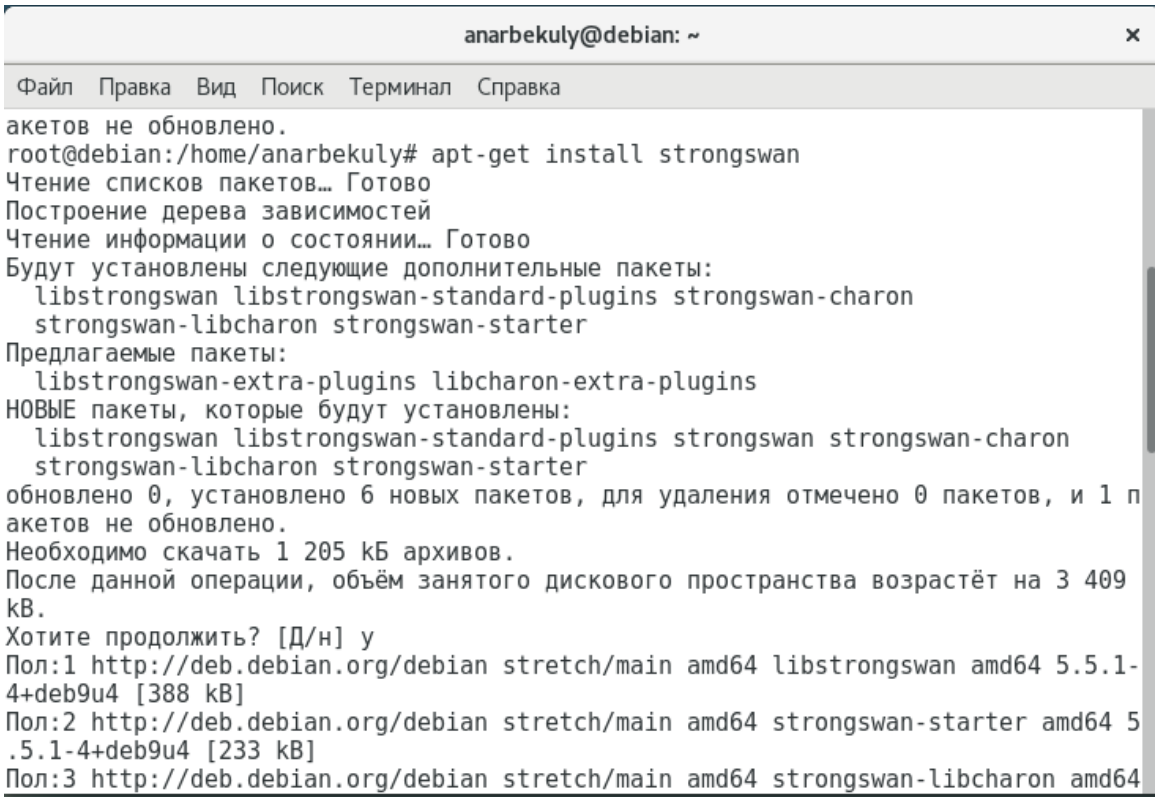

Рисунок 39 – Установка StrongSwan

К детальной настройке strongSwan чуть позже, а пока будут созданы сертификаты, чтобы устройства смогли подключиться по VPN. Будут использоваться самозаверенные сертификаты, поскольку VPN-сервером планируем будет использован только доверенные пользователи SIEM. Для того чтобы создать сертификаты, потребуется пакет strongswan-pki. Его установка указана на рисунке 40.

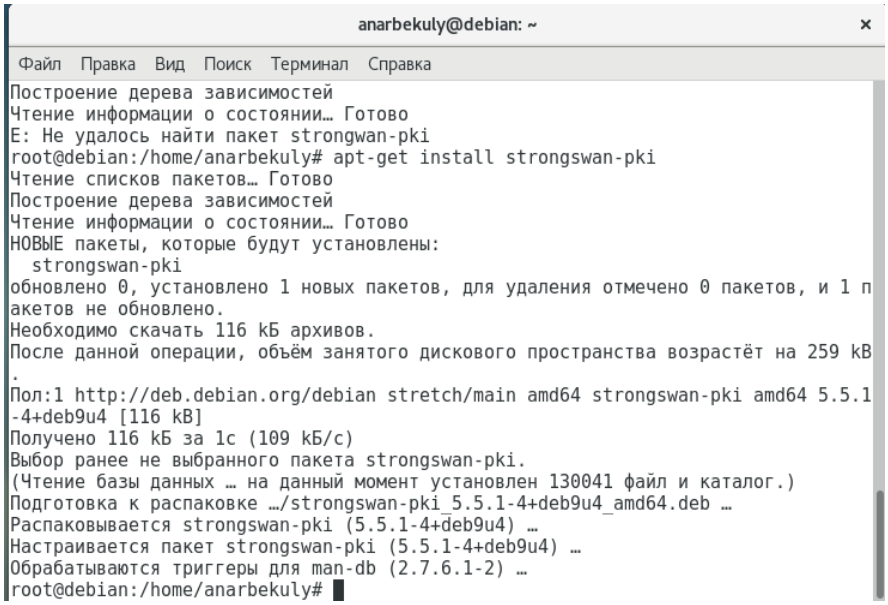

Рисунок 40 – Добавление пакетов strongSwan.pki

Далее необходимо создать сертификаты. В первую очередь нужно создать корневой сертификат, он же “CA” (Certificate Authority), который выпустит остальные сертификаты. Создается в файле ca.pem (рисунок 41).

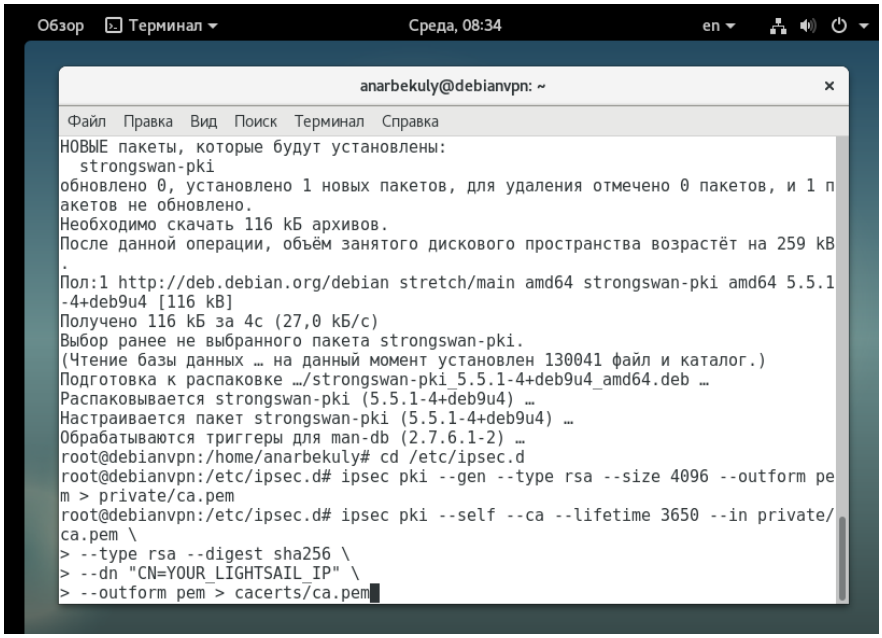

Рисунок 41 – Создание сертификата CA

Дальше необходимо создать сертификат для VPN-сервера в файле debian.pem (рисунок 42).

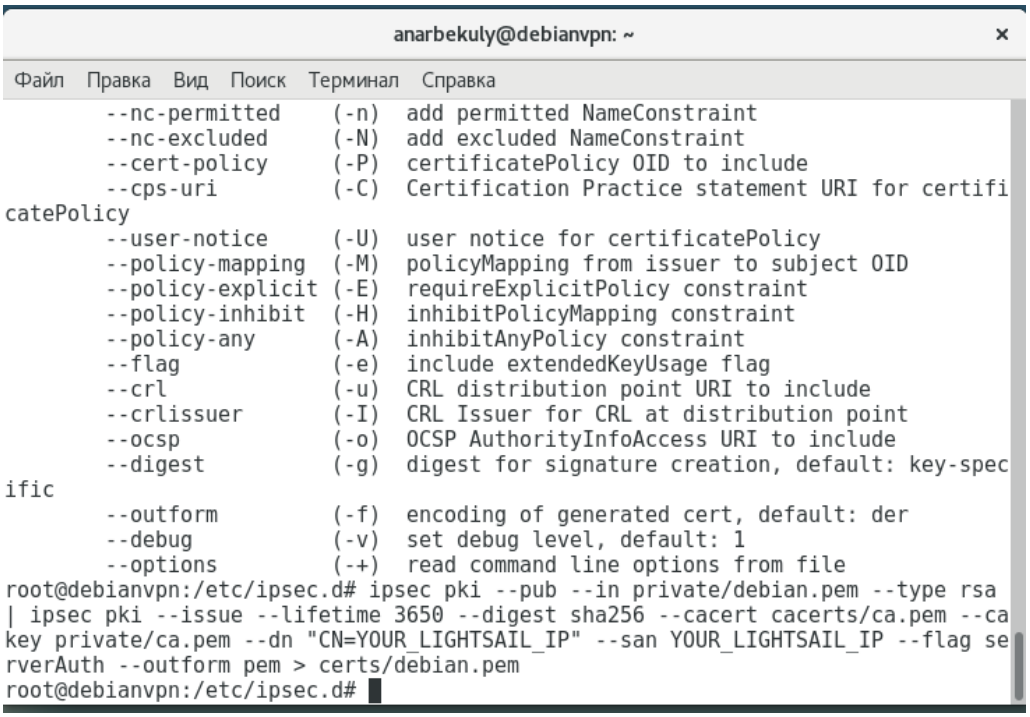

Рисунок 42 – Успешная установка

А теперь, будет создан сертификат для устройств в файле me.pem (рисунок 43).

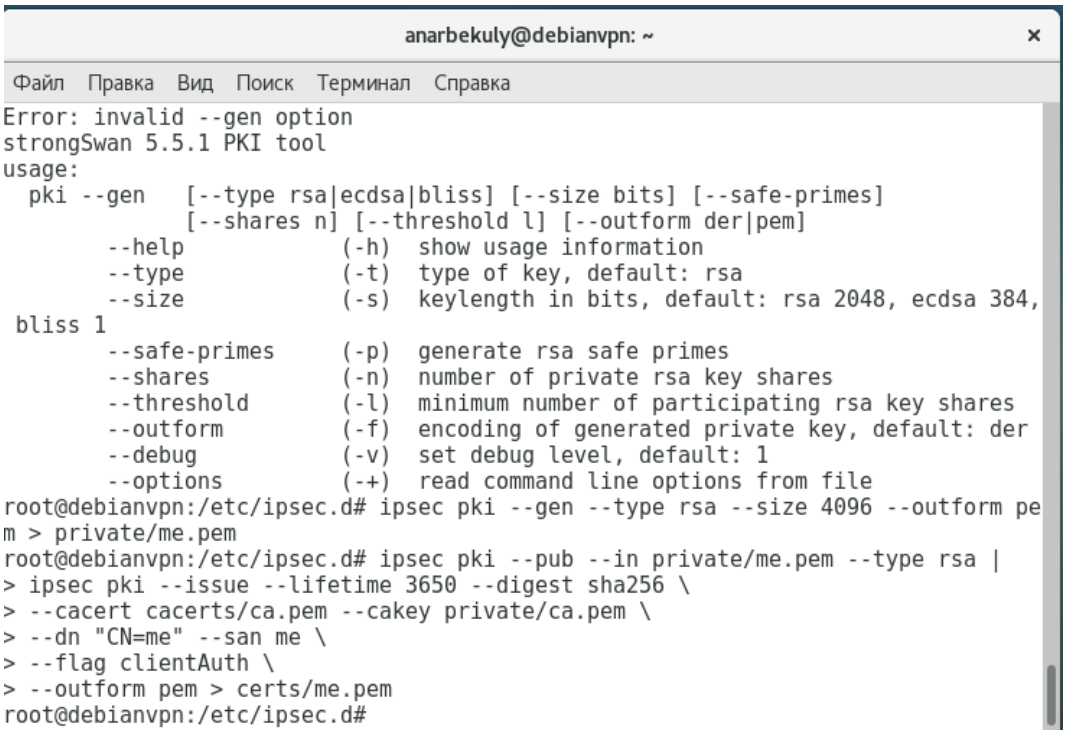

Рисунок 43 – Создание сертификата для устройств

На этом создание сертификатов закончено. Далее будет производиться настройка strongSwan. Вставим внешний IP-адрес машины в AWS Lightsail на рисунке 44.

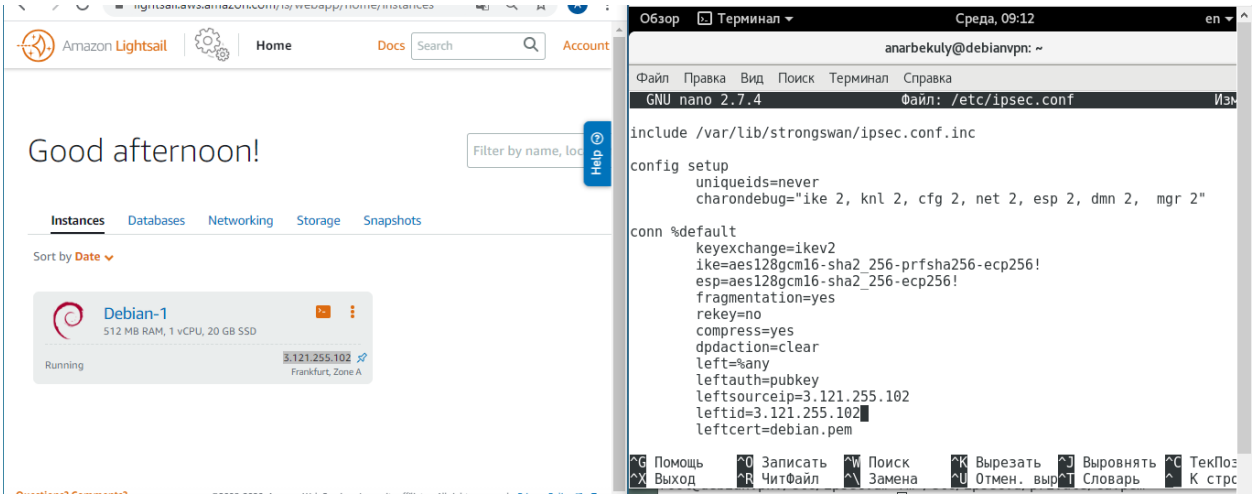

Рисунок 44 – Настройка strongSwan

После сохранения файла идет добавление указателей на сертификат сервера в файл ipsec.secrets, являющийся хранилищем ссылок на сертификаты и ключи аутентификации (рисунок 45).

