Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Школа Информационных технологий и робототехники
Направление подготовки 09.04.01 Информатика и вычислительная техника
Отделение Информационных технологий

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Разработка интеллектуальной системы предсказания, обнаружения и предотвращения сбоев работы компьютерной сети

УДК 004.896:004.72.052

Студент

Группа	ФИО	Подпись	Дата
8ВМ6В	Волшин Максим Евгеньевич		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент отделения ИТ	Фадеев Александр Сергеевич	к.т.н., доцент		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель	Шаповалова Наталья Владимировна			

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ассистент	Авдеева Ирина Ивановна			

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
ИТ	Демин Антон Юрьевич	к.т.н.		

Томск – 2018 г.

Планируемые результаты обучения

Код результатов	Результат обучения (выпускник должен быть готов)
Р1	Воспринимать и самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте.
Р2	Владеть и применять методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях.
Р3	Демонстрировать культуру мышления, способность выстраивать логику рассуждений и высказываний, основанных на интерпретации данных, интегрированных из разных областей науки и техники, выносить суждения на основании неполных данных, анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями.
Р4	Анализировать и оценивать уровни своих компетенций в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и профессиональной мобильности. Владеть, по крайней мере, одним из иностранных языков на уровне социального и профессионального общения, применять специальную лексику и профессиональную терминологию языка.
Р5	Выполнять инновационные инженерные проекты по разработке аппаратных и программных средств автоматизированных систем различного назначения с использованием современных методов проектирования, систем автоматизированного проектирования, передового опыта разработки конкурентоспособных изделий.
Р6	Планировать и проводить теоретические и экспериментальные исследования в области проектирования аппаратных и программных средств автоматизированных систем с использованием новейших достижений науки и техники, передового отечественного и зарубежного опыта. Критически оценивать полученные данные и делать выводы.
Р7	Осуществлять авторское сопровождение процессов проектирования, внедрения и эксплуатации аппаратных и программных средств автоматизированных систем различного назначения.
Р8	Использовать на практике умения и навыки в организации исследовательских, проектных работ и профессиональной эксплуатации современного оборудования и приборов, в управлении коллективом.
Р9	Осуществлять коммуникации в профессиональной среде и в обществе в целом, активно владеть иностранным языком, разрабатывать документацию, презентовать и защищать результаты инновационной инженерной деятельности, в том числе на иностранном языке.
Р10	Совершенствовать и развивать свой интеллектуальный и общекультурный уровень. Проявлять инициативу, в том числе в ситуациях риска, брать на себя всю полноту ответственности.
Р11	Демонстрировать способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности, способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, способность к педагогической деятельности.

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Школа _Информационных технологий и робототехники_____
Направление подготовки _09.04.01 Информатика и вычислительная техника_____
Отделение _Информационных технологий_____

УТВЕРЖДАЮ:
Зав. отделением
_____ _____ Демин А.Ю.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

Магистерской диссертации

Студенту:

Группа	ФИО
8ВМ6В	Волшин Максим Евгеньевич

Тема работы:

Проектирование и разработка алгоритмического и программного обеспечения симулятора состояния подземного нефтяного резервуара в режиме реального времени	
Утверждена приказом директора (дата, номер)	2739/с от 19.04.2018

Срок сдачи студентом выполненной работы:	06.06.2018

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе	Проектирование и разработка алгоритмического и программного обеспечения управления сетью с целью предотвращения её сбоев на основе анализа сетевых пакетов.
Перечень подлежащих исследованию, проектированию и разработке вопросов	1) Изучение используемых в сети протоколов; 2) Изучение причин сбоев; 3) Изучение уязвимых мест сети; 4) Обзор существующих инструментов диагностики сети; 5) Сбор требований к проектируемой системе; 6) Проектирование архитектуры системы; 7) Определение стоимости и сроков разработки проекта; 8) Рассмотрение условий труда исполнителей проекта.
Перечень графического материала	

Консультанты по разделам выпускной квалификационной работы

Раздел	Консультант
Финансовый менеджмент,	Шаповалова Наталья Владимировна

ресурсоэффективность и ресурсосбережение	
Социальная ответственность	Авдеева Ирина Ивановна
Раздел на иностранном языке	Рыбушкина Светлана Владимировна
Названия разделов, которые должны быть написаны на русском и иностранном языках:	
Обзор причин нарушения работы сети	

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	01.03.2018

Задание выдал руководитель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент отделения ИТ	Фадеев Александр Сергеевич	к.т.н., доцент		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ6В	Волшин Максим Евгеньевич		

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Школа _Информационных технологий и робототехники_____
Направление подготовки _09.04.01 Информатика и вычислительная техника_____
Уровень образования _магистратура_____
Отделение _Информационных технологий_____
Период выполнения весенний семестр 2017/2018 учебного года__

Форма представления работы:

Магистерская диссертация

КАЛЕНДАРНЫЙ РЕЙТИНГ-ПЛАН
выполнения выпускной квалификационной работы

Срок сдачи студентом выполненной работы:	06.06.2018

Дата контроля	Название раздела (модуля) / вид работы (исследования)	Максимальный балл раздела (модуля)
10.02.2018	Раздел 1. Обзор причин нарушения работы сети	20
10.03.2018	Раздел 2. Разработка программного обеспечения	15
25.03.2018	Раздел 3. Анализ данных	20
20.04.2018	Раздел 4. Результаты	20
05.05.2018	Раздел 5. Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	15
06.05.2018	Раздел 6. Социальная ответственность	10

Составил преподаватель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент отделения ИТ	Фадеев Александр Сергеевич	к.т.н., доцент		

СОГЛАСОВАНО:

Руководитель ООП	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ ИШИТР	Ботыгин Игорь Александрович	к.т.н.		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА «ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	**ФИО**
8ВМ6В	Волшину Максиму Евгеньевичу

Школа	Информационных технологий и робототехники	**Отделение**	Информационных технологий
Уровень образования	Магистратура	**Направление/специальность**	09.04.01 Информатика и вычислительная техника

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих	Планирование сметы затрат проекта и используемого материально-технического обеспечения, а также использования человеческого ресурса. Ставка социального налога 30% согласно системе налогообложения.
2. Нормы и нормативы расходования ресурсов	
3. Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования	
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Оценка коммерческого и инновационного потенциала НТИ	Оценка научно-технического эффекта разработки, анализ перспективности проекта.
2. Организация и планирование работ	Планирование этапов разработки программы, определение трудоемкости, и построение диаграммы Ганта.
3. Формирование бюджета научных исследований	Расчёт сметы затрат на выполнение проекта.
4. Определение ресурсной, финансовой, экономической эффективности	Оценка эффективности исследования.
Перечень графического материала	
1. Диаграмма Ганта 2. Круговая диаграмма затрат	

Дата выдачи задания для раздела по линейному графику	01.03.2018

Задание выдал консультант:

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Старший преподаватель	Шаповалова Наталья Владимировна			01.03.2018

Задание принял к исполнению студент:

Группа	**ФИО**	**Подпись**	**Дата**
8ВМ6В	Волшин Максим Евгеньевич		01.03.2018

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
8ВМ6В	Волшину Максиму Евгеньевичу

Школа	Информационных технологий и робототехники	**Отделение**	Информационных технологий
Уровень образования	Магистратура	**Направление/специальность**	09.04.01 Информатика и вычислительная техника

Исходные данные к разделу «Социальная ответственность»:	
1. Характеристика объекта исследования (вещество, материал, прибор, алгоритм, методика, рабочая зона) и области его применения	Программно-аппаратный комплекс анализа сетевого широковещательного трафика, включающий в себя компьютер с доступом к локальной сети и необходимое программное обеспечение. Работа происходит в условиях учебной аудитории, оснащенной персональными компьютерами с периферийными устройствами. Область применения: администрирование компьютерных сетей и предоставление доступа в Интернет
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. **Производственная безопасность** 1.1. Анализ выявленных вредных факторов при разработке и эксплуатации проектируемого решения в следующей последовательности: - физико-химическая природа вредности, её связь с разрабатываемой темой; - действие фактора на организм человека; - приведение допустимых норм с необходимой размерностью (со ссылкой на соответствующий нормативно-технический документ); - предлагаемые средства защиты; - (сначала коллективной защиты, затем – индивидуальные защитные средства). 1.2. Анализ выявленных опасных факторов при разработке и эксплуатации проектируемого решения в следующей последовательности:	Опасные и вредные факторы: - неблагоприятный микроклимат - недостаточная освещенность рабочей зоны - повышенный уровень шума - умственное перенапряжение - монотонный режим работы Мероприятия по защите от вредных факторов включают в себя измерение текущих показателей вредных факторов и обеспечение соблюдения нормативных показателей. Опасные факторы: - поражение электрическим током - короткое замыкание, статическое электричество. Для защиты от опасных факторов

- механические опасности (источники, средства защиты; - термические опасности (источники, средства защиты); - электробезопасность (в т.ч. статическое электричество, молниезащита – источники, средства защиты)	необходимо проводить организационные и технические мероприятия по предотвращению возникновения опасных ситуаций.
2. Экологическая безопасность: - защита селитебной зоны - анализ воздействия объекта на атмосферу (выбросы); - анализ воздействия объекта на гидросферу (сбросы); - анализ воздействия объекта на литосферу (отходы); - разработать решения по обеспечению экологической безопасности со ссылками на НТД по охране окружающей среды.	Объекты, несущие угрозу окружающей среде: - люминесцентные лампы - компьютерная техника Необходимо обеспечить утилизацию объектов в специальных организациях
3. Безопасность в чрезвычайных ситуациях: - перечень возможных ЧС при разработке и эксплуатации проектируемого решения; - выбор наиболее типичной ЧС; - разработка превентивных мер по предупреждению ЧС; - разработка действий в результате возникшей ЧС и мер по ликвидации её последствий.	ЧС, которые могут возникнуть в процессе разработки и эксплуатации: - пожар в здании. Требуется следовать инструкциям, чтобы не допустить возникновения ЧС. Однако, если ЧС произошло, требуется следовать протоколу эвакуации из здания, а также вызвать службы для ликвидаций последствий ЧС.
4. Правовые и организационные вопросы обеспечения безопасности: - специальные (характерные при эксплуатации объекта исследования, проектируемой рабочей зоны) правовые нормы трудового законодательства; - организационные мероприятия при компоновке рабочей зоны.	Описание правил компоновки рабочего места с учетом специфики работы исполнителя проекта и пользователя программно-аппаратного комплекса. Описание правовых норм, связанных с работой за ПАК и организации рабочей зоны согласно следующим документам: - Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 05.02.2018) - СанПиН 2.2.2/2.4.1340-03

Дата выдачи задания для раздела по линейному графику	01.03.2018

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ассистент	Авдеева Ирина Ивановна			01.03.2018

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ6В	Волшин Максим Евгеньевич		01.03.2018

РЕФЕРАТ

Выпускная квалификационная работа 113 с., 29 рис., 16 табл., 43 источника, 3 прил.

Ключевые слова: компьютерная сеть, управление сетью, сбой сети, атаки, протоколы передачи данных, управление оборудованием, SNMP.

Объектом исследования является разработка программного обеспечения для обнаружения, предотвращения и предсказания сбоев сети.

Цель работы – проектирование и разработка алгоритмического программного обеспечения, принимающего решения на основе статистики перехваченных сетевых пакетов, совместно с управлением телекоммуникационным оборудованием.

В процессе исследования проводился анализ уязвимостей современных сетевых протоколов передачи данных в компьютерной сети. Изучены протоколы: ARP, ICMP, ICMPv2, NBNS, MDNS, DNS, LLMNR.

В результате исследования были разработаны средства для обнаружения и предотвращения сетевых сбоев для самых уязвимых протоколов и самого популярного стандарта управления оборудованием.

Области применения: средние и крупные организации с компьютерными сетями, Интернет-провайдеры.

Экономическая эффективность/значимость работы: основная выгода разработанного программного обеспечения состоит в сокращении простоя сети, что в свою очередь сокращает простой зависящих от сети процессов, например коллективная разработка программного обеспечения или предоставления услуги доступа в Интернет.

В будущем планируется доработка модуля принятия решений для его работы без участия квалифицированного администратора.

Оглавление

Перечень условных обозначений

OSI	Open Systems Interconnection Basic Reference Model – Базовая эталонная модель взаимодействия открытых систем
IP	Internet Protocol – Межсетевой протокол
MAC	Media Access Control – Управление доступом к среде
ARP	Address Resolution Protocol – Протокол определения адреса
DNS	Domain Name System – Система доменных имён
ICMP	Internet Control Message Protocol – Протокол межсетевых управляющих сообщений
VPN	Virtual Private Network – Виртуальная частная сеть
GUI	Graphical User Interface – Графический интерфейс пользователя
AES	Advanced Encryption Standard – Стандарт симметричного алгоритма блочного шифрования
SQL	Structured Query Language – Язык структурированных запросов
СУБД	Система управления базами данных
БД	База данных
MD5	Message Digest 5 – 128-битный алгоритм хеширования
SNMP	Simple Network Management Protocol – Простой протокол сетевого управления
MIB	Management Information Base – База управляющей информации
DHCP	Dynamic Host Configuration Protocol – Протокол

	динамической настройки узла
UDP	User Datagram Protocol – Протокол пользовательских датаграмм
TCP	Transmission Control Protocol – Протокол управления передачей
NBNS	NetBIOS Name Service – служба имён NetBIOS
LLMNR	Link-local Multicast Name Resolution – Протокол определения имён в локальной подсети
STP	Spanning Tree Protocol – протокол остовного дерева
SSDP	Simple Service Discovery Protocol – Простой протокол обнаружения сервисов
DLNA	Digital Living Network Alliance – набор стандартов, позволяющих совместимым устройствам передавать и принимать по сети медиа-контент
DDoS	Distributed Denial of Service – распределённая атака типа «отказ в обслуживании»
UPnP	Universal Plug and Play – Универсальная автоматическая настройка сетевых устройств
MDNS	Multicast Domain Name System – Система доменных имён на основе мультикаста

Введение

В настоящее время цифровая индустрия развивается гигантскими темпами[1]. Почти каждый день появляются новые мобильные приложения новых сервисов, открываются новые web сайты и прочие ресурсы[2]. Для функционирования этих ресурсов необходимы компьютерные сети и Интернет в том числе. Таким образом, поддержание сети – среды передачи информации от этих сервисов до конечных потребителей в рабочем состоянии является актуальной задачей. А постоянное увеличение типов передаваемой информации и протоколов только усложняет эту задачу.

Целью научно-исследовательской работы является разработка инструмента (системы) для накопления и анализа статистики, а так же принятия решений по управлению на её основе для предотвращения сбоев.

Для достижения поставленной цели были поставлены следующие задачи:

1) Выявление способов нарушения работы сети;
2) Разработка механизма сбора статистики сетевой активности;
3) Анализ полученных данных;
4) Разработка алгоритма обнаружения аномалий в сети;
5) Разработка механизма локализации последствий аномалий;

1. Обзор причин нарушения работы сети

Причины можно разделить на 3 категории [3]:

1) Ограничение доступа к данным;

2) Нарушение конфиденциальности персональных данных;

3) Нарушение целостности данных.

Передача данных по сети почти всегда подразумевает эти риски, при свершении которых, какой-либо сервис может стать недоступным конечному пользователю.

Сеть – сложная система, состоящая из специализированного оборудования, линий связи, клиентских и серверных устройств. Сети разных масштабов обладают своими техническими особенностями и технологиями передачи данных. Например, локальная сеть позволяет сетевым устройствам общаться, начиная со 2 уровня модели OSI. Это позволяет без труда узнать уникальные физические адреса устройств, что в свою очередь открывает несколько векторов для атаки и перехвата данных.

Если речь идёт о глобальной сети (Internet), то общение между разными узлами начинается с 3 уровня модели OSI – уровня IP адресов. Это отсекает большую часть векторов атак, таких как «посредник в середине». Но факт транзита сетевого трафика между узлами в глобальной сети даёт возможность злоумышленникам перехватывать данные без атак, используя для этого специальное программное обеспечение и физический доступ к оборудованию.

1.1. Виды атак

Самый уязвимый участок сети является локальной сетью. А самые распространённые атаки [4]:

1) MAC-spoofing

2) ARP-spoofing

3) DNS-spoofing

4) Flooding

5) Подмена ложного маршрута через протокол ICMP

1.1.1. MAC-spoofing

Суть атаки заключается в подмене MAC адреса устройства злоумышленника на MAC адрес жертвы или маршрутизатора жертвы. Этот метод сработает в сетях, построенных на неуправляемых или ненастроенных должным образом управляемых коммутаторах. Во время такой атаки на коммутаторе на разных портах будет находиться одинаковый мак адрес. Это приведёт к постоянному «переучиванию» его таблицы коммутации. На коммутаторе MAC адрес будет «прыгать» между двумя портами, вследствие чего, пакеты, передаваемые на этот MAC адрес, будут приходить частично к злоумышленнику [5].

Для борьбы с этой проблемой производители сетевого оборудования придумали несколько решений. Первое из них заключается в «выучивании таблицы коммутации», вследствие чего получается статическая таблица коммутации. Второе более продвинутое – построение таблица коммутации по достоверным данным, например списки доступа, сервер авторизации или DHCP-snooping + option 82.

1.1.2. ARP-spoofing

Атака основана на уязвимости протокола ARP. Этот протокол позволяет узнавать принадлежность IP адреса к MAC адресу, проще говоря, связывает 2 и 3 уровень модели OSI.

Атака направлена на то, чтобы сделать устройство злоумышленника посредником между 2 атакуемыми устройствами, например маршрутизатором и клиентом. Для этого злоумышленник отсылает жертвам пакеты, которые будут нести фальсифицированные связки IP и MAC адресов, вследствие чего клиент будет слать свои пакеты злоумышленнику, думая, что он маршрутизатор. Аналогичная ситуация и с маршрутизатором в сторону клиента. После удачной подмены связок IP-MAC трафик будет ходить через

злоумышленника, что даёт возможность его просматривать [6]. Схема атаки представлена на рисунке 1.

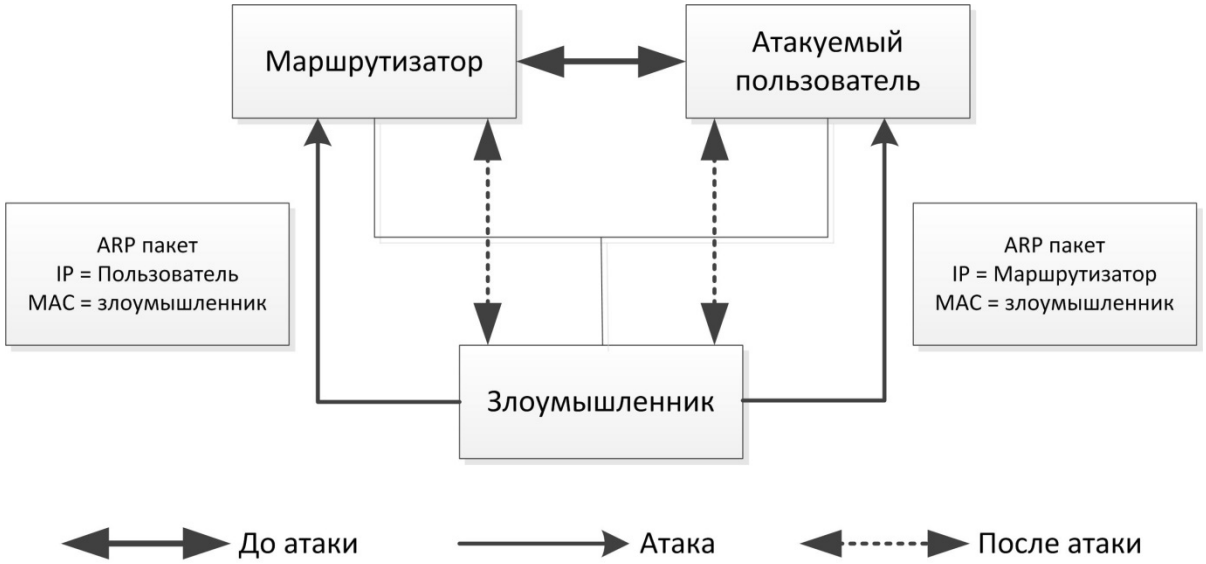


Рисунок 1. ARP-spoofing.

Для борьбы с этой проблемой можно на всех узлах в сети сделать ARP записи статичными, но это усложняет администрирование сети. Кроме того, есть пассивный и активный методы борьбы с этой проблемой.

Пассивный метод заключается в прослушивании ARP пакетов и отслеживания изменений в передаваемых им связках. Метод позволяет обнаружить атаку, но не предотвратить её. Можно снизить эффективность этой атаки, если в сторону злоумышленника направить большое количество случайно сгенерированных пакетов, дабы забить канал его физического подключения, попутно отсылая жертвам верные связки. Но это требует специализированного программного обеспечения и повышает нагрузку на оборудование.

Активный метод заключается в фильтрации ARP пакетов на самом коммутаторе. Коммутатор формирует ARP таблицу по достоверным данным, по средствам, например всё те же списков доступа и сервер авторизации. Пакеты с неверными данными коммутатор отсекает, предотвращая его дальнейшее распространение по сети.

1.1.3. DNS-spoofing

Атака производиться на DNS сервер в локальной сети, целью которой является перехват запроса клиента с целью ответа с подменой в доменной записи некоторого ресурса IP адреса на IP адрес злоумышленника. Делается это для того, чтобы жертва попала на сайт злоумышленника, который может являться его точной копией, и вела свои учётные данные, которые и получит злоумышленник [7]. Схема атаки представлена на рисунке 2.

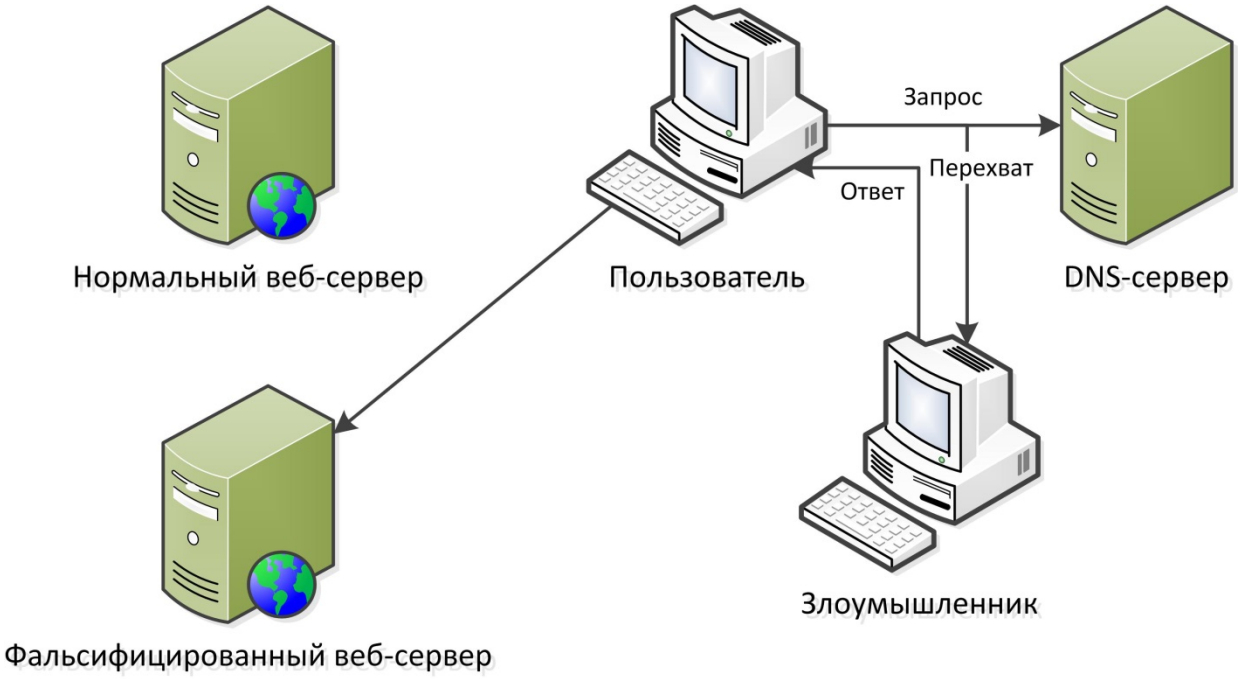


Рисунок 2. DNS-spoofing.

1.1.4. Flooding

Атака направлена на заполнение пропускной способности канала случайно сгенерированными пакетами. Учитывая, что приходящий на устройство пакет обрабатывается, то страдает не только канал, но и центральный процессор атакуемого устройства.

Защититься от этого практически невозможно, однако вычислить источник с последующей его блокировкой вполне реально. Для этого необходимо следить за трафиком на клиентских устройствах, что не всегда возможно.

1.1.5. Подмена ложного маршрута через протокол ICMP

Протокол ICMP (Internet Control Message Protocol) обладает одной функций для информирования сетевых узлов о смене текущего маршрутизатора. Данное управляющее сообщение носит название redirect. Для атаки узла, чтобы тот сменил маршрутизатор, необходимо отправить ложное redirect-сообщения от имени действующего маршрутизатора. В результате на атакуемом узле изменяется основной маршрут в таблице маршрутизации, что направит весь сетевой трафик данного узла злоумышленнику, отославшего ложное redirect-сообщение [3][8]. Схема атаки представлена на рисунке 3.

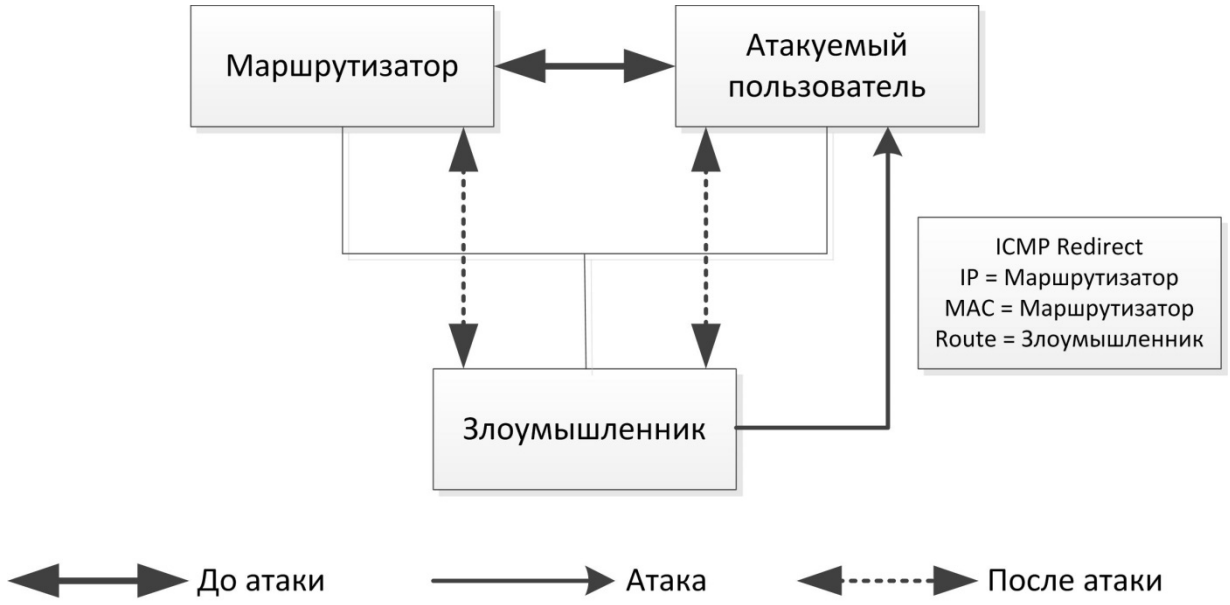


Рисунок 3. ICMP Redirect.

