

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

**Колледж программирования и кибербезопасности**

КУРСОВОЙ ПРОЕКТ

СПЕЦИАЛЬНОСТЬ 10.02.05

Обеспечение информационной безопасности автоматизированных систем

**на тему:**

Обеспечение эффективного управления безопасностью в корпоративной сети ГУП «Московский метрополитен»

Выполнил студент:

группы ЩИКО–02–22 (ИБ–42)

М.О. Маркаров

подпись ФИО студента

Руководитель

П.С. Дмитренко

подпись ФИО руководителя

Нормоконтроль

В.Ю. Герасин

подпись ФИО руководителя

Москва 2025

|  |  |
| --- | --- |
|  | **Утверждаю** |
|  | Председатель ПЦК  «Информационной безопасности» .\_\_\_\_\_\_\_\_\_\_\_\_\_\_.*Герасин В.Ю.*.  *подпись ФИО* |
|  | «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_2025 г. |
| **ЗАДАНИЕ** | |
| **на курсовой проект** | |

|  |  |  |
| --- | --- | --- |
| студенту | Маркарову Михаилу Оганесовичу | группы ЩИКО–02–22 |
| по специальности | 10.02.05 Обеспечение информационной безопасности  автоматизированных систем | |

|  |  |
| --- | --- |
| **Тема** | Обеспечение эффективного управления безопасностью в корпоративной сети ГУП «Московский метрополитен» |
| **Пояснительная записка** | |
| **Введение** | |
| **1 Аналитический раздел**  1.1 Анализ и описание предприятия  1.2 Законодательные и нормативно–правовые акты федерального уровня, регламентирующие обеспечение информационной безопасности  [1.3 Анализ моделей рисков и злоумышленников](#_Toc207714001) | |
| **2 Исследовательский раздел**  2.1 Проектирование архитектуры системы защиты  2.2 Проведение атаки на рабочую станцию с целью выявления уязвимостей сети  2.3 Функциональность и роль выбранных систем в архитектуре безопасности  **3 Технический раздел**  3.1 Настройка модуля контроля сети и обнаружения вторжений  3.2 Реализация настройки политик контроля доступа и целостности 3.3 Внедрение системы автоматического мониторинга | |
| **Заключение**  **Список использованных источников**  **Графическая часть проекта** | |

Приложение к заданию на курсовой проект

В информационную систему ГУП «Московский метрополитен» необходимо внедрить комплекс программных средств Secret Net Studio для обеспечения комплексной защиты от угроз сетевых атак. Для этого необходимо реализовать модуль контроля сети, предназначенный для защиты сетевых узлов и оповещения об атаках.

Система защиты должна использовать модуль контроля сетевого трафика для анализа и фильтрации передаваемых данных в реальном времени, блокируя потенциально опасные соединения и несанкционированные попытки обмена информацией.

Для обеспечения соответствия установленным классам защищенности автоматизированной системы должны быть настроены параметры пользователей. Дополнительно для формирования целостной картины безопасности должен быть обеспечен просмотр всех системных событий и централизованный мониторинг благодаря интеграции с системой RuSIEM, которая осуществляет сбор, корреляцию и анализ данных с всех компонентов комплекса защиты.

|  |  |  |  |
| --- | --- | --- | --- |
| Задание на курсовой проект выдал | « » 202 г. |  | *Дмитренко П.С.* |
|  |  | *Подпись руководителя проекта* | *ФИО руководителя проекта* |
| Задание на курсовой проект получил | « » 202 г. |  | *Маркаров М.О.* |
|  |  | *Подпись студента– исполнителя проекта* | *ФИО студента– исполнителя проекта* |

**Срок представления к защите курсового проекта: до** « » 2025 г.

## **СОДЕРЖАНИЕ**

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И УЛОВНЫХ ОБОЗНАЧЕНИЙ 3

ВВЕДЕНИЕ 4

1 АНАЛИТИЧЕСКИЙ РАЗДЕЛ 6

1.1 Анализ и описание предприятия 6

1.2 Нормативно правовые акты, регламентирующие обеспечение информационной безопасности 9

1.3 Анализ моделей рисков и злоумышленников 12

2 ИССЛЕДОВАТЕЛЬСКИЙ РАЗДЕЛ 15

2.1 Проектирование архитектуры системы защиты 15

2.2 Проведение атаки на рабочую станцию с целью выявления уязвимостей сети 18

2.3 Функциональность и роль выбранных систем в архитектуре безопасности 22

3 ТЕХНИЧЕСКИЙ РАЗДЕЛ 25

3.1 Настройка модуля контроля сети и обнаружения вторжений 25

3.2 Реализация настройки политик контроля доступа и целостности 28

3.3 Внедрение системы автоматического мониторинга 31

ЗАКЛЮЧЕНИЕ 35

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 36

# **ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ**

|  |  |  |
| --- | --- | --- |
| APT | – | англ. Advanced Persistent Threat – целенаправленная постоянная угроза. |
| ARP | – | англ. Address Resolution Protocol – протокол разрешения адресов. |
| CMS | – | англ. Content Management System – система управления контентом. |
| CPU | – | англ. Central Processor Union – центральный процессор. |
| HTTP | – | англ. Hyper Text Transfer Protocol – протокол передачи гипертекстов. |
| MITM | – | англ. Man-in-the-Middle – человек посередине. |
| RAM | – | англ. Random Access Memory – оперативное запоминающее устройство. |
| SSD | – | англ. Solid–State Disk – твердотельный накопитель. |
| SNS | – | англ Secret Net Studio – программный комплекс для защиты информации |
| БД | – | База данных. |
| ГУП | – | Государственное унитарное предприятие. |
| ГОСТ | – | Государственный стандарт. |
| ИБ | – | Информационная безопасность. |
| ИТ | – | Информационные технологии. |
| КИИ | – | Критическая информационная инфраструктура. |
| ОC | – | Операционная система. |
| ПО | – | Программное обеспечение. |
| СЗИ | – | Система защиты информации. |
| СУБД | – | Cистема управления базами данных. |
| ФЗ | – | Федеральный закон. |
| ФСБ | – | Федеральная служба безопасности. |
| ФСТЭК | – | Федеральная служба по техническому и экспортному контролю. |

# 

# **ВВЕДЕНИЕ**

В постиндустриальном мире, характеризующемся повсеместной цифровизацией, технологии и инструменты обеспечения информационной безопасности играют критически важную роль в защите государственной безопасности, национальных интересов, а также прав граждан. Однако в условиях постоянной и динамической эволюции киберугроз сохраняется высокий уровень инцидентов информационной безопасности, а в обозримой перспективе вероятна эскалация кибератак, последствия которых будут носить более масштабный, тяжелый и долгосрочный характер. В связи с этим вопросы защиты информации остаются крайне актуальными и требуют непрерывного развития.

Неотъемлемой частью обеспечения комплексной защиты информации является своевременный мониторинг событий информационной безопасность в условиях, растущих и меняющихся киберрисков. Это обуславливает необходимость проведения регулярного анализа защищенности корпоративных информационных систем для выявления и устранения уязвимостей до их эксплуатации злоумышленниками.

Целью курсового проекта является установка и настройка комплекса средств системы мониторинга и программного обеспечения (далее – SNS англ. Secret Net Studio – программный комплекс для защиты информации) для контроля уровнями доступа пользователей в корпоративной сети государственное унитарное предприятие (далее – ГУП) «Московский метрополитен».

Для достижения поставленной цели необходимо решить следующие задачи:

* анализ организационной структуры;
* изучение существующей нормативно–правовой базы;
* проведения анализа внутренних структуры и функционирования корпоративной сети;
* осуществить установку и настройку (далее – СЗИС – система защиты информации);
* разграничение прав пользователей и обеспечение среды;
* сформировать модель угроз для выявления потенциальных уязвимостей и рисков.

Результатом курсового проекта является успешно реализованная комплексная система обеспечения информационной безопасности в корпоративной сети ГУП «Московский метрополитен».

# **АНАЛИТИЧЕСКИЙ РАЗДЕЛ**

## **1.1 Анализ и описание предприятия**

Государственное унитарное предприятие ГУП «Московский метрополитен» является корпорацией транспортной инфраструктуры столицы и относится к категории критической информационной инфраструктуры Российской Федерации.

Основные направления деятельности предприятия включают в себя:

* перевозку пассажиров метрополитеном;
* техническое обслуживание;
* ремонт транспортных средств подвижного состава;
* содержание и развитие инфраструктуры метрополитена.

В ГУП «Московский метрополитен» осуществляются следующие основные виды транспортного обслуживания в рамках бюджетного финансирования, системы городских заказов и внебюджетной деятельности:

* регулярные пассажирские перевозки на линии метрополитена;
* эксплуатация и техническое обслуживание подвижного состава;
* обеспечение транспортной доступности и бесперебойности работы метро;
* предоставление услуг по организации перевозок для городских нужд;
* реализация инвестиционных проектов по развитию метрополитена.

Руководящими лицами являются: начальник метрополитена; первый заместитель начальника метрополитена по пассажирской работе; главный инженер первый заместитель начальника метрополитена; первый заместитель начальника метрополитена.

Так же в каждом депо и эксплуатационной службе работают инженеры, техники и обслуживающий персонал, которые составляют основу эксплуатационного штата предприятия. В структуре метрополитена функционирует дирекция по информационным технологиям и служба информационной безопасности, сотрудники которых осуществляют непрерывный мониторинг, аудит и защиту информационных ресурсов и технологических систем предприятия.

В Приложении 1 представлена схема организационной структуры ГУП «Московский метрополитен», отражающая структуру подчинения, функциональные взаимосвязи между подразделениями и зоны ответственности ключевых специалистов. Схема имеет как эксплуатационные службы, так и обеспечивающие подразделения.

Программные обеспечения для рабочих станций включают в себя:

* пакет Microsoft Office для работы с электронной почтой, документами, электронными таблицами и презентациями;
* Система управления контентом (далее – CMS англ. Content Management System) для управления контентом на сайте и социальных сетях;
* системы мониторинга и управления сетью для мониторинга сетевых узлов, управления беспроводными сетями и обеспечения безопасности сети;
* Программное обеспечение (далее – ПО) Kaspersky Total Security для обеспечения много–комплексной защиты рабочих станций от программно–аппаратных и программно–технических угроз.