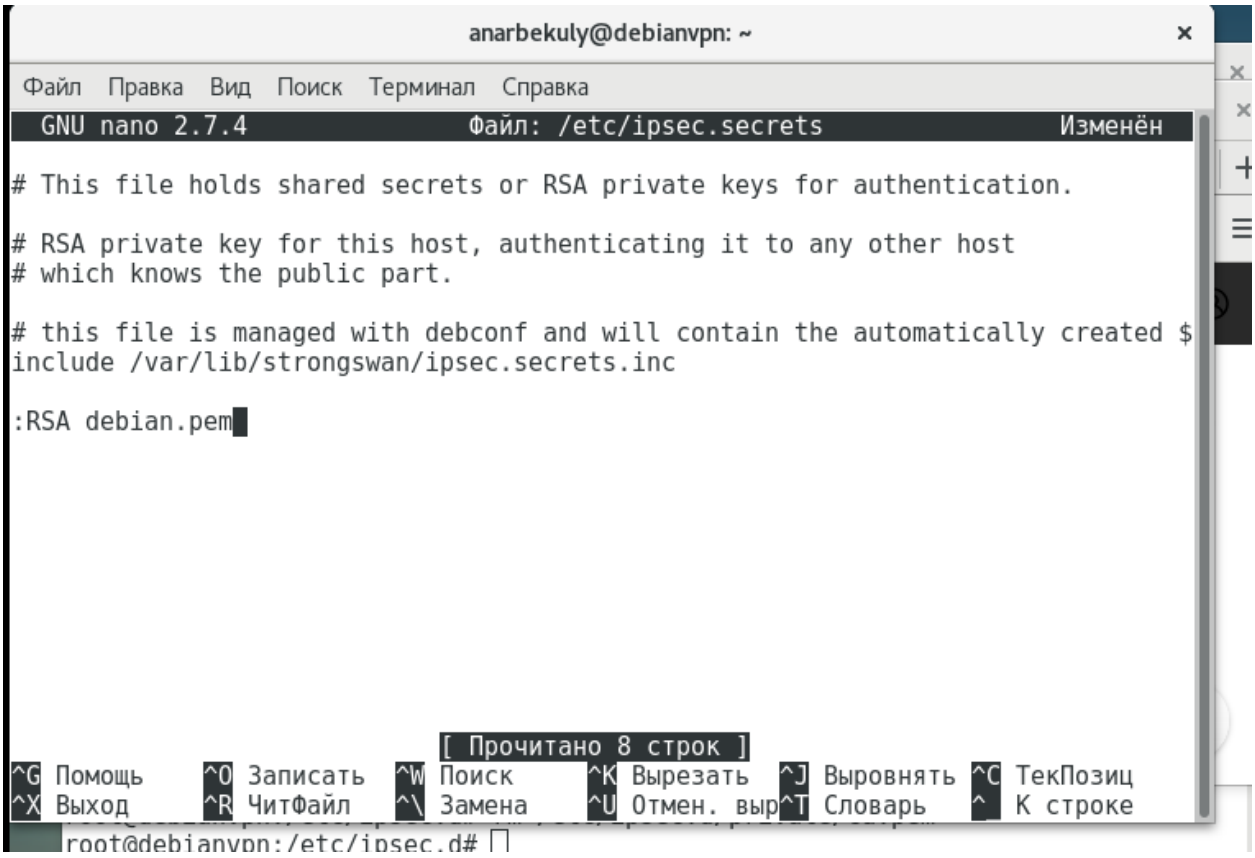

Рисунок 45 – Добавление ссылки на сертификат

Настройка strongSwan завершена. При перезапуске системы видно, что сервер запустился (рисунок 46). Далее необходимо настроить сетевые параметры ядра (рисунок 47).

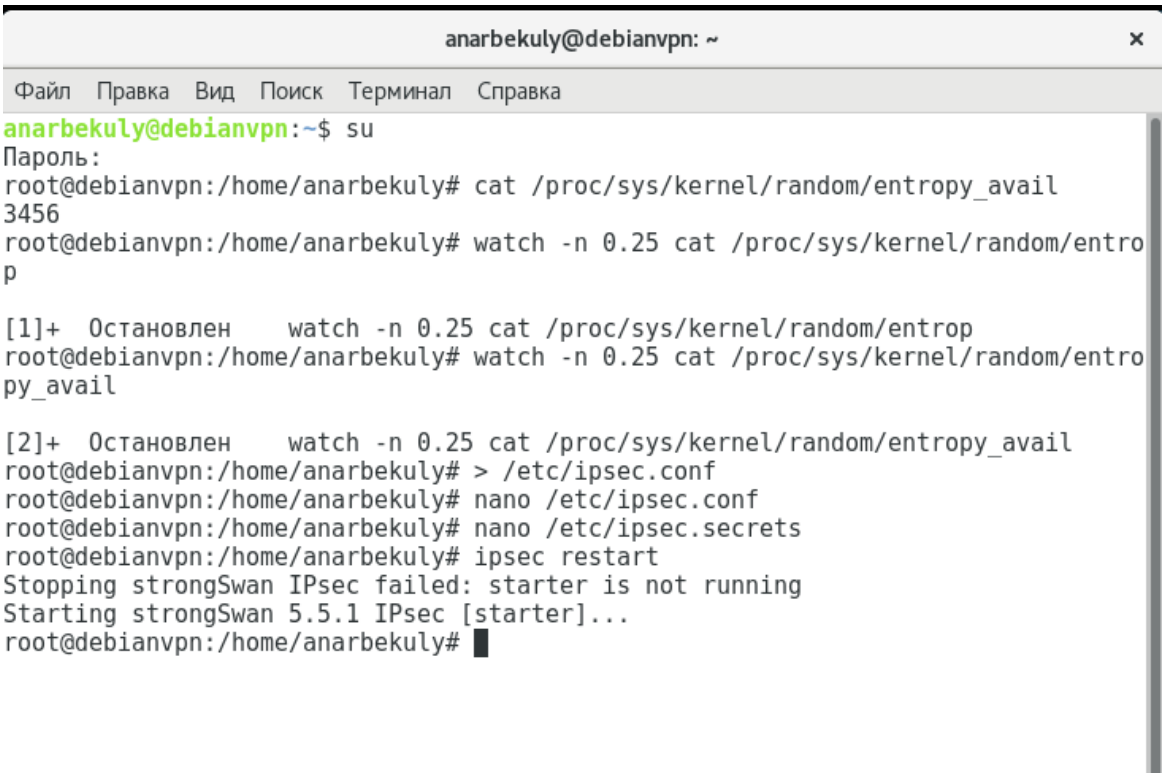

Рисунок 46 – Запуск сервера

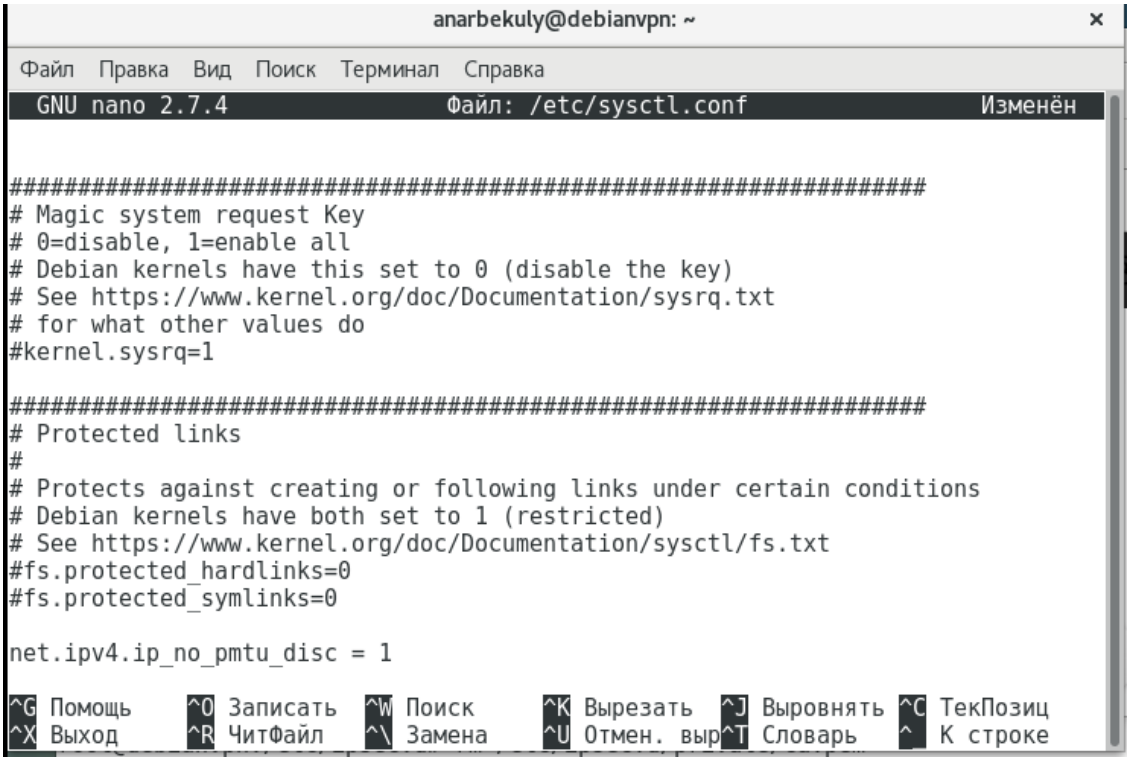

Рисунок 47 – Сетевые параметры ядра

На этом настройка сетевых параметров ядра закончены. Далее будет произведена настройка Iptables. Iptables — это утилита, которая управляет встроенным в Linux файрволом netfilter. Для того, чтобы сохранять правила iptables в файле и подгружать их при каждом запуске системы, нужно установить пакет iptables-persistent (рисунок 48).

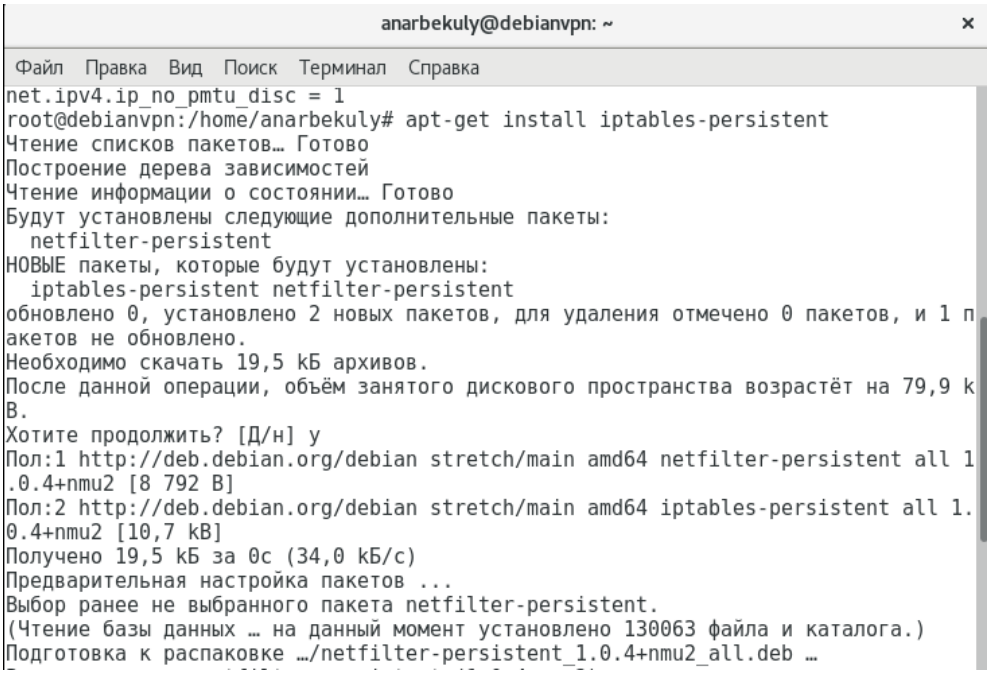

Рисунок 48 – Установка пакета iptables-pertsistent

Далее формируются правила iptables. Для начала нужно очистить все цепочки (рисунок 49).

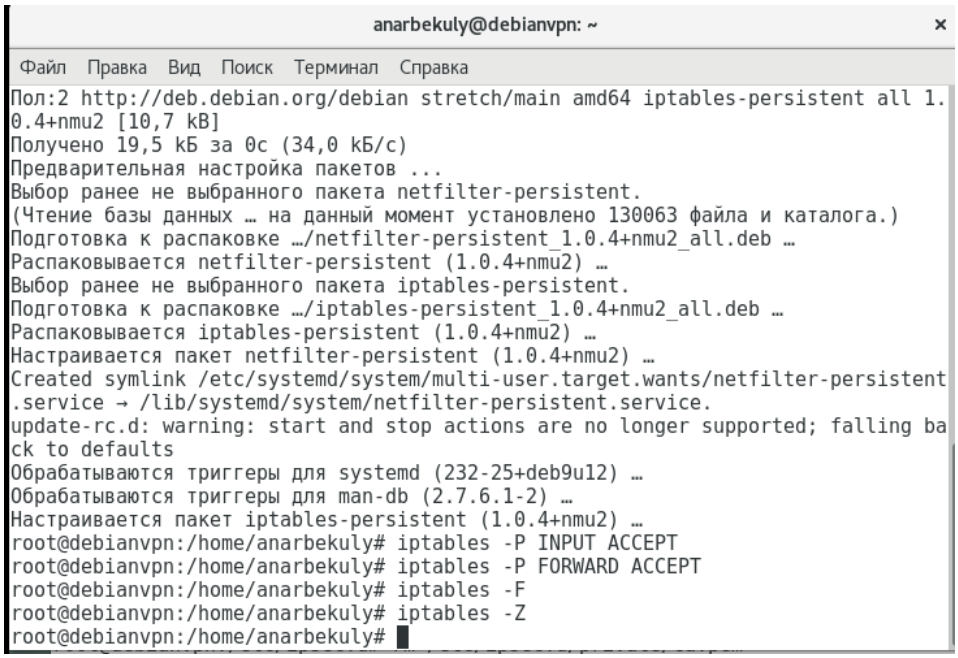

Рисунок 49 – Очистка цепочки

Дается разрешение для соединения по SSH на 22 порту, чтобы доступ к машине не был утерян, дается разрешение соединения на loopback-interface и входящие ipsec-соединения на UDP-портах 4500 и 500 (рисунок 50).

```
root@debianvpn:/home/anarbekuly# iptables -A INPUT -m state --state ESTABLISHED,
RELATED -j ACCEPT
root@debianvpn:/home/anarbekuly# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
root@debianvpn:/home/anarbekuly# iptables -A INPUT -i lo -j ACCEPT
root@debianvpn:/home/anarbekuly# iptables -A INPUT -p udp --dport 500 -j ACCEPT
root@debianvpn:/home/anarbekuly# iptables -A INPUT -p udp --dport 4500 -j ACCEPT
root@debianvpn:/home/anarbekuly#
```