Для борьбы с данным типом атаки необходимо блокировать часть типов сообщений протокола ICMP на клиентских устройствах. Так как не на всех устройствах это можно реализовать, задача становится очень сложной.

1.2. Перехват и анализ пакетов

Для накопления пакетной статистики самая ценная информация в перехваченном пакете это:

- Адрес отправителя – потенциальный злоумышленник;
- Адрес получателя – потенциальная жертва;

- Протокол – основной вектор атаки.

Для работы с сетевыми данными, сначала их нужно получить. На сегодняшний момент есть несколько инструментов позволяющие это сделать. Разберём их поподробнее.

1.2.1. Pcap

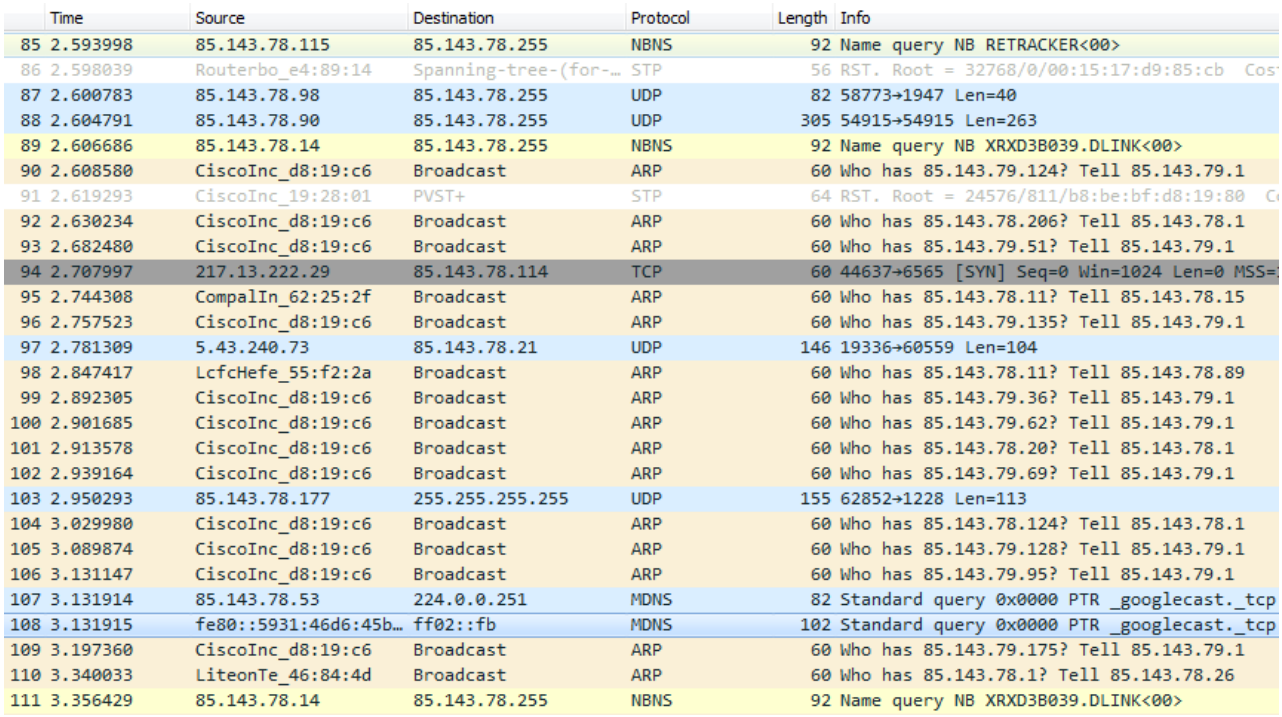
Кроссплатформенная библиотека, написанная на C, предназначена для низкоуровневого перехвата пакетов с сетевых интерфейсов. Она является основой всех современных программных решений для анализа сетевых данных. Библиотека поддерживает практически все типы сетевых интерфейсов – от физических до виртуальных (VPN туннели и пр.). На выходе работы библиотеки, мы получаем бинарные данные пакета. Для дальнейшего анализа пакета надо знать его тип, сигнатуру полей, инкапсулируемые в пакет протоколы и многое другое [9].

1.2.2. Wireshark

Wireshark – очень мощный инструмент для анализа сетевого трафика с интуитивно понятным и удобным пользовательским интерфейсом. На сегодняшний день Wireshark является самым мощным инструментом для анализа сетевого трафика [10].

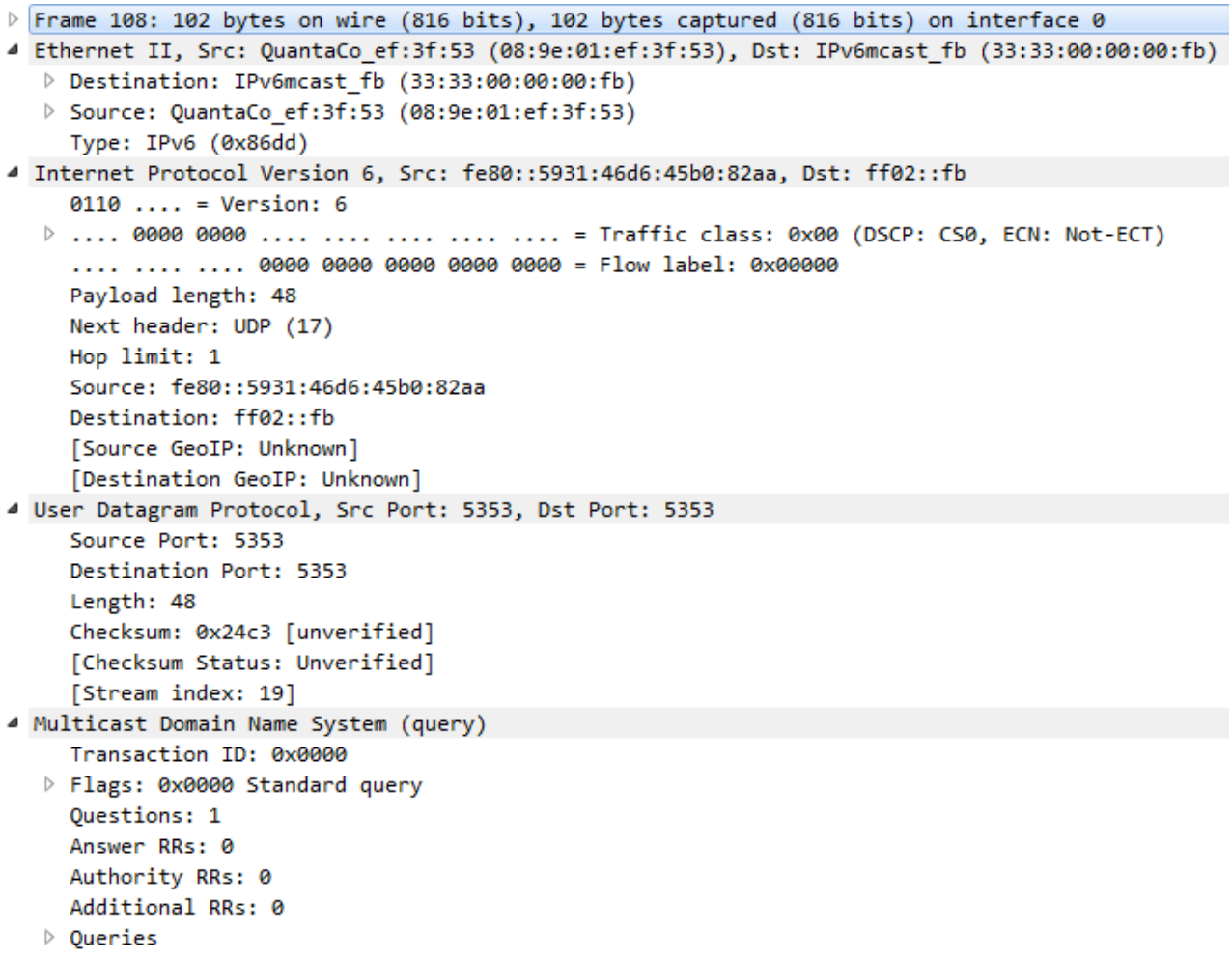
Wireshark отображает информацию о перехваченных пакетах двумя способами: сокращённо (рис. 4) и детально. Детальный способ позволяет раскладывать пакет по уровням модели OSI (рис. 5).

Wireshark подходит как компонент перехвата и анализа пакетов, но его применение осложняется GUI. Для человеческого восприятия Wireshark походит отлично, однако для связи с программой, отрабатывающий какой-либо алгоритм будет крайне сложно.



	Time	Source	Destination	Protocol	Length	Info
85	2.593998	85.143.78.115	85.143.78.255	NBNS	92	Name query NB RETRACKER<00>
86	2.598039	Routerbo_e4:89:14	Spanning-tree-(for-…	STP	56	RST. Root = 32768/0/00:15:17:d9:85:cb Cos
87	2.600783	85.143.78.98	85.143.78.255	UDP	82	58773→1947 Len=40
88	2.604791	85.143.78.90	85.143.78.255	UDP	305	54915→54915 Len=263
89	2.606686	85.143.78.14	85.143.78.255	NBNS	92	Name query NB XRXD3B039.DLINK<00>
90	2.608580	CiscoInc_d8:19:c6	Broadcast	ARP	60	Who has 85.143.79.124? Tell 85.143.79.1
91	2.619293	CiscoInc_19:28:01	PVST+	STP	64	RST. Root = 24576/811/b8:be:bf:d8:19:80 C
92	2.630234	CiscoInc_d8:19:c6	Broadcast	ARP	60	Who has 85.143.78.206? Tell 85.143.78.1
93	2.682480	CiscoInc_d8:19:c6	Broadcast	ARP	60	Who has 85.143.79.51? Tell 85.143.79.1
94	2.707997	217.13.222.29	85.143.78.114	TCP	60	44637→6565 [SYN] Seq=0 Win=1024 Len=0 MSS=
95	2.744308	CompalIn_62:25:2f	Broadcast	ARP	60	Who has 85.143.78.11? Tell 85.143.78.15
96	2.757523	CiscoInc_d8:19:c6	Broadcast	ARP	60	Who has 85.143.79.135? Tell 85.143.79.1
97	2.781309	5.43.240.73	85.143.78.21	UDP	146	19336→60559 Len=104
98	2.847417	LcfcHefe_55:f2:2a	Broadcast	ARP	60	Who has 85.143.78.11? Tell 85.143.78.89
99	2.892305	CiscoInc_d8:19:c6	Broadcast	ARP	60	Who has 85.143.79.36? Tell 85.143.79.1
100	2.901685	CiscoInc_d8:19:c6	Broadcast	ARP	60	Who has 85.143.79.62? Tell 85.143.79.1
101	2.913578	CiscoInc_d8:19:c6	Broadcast	ARP	60	Who has 85.143.78.20? Tell 85.143.78.1
102	2.939164	CiscoInc_d8:19:c6	Broadcast	ARP	60	Who has 85.143.79.69? Tell 85.143.79.1
103	2.950293	85.143.78.177	255.255.255.255	UDP	155	62852→1228 Len=113
104	3.029980	CiscoInc_d8:19:c6	Broadcast	ARP	60	Who has 85.143.78.124? Tell 85.143.78.1
105	3.089874	CiscoInc_d8:19:c6	Broadcast	ARP	60	Who has 85.143.79.128? Tell 85.143.79.1
106	3.131147	CiscoInc_d8:19:c6	Broadcast	ARP	60	Who has 85.143.79.95? Tell 85.143.79.1
107	3.131914	85.143.78.53	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp
108	3.131915	fe80::5931:46d6:45b…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp
109	3.197360	CiscoInc_d8:19:c6	Broadcast	ARP	60	Who has 85.143.79.175? Tell 85.143.79.1
110	3.340033	LiteonTe_46:84:4d	Broadcast	ARP	60	Who has 85.143.78.1? Tell 85.143.78.26
111	3.356429	85.143.78.14	85.143.78.255	NBNS	92	Name query NB XRXD3B039.DLINK<00>

Рисунок 4. Пример отображения перехваченных пакетов



```
▷ Frame 108: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
◢ Ethernet II, Src: QuantaCo_ef:3f:53 (08:9e:01:ef:3f:53), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
    ▷ Destination: IPv6mcast_fb (33:33:00:00:00:fb)
    ▷ Source: QuantaCo_ef:3f:53 (08:9e:01:ef:3f:53)
      Type: IPv6 (0x86dd)
◢ Internet Protocol Version 6, Src: fe80::5931:46d6:45b0:82aa, Dst: ff02::fb
      0110 .... = Version: 6
    ▷ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
      .... .... .... 0000 0000 0000 0000 0000 = Flow label: 0x00000
      Payload length: 48
      Next header: UDP (17)
      Hop limit: 1
      Source: fe80::5931:46d6:45b0:82aa
      Destination: ff02::fb
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
◢ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
      Source Port: 5353
      Destination Port: 5353
      Length: 48
      Checksum: 0x24c3 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 19]
◢ Multicast Domain Name System (query)
      Transaction ID: 0x0000
    ▷ Flags: 0x0000 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    ▷ Queries
```

Рисунок 5. Детальный разбор пакета по уровням модели OSI

1.2.3. Tshark

Tshark – консольная версия Wireshark. Он способен перехватывать пакеты и разбирать их на параметры (рис. 6), что и Wireshark в списке перехваченных пакетов. Однако Tshark выводит информацию в текстовом виде в стандартный поток вывода – **stdout**, что существенно упрощает задачу взаимодействия с основной программой алгоритма [11].

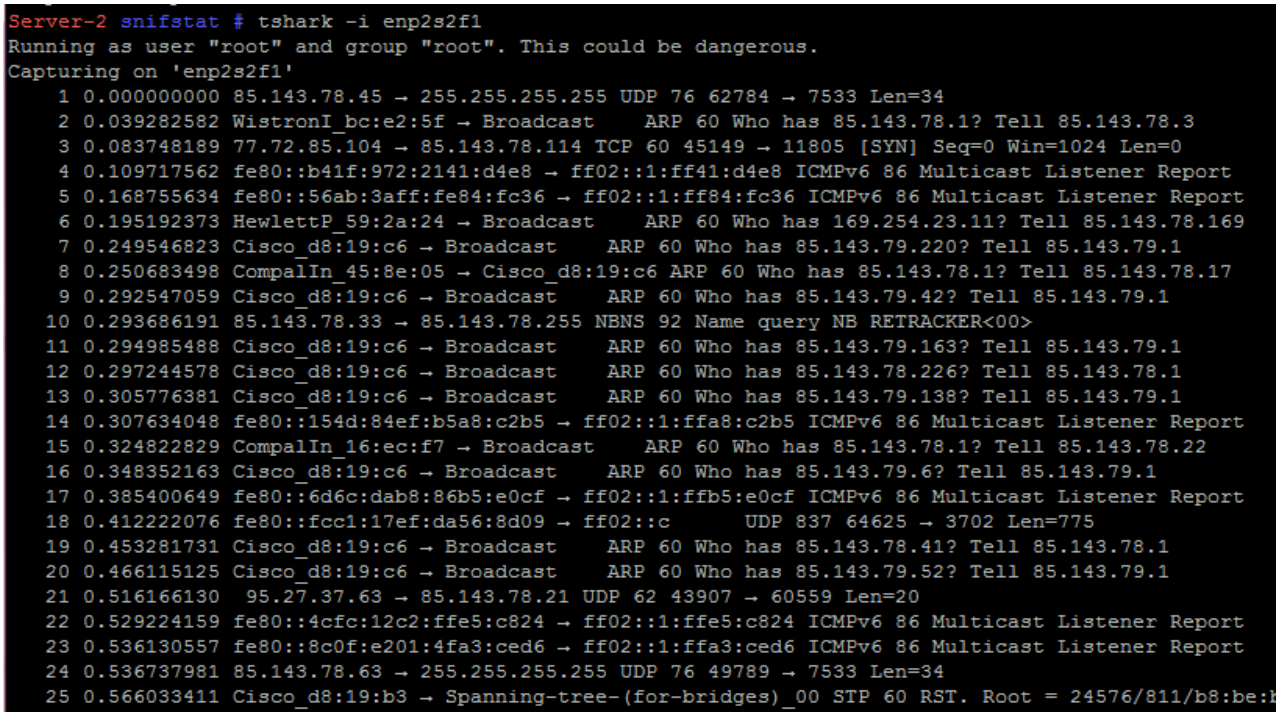


Рисунок 6. Пример вывода Tshark.

Таким образом, запуск Tshark в отдельном дочернем процессе с перенаправление стандартного потока вывода является самым оптимальным вариантом захвата трафика. Большим преимуществом такого решения является вывод краткой информации о содержании пакета, что облегчит диагностику.

2. Разработка программного обеспечения

2.1. Механизм сбора статистики

Это один из самых ответственных механизмов в разрабатываемой системе. Именно на этот узел будет ложиться основная нагрузка постоянно прослушиваемого трафика, поэтому очень важно этот механизм сделать достаточно производительным. С этой целью был выбран язык программирования C как самый производительный в процессе исполнения кода. Такая производительность объясняется тем, что все системные средства и библиотеки взаимодействия с системой и сетью написаны именно на этом языке, что обеспечивает наилучшее взаимодействие между компонентами. Так же стоит отметить возможность оптимизации исполняемых файлов под конкретный тип процессора, что позволяет задействовать дополнительные аппаратные средства, например криптографический блок AES в процессорах Intel.

2.1.1. Архитектура

Архитектура механизма сбора статистики состоит из трёх основных компонентов (рис. 7): Tshark (перехватчик пакетов), базы данных и разработанного связующего звена – ядра системы.

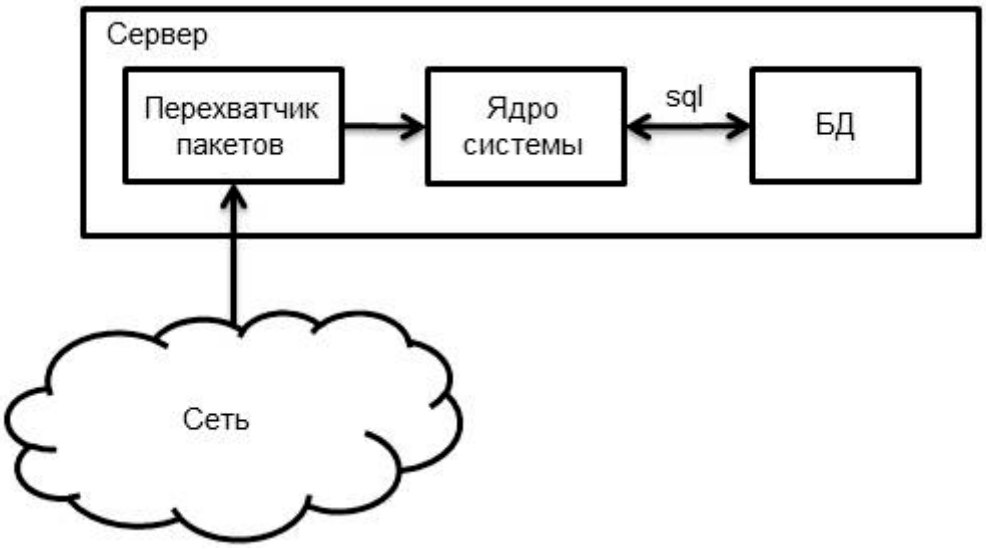


Рисунок 7. Архитектура механизма сбора статистики.

2.1.2. Вывод и перехват stdout от Tshark

Tshark перехватывает пакеты и производит их сигнатурный разбор. Далее он для каждого обработанного пакета выводит в stdout строку содержащую следующую информацию:

1. Номер пакета;
2. Временной штамп;
3. Источник отправителя;
4. Источник получателя;
5. Протокол;
6. Длину пакета;
7. Пояснение содержание пакета.

Для интеграции Tshark в проект были выбраны следующие инструменты:

1. Posix threads – даёт возможность в пределах одного процесса делать параллельно обрабатываемые потоки;
2. Pipe – обеспечивает лёгкую передачу данных между процессами.

Таким образом, для внедрения Tshark требуется 2 дополнительных потока. Первый поток запускает Tshark с перенаправлением **stdout** в заранее подготовленный **pipe**. Второй поток прослушивает **pipe** и по приходу строки производит её разбор. Из полученной строки в специальную структуру помещаются 4 параметра:

1. Источник отправителя;
2. Источник получателя;
3. Протокол;
4. Пояснение содержание пакета.

Далее со структурой каждого пакета работает система хранения данных.

2.1.3. Система хранения данных

Система хранения данных состоит из внутренней и внешней БД. Внутренняя БД – это динамический массив данных в оперативной памяти. Внешняя БД – MySQL. Такой подход обусловлен тем, что сетевые пакеты приходят во много раз чаще, чем внешняя БД способна обрабатывать запросов. Поэтому часть операций пришлось вынести во внутреннюю БД. К таким операциям относятся операции первичной агрегирования данных и подсчёт контрольной суммы **md5** для более быстрой работы с базой данных.

Алгоритм обработки пакета внутренней базы данных представлен на рисунке 8.

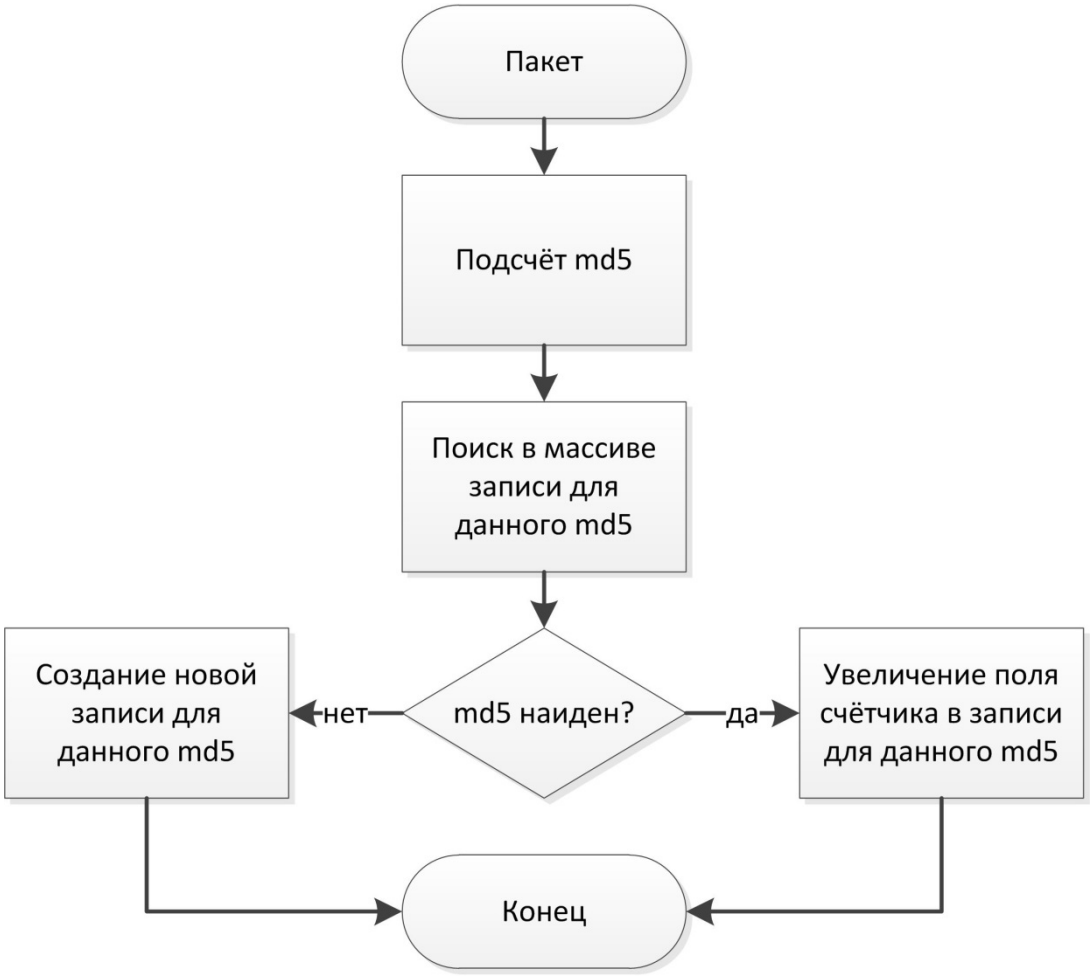


Рисунок 8. Алгоритм обработки пакета.

Таким образом, формируется внутренняя база данных пакетов с их счётчиками. Раз в минуту происходит выгрузка данных во внешнюю БД по алгоритму, представленному на рисунке 9.

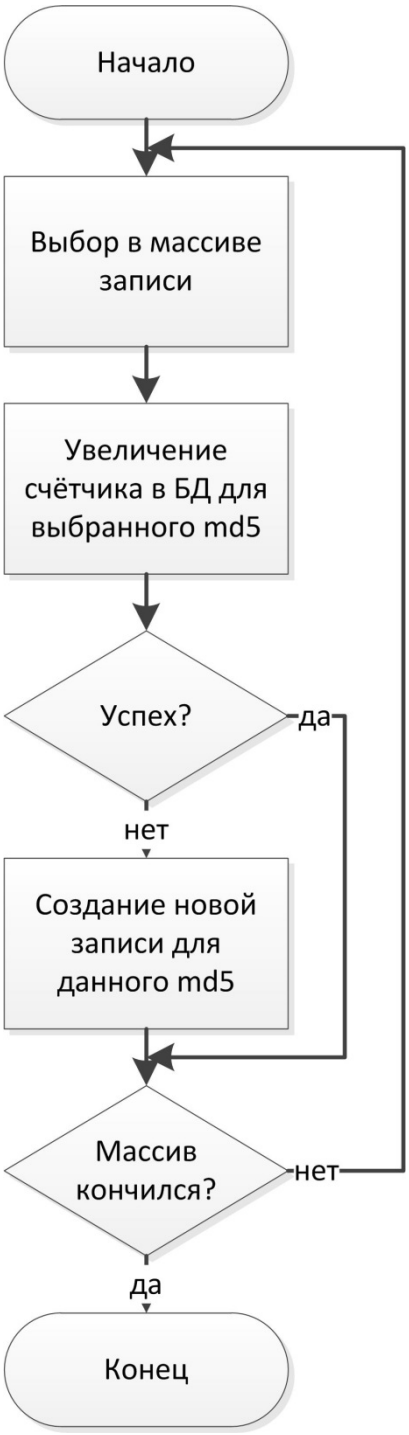


Рисунок 9. Алгоритм выгрузки данных во внешнюю БД.