Этот набор информационных ресурсов и программного обеспечения обеспечивает функционирование различных отделов предприятия и средства для противодействия к кибератакам.

Для выполнения стабильной и эффективной работы критически важных подразделений, к техническим характеристикам персональных компьютеров предъявляются следующие требования.

Для сотрудников и отделов службы безопасности, служба инвестиционного развития и ситуационного центра рассматриваются выполнения стандартных офисных задач, работы с документами и корпоративными приложениями с помощью комплектующих такими как:

* центральный процессор (далее – CPU англ. Central Processing Unit): IntelCore i7 поколение не ниже 10–го;
* оперативная память (далее – RAM англ. Random Access Memory – оперативное запоминающее устройство):8 ГБ DDR4;
* Твердотельный накопитель данных (далее – SSD англ. Solid–State Disk): 256 ГБ (твердотельный накопитель типа SSD);
* Операционная система (далее – ОC): Microsoft Windows 10 Pro (64–битная, лицензионная версия с актуальными обновлениями безопасности).

Для сотрудников подразделений, выполняющих задачи, связанные с обработкой больших объемов данных, проектированием, анализом и управлением сетевой инфраструктурой к этой категории относятся служба (далее – ИТ – информационные технологии) и служба связи.

Требуются высокопроизводительные рабочие станции. В эту категорию входят комплектующие:

* центральный процессор CPU: Intel Core i9 (поколение не ниже 12–го);
* оперативная память RAM: 16 ГБ DDR4 (рекомендуется возможность последующего расширения);
* накопитель данных SSD: 512 ГБ (высокоскоростной твердотельный накопитель типа NVMe SSD;
* ОС: Microsoft Windows 10 Pro (64–битная, лицензионная версия с актуальными обновлениями безопасности).

Для сотрудников метрополитена и IT–специалистов будут использоваться компьютеры HP Z2 G5 TWR, под управлением операционной системы Windows 10 Pro. Внешний вид устройства представлен на рисунке 1.



Рисунок 1 – рабочая станция HP Z2 Tower G5

Указанные конфигурации рабочих станций разработаны для обеспечения эффективной работы сотрудников метрополитена в корпоративной сети, включая выполнение офисных задач, обработку данных, анализ и управление инфраструктурой. Они обеспечивают необходимую производительность, безопасность и совместимость с корпоративными приложениями.

## **1.2 Законодательные и нормативно–правовые акты федерального уровня, регламентирующие обеспечение информационной безопасности**

В своей деятельности ГУП «Московский метрополитен» руководствуется следующими нормативно–правовыми актами в области информационной безопасности федеральный закон (далее – ФЗ) от 27 июля 2006 г. N 149–ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями):

* статья 15. Использование информационно–телекоммуникационных сетей;
* статья 16.2. Мониторинг информационно–телекоммуникационных сетей, в том числе сети "Интернет";

статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

ФЗ от 26.07.2017 № 187–ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»:

* статья 4. Принципы обеспечения безопасности критической информационной инфраструктуры;
* статья 7. Категорирование критической информационной инфраструктуры;
* статья 8. Требования к обеспечению безопасности значимых критической информационной инфраструктуры;
* статья 9. Права и обязанности субъектов критической информационной инфраструктуры;
* статья 10. Государственный контроль в области безопасности критической информационной инфраструктуры.

ФЗ от 27.07.2006 № 152–ФЗ «О персональных данных»:

* статья 6. Условия обработки персональных данных;
* статья 7. Конфиденциальность персональных данных;
* статья 18.1. Меры по обеспечению безопасности персональных данных при их обработке;
* статья 19. Обязанности оператора при обращении к нему субъекта персональных данных;
* статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях;
* постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требовании по обеспечению безопасности значимых точек критической информационной инфраструктуры Российской Федерации»;
* приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
* приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

ФЗ от 06.04.2011 № 63–ФЗ «Об электронной подписи»:

* статья 10. Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей;
* статья 11. Признание квалифицированной электронной подписи.

Уголовную ответственность в сфере компьютерных атак регулирует уголовный кодекс Российской Федерации от 13.06.1996:

* статья 272. Неправомерный доступ к компьютерной информации;
* статья 273. Создание, использование и распространение вредоносных компьютерных программ;
* статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно–телекоммуникационных сетей;
* статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Правомерность проводимых работ по обеспечению информационной безопасности определяется следующими нормативно–правовыми актами:

* Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
* (далее – ГОСТ – государственный стандарт) Р 58143–2018 «Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения»;

В связи с тем, что ГУП «Московский метрополитен» функционирует как объект транспортной инфраструктуры, предприятие дополнительно руководствуется:

* Федеральным законом от 09.02.2007 № 16–ФЗ «О транспортной безопасности»;
* Приказами Минтранса России в области обеспечения транспортной безопасности;
* Отраслевыми стандартами и методическими рекомендациями в сфере защиты информации на объектах транспортной инфраструктуры.

Представленный перечень законодательных актов и нормативов направлен на комплексное обеспечение информационной безопасности (далее – ИБ) в деятельности ГУП «Московский метрополитен», включая защиту данных, управление рисками, контроль за использование технологий и ответственность. Они регулируют принципы, требования и механизмы защиты информации в государственных информационных системах, критической инфраструктуре и транспортной сфере.

## **1.3** [**Анализ моделей рисков и злоумышленников**](#_Toc207714001)

Модель угроз информационной безопасности корпоративной сети. Предприятия формируется на основе модели нарушителя. По критерию доступа к инфраструктуре потенциальных нарушителей разделяют на две категории:

* внешние нарушители — это физические лица или группы, не имеющие санкционированного доступа к ресурсам корпоративной сети;
* внутренними нарушителями являются физические лица, имеющие легальный доступ на территорию или к информационным ресурсам предприятия.

В Приложении 2 представлена классификация модель нарушителя и угроз информационных ресурсов корпоративной сети.

Таким образом, для ГУП «Московский метрополитен» определены категории потенциальных нарушителей и построена соответствующая модель угроз, учитывающая особенности критической информационной инфраструктуры предприятия.

Классификация нарушителей информационной безопасности, установленная ФСТЭК России, представляет собой систематизированную модель оценки потенциальных угроз на основе критериев уровня технической подготовки, характера доступа к информационным ресурсам.

Категории внешних нарушителей (H1–H4):

* H1 неквалифицированные внешние нарушители. Низкий уровень технической подготовки используют общедоступные инструменты и утилиты. Не имеют доступа к специализированному оборудованию;
* H2 квалифицированные внешние нарушители. Средний уровень технической подготовки используют модифицированные версии общедоступных инструментов, создавать простые эксплойты;
* H3 высококвалифицированные внешние нарушители. Высокий уровень технической подготовки. Разрабатывают специализированные инструменты атак используют цепочки уязвимостей;
* H4 организованные группы внешних нарушителей. Коллектив высококвалифицированных специалистов. Используют сложные целевые атаки (далее – APT с англ. Advanced Persistent Threat – целенаправленная постоянная угроза.) имеют значительные ресурсы и финансирование.

Таким образом, проведенный анализ позволил классифицировать потенциальных нарушителей информационной безопасности ГУП «Московский метрополитен» по критериям федеральная служба по техническому и экспортному контролю (далее – ФСТЭК) и федеральная служба безопасности (далее – ФСБ), и выявив спектр угроз со внешних, так и внутренних источников. А построенная модель угроз учитывает специфику предприятия как критической информационной инфраструктуры и выделяет наиболее вероятные сценарии атак, включая непреднамеренные действия персонала, целенаправленные действия квалифицированных злоумышленников и APT. Эта модель служит фундаментом для дальнейшего проектирования мер защиты, направленных на предотвращения выявленных рисков в корпоративной сети.

# **ИССЛЕДОВАТЕЛЬСКИЙ РАЗДЕЛ**

## **2.1 Проектирование архитектуры системы защиты**

Ежедневно обрабатываются большие объемы данных от клиентских баз до конфиденциальных документов. Простая установка антивируса или межсетевого экрана не обеспечивает надежную защиту. Для снижения рисков и обеспечения стабильной работы требуется выстроенная архитектура информационной безопасности, которая объединяет технологии, процессы и политику защиты в единую систему.

В задачи модели архитектуры безопасности имеет несколько ключевых элементов:

* минимизация рисков утечек и кибератак;
* соблюдение требований отраслевых или общих стандартов ГОСТ 27001, ГОСТ 57580;
* интеграция мер защиты в общую стратегию управления ИТ.

На Рисунке 2 представлена базовая архитектура системы защиты на базе SNS.

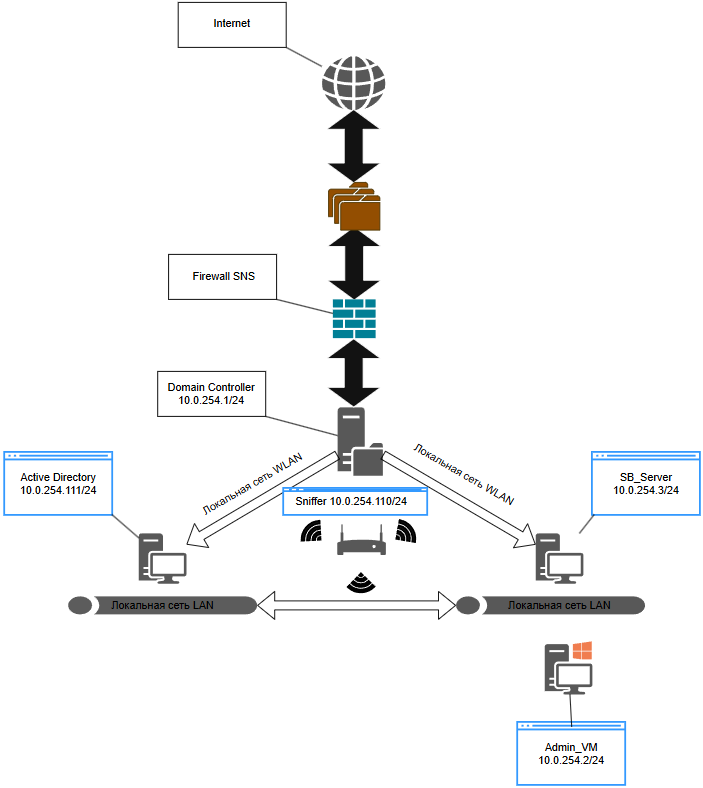


Рисунок 2 – Архитектура системы защиты на базе SNS

Архитектура решения на основе SNS включает в себя следующие сетевые элементы:

* Контроллер домена (DC) с IP–адресом 10.0.254.1/24, выполняющий функции центра аутентификации и управления политиками безопасности.
* Рабочая станция администратора (Admin\_VM) с IP–адресом 10.0.254.2/24, с которой осуществляется централизованное управление комплексом защиты.
* Сервер SNS (SBP\_Server) с IP–адресом 10.0.254.3/24, являющийся ядром системы и обеспечивающий контроль доступа, целостности и сетевую защиту рабочих станций и серверов.

