

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Ярославский государственный технический университет»  
Кафедра «Информационные системы и технологии»

УДК 004.056

ДОПУСКАЕТСЯ К ЗАЩИТЕ

Заведующий кафедрой  
канд. техн. наук  
\_\_\_\_\_ С.Ю. Бойков  
«\_\_» \_\_\_\_\_ 2024

**РАЗРАБОТКА ТЕХНИЧЕСКОГО РЕШЕНИЯ ПО ОРГАНИЗАЦИИ  
ЗАЩИЩЕННОГО КАНАЛА С ИСПОЛЬЗОВАНИЕМ АПКШ  
«КОНТИНЕНТ» 3.9 ДЛЯ АО «КОМПАНИЯ ТРАНСТЕЛЕКОМ»**

Пояснительная записка к выпускной квалификационной работе по  
направлению подготовки «Информационные системы и технологии»

ЯГТУ 09.03.02 – 001 ВКР

СОГЛАСОВАНО

Руководитель  
\_\_\_\_\_ Е. В. Александрова  
«\_\_» \_\_\_\_\_ 2024

Нормоконтролер  
\_\_\_\_\_ Е. В. Александрова  
«\_\_» \_\_\_\_\_ 2024

Консультант по экономике и  
организации производств  
\_\_\_\_\_ М. И. Маркин  
«\_\_» \_\_\_\_\_ 2024

Проект выполнил  
студент группы ЭИСБ-44  
\_\_\_\_\_ В. А. Багрова  
«\_\_» \_\_\_\_\_ 2024

2024

## РЕФЕРАТ

80 с., 49 рис., 14 табл., 15 источников, 1 приложение.

### ШИФРОВАНИЕ, ЗАЩИТА ИНФОРМАЦИИ ПРИ ЕЕ ПЕРЕДАЧЕ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, VPN, АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС ШИФРОВАНИЯ.

Объектом работы является Акционерное Общество «Компания ТрансТелеКом».

Предмет работы – защищенный канал передачи данных между главным офисом и филиалом банковской организации.

Целью работы является проектирование защищенного канала связи между главным офисом и филиалом банковской организации с использованием аппаратно-программного комплекса шифрования «Континент» 3.9.

Задачами работы являются:

1. Проанализировать требования заказчика и законодательства в области защиты информации при ее передаче с использованием СКЗИ;
2. Рассмотреть существующие решения по реализации VPN-соединений, выбрать средство для дальнейшей работы;
3. Спроектировать схему организации сети, согласно которой будет производиться шифрование;
4. Произвести настройку выбранного оборудования (в тестовом режиме);
5. Проверить систему на корректность функционирования и наличие ошибок;
6. Рассчитать стоимость спроектированного решения.

В первой главе был произведен анализ деятельности «Компании ТрансТелеКом», изучены и проанализированы требования заказчика и законодательства в области защиты информации при ее передаче с использованием средств криптографической защиты информации, рассмотрены основные виды VPN-соединений и инструменты для реализации данной технологии.

Во второй главе была проанализирована изначальная схема построения сети главного офиса, а также схема сети после внедрения аппаратно-программного комплекса шифрования. Представлены диаграмма компонентов криптографического шлюза, схемы аутентификации пользователя, процесса сбора журналов событий.

В третьей главе была произведена настройка оборудования с использованием тестового стенда АПКШ «Континент» версии 3.9, а также проведено тестирование работоспособности системы.

Результатом данной работы является разработанный зашифрованный канал между главным офисом и филиалом банковской организации.

## Содержание

Перечень сокращений и обозначений.....	6
Введение.....	7
1. Аналитическая часть.....	8
1.1 Описание деятельности компании «ТрансТелеКом», схема организационной структуры .....	8
1.2 Анализ требований, предъявляемых к проекту .....	9
1.3 Анализ требований из нормативно-правовых актов в области защиты информации при передаче ее по каналам связи и выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию .....	11
1.4 Анализ существующих решений и средств реализации VPN-технологий при построении защищенной сети.....	12
1.5 Основные виды VPN-соединений .....	13
1.6 Оборудование, реализующее VPN соединение .....	15
1.6.1 Виртуальная частная сеть на базе межсетевых экранов .....	15
1.6.2 Виртуальная частная сеть на базе маршрутизаторов .....	16
1.6.3 Виртуальная частная сеть на базе программного обеспечения .....	16
1.6.4 Виртуальная частная сеть на базе сетевой ОС.....	16
1.7 Оборудование для реализации VPN, их описание .....	16
1.8 Возможности АПКШ Континент 3.9 .....	18
1.9 Анализ требований и ограничений к использованию АПКШ «Континент».....	19
1.10 Вывод по разделу .....	21
2 Проектная часть.....	22
2.1 Постановка задачи.....	22
2.2 Анализ построения сети до и после внедрения комплекса .....	22
2.3 Диаграмма компонентов криптографического шлюза.....	25
2.4 Схема процесса сбора записей журналов событий .....	27
2.5 Схема аутентификация и авторизация пользователей .....	28
2.2 Вывод по проектной части.....	31
3 Технологическая часть .....	32
3.1 Инициализация ЦУС и СД.....	32
3.2 Установка подсистемы управления комплексом.....	33
3.3 Конфигурирование базы данных журналов, настройка агента ЦУС и СД...	36
3.4 Инициализация КШ .....	42
3.5 Настройка правил фильтрации .....	46
3.6 Организация L3VPN .....	49
3.8 Вывод по технологической части.....	54
4 Экономическая часть .....	55
4.1 Обоснование целесообразности разработки проекта.....	55
4.1.1 Основание для разработки .....	55
4.1.2 Назначение ввода комплекса в эксплуатацию .....	55
4.1.3 Жизненный цикл проекта.....	55

4.1.4 Реестр заинтересованных лиц .....	56
4.1.5 Структура команды проекта .....	58
4.2 Описание продукта .....	58
4.3 Бизнес-модель проекта .....	58
4.4 Планирование комплекса работ.....	58
4.5 Расчет затрат на реализацию проекта .....	61
4.5.1 Анализ структуры затрат.....	61
4.5.2 Затраты на оборудование и программное обеспечение .....	63
4.5.3 Расчет затрат на содержание и эксплуатацию оборудования .....	65
4.5.4 Затраты на электроэнергию.....	65
4.5.5 Затраты на внедрение .....	65
4.5.6 Накладные расходы.....	66
4.5.7 Прочие расходы.....	66
4.5.8 Общие затраты на разработку.....	68
4.6 Оценка эффекта .....	68
4.7 Вывод по экономической части.....	68
Заключение .....	69
Список использованной литературы.....	70
Приложение А .....	72

## Перечень сокращений и обозначений

АБС	– автоматизированная банковская система
АПКШ	– аппаратно-программный комплекс шифрования
АРМ	– автоматизированное рабочее место
АС	– автоматизированная система
ЗО	– зона ответственности
ИБ	– информационная безопасность
КШ	– криптографический шлюз
ЛВС	– локально-вычислительная сеть
ПО	– программное обеспечение
СЗИ	– средство защиты информации
СКЗИ	– средство криптографической защиты информации
СУ	– система управления
ФСБ	– федеральная служба безопасности
ФСТЭК	– федеральная служба по техническому и экспортному контролю
ЦУС	– центр управления сетью
ЦУСС	– центр управления сетями связи

## Введение

В современном обществе цифровые технологии являются неотъемлемой частью повседневной жизни, а сама информация является одним из наиболее ценных и востребованных ресурсов. Поэтому обеспечение безопасности передачи информации становится одним из ключевых аспектов, требующих пристального внимания как для коммерческих организаций, так и для общества в целом.

Большая часть современных коммерческих организаций имеют распределенную структуру и множество филиалов, из-за чего встает вопрос о защите информации при ее передаче по каналам связи. Часто компании становятся жертвами злоумышленников, которые каким-либо образом получили доступ к конфиденциальной информации и тем или иным образом использовали ее для получения собственной выгоды. Подобная утечка может быть вызвана множеством факторов, которые чаще всего связаны с несовершенством системы защиты информации, уязвимостями в программном обеспечении и оборудовании для передачи информации, отсутствием мониторинга событий и аудита безопасности в сети.

Согласно результатам исследования экспертного-аналитического центра ГК «InfoWatch» за прошедший 2023 год в России на 12,3% возросло количество утечек конфиденциальной информации в финансовых организациях. Поэтому финансовым организациям, в том числе банкам, необходимо защищать информацию при ее передаче по каналам связи по нескольким причинам:

- а. Конфиденциальность своих клиентов, поскольку банковские организации работают с большим объемом их персональных и финансовых данных;
- б. Финансовая безопасность, поскольку банки осуществляют финансовые транзакции между своими филиалами, включая переводы и платежи;
- в. Репутационный риск, так как утечка или несанкционированный доступ к передаваемой информации может серьезно повлиять на репутацию банка;
- г. Соблюдение законодательства, потому что банковские организации обязаны соблюдать нормативные акты, регулирующие обеспечение безопасности информации.

Для защиты информации передаваемой по каналам связи между двумя элементами виртуальной частной сети (VPN), при объединении локальных сетей главного офиса ПАО «Банк» и его филиалом, находящихся в разных городах, в единую сеть через VPN, предлагается использовать аппаратно-программный комплекс шифрования «Континент» версии 3.9.

## 1. Аналитическая часть

### 1.1 Описание деятельности компании «ТрансТелеКом», схема организационной структуры

АО «Компания ТТК» занимает важное место на рынке связи в России, предоставляя магистральные услуги для операторов и крупных корпораций. Также является одним из ведущих провайдеров широкополосного доступа в Интернет, телевидения и телефонии для жителей различных регионов страны.

ТТК активно участвует в процессах цифровой трансформации ОАО «РЖД» и транспортно-логистической сферы в целом. Она предоставляет услуги связи и высокоскоростных корпоративных сетей холдингу «РЖД» и развивает инфраструктуру систем связи и транспортной безопасности. Также компания активно внедряет системы видеонаблюдения и видео аналитики, а также технологии искусственного интеллекта.

Одной из ключевых деятельности ТТК является эксплуатация и обслуживание волоконно-оптических линий связи. Компания управляет одной из крупнейших в России сетей, протяженность которых составляет 78 тысяч километров и пропускной способностью свыше 4,8 Тбит/с.

Схема организационной структуры представлен на рисунке 1:

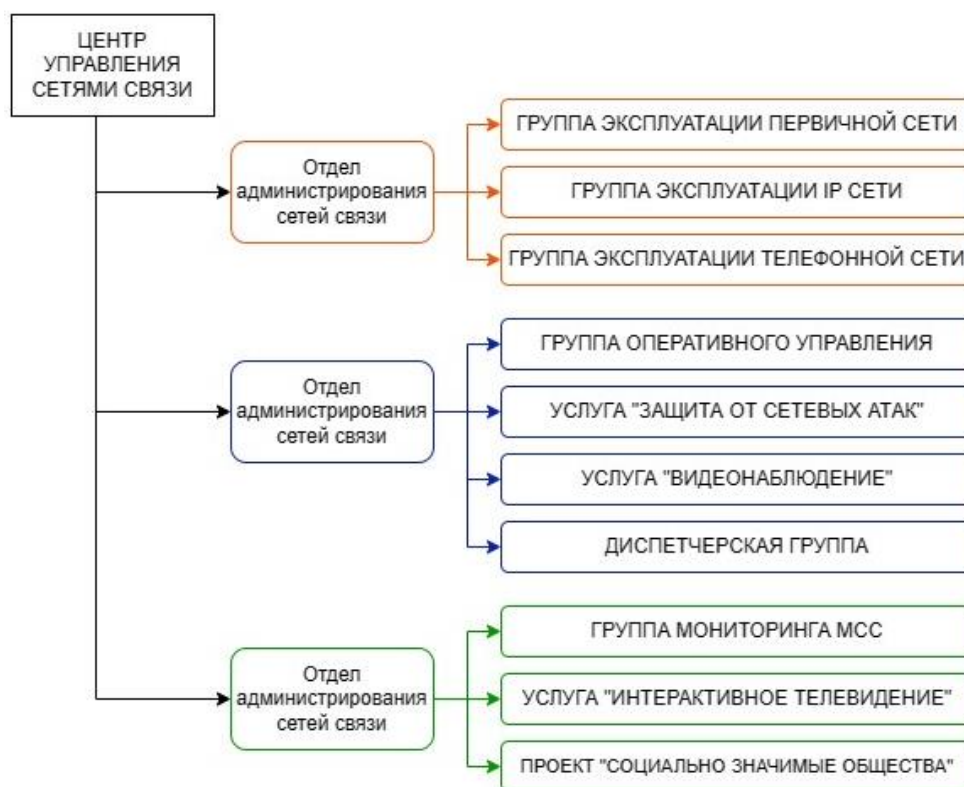


Рисунок 1 – Схема организационной структуры Центра Управления Сетями Связи г. Ярославля

«Компания ТТК» предоставляет свои услуги не только государственным заказчикам, но и бизнес-клиентам и частным лицам на всей территории России. В том числе компания предоставляет услуги по шифрованию каналов связи с соблюдением российского законодательства – VPN ГОСТ. Такая услуга позволяет коммерческим и государственным организациям избежать затрат на закупку необходимого оборудования у поставщиков решений средств криптографической защиты информации и организацию технической поддержки. Такая услуга обеспечивает защиту передаваемых данных по открытым каналам связи, обеспечивая конфиденциальность и целостность информации.

«Компания ТрансТелеКом» предоставляет комплексные услуги в области обеспечения безопасности информации, выполняет работы на каждом этапе предоставления услуги: от разработки модели нарушителя и выбора соответствующего уровня защиты до предоставления гарантированно безопасного VPN. В конечном итоге ТТК гарантирует предоставление VPN, который обеспечивает защищенную передачу данных между точками подключения, обеспечивает клиентам требуемый уровень защиты информации.

Преимущества данной услуги является использование сертифицированных ФСТЭК и ФСБ России СКЗИ, возможность делегирования ответственности за задачу криптозащиты на Компанию ТрансТелеКом, консультации квалифицированных специалистов и оперативность предоставления услуги. Клиентам также предоставляется выбор из лучших поставщиков средств криптографической защиты информации.

## 1.2 Анализ требований, предъявляемых к проекту

Поскольку одной из важнейших задач современных компаний, особенно финансовых, является обеспечение защиты передачи информации от кибератак и несанкционированного доступа к конфиденциальной информации, актуальным становится вопрос организации защищенных каналов передачи информации между территориально удаленными друг от друга офисами и филиалами.

В контексте данной проблемы АО «Компания ТТК» получила запрос на разработку и организацию такого решения, а также на оценку затрат на его реализацию. Задача заключается в создании защищенного канала с шифрованием с использованием алгоритмов ГОСТ между двумя точками: главным офисом в г. Екатеринбург и филиалом в г. Рязань.

Поскольку Заказчик выразил желание сохранить конфиденциальность своих данных и не раскрывать идентификацию своей организации, в данной выпускной квалификационной работе банковская организация будет указываться как ПАО «Банк».

Для удобства восприятия требований, выдвинутые Заказчиком требования к разрабатываемому решению представлены в таблице 1.