Рисунок 50 – Разрешение SSH

Далее дается разрешение на переадресацию ESP-трафика (рисунок 51) и настройка маскирования трафика (рисунок 52).

```
root@debianvpn:/home/anarbekuly# iptables -A FORWARD --match policy --pol ipsec
--dir in --proto esp -s 10.10.10.0/24 -j ACCEPT
root@debianvpn:/home/anarbekuly# iptables -A FORWARD --match policy --pol ipsec
--dir out --proto esp -d 10.10.10.0/24 -j ACCEPT
root@debianvpn:/home/anarbekuly#
```

Рисунок 51 – Переадресация ESP-трафика

```
root@debianvpn:/home/anarbekuly# iptables -t nat -A POSTROUTING -s 10.10.10.0/24
 -o eth0 -m policy --pol ipsec --dir out -j ACCEPT
root@debianvpn:/home/anarbekuly# iptables -t nat -A POSTROUTING -s 10.10.10.0/24
 -o eth0 -j MASQUERADE
```

Рисунок 52 – Маскирование трафика

Далее идет настройка максимального размера сегмента пакетов (рисунок 53) и запрет на все прочие соединения к серверу кроме используемого (рисунок 54).

```
Try `iptables -h' or 'iptables --help' for more information.
root@debianvpn:/home/anarbekuly#
root@debianvpn:/home/anarbekuly# iptables -t mangle -A FORWARD --match policy --
pol ipsec --dir in -s 10.10.10.0/24 -o eth0 -p tcp -m tcp --tcp-flags SYN,RST SY
N -m tcpmss --mss 1361:1536 -j TCPMSS --set-mss 1360
root@debianvpn:/home/anarbekuly#
```

Рисунок 53 – Размер сегмента пакета

```
root@debianvpn:/home/anarbekuly# iptables -A INPUT -j DROP
root@debianvpn:/home/anarbekuly# iptables -A FORWARD -j DROP
root@debianvpn:/home/anarbekuly#
```

Рисунок 54 – Запрет соединений

На этом настройка Iptables закончена. Необходимо перезагрузить машину. Просмотр правила Iptables (рисунок 55) и работоспособность strongSwan (рисунок 56).

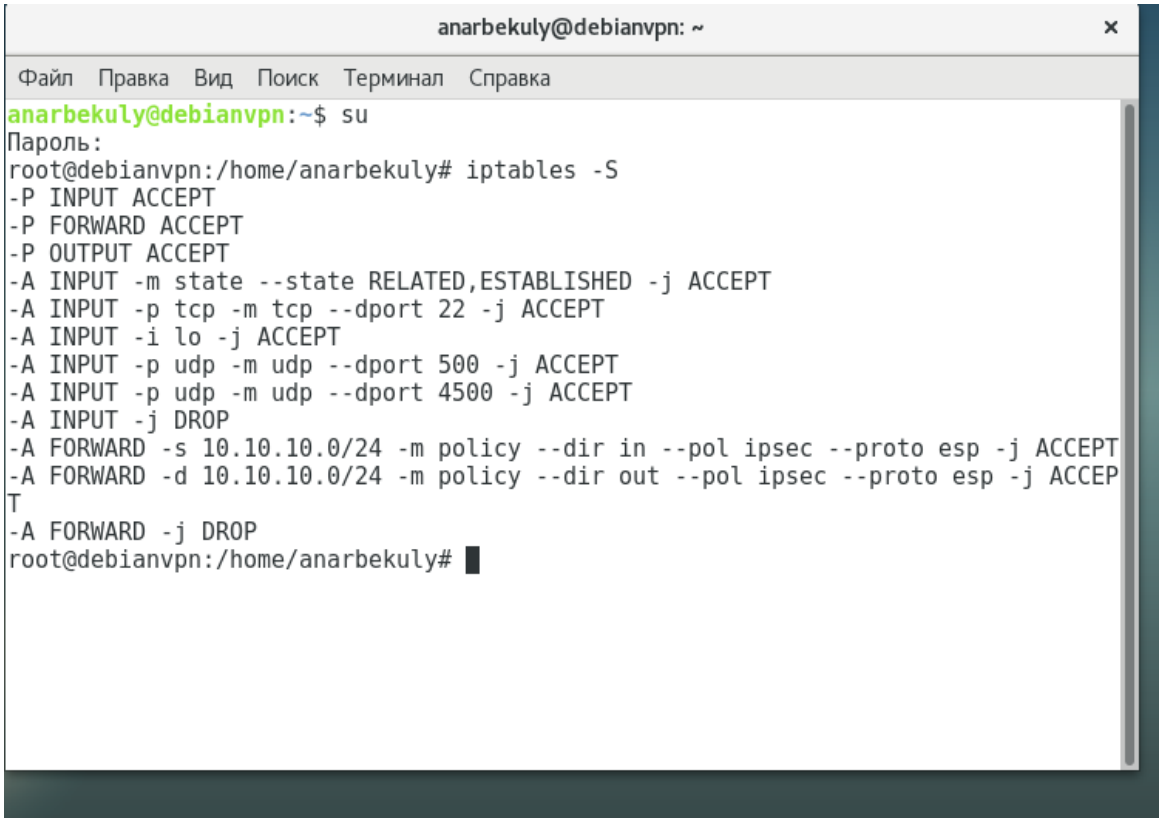

Рисунок 55 – Результат настроек Ipsec

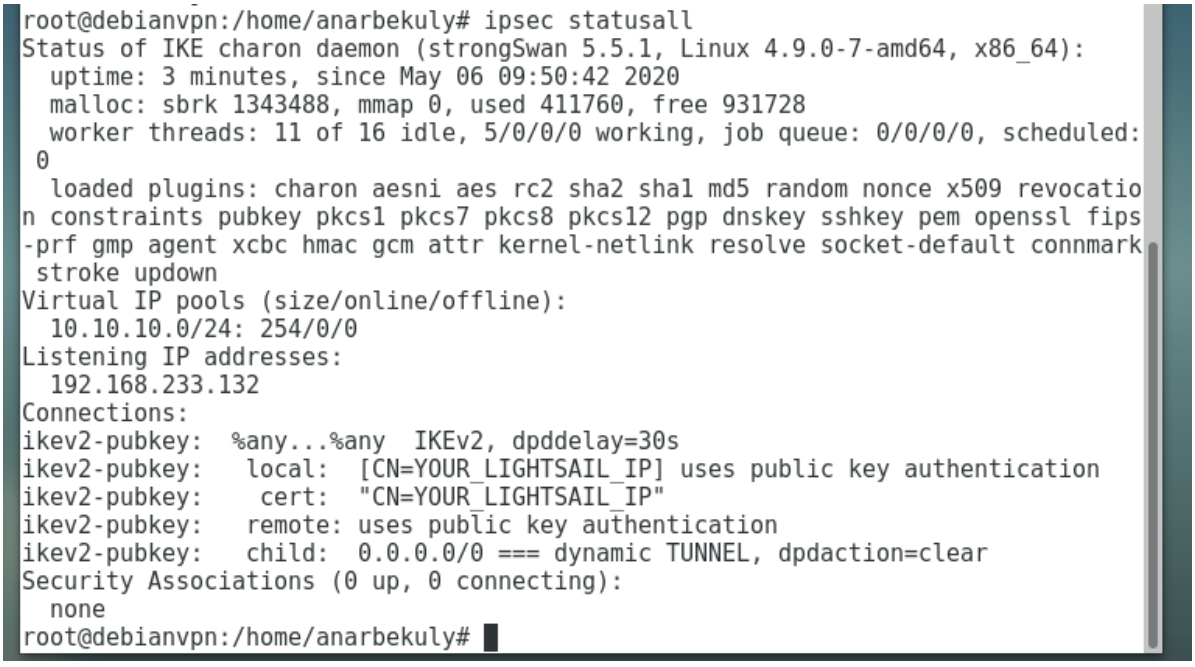

Рисунок 56 – StrongSwan

После убеждения, что все работает, необходимо дать разрешение соединения в файрволе lightstail. AWS Lightsail использует собственный

файрвол для защиты виртуальных машин. Настройка фаервола представлена на рисунке 57.

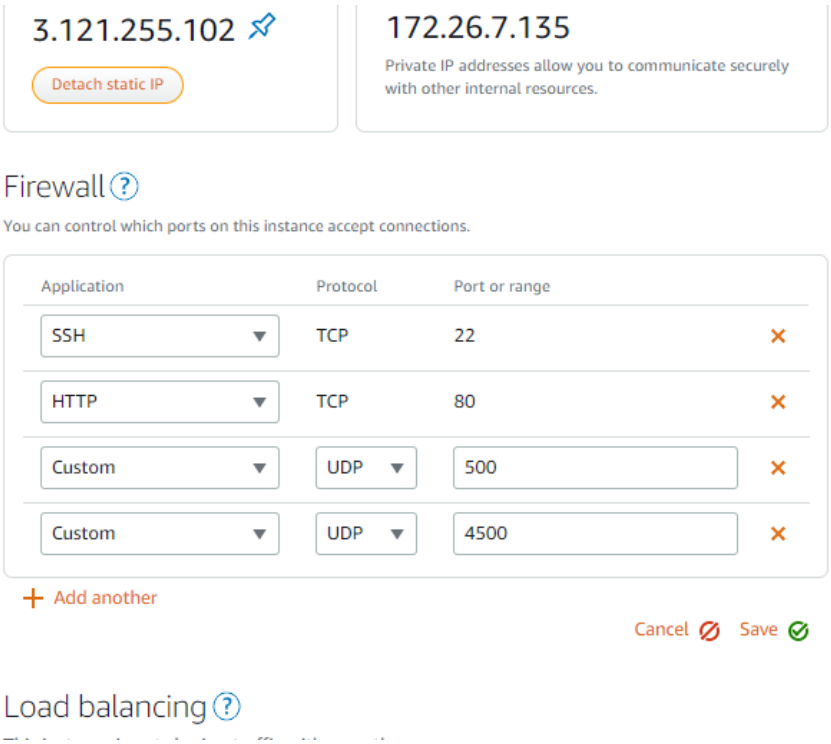

Рисунок 57 – Настройка файрвола в lightstail

Далее создается .mobileconfig для клиентов. Будет использован один VPN-профайл .mobileconfig для всех устройств. Создание конфигурационного файла показано на рисунке 58.

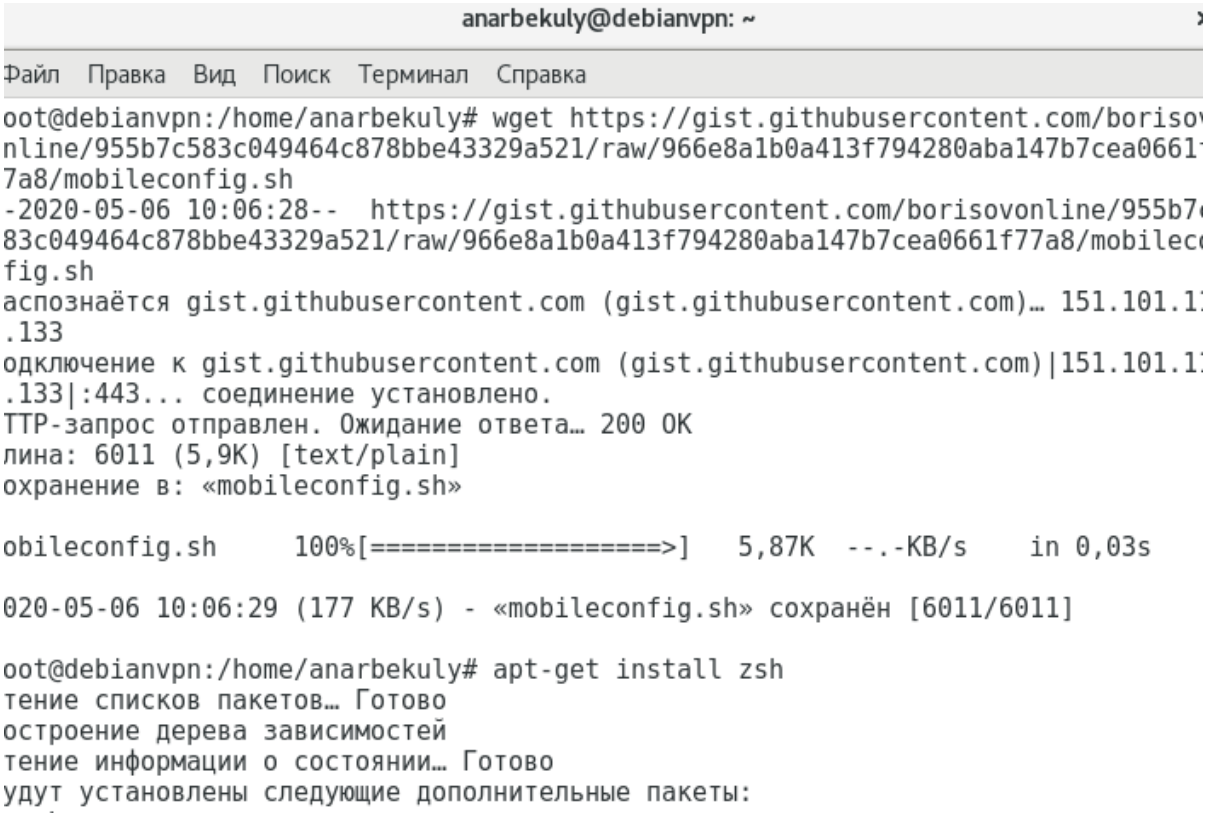

Рисунок 58 – Создание конфигурационного файла

Далее скачивается скрипт, благодаря которому создается конфигурационный файл (рисунок 59).