Архитектура позволяет реализовать строгую аутентификацию, контролировать целостность программной среды и централизованно применять политики безопасности ко всем узлам сети.

Для обеспечения мониторинга безопасности запланировано внедрение системы RuSIEM. Агенты системы осуществляют сбор и корреляцию событий безопасности из разнородных источников, включая текстовые журналы локальных и удаленных систем.

Для обеспечения всестороннего мониторинга и оперативного реагирования на инциденты в архитектуру интегрирована система RuSIEM. Её задача — сбор, нормализация и корреляция событий безопасности из разнородных источников. Архитектура сбора данных агентом RuSIEM, представленная на рисунке 3, реализует три основных сценария:

* сбор событий безопасности и системных журналов с рабочих станций пользователей. Агент RuSIEM выполняет фильтрацию событий в соответствии с заданными политиками безопасности;
* применение инструментария WMI для мониторинга и управления компонентами компьютерной инфраструктуры. Метод предоставляет детальную информацию о состоянии системных ресурсов и показателях производительности;
* сбор, нормализация и передача событий безопасности из журналов операционной системы Windows в централизованное хранилище SIEM–системы.

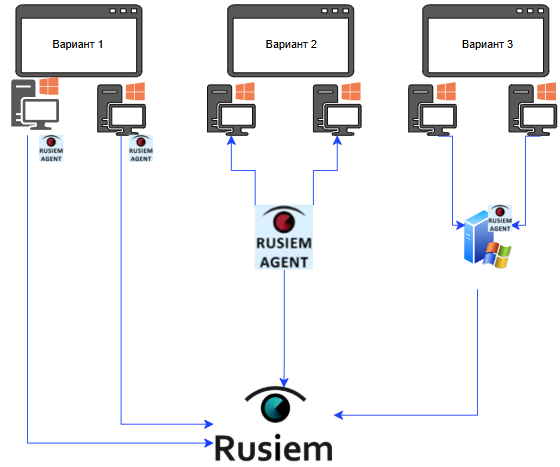


Рисунок 3 – Архитектура сбора данных агентом RuSIEM

Таким образом, в рамках проектирования архитектуры системы защиты разработана эшелонированная модель безопасности, интегрирующая два ключевых компонента: систему контроля доступа SNS и платформу мониторинга RuSIEM. Такая архитектура позволяет обеспечить комплексную защиту корпоративной сети ГУП «Московский метрополитен» за счёт централизованного управления доступом, контроля целостности узлов, обнаружения сетевых атак и оперативного реагирования на инциденты. Это формирует надёжную основу для выполнения требований регуляторов и противодействия современным киберугрозам.

## **2.2 Проведение атаки на рабочую станцию с целью выявления уязвимостей сети**

В рамках исследования безопасности корпоративной сети моделируется комплексная атака на рабочую станцию пользователя для выявления уязвимостей. В качестве цели выступала система под управлением Windows 10, а в роли злоумышленника — рабочая станция с дистрибутивом Kali Linux. Общая топология эксперимента, иллюстрирующая сценарий атаки человек посередине (далее – MITM Man-in-the-Middle – человек посередине), представлена на рисунке 4.

Такой пример топологии обосновывает, что злоумышленник, скрываясь от систем защиты, изменяет свой IP–адрес и осуществляет перехват трафика в локальной сети. Основная цель злоумышленника в этом сценарии заключается в перехвате и анализе сетевого трафика. В случае передачи незашифрованных данных это позволяет извлекать учетные данные и аутентификационные cookie из (далее – HTTP англ. Hyper Text Transfer Protocol – протокол передачи гипертекстов), а также проводить анализ передаваемой текстовой информации для получения доступа к конфиденциальным данным, передаваемым в открытом виде.

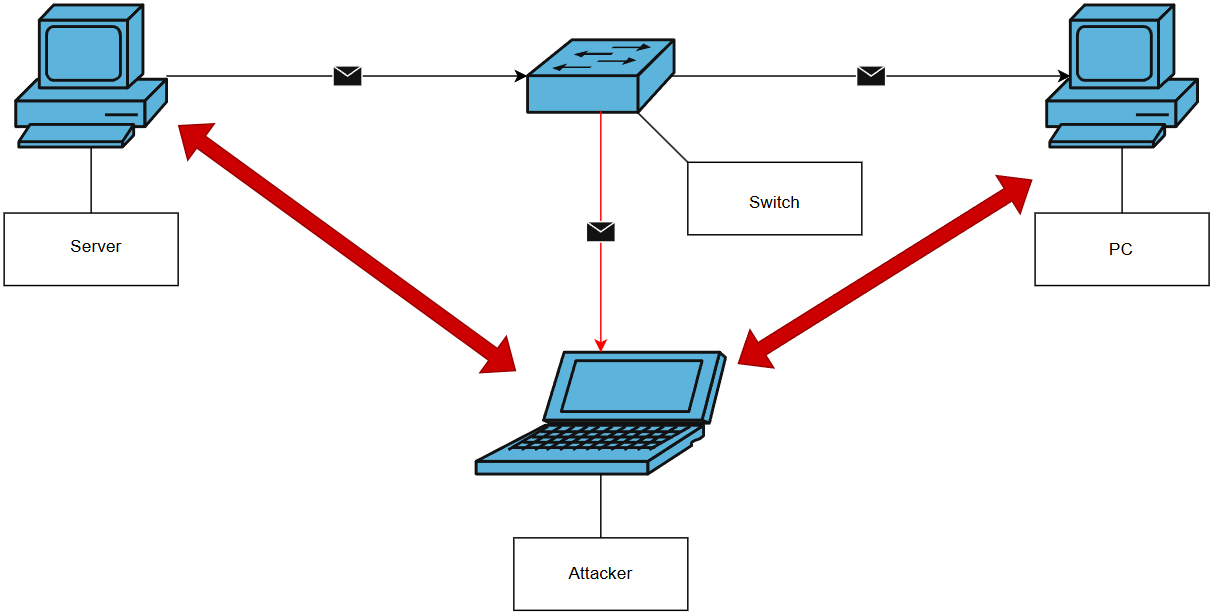


Рисунок 4 – Топология атаки человек посередине

На следующем этапе производится атака и разведка сетевой инфраструктуры. С помощью сканирования определяется перечень активных узлов в сегменте сети. Результат сканирования, отображающий устройства, подключенные к маршрутизатору, представлен на рисунке 5.

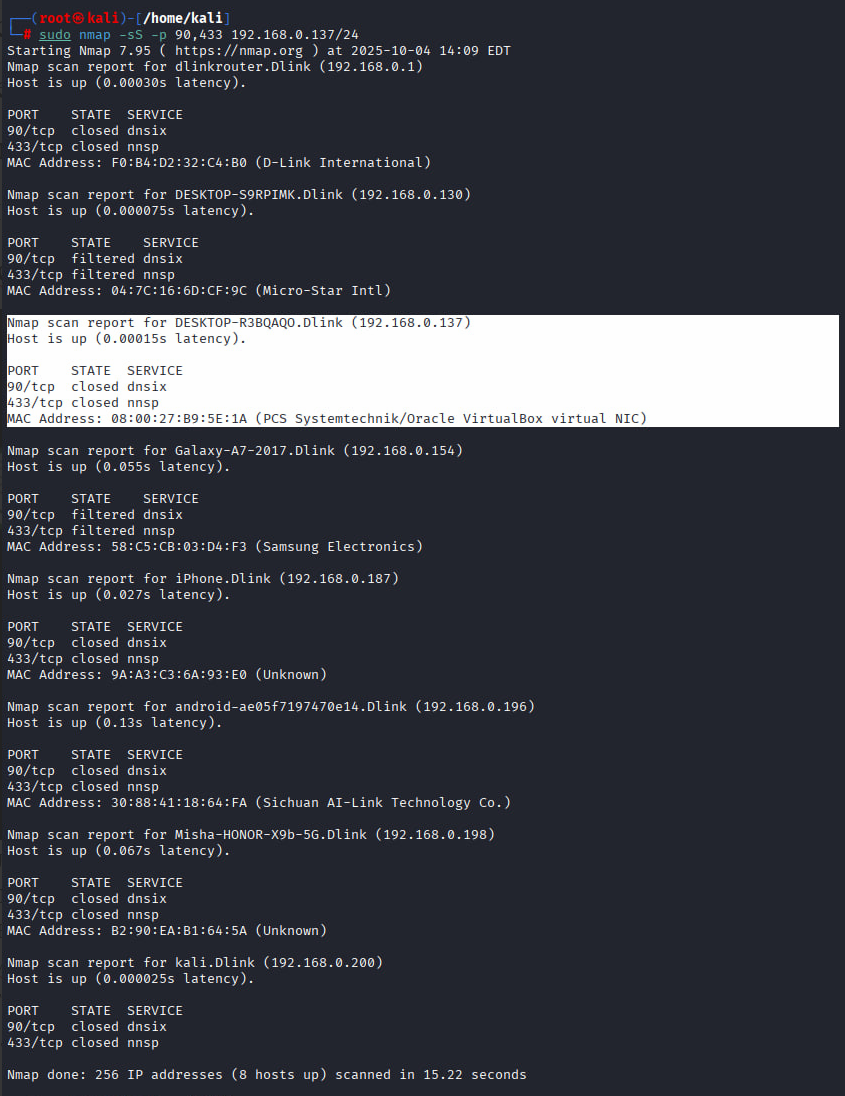


Рисунок 5 – Скан маршутизатора к которому подключены устройства

Далее выполняется подмена (далее – ARP – запросов Address Resolution Protocol – протокол разрешения адресов) с использованием утилиты arpspoof. Как показано на рисунке 6, атакующая система направляет целевой станции фиктивные ARP – ответы, представляясь маршрутизатором, и наоборот. В результате весь трафик между жертвой и шлюзом перенаправляется через компьютер злоумышленника, что позволяет осуществить перехват данных.