Таблица 1 – Требования Заказчика к разрабатываемому решению

№	Вопрос	Ответ
А. Общие требования		
1	Требуется ли дополнительная установка межсетевого экрана между криптошлюзом и оборудованием Заказчика?	Нет
2	Топология VPN	Site-to-Site
3	Планируется установка оборудования СКЗИ на периметре сети или за маршрутизатором?	На периметре сети
4	Перед принятием решения о применении реализованного проекта по шифрованию необходимо ли организовать его тестирование?	Да, тестирование будет производиться на удаленном сервере
5	Требуется ли резервирование?	Резервирование требуется для КШ
6	Другие требования	Будут запускаться удаленные приложения АБС, важна комфортная работа с этими удаленными приложениями
Б. Требования к шифрованию		
7	Необходимо ли использование отечественных алгоритмов при шифровании?	Да
8	Требуемая скорость шифрования	50 Mbps
9	Необходимо ли использование сертифицированных СЗИ?	Сертификация ФСТЭК России
В. Технические требования к оборудованию		
10	Требования к классу защиты СКЗИ	КС1
11	Уровень VPN	L3VPN

№	Вопрос	Ответ
12	Количество физических интерфейсов для стыка криптографических шлюзов с оборудованием Заказчика на каждом узле	По 1
В. Технические требования к оборудованию		
13	Количество рабочих станций, подключаемых к VPN через криптографические шлюзы на каждой площадке	По 1
14	Используется ли аналогичное оборудование в инфраструктуре?	Нет
Г. Требование к обслуживанию и мониторингу		
15	Управление и мониторинг криптографических шлюзов, управление ключевым и удостоверяющим центром – в ЗО ТТК?	Да

1.3 Анализ требований из нормативно-правовых актов в области защиты информации при передаче ее по каналам связи и выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию

Анализ нормативно-правовых актов в области защиты информации при ее передаче по каналам связи и выполнению работ, оказанию услуг в области шифрования информации и техническому обслуживанию необходим для того, чтобы, в первую очередь соблюдать установленное законодательство.

Поскольку защита информации является критически важным аспектом для организаций, для предотвращения утечек или несанкционированного доступа к ней, необходим анализ нормативно-правовых актов, который позволяет определить требования к обеспечению безопасности передаваемой информации.

В некоторых случаях клиенты или партнеры требуют соблюдения определенных стандартов и требований законодательства в области защиты информации, а анализ нормативных актов помогает оценить, насколько компания, которая предоставляет услугу, соответствует этим требованиям. Также соблюдение выдвигаемых законодательством требований создает положительное впечатление о компании у потенциальных клиентов и повышает их доверие.

Требования из нормативно правовых актов в области выполнения работ, оказания услуг в области шифрования информации, техническому

обслуживанию подробно представлены в Приложении А к настоящей пояснительной записке.

#### 1.4 Анализ существующих решений и средств реализации VPN-технологий при построении защищенной сети

Безопасность информационных активов при их обработке в информационных системах обеспечивается с помощью систем защиты информации.

Информационные активы обрабатываются и хранятся в информационных системах, а также передаются с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

В рамках поставленной задачи необходимо установить защищенное соединение между главным офисом ПАО «Банк» и открывающимся филиалом.

Самым распространенным решением является применение технологии Virtual Private Network (VPN), которая позволяет организации использовать сеть «Интернет» в качестве среды для построения VPN, для соединения ЛВС. Удобство заключается в том, что нет необходимости прокладки кабелей, а также, как правило, оборудование, позволяющее строить такого вида соединение, помимо этого может выполнять ряд других задач, в зависимости от комплектации и настройки выбранного оборудования.

Главным аспектом при выборе такого оборудования является наличие сертификата ФСТЭК или ФСБ у используемого средства защиты информации, и будет ли обеспечен требуемый уровень защищенности информации при ее передаче по каналам связи

Классифицировать VPN решения можно по нескольким основным параметрам:

##### 1. По типу используемой среды:

а. защищенные VPN сети – это наиболее распространенный вариант частных сетей. Они позволяют создать надежную и защищенную подсеть на основе ненадежной сети, как правило, сети «Интернет». Примерами защищенных VPN являются OpenVPN и PPTP.

б. доверительные VPN сети. Такие сети применяются в случаях, когда среду передачи данных можно считать надежной, и основной задачей становится создание виртуальной подсети в рамках уже существующей. Вопросы обеспечения безопасности становятся неактуальными. Примерами подобных VPN решений являются MPLS и L2TP. Корректнее сказать, что эти протоколы перекладывают задачу обеспечения безопасности на другие протоколы, такие как L2TP, который обычно используется в паре с IPSec.

## 2. По способу реализации:

а. VPN сети в виде специального программно-аппаратного обеспечения. Такой тип виртуальной частной сети создается при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищенности;

б. VPN сети, реализованные в виде программного обеспечения. В этом случае используется персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN;

в. VPN сети с интегрированным решением. Функциональность VPN обеспечивается комплексом, решающим задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

## 3. По назначению:

а. Intranet VPN. Этот тип используется для объединения в единую защищенную сеть нескольких распределенных филиалов одной организации, которые обмениваются данными по общедоступным каналам связи.

б. Remote Access VPN. Этот тип используется для создания защищенного канала связи между сегментом корпоративной сети и одиночным пользователем, который работает удаленно и подключается к корпоративным ресурсам со своего личного компьютера.

в. Extranet VPN. Используется для сетей, к которым подключаются внешние «внешние» пользователи. Уровень доверия к ним на порядок ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных защитных механизмов, которые предотвращают или ограничивают доступ таких пользователей к особо ценной, конфиденциальной информации.

## 4. По типу протокола:

Существуют реализации виртуальных частных сетей под такие протоколы как TCP/IP, IPX и AppleTalk. Но в настоящее время можно наблюдать тенденцию ко всеобщему переходу на протокол TCP/IP, и абсолютное большинство VPN решений поддерживают именно его.

## 5. По уровню сетевого протокола:

По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели OSI.

### 1.5 Основные виды VPN-соединений

Повышенный интерес к виртуальным частным сетям обусловлен тем, что организациям необходимо снижать расходы на содержание корпоративных сетей за счет более дешевого подключения удаленных офисов и удаленных пользователей через сеть Интернет.

Однако, стоит заметить, что при объединении сетей через «Интернет», сразу возникает вопрос о безопасности передаваемых данных, поэтому и возникает необходимость создания механизмов, позволяющих обеспечить

конфиденциальность и целостность передаваемой информации. Сети, построенные на базе таких механизмов, называются VPN.

Пример построения виртуальной частной сети представлен на рисунке 2:

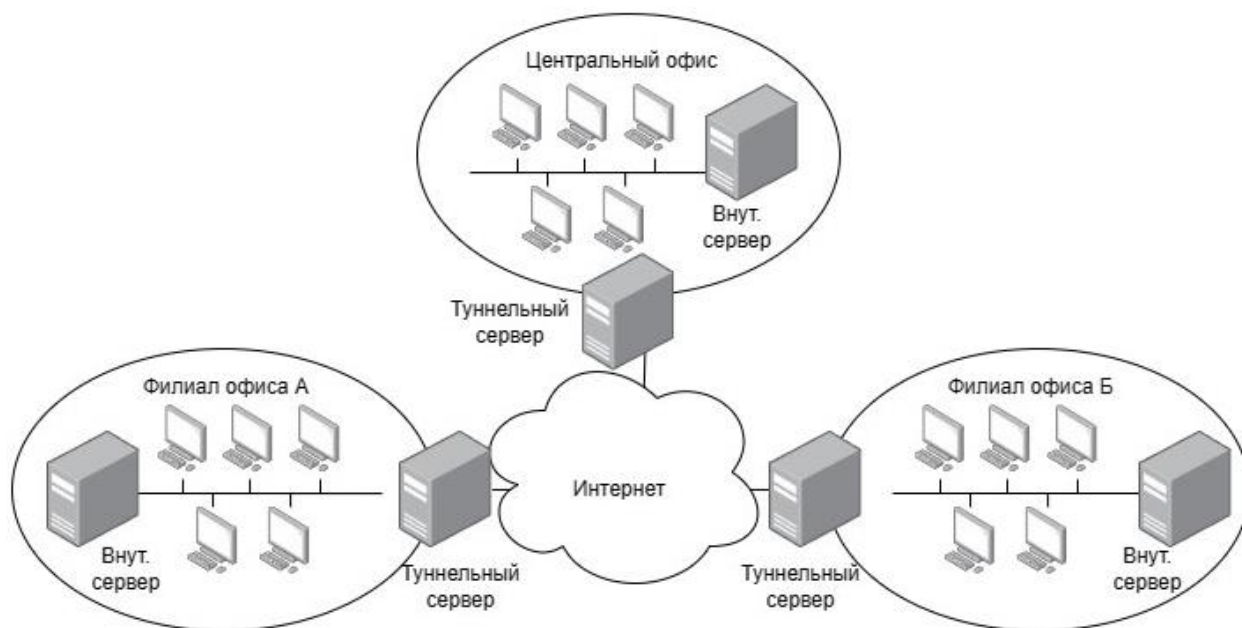


Рисунок 2 – Пример построения VPN

Структура VPN включает в себя каналы глобальной сети, защищенные протоколы и маршрутизаторы.

Для объединения удаленных локальных сетей в виртуальную сеть организации используются «виртуальные выделенные каналы». Инициатор туннеля инкапсулирует пакеты локальной сети в новые IP-пакеты, содержащие в своем заголовке адрес инициатора туннеля и адрес конечного пользователя (терминатора) туннеля. На противоположном конце терминатором туннеля производится обратный процесс извлечения исходного пакета.

При осуществлении такой передачи необходимо учитывать вопросы целостности и конфиденциальности данных, которые невозможно обеспечить туннелированием, без шифрования. Для достижения конфиденциальности передаваемой корпоративной информации необходимо использовать некоторый алгоритм шифрования, причем одинаковый на концах туннеля.

Для того, чтобы была возможность создания VPN на базе оборудования и программного обеспечения от различных производителей необходим некоторый стандартный механизм. VPN могут строиться на базе различных протоколов, которые реализуют этот механизм.

VPN на базе протокола Internet Protocol Security (IPSec). Он описывает все стандартные методы VPN. Этот протокол определяет методы идентификации при инициализации туннеля, методы шифрования, используемые конечными точками туннеля и механизмы обмена и управления ключами шифрования между этими точками. Из недостатков этого протокола можно выделить то, что

он ориентирован на протокол IP. Протокол IPSec тесно связан с протоколом IKE (Internet Key Exchange), позволяющим обеспечить передачу информации по туннелю и решить задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами в то время, как IPSec кодирует и подписывает пакеты;

VPN на базе протокола PPTP (Point-to-Point Tunneling Protocol). Туннельный протокол типа “точка-точка”, позволяющий компьютеру устанавливать защищенное соединение с сервером за счет создания специального туннеля в стандартной, незащищенной сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, такой как «Интернет». Протокол считается менее безопасным, чем IPSec. PPTP работает, устанавливая обычную PPP сессию с противоположной стороной с помощью протокола GRE (Generic Routing Encapsulation). Второе соединение на TCP-порту 1723 используется для инициализации и управления GRE-соединением. PPTP сложно перенаправлять за межсетевой экран, так как он требует одновременного установления двух сетевых сессий.

VPN на базе протокола OpenVPN. OpenVPN – это свободная реализация технологии виртуальной частной сети с открытым исходным кодом для создания зашифрованных каналов типа «точка-точка» или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за границами NAT и межсетевым экраном, без необходимости изменения их настроек. Для обеспечения безопасности управляющего канала и потока данных OpenVPN использует библиотеку OpenSSL. OpenVPN проводит все сетевые операции через TCP или UDP транспорт.

VPN на базе протокола L2TP (Layer 2 Tunneling Protocol). Протокол туннелирования второго уровня используется для поддержки виртуальных частных сетей. Главное его достоинство в том, что он позволяет создавать туннель не только в IP сетях, но и в таких, как ATM, X.25 и FrameRelay.

## 1.6 Оборудование, реализующее VPN соединение

Существуют различные варианты построения VPN. При выборе решения требуется учитывать факторы производительности средств построения VPN. Для построения VPN-соединения лучше всего использовать специализированное оборудование.

### 1.6.1 Виртуальная частная сеть на базе межсетевых экранов

Межсетевые экраны многих производителей поддерживают функцию туннелирования и шифрования данных. Такие продукты обычно основаны на том, что если трафик проходит через межсетевой экран, то его можно зашифровать. Для этого к программному обеспечению меж сетевого экрана добавляется модуль шифрования. Однако недостатком этого подхода можно назвать зависимость производительности от аппаратного обеспечения, на котором работает межсетевой экран. Если межсетевой экран используется на

базе персональных компьютеров, то необходимо помнить, что такое решение можно применять только для небольших сетей с невысоким объемом передаваемой информации. Тем не менее, использование межсетевых экранов с поддержкой шифрования успешно используется для обеспечения безопасности информации, передаваемой через общедоступные сети.

#### 1.6.2 Виртуальная частная сеть на базе маршрутизаторов

Другим способом построения VPN является применение для создания защищенных каналов маршрутизаторов. Так как вся информация, исходящее из локальной сети, проходит через маршрутизатор, то целесообразно возложить на этот маршрутизатор и задачи шифрования. Преимуществами такой настройки VPN являются защита нескольких устройств одновременно, отсутствие необходимости настройки программного обеспечения VPN на каждом устройстве – достаточно настроить VPN на самом маршрутизаторе.

#### 1.6.3 Виртуальная частная сеть на базе программного обеспечения

Следующим подходом к построению VPN являются программные решения. При реализации такого решения используются специализированные программное обеспечение, которая работает на выделенном компьютере и в большинстве случаев выполняет роль прокси-сервера. Компьютер с таким программным обеспечением может быть расположен за межсетевым экраном.

#### 1.6.4 Виртуальная частная сеть на базе сетевой ОС

Решение на базе сетевой операционной системы можно рассмотреть на примере системы Windows NT компании Microsoft. Для создания VPN Microsoft используют протокол PPTP, который интегрирован в систему Windows NT. Данное решение очень привлекательно для организации использующих Windows в качестве корпоративной операционной системы. Важно отметить, что стоимость подобного решения значительно ниже стоимости прочих решений. Для шифрования трафика используется нестандартный протокол Microsoft Point-to-Point Encryption с 40 или 128-битным ключом.

### 1.7 Оборудование для реализации VPN, их описание

Для создания эффективного и безопасного VPN-соединения между главным офисом и филиалом ПАО «Банк» необходимо правильно подобрать соответствующее оборудование. Важно учесть такие аспекты, как производительность, безопасность и масштабируемость сетевых решений. Выбор конкретного оборудования зависит от масштаба сети, требований безопасности и бюджета организации. Важно помнить о том, что правильно спроектированная инфраструктура обеспечит надежное и безопасное соединение и обеспечит эффективную работу организации.

Для организации защищенного канала связи были подобраны следующие варианты программно-аппаратного оборудования:

1. Аппаратная платформа Ideco MX Cert – высокопроизводительное устройство, специализирующееся на обеспечении безопасности и управлении идентификацией в корпоративной среде. Он объединяет в себе несколько функций, включая аутентификацию, управление доступом, контроль и аудит действий пользователей, что позволяет организациям эффективно управлять безопасностью своих информационных ресурсов. Платформа обеспечивает надежную защиту конфиденциальности данных и ресурсов, используя передовые методы шифрования и механизмы контроля доступа;

2. Межсетевой экран Usergate – программно-аппаратный комплекс, предназначенный для обеспечения безопасности сетевого трафика организации. Он обеспечивает гибкое управление доступом к сетевым ресурсам, позволяя администраторам определять правила доступа на основе различных параметров, таких как IP-адреса, порты, протоколы. Также Usergate выполняет роль межсетевого экрана, обеспечивая фильтрацию и контроль трафика между различными сетями, а также маршрутизацию данных внутри организации, что позволяет оптимизировать сетевую инфраструктуру и обеспечить безопасное взаимодействие между внутренними и внешними сетями;

3. Межсетевой экран Diamond VPN/FW – комплексное решение для обеспечения безопасности сетевого трафика и управления сетью. Обеспечивает защиту сети от внешних угроз, фильтрацию трафика, позволяет организовать защищенное соединение между удаленными сетями и устройствами через Интернет, что обеспечивает конфиденциальность и целостность данных при их передаче. Продукт обеспечивает шифрование данных, передаваемых через VPN-канал. Diamond VPN/FW является мощным решением для обеспечения безопасности и эффективного управления корпоративной сетью, особенно в условиях удаленной работы и распределенных офисов;

4. АПКШ «Континент» 3.9 IPC-10 – современное интегрированное решение для построения и управления сетевой инфраструктурой, обладает высокой производительностью и масштабируемостью, что позволяет обрабатывать большие объемы сетевого трафика. Продукт легко интегрируется с существующими сетевыми устройствами и инфраструктурой, что позволяет его использовать в совокупности с уже существующим оборудованием;

5. xFirewall 5 – современный межсетевой экран, предназначенный для обеспечения безопасности и контроля доступа в корпоративных и сетевых средах. Обеспечивает высокоэффективную фильтрацию сетевого трафика.