Внешняя БД имеет 2 типа таблиц: с данными и счётчиками пакетов. На рисунке 10 представлен пример этих таблиц packets и packets_cnt соответственно.

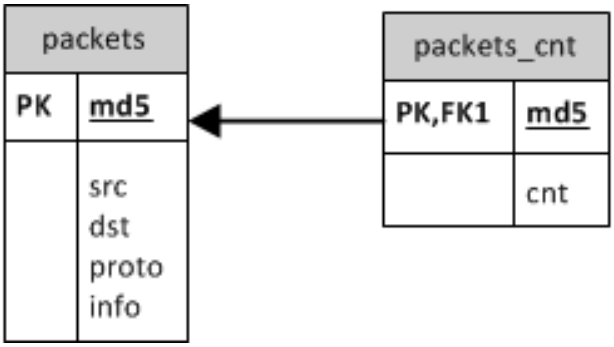


Рисунок 10. Таблицы статистики.

Отдельные таблицы для счётчиков необходимы для ведения статистики на разных временных интервалах:

1. На всём интервале;
2. Последний месяц;
3. Последняя неделя;
4. Последний день;
5. Последний час;
6. Последние 15 минут;
7. Последняя минута.

Для каждой таблицы счётчиков в определённый интервал запускается выгрузка значений счётчиков в таблицу с большим временным интервалом.

2.2. Механизм отображения статистики

Основой вывода статистики служат SQL запросы к нужной временной таблице. Такой способ удобен тем, что всю работу фильтрования результата можно поручить СУБД. Например, подвести статистику по количеству пакетов всех сохранённых протоколов:

```
SELECT snifstat.packets.proto, sum(cnt) AS s
FROM snifstat.packets JOIN snifstat.packets_cnt
ON snifstat.packets.md5 = snifstat.packets_cnt.md5
GROUP BY proto
```

```
ORDER BY s desc;
```

Или посмотреть данные всех пакетов (пример рис 11):

```
SELECT * FROM snifstat.packets;
```

md5	src	dst	proto	info
b1f031b20a16a55c19532a0bca450b20	HewlettP_61:a...	Broadcast	ARP	Who has 85.143.78.1? Tell 85.143.78.52
11ec42aee63d5b664218c816cc13bec0	fe80::14c0:c2...	ff02::1:ff3d:f7f4	ICMPv6	Neighbor Solicitation for fe80::e855:35d7:..
4a7cdbab413159c05378c33ec4a76116	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.92? Tell 85.143.79.1
7dbaf9397d8ed42dcd27b3ebd5819e4c	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.125? Tell 85.143.79.1
e02db92f2185ce3a9f984021f5c20b9d	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.254? Tell 85.143.79.1
b2cc6372f167b784e1565d6cf66c2bf4	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.133? Tell 85.143.79.1
9071999891d6074efb02ad5fb77e2c63	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.253? Tell 85.143.79.1
77e7cfa460ffdf294237aea015fd7bcd	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.89? Tell 85.143.79.1
38ccab42a4c078969247e6a2d4a9d0d7	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.157? Tell 85.143.79.1
3be7861bd22365738a4de38011d8a39d	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.105? Tell 85.143.79.1
27b021f8b02e95da2675484679d81d9e	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.196? Tell 85.143.79.1
ee5874f53850127df6d03e131ff9726d	85.143.78.15	255.255.255.255	UDP	54376 → 7533 Len=34
f826726ef3b351d2ab952816a55dd726	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.90? Tell 85.143.79.1
e9f8072f20b2fd033a0e1d28d1c7467e	85.143.78.244	255.255.255.255	UDP	65006 → 7533 Len=34
01661fe772beabd8e38176bffdf74710	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.78.21? Tell 85.143.78.1
7ce56b23946db3e82c0c3d9d6e5143ca	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.52? Tell 85.143.79.1
03f89156140e763d07b49b1bd35b5ddb	85.143.78.90	85.143.78.255	UDP	54915 → 54915 Len=263
9db7d995d067c91d39d0505a3cb16cd9	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.232? Tell 85.143.79.1
4ff94350afa60afef67a6361addcb7da	Cisco_19:28:34	Spanning-tree-(f...	STP	RST. Root = 24576/811/b8:be:bf:d8:19:8..

Рисунок 11. Часть перехваченных пакетов.

2.3. Механизм локализации аномалий в сети

Наиболее эффективное средство локализации аномалии это блокировка источника этой аномалии. Для данной задачи было решено использовать аппаратные средства оборудования в сочетании с внешним управлением по протоколу SNMP [12].

Протокол SNMP позволяет получать и задавать значения элементов MIB управляемого устройства. MIB – древовидная база параметров различных типов, среди которых присутствуют INTEGER, STRING, TIME и многие другие [13].

2.3.1. Алгоритм обнаружения аномалий

Основой алгоритма лежит анализ статистических данных, а именно названия протоколов и типов сообщений. При появлении в статистике нового

протокола или новых типов сообщений уже известного протокола происходит информирование системного администратора по протоколу **syslog**. Такой способ информирования очень удобен, а так же упрощает интеграцию с общей системой мониторинга предприятия. Администратор производит анализ данных пакетов и принимает решение о том, к какой группе опасности отнести данные тип пакетов:

1. Полностью безопасные пакеты – пакет не будет рассматриваться как угроза;
2. Безопасные от конкретных хостов – пакет считается безопасным, если исходит от конкретного хоста или группы хостов, иначе – блокировка источника;
3. Потенциально опасные – до определённого порога пакетов в единицу времени считаются безопасными, по превышению этого порога наступают блокирующие действия (алгоритм обработки пакетов по этому правилу представлен на рисунке 12);
4. Опасные пакеты – моментальная блокировка источника пакета.

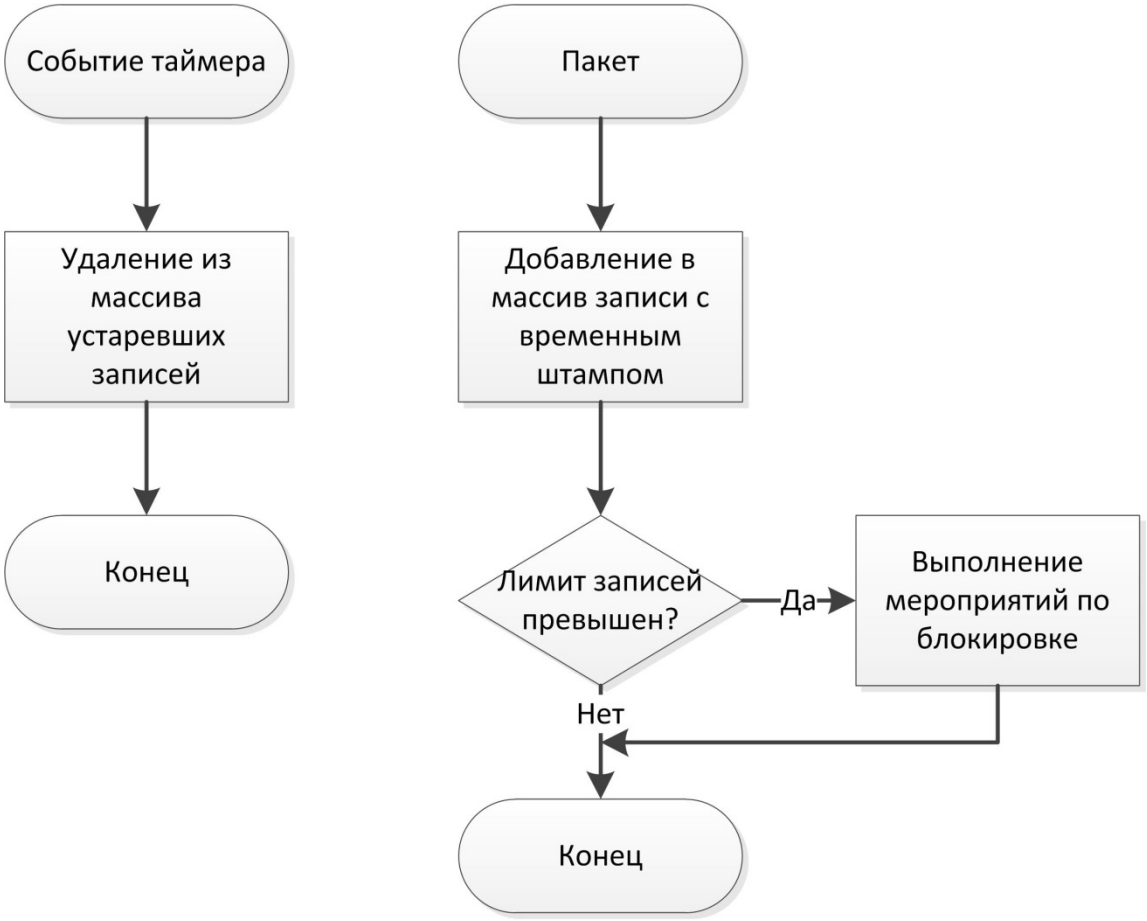


Рисунок 12. Алгоритм обработки пакетов с временным ограничением.

На хранение данных правил в БД выделена отдельная таблица, формат которой представлен на рисунке 13.

actions	
PK	**rule_id**
	type **protocol** protocol_info src limit limit_interval

Рисунок 13. Таблица правил.

Где:

rule_id – уникальный идентификатор правила;

type – тип пакета (описаны выше);

protocol – название протокола;

protocol_info – дополнительная информация и пакете;

src – источник пакета;

limit – ограничение количества пакетов;

limit_interval – интервал учёта лимита пакетов;

Дополнительно в помощь администратору разработаны алгоритмы обнаружения аномалий в полностью автоматическом режиме.

2.3.1.1. Алгоритм обнаружения аномалий протокола ARP

Работа алгоритма делится на 2 этапа:

1. Обучение – выучивание связок MAC – IP;
2. Слежение – регистрация изменений с последующими действиями.

Общий алгоритм представлен на рисунке 14.

Рисунок 14. Алгоритм обнаружения аномалий протокола ARP.

2.3.1.2. Алгоритм обнаружения аномалий протокола ICMP

Алгоритм базируется на блокировке сообщений некоторых типов:

5 – Перенаправление:

9 – объявление маршрутизатора:

10 – запрос маршрутизатора.

Блокировка сообщений типа 5 и 9 будут срабатывать на злоумышленнике, в то время как 10 тип сработает на клиенте, предотвращая замену безопасного маршрутизатора, полученного по DHCP. В этом случае требуется уведомление администратора по средствам **syslog.**

Общий алгоритм представлен на рисунке 15.

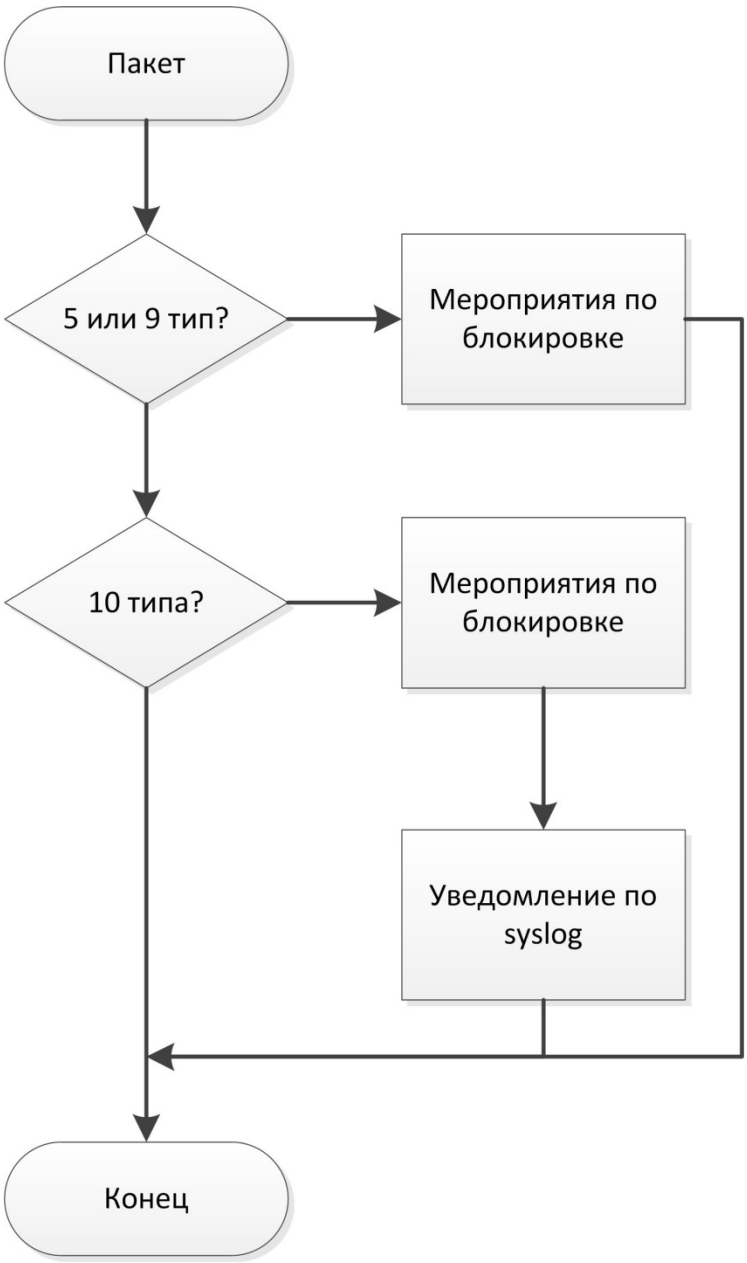


Рисунок 15. Алгоритм обнаружения аномалий протокола ICMP.

2.3.2. Управление оборудованием

Конечные клиенты подключаются к Ethernet коммутатором, поэтому было принято решение управлять только коммутаторами. В сети используются коммутаторы фирмы Cisco, модели: 2950, 2960 и 3750. Они очень схожи в управлении и имеют почти идентичные MIB. Для блокировки злокачественного клиента необходимо знать его MAC или IP адрес. Общий

алгоритм отключения порта представлен на рисунке 16. Для его реализации требуются следующие узлы:

1. База коммутаторов с их данными для подключения;
2. База связок IP – MAC и IPv6 – MAC;
3. SNMP Manager для взаимодействия с коммутаторами.

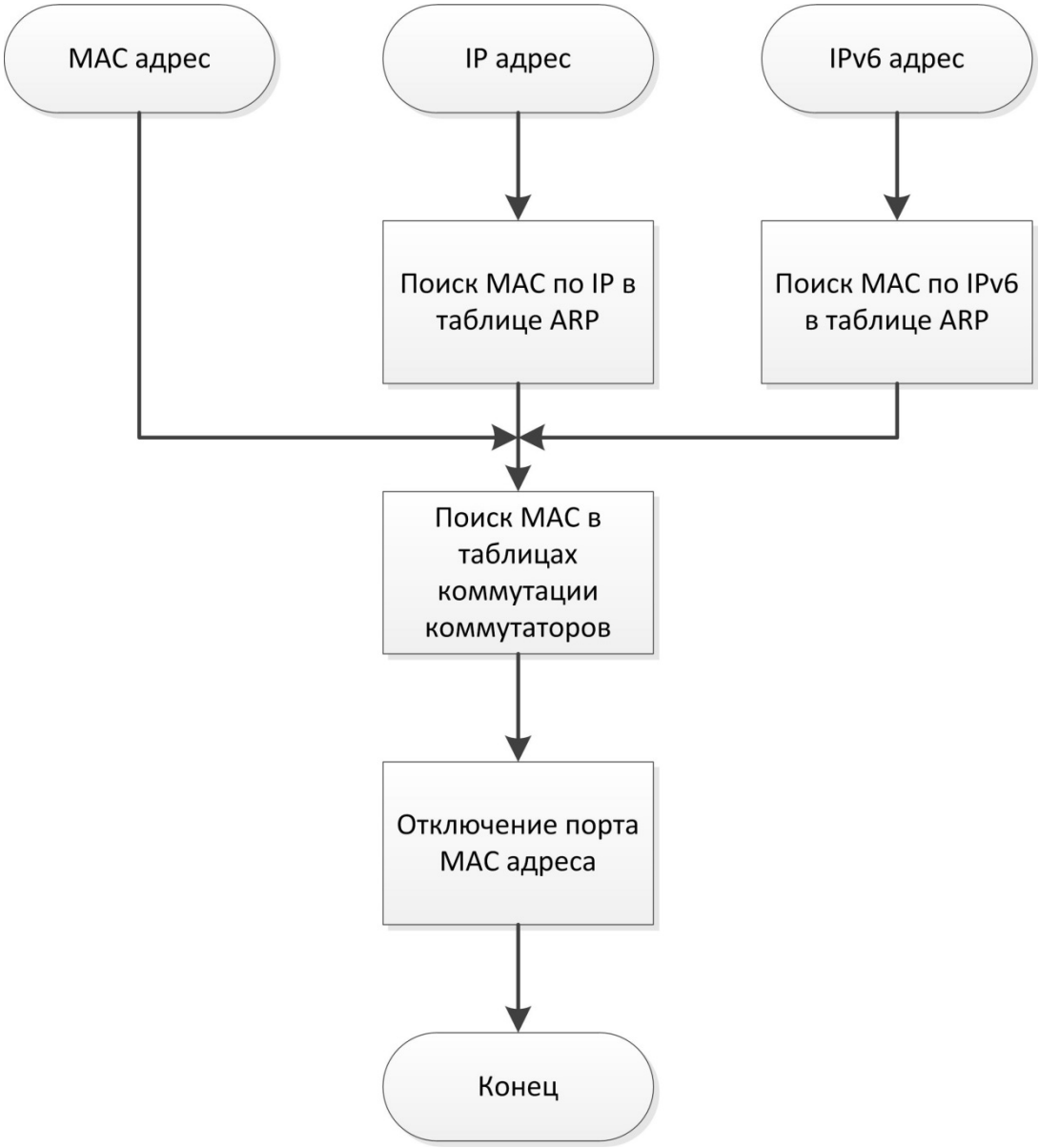


Рисунок 16. Алгоритм изоляции источника аномалии.

2.3.2.1. База коммутаторов

База с данными для подключения к коммутаторам храниться в MySQL в виде таблицы (рис. 17)

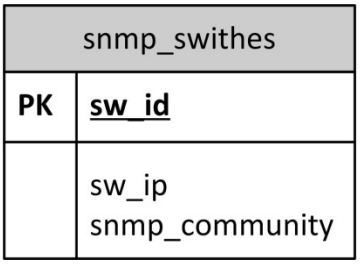


Рисунок 17. Справочник коммутаторов.

Где:

sw_id – уникальный идентификатор коммутатора;

sw_ip – IP-адрес коммутатора;

snmp_community – строка авторизации протекла SNMP.

2.3.2.2. База связок IP – MAC и IPv6 – MAC

Для получения этих связок было решено использовать готовый проект с открытыми исходными кодами **addrwatch**. Эта утилита прослушивает сетевой интерфейс и перехватывает arp пакеты, составляя по ним актуальную базу данных. Утилита поддерживает несколько способов вывода данных:

1. Stdout – построчный вывод изменений в окно терминала;
2. Syslog – протокол для службы регистрации сообщений о системных событиях. Для регистрации подобных сообщений создано большое количество программного обеспечения с различным функционалом;
3. MySQL – выгрузка готовой базы в виде таблицы (рис. 18)

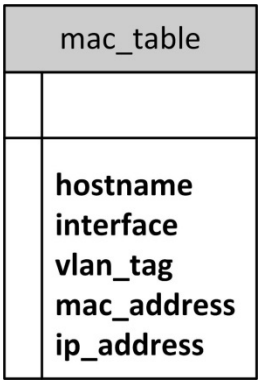


Рисунок 18. Таблица актуальных сетевых узлов.

Где:

hostname – имя компьютера который заносит запись в таблицу (в данном случае это имя одного сервера);

interface – имя сетевого интерфейса где был обнаружен MAC адрес;

vlan_tag – номер vlan а котором был обнаружен MAC адрес;

mac_address – сам MAC адрес;

ip_addres – IP или IPv6 адрес.

Для удобства было решено использовать выгрузку в БД MySQL для упрощения поиска и снижения временных затрат на разработку.

2.3.2.3. SNMP Manager

Для написания SNMP менеджера, было принято решения за основу взять библиотеку с открытыми исходными кодами Net-SNMP. Данная библиотека написана на языке C и обеспечивает базовые рутинные действия для работы по протоколу SNMP:

1. Открыть соединение;
2. Сконфигурировать запрос;
3. Отправить запрос;
4. Отправить асинхронный запрос;
5. Получить ответ;
6. Закрыть соединение.

Работа SNMP менеджера делится на несколько этапов:

1. Получение списка с IP и SNMP Community;
2. Открытие соединений со всеми коммутаторами
3. Получение базово необходимых параметров (о них ниже);
4. Периодическое сканирование коммуникационных таблиц коммутаторов для составления копии внутри процесса, что ускоряет поиск порта MAC адреса.

2.3.2.3.1. Базовые параметры коммутаторов

В MIB дереве коммутатора было выявлено несколько ключевых веток:

1. Управление портами и прочими интерфейсами;
2. Управление сетевым мостом, в который «подключены» интерфейсы;
3. Таблица связок MAC адрес – номер порта в мосту (мост – виртуальное понятие);
4. Таблица связок номер порта в коммутаторе – ID интерфейса из первой ветки.

Для дальнейшей разработки проекта было принято решение для каждого коммутатора использовать массивы со следующими структурами:

```
struct snmp_switch_port_state
{
    // Interface index
    int32_t        id;
    // Hardware interface name
    char           *description;
    // 1 – on, 2 - off
    int32_t        admin_status;
    // 1 – link ok, 2 – no link
    int32_t        operation_status;
    // bridge port number
    uint32_t       bridge_port;
    // 0 – off, 1 - on
    unsigned int   enable;
} typedef snmp_switch_port_state_t;

struct snmp_switch_mac_address
{
    Char           mac_address[6];
    // bridge port number
```

```
    uint32_t       bridge_port;
} typedef snmp_switch_mac_address_t;
```

В первую очередь для каждого коммутатора строится массив структур snmp_switch_port_state по ветке со всеми интерфейсами. Во время выполнения данного этапа заполняются поля: id и description.

Следующим этапом идёт сканирование таблицы соответствий id интерфейса – номер порта в мосту. Пример таблицы представлен на рисунке 19, где:

SNMPv2-SMI::mib-2.17.1.4.1.2.**39** = INTEGER: **10035**

39 – bridge port;

10035 – id интерфейса.

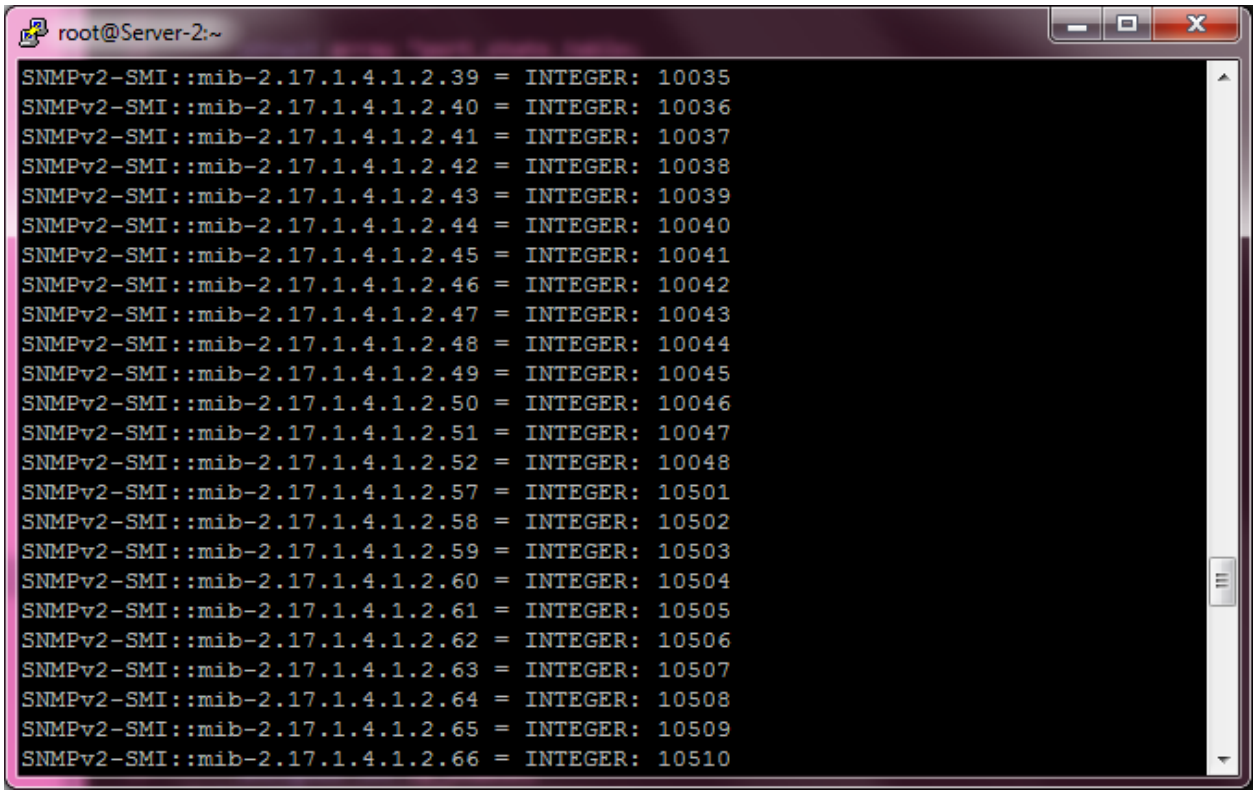


Рисунок 19. SNMP таблица соответствий id интерфейса – номер порта в мосту.

Для этого сканируется соответствующая ветка, по данным которым происходит перебор всех id интерфейсов и при совпадении заполняется поле bridge_port в структуре snmp_switch_port_state.

После выполнения выше описанных подготовительных мероприятий начинается циклический опрос ветки таблицы коммутации, пример которой представлен на рисунке 20, где:

SNMPv2-SMI::mib-2.17.4.3.1.2 – адрес ветки;

252.69.150.227.198.3 – MAC адрес в десятичном формате (выделенная на рисунке часть);

INTEGER – тип данных в листике полученного дерева;

353 – номер порта в мосту.

Таким образом, SNMP Manager получает локальную копию таблицы коммутации, что значительно ускоряет работу. Сканирование веток самого коммутатора может проходить с разной скоростью, в зависимости от производительности оборудования и его загруженности.