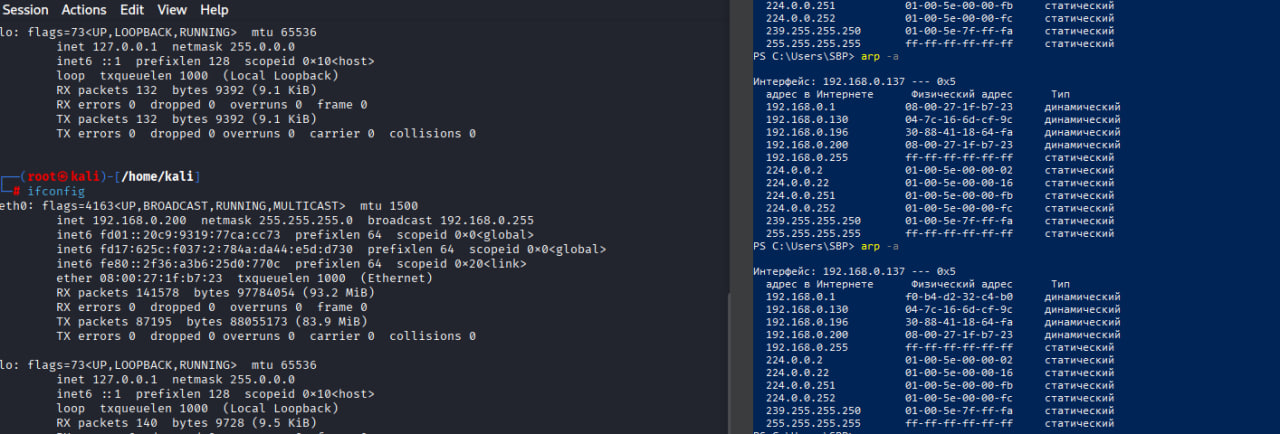


Рисунок 6 – Подмена ARP–запроса

После успешного внедрения в канал связи производится перехват сетевого трафика. Для демонстрации уязвимости передачи незашифрованных данных используется тестовый ресурс vulnweb.com. При передаче учетных данных с целевой рабочей станции атакующая сторона получает возможность в реальном времени отслеживать и извлекать конфиденциальную информацию из HTTP – запросов, что наглядно показано на рисунке 7.

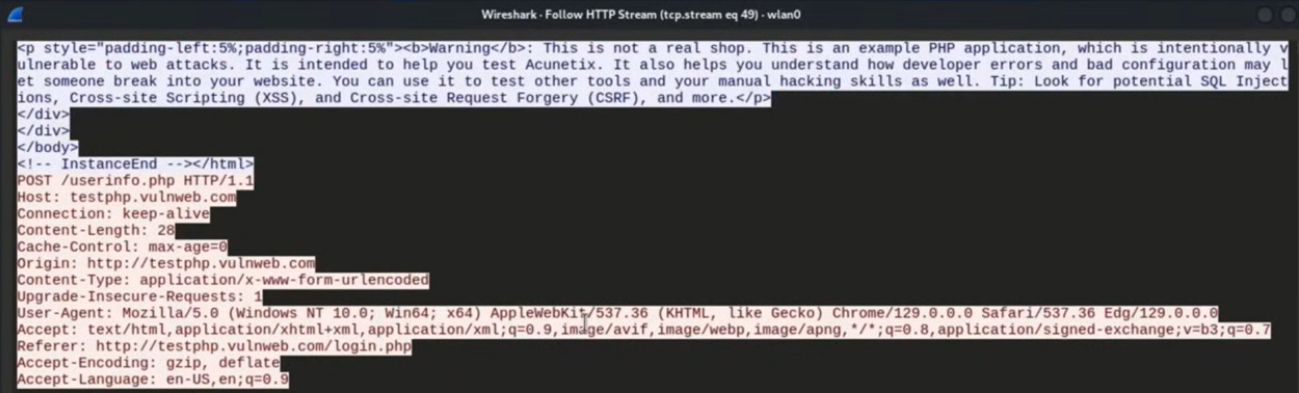


Рисунок 7 – Содержимое HTTP запроса

Далее происходит моделирование угрозы и компрометации рабочих станций для организации скрытого майнинга криптоджекинга. Для этого использован онлайн–конструктор, позволяющий сгенерировать исполняемый файл майнера крипто валюты Monero. Интерфейс конструктора с настраиваемыми параметрами, такими как адрес кошелька и пул для майнинга, представлен на рисунке 8.

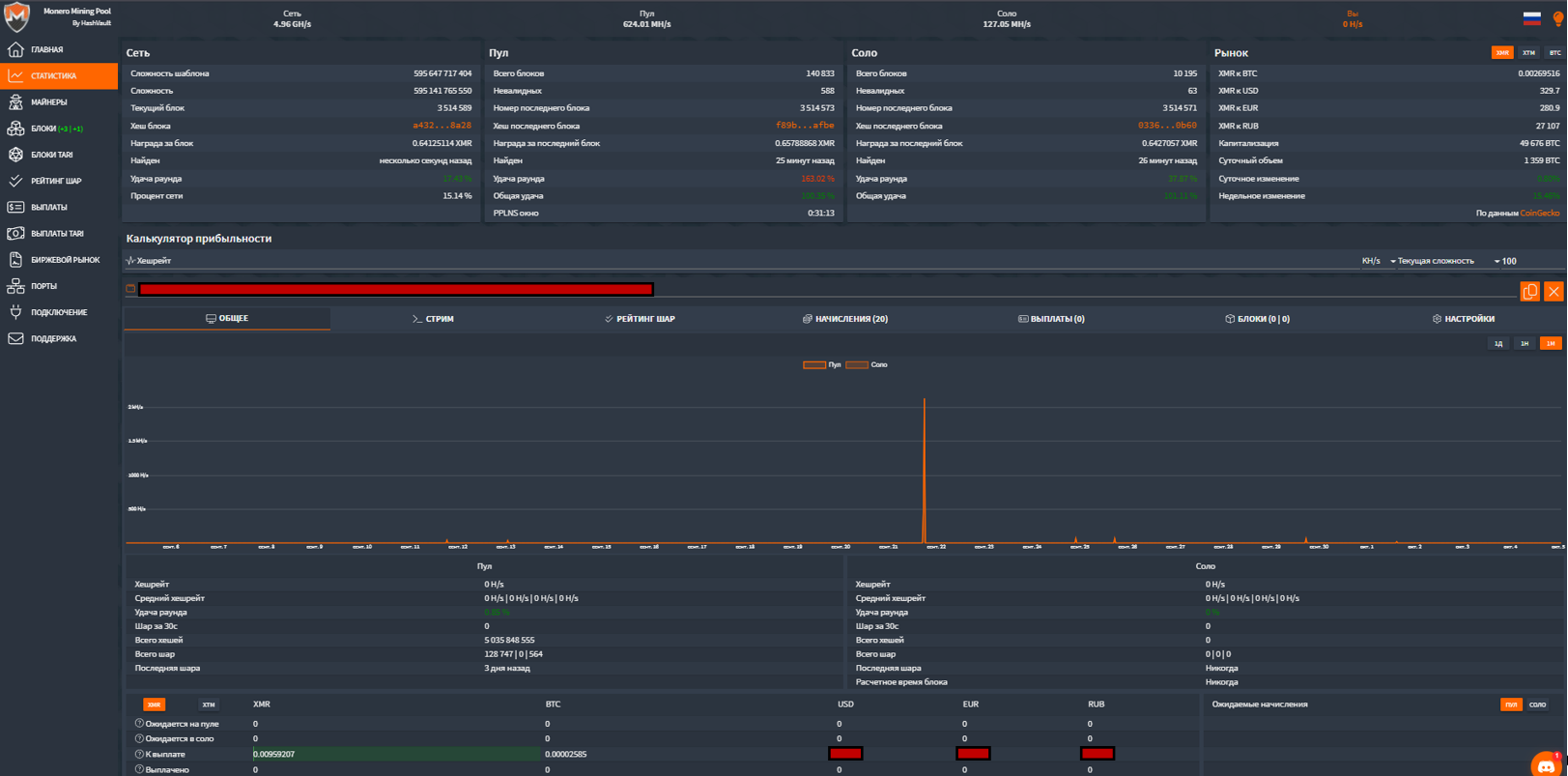


Рисунок 8 – Веб–интерфейс генератора криптоджекинга

После внедрения майнера злоумышленник получает возможность удаленного мониторинга и управления вредоносной активностью через специализированную веб–панель. Как показано на рисунках 9 и 10, панель отображает ключевые метрики: количество зараженных узлов, совокупную вычислительную мощность хешрейт и расчетный доход.