Для использования был выбран именно АПКШ «Континент» 3.9. Выбор именно этого оборудования обусловлен требованием Заказчика провести тестирование канала в установленные сроки и обозначенной только компанией «Код Безопасности» готовностью предоставить безвозмездно на тесты соразмерное решение. Преимуществом комплекса является то, что он является отечественным продуктом, использование только отечественных алгоритмов шифрования, а именно ГОСТ 34.12-2018, а также имеет сертификаты ФСТЭК и ФСБ, действующие до сентября 2027 года и апреля 2026 года соответственно.



### 1.8 Возможности АПКШ Континент 3.9

Компания «Код Безопасности» - российская IT-компания, основной сферой деятельности которой является разработка средств защиты информации. Компания известна не только среди частных пользователей, но и крупных государственных и коммерческих организаций благодаря разрабатываемому программному и аппаратному обеспечению, которое подходит для всех классов защищенности информационных систем. Решения этой компании задействованы в Министерстве обороны РФ, ФНС России, «РЖД» и других. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, среды виртуализации, коммерческой и государственной тайны.

Аппаратно-программный комплекс шифрования «Континент» 3.9 – продукт компании «Код Безопасности», централизованный комплекс для защиты сетевой инфраструктуры и создания VPN-сетей и использованием алгоритмов ГОСТ. Представляет собой современное программное обеспечение, которое обеспечивает безопасность при подключении пользователей к общедоступным сетям с помощью создания частных виртуальных сетей и детектора атак. Комплекс обладает высокопроизводительной платформой и поддерживает самые современные коммуникационные приложения. С помощью АПКШ «Континент» возможно создание защищенного доступа для удаленных пользователей к защищенным ресурсам, а также использовать комплекс как программно-аппаратный модуль для выявления сетевых атак.

Комплекс реализует следующие основные функции:

1. криптографическая защита данных, передаваемых по каналам связи общих сетей передачи данных между составными частями VPN;
2. предоставление доступа удаленным пользователям к ресурсам защищаемой сети;
3. межсетевое экранирование;
4. автоматическая регистрация событий, связанных с функционированием комплекса;
5. централизованное управление компонентами комплекса, который предназначен для работы в сетях, использующих для передачи данных протоколы семейства TCP/IP версии 4, а также в общих сетях передачи данных, поддерживающих протоколы IPv6.

В состав АПКШ "Континент" входят следующие компоненты:

1. криптографический шлюз;
2. ЦУС;
3. программа управления ЦУС;
4. клиент аутентификации пользователя.

Компоненты комплекса можно устанавливать как на аппаратных, так и на виртуальных платформах.

### 1.9 Изучение и анализ требований и ограничений по использованию АПКШ «Континент» 3.9

Перед началом использования АПКШ необходимо изучить требования к использованию из формуляров по следующим причинам:

1. проверка совместимости с существующей инфраструктурой: перед внедрением нового оборудования важно удостовериться, что оно совместимо с существующей инфраструктурой организации, что помогает предотвратить возможные конфликты с другими системами и обеспечивает корректную и бесперебойную работу;

2. оценка эффективности и производительности: исследование требований позволяет оценить эффективность и производительность оборудования, что важно для обеспечения соответствия системы потребностям и ожиданиям организации в области защиты передаваемых данных;

3. решение о необходимости обучения сотрудников: проверка требований также включает оценку необходимости обучения персонала и наличия поддержки со стороны поставщика. Это гарантирует, что сотрудники организации смогут эффективно использовать и поддерживать внедренный программно-аппаратный комплекс.

Требования и ограничения по использованию АПКШ «Континент» 3.9 представлены в таблице 6:

Таблица 6 - Требования и ограничения по использованию АПКШ «Континент» 3.9

Требование из нормативных документов	Возможные реализуемые меры
АПКШ Континент 3.9 Формуляр RU.88338853.501430.022 30	
<p>П.4.5: Комплекс обеспечивает выполнение заявленных функций при реализации на предприятии (в организации) следующих ограничений по применению:</p> <p>1. реализация защиты от электромагнитного, акустического и других видов излучения, в том числе проведение специальных исследований технических средств;</p> <p>2. обеспечение условий хранения и распространения носителей ключевой информации, исключающих возможность компрометации ключей;</p> <p>3. обеспечение сохранности оборудования и физической целостности системных блоков компьютеров;</p>	<p>Проведение специальных исследований технических средств по внутренним регламентам компании</p>

Требование из нормативных документов	Возможные реализуемые меры
<p>4. обеспечение свободной от вирусов программной среды компьютеров; обеспечение контроля изменения прикладной программной среды, исключение ввода в компьютеры программных средств без их предварительной гарантированной проверки.</p>	
<p>АПКШ Континент 3.9 Правила пользования RU.88338853.501430.022 99</p>	
<p>П.3.6: Помещение, в котором устанавливается комплекс, должно быть аттестовано в соответствии с руководящими документами специально созданной комиссией. Результатом работы комиссии является акт проверки выделенного помещения для работы с комплексом, утвержденный начальником организации-пользователя.</p>	<p>Проведение аттестации помещения в соответствии с нормативными документами организации</p>
<p>П.3.7: Порядок допуска в помещение определяется внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры организации, использующей комплекс, с учетом хранения ключевой информации на КШ.</p>	<p>Проверка наличия Инструкции по организации доступа в помещения или иного документа, регламентирующего порядок доступа в помещения</p>
<p>П.3.11: Должны быть предприняты меры, препятствующие несанкционированному вскрытию системных блоков компьютеров, входящих в состав комплекса, то есть системные блоки должны быть опечатаны специально выделенной для этих целей печатью. Наряду с этим допускается применение других средств контроля доступа к комплексу</p>	<p>Проверка опечатывания СКЗИ</p>
<p>П.3.13: Должны быть предприняты меры, которые определяются внутренней инструкцией, исключающие несанкционированный доступ к комплексу лиц, по роду своей деятельности не являющихся персоналом</p>	<p>Проверка наличия Инструкции по организации доступа в помещения или иной документ регламентирующий доступ в помещение, где хранится/эксплуатируется СКЗИ.</p>

Требование из нормативных документов	Возможные реализуемые меры
с правами администратора, допущенным к работе с комплексом.	
П.3.17: Порядок действий при обнаружении вскрытия системного блока компьютера комплекса должен определяться регламентами организации, эксплуатирующей комплекс, и быть прописан во внутренних инструкциях.	Проверка регламентации порядка при обнаружении вскрытия системного блока компьютера АПКШ Континент 3.9 и внесение порядка во внутренние инструкции, регламенты и т.д.
П.7.3: При установке параметров, позволяющих создавать криптографически незащищенные соединения, должны быть приняты меры, исключающие утечку требующей защиты информации с защищаемого объекта информатизации. Проверка достаточности принятых мер защиты проводится при аттестации объекта информатизации с АПКШ «Континент» по требованиям информационной безопасности.	Проведение аттестации объекта информатизации в случае установки параметров, позволяющих создавать криптографически незащищенные соединения (необходимо использовать только защищенные соединения, исключить незащищенный (открытый) трафик)

### 1.10 Вывод по разделу

В данном разделе были решены крайние три задачи, поставленные для достижения цели выпускной квалификационной работы, а также рассмотрены следующие вопросы:

- описаны возможности VPN туннелирования;
- произведен сравнительный анализ оборудования, с помощью которого можно организовать VPN туннелирование, используя метод иерархий. Выбран вариант АПКШ «Континент» 3.9;
- описан выбранный для дальнейшего исследования и использования вариант защиты распределенной сети организации;

Проанализировав все возможные варианты построения виртуальных частных сетей, можно сделать вывод, что построение на базе комбинированного решения, то есть на базе программно-аппаратного комплекса, будет наиболее успешным вариантом. Недостаток его относительно высокой стоимости компенсируется многообразием выполняемых функций комплекса и гарантированной защиты путем шифрования по отечественным стандартам. Наличие сертификатов также является признаком его надежной и эффективной работы.

## 2 Проектная часть

### 2.1 Постановка задачи

Главной задачей работы является организация зашифрованного канала между офисами банковской организации, для чего будет использоваться аппаратно-программный комплекс шифрования «Континент».

### 2.2 Анализ построения сети до и после внедрения комплекса

Для построения схем сети, процесса аутентификации пользователей, взаимодействия ПО для аутентификации пользователей с центром управления сетью, процесс сбора агентом ЦУС и СД записей журналов событий, а также для визуализации взаимодействия компонентов аппаратно-программного комплекса шифрования «Континент» будет использоваться онлайн-сервис Draw.io.

Draw.io – бесплатный онлайн-сервис для создания диаграмм, предоставляющий удобный и интуитивно понятный интерфейс, который позволяет пользователям создавать и редактировать различные типы диаграмм непосредственно в веб-браузере. Draw.io предоставляет возможность создания UML (Unified Modeling Language) диаграмм, которые используются для визуализации, конструирования и документирования программных систем. Сервис предоставляет множество инструментов для создания различных типов UML диаграмм, таких как диаграммы классов, вариантов использования, компонентов, последовательностей, а также имеет обширную библиотеку предопределенных элементов, таких как узлы сети, маршрутизаторы, коммутаторы и другие сетевые устройства, что делает процесс создания схем более удобным и эффективным.

До внедрения аппаратно-программного комплекса шифрования для связи главного офиса и филиала банковской организации использовалась технология VPN MPLS. Сеть MPLS VPN разделена на магистраль провайдера и IP-сети клиентов. При такой организации VPN доставка трафика до пограничного устройства сети провайдера осуществляется с помощью протокола IP, а внутри сети провайдера – с помощью MPLS.

Преимуществами такой организации виртуальной частной сети является масштабируемость, которая достигается за счет подключения нового узла в существующую виртуальную частную сеть только перенастройкой одного оборудования провайдера, к которому подключается данный узел, возможность пересечения адресных пространств и узлов, подключенных в различные VPN, а также изолирование трафика VPN друг от друга на втором уровне модели OSI (Open System Interconnection).

Масштабируемость является крайне полезным свойством для виртуальных частных сетей, так как зачастую такие сети нуждаются в

расширении с ростом бизнеса предприятия. Также сети VPN должны быть управляемыми для того, чтобы обеспечить возможность их оперативного конфигурирования и контроля в соответствии с постоянно меняющимися бизнес-процессами предприятий клиентов.

Многопротокольная коммутация меток представляет собой технологию продвижения пакетов, которое происходит на основании «меток», для чего в заголовок добавляется блок данных, в котором и содержится метка, на основании которой и принимается решение о дальнейшем перемещении пакета.

Когда пакет IP достигает магистрали на базе MPLS, он в первую очередь классифицируется – по адресу назначения или по принадлежности к определенной клиентской виртуальной частной сети, затем снабжается одной или несколькими метками и направляется дальше. На каждом транзитном уровне верхняя метка заменяется на новую, после чего пакет передается следующему маршрутизатору.

О метках и значениях соседние устройства договариваются при помощи протокола LDP (Label Distribution Protocol). Благодаря такому согласованию соседних маршрутизаторов отпадает необходимость централизованного механизма управления метками.

Ядро сети строится на базовых маршрутизаторах MPLS, называемых внутренними маршрутизаторами провайдера P и не взаимодействует с пользователем VPN напрямую. Взаимодействие происходит за счет соединения между граничным устройством маршрутизации заказчика CE (Customer Edge Router) и граничным устройством маршрутизации провайдера PE (Provider Edge Router).

Устройства маршрутизации заказчика могут быть статически соединены к устройствам маршрутизации провайдера через закрепленные каналы или могут использовать коммутируемые линии связи. При этом при подключении CE и PE могут задействоваться каналы любого типа, а также механизмы туннелирования.

Эталонная модель MPLS VPN представлена на рисунке 3:

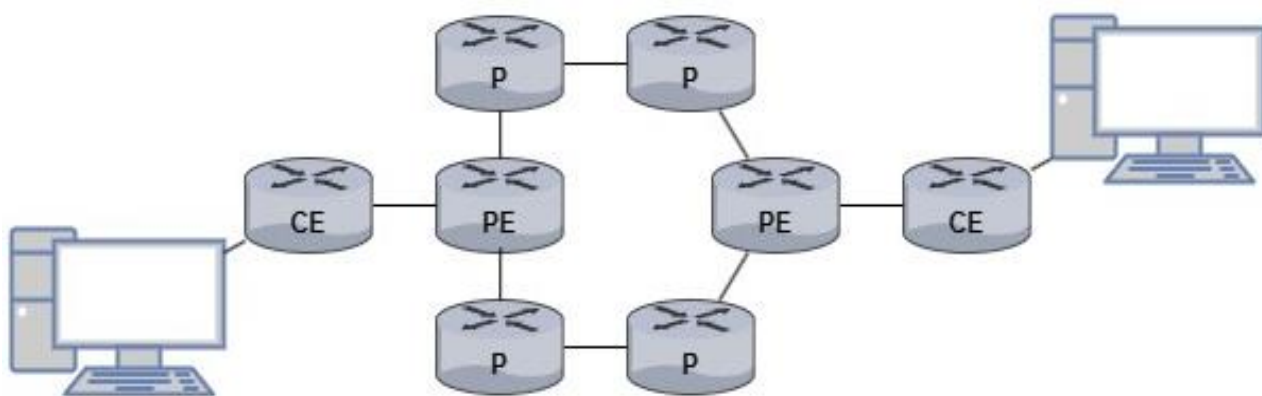


Рисунок 3 – Эталонная модель MPLS VPN

На рисунке 4 представлен сегмент сети до внедрения аппаратно-программного комплекса шифрования «Континент» в г. Екатеринбурге:

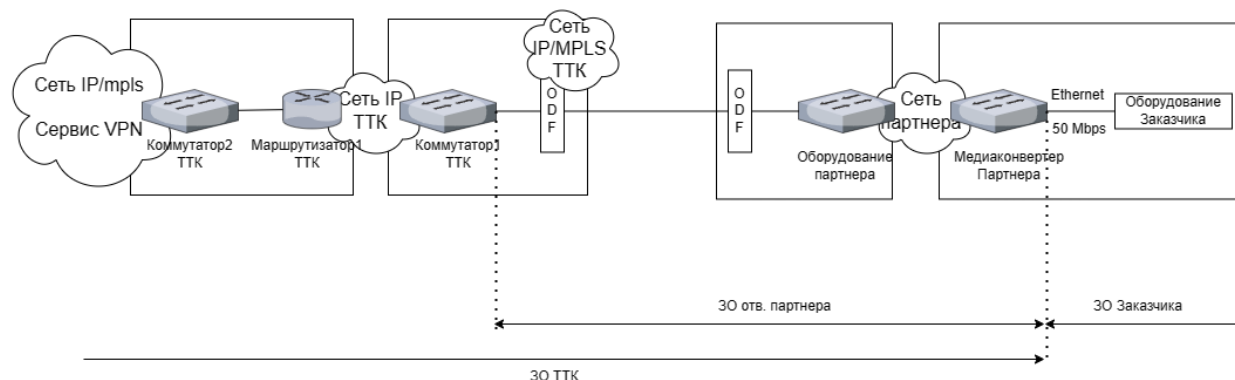


Рисунок 4 – Сегмент сети в г. Екатеринбурге до внедрения комплекса шифрования

Важно отметить, что MPLS VPN, используемый для связи между главным офисом и филиалом банковской организации, сам по себе не предоставляет механизмы шифрования передаваемых данных, что означает, что информация может быть уязвима для перехвата и неправомерного доступа. Эта недостаточная защита передаваемых данных становится одной из главных причин для модернизации существующей сети.