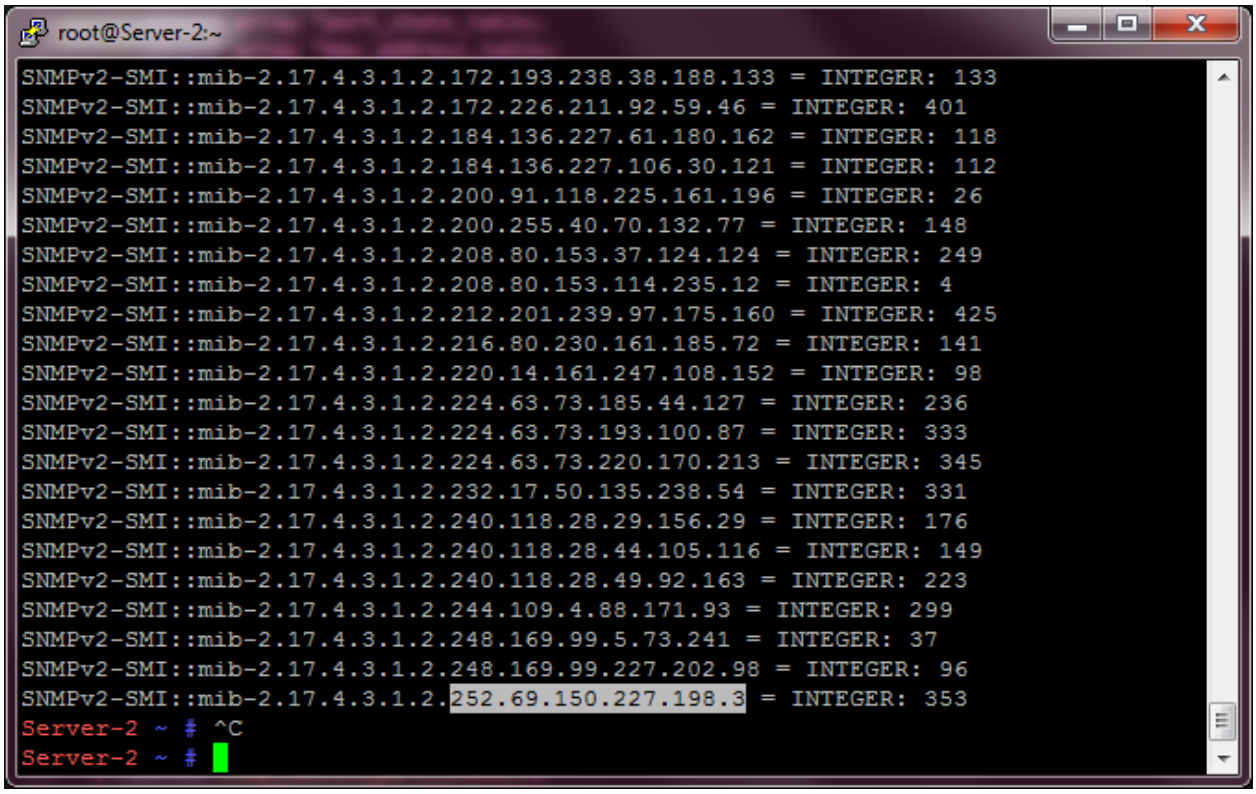


Рисунок 20. SNMP таблица коммутации

2.3.2.3.2. Алгоритм отключения порта

Как только поступает команда отключить порт по MAC адресу злоумышленника, происходит:

1. поиск MAC адреса по локальным копиям таблиц коммутации всех коммутаторов
2. вычисляется номер порта в мосту
3. по номеру порта в мосту вычисляется id интерфейса, и по id интерфейса на коммутатор формируется команда для перевода физического порта в состояние disable.

Полный алгоритм представлен на рисунке 21.

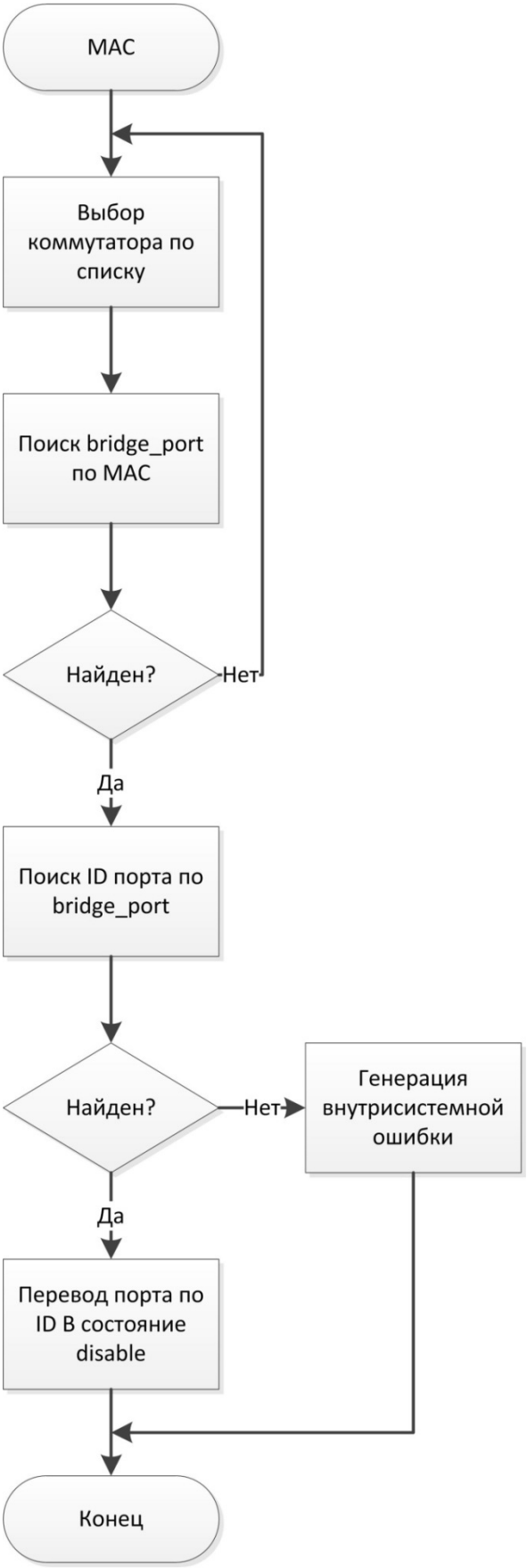


Рисунок 21. Алгоритм отключения порта на оборудовании.

3. Анализ данных

3.1. Наиболее используемые протоколы

Гистограмма, построенная на основе перехваченных пакетов, представлена на рисунке 22. Полный список протоколов представлен в приложении А.

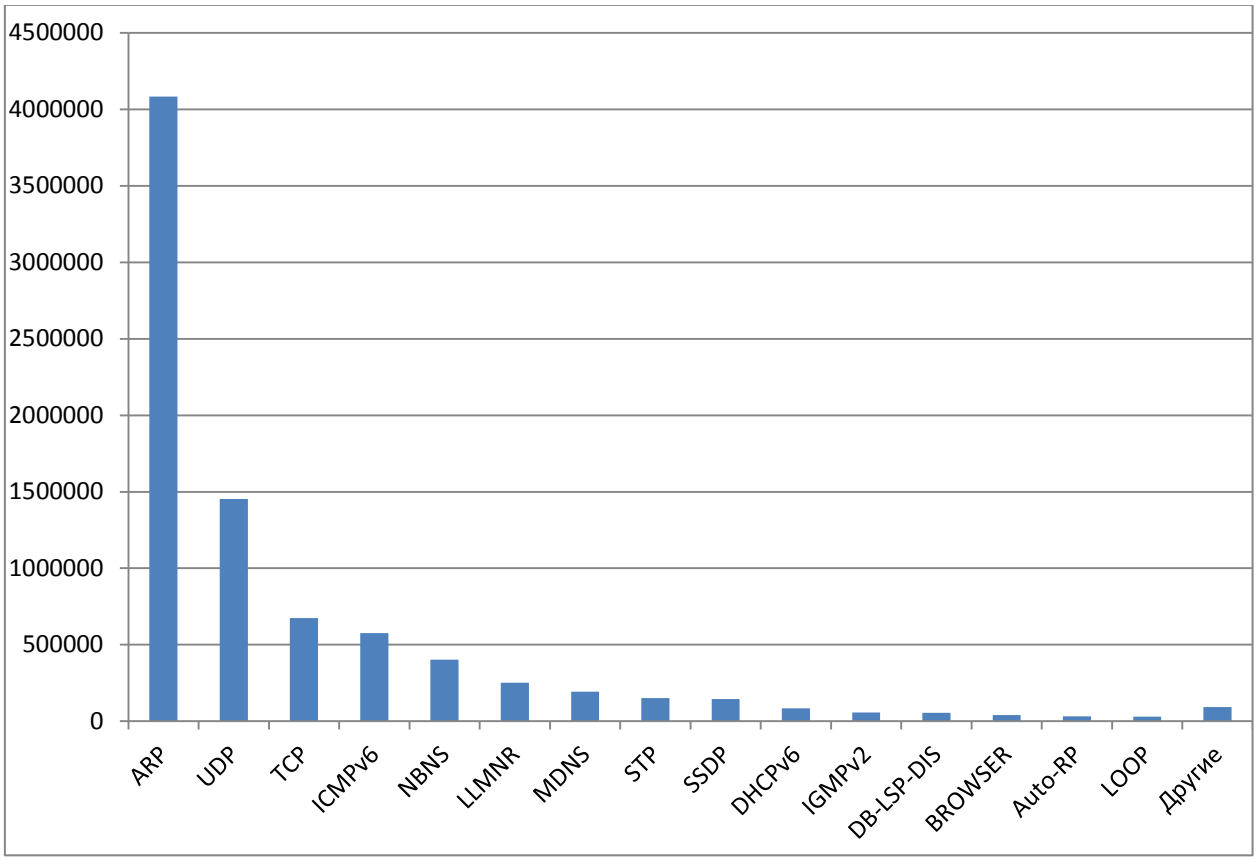


Рисунок 22. Наиболее используемые протоколы.

3.1.1. ARP

ARP (Address Resolution Protocol) основная его задача – получить L2-адрес устройства (MAC-адрес) при известном L3-адресе устройства (IP-адрес) [14]. Для просмотра статистики подготовим SQL запрос:

```
SELECT proto,info,cnt FROM snifstat.packets
JOIN snifstat.packets_cnt
ON snifstat.packets.md5 = snifstat.packets_cnt.md5
WHERE snifstat.packets.proto = 'ARP'
GROUP BY info;
```

Результат показал, что в сети были следующие типы запросов (IP адреса для примера):

1. «Who has 85.143.78.106? Tell 85.143.78.182» – обычный запрос на получение MAC адреса конкретного IP;
2. «85.143.78.112 is at 50:9a:4c:c9:3d:0d» – обычный ответ на запрос выше;
3. «Gratuitous ARP for 85.143.78.159 (Request)» – такие сообщения используется для оповещения о появлении новой связки IP и MAC адресов. Так же это помогает обнаружить конфликты IP-адресов.

Анализ пакетов данного протокола показал, что потенциально есть места возникновения неисправностей – сообщения Gratuitous ARP о смене MAC адреса.

3.1.2. UDP

UDP (User Datagram Protocol) востребованный транспортный протокол передачи данных. Используется многими приложениями и сервисами для быстрой доставки сообщений без контроля доставки [15].

Для просмотра статистики подготовим SQL запрос:

```
SELECT src,dst,info,cnt FROM snifstat.packets
JOIN snifstat.packets_cnt
ON snifstat.packets.md5 = snifstat.packets_cnt.md5
WHERE snifstat.packets.proto = 'UDP'
GROUP BY info;
```

Анализ статистики для данного протокола позволил выявить выделяющееся из сети устройство:

«85.143.78.90 → 85.143.78.255; 54915 → 54915 Len=263»

Именно UDP сообщения от 85.143.78.90 преобладают в сети над другими сообщениями, с большим отрывом в 5 раз.

Далее целый ряд широковещательных сообщений от большинства участников сети:

«85.143.78.45 → 255.255.255.255; 63868 → 7533 Len=34»

Опасность они не представляют, так как это пакеты известной игры World Of Tanks [16].

Остальные типы пакетов приходят из глобальной сети для конкретных устройств. Для сети это безопасно, за исключением возможности чрезмерной нагрузки на канал.

3.1.3. ICMPv6

ICMPv6 – протокол управляющих сообщений для IPv6. ICMPv6 отвечает за сообщения о сетевых ошибках, обладает диагностическими функциями, используется для поиска соседних устройств, а так же служит для определения MTU[17].

«fe80::8e89:a5ff:fec4:3ebf → ff02::2; Router Solicitation» – предложение маршрута;

«fe80::8e89:a5ff:fec4:3ebf → ff02::2; Neighbor Solicitation» – предложение соседства;

Протокол в сети используют мало устройств, обусловлено это тем, что протокол IPv6 новый и в данной сети не внедрён, да и к тому же не все устройства поддерживают IPv6. А те устройства, где этот протокол поддерживаются, уязвимы из-за угрозы подмены маршрута. Для устранения уязвимости необходимо на устройствах вручную отключать IPv6.

3.1.4. TCP

TCP (Transmission Control Protocol) – так же как и UDP, является одним из основных протоколов передачи данных. Запрос статистики:

```
SELECT src,dst,info,cnt FROM snifstat.packets
JOIN snifstat.packets_cnt
ON snifstat.packets.md5 = snifstat.packets_cnt.md5
WHERE snifstat.packets.proto = 'TCP'
```

```
GROUP BY info;
```

Анализ результата показал наличие большого количества SYN пакетов (запрос на подключение по протоколу TCP) из глобальной сети, что можно считать за атаку, так как это нагружает как сетевое оборудование, так и клиентское [18].

Так же очень много TCP Retransmission пакетов. Это говорит о потере пакетов. Причиной может служить перегрузка оборудования или канала, так же неисправные соединения [19]. Кроме как нагрузки на канал вредных воздействий нет.

3.1.5. NBNS

NBNS – протокол службы NetBIOS. Служит для выполнения регистрации имён компьютеров в сети и преобразование имён в адрес [20].

```
SELECT src,dst,info,cnt FROM snifstat.packets
JOIN snifstat.packets_cnt
ON snifstat.packets.md5 = snifstat.packets_cnt.md5
WHERE snifstat.packets.proto = 'NBNS'
GROUP BY info;
```

Результат показал, что по протоколу NBNS есть только 2 типа пакетов:

«85.143.78.45', '85.143.78.255; Registration NB HOME14NEW<00>» – анонсирование NetBIOS имени нового узла;

«85.143.78.32 → 85.143.78.255; Name query NB DESKTOP-VFP3234<1c>» – запрос IP по NetBIOS имени узла.

Протокол представляет угрозу для внутренних ресурсов, таких как общие папки на компьютерах рабочей группы, так как протокол подвержен spoofing атаке – подмене адреса [21].

3.1.6. LLMNR

Аналогичен NBNS. В сети используется намного реже и ещё меньшим количеством узлов. Объясняется это тем, что протокол относительно новый и не везде поддерживается. Уязвимости неаналогичные как и в NBNS [22].

3.1.7. STP

STP – канальный протокол в сети Ethernet, основной задачей которого является устранение петель (избыточных соединений) [23]. В сети есть только один тип пакета:

«Cisco_19:28:34 → Spanning-tree-(for-bridges)_00; RST. Root = 24576/811/b8:be:bf:d8:19:80 Cost = 0 Port = 0x81ae» – анонсирование корневого коммутатора.

STP уязвим атаке. Суть атаки заставить сеть постоянно перестраивать топологию, во время чего сеть становиться неработоспособной. Делается это путём анонсирование ложного корневого коммутатора. Единственная защита от этого – аппаратная фильтрация STP пакетов [23].

3.1.8. SSDP

SSDP (Simple Service Discovery Protocol) используется для того, чтобы сетевые клиенты могли обнаруживать различные сетевые сервисы. Данный протокол позволяет обнаруживать UPnP-устройств в сети, например, телевизор с поддержкой DLNA/UPNP или маршрутизаторы [24].

Анализ показал наличие всего одного IPv6 адреса, который производит поиск UPnP устройств по этому протоколу. Никакой опасности тут нет.

3.1.9. MDNS

Multicast DNS – протокол разрешения доменных имён компьютеров в IP адреса. В отличие от чистого DNS, использует мультикаст как способ передачи сообщений. Это позволяет фальсифицировать ответы на запросы. Более того, эту службу можно использовать как инструмент для организации DDoS атак [25].

Анализ статистики показал, что данный протокол активно используется в сети почти всеми участниками. Следовательно, этот протокол требует отдельного контроля.

3.1.10. DHCPv6

DHCP (Dynamic Host Configuration Protocol) – используется для автоматической настройки сетевых параметров таких как IP адрес, шлюз и прочее на клиентских устройствах [26].

В сети отсутствует DHCP сервер для IPv6. Следовательно, устройства не могут получить IPv6 адрес, поэтому они назначают себе IPv6 адрес самостоятельного из определённого диапазона и анонсируют это в сеть. Именно о таких пакетах говорит статистика.

3.1.11. IGMPv2

IGMP (Internet Group Management Protocol) – протокол для управления мультикастами (групповой передачей данных) в сетях, основанных на протоколе IP [27].

Анализ статистики показал, что в сети используется 10 мултикаст групп, 8 из которых относятся к неправильно подключенному маршрутизатору (рис. 23).

192.168.0.1	224.0.0.252	Membership Query, specific for group 224.0.0.252	13361
192.168.0.1	224.0.0.253	Membership Query, specific for group 224.0.0.253	2161
192.168.0.1	224.0.0.251	Membership Query, specific for group 224.0.0.251	2041
85.143.79.1	224.0.1.40	Membership Report group 224.0.1.40	1773
85.143.79.1	224.0.0.1	Membership Query, general	1770
192.168.0.1	224.0.1.40	Membership Query, specific for group 224.0.1.40	95
192.168.0.1	224.0.0.5	Membership Query, specific for group 224.0.0.5	8
192.168.0.1	224.0.2.60	Membership Query, specific for group 224.0.2.60	8
192.168.0.1	230.0.0.1	Membership Query, specific for group 230.0.0.1	4
192.168.0.1	224.2.2.2	Membership Query, specific for group 224.2.2.2	2

Рисунок 23. Анализ перехваченных IGMPv2 пакетов

3.1.12. DB-LSP-DIS

Dropbox LAN sync Discovery Protocol – протокол локальной синхронизации известного приложения DropBox [28].

Наличие этих пакетов говорит о работе DropBox в сети. На работу сети это не влияет, а вот синхронизация между двумя устройствами, подключенными к одному аккаунту, будет проходить в разы быстрее.

3.1.13. BROWSER

Данный протокол позволяет пользователям операционной системы Windows делиться информацией об общих ресурсах. Протокол нужен только для информирования, никакого управления он не оказывает [29].

3.1.14. Auto-RP

Auto-RP это проприетарный протокол на маршрутизаторах Cisco, который позволяет автоматизировать анонсирование информации о группах и RP (Rendezvous Point), которые за них отвечают [30].

В сети все пакеты данного типа исходят от одного доверенного узла.

3.1.15. LOOP

Это протокол для обнаружения петель на канальном уровне [31]. Так же как и Auto-RP, все пакеты данного типа исходят от одного доверенного узла.

3.2. Наиболее активные узлы

Для нахождения наиболее активных узлов был использован запрос:

```
select src, sum(cnt) as s
from snifstat.packets join snifstat.packets_cnt
on snifstat.packets.md5 = snifstat.packets_cnt.md5
group by src
order by s desc;
```

Результат выдал 4 наиболее активных узлов:

1. Cisco_d8:19:c5 – маршрутизатор;
2. 85.143.78.90

3. 85.143.78.15
4. 85.143.78.14

Полный список активный хостов представлен в приложении Б.

Для вывода трафика конкретного узла, например 85.143.78.90 воспользуемся запросом:

```
select src,dst,proto,info, sum(cnt) as s
from snifstat.packets join snifstat.packets_cnt
on snifstat.packets.md5 = snifstat.packets_cnt.md5
where src like '85.143.78.90'
group by proto
order by s desc;
```

Результат выполнения запроса представлен на рисунке 24.

src	dst	proto	info	s
85.143.78.90	85.143.78.255	UDP	54915 → 54915 Len=263	67311
85.143.78.90	85.143.78.255	NBNS	Name query NB WPAD<00>	643
85.143.78.90	224.0.0.251	MDNS	Standard query response 0x0000 PTR 3.11.0.73-DESKTOP-D9O5FQN.51147c...	626
85.143.78.90	224.0.0.252	LLMNR	Standard query 0x49ef A wpad	293
85.143.78.90	85.143.78.255	BROWSER	Host Announcement DESKTOP-D9O5FQN, Workstation, Server, NT Workstation	108

Рисунок 24. Наиболее используемые протоколы узла 85.143.78.90.

Из выше представленного результата можно сделать вывод, что это обычный компьютер на операционной системе Windows, имя компьютера DESKTOP-D9O5FQN. Так же присутствует аномальная широковещательная рассылка UDP пакетов.

Следующий узел 85.143.78.15 (рис. 25):

src	dst	proto	info	s
85.143.78.15	255.255.255.255	UDP	54376 → 7533 Len=34	56568
85.143.78.15	85.143.78.255	NBNS	Registration NB SAMSUNG-<8f><8a><00>	783
85.143.78.15	224.0.0.252	LLMNR	Standard query 0x4fd6 ANY samsung-\320\277\320\272	552
85.143.78.15	224.0.0.251	MDNS	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question	502
85.143.78.15	85.143.78.255	BROWSER	Host Announcement SAMSUNG-Åè, Workstation, Server, SQL Server, NT Wor...	102

Рисунок 25. Наиболее используемые протоколы узла 85.143.78.15.

Для данного узла вывод аналогичен предыдущему. Исключение составляет имя компьютера – SAMSUNG-ПК. Так же на нём установлен SQL сервер.

А вот для следующего узла 85.143.78.14 можно сделать вывод, что это маршрутизатор фирмы D-Link по NBNS запросам (рис. 26).

src	dst	proto	info	s
85.143.78.14	85.143.78.255	NBNS	Name query NB XRXD3B039.DLINK<00>	53571
85.143.78.14	85.143.78.255	BROWSER	Host Announcement èôçƒ, Workstation, Server, Print Queue Server, NT Work...	147
85.143.78.14	224.0.0.251	MDNS	Standard query response 0x0000 PTR 3.13.1.30-\320\232\320\243\320\227\...	64
85.143.78.14	224.0.0.252	LLMNR	Standard query 0xe176 ANY \320\272\321\203\320\267\321\217	8
85.143.78.14	85.143.78.178	UDP	27036 → 27036 Len=107	1

Рисунок 26. Наиболее используемые протоколы узла 85.143.78.14.

В заключении по анализу статистики можно отметить наиболее уязвимые протоколы: ARM, ICMP (вектор атаки – посредник в середине) и MDNS (вектор атаки – подмена хоста).

4. Финансовый менеджмент, ресурсоэффективность и ресурсосбережение

4.1. Предпроектный анализ

4.1.1. Потенциальные потребители результатов исследования

Диссертация посвящена разработке и проектированию программно-алгоритмического обеспечения для системы предсказания, обнаружения и предотвращения сбоев работы компьютерной сети. Для любого проекта имеет место быть необходимость оценки экономической составляющей. В данной диссертации будет оцениваться экономическая выгода от реализации проекта.

Потенциальными потребителями результатов данного исследования являются: системные администраторы, провайдеры, предоставляющие доступ к сети Интернет.

4.1.2. Анализ конкурентных технических решений

Детальный анализ конкурирующих разработок, существующих на рынке, необходимо проводить систематически, поскольку рынки пребывают в постоянном движении. Такой анализ помогает вносить коррективы в научное исследование, чтобы успешнее противостоять своим соперникам. Важно реалистично оценить сильные и слабые стороны разработок конкурентов. В данном случае есть два потенциальных конкурента: «Wireshark» - k1, «CommView» - k2.

Целесообразно проводить данный анализ с помощью оценочной карты, пример которой приведен в таблице 4.1.

Таблица 4.1 – оценочная карта для сравнения конкурентных разработок

Показатели	Вес критерия	Баллы			Конкурентоспособность		
		Бф	Бк1	Бк2	Кф	Кк1	Кк2
Технические критерии оценки ресурсоэффективности							
Удобство в эксплуатации	0,06	4	4	3	0,24	0,24	0,18
Надежность	0,1	4	4	3	0,4	0,4	0,3
Отказоустойчивость	0,2	4	2	2	0,8	0,4	0,4
Качество интерфейса	0,05	4	4	4	0,2	0,2	0,2
Кол-во ресурсов памяти	0,07	3	4	3	0,21	0,28	0,21
Функциональность продукта	0,13	4	4	3	0,52	0,52	0,39
Отсутствие потери данных	0,1	3	4	4	0,3	0,4	0,4
Экономические критерии оценки эффективности							
Уровень конкурентоспособности	0,08	4	5	4	0,32	0,4	0,32
Стоимость	0,05	4	3	2	0,2	0,15	0,1
Срок эксплуатации	0,05	4	4	4	0,2	0,2	0,2
Поддержка продукта	0,07	3	5	4	0,21	0,35	0,28
Способность проникнуть на рынок	0,04	4	4	4	0,16	0,16	0,16
Итого	1				3,76	3,7	3,14

Найдем коэффициент конкурентоспособности разработки:

К = (Кф / Кк1 + Кф / Кк2) / 2 = (3,76/3,7+3,76/3,14)/2 = 1,1

Так как найденный коэффициент больше 1, наш проект конкурентоспособен, несмотря на то что он уступает продукту к1 по показателям: использованием памяти и поддержкой продукта, он имеет преимущество в удобстве использования и надежности относительно k2.

4.2. Инициализация проекта

Группа процессов инициации состоит из процессов, которые выполняются для определения нового проекта или новой фазы существующего. В рамках процессов инициации определяются изначальные цели и содержание и фиксируются изначальные финансовые ресурсы. Определяются внутренние и внешние заинтересованные стороны проекта, которые будут взаимодействовать и влиять на общий результат научного проекта.

4.2.1. Цели и результаты проекта

В данном разделе приводится информация о заинтересованных сторонах проекта, иерархии целей проекта, а также критериях достижения целей. Под заинтересованными сторонами проекта понимаются лица или организации, которые активно участвуют в проекте или интересы которых могут быть затронуты как положительно, так и отрицательно в ходе исполнения или в результате завершения проекта. Информация по заинтересованным сторонам проекта представлена в таблице 4.2.

Таблица 4.2 – заинтересованные стороны проекта

Заинтересованные стороны проекта	Ожидания заинтересованных сторон
Сервисные компании по оказанию услуг поддержки компьютерных сетей	Разработанное программное обеспечение для выявления и блокировки нежелательного трафика, препятствующего работе сети. Выявление новой сетевой активности.
Интернет провайдеры	Разработанное программное обеспечение для интеграции с существующим оборудованием.

В таблице 4.3 представлена информация о иерархии целей проекта и критериев их достижения.