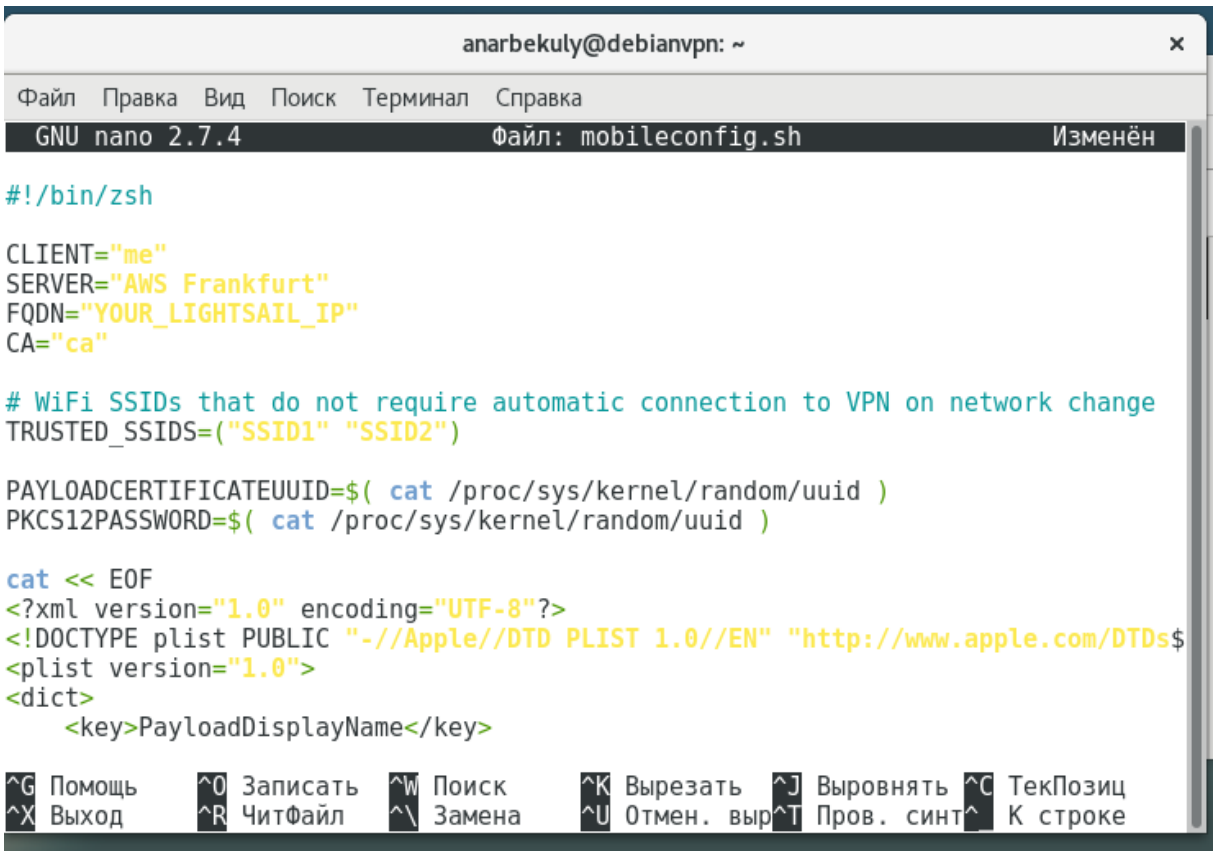

Рисунок 59 – Скрипт

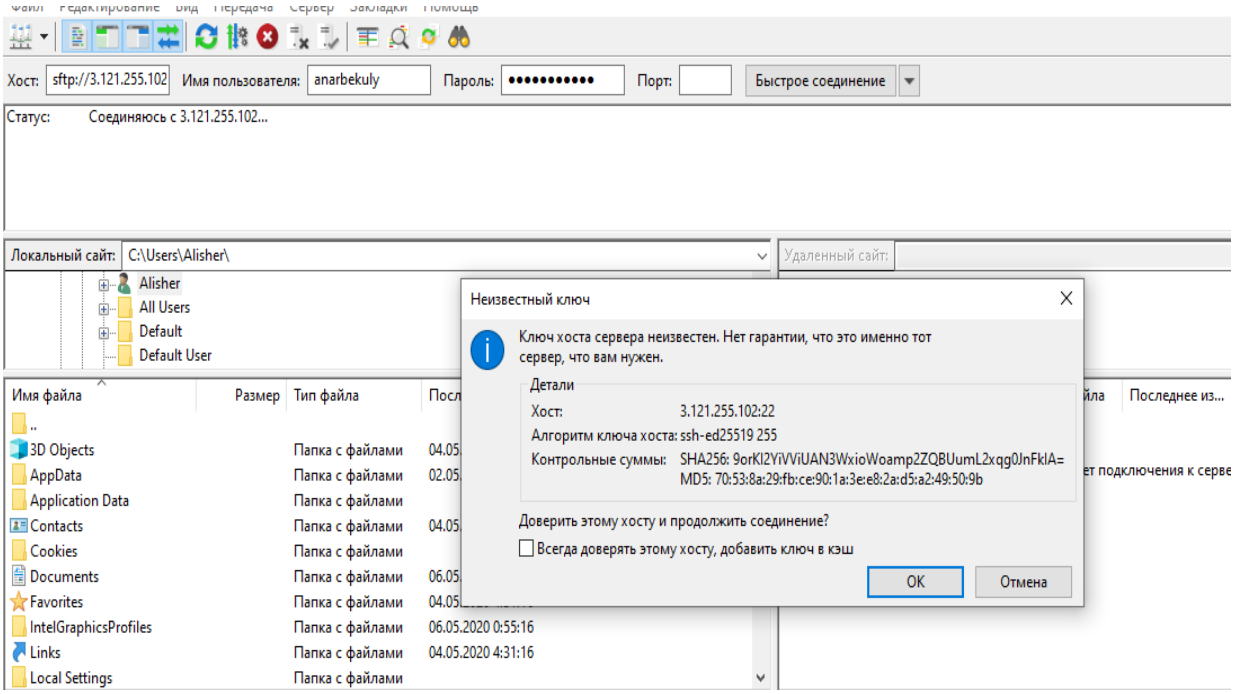

Рисунок 60 – Загрузка ключа

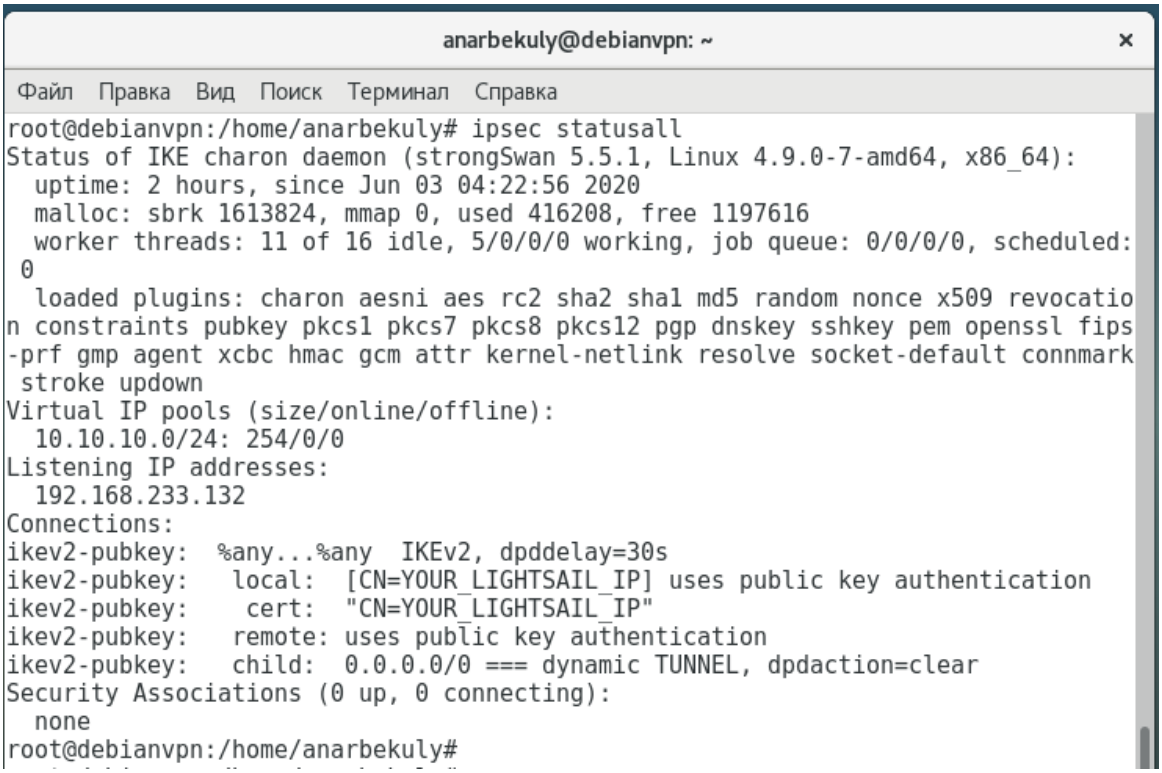

Рисунок 61 – Включение сервера

Далее необходимо установить strongSwan клиент, для подключения к серверу. И подключаемся по VPN туннелю к серверу.

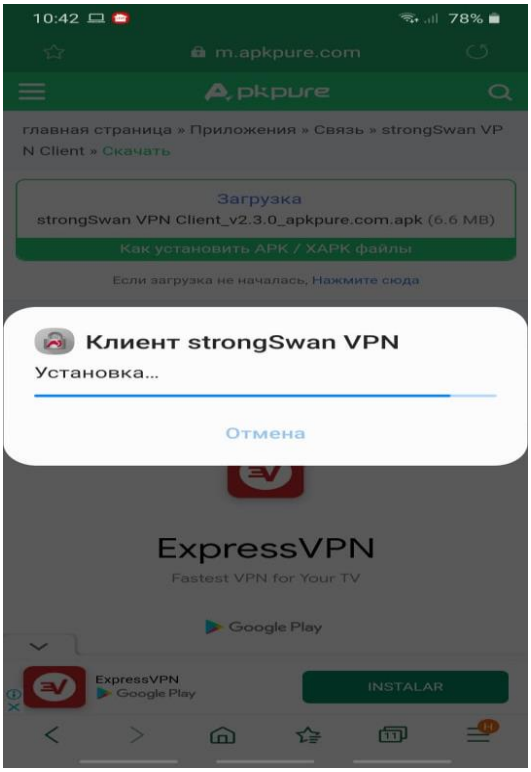

Рисунок 62 – Установка strongSwan клиента

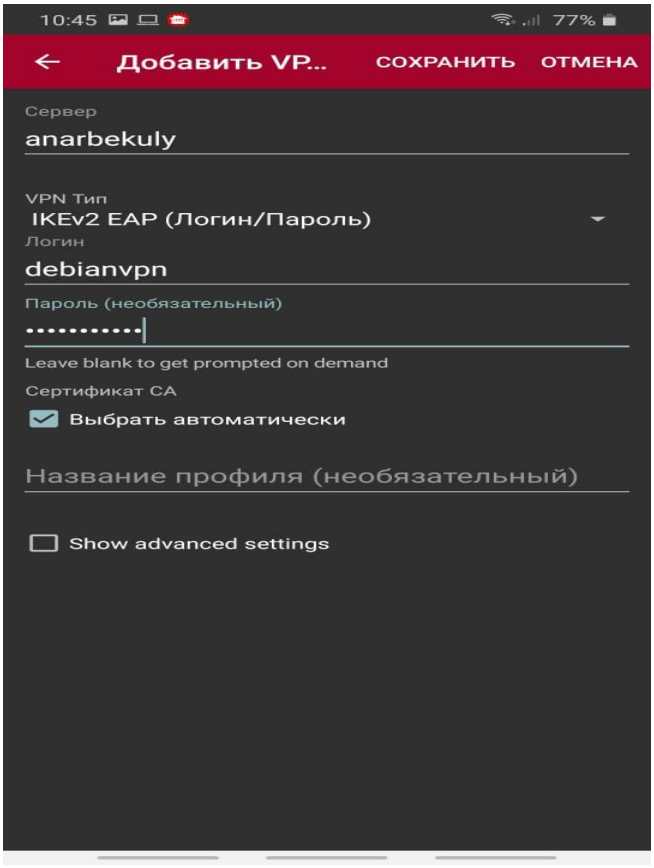

Рисунок 63 – Подключение к серверу

3 Безопасность жизнедеятельность

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

Вредный производственный фактор – это фактор трудового процесса или среды, воздействие которого на при определенных условиях на работника может вызвать профессиональное заболевание, снижение работоспособности. Опасный производственный фактор – фактор способный стать причиной острого заболевания, резкого ухудшения здоровья или летального исхода.

Опасные и вредные производственные факторы, согласно ГОСТ 12.0.003, делятся по категориям:

- физические;
- химические;
- биологические;
- психофизиологические.

Опасные производственные факторы – механические, электрические, падение с высоты, падение предметов, термические ожоги, химические ожоги, воздействие повышенных или пониженных температур, ДТП, падение, обрушение обвалы предметов и деталей, воздействие вредных веществ, и т. д.

Физические факторы:

- движущиеся машины и механизмы, подвижные части торгово-технологического оборудования, перемещаемые товары, тара, обрушивающиеся штабели складируемых материалов;
- повышенная/пониженная температура поверхностей оборудования, изделий;
- повышенная запыленность воздуха рабочей зоны;
- повышенная/пониженная температура воздуха рабочей зоны;
- повышенный уровень шума, вибрации, влажности воздуха на рабочем месте;
- затруднение дыхания, сухость слизистых оболочек дыхательных путей;
- повышенная/пониженная подвижность воздуха;
- повышенное напряжение в электрической цепи, замыкание которой может пройти через тело человека;
- повышенные уровни электромагнитных излучений;
- отсутствие или недостаток естественного освещения и т. д.

Химические факторы – кислоты, едкие щелочи, дезинфицирующие, моющие средства.

Психофизиологические факторы — физические нервно-психические перегрузки, перенапряжение анализа-торов, монотонность труда.

Биологические факторы – воздействие окружающей среды, возможность столкновения с факторами, отравляющими воздух, что приводит к временной или продолжительной утрате работоспособности. [11]

Опасные и вредные производственные факторы по характеру своего происхождения подразделяют на:

- факторы, порождаемые физическими свойствами и характеристиками состояния материальных объектов производственной среды;
- факторы, порождаемые химическими и физико-химическими свойствами используемых или находящихся в рабочей зоне веществ и материалов;
- факторы, порождаемые биологическими свойствами микроорганизмов, находящихся в биообъектах и (или) загрязняющих материальные объекты производственной среды;
- факторы, порождаемые поведенческими реакциями и защитными механизмами живых существ (укусы, ужаливания, выброс ядовитых или иных защитных веществ и пр.);
- факторы, порождаемые социально-экономическими и организационно-управленческими условиями осуществления трудовой деятельности (плохая организация работ, низкая культура безопасности и пр.);
- факторы, порождаемые психическими и физиологическими свойствами и особенностями человеческого организма и личности работающего (плохое самочувствие работника, нахождение работника в состоянии алкогольного, наркотического или токсического опьянения или абсистенции, потеря концентрации внимания работниками и пр.). [12]

Условия труда подразделяются на 4 класса:

- 1-й класс – оптимальные условия труда;
- 2-й класс – допустимые условия труда, которые могут вызывать функциональные отклонения, но после регламентированного отдыха организм человека приходит в нормальное состояние (оптимальный и допустимый классы соответствуют нормальным условиям труда);
- 3-й класс – вредные условия труда, характеризующиеся наличием вредных производственных факторов, превышающих гигиенические нормы. Они оказывают неблагоприятное воздействие на работающего и могут негативно влиять на его потомство. Вредные условия труда по степени превышения гигиенических норм и выраженности изменений в организме работающих, в свою очередь, подразделяются на четыре степени вредности и опасности;
- 4-й класс – опасные (экстремальные) условия труда, при которых в течение рабочей смены, небольшого промежутка времени создается угроза для жизни, высокий риск возникновения тяжелых и острых профессиональных поражений. Работа в экстремальных условиях труда не допускается за исключением ликвидации аварийных ситуаций, проведения ремонтных работ.