В ответ на эту уязвимость банковская организация совместно с АО «Компания ТТК» приняла решение о внедрении дополнительного механизма безопасности – шифрования трафика с помощью программно-аппаратного комплекса шифрования «Континент» от компании «Код Безопасности», который предоставляет надежное и эффективное оборудование для обеспечения конфиденциальности и целостности данных при их передаче.

Изначально для организации связи между филиалом и главным офисом банковской организации «Компания ТТК» использовала услуги партнера, который выступал в качестве поставщика услуг связи для клиентов в этом регионе. Однако внедрение АПКШ «Континент» позволяет исключить его участие, так как это снижает вероятность возникновения проблем, связанных с недоступностью услуг провайдера или сетевых сбоев, что значительно повышает надежность и устойчивость сети.

Модернизация сети играет ключевую роль в повышении эффективности и надежности инфраструктуры как для АО «Компания ТТК», так и для ПАО «Банк», так как она позволяет сэкономить средства за счет отказа от услуг ответственного партнера в г. Екатеринбурге. Модернизация позволит снизить компаниям операционные расходы, что позволяет перераспределить ресурсы на другие направления развития. Также новая инфраструктура обеспечит полный контроль над всей сетью.

Такое централизованное управление сетью позволяет мониторить и реагировать на любые потенциальные угрозы или аномалии в реальном времени. Модернизированная схема сети представлена на рисунке 5:

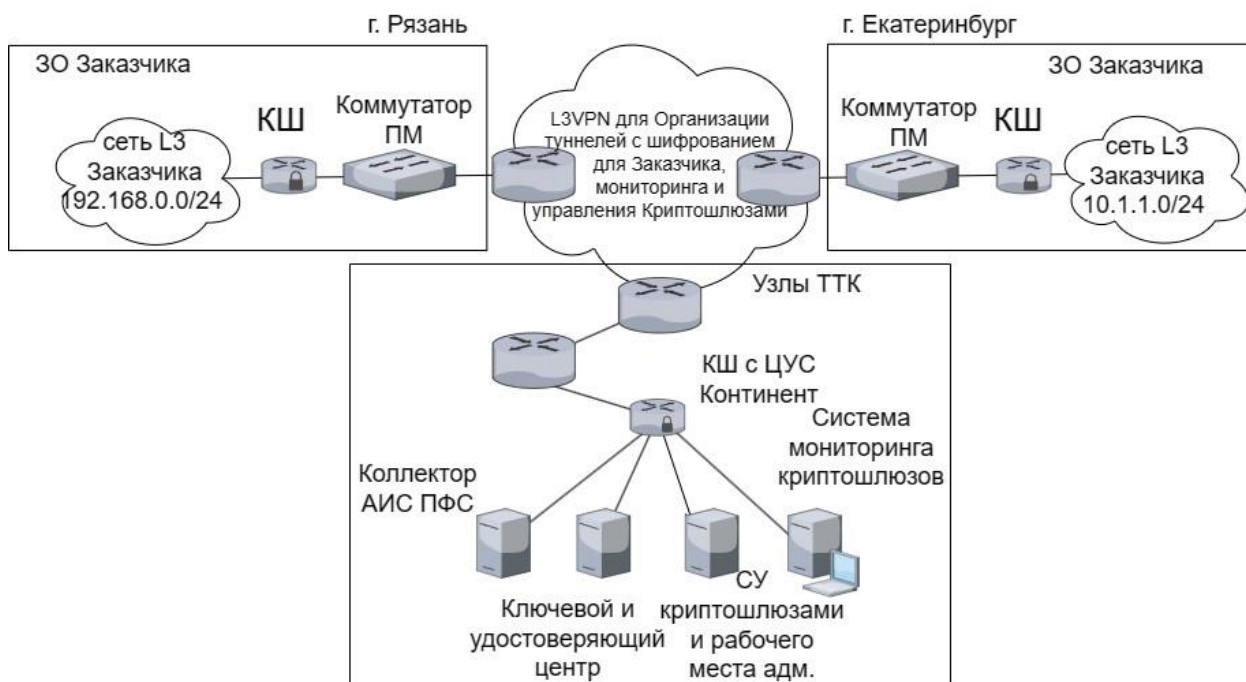


Рисунок 5 – Схема построения сети

### 2.3 Диаграмма компонентов криптографического шлюза

Криптографический шлюз играет ключевую роль в обновленной схеме построения сети между главным офисом банковской организации, именно он обеспечивает защищенную передачу данных. Понимание его компонентов и функций крайне важно для обеспечения высокого уровня защиты передаваемых данных, а также эффективной настройки и управления сетью в целом.

Для визуализации компонентов криптографического шлюза была разработана диаграмма компонентов (рисунок 6), были выделены следующие компоненты:

а. Модуль генерации и управления ключами – компонент, отвечающий за создание, хранение и управление криптографическими ключами, необходимыми для шифрования и расшифрования передаваемых данных. Генерация ключей подразумевает собой процесс создания криптографических ключей, используемых для шифрования и расшифрования данных, что включает в себя выбор подходящих алгоритмов шифрования и параметров ключей. Созданные ключи хранятся в защищенном хранилище для предотвращения их утечки или несанкционированного доступа. Управление ключами подразумевает собой механизмы для эффективного управления всеми этапами жизненного



цикла ключей (создание, использование, обновление, уничтожение), включая их ревокацию в случае утечки или угрозы компрометации;

б. Шифровальный процессор – компонент криптографического шлюза, обеспечивающий высокую скорость и эффективность шифрования и расшифрования передаваемых данных. Обладает высокой вычислительной мощностью, необходимой для выполнения сложных алгоритмов шифрования в реальном времени, поддерживает широкий спектр криптографических алгоритмов, обеспечивает механизмы для эффективного управления криптографическими ключами. Процессор обеспечивает аппаратную защиту от различных атак, таких как атаки физического воздействия. Процессор взаимодействует с другими компонентами криптографического шлюза для обеспечения согласованной и безопасной работы всей системы;

в. Конфигурация – компонент шлюза, определяющий его функциональность, настройки и параметры работ. Конфигурация определяет параметры безопасности, такие как метод шифрования, аутентификация и управление доступом, а также сетевые параметры: конфигурация сетевых интерфейсов, VLAN (Virtual Local Area Network), маршрутизацию и ее протоколы. Также с помощью конфигурации определяются такие параметры производительности, как размеры буферов, сжатие данных и механизмы оптимизации трафика, параметры мониторинга и журналирования;

г. Управляющая и мониторинговая система – обеспечивает эффективное управление, контроля и мониторинга работы шлюза. Такая система позволяет администраторам комплекса управлять конфигурацией, отслеживать производительность шлюза, обнаруживать и предотвращать атаки, аномальное поведение системы и нарушения политики безопасности. Система обеспечивает осуществление управления обновлениями программного обеспечения, а также откаты изменений в случае возникновения ошибок;

д. Средства защиты от атак и «взлома» – компонент криптографического шлюза, обеспечивающий его механизмами аутентификации и авторизации для предотвращения несанкционированного доступа к системе, а также механизмами регистрации событий, обнаружения аномалий;

е. Интерфейсы подключения – компонент, обеспечивающий взаимодействие криптографического шлюза с внешними и внутренними сетями и устройствами, удаленное управление и настройку криптографического шлюза, взаимодействие с системами безопасности, такими как аутентификации пользователей, системы управления доступом;

ж. Центр управления сетью – важный компонент криптографического шлюза, предоставляющий централизованный контроль и управление всеми компонентами его работы, обеспечивает постоянный мониторинг работы шлюза, анализ его производительности, загрузки ресурсов, сетевого трафика. ЦУС позволяет отслеживать безопасность сетевого периметра, обнаруживать и анализировать потенциальные уязвимости;

з. База данных – компонент криптографического шлюза с установленным на него центром управления сетью. В базе данных хранятся все

содержимое журналов с сетевых объектов, которые передаются на ЦУС с помощью агента по заданному расписанию или специальной команде. События, связанные с работой агента ЦУС также регистрируются в отдельном журнале приложения. Также в базе данных хранится информация о зарегистрированных пользователях.

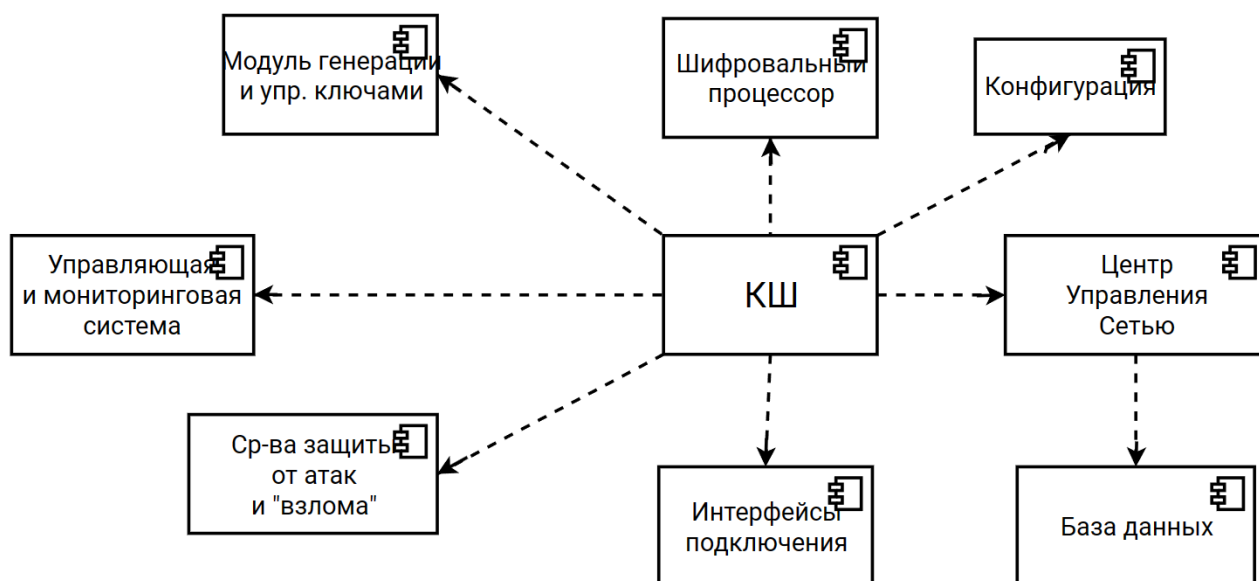


Рисунок 6 – Диаграмма компонентов КШ

#### 2.4 Схема процесса сбора записей журналов событий

Каждый криптографический шлюз, используемый в системе, локально сохраняет у себя в буфере записи журналов до момента их передачи на центр управления сетью.

Такой подход гарантирует надежное хранение данных даже в случае временной недоступности связи с центром управления.

Процесс выгрузки записей журналов осуществляется агентом ЦУС и СД по заданному расписанию, либо по специальной команде от администратора, что обеспечивает своевременное и систематическое обновление данных в базе данных ЦУС, а также оперативно реагировать на инциденты и проводить аудит.

Для наглядного отслеживания каждого этапа процесса передачи записей журналов событий в базу данных журналов компонентов комплекса была разработана схема, которая позволяет наглядно отслеживать каждый этап процесса: от накопления данных в буфере криптографического шлюза до их сохранения в централизованной базе данных, представленная на рисунке 7:

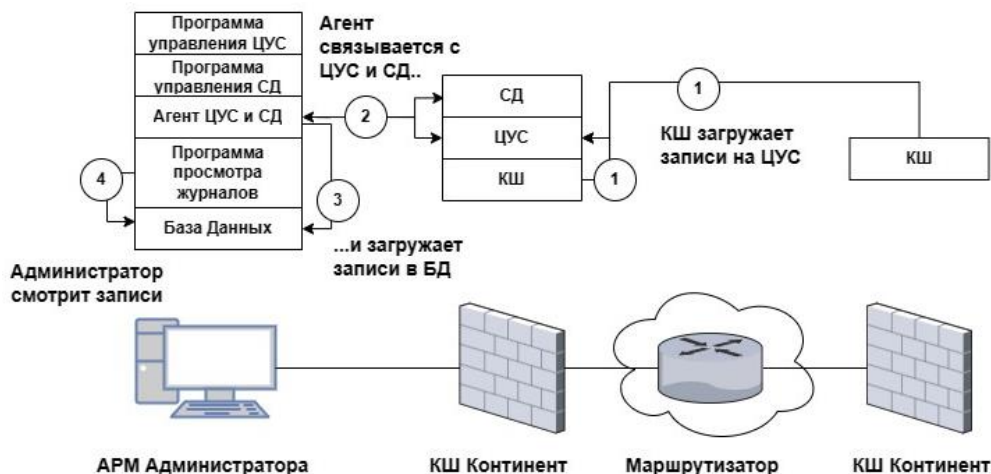


Рисунок 7 – Процесс сбора записей журнала событий агентом ЦУС и СД

## 2.5 Схема аутентификация и авторизация пользователей

Идентификация и аутентификация пользователей, которые работают на компьютерах в защищенной сети криптографических шлюзов, выполняются с помощью программы «Континент. Аутентификация пользователя», установленной на компьютере пользователя с помощью протокола CHAP.

Регистрация пользователей выполняется средствами программы управления центром управления сетью, при регистрации пользователей присваиваются имя и пароль, которые в дальнейшем пользователи указывает при аутентификации на своей рабочей станции. Схема аутентификации и схема взаимодействия ПК пользователя с криптографическим шлюзом представлены на рисунке 8 и рисунке 9.

Протокол проверки подлинности с вызовом по рукопожатию CHAP (Challenge Handshake Authentication Protocol) – протокол аутентификации по протоколу PPP, разработанный IETF (Internet Engineering Task Force). Он используется при первоначальном запуске канала, а также выполняет периодические проверки, чтобы удостовериться, что система обменивается данными с тем же хостом.

Для инициализации процесса аутентификации по протоколу CHAP сервер доступа после установления сеанса связи высылает хосту пакет LCP, который указывает на необходимость применения протокола CHAP, а также требуемого алгоритма хэширования. Если устройство поддерживает предложенный алгоритм хэширования, то он должен ответить пакетом LCP о согласии с предложенными параметрами. В противном случае выполняется обмен пакетами LCP для согласования алгоритма хэширования.

Протокол использует 3-сторонний протокол подтверждения связи. Сначала аутентификатор отправляет пакет запроса одноранговому узлу, затем одноранговый узел отвечает значением, используя свою одностороннюю хэш-функцию. Затем аутентификатор сопоставляет полученное значение со своим

собственным вычисленным хэш-значением. Если значения совпадают, то аутентификация подтверждена, в противном случае соединение будет прервано.

Протокол использует одностороннюю хеш-функцию, называемую MD5 и обеспечивает большую безопасность, чем процедура проверки паролем PAP (Password Authentication Procedure), поскольку используемое значение, которое определяется с помощью хэш-функции, может изменяться.

Существует четыре типа пакета CHAP:

1. Пакет запроса – пакет, отправляемый аутентификатором одноранговому узлу в начале трехстороннего «рукопожатия» CHAP. Пакет запроса также периодически отправляется для проверки того, не изменено ли соединение. Он содержит значение идентификатора, поле значения, которое содержит случайное значение, а также содержит поле имени, в котором содержится имя аутентификатора. Поле имени используется для поиска пароля, а также передается в генератор хэша MD5, и генерируется одностороннее хэш-значение;

2. Пакет ответа – пакет, используемый для ответа на пакет запроса. Он содержится в поле, содержащее сгенерированное одностороннее хэш-значение, значение идентификатора и поле имени. В поле имени пакета ответа задается имя хоста однорангового маршрутизатора. Теперь в поле имени пакета запроса выполняется поиск пароля. Маршрутизатор ищет запись, которая соответствует имени пользователя в поле имени пакета запроса, и получает пароль. Затем этот пароль хэшируется путем отправки его в генератор хэша MD5, и генерируется одностороннее хэш-значение. Это значение вставляется в поле значения пакета ответа и отправляется аутентификатору;

3. Пакет успешного соединения – теперь аутентификатор также выполняет то же самое, просматривая в поле имени (если в нем есть запись для этого имени пользователя) ответный пакет и используя его, генерирует хэш-значение. Если сгенерированное значение совпадает с значением однорангового узла, то отправляется пакет, сигнализирующий об успешной установке соединения;

4. Пакет сбоя – если сгенерированное значение отличается, то пакет сбоя отправляется одноранговому узлу.