Таблица 4.3 – иерархия целей проекта и критерии их достижения

Цели проекта:	Разработка проекта программно-аппаратной для осуществления двух основных целей: Сбор статистических данных о сетевом трафике в режиме реального времени для прогнозирования сбоев; Разработка программного способа агрегации и приведения разнородных данных к единому стандарту.
Ожидаемые результаты проекта:	Обнаружения нежелательного трафика; Вывод статистических данных в виде веб-интерфейса.
Критерии приемки результата проекта:	Блокировка нежелательного трафика
Требования к результату проекта:	Требования:
	Стоимость: менее 1 млн. руб. в год
	Поддержка современных протоколов
	Формализованное описание работы всех программных модулей проекта
	Бесперебойная работа всех программных модулей проекта

4.3. Организация и планирование работы

В данном разделе составляется список проводимых работ, определяются их исполнители и продолжительность. Так как число исполнителей не превышает двух, линейный график работ является наиболее удобным и компактным способом представления данных планирования. Данные по перечню работ и степени участия представлены в таблице Таблица 4.4 Исполнителей в данном проекта двое – исполнитель (И) и научный руководитель (НР).

Таблица 4.4 – Перечень работ и продолжительность их выполнения

Этапы работы	Исполнители
1. Постановка задачи, определение целей, получение исходных данных	НР
2. Выявлений требований к программе	НР, И
3. Обзор литературы и существующих решений	НР, И
4. Календарное планирование	НР, И
5. Проектирование модели системы	И
6. Разработка алгоритма сбора данных	И
7. Разработка алгоритма обработки данных	И
8. Разработка блока агрегации статистики	И
9. Разработка веб-интерфейса	И
10. Тестирование	НР, И
11. Анализ результатов	НР, И
12. Расчет показателей ресурсоэффективности	И
13. Оценка показателей социальной ответственности	И
14. Оформление пояснительной записки	И
15. Проверка работы	НР, И

4.3.1. Продолжительность этапов работ

Расчет продолжительности этапов работ осуществляется с использованием опытно-статистического метода. Аналоговый метод здесь не применим, в силу отсутствия идентично выполняемой научно-исследовательской работы/проекта, поэтому принято решение применять экспертный способ. Для расчета ожидаемого значения продолжительности работ $t_{ож}$ применяются две оценки: t_{min} и t_{max} (метод двух оценок). Для построения таблицы продолжительности этапов работ используются следующие параметры:

- Ожидаемые (вероятные) значения продолжительности работ ($t_{ож}$):

$t_{ож} = \frac{3 \cdot t_{min} + 2 \cdot t_{max}}{5}$, где

t_{min} – минимальная трудоемкость работ, дни;

t_{max} – максимальная трудоемкость работ, дни;

Для построения линейного графика рассчитывается длительность этапов в рабочих днях, а затем осуществляется её перевод в календарные дни.

- Продолжительность выполнения каждого этапа в рабочих днях ($T_{РД}$):

$T_{РД} = t$ож, где

$t_{ож}$ – продолжительность работы, дни;

- Продолжительность выполнения этапа в календарных днях ($T_{КД}$):

$T_{КД} = T_{РД} \cdot T_{К}$, где

$T_{рд}$ – продолжительность выполнения этапа в рабочих днях;

$T_{К}$ – коэффициент календарности.

$T_{К} = \frac{T_{КАЛ}}{T_{КАЛ} - T_{ВД} - T_{ПД}}$, где

$T_{КАЛ}$ – календарные дни ($T_{КАЛ}$ =365);

$T_{ВД}$ – выходные дни ($T_{ВД} = 52$);

$Т_{ПД}$ – праздничные дни ($Т_{ПД}$ = 10)

Таким образом, для шестидневной рабочей недели получаем следующий коэффициент календарности:

$$Т_К = \frac{365}{365-52-10} = 1{,}205$$

Таблица 4.5 – Трудозатраты на выполнение проекта

Этап	Исполнители	Продолжительность работ, дни			Трудоемкость работ по исполнителям чел.-дн.			
					$T_{РД}$		$T_{КД}$	
		t_{min}	t_{max}	$t_{ож}$	НР	М	НР	М
Постановка задачи, определение целей, получение исходных данных	НР	2	4	2,8	2,80	0,00	3	0
Выявлений требований к программе	НР, И	2	3	2,4	2,40	2,40	3	3
Обзор литературы и существующих решений	НР, И	10	14	11,6	11,60	11,60	14	14
Календарное планирование	НР, И	2	4	2,8	2,80	2,80	3	3
Проектирование модели системы	И	8	10	17	0,00	17,00	0	20
Разработка алгоритма сбора данных	И	7	10	8,2	0,00	8,20	0	10

Разработка алгоритма обработки данных	И	20	25	22	0,00	22,00	0	27
Разработка блока агрегации данных	И	25	30	27	0,00	27,00	0	33
Разработка веб-интерфейса	И	100	120	108	0,00	108,00	0	130
Тестирование	НР, И	1	2	1,4	1,40	1,40	2	2
Анализ результатов	НР, И	10	15	12	12,00	12,00	14	14
Расчет экономических показателей	И	2	4	2,8	0,00	2,80	0	3
Оценка показателей безопасности жизнедеятельности	И	2	4	2,8	0,00	2,80	0	3
Оформление пояснительной записки	И	7	14	9,8	0,00	9,80	0	12
Подведение итогов	НР, И	3	5	3,8	3,80	3,80	5	5
Итого				234,4	36,80	231,60	44	279

Календарный план-график проведения работ для научного руководителя и исполнителя проекта представлена на рисунке 27 в календарных днях.

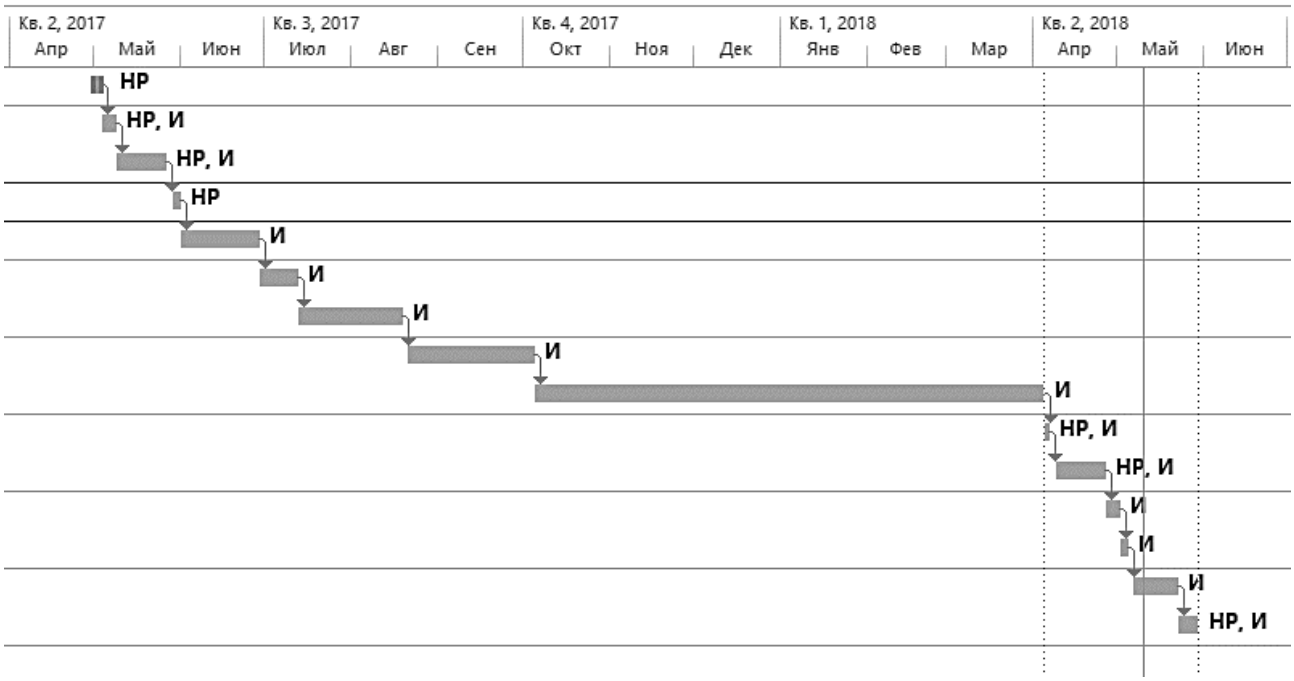


Рисунок 27. План-график проведения работ.

4.3.2. Расчёт сметы затрат на выполнение проекта

Состав затрат на научно-исследовательскую работу состоит из всех расходов, необходимых для реализации комплекса работ, составляющих содержание данного исследования. С учетом специфики проделанной работы для рассматриваемого проекта производится оценка следующих расходов:

- Материалы и покупные изделия;
- Заработная плата;
- Социальный налог
- Расходы на электроэнергию (без освещения);
- Амортизационные отчисления;
- Прочие (накладные) расходы.

Расходы по командировкам, консалтинговым услугах и привлечения помощи сторонних организаций в рамках данного проекта отсутствуют. Также не учитываются затраты на расходные материалы и канцелярию в силу отсутствия значительного вклада в расходы по проекту.

4.3.3. Расчёт заработной платы

В данном разделе расчет основной заработной платы производится на основе величины месячного оклада исполнителей, а также премии и надбавки, входящие в фонд заработной платы. Оклады участникам проекта взяты на основе отраслевой системы оплаты труда ТПУ.

Расчет затрат на заработную плату представлен в таблице 4.7. Для расчета данной таблицы использовались следующие параметры:

- Месячный оклад исполнителей проекта (МО):

В данном случае рассматриваются следующие оклады:

1) научный руководитель: должность – доцент, степень – кандидат технических наук;
2) исполнитель: учебно-вспомогательный персонал.

- Среднедневная тарифная заработная плата ($ЗП_{дн-т)}$, расчитывается по формуле:

$ЗП_{дн-т} = \frac{МО}{24,83}$, где

МО – месячный оклад исполнителя,

Значение 24,83 – количество рабочих дней при шестидневной рабочей неделе при условии 298 рабочих дней в году.

Таблица 4.7 – Затраты на заработную плату

Исполнитель	Оклад, руб./мес. (2017)	Оклад, руб./мес. (2018)	Среднедневная ставка, руб./раб.день (2017)	Среднедневная ставка, руб./раб.день (2018)	Затраты времени, раб. дни	Коэф-т	Фонд з/платы, руб.
НР	26300	33664	1059,20	1355,78	44	1,3	68682,93
И	9489	9489	382,16	382,16	279	1,3	138609
Итого:							207291,9

4.3.4. Расчёт затрат на социальный налог

Затраты на единый социальный налог (ЕСН) включают в себя следующие отчисления:

- социальное страхование;
- пенсионный фонд;
- медицинское страхование.

ЕСН составляет 30% от заработной платы по проекту:

$С_{соц} = С_{зп} \cdot 0{,}3$

Таким образом, для разрабатываемого проекта получаем:

$С_{соц} = 207291 \cdot 0{,}3 = 62187{,}6$ руб.

4.3.5. Расчёт затрат на электроэнергию

Данный вид расходов включает в себя затраты на электроэнергию, используемую оборудованием в ходе выполнения проекта и рассчитывается по формуле:

$С_{эл.об} = Р_{об} \cdot t_{об} \cdot Ц_э$, где

$Р_{об}$ – мощность, потребляемая оборудованием, кВт;

$t_{об}$ – время работы оборудования, час;

$Ц_э$ – тариф на 1кВт·час на первое полугодие 2018 года (включающий в себя: одноставочный тариф, содержание сетей, ставка на оплату технологического расхода).

Значения параметров:

1) $Ц_э$- для ТПУ составляет 14,235 руб/ кВт·час (с НДС)
2) $t_{об} = Т_{РД} \cdot K_t$, где
   - $Т_{РД}$ – трудозотраты исполнителя из расчета на 8 часовой рабочий день;
   - $K_t \leq 1$ – коэффициент использования оборудования по времени
3) $Р_{об} = Р_{ном} \cdot К_с$, где
   - $Р_{ном}$ – номинальная мощность оборудования, кВТ;

- $К_с \leq 1$ – коэффициент загрузки, зависит от средней степени использования номинальной мощности.

Расчет затрат электроэнергию представлен в таблице 4.8

Таблица 4.8 – Затраты на электроэнергию технологическую

Наименование оборудования	Время работы оборудования $t_{ОБ}$, час	Потребляемая мощность $P_{ОБ}$, кВт	Тариф $Ц_э$, руб/ кВт·час	Затраты $Э_{ОБ}$, руб.
Персональный компьютер	8*279*0,8 = 1785	0,275	14,235	6987,6
Персональный компьютер	8*44*0,8 = 282	0,25	14,235	1003,5
Сервер коллективной разработки	24*279*0,5 = 3348	0,5	14,235	23829,4
Сервер хранения данных	24*279*0,5 = 3348	0,65	14,235	30978,2
Лазерный принтер	8	0,1	14,235	11,39
Итого				62810,1

4.3.6. Расчёт прочих расходов

Величина прочих расходов составляет 10% от суммы всех предыдущих расходов и рассчитывается по формуле:

$С_{проч.} = (С_{зп} + С_{соц} + С_{эл.об.}) \cdot 0,1$

Для данного проекта получаем:

$С_{проч.} = (207291,9 + 60948,3 + 62810,1) \cdot 0,1 = 33105$ руб.

Накладные расходы составляют 80-100 % от суммы основной и дополнительной заработной платы, работников, непосредственно участвующих в выполнении темы.

$C_{накл.} = 207291,9 \cdot 0,8 = 165833,6$ руб.

4.3.7. Расчёт общий себестоимости разработки

Общая себестоимость разработки представляет суммарное значение затрат по всем статьям сметы затрат на разработку. Расчет общей себестоимости разработки представлен в таблице 4.9

Таблица 4.9 - Смета затрат на разработку проекта

Статья затрат	Условное обозначение	Сумма, руб.
Основная заработная плата	$C_{зп}$	207291,9
Отчисления в социальные фонды	$C_{соц}$	60948,3
Расходы на электроэнергию	$C_{эл.}$	62810,1
Накладные расходы	$C_{накл}$	165833,6
Прочие расходы	$C_{проч}$	33105
Итого		531228

Круговая диаграмма (рис. 28) наглядно отображает доли расходов проекта по статьям затрат.

Рисунок 28. Структура расходов проекта.

4.3.8. Оценка научно-технического уровня НИР

Научно-технический уровень характеризует влияние проекта на уровень и динамику обеспечения научно-технического прогресса в данной области. Для данной оценки используется метод балльных оценок, сущность которого заключается в присвоении каждому из показателей НИР определенного количества баллов по соответствующей для данного показателя шкале.

Научно-технический уровень определяется на основании его интегрального показателя, который выражается следующей формулой:

$I_{\text{НТУ}} = \sum_{i=1}^{3} R_i \cdot n_i$, где

$I_{\text{НТУ}}$ - интегральный индекс научно-технического уровня;

R_i – весовой коэффициент i-го признака научно-технического эффекта;

n_i – количественная оценка i-го признака научно-технического эффекта в баллах.

Таблица 4.10 – Оценка научно технического уровня НИР

Уровень новизны разработки	Характеристика уровня новизны	Баллы
Принципиально новая	Результаты исследований открывают новое направление в данной области науки и техники	8 – 10
Новая	По-новому или впервые объяснены известные факты, закономерности	5 – 7
Относительно новая	Результаты исследований систематизируют и обобщают имеющиеся сведения, определяют пути дальнейших исследований	2 – 4
Традиционная	Работа выполнена по традиционной методике, результаты которой носят информационный характер	-
Не обладающая новизной	Получен результат который ранее был известен	-

Оценка научно-технического уровня представлена в таблице 4.10

Таблица 4.11 – Оценка научно технического уровня НИР

Значимость	Фактор НТУ	Уровень фактора	Выбранный балл	Обоснование выбранного балла
0,3	Уровень новизны	Новый	7	Новый способ организации информационной инфраструктуры, новый способ предотвращения сбоев
0,2	Теоретический уровень	Разработка способа	5	Разработка нового способа агрегирования и представления информации
0,5	Возможность реализации	В течение первых лет	8	Реализуется на основе хорошо известных технологий

Таким образом, для данного проекта получаем следующий показатель научно-технического уровня:

$$I_{\text{НТУ}} = 0{,}3 \cdot 7 + 0{,}2 \cdot 6 + 0{,}5 \cdot 8 = 7{,}1$$

В таблице 4.12 приводится оценка качественных уровней НИР.

Таблица 4.12 - Качественная оценка показателей НИР

Уровень НТЭ	Показатель НТЭ
Низкий	1-4
Средний	4-7
Высокий	8-10

На основании таблицы 4.12 данная работа относится к среднему уровню научно технического эффекта. Средний уровень НТЭ обусловлен тем, что данная работа представляет новой подход к организации инструментария для борьбы со сбоями в сети.

4.4. Определение экономической эффективности исследования

С каждым годом в компьютерных сетях появляются новые типы устройств и новые протоколы передачи данных. Естественным фактом является наличие уязвимости в протоколах передачи данных, которые можно использовать в корыстных целях, что может стать причиной экономических убытков из-за простоя.

Исследование данной магистерской диссертации ведется для достижения следующей цели: создание проекта программно-аппаратного комплекса для выявления новых протоколов передачи данных, а так же в случае необходимости их блокировке. В работе используется несколько алгоритмов обработки накопленных статистических данных, а так же алгоритм голосования, что способствует обучаемости системы

4.5. Вывод

В данном разделе была произведена оценка различных экономических аспектов разработанного проекта. На основании полученных результатов проекту можно дать следующую характеристику:

- по времени разработки (11 месяцев) проект относится к краткосрочному виду проектов;
- по масштабности (с учетом себестоимости и времени разработки) проект можно отнести к категории малых проектов;
- наличие новизны метода и актуальность решаемой проблемы повышают конкурентоспособность проекта в заданной предметной области.

5. Социальная ответственность

5.1. Производственная безопасность на стадии разработки проекта

Проектная деятельность выполнялась в помещении отделения «Центрального телекоммуникационного узла» кибернетического корпуса ТПУ в кабинете 303. Помещение оснащено видео-дисплейными терминалами (ВДТ), персональными электронно-вычислительными машинами (ПЭВМ), компьютерными столами, стульями, столом для коллективной работы, огнетушителями, кондиционером, противопожарной сигнализацией и датчиками дыма.

Для обеспечения производственной безопасности необходимо проанализировать воздействия на человека вредных и опасных производственных факторов, которые могут возникать при разработке проекта.

Все производственные факторы классифицируются по группам элементов: физические, химические, биологические и психофизические. Для данной работы целесообразно рассмотреть физические и психофизические вредные и опасные факторы производства, характерные для рабочей зоны программиста, разработчика приложения, пользователя. Выявленные факторы представлены в таблице 5.1.

Таблица 5.1 – Вредные и опасные производственные факторы при выполнении работ за ПЭВМ

Источник фактора, наименование видов работ	Факторы (по ГОСТ 12.0.003-74)		Нормативные документы
	Вредные	Опасные	
1) Проектирование системы; 2) Реализация	1) Отклонение показателей микроклимата;	1) Опасность поражения электрическим	1) СанПиН 2.2.4.548-96; 2) СанПиН

системы.	2) Недостаточная освещенность рабочей зоны; 3) Умственное перенапряжение; 4) Монотонный режим работы 5) Шумовое загрязнение и вибрации	током 2) Короткое Замыкание 3) Статическое электричество	2.2.2/2.4.1340-03; 3) СП 52.13330.2011; 4) ГОСТ Р 12.1.019-2009 ССБТ; 5) СНиП 21-01-97.

5.1.1. Вредные производственные факторы

5.1.1.1. Отклонения показателей микроклимата

Показателями, характеризующими микроклимат, являются:

– температура воздуха;

– относительная влажность воздуха;

– скорость движения воздуха.

Оптимальные показатели микроклимата распространяются на всю рабочую зону, допустимые показатели устанавливаются дифференцированно для постоянных и непостоянных рабочих мест. Оптимальные и допустимые показатели температуры, относительной влажности и скорости движения воздуха в рабочей зоне производственных помещений должны соответствовать значениям, указанным в таблицах 5.2 и 5.3 [32]. Работа программиста относится к категории работ – Iа, потому что производится сидя и сопровождается незначительным физическим напряжением.

Температура воздуха в рабочей зоне, измеренная на разной высоте и в различных участках помещений, не должна выходить в течение смены за пределы оптимальных величин, указанных таблице 5.2 для отдельных категорий работ [30].

Таблица 5.2 – Оптимальные показатели температуры в рабочей зоне, согласно СанПиН 2.2.4-548-96

Период года	Категория работ	Температура, °С				
		Оптимальная	Допустимая			
			Верхняя граница		Нижняя граница	
			На рабочих местах			
			Посто-янных	Непосто-янных	Посто-янных	Непо-стоянных
Холодный	Легкая I-а	22-24	25	26	21	18
Теплый	Легкая I-а	23-25	28	30	22	20

Таблица 5.3 – Оптимальные показатели влажности и скорости движения воздуха в рабочей зоне, согласно СанПиН 2.2.4-548-96

Относительная влажность		Скорость движения, м/с	
Оптимальная	Допустимая на рабочих местах	Оптимальная, не более	Допустимая на рабочих местах постоянных и непостоянных
40-60	75	0,1	Не более 0,1
40-60	55 (при 28 ° С)	0,1	0,1-0,2

При обеспечении оптимальных и допустимых показателей микроклимата в холодный период года следует применять средства защиты рабочих мест от охлаждения от остекленных поверхностей оконных проемов, в теплый период года – от попадания прямых солнечных лучей, например, жалюзи.

Температура воздуха в аудитории, где находится рабочее место, составляет 23-24 градуса, что соответствует оптимальным показателям температуры рабочей зоны. Относительная влажность воздуха составляет 52,43%, что также соответствует оптимальным показателям влажности

воздуха в рабочей зоне. При закрытых окнах движения воздуха не ощущается. Для регулирования температурного режима в аудитории предусмотрен кондиционер.

5.1.1.2. Недостаточная освещённость рабочей зоны

Недостаточная освещенность рабочей зоны является вредным производственным фактором, возникающим при работе с ПЭВМ, уровни которого регламентируются СП 52.13330.2011.

Работа с компьютером подразумевает постоянный зрительный контакт с дисплеем ПЭВМ и занимает от 80 % рабочего времени. Недостаточность освещения снижает производительность труда, увеличивает утомляемость и количество допускаемых ошибок, а также может привести к появлению профессиональных болезней зрения.

Разряд зрительных работ программиста и оператора ПЭВМ относится к разряду III и подразряду Г (работы высокой точности). В таблице 5.5 представлены нормативные показатели искусственного освещения при работах заданной точности [33].

Таблица 5.5 – Требования к освещению помещений промышленных предприятий для операторов ПЭВМ.

Характеристика зрительной работы	Наименьший или эквивалентный размер объекта различения, мм	Разряд зрительной работы	Подразряд зрительной работы	Контраст объекта с фоном	Характеристика фона	Искусственное освещение		
						Освещённость, лк		
						При системе комбинированного освещения		При системе общего освещения
						Всего	В том числе от общего	
Высокой точности	0,264	III	Г	Средний, большой	Светлый, средний	400	200	200

Для создания и поддержания благоприятных условий освещения для операторов ПЭВМ, их рабочие места должны соответствовать санитарно-эпидемиологическим правилам СанПиН 2.2.2/2.4.1340-03. Для рассеивания естественного освещения следует использовать жалюзи на окнах рабочих помещений. В качестве источников искусственного освещения должны быть использованы люминесцентные лампы, лампы накаливания – для местного освещения [34].

В аудитории, где находится рабочее место, находятся следующие приспособления для регулирования уровня освещенности: вертикальные жалюзи на окне, 6 осветительных люминесцентных ламп на 18 Вт, размещенных на потолке, и поделенных на две рабочие зоны. Данное освещение обладает освещённостью 421 лк., чего достаточно для рабочего помещения общий площадью 20 м^2.

5.1.1.3. Умственное перенапряжение

Умственное перенапряжение вызывается большим объемом информации, которую надо анализировать, и чтобы избежать умственного перенапряжения необходимо устраивать небольшие перерывы в течение рабочего дня продолжительностью не более 5 минут.

При умственной работе, по сравнению с физической работой потребление кислорода мозгом увеличивается в 15-20 раз. Если для умственной работы требуется значительное нервно-эмоциональное напряжение, то возможны значительные изменения кровяного давления, пульса. Длительная работа этого характера может привести к заболеванию, в частности сердечно-сосудистым и некоторым другим заболеваниям [33].

Рабочее место позволяет делать перерывы в течение дня. Для этого в кибернетическом центре предусмотрены длинные коридоры, где можно погулять и сбросить умственное напряжение, а также автоматы с едой и

напитками, где можно восстановить энергетический уровень мозгового вещества для дальнейшей продуктивной работы.

5.1.1.4. Недостаточная освещённость рабочего места

При работе с ПЭВМ основным фактором, влияющим на нервную систему программиста или пользователя, является огромное количество информации, которое он должен воспринимать. Поэтому меры, позволяющие снизить воздействие этого вредного производственного фактора, которые регулируются СанПиН 2.2.2/2.4.1340-03, являются важными в работе оператора ПЭВМ. Они позволяют увеличить производительность труда и предотвратить появление профессиональных болезней.

Таблица 5.6 – Суммарное время регламентированных перерывов в зависимости от продолжительности работы, вида категории трудовой деятельности с ПЭВМ

Категория работы с ПЭВМ	Уровень нагрузки за рабочую смену при видах работ с ПЭВМ			Суммарное время регламентированных перерывов, мин.	
	группа А, количество знаков	группа Б, количество знаков	группа В, ч	при 8-часовой смене	при 12-часовой смене
I	до 20 000	до 15 000	до 2	50	80
II	до 40 000	до 30 000	до 4	70	110
III	до 60 000	до 40 000	до 6	90	140

Для предупреждения преждевременной утомляемости пользователей ПЭВМ организована рабочая смена путем чередования работ с использованием ПЭВМ и без него. В случаях, когда характер работы требует постоянного взаимодействия с компьютером, организованы перерывы на 10–15 мин. через каждые 45–60 мин. работы. При высоком уровне

напряженности работы организована психологическая разгрузка в специально оборудованных помещениях [34].

5.1.2. Опасные производственные факторы

5.1.2.1. Опасность поражения электрическим током, статическим электричеством и коротким замыканием

Поражение электрическим током является опасным производственным фактором и, поскольку программист имеет дело с электрооборудованием, то вопросам электробезопасности на его рабочем месте должно уделяться особое внимание. Нормы электробезопасности на рабочем месте регламентируются СанПиН 2.2.2/2.4.1340-03, вопросы требований к защите от поражения электрическим током освещены в ГОСТ Р 12.1.019-2009 ССБТ.

Основным организационным мероприятием по обеспечению безопасности является инструктаж и обучение безопасным методам труда, а также проверка знаний правил безопасности и инструкций в соответствии с занимаемой должностью применительно к выполняемой работе.

К мероприятиям по предотвращению возможности поражения электрическим током относятся:

– с целью защиты от поражения электрическим током, возникающим между корпусом приборов и инструментом при пробое сетевого напряжения на корпус, корпуса приборов и инструментов должны быть заземлены;

– при включенном сетевом напряжении работы на задней панели корпуса приборов должны быть запрещены;

– все работы по устранению неисправностей должен производить квалифицированный персонал;

– необходимо постоянно следить за исправностью электропроводки;

[3, 4].