Медицинские обследования работников показали, что помимо снижения производительности труда высокие уровни шума приводят к ухудшению слуха. Длительное нахождение человека в зоне комбинированного воздействия различных неблагоприятных факторов может привести к профессиональному заболеванию. Анализ травматизма среди работников показывает, что в основном несчастные случаи происходят от воздействия физически опасных производственных факторов при выполнении сотрудниками несвойственных им работ. На втором месте случаи, связанные с воздействием электрического тока.

В соответствии с правилами электробезопасности в служебном помещении должен осуществляться постоянный контроль состояния электропроводки, предохранительных щитов, шнуров, с помощью которых включаются в электросеть компьютеры, осветительные приборы, другие электроприборы.

Электрические установки, к которым относится практически все оборудование ЭВМ, представляют для человека большую потенциальную опасность, так как в процессе эксплуатации или проведении профилактических работ человек может коснуться частей, находящихся под напряжением. Специфическая опасность электроустановок – токоведущие проводники, корпуса стоек ЭВМ и прочего оборудования, оказавшегося под напряжением в результате повреждения (пробоя) изоляции, не подают каких-либо сигналов, которые предупреждают человека об опасности. Реакция человека на электрический ток возникает лишь при протекании последнего через тело человека. Исключительно важное значение для предотвращения электротравмотизма имеет правильная организация обслуживания действующих электроустановок, проведения ремонтных, монтажных и профилактических работ.

В зависимости от категории помещения необходимо принять определенные меры, обеспечивающие достаточную электробезопасность при эксплуатации и ремонте электрооборудования.

Другим методом защиты является нейтрализация заряда статического электричества ионизированным газом. В промышленности широко применяются радиоактивные нитрализаторы. К общим мерам защиты от статического электричества можно отнести общие и местное увлажнение воздуха.

Также к мерам обеспечения электробезопасности можно отнести защитное заземление и защитное зануление.

Защитное заземление — преднамеренное электрическое соединение с землёй или её эквивалентом металлических нетоковедущих частей электроустановок, которые могут оказаться под напряжением.

Пожарная безопасность обеспечивается системой предотвращения пожара и системой пожарной защиты. Во всех служебных помещениях обязательно должен быть “План эвакуации людей при пожаре”,

регламентирующий действия персонала в случае возникновения очага возгорания и указывающий места расположения пожарной техники.

Пожары в вычислительных центрах представляют особую опасность, так как сопряжены с большими материальными потерями. Характерная особенность ВЦ – небольшие площади помещений. Как известно пожар может возникнуть при взаимодействии горючих веществ, окисления и источников зажигания. В помещениях ВЦ присутствуют все три основные фактора, необходимые для возникновения пожара.

Одной из наиболее важных задач пожарной защиты является защита строительных помещений от разрушений и обеспечение их достаточной прочности в условиях воздействия высоких температур при пожаре. Учитывая высокую стоимость электронного оборудования ВЦ, а также категорию его пожарной опасности, здания для ВЦ и части здания другого назначения, в которых предусмотрено размещение ЭВМ должны быть 1 и 2 степени огнестойкости.

Объекты ВЦ кроме АПС необходимо оборудовать установками стационарного автоматического пожаротушения. Наиболее целесообразно применять в ВЦ установки газового тушения пожара, действие которых основано на быстром заполнении помещения огнетушащим газовым веществом с резким сжижением содержания в воздухе кислорода. [13]

Для работающих в офисе наиболее вредные производственные факторы связаны именно с продолжительной работой за компьютером.

Компьютеры могут оказывать вредное воздействие на организм работающего человека.

Пользователь ПЭВМ и его руководитель должны знать о вредном воздействии факторов и об эффективных способах зашиты от них, что уменьшает вероятность получения ими различных профессиональных заболеваний, а также снижает количество сбоев и ошибок в работе операторов.

Необходимо более подробно остановиться именно на анализе вредных и опасных производственных факторов, воздействующих на персонал, работающий в офисе.

На работников могут оказывать неблагоприятное воздействие следующие опасные и вредные производственные факторы:

- повышенный уровень электромагнитных излучений;
- повышенный уровень ионизирующих из-лучений;
- повышенный уровень статического эле-ктричества;
- повышенная напряженность электростатического поля;
- повышенная или пониженная ионизация воздуха;
- повышенная яркость света;
- прямая и отраженная блесткость;
- повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека;

- статические перегрузки костно-мышеч-ного аппарата и динамические локальные перегрузки мышц кистей рук;

- перенапряжение зрительного анализатора;

- умственное перенапряжение;

- эмоциональные перегрузки;

- монотонность труда.

В зависимости от условий труда, в которых применяются ПК, и характера работы на работников могут воздействовать также другие опасные и вредные производственные факторы.

Приведем пример из другой типовой инструкции. Согласно п. 7 Межотраслевой типовой инструкции по охране труда для электромонтера по ремонту и обслуживанию электрооборудования в процессе труда на электромонтера могут воздействовать следующие опасные и вредные производственные факторы:

- повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека при приближении на расстояние менее допустимого к неизолированным токоведущим частям и элементам оборудования, находящегося под напряжением, а также при перемещении и работе в зонах растекания тока на землю, влияния электрического поля и наведенного напряжения;

- повышенная напряженность электрического и магнитного полей;

- возникшая электрическая дуга при переключениях в электроустановках или в аварийных ситуациях;

- работа на расстоянии менее 2 м от неогражденных перепадов по высоте на 1,3 м и более;

- недостаточная освещенность рабочей зоны;

- повышенная или пониженная температура воздуха рабочей зоны, а также поверхностей оборудования, материалов;

- повышенная или пониженная влажность воздуха, а также сильный ветер при работе вне помещения;

- движущиеся машины и механизмы;

- подвижные части производственного оборудования; передвигающиеся изделия, заготовки, материалы;

- разрушающиеся конструкции и элементы оборудования в процессе выполнения работы и в аварийных ситуациях;

- острые кромки, заусеницы и шероховатости на поверхности заготовок, инструментов, оборудования;

- повышенная запыленность и загазованность воздуха рабочей зоны.

Таким образом, можно сделать вывод о том, что количество опасных и вредных производственных факторов у электромонтера меньше, чем у офисного работника. Конечно, вероятность получить производственную травму, а также степень тяжести травмы у электромонтера выше, чем у сотрудника, работающего в офисе.

Однако основной сложностью трудового процесса (при условии использования хорошей оргтехники), связанного с работой на компьютере, является тяжесть трудового процесса (а именно стереотипные рабочие движения, рабочая поза), а также напряженность трудового про-цесса:

- интеллектуальная нагрузка (восприятие сигналов и их оценка);
- сенсорная нагрузка (длительность сосредо-точенного наблюдения, плотность сигналов, наблюдение за экранами видеотерминалов);
- эмоциональная нагрузка (степень ответственности за результат своей деятельности);
- монотонность нагрузок (продолжительность выполнения повторяющихся операций). [14]

3.2 Расчет защитного заземления

В одном из офисных помещений компании находится электроустановка - серверная стойка, которую в целях обеспечения электробезопасности необходимо заземлить. Необходимо рассчитать заземляющее устройство (контурное заземление).

Для расчета приняты следующие параметры:

- напряжение электроустановки «серверная стойка» - 380 В;
- тип грунта - суглинок;
- климатическая зона - четвертая (южные районы Казахстана);
- параметры контура заземления – 20х30 м;
- заземлители – вертикальные стержни длиной 5 м из стальных труб диаметром 100 мм, заземлители соединяются сваркой стальной полосой шириной 50 мм;
- глубина заложения заземлителей от поверхности – 0,7 м.

Для начала необходимо вычислить удельное сопротивление грунта, на котором находится здание с заземляемым объектом.

Сопротивление грунта с учетом коэффициента сезонности (представлен в таблице 2) для вертикальных стержней вычисляется по формуле (1):

$$\rho_{о.с.} = \Psi_в * \rho_о, \quad (1)$$

где $\Psi_в$ – коэффициент сезонности;

$\rho_о$ – удельное сопротивление грунта.

Удельное электрическое сопротивление грунта и воды представлено в таблице 2.

Таблица 2 - Удельные сопротивления грунтов и воды р, Ом•м

Наименование грунта	Удельное сопротивление, Ом*м
песок	700
суглинок	100
глина	40

садовая земля	40
скалы, валуны	2000-4000
чернозем	20
торф	20
речная вода	10-100
морская вода	0,2-1

Таблица 3 – Коэффициент сезонности

Климатическая зона	Значения коэффициентов сезонности при влажности		
	повышенной	нормальной	малой
Вертикальный электрод длиной 4-5 м			
1	1,5	1,4	1,3
2	1,4	1,3	1,2
3	1,3	1,2	1,1
4	1,2	1,1	1,0
Горизонтальный электрод длиной до 50 м			
1	7,2	4,5	3,6
2	4,8	3,0	2,4
3	3,2	2,0	1,6
4	2,2	1,4	1,12

Из таблицы 2 понятно, что удельное сопротивление глины = 40 Ом*м.

Из таблицы 3 понятно, что коэффициент сезонности для г. Алматы = 1,1.

Рассчитаем удельное сопротивление грунта.

$\rho_{o.c.} = 100 * 1,1$ (Ом*м) = 110 Ом*м.

Следующий этап – расчет сопротивления растеканию тока одиночного стержня. Вычисляется по формуле (2):

$$R_c = (\rho_{o.c.}/(2*\pi*l_c))(\ln(2*l_c/d)+0,5\ln((4*t+l_c)/4*t-l_c))), \quad (2)$$

где l_c – длина стержня, м;

d – диаметр стержня из труб, м;

$t = H+(1/2)*l_c$ – расстояние от поверхности земли до середины стержня, м;

H – глубина заложения стержня, м.

Производится расчет.

t = 0,7 + 5/2 = 3,2 м.

R_c = (110/(2*3,14*5)) * (ln(2*5/0,1) + 0,5ln((4*3,2+5)/(4*3,2-5))) = (110/31,4) * (ln(100) + 0,5ln(17,8/7,8)) = 3,5 * (4,6 + 0,5*0,825) = 3,5 * 5 = 17,5 Ом * м.

Третий этап – расчет предварительного количества заземлителей и длины соединительной полосы. Предварительное количество заземлителей вычисляется по формуле (3), длина соединительной полосы (при расположении по контуру) рассчитывается по формуле (4).

$$\eta_{пр} * \eta_c = R_c / R_З, \quad (3)$$

где Rз – сопротивление растеканию тока заземляющего устройства (берется из таблицы 3);

η_c – коэффициент использования вертикальных стержней (берется из таблицы 4).

$$l_п = 1{,}5 * n * \alpha, \quad (4)$$

где α – расстояние между стержнями.

Таблица 4 - Допустимые сопротивления заземляющего устройства в электроустановках

Наибольшие допустимые значения Rз, Ом	Характеристика электроустановок
Rз < 0,5	Для электроустановок напряжением выше 1000В и расчётным током замыкания на землю Iз < 500А
Rз = 250 / Iз < 10	Для электроустановок напряжением выше 1000В и расчётным током замыкания на землю Iз < 500А
Rз = 125 / Iз < 10	При условии, что заземляющее устройство является общим для злектроустановок напряжением до и выше 1000 В и расчётном токе замыкания на землю Iз < 500
Rз < 2	В электроустановках напряжением 660/380 В
Rз < 4	В электроустановках напряжением 380/220 В
Rз < 8	В электроустановках напряжением 220/127 В

Таблица 5 – Коэффициенты использования вертикальных стержней

Число стержней	Отношение расстояния между заземлителями к их длине (α/l_c) при размещении		
	1	2	3
	по контуру		
2	-	-	-
4	0,69	0,78	0,85
6	0,61	0,73	0,8
10	0,55	0,68	0,76
20	0,47	0,63	0,71
40	0,41	0,58	0,66
60	0,39	0,55	0,64
100	0,36	0,52	0,62

Таблица 6 – Коэффициенты использования горизонтальных стержней

Отношение α/l_c	Число стержневых заземлителей							
	2	4	6	10	20	40	60	100
стержни размещены по контуру								
1	-	0,45	0,4	0,34	0,27	0,22	0,2	0,19
2	-	0,55	0,48	0,4	0,32	0,29	0,26	0,23
3	-	0,7	0,64	0,56	0,45	0,39	0,36	0,33

Расчет:

$\eta_{пр}*\eta_c = 17,5/4 \approx 4$.

$l_п = 2*20+ 2*30 = 100$.

$\alpha = 100/4 = 25$.

$\alpha/l_c = 25/5 = 5$.

Четвертый этап – расчет удельного сопротивления грунта для соединительной полосы. Расчет осуществляется по формуле (5):

$$\rho_{с.п.} = \Psi_{г.} * \rho_о, \quad (5)$$

где $\Psi_в$ – коэффициент сезонности;

$\rho_о$ – удельное сопротивление грунта.

Из таблицы 2 видно, что при длине более 50 м, $\Psi_г = 1,4$.

$\rho_{с.п.} = 1,4 * 100 = 140$ Ом*м.

Пятый этап – расчет сопротивления растеканию тока соединительной полосы. Вычисляется по формуле (6):

$$R_П = (\rho_{с.п.}/2*\pi*l_п)*(l_п(2*l^2_п)/(b*H)), \quad (6)$$

где $l_п$ – длина полосы, м;

b – длина полосы, м.

Расчет:

$R_п = (140/(2*3,14*100)) * \ln((2*100^2)/0,05*0,7)) = (140/628) * \ln(20000/0,035) = 0,23 * \ln(571429) = 0,23 * 13,26 = 3$.

Заключительный этап – расчет результирующего сопротивления заземляющего устройства. Вычисляется по формуле (7):

$$R_{з.у.} = (R_с * R_п)/((R_с * \eta_п) + (R_п * \eta_{пр} * \eta_с)) \leq R_З \quad (7)$$

Из таблицы 5 видно, что коэффициент $\eta_п = 0,7$ и $\eta_с = 0,85$.