Протокол CHAP обеспечивает строгую аутентификацию, запрашивая у пользователя случайно сгенерированную строку запроса, которая изменяется с каждым новым сеансом, гарантируя, что пользовательский пароль или секретный ключ не передаются по сети.

Протокол является безопасным протоколом аутентификации, так как он использует одностороннюю хэш-функцию для шифрования строки пароля и запроса, что значительно затрудняет возможность перехвата и расшифровки учетных данных пользователей.

CHAP является масштабируемым протоколом проверки подлинности, поскольку он может обрабатывать большое количество пользователей и устройств в сети.

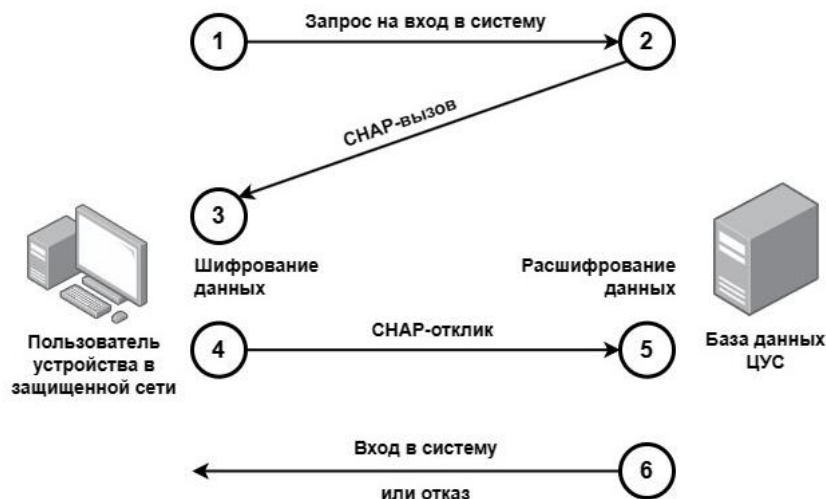


Рисунок 8 – Схема аутентификации по протоколу СНАР

Аутентификация возможна только на тех компьютерах, которые подключены к внутренним интерфейсам КШ. Аутентификация пользователя на компьютерах, подключенных к внешнему интерфейсу КШ, не выполняется.

Обмен данными между КШ и подключаемым компьютером осуществляется по протоколу TCP по порту 4446 (рисунок 9). Клиент аутентификации устанавливает подключение со случайного порта 1024-65535 на порт ЦУС 4446. ЦУС отвечает на тот же порт, с которого отправлялось обращение.

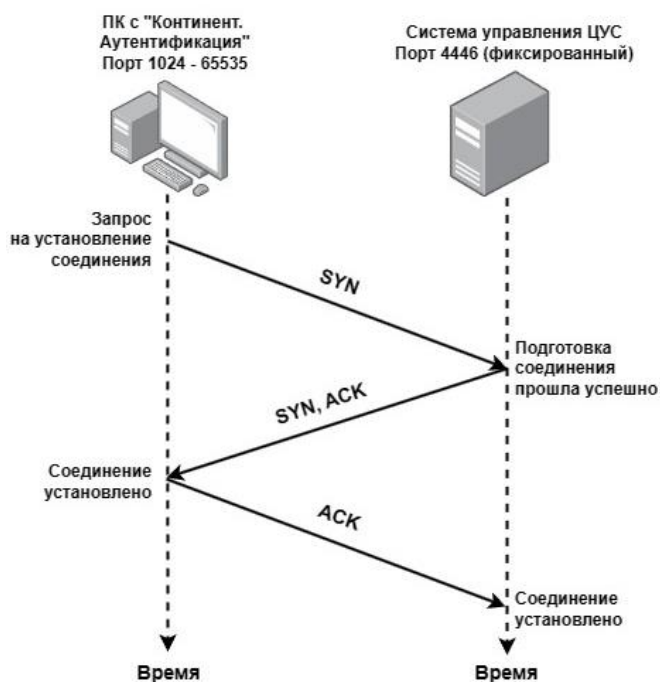


Рисунок 9 – Взаимодействие ПК с программой «Континент. Аутентификация пользователей» с ЦУС

## 2.2 Вывод по проектной части

В данном разделе был проведен анализ изначально построенной и модернизированной схем сети, разработаны и представлены диаграмма компонентов, схема аутентификации пользователей с помощью программы «Аутентификация пользователей», схема взаимодействия компьютера с установленной программой для аутентификации пользователей и криптографическим шлюзом с ЦУС, также была выполнена задача, поставленная для достижения цели выпускной квалификационной работы, а именно: разработана схема сети, согласно которой будет производиться шифрование трафика.

### 3 Технологическая часть

#### 3.1 Инициализация ЦУС и СД

Центр управления сетью является программным обеспечением, установленным на одном из криптографических шлюзов аппаратно-программного комплекса.

Для инициализации ЦУС требуется клавиатура, монитор для подключения к системному блоку криптографического шлюза, а также USB-накопитель для того, чтобы записать на него идентификаторы администратора АПКШ «Континент». Перед началом работы была подготовлена информация об IP-адресе маршрутизатора по умолчанию, выделены адреса для внешнего и внутреннего интерфейса криптографического шлюза. После проверки целостности файлов установленного программного обеспечения была выполнена загрузка операционной системы.

В ходе инициализации ЦУС был выбран внешний интерфейс – публичный интерфейс, по которому могут обращаться пользователи из сети общего доступа, через который будет передаваться весь зашифрованный трафик, внутренний интерфейс – интерфейс, который принадлежит защищаемой сети криптографического шлюза, либо используется в качестве промежуточной сети к другим защищаемым сетям, указан внешний и внутренний IP-адрес шлюза. Введенные параметры представлены на рисунок 10 и рисунок 11:

```

Начальная конфигурация ЦУС
Инициализировать ЦУС с использованием файла конфигурации? (Y/N): n
Обнаруженные интерфейсы:
    Номер  Имя
    1.     en0
    2.     en1
    3.     en2
    4.     en3
    5.     tun0
Укажите номер внешнего интерфейса: 1
Введите внешний IP адрес шлюза: 192.168.1.24
Продолжить? (Y/N): y
Обнаруженные интерфейсы:
    Номер  Имя
    2.     en1
    3.     en2
    4.     en3
Укажите номер внутреннего интерфейса. Если их несколько -- того, к которому
подключается АРМ администратора: 2
  
```

Рисунок 10 – Информация о внешнем интерфейсе, IP-адресе шлюза

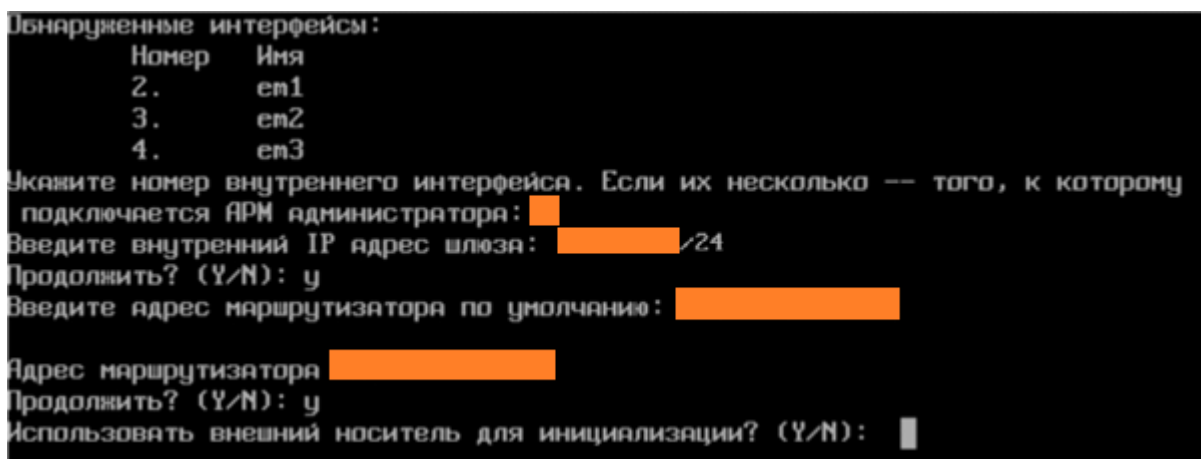


Рисунок 11 – Информация о внутреннем интерфейсе, IP-адресе шлюза

Для завершения инициализации была сохранена созданная конфигурация, создан профиль администратора, придуман пароль, который будет использован для шифрования административного ключа и в дальнейшем понадобится для запуска программы управления ЦУС и ее подключения к ЦУС. Исходный ключевой материал был загружен в центр управления сетью, где был сформирован ключ администратора ЦУС. На внешний USB-флэш-накопитель формата FAT32 сохранен файл «contkey.str» в котором записан сформированный ключ.

Для настройки сервера доступа необходимо сформировать и записать на внешний носитель ключ администратора СД. Ключ был записан в уже созданный файл «contkey.str». После выполнения всех необходимых действий появляется сообщение об успешном запуске, что означает, что с этого момента центр управления сетью готов к работе.

Итогом выполнения инициализации центра управления сетью являются записанные на внешний носитель ключи администратора центра управления сетью и сервера доступа.

### 3.2 Установка подсистемы управления комплексом

Подсистема управления комплексом устанавливается на рабочий компьютер администратора. Для установки была проведена авторизация в ОС под учетной записью администратора, подключен съемный носитель, содержащий файл «contkey.str» с ключами администратора ЦУС и СД, созданный при инициализации ЦУС ранее.

Для запуска процесса установки подсистемы управления были выбраны компоненты, которые должны быть установлены до начала установки самой подсистемы. Дополнительные компоненты представлены на рисунке 12:



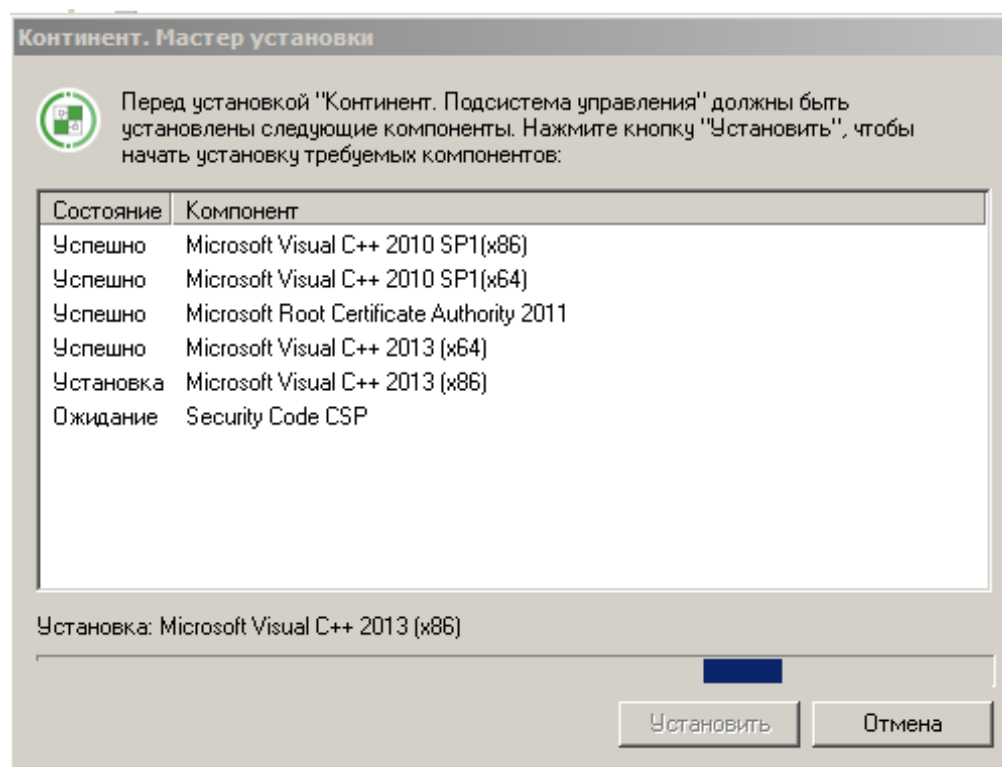


Рисунок 12 – Компоненты для установки подсистемы управления

После установки компонентов было прочитано лицензионное соглашение и приняты его условия. Далее предлагаются два варианта установки: типовая и выборочная. При типовой установке устанавливаются основные компоненты программы, а именно:

1. Программа управления ЦУС;
2. Программа копирования ключей;
3. Программа просмотра журналов;
4. Агент ЦУС и СД.

Для дальнейшей работы использовалась выборочная установка, при которой были загружены следующие компоненты:

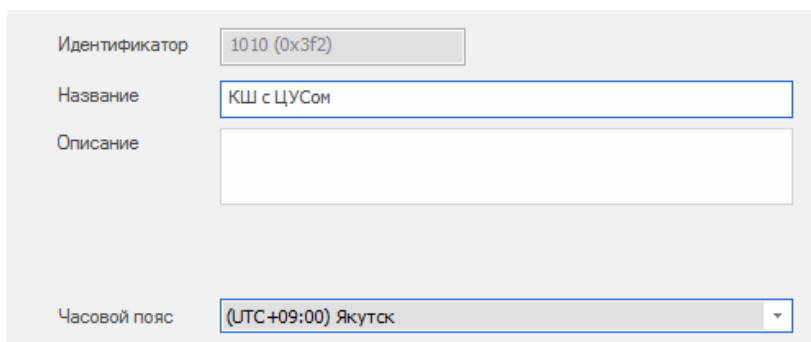
1. Агент ЦУС и СД;
2. Отчеты ЦУС;
3. Программа копирования ключей;
4. Программа журналов ЦУС и СД;
5. Программа управления СД;
6. Программа управления ЦУС.

После полной загрузки компьютер администратора был перезагружен, после чего на рабочем столе появились ярлыки программы управления ЦУС и программы управления СД, а также были загружены все выбранные ранее дополнительные компоненты.

После запуска программы управления ЦУС открывается основное окно программы, а также запрос на определение параметров подключения ЦУС, в котором были установлены значения, представленные на рисунке 13:



Также были указаны текущая дата и время в свойствах самого центра управления сетью. Результат представлен на рисунке 15 и рисунке 16:



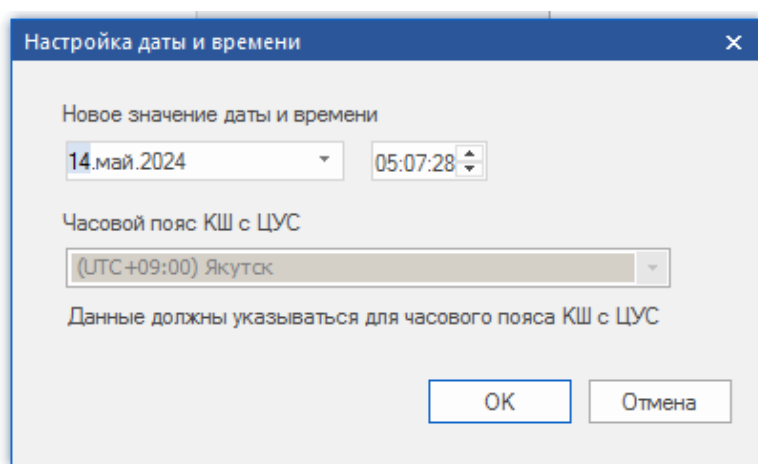
Идентификатор: 1010 (0x3f2)

Название: КШ с ЦУСом

Описание:

Часовой пояс: (UTC+09:00) Якутск

Рисунок 15 – Настройка часового пояса сетевого объекта «КШ с ЦУСом»



Настройка даты и времени

Новое значение даты и времени

14.май.2024 05:07:28

Часовой пояс КШ с ЦУС

((UTC+09:00) Якутск)

Данные должны указываться для часового пояса КШ с ЦУС

OK Отмена

Рисунок 16 – Настройка даты и времени ЦУС

Итогом данной настройки является установка подсистемы управления аппаратно-программного комплекса, а также настроены параметры защищенного соединения между криптографическим шлюзом с центром управления сетью и пунктом управления центром управления сетью.