5.2. Экологическая безопасность

5.2.1. Влияние объекта исследования на окружающую среду

В ходе выполнения ВКР и дальнейшем использовании алгоритмов отсутствуют выбросы каких-либо вредных веществ в атмосферу и гидросферу, следовательно, загрязнение воздуха и воды не происходит.

Однако, люминесцентные лампы, применяющиеся для искусственного освещения рабочих мест, требуют особой утилизации, т.к. в них присутствует от 10 до 70 мг ртути, которая относится к чрезвычайно-опасным химическим веществам и может стать причиной отравления живых существ, а также загрязнения атмосферы, гидросферы и литосферы. Сроки службы таких ламп составляют около 5-ти лет, после чего их необходимо сдавать на переработку в специальных пунктах приема.

5.2.2. Мероприятия по защите окружающей среды

Для уменьшения вредного влияния на литосферу необходимо производить сортировку отходов и обращаться в службы по утилизации для дальнейшей переработки или захоронения. [36]

Такие лампы нельзя выкидывать в мусоропровод или уличные контейнеры, а нужно отнести в свою районную Дирекцию единичного заказчика (ДЕЗ) или Ремонтно-эксплуатационное управление (РЭУ), где есть специальные контейнеры. Там они принимаются бесплатно, основанием должна служить утилизация в соответствии с Управлением Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Томской области. Пункты приёма отработавших свой срок люминесцентных ламп по городам можно найти в интернете. [37]

Переработка макулатуры представляет собой многоэтапный процесс, цель которого заключается в восстановлении бумажного волокна и, зачастую, других компонентов бумаги (таких как минеральные наполнители) и использование их в качестве сырья для производства новой бумаги.

5.3. Безопасность в чрезвычайных ситуациях

5.3.1. Типичные чрезвычайные ситуации

Наиболее вероятная чрезвычайная ситуация, которая может возникнуть при работе с ПЭВМ – пожар, так как в современных ЭВМ очень высокая плотность размещения элементов электронных схем. В непосредственной близости друг от друга располагаются соединительные провода и кабели, при протекании по ним электрического тока выделяется значительное количество теплоты, при этом возможно оплавление изоляции и возникновение возгорания.

Возникновение пожара является опасным производственным фактором, т.к. пожар на предприятии наносит большой материальный ущерб, а также часто сопровождается травмами и несчастными случаями. Регулирование пожаробезопасности производится СНиП 21-01-97.

Возможные виды источников воспламенения:

- искра при разряде статического электричества;
- искры от электрооборудования;
- искры от удара и трения;
- открытое пламя [38].

Для профилактики организации действий при пожаре должен проводиться следующий комплекс организационных мер:

- должны обеспечиваться регулярные проверки пожарной сигнализации, первичных средств пожаротушения;
- должен проводиться инструктаж и тренировки по действиям в случае пожара;
- не должны загромождаться или блокироваться пожарные выходы;
- во всех служебных помещениях должны быть установлены «Планы эвакуации людей при пожаре и других ЧС», регламентирующие действия персонала при возникновении пожара.

Для предотвращения пожара помещение с ПЭВМ должно быть оборудовано первичными средствами пожаротушения: углекислотными огнетушителями типа ОУ-2 или ОУ-5; пожарной сигнализацией, а также, в некоторых случаях, автоматической установкой объемного газового пожаротушения [38].

5.3.2. Действия в результате возникновения чрезвычайной ситуации и мер по ликвидации её последствий

При работе компьютерной техники выделяется много тепла, что может привести к пожароопасной ситуации. Источниками зажигания так же могут служить приборы, применяемые для технического обслуживания, устройства электропитания, кондиционеры воздуха. В связи с этим, участки, на которых используется компьютерная техника, по пожарной опасности относятся к категории пожароопасных «В». Меры, соблюдение которых поможет исключить с большой вероятностью возможность возникновения пожара:

– для понижения воспламеняемости и способности распространять пламя кабели покрывают огнезащитным покрытием;

– при ремонтно-профилактических работах строго соблюдаются правила пожарной безопасности;

– помещения, в которых должны располагаться ПЭВМ проектируют I или II степени огнестойкости;

– каждое из помещений, где производится эксплуатация устройств ПЭВМ, должно быть оборудовано первичными средствами пожаротушения и обеспечено инструкциями по их применению. В качестве средств пожаротушения разрешается использование углекислотного огнетушителя типа ОУ-2, ОУ-5, а также порошковый тип. Применение пенных огнетушителей не допускается, так как жидкость пропускает ток;

– устройства ПЭВМ необходимо устанавливать вдали отопительных и нагревательных приборов (расстояние не менее 1 м и в местах, где не затруднена их вентиляция и нет прямых солнечных лучей);

– разрабатываются организационные меры по обучению персонала навыкам ликвидации пожара имеющимися в наличии средствами тушения пожара до прибытия пожарного подразделения [39].

При пожаре люди должны покинуть помещение в течение минимального времени.

В помещениях с компьютерной техникой, недопустимо применение воды и пены ввиду опасности повреждения или полного выхода из строя дорогостоящего электронного оборудования.

5.4. Правовые и организационные вопросы обеспечения безопасности

5.4.1. Специальные правовые нормы трудового законодательства

Регулирование отношений между работником и работодателем, касающихся оплаты труда, трудового распорядка, особенности регулирования труда женщин, детей, людей с ограниченными способностями и проч., осуществляется законодательством РФ, а именно трудовым кодексом РФ.

Нормальная продолжительность рабочего времени не может превышать 40 часов в неделю.

Порядок исчисления нормы рабочего времени на определенные календарные периоды (месяц, квартал, год) в зависимости от установленной продолжительности рабочего времени в неделю определяется федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере труда.

Продолжительность ежедневной работы (смены) не может превышать:

– При 36-часовой рабочей неделе – 8 часов;

– При 30-часовой рабочей неделе и менее – 6 часов.

В течение рабочего дня (смены) работнику должен быть предоставлен перерыв для отдыха и питания. Время предоставления перерыва и его конкретная продолжительность устанавливаются правилами внутреннего трудового распорядка или по соглашению между работником и работодателем.

Всем работникам предоставляются выходные дни (еженедельный непрерывный отдых).

Организация-работодатель выплачивает заработную плату работникам. Возможно удержание заработной платы только в случаях, установленных ТК РФ ст. 137. В случае задержки заработной платы более чем на 15 дней, работник имеет право приостановить работу, письменно уведомив работодателя.

Законодательством РФ запрещена дискриминация по любым признакам и принудительный труд [40].

5.4.2. Организованные мероприятия при компоновке рабочей зоны

Если пользователь постоянно загружен работой с ЭВМ, приемлемой является поза сидя. В положении сидя основная нагрузка падает на мышцы, поддерживающие позвоночный столб и голову. В связи с этим при длительном сидении время от времени необходимо сменять фиксированные рабочие позы.

Исходя из общих принципов организации рабочего места, в нормативно-методических документах сформулированы требования к конструкции рабочего места.

Основными элементами рабочего места программиста являются: рабочий стол, рабочий стул (кресло), дисплей, клавиатура, мышь; вспомогательными - пюпитр, подставка для ног [41].

Взаимное расположение элементов рабочего места должно обеспечивать возможность осуществления всех необходимых движений и перемещений для эксплуатации и технического обслуживания оборудования [42].

Рабочие места с ЭВМ должны располагаться па расстоянии не менее 1,5 м от стены с оконными проемами, от других стен – на расстоянии 1 м, между собой – на расстоянии не менее 1,5 м (рис. 29) [41, 43].

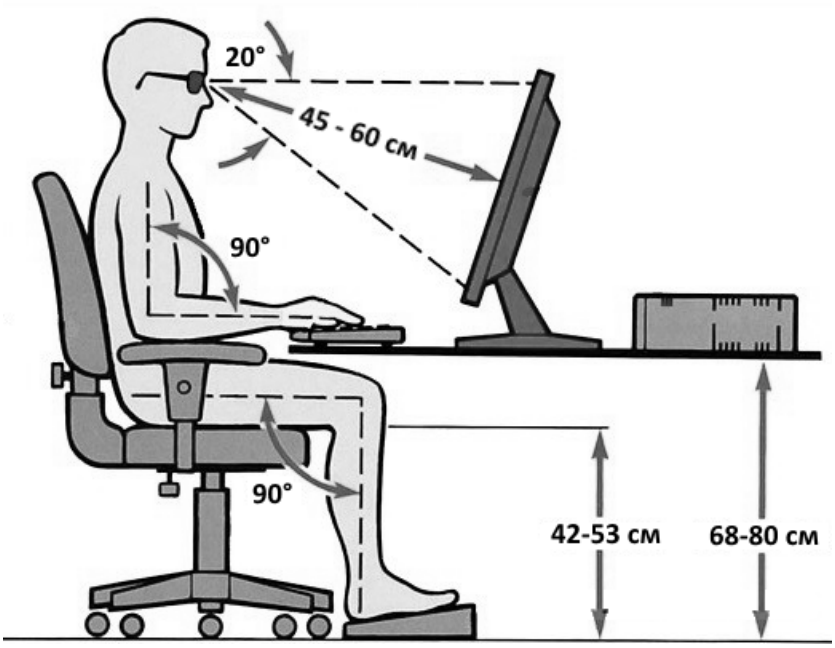


Рисунок 29. Организация рабочего места.

5.5. Вывод

Выявлены необходимые условия для безопасной работы человека в помещение оборудованном электроприборами, в том числе ПЭВМ. Соблюдение норм условий труда гарантирует безопасную работу и снижение влияние вредных факторов до безопасного для человека уровня.

Список используемых источников

1. Развитие цифровых технологий радикально меняет модель глобальных инвестиционных потоков [Электронный ресурс]. URL: http://www.finmarket.ru/database/news/4545545. Дата обращения 30.05.2018
2. Тенденции и перспективы рынка мобильных приложений: поговорим о деньгах [Электронный ресурс]. https://habr.com/company/alconost/blog/323020/. Дата обращения 30.05.2018
3. Удалённые сетевые атаки [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Удалённые_сетевые_атаки. Дата обращения 30.05.2018
4. Безопасность канального уровня [Электронный ресурс]. URL: http://xgu.ru/wiki/Безопасность_канального_уровня. Дата обращения 30.05.2018
5. MAC-spoofing [Электронный ресурс]. URL: http://xgu.ru/wiki/MAC-spoofing. Дата обращения 30.05.2018
6. ARP-spoofing [Электронный ресурс]. URL: http://xgu.ru/wiki/ARP-spoofing. Дата обращения 30.05.2018
7. DNS-spoofing [Электронный ресурс]. URL: http://xgu.ru/wiki/DNS-spoofing. Дата обращения 30.05.2018
8. ICMP [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/ICMP. Дата обращения 30.05.2018
9. Захват пакетов при помощи библиотеки libpcap [Электронный ресурс]. URL: http://rus-linux.net/MyLDP/algol/libpcap.html. Дата обращения 30.05.2018
10. Лучшие инструменты пен-тестера: сниферы и работа с пакетами [Электронный ресурс]. URL: https://xakep.ru/2009/07/02/48736/. Дата обращения 30.05.2018

11. Анализ сетевого трафика на сервере при помощи tshark [Электронный ресурс]. URL: https://blog.selectel.ru/analiz-setevogo-trafika-na-servere-pri-pomoshhi-tshark. Дата обращения 30.05.2018
12. SNMP в CISCO [Электронный ресурс]. URL: http://xgu.ru/wiki/SNMP_в_Cisco. Дата обращения 30.05.2018
13. SNMP [Электронный ресурс]. URL: http://xgu.ru/wiki/SNMP. Дата обращения 30.05.2018
14. ARP [Электронный ресурс]. URL: http://xgu.ru/wiki/ARP. Дата обращения 30.05.2018
15. Протокол UDP [Электронный ресурс]. URL: https://www.opennet.ru/docs/RUS/inet_book/4/44/udp_442.html. Дата обращения 30.05.2018
16. Broadcast на порт 7533 [Электронный ресурс]. URL: http://sysadmins.ru/post9605507.html. Дата обращения 30.05.2018
17. ICMPv6 [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/ICMPv6. Дата обращения 30.05.2018
18. SYN-флуд [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/SYN-флуд. обращения 30.05.2018
19. TCP Retransmissions – что это и как их анализировать с помощью Wireshark? [Электронный ресурс]. URL: https://networkguru.ru/tcp-retransmission-wireshark-chto-eto. Дата обращения 30.05.2018
20. NetBIOS [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/NetBIOS. Дата обращения 30.05.2018
21. NetBIOS протокол подвержен spoofing'y [Электронный ресурс]. URL: https://m.habr.com/post/82085/. Дата обращения 30.05.2018
22. Easy Hack: Хакерские секреты простых вещей [Электронный ресурс]. URL: https://xakep.ru/2013/12/11/easy-hack-173. Дата обращения 30.05.2018

23. STP [Электронный ресурс]. URL: http://xgu.ru/wiki/STP. Дата обращения 30.05.2018
24. Simple Service Discovery Protocol [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Simple_Service_Discovery_Protocol. Дата обращения 30.05.2018
25. Уязвимость в Multicast DNS провоцирует DDoS с плечом [Электронный ресурс]. URL: https://threatpost.ru/ujazvimost_multicast_dns_provotsiruet_ddos_s_plechom/7444/. Дата обращения 30.05.2018
26. DHCPv6 [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/DHCPv6. Дата обращения 30.05.2018
27. IGMP [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/IGMP. Дата обращения 30.05.2018
28. Dropbox: LAN sync protocol [Электронный ресурс]. URL: https://geeklogsblog.wordpress.com/2011/09/10/dropbox-lan-sync-protocol. Дата обращения 30.05.2018
29. Microsoft Windows Browser Protocol [Электронный ресурс]. URL: https://www.wireshark.org/docs/dfref/b/browser.html. Дата обращения 30.05.2018
30. PIM-SM [Электронный ресурс]. URL: http://xgu.ru/wiki/PIM-SM. Дата обращения 30.05.2018
31. Loop protocol [Электронный ресурс]. URL: https://supportforums.cisco.com/t5/lan-switching-and-routing/loop-protocol/td-p/1713443. Дата обращения 30.05.2018
32. СанПиН 2.2.4.548-96 «Гигиенические требования к микроклимату производственных помещений. Санитарные правила и нормы» [Электронный ресурс]. URL: https://ohranatruda.ru/ot_biblio/normativ/data_normativ/5/5225/, свободный. – Загл. с экрана. – Дата обращения: 06.03.2018 г.

33. Попов В.М. Психология безопасности профессиональной деятельности: учебное пособие / В. М. Попов; Новосибирский государственный технический университет. – Новосибирск: Изд-во Новосибирского государственного технического университета, 1996 г. – 155 с.
34. СанПиН 2.2.2/2.4.1340-03. Санитарно-эпидемиологические правила и нормы. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы // Электронный фонд правовой и нормативно-технической документации. [Электронный ресурс]. URL: http://docs.cntd.ru/document/901865498, свободный. – Загл. с экрана. – Дата обращения: 06.03.2018 г.
35. ГОСТ Р 12.1.019-2009 ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты // Электронный фонд правовой и нормативно- технической документации. [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200080203, свободный. – Загл. с экрана. – Дата обращения: 06.03.2018 г.
36. Постановление Правительства РФ от 03.09.2010 N 681 (ред. от 01.10.2013) "Об утверждении Правил обращения с отходами производства и потребления в части осветительных устройств, электрических ламп, ненадлежащие сбор, накопление, использование, обезвреживание, транспортирование и размещение которых может повлечь причинение вреда жизни, здоровью граждан, вреда животным, растениям и окружающей среде // Государственная система правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102141053, свободный. – Загл. с экрана. – Дата обращения: 06.03.2018 г.

37. Как утилизировать люминесцентную лампу? | Экологические проблемы и их решения [Электронный ресурс]. URL: http://eco63.ru/lampalum.html, свободный. – Загл. с экрана. – Дата обращения: 06.03.2018 г.
38. Чрезвычайные ситуации при работе с ПЭВМ // Студопедия — Ваша школопедия. [Электронный ресурс]. URL: https://studopedia.ru/8_107307_osveshchenie-pomeshcheniy-vichislitelnih-tsentrov.html, свободный. – Загл. с экрана. – Дата обращения: 06.03.2018 г.
39. Долин П.А. Справочник по технике безопасности. М.: Энергоатомиздат, 1984 г. – 824 с.
40. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 3.07.2016) // Электронный фонд правовой и нормативно-технической документации. [Электронный ресурс]. URL: http://docs.cntd.ru/document/901807664, свободный. – Загл. с экрана. – Дата обращения: 06.03.2018 г.
41. ГОСТ Р 50923-96 Дисплеи. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения // Электронный фонд правовой и нормативно-технической документации. [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200025975, свободный. – Загл. с экрана. – Дата обращения: 06.03.2018 г.
42. ГОСТ 22269-76 Система "Человек-машина". Рабочее место оператора. Взаимное расположение элементов рабочего места. Общие эргономические требования // Электронный фонд правовой и нормативно-технической документации. [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200012834, свободный. – Загл. с экрана. – Дата обращения: 06.03.2018 г.

43. ГОСТ 12.2.032-78 ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования // Электронный фонд правовой и нормативно-технической документации. [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200003913, свободный. – Загл. с экрана. – Дата обращения: 06.03.2018 г.

Приложение А.

Протокол	Перехвачено пакетов
ARP	4084826
UDP	1452997
TCP	674985
ICMPv6	576147
NBNS	402383
LLMNR	252027
MDNS	192013
STP	150698
SSDP	144371
DHCPv6	83446
IGMPv2	56117
DB-LSP-DIS	54702
BROWSER	38799
Auto-RP	30550
LOOP	30309
Другие	91674
ADwin	27762
RakNet	11658
PIMv2	10270
ICMP	7707
QUIC	6344
HIP	6302
SIP	5113
NTP	3993
TLSv1.2	3432
DNS	1600
STUN	1161
BJNP	1104
CAT-TP	766
DHCP	407
ISAKMP	286
SSL	276
CLDAP	270
QUAKE3	266
DTLSv1.2	258
Chargen	237
PPP	175
LLC	137
NAT-PMP	129
SMB	93
DIS	90
HTTP	83
TFTP	82
ENIP	73
OpenVPN	70
CN/IP	70
IPMI	67
TLSv1	59
MPTCP	56
XDMCP	55
BACnet-APD	52
0x0000	43
WSP	42
PKTC	35
UAUDP	33
SIP/SDP	32
SliMP3	30
TPCP	29
GTP	29
RTPproxy	29
ANSI	28
GPRS-NS	28
RIPv1	25
SEBEK	24
Syslog	24
Vuze-DHT	21
RDT	20
IAPP	19
QUAKEWORLD	19
LTP	18
MiNT	18
ESP	18
PPTP	17
CoAP	16
ECHO	15
H.225.0	15
SCTP	15
RTCP	14
BitTorrent	14
ASAP	14

QUAKE	14
ENRP	13
KRB5	13
Geneve	13
HART_IP	13
0x9d38	12
BAT_GW	12
LWAPP	11
IPVS	11
MSproxy	10
BFD	10
A21	10
DTLS	10
DAYTIME	9
WTLS+WSP	9
DMP	9
HiQnet	8
KNET	8
WTLS+WTP+W	8
TPKT	8
QUAKE2	7
SAP	7
KINK	7
EGD	7
BAT_VIS	6
0x0de5	6
802.11	6
Elasticsea	5
KDP	5
H.248	5
XMPP	5
DNPv100	5
0x21ac	5
0x7cec	5
CAPWAP-Con	5
SCoP	5
VITA	5
0x5ab4	4
TS2	4
HCrt	4
MIH	4
IPv6	4
ADP	4
ECMP	4

LISP	4
KNXnetIP	4
ICP	4
SABP	4
SSLv2	4
TiVoConnec	4
Who	3
RSVP	3
IO-RAW	3
60	3
ALLJOYN-NS	3
TZSP	3
ALC	3
DPNET	3
AX4000	3
WLCCP	3
CLASSIC-ST	3
L2TP	2
collectd	2
85.143.79.	2
0xf2c9	2
DNPv65	2
MIPv6	2
BOOTP	2
CAPWAP-Dat	2
TLSv1.1	2
TETRA	2
ATH	2
ULP	2
HTTP/XML	2
ASTERIX	2
0xf878	1
GTPv2	1
0x10a3	1
AR41aa:6ed	1
MANOLITO	1
0xd53d	1
0xedff	1
LL	1
Tell	1
0xd1d4	1
fe80::b41f	1
RX	1
AYIYA	1

SNMP	1
PTR	1
0xb424	1
0xfe2c	1
Solicit	1
0x0700	1
145	1
DCC	1
query	1
VxLAN	1
0xba80	1
SMPP	1
IAX2	1
0x4e72	1
Ethernet	1
27885	1
0xbf70	1
TC	1
ALLJOYN-AR	1
0xf5f8	1
Solicitati	1
OCSP	1

cache	1
0x4998	1
95	1
Bitcoin	1
OMRON	1
question	1
0xf40c	1
RETRACKER<	1
POWERLINK/	1
0x8854	1
54915	1
WTP+WSP	1
X11	1
BAT_BATMAN	1
NBSS	1
0xdd3c	1
0x4db9	1
MPLS	1
305	1
DCP-AF	1
RRoCE	1

Приложение Б.

Источник	Получатель	Протокол	Пояснение	Пакетов
85.143.78.15	255.255.255.255	UDP	54376 → 7533 Len=34	1382413
5.53.113.210	85.143.78.177	TCP	55501 → 44525 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1	685687
85.143.78.14	85.143.78.255	NBNS	Name query NB XRXD3B039.DLINK<00>	395524
85.143.78.164	224.0.0.251	MDNS	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _acestreamcast._tcp.local, "QM" question	131671
85.143.78.10	224.0.0.252	LLMNR	Standard query 0x6b67 ANY DESKTOP-8A352TT	123959
85.143.78.31	255.255.255.255	DB-LSP-DIS	Dropbox LAN sync Discovery Protocol	55194
85.143.78.69	85.143.78.255	BROWSER	Host Announcement KEENETIC_GIGA, Server, Print Queue Server, NT Server	38531
85.143.78.13	255.255.255.255	ADwin	146	27762
85.143.79.1	224.0.0.13	PIMv2	Hello	10434
85.143.79.1	224.0.0.1	IGMPv2	Membership Query, general	10188
46.234.125.89	85.143.78.48	ICMP	Echo (ping) request id=0x2649, seq=50138/56003, ttl=50	7741
185.200.118.53	85.143.78.97	QUIC	Payload (Encrypted)[Malformed Packet]	6357
196.52.43.59	85.143.78.100	SIP	Request: OPTIONS sip:HzanusfH@85.143.78.100 |	5193
85.143.79.1	255.255.255.255	NTP	NTP Version 3, broadcast	4069
173.194.222.188	85.143.78.97	TLSv1.2	Application Data	3425
123.249.3.162	85.143.78.151	DNS	Standard query 0x4b05 A www.google.it	1640
184.105.139.81	85.143.78.148	SSDP	M-SEARCH * HTTP/1.1	1638
37.21.113.89	85.143.78.151	STUN	Binding Request user: hfLx:tyKc	1161
109.252.91.228	85.143.78.177	BJNP	Unknown type (8): Unknown code (153)	1037
37.203.203.250	85.143.78.177	CAT-TP	39878 > 53496 [ACK PDU] Flags=0x40 Ack=0 Seq=0 WSize=0	768
184.105.247.224	85.143.79.63	CLDAP	searchRequest(1) "<ROOT>" baseObject	292
46.72.103.96	85.143.78.6	ISAKMP	Unknown 243	286
5.189.183.129	85.143.78.114	QUAKE3	Game Server to Client	281
213.180.204.127	85.143.78.151	SSL	Continuation Data	274
37.21.113.89	85.143.78.151	DTLSv1.2	Application Data	254
125.212.217.214	85.143.78.13	Chargen	Chargen	243
31.24.24.1	85.143.79.88	PPP	62 Echo Request	175
184.105.247.235	85.143.78.40	NAT-PMP	External Address Request	129
85.143.78.214	85.143.78.255	SMB	632 Write Mail Slot	94
185.206.209.162	85.143.78.202	DIS	PDUType: 58 Data Query-R[Malformed Packet]	90
77.234.45.60	85.143.78.174	HTTP	HTTP/1.1 200 OK (application/octet-stream)	83
184.105.139.114	85.143.78.192	TFTP	Read Request, File: a.pdf, Transfer type: octet	82
80.82.77.139	85.143.78.53	ENIP	List Identity (Req)	75
188.13.16.236	85.143.78.32	CN/IP	Priority: normal Type: Unknown[Malformed Packet]	70
154.45.216.222	85.143.78.100	OpenVPN	MessageType: Unknown Messagetype[Malformed Packet]	70
184.105.247.230	85.143.78.99	IPMI	Session ID 0x0	68
213.180.204.179	85.143.78.151	TLSv1	Application Data	59
166.111.8.246	85.143.78.27	MPTCP	56280 → 53 [SYN] Seq=0 Win=65535 Len=0 SACK_PERM=1 TSval=4294967295 TSecr=16843009 WS=2 TFO=R	59
85.143.78.130	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x248c952d	58
184.105.139.93	85.143.78.67	XDMCP	Query	55