Производим расчет:

$R_{з.у.} = (17,8*3) / ((7*0,7) + (3 * 4 * 0,85)) < R_З$

$R_{з.у.} = 5,93 / 15,1 < R_З$

$0,39 < 4$, верно.

Далее необходимо уточнить количество стержней и полосы, окончательно определить результирующее сопротивление заземляющего устройства.

$n = (n_{пр} * \eta_c) / \eta_c = 4/0,85 = 4,7$.

Расстояние от системы заземления до здания: $L = 0,6 * R_{з.у} = 0,6 * 0,39 = 0,2$ м.

Ответ: стержни размещаются по периметру территории через 4,7 метров, расстояние от системы заземления до здания – 0,2 м.

3.3 Расчет параметров микроклиматических условий в офисе

Необходимо:

- определить приемлемые значения параметров микроклимата – температуры и влажности воздуха в офисе;
- рассчитать количество влаги, выделяющейся в воздух офиса от персонала;
- рассчитать расход воздуха, подаваемого в помещение;
- рассчитать кратность требуемого воздухообмена для поддержания оптимальных параметров микроклимата.

Офисное помещение имеет следующие параметры:

- длина: 20 м;
- ширина: 14 м;
- высота: 4 м.

Число человек, постоянно находящихся в помещении офиса: 6.

Первый этап – определение оптимальных температуры и влажности воздуха в офисе (для теплого времени года) с помощью таблицы 7.

Таблица 7 – Нормы температуры и относительной влажности

Категория работ	Температура на рабочих местах, °С					Относительная влажность, %	
	оптимальная	допустимая				оптимальная	допустимая на рабочих местах и постоянных, и не постоянных, не более
		постоянных	непостоянных	постоянных	непостоянных		
Легкая - Iа	23-25	28	30	22	20	40-60	55 (при 28°С)
Легкая - Iб	22-24	28	30	21	19	40-60	60 (при 27°С)

Средней тяжести - IIа	21-23	27	29	18	17	40-60	65 (при 26°С)
Средней тяжести - IIб	20-22	27	29	16	15	40-60	70 (при 25°С)
Тяжелая - III	18-20	26	28	15	13	40-60	75 (при 24°С)

По таблице 7 определяем, что оптимальная температура – 23-25 °С (среднее значение– 24 °С), оптимальная влажность – 40-60 % (среднее значение – 50 %).

Расчет количества влаги, выделяемой в воздух офиса от персонала, производится по формуле (8):

$$W = W_1 n, \text{ кг/с}, \quad (8)$$

где W_1 – количество влаги, выделяемой в воздух человеком в течение 1 часа;

n - число человек, постоянно находящихся в помещении офиса.

При температуре 24 °С $W_1 = 0,09$ кг/чел.

$W = 0,09 * 6 = 0,54$ кг/с.

Расчет расхода воздуха, подаваемого в помещение, производится по формуле (9):

$$V = W/((x_1 - x_0)*\rho_п), \text{ м/с}, \quad (9)$$

где $\rho_п = 1,293(T_0/T)$, кг/м^3 – плотность поступающего воздуха; $T_0 = 273$ К, $T = t_0 + 273$К;

x_1 – влагосодержание в воздухе офисного помещения для оптимальных значений микроклимата (определяется с помощью диаграммы, представленной на рисунке 1);

x_0 – влагосодержание воздуха, поступающего в помещение (определяется с помощью диаграммы, представленной на рисунке 64).

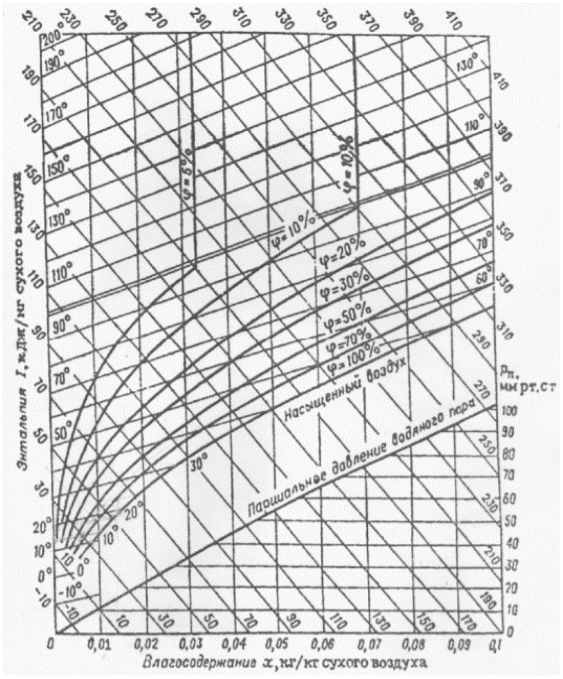

Рисунок 64 – Диаграмма состояния влажного воздуха

Примем t_0 = 20 °С.

$\rho_п$ = 1,293*(273 /(20+273)) = 1,293*0,93= 1,2.

x_1 (при t = 25 °С и φ = 50 %) = 0,01.

x_0 (при t = 20 °С и φ = 50 %) = 0,008.

V = 0,54 / ((0,01-0,008) * 1,2) = 0,54/0,024 = 22,5 м/с.

Заключительный этап – расчет воздухообмена в помещении. Расчет производится по формуле (10):

$$K = V/V_1*3600, \quad (10)$$

где V_1 – объем помещения.

Расчет:

V_1 = 20*14*4 = 1120 м^3.

K = (22,5/1120) * 3600 = 72 ч$^{-1}$.

Ответ: для офисного помещения в теплое время года оптимальная температура воздуха составляет 24-26 °С, оптимальная влажность – 50%, а кратность воздухообмена - 72 ч$^{-1}$.

4 Анализ и оценка рисков информационной безопасности

4.1 Идентификация активов

В целях анализа и расчета рисков информационной безопасности в первую очередь необходимо произвести инвентаризацию активов, подлежащих защите. Среди них, опираясь на специфику темы работы, для анализа и расчета рисков были выделены три актива: внутренняя (локальная) сеть, VPN-сервер, веб-приложения.

Защищаемые активы и риски были выбраны исходя из того, что работа посвящена в основном разбору и анализу возможностей SIEM-системы.

Перечень защищаемых активов:

- внутренняя сеть компании – актив был выбран, так как возможности мониторинга SIEM-системы направлены по большей части именно на регистрацию подозрительной активности в защищаемой сети;
- VPN-сервер – это важный элемент сетевой инфраструктуры компании, также на нем и располагается SIEM-система;
- веб – приложения – именно через приложения (часто это именно веб-приложения) клиент взаимодействует с сервером, поэтому важно осуществлять мониторинг подозрительной активности данного элемента сетевой инфраструктуры, с помощью SIEM-системы, например.

Важно отметить, что, SIEM-система –это средство мониторинга, а не средство защиты. Тем не менее, она является важным элементом обеспечения информационной безопасности. Знания о подозрительной активности позволяют определить, где необходимо внедрить защитные меры (или усилить их, если само наличие произошедшего инцидента свидетельствует об их неэффективности). Подозрительная активность, зарегистрированная SIEM-системой, может быть прервана средствами защиты. Именно поэтому при анализе некоторых выбранных рисков был указан мониторинг SIEM-системой вкупе с прочими защитными средствами.

4.2 Анализ и оценка рисков

Для анализа и оценки рисков был выбран алгоритм, представленный в стандарте ISO-27005. Расчет по данному алгоритму (исходя из ценности актива, степени вероятности возникновения угрозы и простоты использования уязвимости) производится на основе приложения Е стандарта ISO-27005. Алгоритм оценки рисков представлен в таблице 8.

Таблица 8 - Ценность активов, уровни угроз и уязвимостей

Вероятность угрозы		Низкая			Средняя			Высокая		
Простота использования		Н	С	В	Н	С	В	Н	С	В
Ценность активов	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Простой общий рейтинг рисков:
- низкий риск (приемлемый): 0-2;
- средний риск: 3-5;
- высокий риск (неприемлемый): 6-8.

Анализ рисков (угроз и уязвимостей) информационной безопасности для вышеперечисленных активов представлен в таблице 9.

Таблица 9 – Анализ и оценка рисков информационной безопасности

Угрозы	**Уязвимости**	**Максимальный уровень риска**	**Меры по обработке риска**	**Остаточный уровень риска**	**Комментарии, ресурсы, ответственный**
Актив 1: Внутренняя (локальная) сеть компании					
1 Сетевая разведка и, как следствие, сбор критической информации о сетевой инфраструктуре	Отсутствие системы обнаружения/предотвращения вторжений. Некорректная настройка межсетевого экрана	7	SIEM как средство мониторинга подозрительной активности и фильтрация трафика с помощью межсетевого экрана	1	Сетевой администратор
2 Атака "man-in-the-middle"; как следствие, перехват и модификация передаваемых по сети данных	Отсутствие защиты передаваемого трафика. Отсутствие шифрования трафика	7	SIEM - для мониторинга попыток перехвата. Шифрование трафика, использование VPN - для предотвращения перехвата	1	Сетевой администратор
3 DDOS-атака; как следствие - отказ в обслуживании элемента сети	Отсутствие ограничения объема проходящего трафика	8	SIEM - для регистрации попыток DDOS + анализатор отдельных пакетов трафика на предмет того, является ли он разрешенным	2	Сетевой администратор
4 IP-спуфинг и, как следствие, вставка ложной информации в поток данных между клиентом и сервером	Отсутствие контроля управления сетевым доступом	6	SIEM – для регистрации попыток IP-спуфинга. Система контроля управления доступом – для предотвращения дальнейших инцидентов	1	Сетевой администратор
5 Получение возможности удаленного управления компьютером сети	Неверная конфигурация фаервола (фаервол пропускает нелегитимный трафик)	5	SIEM – для регистрации подозрительного трафика. Затем – применение межсетевого экрана (или более корректная его настройка)	1	Сетевой администратор

Актив 2: VPN-сервер					

Продолжение таблицы 9

6 Несанкционированная аутентификация на сервере. Компрометация аккаунтов пользователей и администраторов сервера	Отсутствие мониторинга подозрительной активности на сервере	8	Внедрение системы мониторинга	2	Системный администратор
7 Заражение сервера «троянским конем». Следствие – шпионаж за действиями над сервером	Отсутствие антивирусной программы на сервере	7	SIEM - для мониторинга инцидентов, связанным с заражением станций вирусами и «троянами». Использование антивируса	1	Системный администратор
8 Внедрение на сервер rootkit-a	Некорректная настройка межсетевого экрана. Отсутствие антируткитов	5	Использование антируткита	1	Системный администратор
Актив 3: Веб-приложения компании					
9 Хранимая XSS-атака	Отсутствие фильтрации спецсимволов в формах веб-приложения	5	Использование SIEM для регистрации подозрительной активности в веб-приложения. Затем – корректная фильтрация спецсимволов в веб-приложениях	1	Разработчик веб-приложения
10 SQL-инъекция. Одно из возможных последствий – удаление базы данных, с которой связано веб-приложение	Отсутствие фильтрации вводимых в приложении параметров	7	Использование SIEM для регистрации подозрительной активности в веб-приложения. Затем – фильтрация входных данных форм веб-приложений	1	Разработчик веб-приложения

4.3 Диаграммы взаимосвязи элементов в программе CORAS

Далее представлены диаграммы взаимосвязи элементов анализа и оценки представленных в таблице 9 рисков (источники, активы, угрозы, уязвимости, защитные меры, последствия реализации угрозы и т.д.), реализованные в программе CORAS.

Все нижеперечисленные диаграммы, представленные на рисунках 65-70, следует читать слева направо.

На рисунке 65 показана диаграмма защищаемых активов (активы были упомянуты выше) и их категорий. Первая часть диаграммы – это категории,

на которые условно поделены защищаемые активы. Категории: Среда передачи данных, коечные элементы сетевой инфраструктуры, прикладные программы. Вторая часть диаграммы – это непосредственно сами активы. Активы: локальная сеть (принадлежит категории «Среда передачи данных»), VPN-сервер (принадлежит категории «Конечные элементы сетевой инфраструктуры»), веб-приложения (принадлежит категории «Прикладные программы»).

На рисунке 66 представлена диаграмма модели угроз. Элементы диаграммы: источники угроз, уязвимости, этапы реализации угроз, последствия реализации угроз (инциденты), защищаемые активы. Данная диаграмма по сути своей частично является «иллюстрацией» к таблице 9 (если быть точным, к части с анализом максимальных значений рисков, до внедрения защитных мер) и наглядно демонстрирует процесс реализации угрозы. К примеру, источник угрозы «Сторонний нарушитель», используя уязвимость «Отсутствие шифрования», осуществляет атаку «Человек посередине» и осуществляет «Перехват и модификацию передаваемого по сети трафика» Актив, на который направлена атака – «Локальная сеть компании».

На рисунке 67 представлена диаграмма модели угроз с учетом вероятности возникновения инцидента. Она во многом схожа с диаграммой, представленной на рисунке 66. Элементы диаграммы: источники угроз, уязвимости, этапы реализации угроз, последствия реализации угроз (инциденты), степень вероятности возникновения инцидента, защищаемые активы. Степень вероятности возникновения инцидента – это величина, которая согласно таблице 8 определяется как «высокая», «средняя» или «низкая» (используется при расчете рисков). Пример того, как читается данная часть диаграммы: вероятность возникновения инцидента «Отказ в обслуживании одного из элементов сети» (атака направлена на актив «Внутренняя сеть») – «высокая».

На рисунке 68 представлена диаграмма рисков с характеристиками влияния угроз. Элементы диаграммы: источники угроз, уязвимости, этапы реализации угроз, характеристики влияния угроз на бизнес, защищаемые активы. Характеристика влияния угрозы на бизнес-процессы – это величина, которая согласно таблице 8 определяется как «высокое влияние», «среднее» или «низкое» (используется при расчете рисков). Пример того, как читается данная диаграмма: источник угрозы «Сторонний нарушитель», используя уязвимость «Отсутствие шифрования», мог бы осуществить атаку «Человек посередине», влияние которой на бизнес-процессы компании характеризуется как «высокое», атака направлена на актив «Внутренняя сеть».

На рисунке 69 представлена диаграмма модели угроз с учетом защитных мер. Она во многом схожа с диаграммой, представленной на рисунке 66, однако иллюстрирует в том числе и часть таблицы 9, в которой выбирается мера обработки риска. Ее следует читать почти так же, как и

диаграмму, представленную на рисунке 66, с единственным отличием: между уязвимостями и способами реализации угроз добавлены защитные меры для уменьшения рисков. К примеру, для уязвимости «Отсутствие шифрования» внедрена защитная мера «SIEM+шифрование трафика» (SIEM - для мониторинга попыток перехвата. Шифрование трафика, использование VPN - для предотвращения перехвата).