### 3.3 Конфигурирование базы данных журналов, настройка агента ЦУС и СД

После установки подсистемы управления была сконфигурирована база данных, где хранятся регистрационные журналы комплекса, которые содержат все данные о событиях, которые происходят в процессе работы всех компонентов комплекса.

Каждый криптографический шлюз локально хранит в буфере записи журналов до момента их передачи на центр управления сетью. Отправка содержимого журналов осуществляется по мере регистрации событий при

условии наличия связи с ЦУС. Если связи с ЦУС в данный момент нет, то записи накапливаются в буфере и записываются в локальных журналах криптографических шлюзов.

На ЦУС выделен специальный буфер для временного хранения принятых записей журналов, которые, как и локальные, хранятся до момента их передачи в базу данных. Параметры хранения журналов на КШ комплекса и на ЦУС можно просматривать, настраивать, в окне их свойств через ПУ ЦУС (рисунок 17, рисунок 18):

Максимальные размеры журналов (Кбайт)

Системный журнал	2048
Журнал НСД	2048
Журнал сетевого трафика	4096

Регистрировать в журнале сетевого трафика пакеты

- ☐ Переданные получателям
- ☐ Отброшенные фильтром
- ☐ Не соответствующие правилам фильтрации

Отладочный журнал

- ☐ Уровень детализации: 3-Warning

Рисунок 17 – Журналы на криптографическом шлюзе

Режим управления ключевой информацией

- ☐ Схема трёхлетнего хранения ключевой информации, генерация ключей сетевых устройств средствами АРМ ГК
- ☒ Схема однолетнего хранения ключевой информации, генерация ключей сетевых устройств средствами ЦУС

Максимальные размеры журналов (Кбайт)

Системный журнал	2048
Журнал НСД	2048
Журнал сетевого трафика	4096

☐ Режим изолированной сети

Рисунок 18 – Журналы на центре управления сетью

Непосредственная передача журналов из буфера ЦУС и СД в базу данных осуществляется агентом ЦУС и СД согласно заданному расписанию или по специальной команде «Сбор журналов» от администратора ПУ ЦУС. Параметры подключения агента к СУБД, учетная запись базы данных настраиваются в программе «Конфигуратор БД журналов ЦУС и СД».

Администраторы комплекса получают доступ к содержимому журналов через специальную программу просмотра журналов ЦУС и СД.

Для конфигурирования базы данных и настройки агента ЦУС и СД было необходимо установить СУБД на компьютере администратора комплекса и в списке установленных СУБД подключиться к SQLEXPRESS с указанными на рисунке 19 реквизитами:

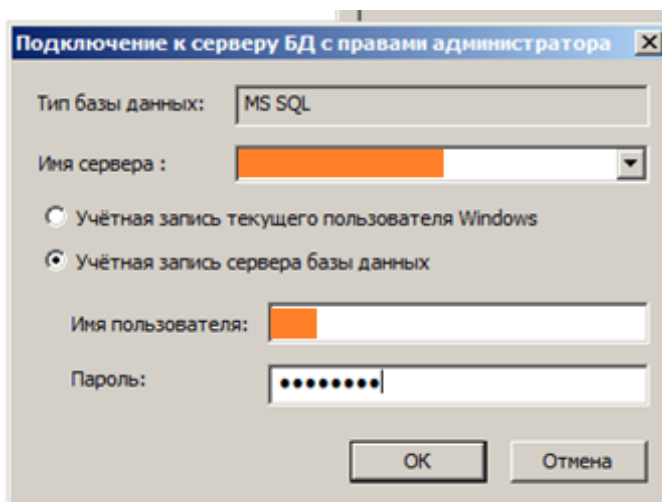


Рисунок 19 – Подключение к SQLEXPRESS

Далее была создана новая база данных с названием «39» по версии программного обеспечения «Континент». Для доступа к БД была создана учетная запись, которая будет использоваться агентом, загружаемым в базу данных регистрационные записи, и программой просмотра журналов. Для этого была выделена запись в созданной базе данных, создана учетная запись для СУБД агента, введены реквизиты, продемонстрированные на рисунке 20:

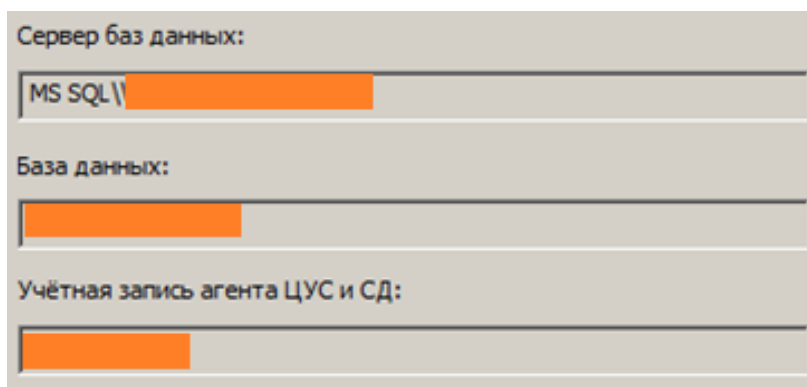


Рисунок 20 – Учетная запись СУБД для агента и для ППЖ

После проделанных действий конфигурация агента ЦУС и СД, которая содержит настроенные параметры подключения к базе данных, была сохранена.

Для подключения агента к ЦУС и к СД помимо конфигурации необходим ключевой носитель. По нему агент проходит аутентификацию и связывается с ЦУС и с СД по защищенному каналу.

Далее ключевые данные агента вместе с данными администратора ЦУС и СД необходимо сохранить в одном файле. При добавлении ключевых данных агента в файл «contkey.str» необходимо добавить ключи администратора ЦУС и СД в хранилище, указав его источник.

Для это в программе создания ключевого носителя для агента ЦУС и СД была проведена операция чтения ключей со съемного носителя, введены внутренний IP-адрес шлюза. Результат представлен на рисунке 21-рисунке 23:

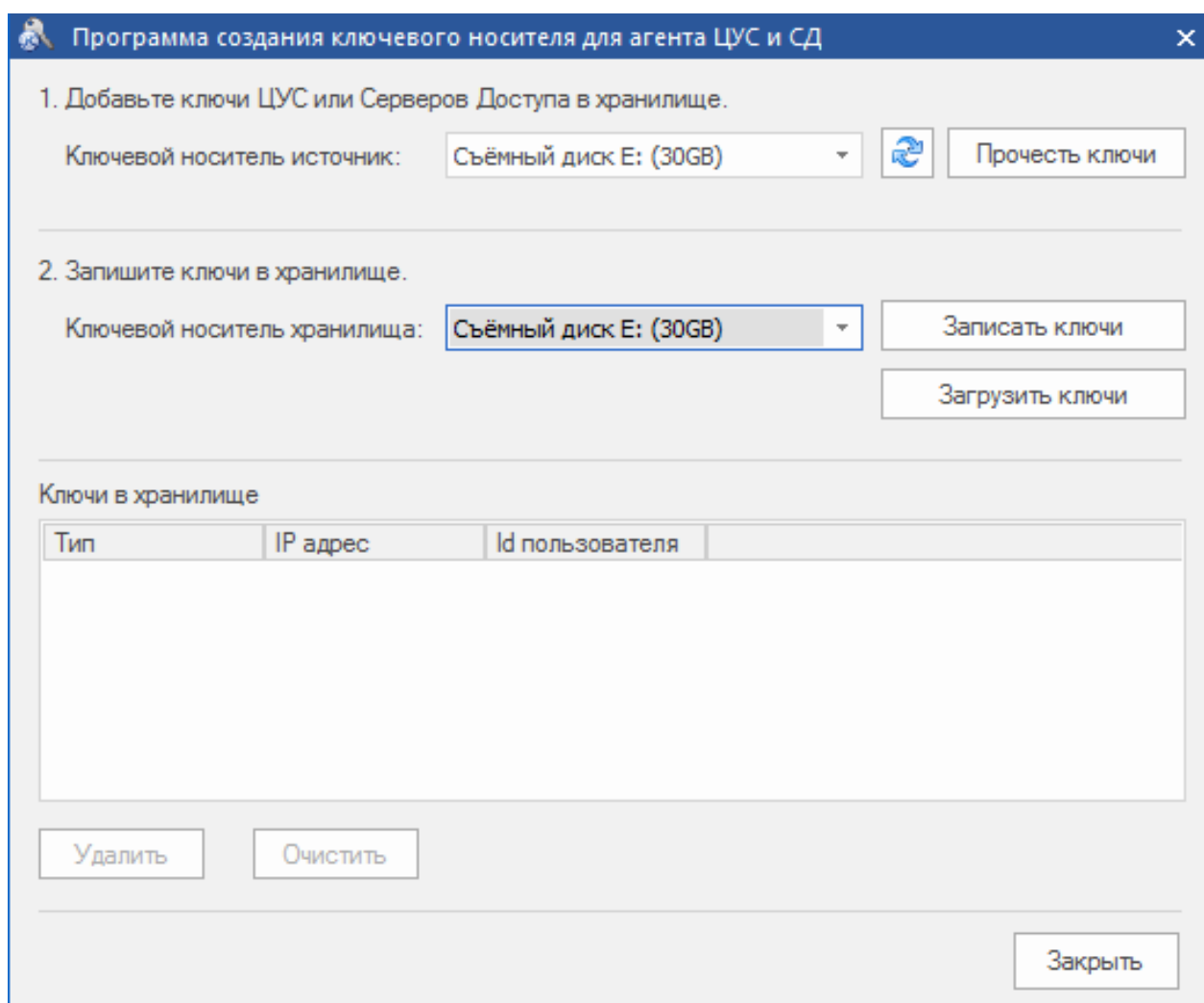


Рисунок 21 – Программа создания ключевого носителя для агента  
ЦУС и СД

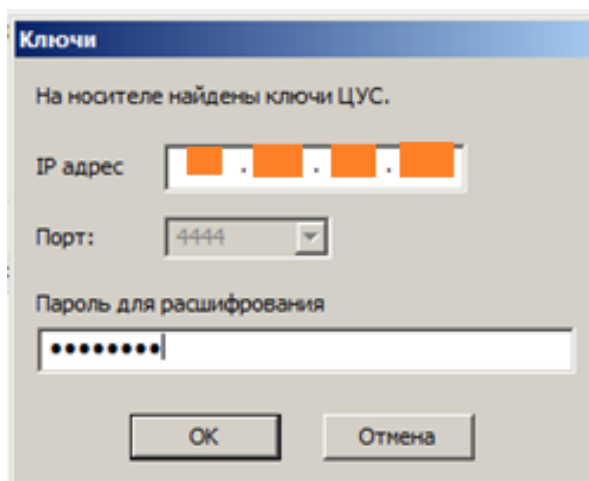


Рисунок 22 – Окно запроса IP-адреса ЦУС и пароля для расшифрования ключа администратора ЦУС

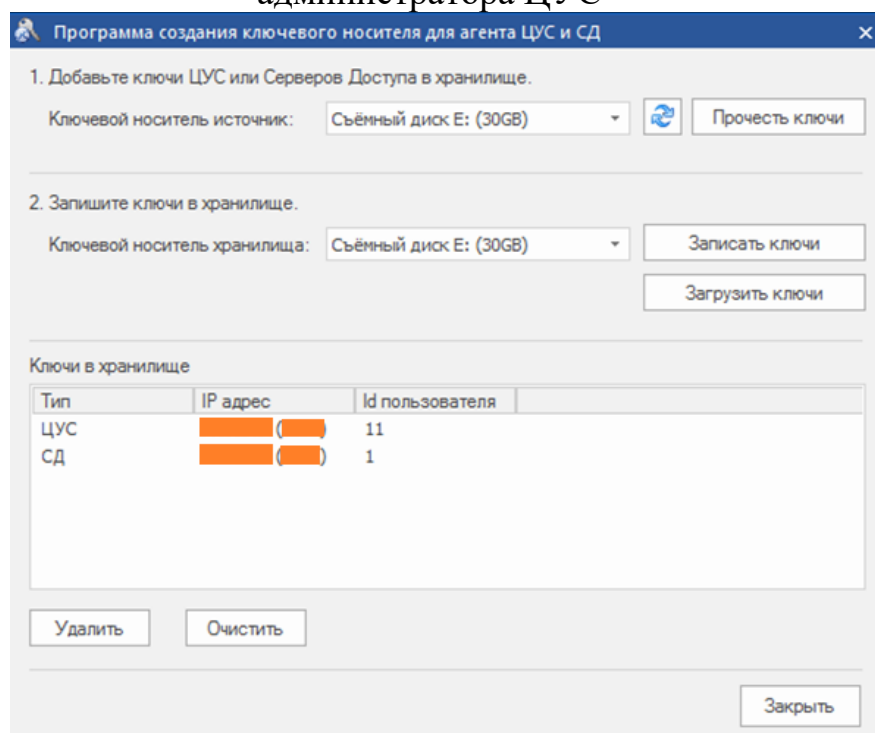


Рисунок 23 – Ключи в хранилище

В результате проделанных действий на USB-флэш-накопителе в файле «contkey.str» в дополнение к ключам администратора ЦУС (защищенное соединение ПУ ЦУС с ЦУС) и администратора СД (защищенное соединение ПУ СД с СД) были добавлены ключевые данные агента ЦУС и СД (агент забирает журналы с ЦУС и СД и загружает их в базу данных на АРМ).

После сохранения конфигурации и ключевого носителя агента для его запуска в параметрах агента был указан источник ключевого носителя, где была сохранена конфигурация, и ключевые данные, параметры подключения к базе данных и пароль для сохранения конфигурации ЦУС.

Для того, чтобы проверить загружает ли агент журналы с ЦУС и СД в базу данных, была настроена программа просмотра журналов.

Для этого в программе просмотра журналов необходимо заполнить следующие поля:

1. Имя сервера БД;
2. Тип входа на сервер;
3. Имя базы данных.

Указанные параметры представлены на рисунке 24:

Настройка соединения с базой данных

Для подключения к базе данных укажите следующие сведения:

- Тип СУБД:
  - ☒ MS SQL
  - ☐ Oracle
- Имя сервера базы данных: [Поле для ввода]
- Для входа на сервер использовать:
  - ☐ Учетную запись пользователя Windows
  - ☒ Имя и пароль пользователя:
    - Пользователь: [Поле для ввода]
    - Пароль: [Поле для ввода]
- Имя базы данных: [Поле для ввода]

Проверить подключение OK Закрыть

Рисунок 24 – Параметры для соединения с базой данных

После соединения с базой данных в окне программы просмотра журналов появилась структура журналов, в разделах которой можно просматривать события по таким категориям как журнал НСД и системный журнал.