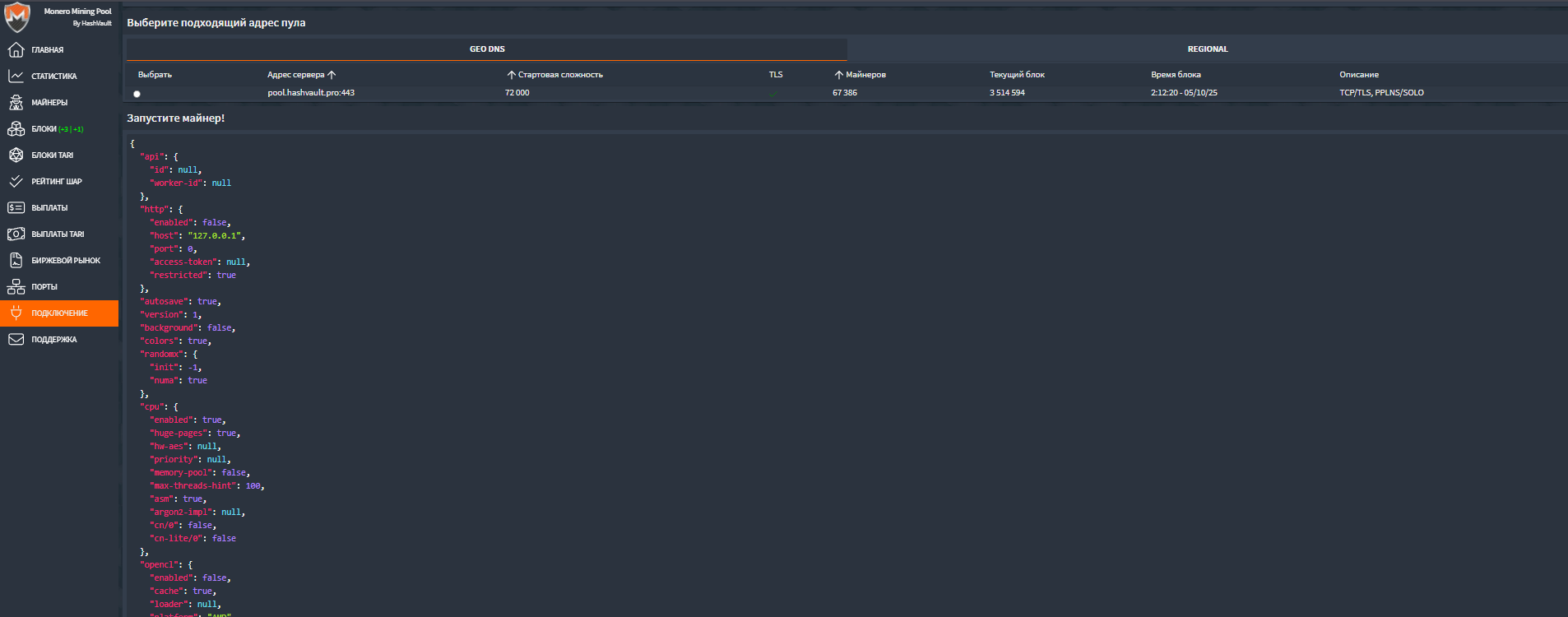


Рисунок 9 – Панель управления для созданного майнера

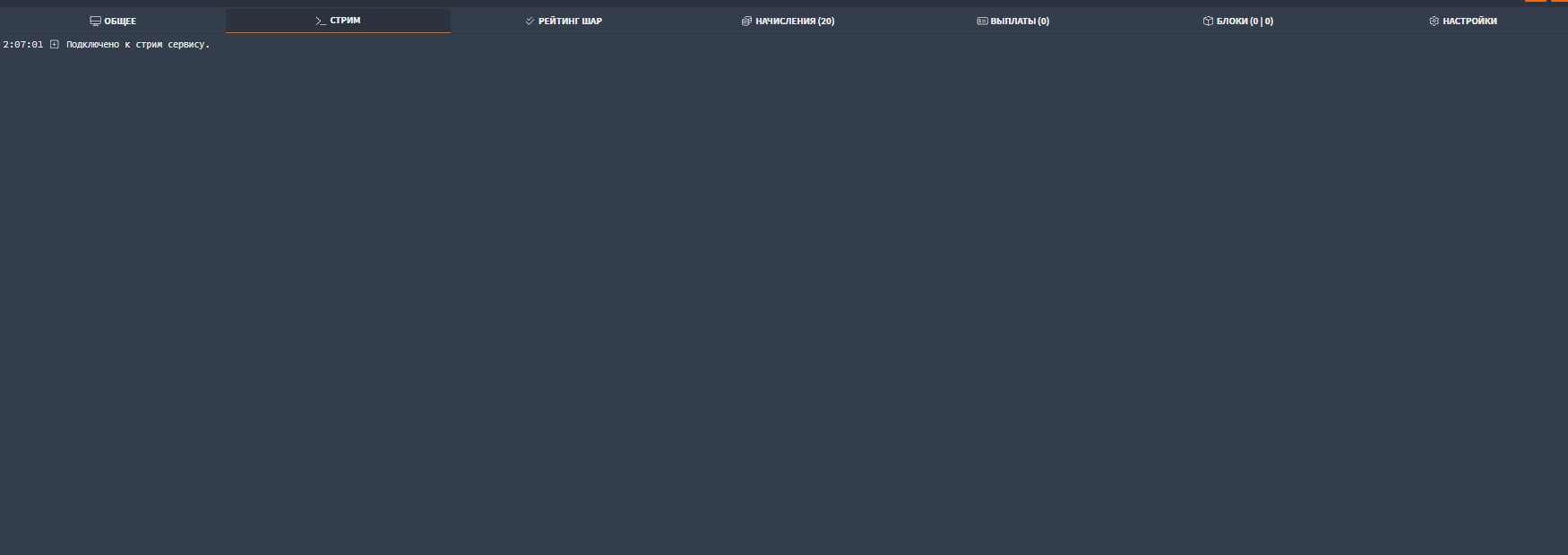


Рисунок 10 – Панель админа для просмотра заражённых узлов

Вредоносная активность майнера приводит к значительной нагрузке на вычислительные ресурсы целевой системы. На рисунке 11 наглядно демонстрируется аномально высокая загрузка центрального процессора, что подтверждает факт несанкционированного использования ресурсов.

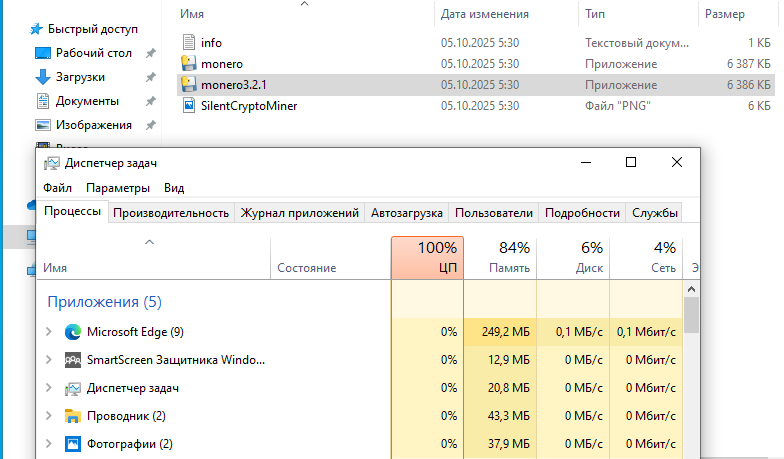


Рисунок 11 – Понижение производительности центрального процессора

Проведенное моделирование атаки наглядно демонстрирует наличие критических уязвимостей в незащищенной сетевой инфраструктуре. Успешная реализация сценария MITM позволяет не только перехватить конфиденциальные данные, но и развернуть вредоносную инфраструктуру для скрытого майнинга, что наносит прямой финансовый и операционный ущерб предприятию. Полученные результаты подтверждают необходимость внедрения комплексных мер защиты, включая систему SNS, а также систем мониторинга для блокирования подобных угроз на ранних стадиях.

## **2.3 Функциональность и роль выбранных систем в архитектуре безопасности**

Внедряемые системы защиты SNS и RuSIEM автоматизировано выполняют ключевые функции в архитектуре безопасности информационной инфраструктуры ГУП «Московский метрополитен». Интеграция указанных систем обеспечивает реализацию принципов эшелонированной защиты.

Функциональность системы контроля доступа SNS:

* реализация строгой аутентификации и авторизации на всех узлах сети;
* управление политиками безопасности из единой консоли администрирования;
* контроль целостности программной среды рабочих станций и серверов.

Защита от несанкционированного доступа:

* двухфакторная аутентификация для привилегированных пользователей;
* блокирование несанкционированных попыток доступа к критическим ресурсам;
* мониторинг и аудит действий пользователей в режиме реального времени.

Соответствие требованиям регуляторов:

* обеспечение выполнения требований Федерального закона № 152–ФЗ «О персональных данных»;
* выполнение приказов ФСТЭК России и отраслевых стандартов безопасности.

Централизованный сбор и анализ событий безопасности:

* агрегация от разнородных источников (серверы, рабочие станции, сетевое оборудование);
* корреляция событий для выявления сложных многомодальных атак;
* хранение событий безопасности в течение установленного периода.

Обнаружение и реагирование на инциденты:

* автоматическое оповещение о подозрительной активности;
* возможность интеграции с системами безопасности для автоматического реагирования;
* проведение расследований инцидентов информационной безопасности.

Мониторинг и отчетность:

* предоставление средств для непрерывного мониторинга безопасности;
* формирование отчетов для руководства и регуляторов;
* визуализация данных о состоянии защищенности инфраструктуры.

Роль систем в архитектуре безопасности:

SNS формирует первый эшелон защиты, обеспечивая:

* предотвращение несанкционированного доступа к информационным ресурсам;
* выполнение требований политик информационной безопасности.

RuSIEM обеспечивает второй эшелон защиты, предоставляя:

* инструменты для расследования и устранения последствий инцидентов;
* средства для доказательства выполнения требований регуляторов.

Внедрение такой системы позволяет гарантировать бесперебойность работы систем управления транспортными потоками.

# **ТЕХНИЧЕСКИЙ РАЗДЕЛ**

## **3.1 Внедрение SNS для настройки модуля контроля сети и обнаружения вторжений с целью противодействия сетевым атакам**

После настройки контроллера домена и подключения всех рабочих станций к домену metro.local выполняется выбор сервера безопасности, как показано на рисунке 12.