На рисунке 70 показана диаграмма недопустимых рисков. В данной диаграмме показаны только те риски, чье максимальное значение (таблица 9) составляет от 6 до 8. За исключением этого, данная диаграмма по структуре полностью копирует диаграмму, представленную на рисунке 68, поэтому ее следует читать точно так же.

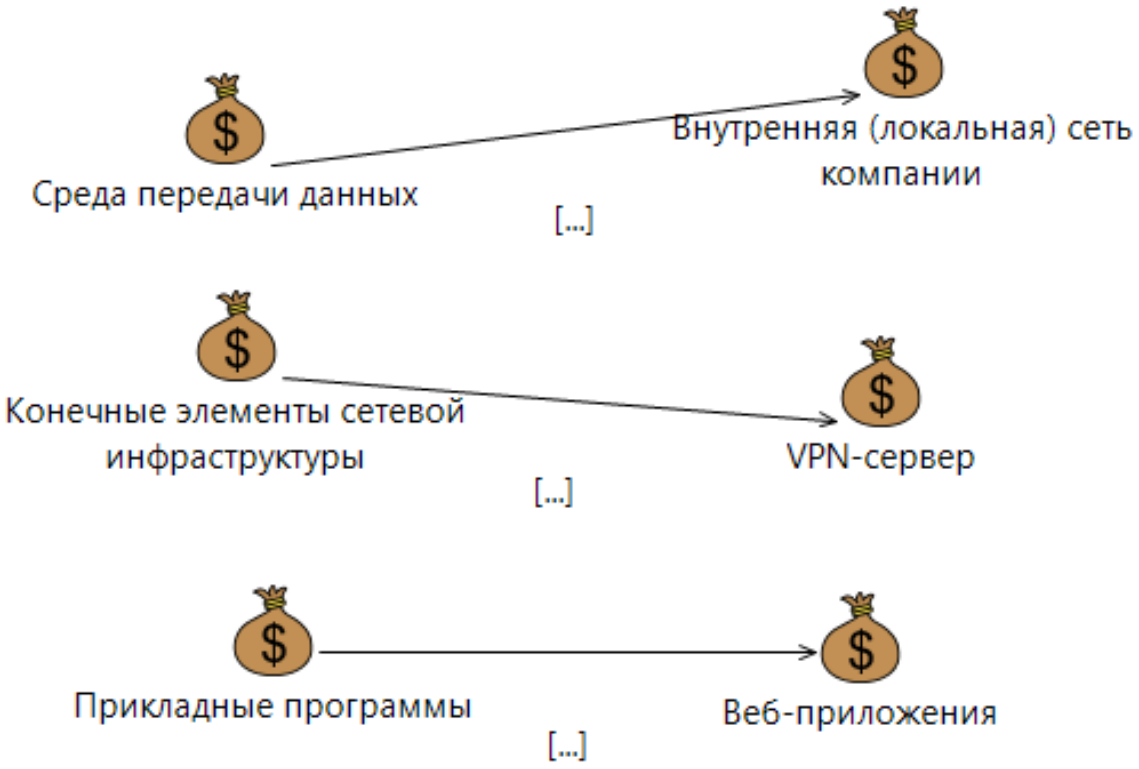

Рисунок 65 – Перечень защищаемых активов

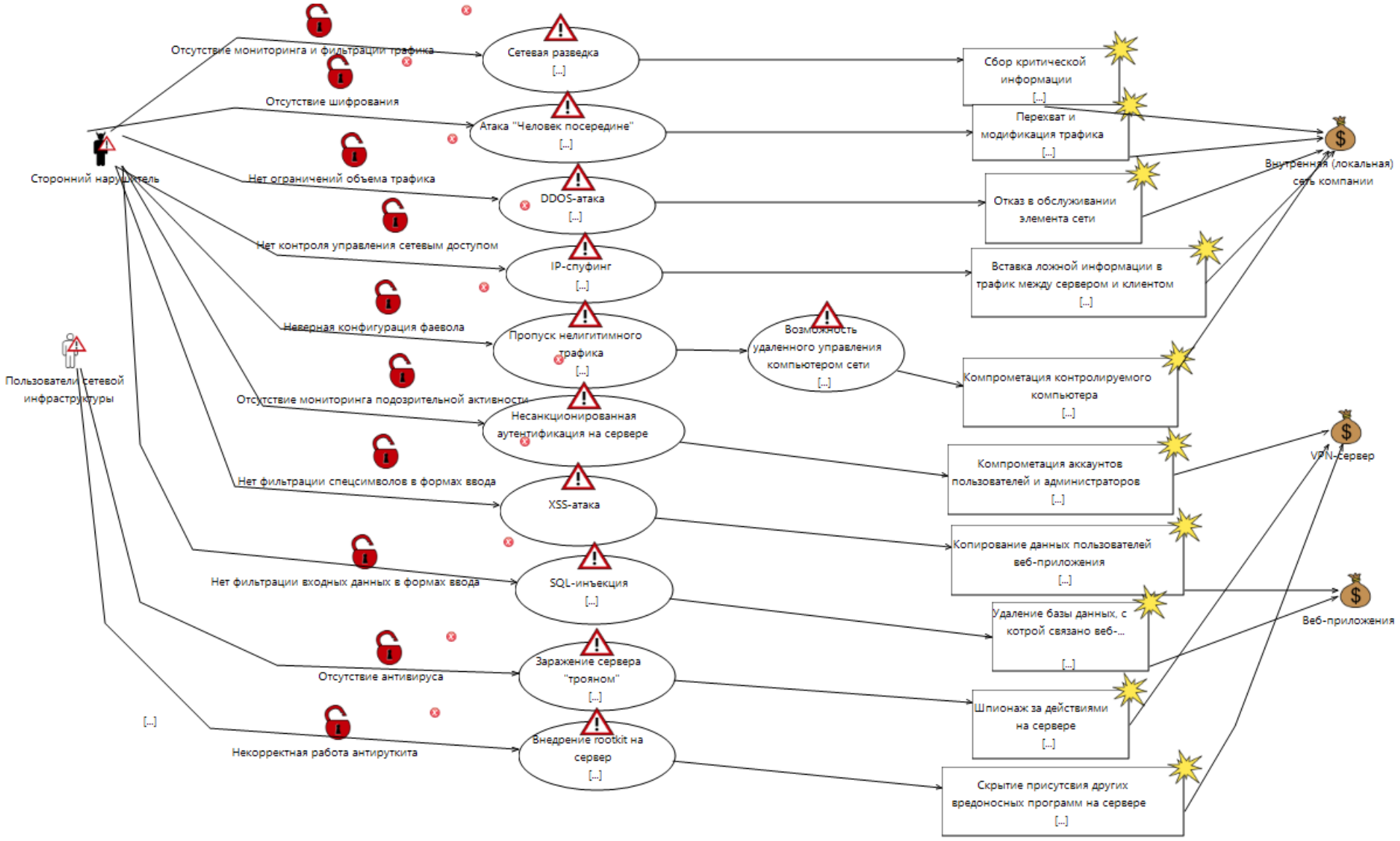

Рисунок 66 – Модель угроз

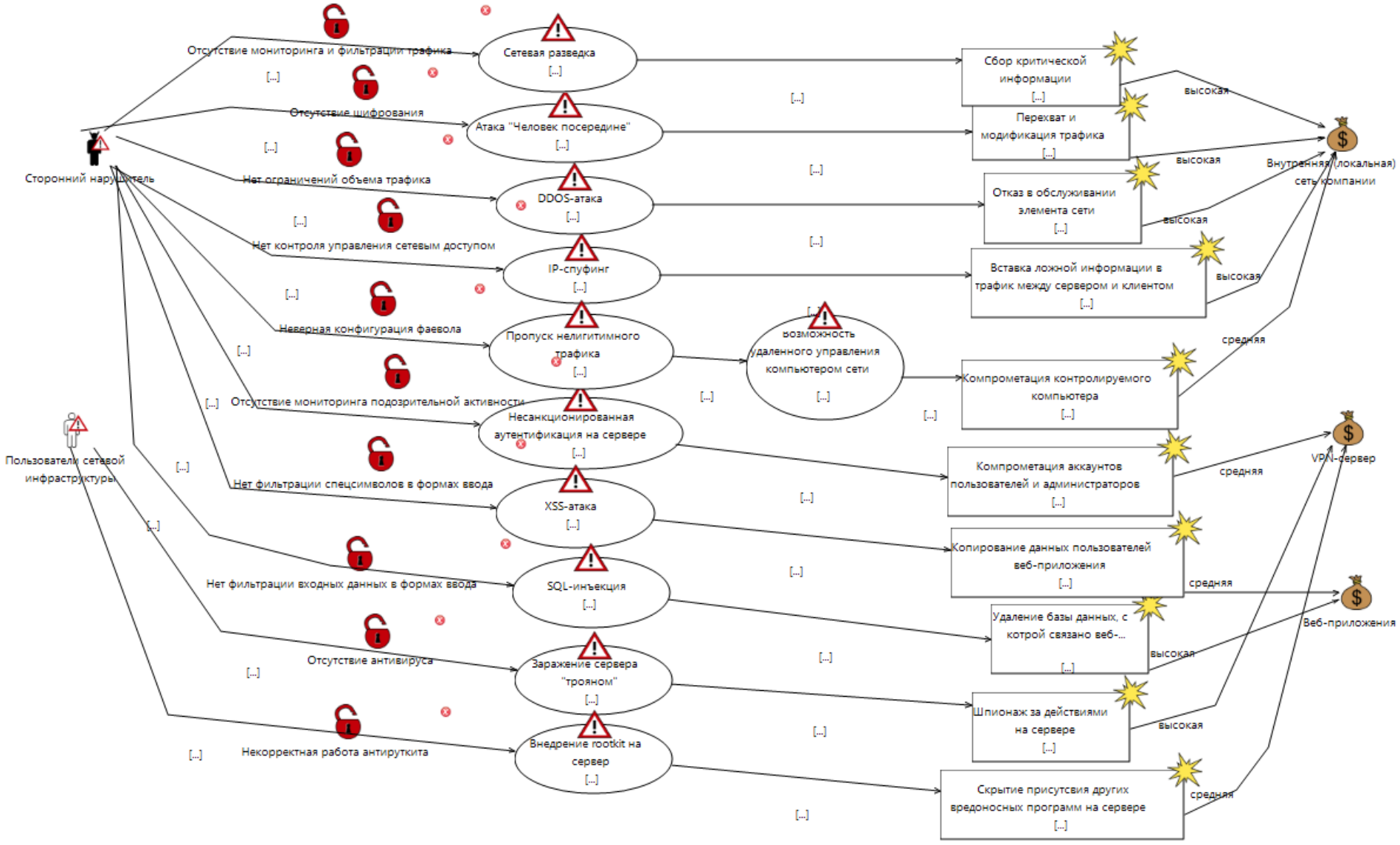

Рисунок 67 - Модель угроз с учетом вероятности возникновения инцидента

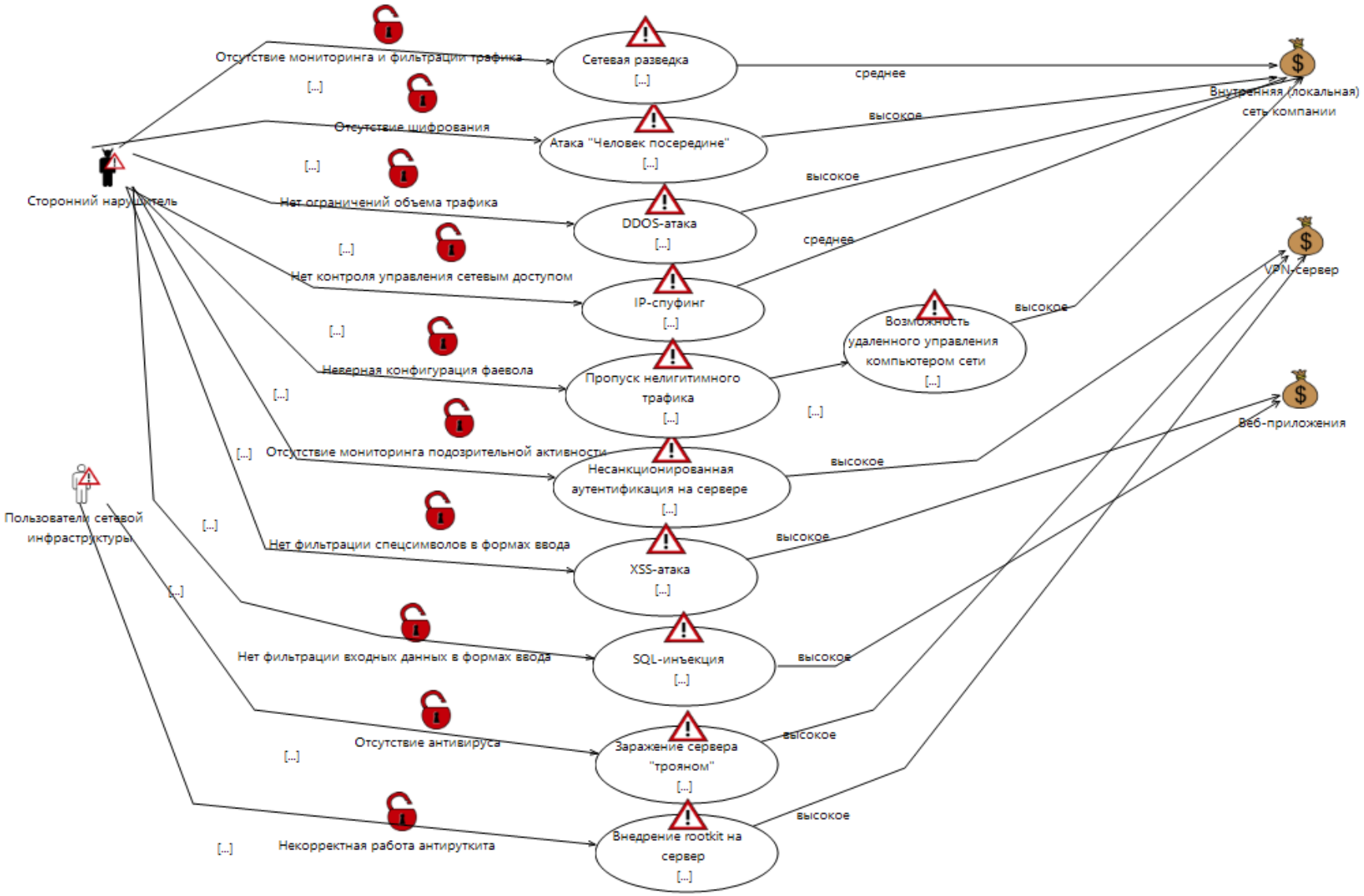

Рисунок 68 – Диаграмма рисков с характеристиками влияния угроз

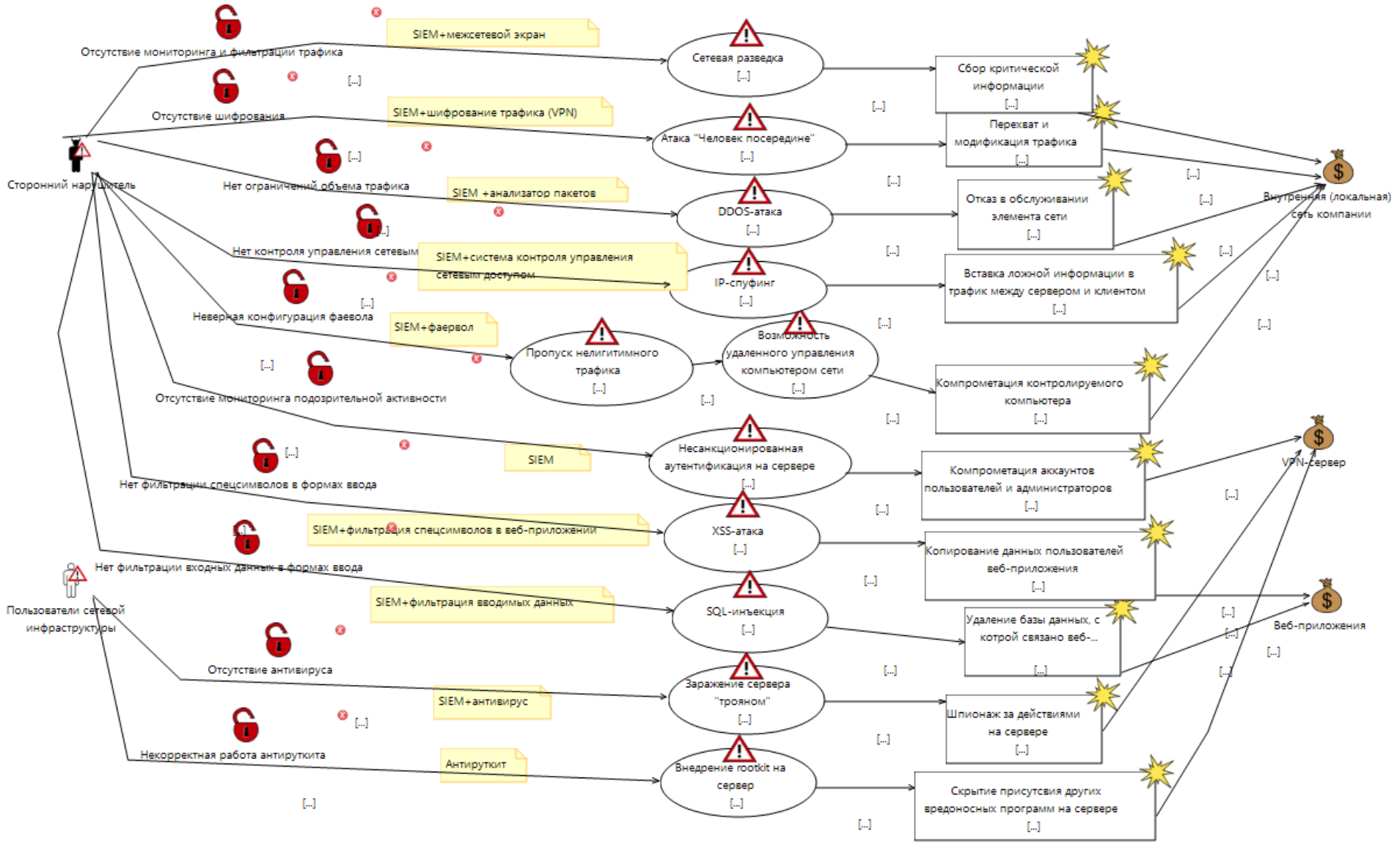

Рисунок 69 – Модель угроз с учетом защитных мер

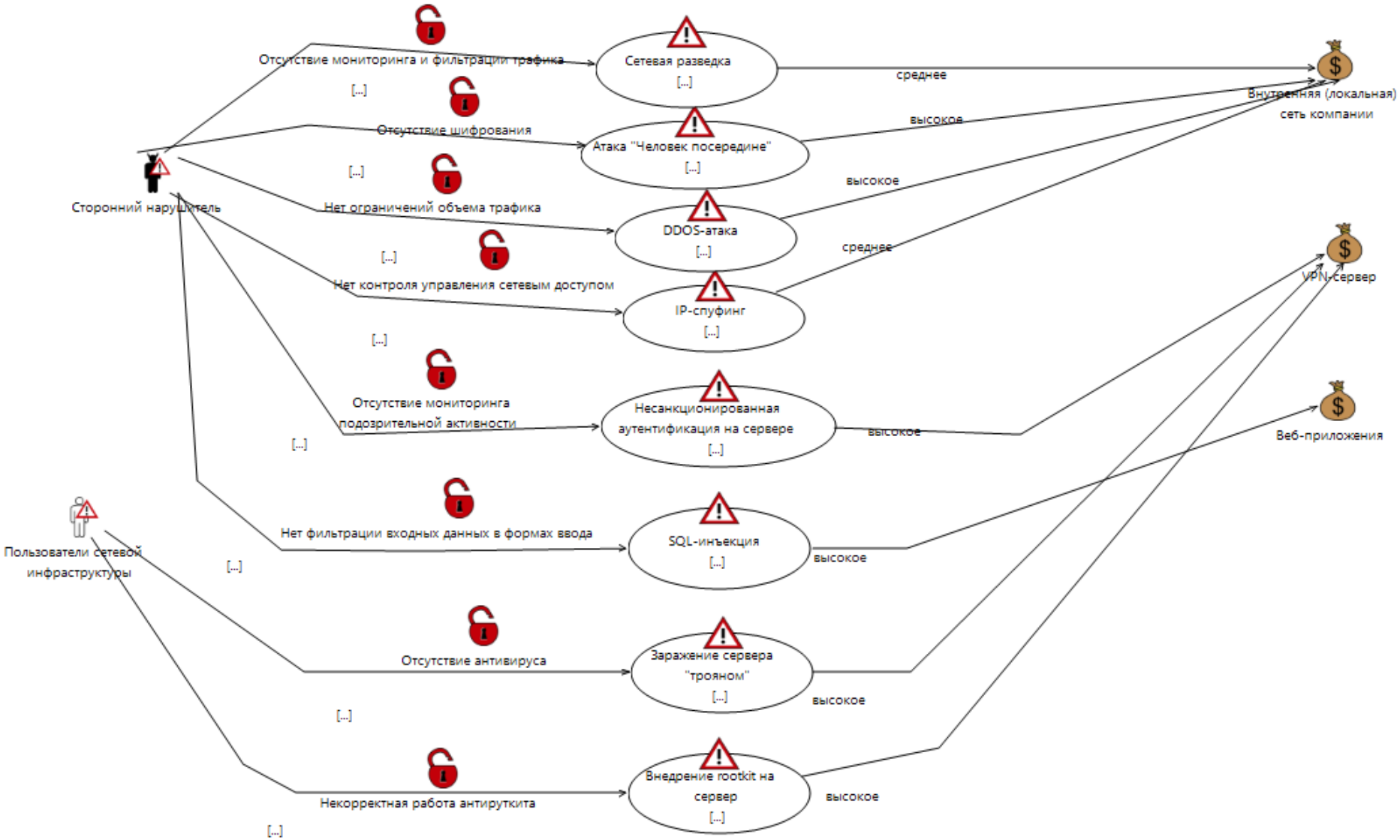

Рисунок 70 – Диаграмма недопустимых рисков

4.4 Выводы

Задача состояла в том, чтобы, опираясь на тему дипломной работы, выделить наиболее важные активы, подлежащие защите, и проанализировать рисковые ситуации для данных активов, а также произвести расчет максимальных рисков и остаточных (рисков, остающихся после внедрения защитных мер). Расчет максимальных рисков показал, что все рисковые ситуации не являются приемлемыми (численное значение рисков составило от 5 до 8 по восьмибалльной шкале), и для них необходимо внедрять меры по обработке рисков. Так как дипломная работа посвящена SIEM – системе, наряду с мерами защиты при анализе рисков SIEM – система внедрялась как средство мониторинга, работающее в связке с другими мерами защиты. Повторный перерасчет (расчет остаточного риска) показал, что после внедрения данных мер риски стали приемлемыми. С учетом того, насколько высоки были первичные риски, и какой ущерб могла бы понести компания при реализации угроз, использование мер защиты, внедренных для обработки рисков, является приемлемым и рентабельным. В среднем риски после принятия вышеуказанных мер обработки уменьшились в 4 раза (к примеру, первичный риск составлял 8 по восьмибалльной шкале, а остаточный - 2).

Заключение

Для достижения поставленных целей и решения предложенной задачи была проделана следующая работа:

- изучены структура и принцип работы SIEM систем;
- произведена сравнительная работа популярных систем на рынке;
- описана система FortiSIEM;
- продемонстрирована работа с инцидентами;
- поднят VPN-сервер.

Практическую ценность в данной работе. Во-первых, освоил и укрепил свои навыки работы с SIEM системой. Во-вторых, проект был успешно внедрен и использован по назначению и имеет актуальность на данный момент.

В ходе выполнения дипломной работы было продемонстрировано работа с облачной системой FortiSIEM.

Данная система предназначена для компаний различных масштабов. С помощью данной системы над каждым пользователем корпоративной сети будет вестись мониторинг деятельности внутри и вне сети.

Был подробно освоено поднятие VPN-сервера на операционной системе Linux Debian 9.5.

Список сокращений

SIEM - Security Information And Event Management (Информация о безопасности и управление событиями).

SIM – Security Information Management (Управление информацией о безопасности).

SEM – Security Event Management (Управление событиями безопасности).

VPN – Virtual Private Network (Виртуальная частная сеть).

CMDB – Configuration Management Database (База данных управления конфигурациями).

ИБ – Информационная безопасность.

SOC - Security operations center (Оперативный центр безопасности).

СМСБ - Системы мониторинга событий безопасности.

НСД - Несанкционированный доступ.

IDS – Intrusion detection system (Система обнаружения вторжений).