После настройки агента ЦУС и СД и ППЖ агент забирает записи журналов с ЦУС и с СД, а в ППЖ можно их посмотреть. Внешний вид журналов представлен на рисунке 25:

Программа просмотра журналов

Главная Вид

Предидущая Следующая Записей: 500 Фильтр Очистить

Страницы журнала

Журналы

- Журналы
- Журнал приложения
- Журнал ЦУС
- Журнал НСД
- Системный журнал
- Криптокопьютеры
- Детекторы атак
- Статистика атак
- Серверы доступа

Дата/Время	Дата/Время на СУ	Категория события	Событие	Описание
14.05.2024 00:55:51	14.05.2024 07:55:51	Сеть Континент	Подключение администратора к ППЖ	Администратор: 'Встроенный администратор'
14.05.2024 00:55:51	14.05.2024 07:55:51	Сеть Континент	Отключение администратора от ППЖ	Администратор: 'Встроенный администратор'
14.05.2024 00:47:03	14.05.2024 07:47:03	Сеть Континент	Подключение администратора к ППЖ	Администратор: 'Встроенный администратор'
14.05.2024 00:46:48	14.05.2024 07:46:48	Сеть Континент	Отключение администратора от ППЖ	Администратор: 'Встроенный администратор'
14.05.2024 00:46:14	14.05.2024 07:46:14	Сеть Континент	Подключение администратора ПУ ЦУС к ЦУС	Администратор: 'Встроенный администратор'
14.05.2024 00:45:22	14.05.2024 07:45:22	Сеть Континент	Отключение администратора ПУ ЦУС от ЦУС	Администратор: 'Встроенный администратор'
14.05.2024 00:41:10	14.05.2024 07:41:10	Сеть Континент	Подключение администратора ПУ ЦУС к ЦУС	Администратор: 'Встроенный администратор'
14.05.2024 00:31:41	14.05.2024 07:31:41	Сеть Континент	Подключение администратора к ППЖ	Администратор: 'Встроенный администратор'
13.05.2024 22:57:22	14.05.2024 05:57:22	Сеть Континент	Отключение администратора ПУ ЦУС от ЦУС	Администратор: 'Встроенный администратор'
13.05.2024 22:08:26	14.05.2024 05:08:26	Управляющая команда	Установка времени ЦУС	Новое время ЦУС: 13.05.2024 22:07:28 Админис
13.05.2024 22:07:31	14.05.2024 05:07:31	Управляющая команда	Установка времени ЦУС	Новое время ЦУС: 13.05.2024 22:07:28 Админис
13.05.2024 21:57:08	14.05.2024 04:57:08	Управляющая команда	Добавление лицензии	Лицензия: L7714 4 123<>1234 Администратор: B
13.05.2024 21:56:54	14.05.2024 04:56:54	Управляющая команда	Добавление лицензии	Лицензия: L771 0 123<>123 Администратор: B
13.05.2024 21:55:22	14.05.2024 04:55:22	Сеть Континент	Подключение администратора ПУ ЦУС к ЦУС	Администратор: 'Встроенный администратор'
13.05.2024 21:52:10	14.05.2024 04:52:10	Сеть Континент	Установлено соединение с КШ	Ю КШ: 1010 (КШ с ЦУСом)

Готово Страница: 1 Загружено записей: 15

Рисунок 25 – Системный журнал



Итогом данной настройки является создание базы данных для хранения записей журналов комплекса. В этой базе данных настроены параметры подключения агента к ЦУС и СД, а также параметры соединения программы просмотра журналов с базой данных.

### 3.4 Инициализация КШ

Для инициализации криптографического шлюза аналогично инициализации ЦУС была начата загрузка ОС «Континент». Конфигурация представляет собой файл с именем «gate.cfg», который содержит информацию о сетевых параметрах устройства. Ключ КШ – файл с именем «keyset», содержащий главный ключ КШ и ключ связи с ЦУС. Он необходим для установления защищенного соединения КШ с ЦУС. Формирование файлов с конфигурацией криптографического шлюза и с ключом КШ производится в программе управления ЦУС.

Для того, чтобы получить файл конфигурации и ключевой файл для КШ, в окне ПУ ЦУС был зарегистрирован этот КШ. Для этого был создан такой сетевой объект, как криптографический шлюз с помощью мастера создания нового устройства (рисунок 26). Было введено название, описание, выбран часовой пояс региона, в котором будет эксплуатироваться оборудование, введен логин и пароль администратора криптографического шлюза. В разделе реквизитов «Конфигурация» была выбрана конфигурация по строке.

Конфигурация устройства задается по его идентификатору и типу платформы или по строке конфигурации, которая указана в его паспорте и определяет аппаратную конфигурацию устройства.

Идентификатор криптографического шлюза – номер, присвоенный оборудованию производителем и указанный в его паспорте и на задней панели корпуса КШ в десятичной форме.

Рисунок 26 – Создание криптографического шлюза

Затем были настроены параметры сетевых интерфейсов криптографического шлюза и указаны следующие параметры: тип интерфейса, интерфейс и тип использования, режим интерфейса, IP-адреса.

Указанные значения представлены на рисунке 27:

Мастер создания нового устройства (шаг 3 из 6)

**Интерфейсы**  
Параметры интерфейса связи с ЦУС.

Тип интерфейса: Физический (с возможностью использования PPPoE)

Интерфейс и тип использования: eth0 Внешний

Режим интерфейса: Автовыбор

IP-адреса:

Адрес	Маска
	255.255.255.0

Добавить... Изменить... Удалить

PPPoE: Не использовать PPPoE

IP-адрес:

Логин:

Пароль:

Имя сервиса:

< Назад Далее > Создать Отмена

Рисунок 27 – Параметры интерфейса связи с ЦУС

Далее были настроены параметры маршрутизации. Выбрана статическая маршрутизация, в разделе маршруты был добавлен новый маршрут. Параметры маршрутизации до ЦУС представлены на рисунке 28:

Мастер создания нового устройства (шаг 4 из 6)

**Маршрутизация**  
Параметры маршрутизации до ЦУС.

Тип маршрутизации: Статическая

Маршруты:

Адрес назначения	Маска	Следующий узел
0.0.0.0	0.0.0.0	

Добавить... Изменить... Удалить

< Назад Далее > Создать Отмена

Рисунок 28 – Параметры маршрутизации

Необходимо отметить, что есть возможность выгрузки файла конфигурации криптографического шлюза на съемный носитель.

В категории параметров «Интерфейсы» в свойствах созданного криптографического шлюза были установлены параметры внутреннего интерфейса КШ. Для этого был выбран интерфейс «em2» и в окне его свойств были настроен его тип, в таблице IP-адреса был добавлен новый адрес. Результат представлен на рисунке 29:

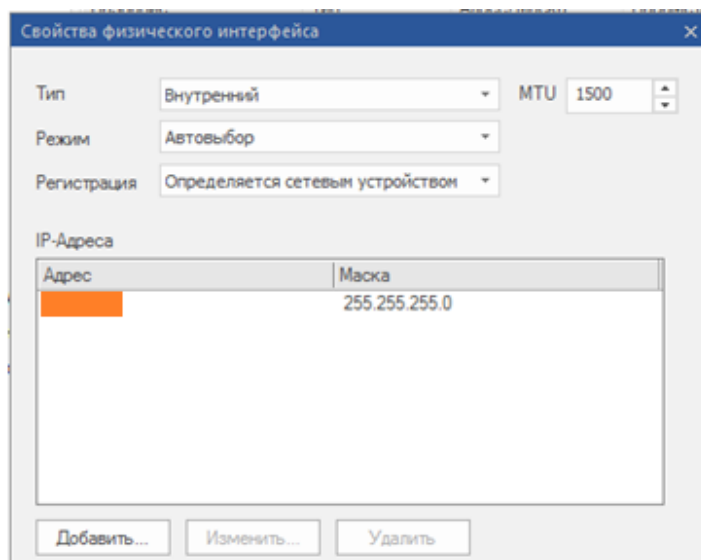


Рисунок 29 – Свойства физического интерфейса «em2»

На этом этапе основные сетевые параметры криптографического шлюза заданы.

Далее на USB-флэш-накопителе были созданы файлы конфигурации и ключей. Для этого в ПУ ЦУС была выбрана опция «Сохранить конфигурацию криптографического шлюза», был введен пароль, ограничивающий доступ к сохраняемой конфигурации КШ, и который запрашивается при считывании конфигурации сетевым устройством, а также указан путь к файлу (рисунок 30):

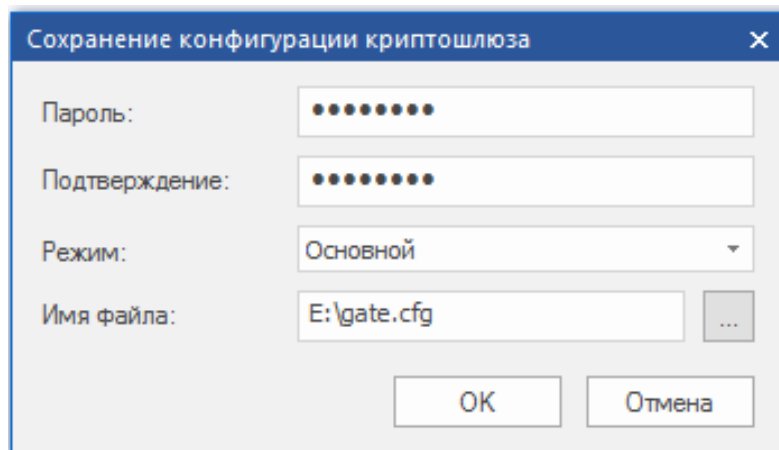


Рисунок 30 – Сохранение конфигурации криптографического шлюза

Для записи ключей КШ на съемный носитель была выбрана опция «Сохранить текущий комплект ключей на носитель», введен пароль, с помощью которого ограничивается доступ к сохраняемому ключевому файлу.

На этом этапе конфигурация и ключи КШ записаны. После записи файлов конфигурации и ключей КШ для продолжения установки ПО на КШ было произведено считывание криптографическим шлюзом конфигурации с внешнего носителя, введен пароль (рисунок 31).

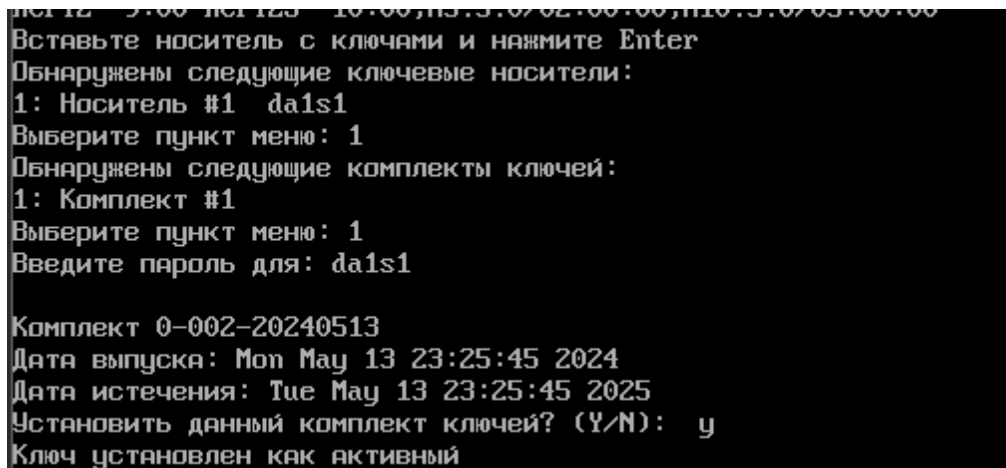


Рисунок 31 – Загрузка конфигурации и ключей криптографического шлюза

После инициализации сетевого устройства, оно было введено в эксплуатацию в ПУ ЦУС. Изменения после проделанных действий представлены на рисунке 32:

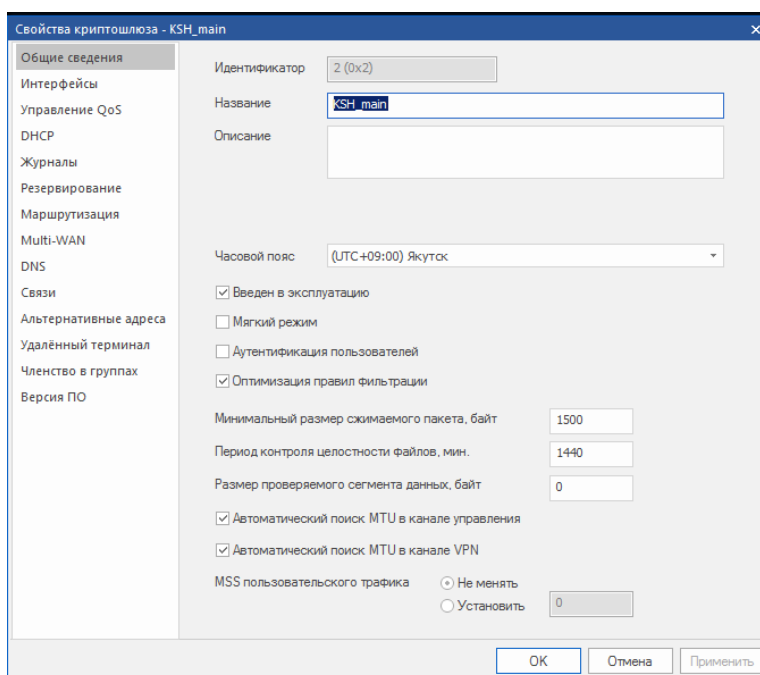


Рисунок 32 – Свойства криптографического шлюза

После ввода в эксплуатацию сетевого устройства становятся доступными управляющие команды, например дистанционная перезагрузка и конфигурационные настройки, например формирование ключей парной связи. При этом в ПУ ЦУС сетевое устройство отображается со статусом «Включен» (рисунок 33):

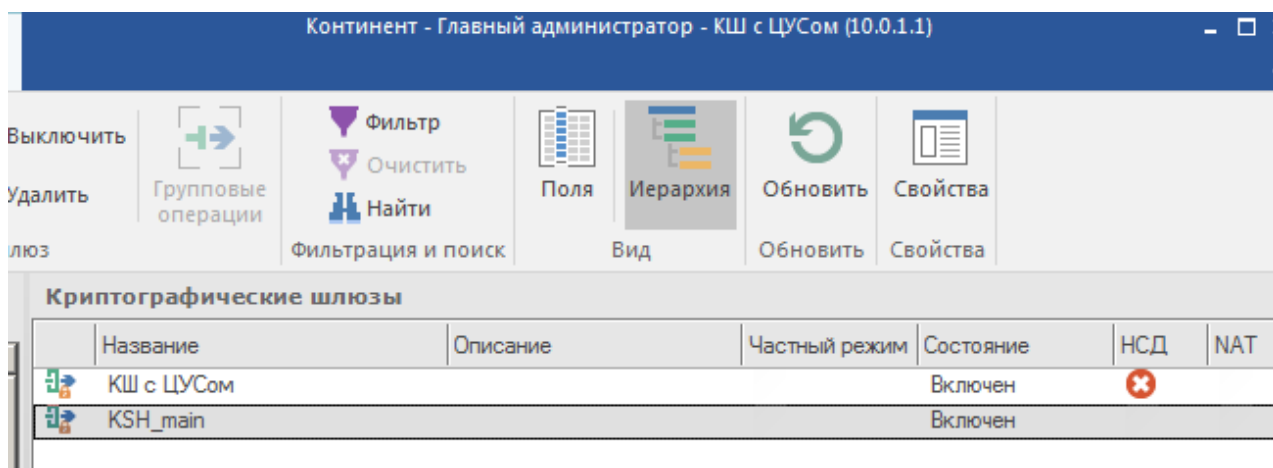


Рисунок 33 – Криптографический шлюз введен в эксплуатацию

На этом этапе в ПУ ЦУС было создано новое сетевое устройство – криптографический шлюз, сформированы и записаны на съемный диск файлы конфигурации и ключей криптографического шлюза.

Также была выполнена инициализация криптографического шлюза с использованием полученных файлов. Криптографический шлюз был подключен к центру управления сетью и введен в эксплуатацию.

### 3.5 Настройка правил фильтрации

На этом этапе необходимо обеспечить возможность подключаться пользователю из одной защищаемой сети к веб-серверу, который находится в защищаемой сети за другим криптографическим шлюзом. Для этого было создано правило фильтрации, позволяющее такому пользователю заходить на этот веб-сервер. Один криптошлюз – с центром управления сетью, другой – управляемый им криптошлюз.

В ПУ ЦУС были созданы сетевые объекты с привязкой к разным криптографическим шлюзам. В ПУ ЦУС написано правило фильтрации, обеспечивающее прохождение IP-трафика по протоколу HTTPS от пользователя к веб-серверу.