Рисунок 12 – Выбор компонентов

После анализа систем и обновлений C/C++ Runtime выполняется создание нового домена в новом лесу доменов безопасности для обеспечения автоматического определения домена системой Secret Net Studio как представлено на рисунке 13.

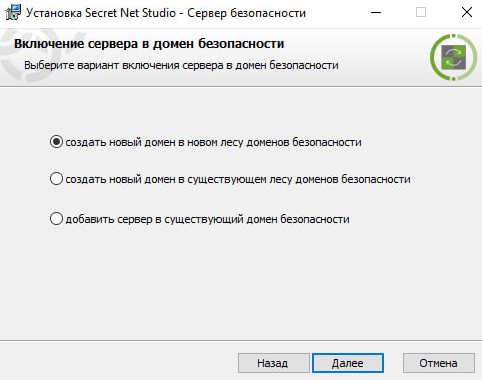
**

Рисунок 13 – Включение сервера в домен безопастности

В настройках домена безопасности для отображения всех рабочих станций, включая сервер, контроллер доменов и рядового пользователя, выполняется переименование контейнеров объекта metro.local/filial в metro.local и изменение имени домена безопасности с METRO.LOCAL.FILIAL на METRO.LOCAL процесс представлен на рисунке 14.

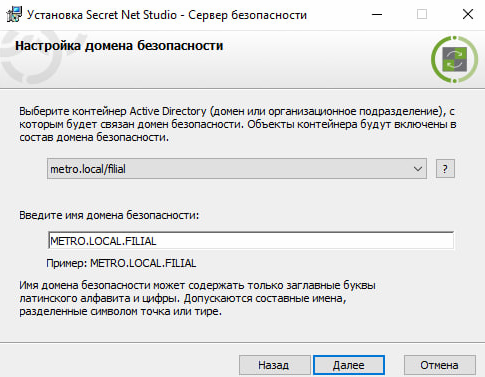


Рисунок 14 – Настройка домена безопастности

В настройки системs управления базами данных (далее – СУБД) с активным доменным пользователем metro.local введены идентификаторы имени баз данных (далее – БД) так же индексатор экземпляра и учётная запись администратора БД как показано на рисунке 15 что является ключевым при работе с SNS.

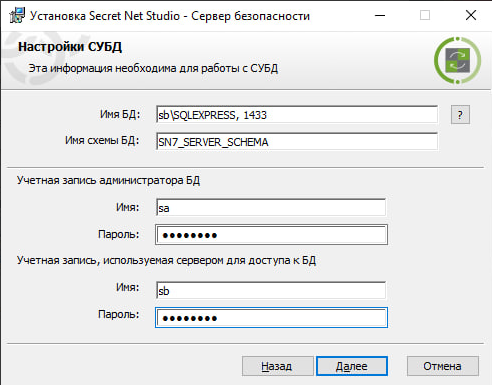


Рисунок 15 – Настройка СУБД

Во избежание ошибок необходимо нажать на зелёный кружок отвечающий за автоматическое нахождения сервера безопасности который имеет вид SB.metro.local (METRO.LOCAL) что представлено на рисунке 16.

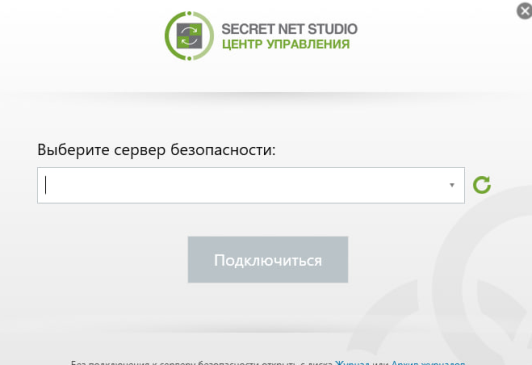


Рисунок 16 – процесс входа на сервер безопастности

Выбор лицензии для доступа к списку защиты от программно-аппаратных средств и программно-технических атак представлена на рисунке 17.

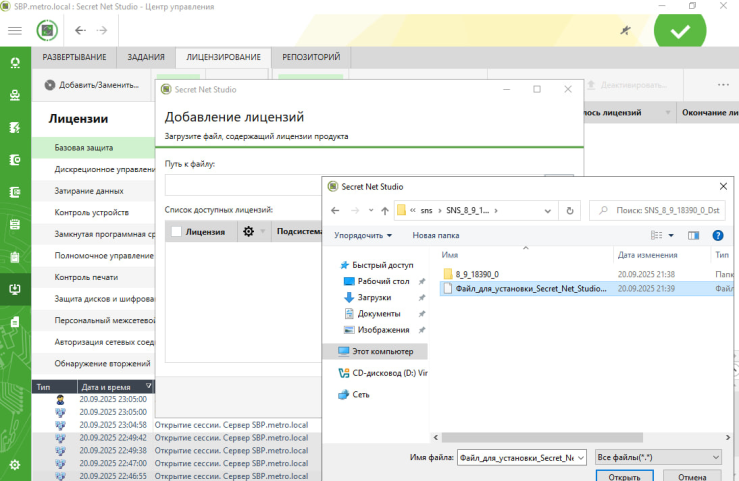


Рисунок 17 – активация ключа лицензии

Повышение уровня защиты на всех рабочих станциях с помощью централизованного способа установки для необходимых компонентов и настройки средств защиты представлен на рисунке 18.

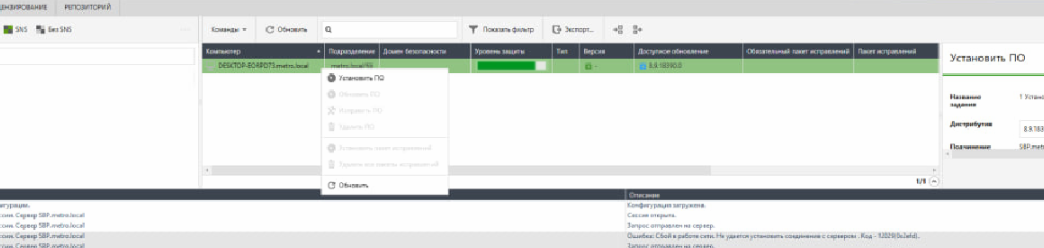


Рисунок 18 – установка ПО SNS удалённо на рабочие станции

После развертывания контроллера домена и присоединения всех рабочих станций к домену metro.local выполняется последовательность по внедрению системы безопасности SNS.

## **3.2 Реализация политик контроля доступа и целостности для блокирования вредоносной активности на рабочих станциях**

В настройках систем защиты используется механизм предотвращения вторжений что позволит выполнять функции такие как:

* применение детектора сетевых атак для блокировки атак и обнаружения попыток сканирования портов;
* применение сигнатурного анализатора, проверяющего входящий и исходящий трафик.

На рисунке 19 активирована опция блокировки атакующего хоста – ключевой компонент эшелонированной защиты.

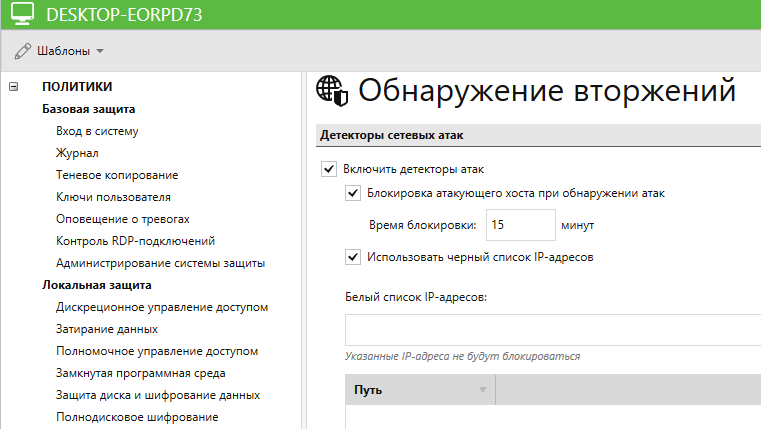


Рисунок 19 – Обнаружение вторжений сетевых атак

Для повышения эффективности обнаружения сетевых угроз, связанных с передачей данных через незашифрованные соединения, в системе активированы дополнительные механизмы мониторинга. В частности, настройка сигнатурных анализаторов представлена на рисунке 20, обеспечивающие детектирование подозрительной активности в HTTP–трафике, и включены дополнительные детекторы как показано на рисунке 21, расширяющие возможности идентификации потенциальных атак на прикладном уровне.