125.64.94.208	85.143.79.63	BACnet-APD	Confirmed-REQ readProperty[1] device,4194303 object-identifier	52
118.166.168.4	85.143.78.234	WSP	WSP Unknown PDU type (0x31) (0x31)	42
31.162.5.220	85.143.78.171	PKTC	MTA FQDN Reply	36
46.242.11.209	85.143.78.138	UAUDP	unknown (0x64)	33
185.40.4.33	85.143.78.2	SIP/SDP	Request: INVITE sip:0014694159341@85.143.78.2 |	32
46.47.46.239	85.143.78.149	LLC	I P, N(R)=48, N(S)=29; DSAP 0x64 Individual, SSAP 0x30 Response	32
190.192.250.205	85.143.78.12	SliMP3	Discovery Request, Device ID: 49. Firmware: 3.10	32
80.82.77.139	85.143.78.56	GTP	Echo request	30
162.253.131.178	85.143.78.48	RTPproxy		29
80.246.81.165	85.143.78.132	TPCP		29
92.125.138.238	85.143.78.138	GPRS-NS	Unknown PDU type	28
113.228.28.177	85.143.78.6	ANSI	157 1153 → 3756 Len=115[Malformed Packet]	28
93.174.95.106	85.143.78.171	RIPv1	Request	25
45.58.114.162	85.143.78.15	Syslog	OPTIONS sip:100@85.143.78.15 SIP/2.0\r\nVia: SIP/2.0/UDP 127.0.0.1:5100;branch=z9hG4bK-2172343486;rport\r\nContent-Length: 0\r\nFrom: "sipvicious"<sip:100@1.1.1.1>;tag=353538663465306631303230320134323731363138343637\r\nAccept: application/sdp\r\nUser-Agent: friendly-scanner\r\nTo: "sipvicious"<sip:100@1.1.1.1>\r\nContact: sip:100@127.0.0.1:5100\r\nCSeq: 1 OPTIONS\r\nCall-ID: 106743907320931445255758 1\r\nMax-Forwards: 70\r\n\r\n	24
183.89.51.139	85.143.78.171	SEBEK	SEBEK -	24
212.112.119.232	85.143.78.6	Vuze-DHT	Action: Unknown	21
88.231.222.157	85.143.78.16	RDT	DATA: stream-id=18 asm-rule=33 seq=12602 ts=1681013353	20
178.210.25.100	85.143.78.31	QUAKEWORLD	Server to Client Game	19
46.39.48.75	85.143.78.171	ESP	ESP (SPI=0x4100bf65)	19
91.227.50.110	85.143.78.114	IAPP	Unknown Packet(49) (version=100)[Malformed Packet]	18
222.162.70.178	85.143.78.234	LTP	157 Green data[Malformed Packet]	18
95.32.12.38	85.143.78.171	MiNT	Type 0x14fa	18
31.24.24.1	85.143.79.88	PPTP	Call-Disconnect-Notify	17
80.82.77.33	85.143.78.119	CoAP	CON, MID:45066, GET, End of Block #0, /.well-known/core	17
82.221.105.6	85.143.78.99	ECHO	Request	16
186.211.69.70	85.143.78.114	H.225.0	1718 → 32393 Len=92[UNKNOWN PER: unknown extension root index in choice][Malformed Packet]	15
180.33.79.184	85.143.78.12	SCTP	RESERVED [Malformed Packet]	15
213.196.52.68	85.143.78.45	RTCP	Sender Report Port Mapping	14
113.15.120.54	85.143.78.48	QUAKE	seq 0x64323a69	14
171.33.252.136	85.143.78.30	ASAP	Unknown ASAP type [Packet size limited during capture]	14
31.207.195.76	85.143.78.171	BitTorrent	Extended	14
89.248.172.16	85.143.78.174	KRB5	AS-REQ	14
217.132.169.172	85.143.78.65	ENRP	Unknown ENRP Type	13
93.174.95.106	85.143.78.130	HART_IP	Session Initiate Request, Sequence Number 1	13
123.162.168.134	85.143.78.149	Geneve	Encapsulated 0x3a61 (unknown)[Malformed Packet]	13
37.201.225.249	85.143.78.106	BAT_GW	Type=Unknown (0x64) IP: 49.58.97.100	12
85.66.140.57	85.143.78.238	LWAPP	CNTL Bad Type: 0x3a	11
101.87.87.161	85.143.78.234	IPVS	[Malformed Packet]	11
91.240.208.9	85.143.78.33	A21	Unknown[Malformed Packet]	10
90.154.70.90	85.143.78.192	BFD	148 Diag: Forwarding Plane Reset, State: AdminDown, Flags: 0x30	10
31.25.27.199	85.143.78.6	MSproxy	Server message: Unknown	10

164.52.24.181	85.143.78.92	DAYTIME	DAYTIME Request	9
83.102.219.5	85.143.78.3	WTLS+WSP	WTLS	9
114.237.120.78	85.143.78.234	DTLS	Continuation Data	9
92.43.188.94	85.143.78.171	DMP	Unsupported Version: 5	9
62.94.49.1	85.143.78.102	WTLS+WTP+W	WTLS	8
188.19.174.181	85.143.78.33	KNET	Packet ID 953444: AppData (100)[Malformed Packet]	8
123.21.194.62	85.143.78.6	HiQnet	Msg: Unknown (0x4c55), Src: 14953.100.50.48.58, Dst: 14458.136.91.35.203[Packet size limited during capture]	8
125.231.17.190	85.143.78.17	TPKT	Continuation	8
185.172.128.151	85.143.78.171	0x0000		8
180.102.206.182	85.143.78.17	EGD	Data Msg: ExchangeID=0x3A303264, RequestID=24890	7
5.189.183.129	85.143.78.48	QUAKE2	Server to Client Game	7
89.222.181.88	85.143.78.234	KINK	unknown[Malformed Packet]	7
174.62.117.44	85.143.78.114	SAP	Deletion (v3)[Malformed Packet]	7
73.170.187.29	85.143.78.149	RakNet	Open Connection Request 1[Malformed Packet]	7
191.102.236.43	85.143.78.192	BAT_VIS	Unsupported Version 100	6
62.192.250.36	85.143.78.33	802.11	VHT NDP Announcement[Malformed Packet]	6
58.38.118.218	85.143.78.48	H.248	2945 → 61381 Len=106	5
188.163.88.4	85.143.78.6	VITA	146 Reserved packet type (0x06)[Malformed Packet]	5
150.117.98.15	85.143.78.12	KDP	SDDP message	5
82.145.215.38	85.143.78.47	XMPP	Whitespace Keepalive	5
36.251.192.108	85.143.78.104	CAPWAP-Con	CAPWAP-Control[Malformed Packet]	5
155.4.131.74	85.143.78.32	DNPv100	5567 → 61511 Len=106	5
60.222.106.162	85.143.78.6	SCoP		5
5.158.98.95	85.143.78.27	Elasticsea	Zen Ping: cluster=0:	5
85.143.78.11	255.255.255.255	TiVoConnec	Discovery Beacon Zona on DESKTOP-2D3P0TL (F4KUIFTZETIC2)	4
120.39.46.70	85.143.78.238	LISP	Map-Referral	4
139.5.231.7	85.143.78.192	SABP	3452 → 32093 Len=103[UNKNOWN PER: unknown extension root index in choice][Malformed Packet]	4
160.86.194.145	85.143.78.11	ICP	Opcode: Unknown (100), Req Nr: 1681013353[Malformed Packet]	4
118.160.77.192	85.143.78.17	ADP		4
114.24.222.191	85.143.78.177	TS2	Type: Unknown (0x613a), Class: Unknown (0x3164)	4
213.118.234.211	85.143.78.138	HCrt	Type: Read, Tag: 0x4, ADL: 314	4
116.252.45.48	85.143.78.234	MIH	Command Service Response "Unknown"	4
89.151.187.104	85.143.78.114	ECMP	Unknown Type:0x32, Request. Transaction ID: 58	4
213.180.204.179	85.143.78.151	SSLv2	Encrypted Data, Encrypted Data	4
213.156.17.14	85.143.78.244	KNXnetIP	CONNECT_REQUEST 3671 > 3671	4
91.237.233.199	85.143.78.139	TZSP	Unknown (61684)[Malformed Packet]	3
31.200.239.199	85.143.78.104	AX4000	Chss:49 Prt:100 Idx:2657 Seq:0xde433a30 TS:8454,413380[msec]	3
177.75.157.49	85.143.78.132	ALLJOYN-NS	VERSION 4 (UNSUPPORTED) ISAT WHOHAS[Malformed Packet]	3
121.1.204.183	85.143.78.114	ALC	Version: 6 (not supported)	3
85.143.78.52	85.143.78.255	SNMP	get-request 1.3.6.1.2.1.1.1.0	3
122.228.156.3	85.143.78.16	RSVP	Unknown (49). [Malformed Packet]	3
185.172.128.151	85.143.78.171	IO-RAW	Raw IO Data	3
176.195.148.233	85.143.78.6	DPNET	DPNET CFrame - Unknown Control (obsolete or malformed?)	3

37.21.190.207	85.143.78.105	CLASSIC-ST	Message: Binding Request	3
91.105.116.166	85.143.78.175	collectd	[Malformed Packet]	2
74.125.232.208	85.143.78.68	TLSv1.1	Server Hello, Change Cipher Spec, Encrypted Handshake Message	2
85.143.78.65	85.143.78.125	HTTP/XML	POST /d6a44ffb-432b-434b-817d-1de6b3840ced/ HTTP/1.1	2
123.231.107.198	85.143.78.104	CAPWAP-Dat	CAPWAP-Data[Malformed Packet]	2
60.242.166.100	85.143.78.11	TETRA	Unknown command: 100	2
1.175.178.253	85.143.78.32	ASTERIX		2
177.55.58.211	85.143.78.146	MIPv6	Unknown Mobility Header (58)[Malformed Packet]	2
95.32.138.81	85.143.78.6	DNPv65	3567 → 3756 Len=20	2
37.205.55.135	85.143.78.33	ATH		2
212.96.82.228	85.143.78.33	VxLAN		2
101.226.70.104	85.143.78.110	L2TP	Control Message - SCCRQ (tunnel id=0, session id=0)	2
81.26.169.218	85.143.78.16	ULP	[UNKNOWN PER: too long integer(per_normally_small_nonnegative_whole_number)][Malformed Packet]	2
60.191.38.77	85.143.78.27	OMRON	Command : Controller Data Read	1
91.205.26.34	85.143.78.238	GTPv2	Reserved[Malformed Packet]	1
62.33.72.37	85.143.78.55	AYIYA	5072 → 40708 Len=104	1
180.191.91.118	85.143.78.49	WTP+WSP	WTP Unknown PDU type 0xc	1
5.187.70.113	85.143.78.33	RX		1
5.140.69.189	85.143.78.11	MPLS	MPLS Label Switched Packet	1
46.147.122.117	85.143.79.230	SMPP	SMPP Cancel_sm	1
85.143.78.35	85.143.79.231	Broadcast	60 Who has 85.143.78.75? Tell 85.143.78.1	1
84.24.69.59	85.143.79.230	Bitcoin	tx	1
85.143.78.33	224.0.0.252	RX	Len=34	1
194.48.218.141	85.143.78.12	TC	19.168035934 Cisco_d8:19:c5 → Broadcast ARP 60 Who has 85.143.79.70? Tell 85.143.79.1	1
85.143.78.1	255.255.255.255	RETRACKER<	54915 Len=263	1
85.143.78.104	224.01	ICMPv6	Neighbor Solicitation for fe80::9100:d544:aa3e:3021 from 2c:fd:a1:2a:d7:2a	1
90.154.71.44	85.143.78.177	DCC	Response: Unknown Op: 97	1
85.143.78.54	224.0.0.252	RX	84 Standard query 0x9018 A wpad	1
85.143.78.35	224.0.0.252	LL	Broadcast ARP 60 Who has 85.143.79.54? Tell 85.143.79.1	1
109.110.68.48	85.143.78.102	BAT_BATMAN	Unsupported Version 100	1
93.184.220.29	85.143.78.45	OCSP	Response	1
46.172.76.24	85.143.78.138	POWERLINK/		1
62.209.197.9	85.143.78.170	RRoCE	UD Send Only QP=0x323a69	1
109.123.182.100	85.143.78.68	NBSS	NBSS Continuation Message	1
121.146.35.120	85.143.78.68	MANOLITO	41170 → 11609 Len=115[Malformed Packet]	1
217.118.95.112	85.143.78.16	X11	Error: Success, <Unknown eventcode 101>, BadGC	1
5.187.70.133	85.143.78.16	IAX2	Mini packet, source call# 25649, timestamp 14945ms, unknown (0x00)	1
85.143.79.230	85.143.78.171	DCP-AF	[Malformed Packet]	1
125.230.50.165	85.143.78.17	ALLJOYN-AR	flags: EAK SEQ: 0 ACK: 0	1

Приложение В.

Development of tools

Студент:

Группа	ФИО	Подпись	Дата
8ВМ6В	Волшин Максим Евгеньевич		

Консультант отделения ИТ:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Чердынцев Евгений Сергеевич	к.т.н.		

Консультант – лингвист отделения ИТ:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель	Рыбушкина Светлана Владимировна			

6. Development of tools

6.1. Mechanism of collection of statistics

The mechanism for collecting statistics is the most loaded module in the developed system. The main load falls on this module. The module listens for network traffic. So it is this module should be sufficiently productive. C programming language was chosen as the most productive language. All system modules and libraries are written in C. This provides the best performance for working with the network and other components. Optimization of compilation allows you to use additional hardware for the processor, for example, the AES cryptography module in Intel processors.

6.1.1. Architecture

The architecture of the statistics collection mechanism consists of three main components (Figure 1): Tshark (packet interceptor), database and developed module - system kernel.

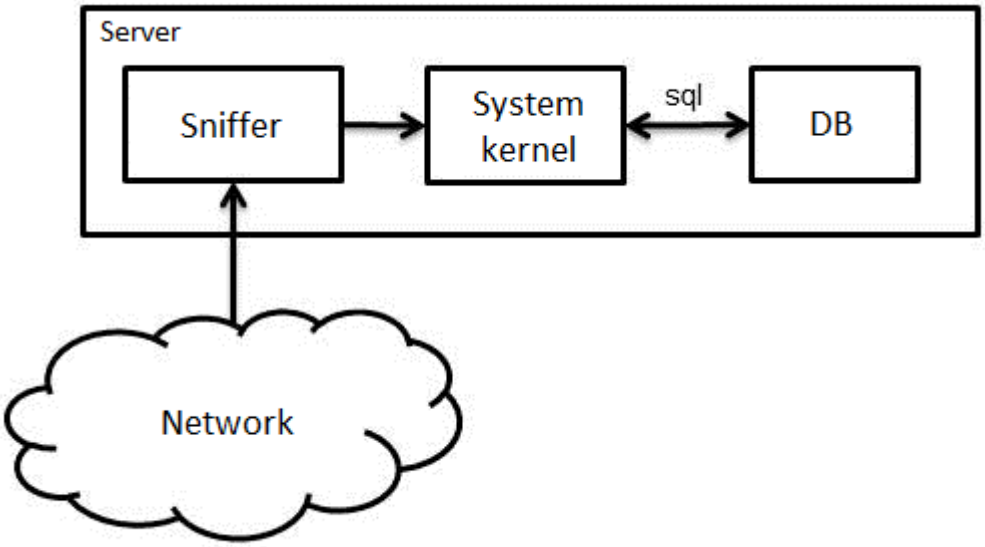


Figure 1. Architecture of the mechanism of collection of statistics.

6.1.2. An output and interception of stdout from Tshark

Tshark intercepts packets and makes their signature analysis. Next, it outputs a string with packet parameters to **stdout**. Parameters are:

8. Number of a packet;
9. Temporal stamp;
10. Source of the sender;
11. Source of the receiver;
12. Protocol;
13. Packet length;
14. Additional information of a packet.

For integration of Tshark into the project the following tools were selected:

3. Posix threads - allows you to create concurrently processed threads within the same process;
4. Pipe – provides easy data transfer between processes.

Thus, implementation of Tshark requires 2 additional flows. The first flow launches Tshark with redirection of stdout in pipe. The second flow listen the pipe and on arrival of a sting makes its analysis. 4 parameters are grouped in a special structure:

5. Source of the sender;
6. Source of the receiver;
7. Protocol;
8. Additional information of a packet.

Further the storage system of data works with the structure of each packet.

6.1.3. Storage system of data

The storage system of data consists of an internal and external DB. The internal DB is a dynamic array of data in a random access memory. An external DB is MySQL. Such approach is caused by the fact that network packets come many times over more often than the external DB is capable to process requests. Therefore a part of operations had to be carried out in an internal DB. Operations

primary aggregations of data and count of checksum of md5 for faster operation with the database belong to such operations.

The algorithm of processing of a packet of the internal database is provided in a figure 2.

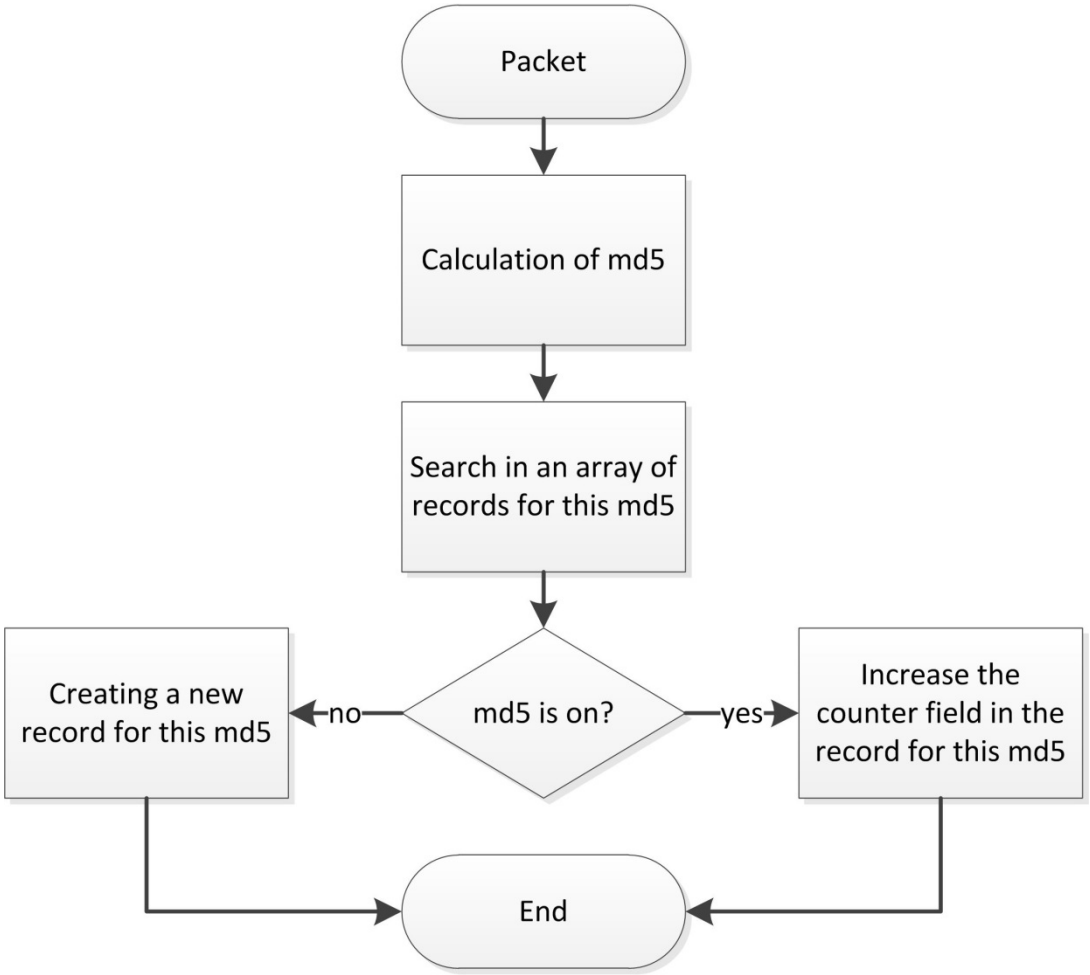


Figure 2. Algorithm of processing of a packet.

Thus, the internal database of packets with their counters is created. Once a minute occurs unloading of data in an external DB on the algorithm provided in a figure 3.

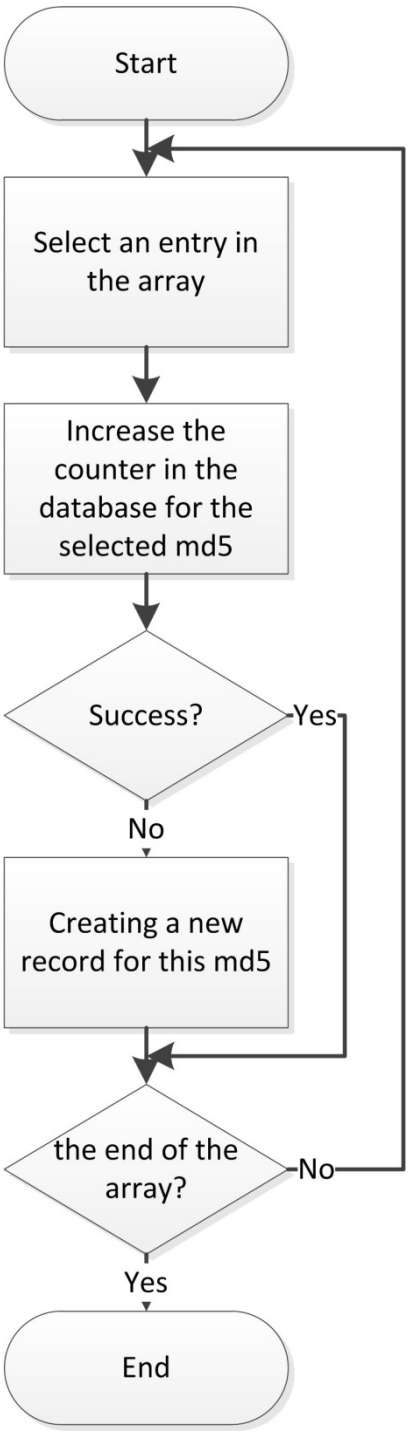


Figure 3. An algorithm of unloading of data in an external DB.

The external DB has 2 types of tables: dataful and counters of packets. In a figure 4 the example of these tables: packets and packets_cnt respectively is provided.

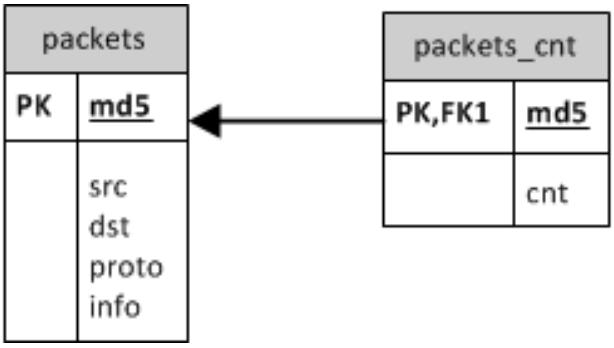


Figure 4. Tables of statistics.

Separation of data tables and counters is required to maintain statistics for different time intervals:

8. On all an interval;
9. Last month;
10. Last week;
11. Last day;
12. Last hour;
13. Last 15 minutes;
14. Last minute.

For each table of counters in a certain interval unloading of values of counters in the table with big time slot is launched.

6.2. Mechanism of display of statistics

SQL queries are the basis of statistics output. This method is convenient in that all the work of filtering the result is performed by the DBMS. For example, to make statistics on quantity of packets of all saved protocols:

```
SELECT snifstat.packets.proto, sum(cnt) AS s
FROM snifstat.packets JOIN snifstat.packets_cnt
ON snifstat.packets.md5 = snifstat.packets_cnt.md5
GROUP BY proto
ORDER BY s desc;
```

Or to look at data of all packets (an example figure 5):

```
SELECT * FROM snifstat.packets;
```

md5	src	dst	proto	info
b1f031b20a16a55c19532a0bca450b20	HewlettP_61:a...	Broadcast	ARP	Who has 85.143.78.1? Tell 85.143.78.52
11ec42aee63d5b664218c816cc13bec0	fe80::14c0:c2...	ff02::1:ff3d:f7f4	ICMPv6	Neighbor Solicitation for fe80::e855:35d7:..
4a7cdbab413159c05378c33ec4a76116	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.92? Tell 85.143.79.1
7dbaf9397d8ed42dcd27b3ebd5819e4c	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.125? Tell 85.143.79.1
e02db92f2185ce3a9f984021f5c20b9d	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.254? Tell 85.143.79.1
b2cc6372f167b784e1565d6cf66c2bf4	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.133? Tell 85.143.79.1
9071999891d6074efb02ad5fb77e2c63	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.253? Tell 85.143.79.1
77e7cfa460ffdf294237aea015fd7bcd	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.89? Tell 85.143.79.1
38ccab42a4c078969247e6a2d4a9d0d7	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.157? Tell 85.143.79.1
3be7861bd22365738a4de38011d8a39d	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.105? Tell 85.143.79.1
27b021f8b02e95da2675484679d81d9e	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.196? Tell 85.143.79.1
ee5874f53850127df6d03e131ff9726d	85.143.78.15	255.255.255.255	UDP	54376 → 7533 Len=34
f826726ef3b351d2ab952816a55dd726	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.90? Tell 85.143.79.1
e9f8072f20b2fd033a0e1d28d1c7467e	85.143.78.244	255.255.255.255	UDP	65006 → 7533 Len=34
01661fe772beabd8e38176bffdf74710	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.78.21? Tell 85.143.78.1
7ce56b23946db3e82c0c3d9d6e5143ca	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.52? Tell 85.143.79.1
03f89156140e763d07b49b1bd35b5ddb	85.143.78.90	85.143.78.255	UDP	54915 → 54915 Len=263
9db7d995d067c91d39d0505a3cb16cd9	Cisco_d8:19:c5	Broadcast	ARP	Who has 85.143.79.232? Tell 85.143.79.1
4ff94350afa60afef67a6361addcb7da	Cisco_19:28:34	Spanning-tree-(f...	STP	RST. Root = 24576/811/b8:be:bf:d8:19:8..

Figure 5. A part of the intercepted packets.

6.3. The mechanism of localization of anomalies on a network

Source blocking is the most effective means of localizing anomalies. For this task it was decided to use equipment hardware in combination with external control according to the SNMP [10] protocol.

The SNMP protocol provides to receive and set values of the MIB elements of the controlled device. MIB is a treelike basis of parameters of different types among which there are INTEGER, STRING, TIME and many others [11].

6.3.1. Algorithm of detection of anomalies

Analysis of statistical data (protocols, types of messages) is the basis of the algorithm. If a new protocol or new types of messages appear in the statistics, the system administrator is notified by the syslog protocol. This method of information simplifies integration with the general enterprise monitoring system. The administrator performs data analysis and decides which group of threats to classify this type of packet:

5. Completely safe packets – the packet will not be considered as threat;
6. Safe from specific hosts – the packet is considered safe if proceeds from a specific host or group of hosts, differently – lock of a source;
7. Potentially dangerous – the algorithm of processing of software packages is provided to this rule in a figure 6;
8. Dangerous packets – momentary lock of a source of a packet.