IPS - Intrusion prevention system (Система Предотвращения Вторжения).

DLP – Data leak prevention (Предотвращение утечек).

СУБД - Система управления базами данных.

ПО – Программное обеспечение.

КВИ - Критический важная инфраструктура.

ИТ – Информационные технологии.

ИС – Информационные системы.

ОС - операционная система.

UDP - User Datagram Protocol (Протокол пользовательских датаграмм).

TCP – Transmission Control Protocol (Протокол управления передачей).

СОВ – Система обнаружения вторжений.

МЭ – Межсетевые экраны.

Список литературы

1 Википедия – свободная энциклопедия // Wikipedia.org: «SIEM». URL: https://ru.wikipedia.org/wiki/SIEM (дата обращения: 06.03.2020).

2 SecurityLab // SecurityLab.ru: Олеся Шелестова «Что такое SIEM?». URL: http://www.securitylab.ru/4300777.php (дата обращения: 02.04.2020).

3 Официальный сайт компании Forti // Fortinet.com: FortiSIEM - мощная технология управления информационной безопасностью и событиями. URL: https://www.fortinet.com/ru/products/siem/fortisiem (дата обращения: 28.04.2020).

4 Хабр // Harrahabr.com: Дмитрий Хамакев «SIEM: ответы на часто задаваемые вопросы». URL: https://habrahabr.ru/post/172389/ (дата обращения: 29.04.2020).

5 Setevoi // Setevoi.ru: Максим Гарусев. «Системы корреляции событий: революция или эволюция?». URL: http://www.setevoi.ru/cgi-bin/text.pl/magazines/2003/7/30 (дата обращения: 03.05.2020).

6 Jet Info ИТ-портал компании «Инфосистемы Джет» // JetInfo.ru: Артем Медведев «самый безопасный SOC». URL: http://www.jetinfo.ru/stati/samyj-bezopasnyj-soc/#1 (дата обращения: 03.05.2020).

7 Официальный сайт компании RuSIEM // RuSIEM.com: «RuSIEM». URL: https://rusiem.com/ (дата обращения: 14.05.2020).

8 Официальный сайт RSA Witness // Rsa.com: «Rsa NetWitness SIEM». URL: https://www.rsa.com/en-us/products/threat-detection-response (дата обращения: 25.05.2020).

9 Официальный сайт anti-malware // https://www.anti-malware.ru URL: https://www.anti-malware.ru/compare/SIEM-systems (дата обращения: 25.05.2020).

10 Официальный сайт vc // https://www.vc.ru URL: https://vc.ru/dev/66942-sozdaem-svoy-vpn-server-poshagovaya-instrukciya (дата обращения: 25.05.2020).

11 Официальный сайт fortinet // https://www.fortinet.com URL: https://help.fortinet.com/fsiem/5-1-0/Online-Help/HTML5_Help/Importing_malware_url_information.htm (дата обращения: 25.05.2020).

12 Официальный сайт security-microtest // https://www.security-microtest.ru.com URL: http://security-microtest.ru/resheniya/information-security-management/security-information-and-event-management/ (дата обращения: 25.05.2020).

13 Официальный сайт «ООО ИТБ» // Itb.spb.ru: «Security Capsule SIEM». URL: https://www.itb.spb.ru/3_2_2.php (дата обращения: 25.05.2020).

14 Обзор SIEM систем: SIEM Analytics // Siem.guru: Алексей Герасимов. «Сравнение SEIM – систем». URL: http://siem.guru/compare_SIEM_systems.php (дата обращения: 29.05.2020).

15 Проведение специальной оценки условий труда // Asot.ru: Классификация опасных и вредных производственных факторов. URL: https://asout.ru/klassifikatsiya-opasnyih-i-vrednyih-proizvodstvennyih-faktorov (дата обращения 02.06.2020).

16 Охрана труда // Protrud.com: Опасные и вредные производственные факторы. URL: https://www.protrud.com/ опасные-и-вредные-производственные-факторы/ (дата обращения 02.06.2020).

17 Учебные материалы // Works.doklad.ru: Опасные и вредные производственные факторы. URL: https://works.doklad.ru/view/xFydZ1T5NZ4.html (дата обращения: 02.06.2020).

18 Журнал Отдел кадров // Otdelkadrov.by: Охрана труда в офисе. URL: https://otdelkadrov.by/number/2013/3/320136/ (дата обращения 02.06.2020).