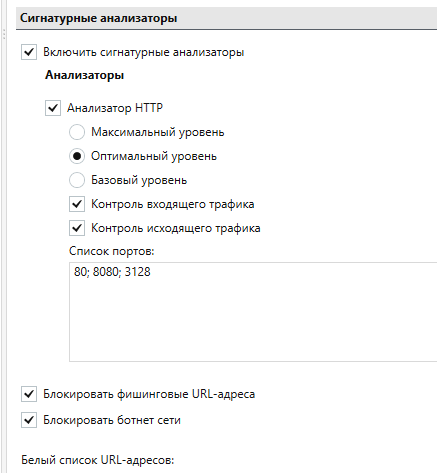


Рисунок 20 – Настройка сигнатур и анализаторов

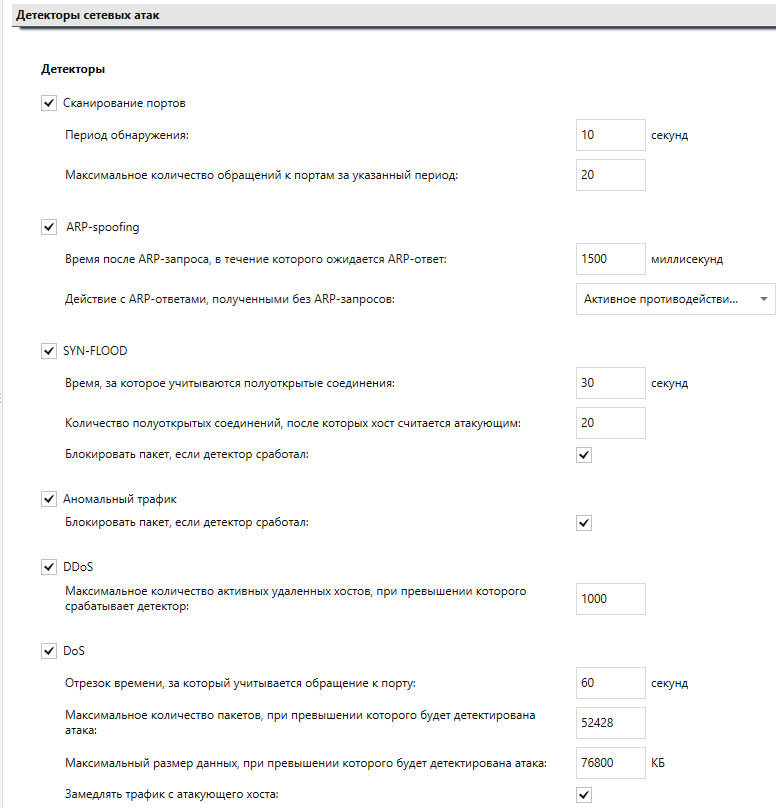


Рисунок 21 – Настройка детекторов сетевых атак

При выявлении подозрительной сетевой активности система оперативно генерирует оповещения с указанием уровня критичности. На рисунке 22 представлен пример уведомления о тревоге, содержащий детальную информацию о характере угрозы и затронутом сетевом узле.

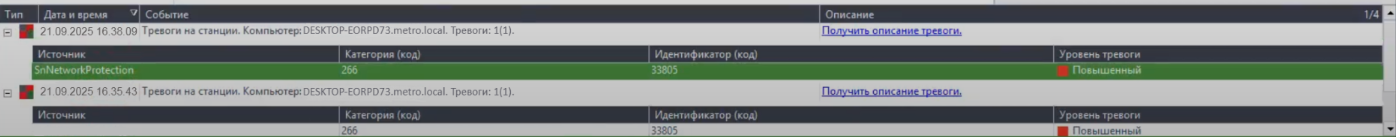


Рисунок 22 – Информация о тревоги на станции

В случае подтверждения кибератаки автоматически инициируется процедура блокировки компрометированного узла. На рисунке 23 показано уведомление о блокировке сетевого интерфейса, предотвращающее дальнейшее распространение вредоносной активности в корпоративной сети.

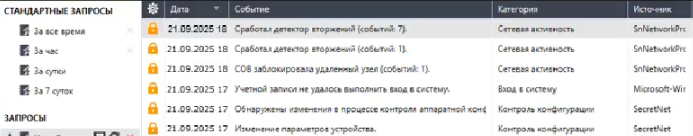


Рисунок 23 – Список отработки противодействия сканирования от подозрительного хоста

Как показано на рисунке 24 атака успешно отражена благодаря модулю контроля трафика.

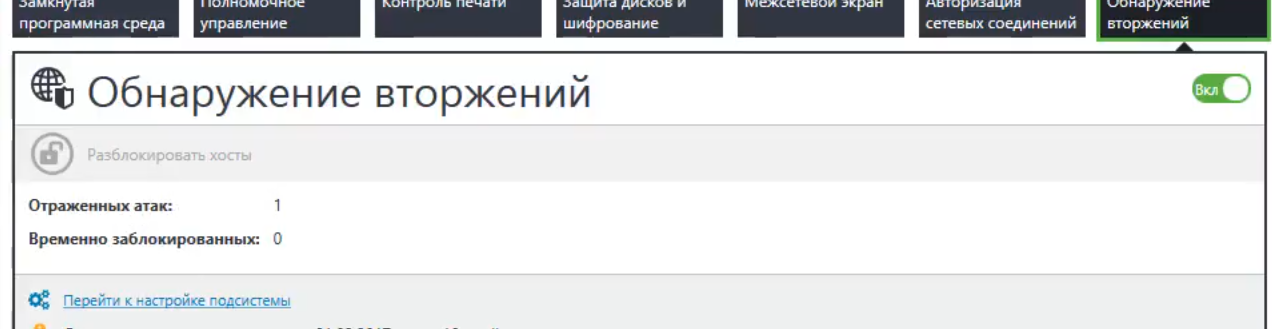


Рисунок 24 – Блокировка узла

Система мониторинга также фиксирует события, связанные с нарушением политик доступа. На рисунке 25 отображен инцидент блокировки учетной записи при попытке несанкционированного доступа к сетевым ресурсам.

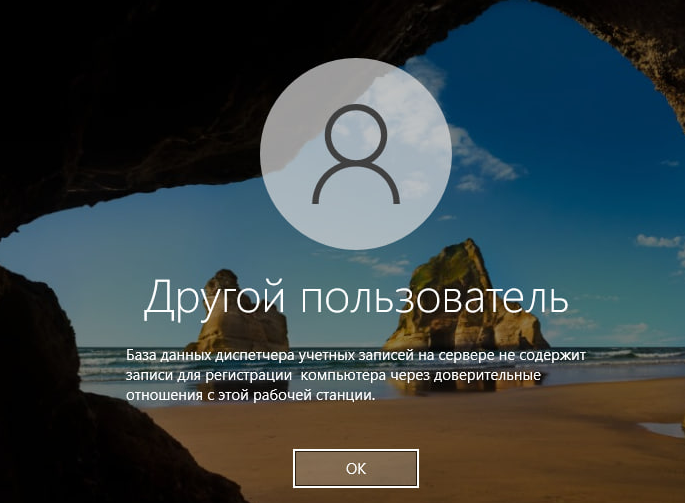


Рисунок 25 – Блокировки учетной записи

В ходе непрерывного мониторинга система безопасности успешно выявила на одной из рабочих станций вредоносное программное обеспечение, предназначенное для скрытого майнинга криптовалюты. Угроза характеризуется созданием аномально высокой нагрузки на центральный процессор, что приводит к значительному снижению производительности рабочей станции и может нарушить штатную работу критически важных приложений. Подтверждение обнаружения подобной активности и ликвидации представлено на рисунке 26.

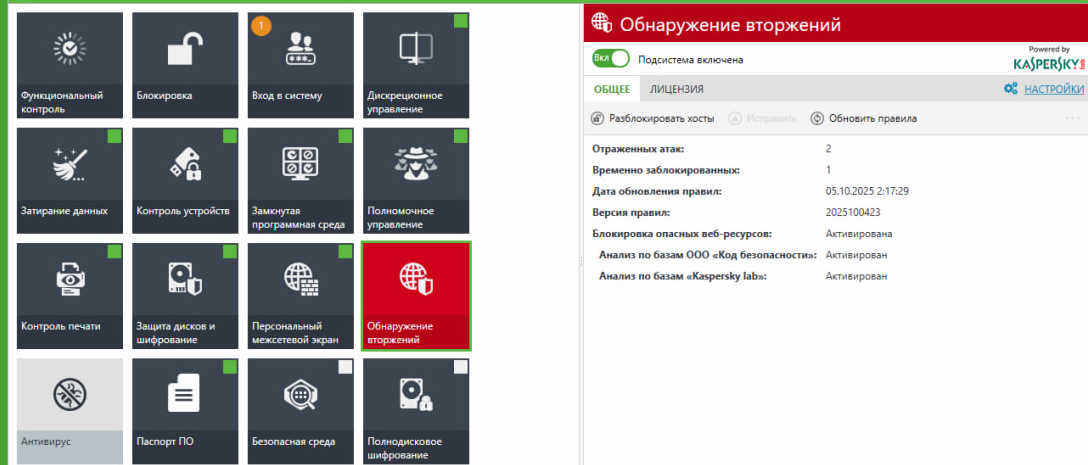


Рисунок 26 – Обнаружение майнерского ПО

При выявлении угрозы система защиты инициировала процедуру ее автоматической ликвидации. Вредоносный процесс принудительно завершен, а его исполняемые файлы удалены с диска. Это позволило немедленно разгрузить вычислительные ресурсы и восстановить нормальное функционирование рабочей станции, предотвратив дальнейший ущерб и потенциальные риски для информационной инфраструктуры предприятия.

## **3.3 Внедрение системы мониторинга RuSIEM для выявления и расследования инцидентов в автоматическом режиме**

Для обеспечения всестороннего мониторинга и оперативного реагирования на инциденты информационной безопасности в корпоративную сеть внедрена система управления событиями и информационной безопасностью RuSIEM. Развертывание системы выполнялось на специализированной операционной системе Astra Linux Special Edition, предварительно интегрированной в домен metro.local.

Для реализации установки SIEM–системы внедрим в архитектуру Secret Net Studio в ОС Astra Special Edition и реализуем подключение к домену metro.local. Далее внесены изменения в sources.list, как показано на рисунке 16. Необходимо для автономной установки отключить или закомментировать все репозитории и добавить новые репозитории, как показано на рисунке 27.

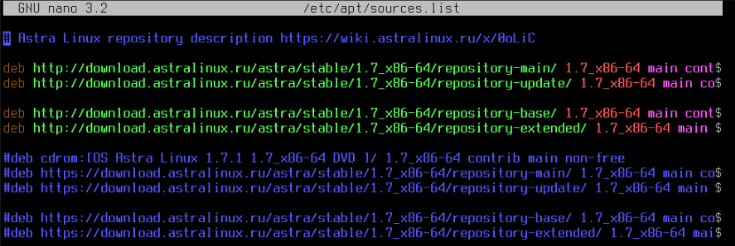


Рисунок 27 – Список активных репозиториев /etc/apt/sources.list

После предоставления вендору компании RuSIEM уникального идентификатора сервера DF9AF8AC–D204–094A–8E02–5C33C0F13228 получен лицензионный ключ, активирующий функционал как ядра RuSIEM, так и аналитического модуля RuSIEM Analytics. Установка выполнена автоматизировано с помощью официального скрипта, где выбран вариант комплектации RuSIEM + RuSIEM Analytics как представлено на рисунке 28.