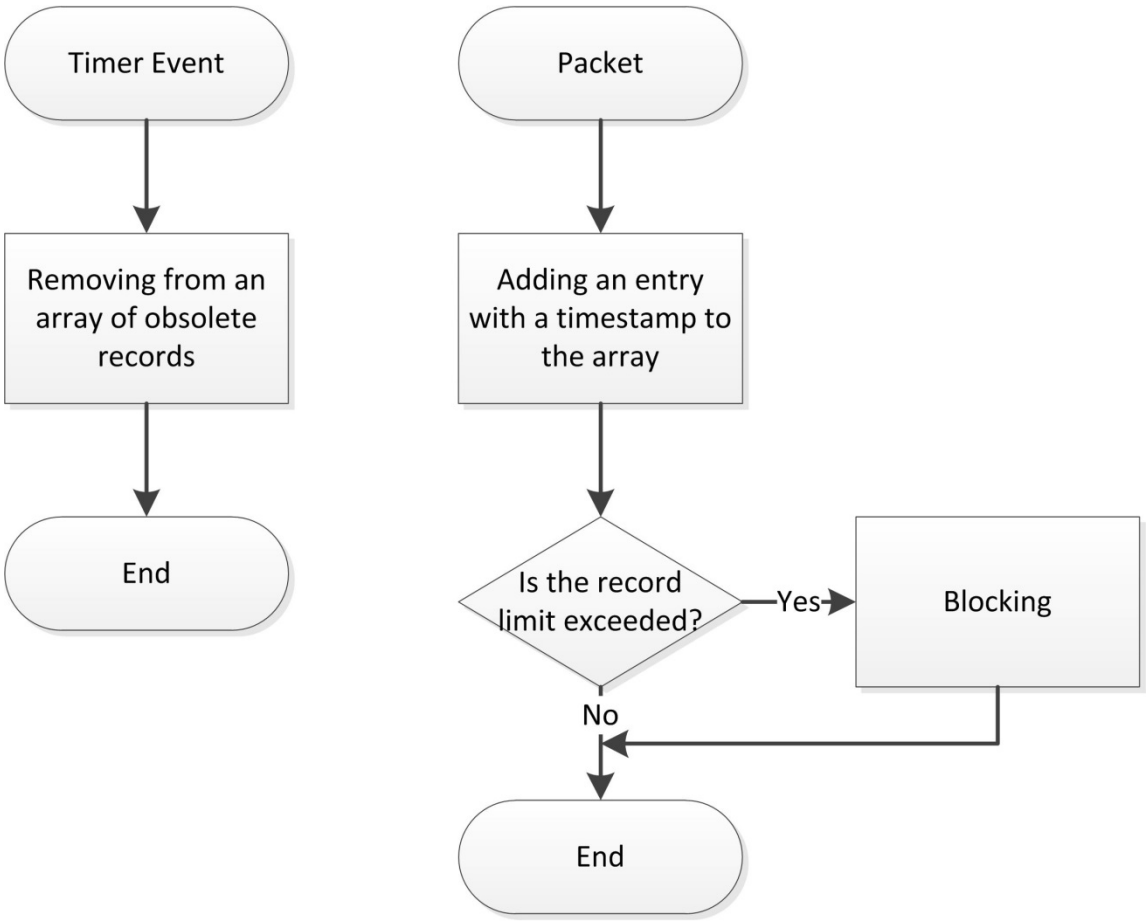


Figure 6. An algorithm of processing of packets with temporary restriction.

The separate table which format is provided in a figure 7 is selected for data storage of rules in a DB.

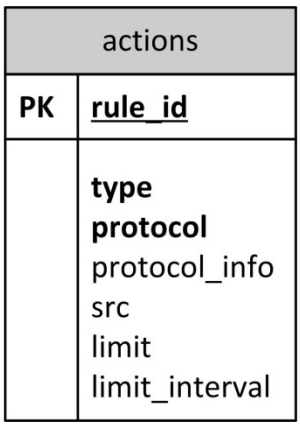


Figure 7. Table of rules.

Where:

rule_id – a unique identifier of the rule;

type – packet type (are described above);

protocol – the name of the protocol;

protocol_info – additional information of packet;

src – a packet source;

limit – restriction of quantity of packets;

limit_interval – an interval of accounting of a limit of packets;

In addition for the aid to the administrator algorithms of detection of anomalies in completely automatic mode are developed.

6.3.1.1. Algorithm of detection of anomalies of the ARP protocol

Operation of an algorithm is divided into 2 stages:

3. Training – studying of linking of MAC – IP;
4. Tracking – registration of changes with the subsequent actions.

The general algorithm is provided in a figure 8.

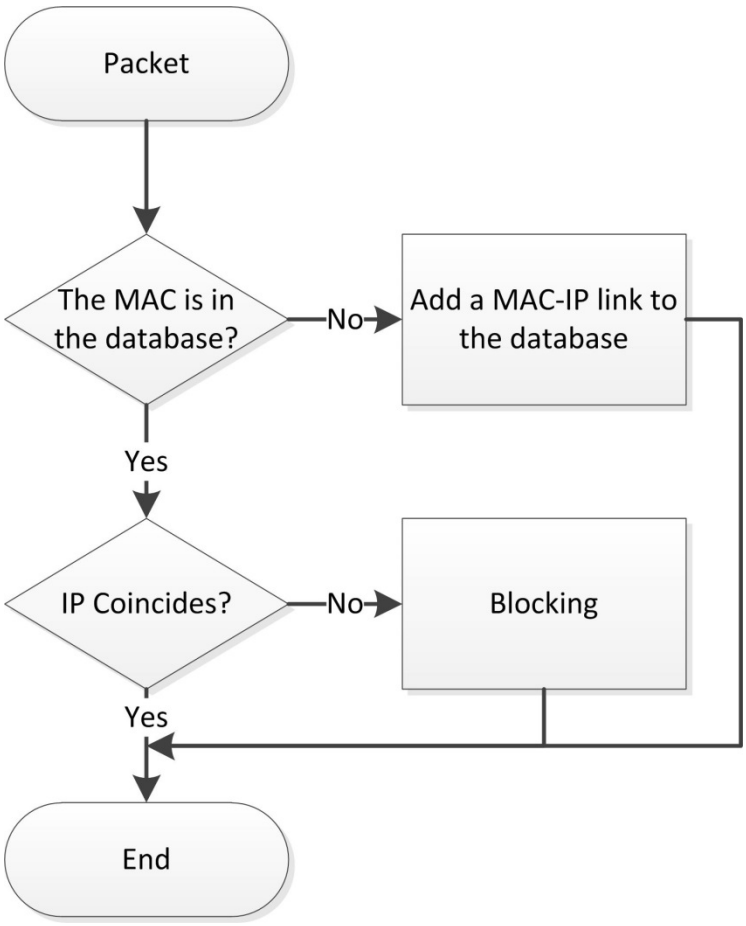


Figure 8. Algorithm of detection of anomalies of the ARP protocol.

6.3.1.2. Algorithm of detection of anomalies of the ICMP protocol

The algorithm is based on lock of messages of some types:

5 – Redirection:

9 – declaration of the router:

10 – router request.

Blocking messages type 5 and 9 will work for the attacker, while the 10th type will work on the client. In this case, the system notifies the administrator.

The general algorithm is provided in a figure 9.

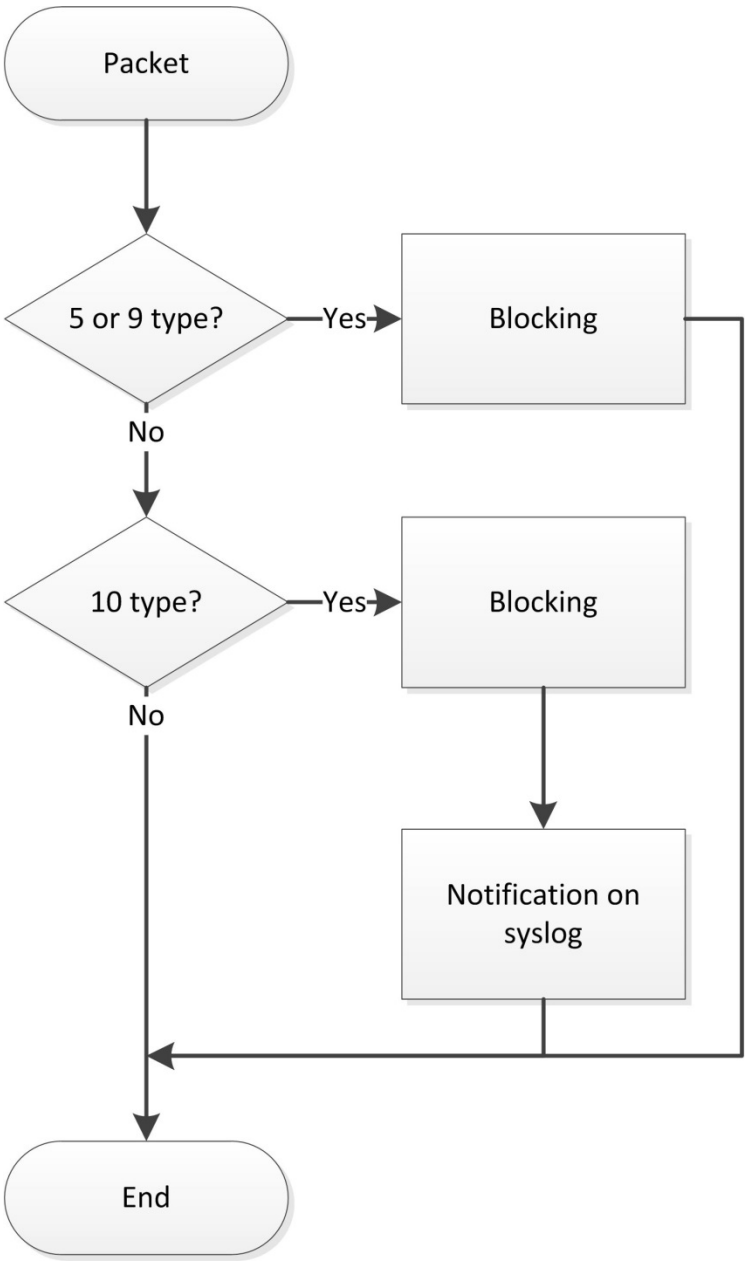


Figure 9. Algorithm of detection of anomalies of the ICMP protocol.

6.3.2. Control of the equipment

End customers are connected to Ethernet by the switch. Therefore the decision to control only switches was made. On a network are used Cisco switches of model: 2950, 2960 and 3750. They are very similar in control and have almost identical MIB. It is necessary to know the MAC or IP-address of a malignant client for blocking. The general algorithm of switch-off of port is provided in a figure 10. For its implementation the following nodes are required:

4. A basis of switches with their data for connection;

5. A basis of linking of IP – MAC and IPv6 – MAC;
6. SNMP Manager for interaction with switches.

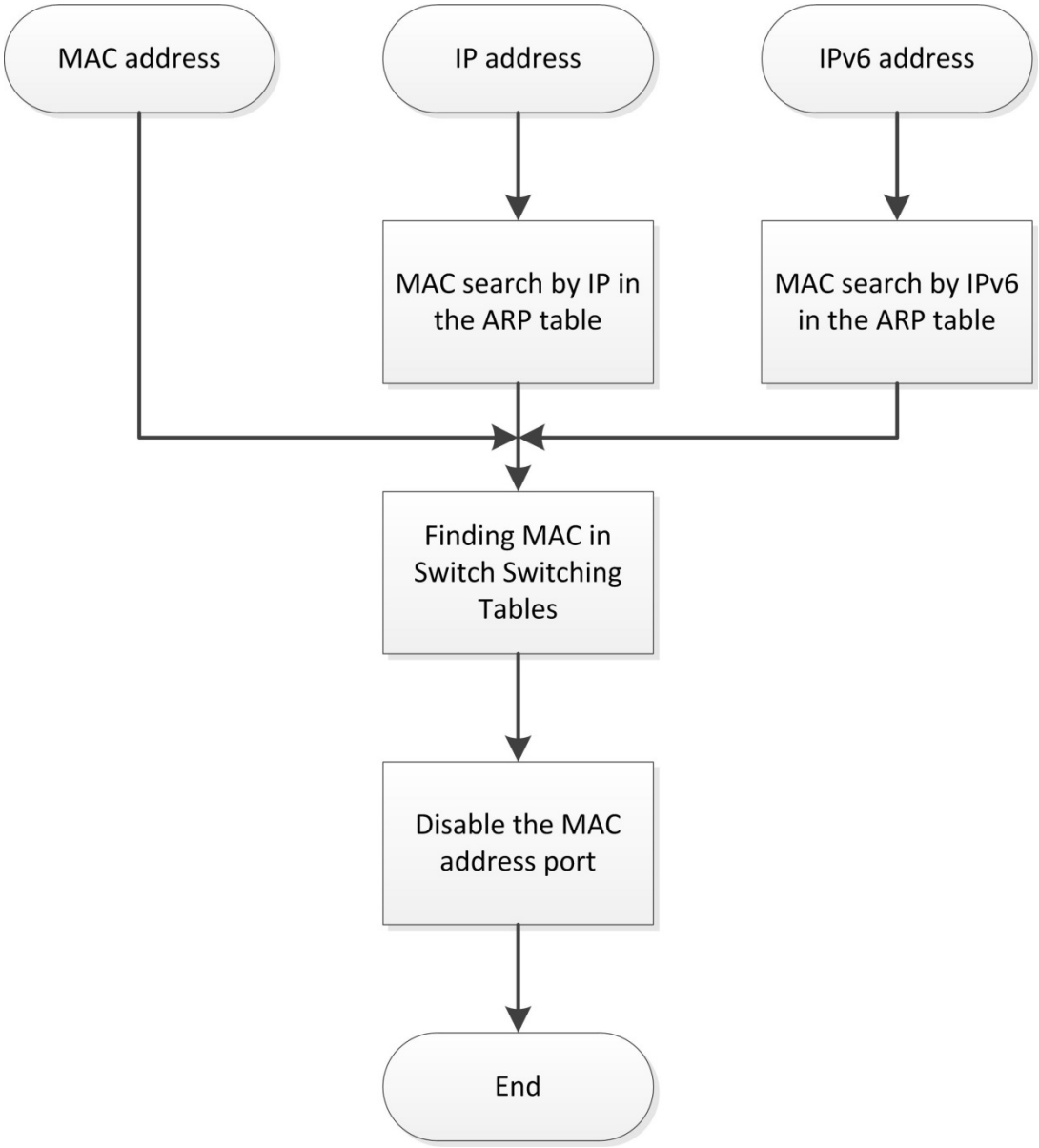


Figure 10. Algorithm of insulation of a source of anomaly.

6.3.2.1. Basis of switches

The dataful basis for connection to switches to be stored in MySQL in the form of the table (fig. 11)

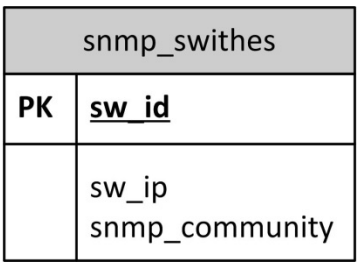


Figure 11. Reference manual of switches.

Where:

sw_id – unique identifier of the switch;

sw_ip – switch IP address;

snmp_community – line of authorization leaked SNMP.

6.3.2.2. A basis of linking of IP – MAC and IPv6 – MAC

It was decided to use the ready-made project with open source code **addrwatch** to obtain these bundles. This utility wiretaps the network interface and intercepts ARP packets, making on them the relevant database. The utility supports several methods of data output:

4. Stdout – a line-by-line output of changes in a terminal window;
5. Syslog – the protocol for service of registration of messages about system events. For registration of similar messages a large number of the software with different functionality is created;
6. MySQL – unloading of a ready basis in the form of the table (fig. 12)

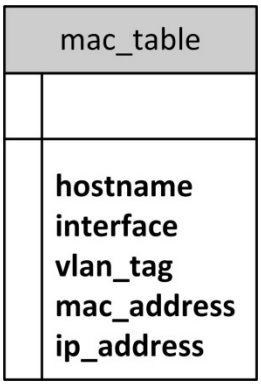


Figure 12. Table of relevant network points.

Where:

hostname – computer name which enters record in the table (in this case this name of one server);

interface – a name of the network interface where was found the MAC address;

vlan_tag – number vlan and which the MAC address was found;

mac_address – the MAC address;

ip_addres – IP or IPv6 the address.

It was decided to use unloading in the MySQL database to simplify the search and reduce the development time.

6.3.2.3. SNMP Manager

it was decided to use the open-source library Net-SNMP as the basis of the SNMP manager. This library is written in language C and provides basic routine actions for operation according to the SNMP protocol:

7. To open connection;
8. To configure a request;
9. To send a request;
10. To send an asynchronous request;
11. To receive the response;
12. To close connection.

Operation of SNMP of the manager is divided into several stages:

5. Obtaining the list with IP and SNMP Community;
6. Opening of connections with all switches
7. Receiving базово necessary parameters (about them below);
8. Periodic scanning of communication tables of switches for compilation of the copy in process that accelerates search of MAC port of the address.

6.3.2.3.1. Basic parameters of switches

In MIB a tree of the switch several key branches were revealed:

5. Control of ports and other interfaces;
6. Control of the network bridge to which interfaces "are connected";
7. The table of sheaves the MAC address – port number in the bridge (the bridge – the virtual concept);
8. The table of sheaves port number in the switch – an interface ID from the first branch.

It was decided for each switch to use arrays with the following structures:

```
struct snmp_switch_port_state
{
    // Interface index
    int32_t        id;
    // Hardware interface name
    char           *description;
    // 1 – on, 2 - off
    int32_t        admin_status;
    // 1 – link ok, 2 – no link
    int32_t        operation_status;
    // bridge port number
    uint32_t       bridge_port;
    // 0 – off, 1 - on
    unsigned int   enable;
} typedef snmp_switch_port_state_t;

struct snmp_switch_mac_address
{
    Char           mac_address[6];
    // bridge port number
    uint32_t       bridge_port;
} typedef snmp_switch_mac_address_t;
```

First of all for each switch the array of structures of snmp_switch_port_state on a branch with all interfaces is built. In runtime of this stage fields are filled: id and description.

Table scan of compliances of an id of the interface – port number in the bridge. The example of the table is provided in a figure 13 where:

SNMPv2-SMI::mib-2.17.1.4.1.2.**39** = INTEGER: **10035**

39 – bridge port;

10035 – interface id.

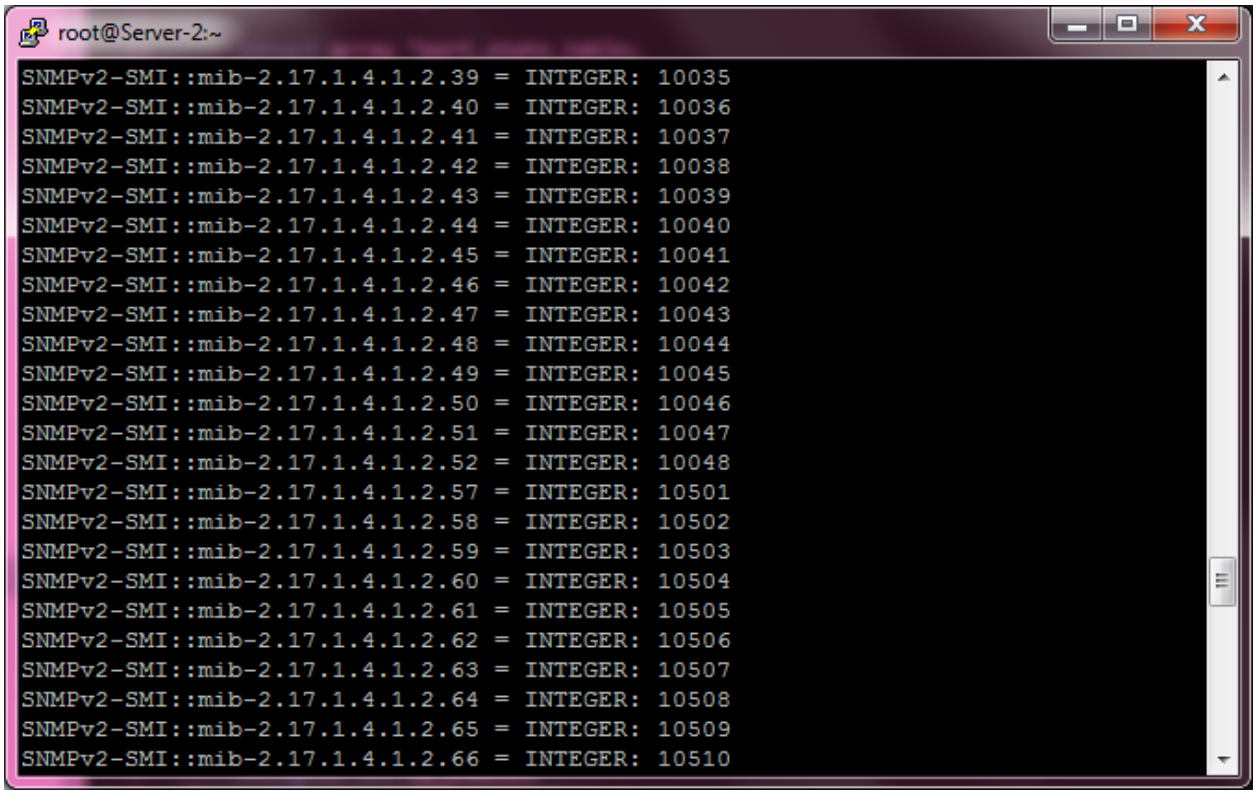


Figure 13. SNMP the table of correspondence of an id of the interface – port number in the bridge.

Next, a cyclic poll of the branch of the switching table begins, an example of which is shown in Figure 14 where:

SNMPv2-SMI::mib-2.17.4.3.1.2 – the branch address;

252.69.150.227.198.3 – the MAC address in a decimal format (the part selected in a figure 14);

INTEGER – data type in a leaf of the received tree;

353 – port number in the bridge.

Thus, the SNMP Manager receives a local copy of the switch table. This greatly speeds up the work. Scanning of the branches of the switch can occur at different speeds, depending on the performance of the equipment and its load.

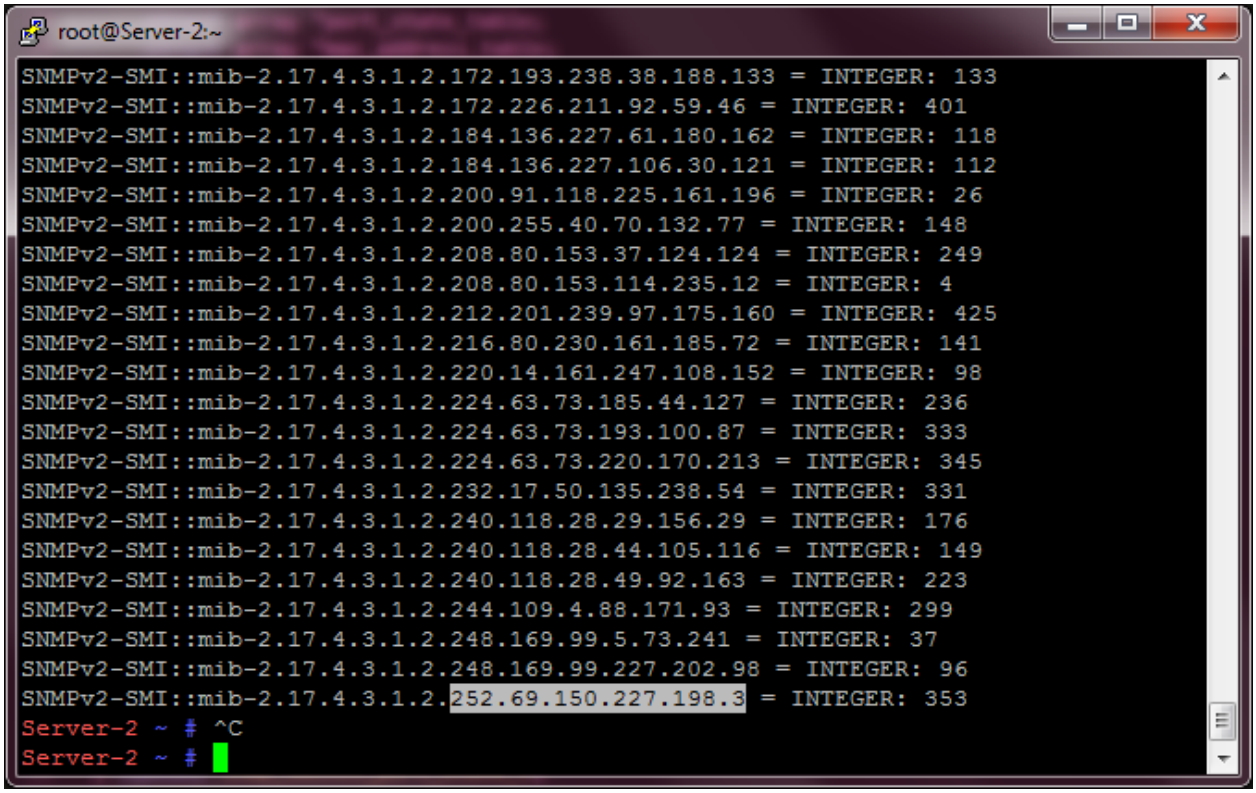


Figure 14. SNMP table of switching.

6.3.2.3.2. Algorithm of switch-off of port

As soon as the command arrives to disconnect port for the MAC address of the malefactor, occurs:

4. Search of the MAC address in local copies of tables of switching of all switches
5. The port number in the bridge is calculated
6. On port number in the bridge the interface id is calculated. And on an interface id on the switch the team for transfer of physical port in disable status is formed.

The complete algorithm is provided in a figure 15.

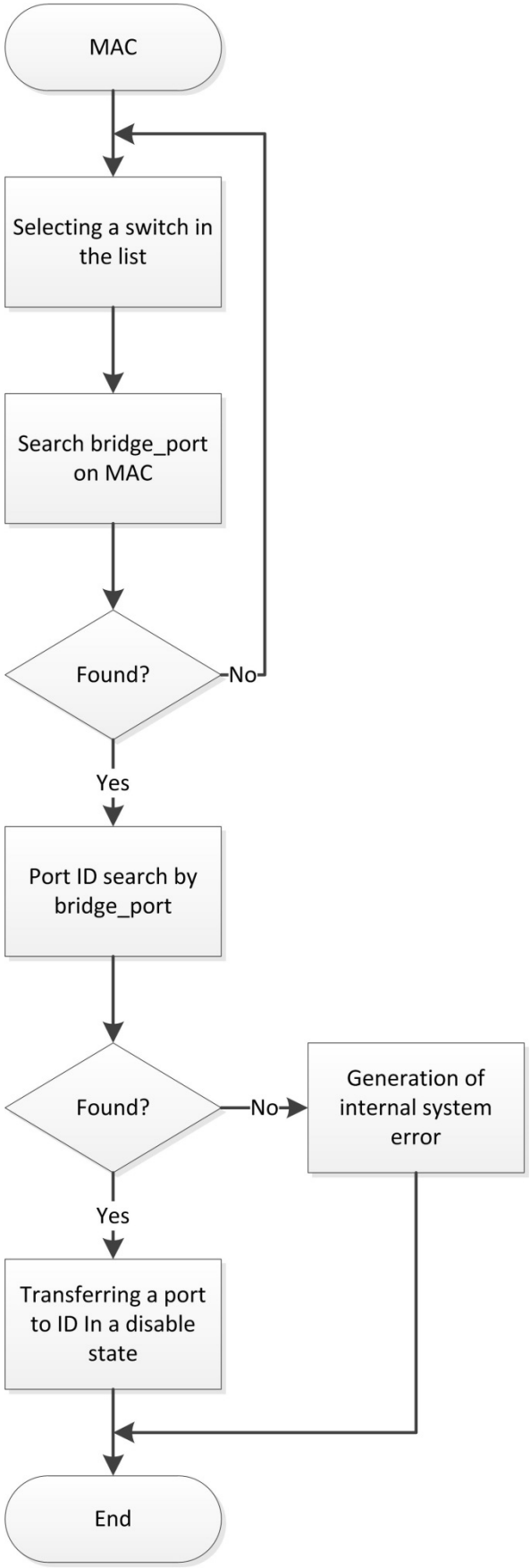


Figure 15. An algorithm of switch-off of port on the equipment