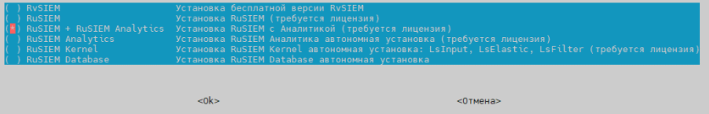


Рисунок 28 – Установка RuSIEM

По завершении установки сервер мониторинга стал доступен через веб–интерфейс по IP–адресу 10.0.254.19, назначенному сетевому интерфейсу. Далее активирован лицензионный ключ в соответствующем разделе панели управления что представлено на рисунке 29, что разблокировало полную функциональность платформы.

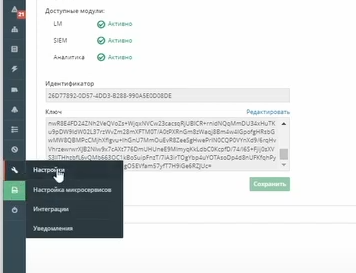


Рисунок 29 – Активация лицензионного ключа

Рабочая станция с SIEM–системой имеет IP–адрес 10.0.254.19. Доступ к веб–интерфейсу осуществляется по IP–адресу, указанному в настройках сетевого интерфейса сервера, что представлено на рисунке 30.



Рисунок 30 – Настройка сетевого интерфейса сервера

Для осуществления администрирования и просмотра событий безопасности в систему добавлен пользователь с правами администратора admin, как показано на рисунке 31*.*

Рисунок 31 – Добавление пользователя admin

Работоспособность системы подтверждена на практике: RuSIEM успешно зафиксировал и отобразил в разделе симптоматика событие, связанное с автоматической блокировкой учётной записи из–за нарушения доверительных отношений с рабочей станцией, результат демонстрируется на рисунке 32. Инцидент скоррелирован и зарегистрирован, что демонстрирует готовность системы к выявлению и расследованию нарушений безопасности в автоматическом режиме.

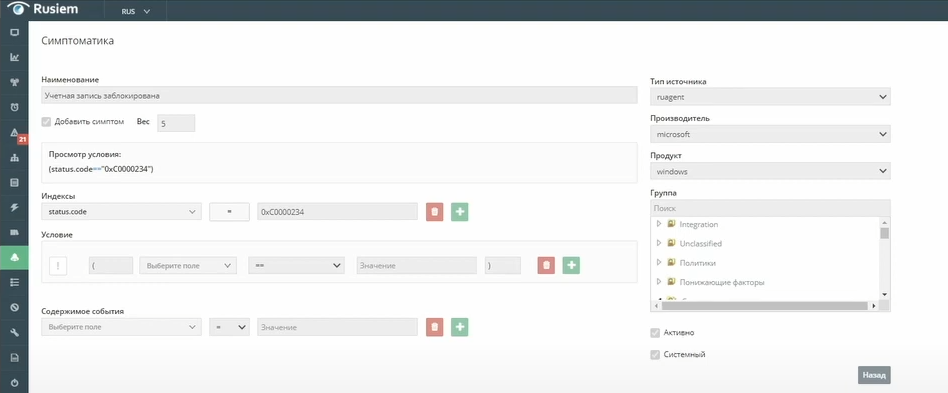


Рисунок 32 – Лог события в разделе симптоматики

Таким образом, успешно развернута и настроена система мониторинга RuSIEM, интегрированная в существующую инфраструктуру безопасности. Система готова к агрегации событий со всех узлов сети, их корреляции и генерации предупреждений, формируя основу для централизованного управления информационной безопасностью предприятия.

## **ЗАКЛЮЧЕНИЕ**

В ходе выполнения курсового проекта задачи успешно выполнены, а поставленные цели достигнуты – разработана, установлена и настроена комплексная система обеспечения информационной безопасности для корпоративной сети ГУП «Московский метрополитен». Проект реализован через решение ряда критически важных задач.

Проведен всесторонний анализ защиты сети, изучена его организационная структура и определен статус как критической информационной инфраструктуры (далее – КИИ). Проанализирована обширная нормативно–правовая база, регламентирующая деятельность предприятия и требования к защите информации, и Федеральные законы № 152–ФЗ, № 149–ФЗ и приказы ФСТЭК России. На основе этого анализа разработана модель нарушителя и классифицированы актуальные угрозы, что позволило сфокусировать усилия на наиболее значимых рисках.

Благодаря исследовательской части спроектирован архитектурный план системы защиты, объединяющий эшелонированную оборону на базе двух ключевых продуктов: системы контроля доступа SNS и системы мониторинга и управления событиями безопасности RuSIEM. Разработан детальный план подготовки к внедрению, включающий настройку доменной инфраструктуры, развертывание СУБД и определение последовательности действий для интеграции всех компонентов.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149–ФЗ (последняя редакция от 31.07.2023).
2. ФЗ «О персональных данных» от 27.07.2006 № 152–ФЗ (последняя редакция от 06.02.2023).
3. ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187–ФЗ (последняя редакция от 04.02.2023).
4. ФЗ «Об электронной подписи» от 06.04.2011 № 63–ФЗ (последняя редакция от 02.07.2021).
5. ФЗ «О транспортной безопасности» от 09.02.2007 № 16–ФЗ (последняя редакция от 26.07.2022).
6. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых точек критической информационной инфраструктуры Российской Федерации»;
7. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
8. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
9. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности: Монография. — М.: Издательство «Юрайт», 2023. — 315 с.
10. Лапонина О.Р. Криптографические основы безопасности: Учебное пособие для вузов. 2–е изд., перераб. и доп. — СПб.: БХВ–Петербург, 2024. — 448 с.
11. Платонов В.В., Ушаков Д.В. Защита критической информационной инфраструктуры: современные вызовы и угрозы. — М.: Горячая линия – Телеком, 2022. — 267 с.
12. Комплексная методика проведения расследования инцидента информационной безопасности / С. И. Смирнов, А. Н. Киселев, В. Д. Азерский [и др.] // Защита информации. Инсайд. – 2023. – № 2. – С. 14–26.
13. Методология тестирования на проникновение – PositiveTechnologies [Электронный ресурс] // URL: [https://www.ptsecurity.com/ru–ru/services/pentest/](https://www.ptsecurity.com/ru-ru/services/pentest/).
14. Glabit[Электронный ресурс] // URL: https://glabit.ru/blog/arhitektura–informacionnoj–bezopasnosti
15. SecretNetStudio [Электронный ресурс] // URL: [https://www.securitycode.ru/products/secret–net–studio](https://www.securitycode.ru/products/secret-net-studio)
16. RuSIEM [Электронный ресурс] // URL <https://rusiem.com/ru/demo>

**Организационная структура**

Приложение 1

Генеральный директор

Главный инженер первый заместитель начальника метрополитена

Первый заместитель начальника метрополитена

Заместитель начальника метрополитена по пассажирской работе

Дирекции инфраструктуры

Начальник службы подвижного состава

Заместитель начальника метрополитена по (ИТ) и связи

Начальник Дирекции строящегося метрополитена

Заместитель начальника метрополитена по стратегическому развитию

Заместитель начальника метрополитена по коммуникациям

Дирекция инфраструктуры

Служба пути

Служба сигнализации централизации

Служба электроснабжения

Эскалаторная служба

Электромеханическая служба

Служба тоннельных сооружений

Служба подвижного состава

Служба движения

Вагоноремонтный комплекс

Монорельсовая транспортная система

Служба связи

Служба (ИТ)

Дирекция строящегося метрополитена

Отдел пожарной охраны

Проектное-конструкторское бюро

Служба качества

Отдел охраны труда

Служба инвестиционного развития

Служба внешних связей

Главный ревизор по безопасности движения поездов

Заместитель начальника метрополитенаслужбы безопасности

Заместитель начальника метрополитена по экономике и финансам

Заместитель начальника метрополитена по управлению персоналом

Заместитель начальника метрополитена начальник контрактной службы

Служба пассажирских сервисов

Служба сборов доходов

Отдел главного метролога

Служба качества

Контрактная служба

Главная бухгалтерия

Финансово экономическая служба

Центр контроля финансово хозяйственной деятельности и закупочных цен

Отдел статистического учета и отчетности

Отдел корпоративных финансов

Служба управления персоналом

Служба профориентации обучения и развития персонала

Отдел рабочего снаряжения

Медицинская служба

Служба безопасности

Аппарат главного ревизора по безопасности движения поездов

Ситуационный центр

Служба технической политики

Таблица 1 – Модель нарушителя и угроз информационных ресурсов

Приложение 2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Вид нарушителя** | **Тип по ФСТЭК** | **Группа** | **Тип по ФСБ** | **Возможные угрозы** |
| **Практиканты** | Внешний | H1 | Группа 5 | Непреднамеренные, неосторожные или неквалифицированные действия. Физическое уничтожение данных или оборудования. |
| **Дирекция** | Внутренний | H3 | Группа 5 | Уничтожение/модификация данных, раскрытие конфиденциальной информации УЦ разработки. Непреднамеренные, неосторожные или неквалифицированные действия |
| **Системный Администратор** | Внутренний | H3 | Группа 5 | Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды |
| Оператор электродепо метрополитена | Внутренний | H3 | Группа 5 | Уничтожение/модификация данных |
| **Веб–програмисты, Инженер–програмист** | Внутренний | H4 | Группа 7,8 | Внедрение дополнительных возможностей в программное обеспечение или программно–технические средства |
| Администратор безопасности | Внутренний | H3 | Группа 6 | Раскрытие конфиденциальной информации УЦ. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды а так же с целью дальнейшего её распространения |
| **Временный сотрудник** | Внутренний | H3 | Группа 2 | Неосторожные или неквалифицированные действия. Продажа конфиденциальной информации с целью получения материальной выгоды |
| **Клиенты** | Внешний | H1 |  | Физическое уничтожение данных или оборудования |
| **Практиканты** | Внешний | H1 |  | Несанкционированное получение и раскрытие конфиденциальной информации |