Также была протестирована возможность подключения из одной защищаемой сети к веб-серверу в другой защищаемой сети.

Настройки сетевого объекта «Веб-сервер» представлен на рисунке 34, настройки сетевого объекта «Пользователь» представлен на рисунке 35.

Рисунок 34 – Сетевой объект «Веб-сервер»

Рисунок 35 – Сетевой объект «Пользователь»

В области объектов управления было написано правило фильтрации с реквизитами, представленными на рисунке 36:

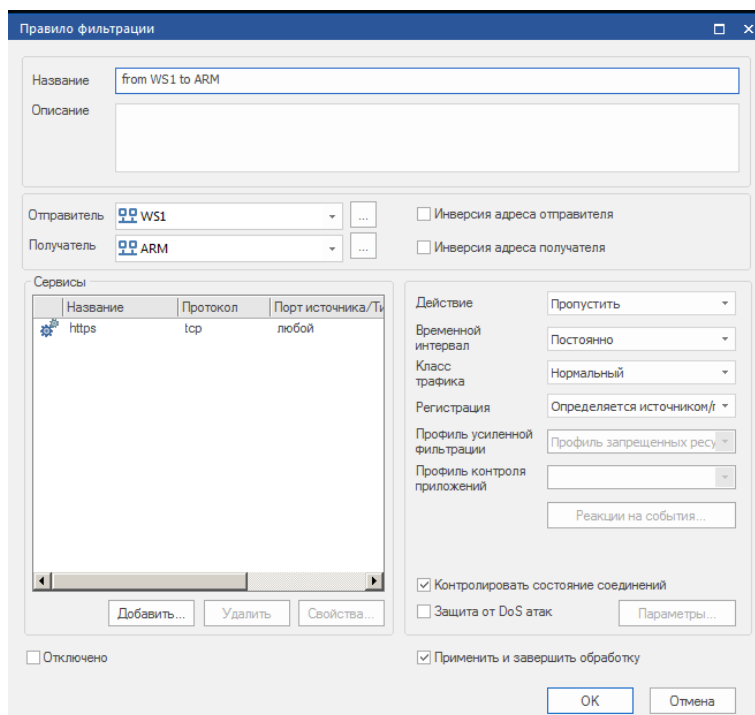


Рисунок 36 – Правило фильтрации «От пользователя к веб-серверу»

По причине того, что при включенном контроле состояния соединений автоматически создаются правила фильтрации, которые разрешают прохождение всех пакетов, относящихся к этому соединению и эти правила сохраняются в таблице состояния соединений и на экране не отображаются, написание еще одного правила, разрешающего прохождение трафика от веб-сервера к пользователю не требуется.

При создании в ПУ ЦУС одного правила фильтрации ПО ЦУС автоматически формирует правила для входящего и исходящего интерфейсов каждого криптографического шлюза. Таким образом, в данном случае были сформированы четыре правила.

Для того, чтобы убедиться в том, что правила фильтрации написаны верно и IP-трафик проходит от пользователя к веб-серверу с АРМ пользователя был сделан запрос в браузере на адрес <http://10.0.1.200/test2.txt>. В конечном итоге был получен доступ к файлу, представленному на рисунке 37:

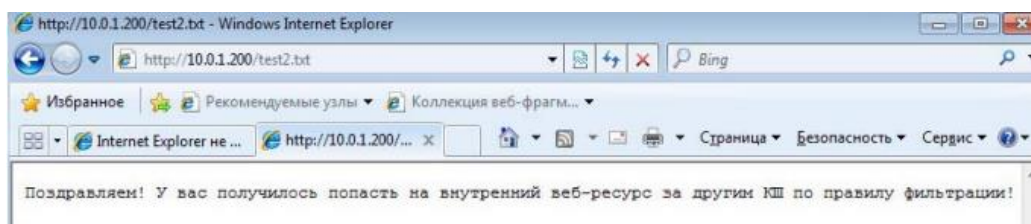


Рисунок 37 – Доступ к файлу test2.txt на веб-сервере

В итоге выполненных действий было создано правило фильтрации, разрешающее прохождение IP-трафика между хостами, находящимися в сегментах сети, защищаемых разными криптошлюзами, а также протестировано действие этого правила.

### 3.6 Организация L3VPN

В разделе необходимо организовать VPN-соединение через сеть общего доступа между пользователями, находящимися в защищаемых сетях за разными криптошлюзами для обмена конфиденциальной информацией.

Для этого в ПУ ЦУС написать правила фильтрации, разрешающее прохождение трафика между АРМ1 и АРМ2, настроить связь между созданными ранее криптошлюзами, а также убедиться, что трафик между КШ с ЦУС и криптографическим шлюзом передается в зашифрованном виде.

Были созданы сетевые объекты АРМ1 и АРМ2, для которых в поле «Тип привязки» указано «Защищаемый».

Результат выполненных действий представлен на рисунке 38, рисунке 39:

The screenshot shows the 'Сетевой объект' (Network Object) configuration window for 'ARM\_vpn'. The window has a title bar with a close button. On the left, there are two tabs: 'Общие' (General) and 'Членство в группах' (Group Membership). The 'Общие' tab is selected. The main area contains the following fields and options:

- Название** (Name): ARM\_vpn
- Описание** (Description): Empty text area.
- Unicast / Multicast**: Radio buttons for 'Unicast' (selected) and 'Multicast'.
- IP-адрес / Маска** (IP address / Mask): A field with an orange icon followed by a slash and the text '255 . 255 . 255 . 255'.
- Тип привязки** (Type of binding): A dropdown menu with 'Защищаемый' (Protected) selected.
- Криптошлюз** (Crypto gateway): A dropdown menu with 'КШ с ЦУСом' (Crypto gateway with CUS) selected.
- Интерфейс** (Interface): A dropdown menu with an orange icon.
- Трансляция адреса внутри VPN** (VPN address translation): An unchecked checkbox.
- Виртуальный адрес** (Virtual address): A field with '0 . 0 . 0 . 0' followed by a slash and '255 . 255 . 255 . 255'.
- Регистрация** (Registration): A dropdown menu with 'Определяется интерфейсом' (Determined by interface) selected.

At the bottom right, there are two buttons: 'OK' and 'Отмена' (Cancel).

Рисунок 38 – Сетевой объект «АРМ1»



Рисунок 39 – Сетевой объект «APM2»

Затем было создано правило фильтрации с использованием реквизитов, представленных на рисунке 40:

Рисунок 40 – Правило фильтрации от APM1 к APM2

Для того, чтобы предоставить возможность пользователям инициализировать соединение как с АРМ1, так и с АРМ2 было написано аналогичное разрешающее правило фильтрации, но в обратную сторону, от АРМ2 к АРМ1 (рисунок 41):

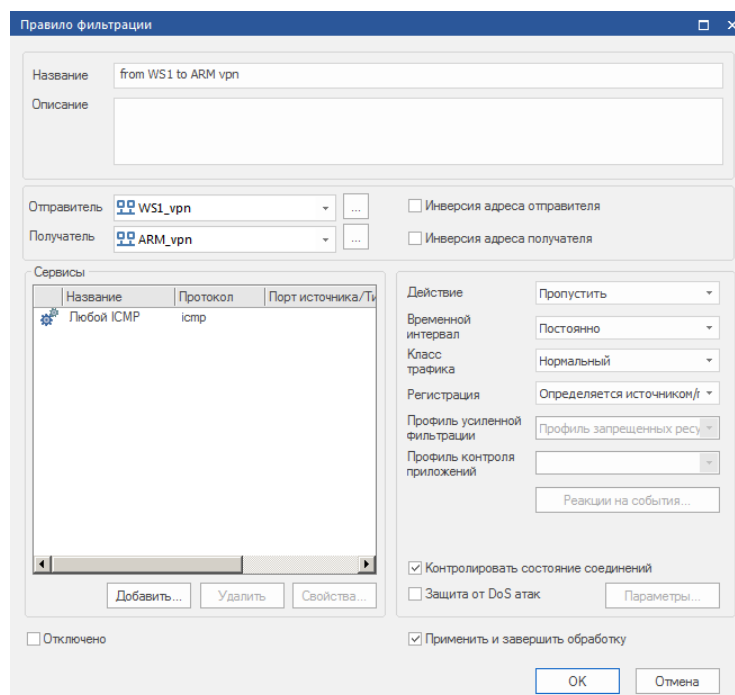


Рисунок 41 – Правило фильтрации от АРМ2 к АРМ1

Далее необходимо установить связь между КШ с ЦУС и криптографическим шлюзом. Для этого были настроены связи в свойствах криптографических шлюзов (рисунок 42):

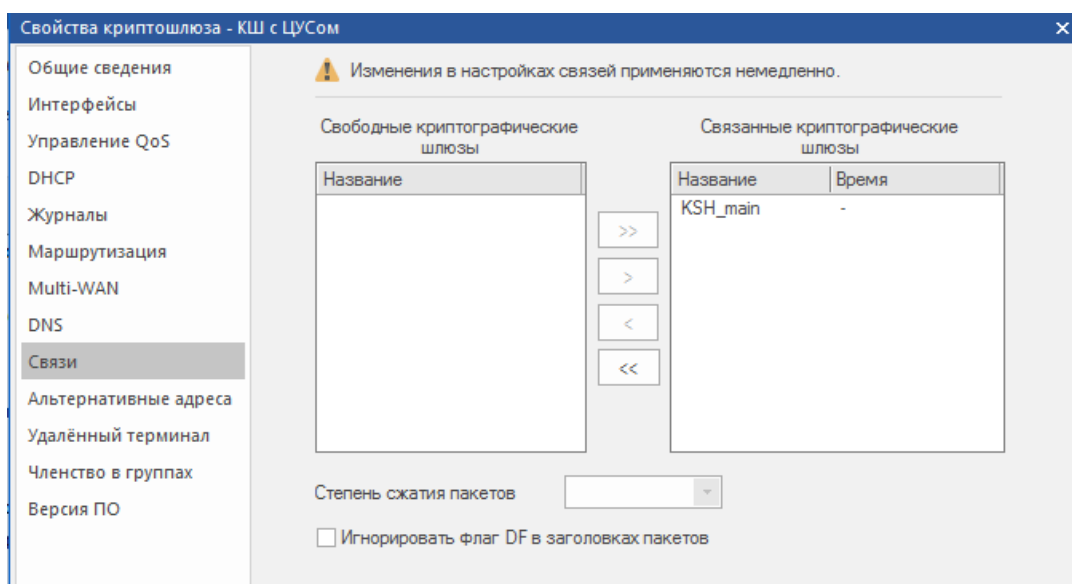


Рисунок 42 – Настройка связи между криптографическими шлюзами

С АРМ1 была проверена доступность АРМ2 с помощью команды ping в консоли АРМ1 (рисунок 43):

```

Администратор: Командная строка - ping [redacted] -t
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corporation), 2009. Все права защищены.

C:\Users\Администратор>ping [redacted] -t

Обмен пакетами с [redacted] по 32 байтами данных:
Ответ от [redacted] : число байт=32 время=1мс TTL=127
Ответ от [redacted] : число байт=32 время=1мс TTL=127
Ответ от [redacted] : число байт=32 время=8мс TTL=127
Ответ от [redacted] : число байт=32 время=1мс TTL=127

```

Рисунок 43 – Проверка доступности к АРМ2 с АРМ1

Чтобы убедиться в том, что между АРМ передается зашифрованный трафик было использовано два способа: просмотрены сведения обо всех промежуточных маршрутизаторах между АРМ с помощью утилиты tracert в командной строке.

Также был изучен дамп передаваемого трафика между АРМ, с использованием средств диагностики криптографического шлюза.

Выполнение трассировки всех промежуточных маршрутизаторов между АРМ была выполнена команда отправки данных указанному узлу сети с отображением сведений обо всех промежуточных маршрутизаторах, через которые проходят данные к целевому узлу. Результат представлен на рисунке 44:

```

C:\Users\Администратор>tracert -d [redacted]

Трассировка маршрута к 10.0.2.200 с максимальным числом прыжков 30

 1      *          *          *      Превышен интервал ожидания для запроса.
 2      2 ms       1 ms       1 ms    [redacted]

Трассировка завершена.

```

Рисунок 44 – Результат трассировки

Как видно из трассировки, отображается только конечная точка получателя, а значит, после проделанных действий создается защищенное логическое соединение между КШ-отправителем и КШ-получателем – VPN-туннелирование.

В случае отключения шифрования данных между криптографическими шлюзами с помощью трассировки удастся определить IP-адреса всех маршрутов, через которые проходят пакеты.

Для просмотра в режиме реального времени дампа зашифрованного трафика (процесс записи или захвата данных, передаваемых по сети в зашифрованном виде) были выполнены настройки, представленные на рисунке 45, а также выведен отчет, представленный на рисунке 46:

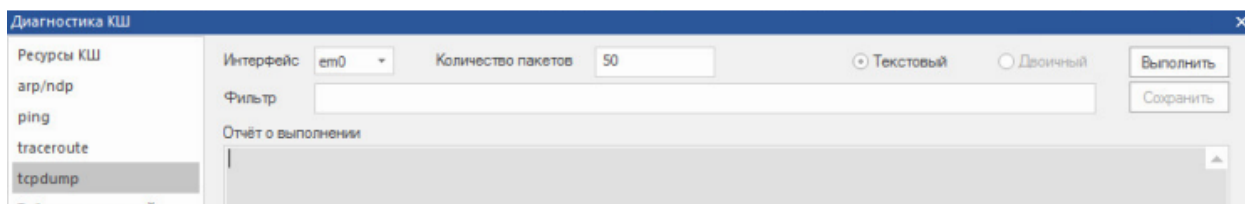


Рисунок 45 – Примененные настройки tcpdump

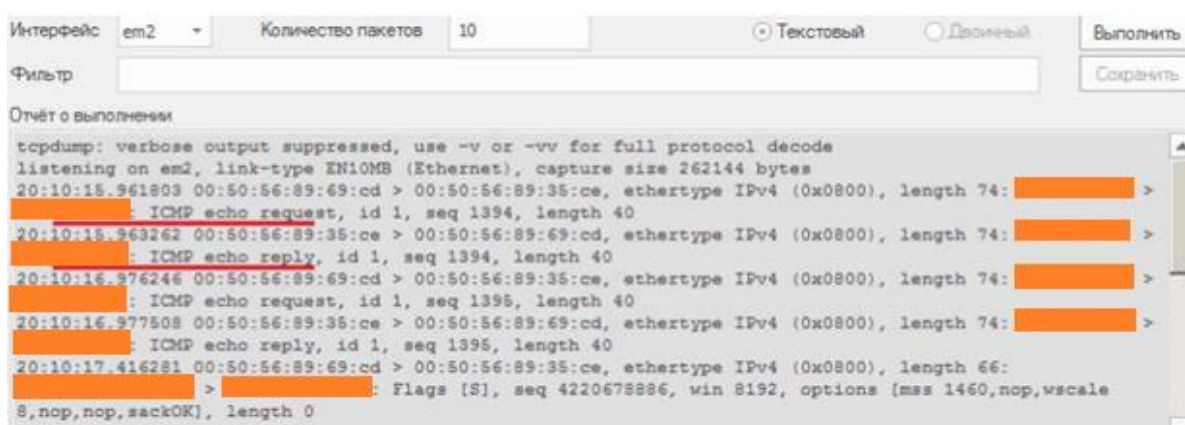


Рисунок 46 – Сформированный отчет em2

Из сформированного отчета можно увидеть, что зашифрованный трафик между внешними интерфейсами криптографических шлюзов передается по UDP-протоколу и портам 10000-10031, а локальные IP-адреса отправителя и получателя пакетов не определяются. Следует обратить внимание на размер пакета (Ethernet-кадра) – 126 байт.

Далее в поле «Интерфейс» был установлен внутренний интерфейс КШ с ЦУСом (em2) и сформирован отчет, представленный на рисунке 47:

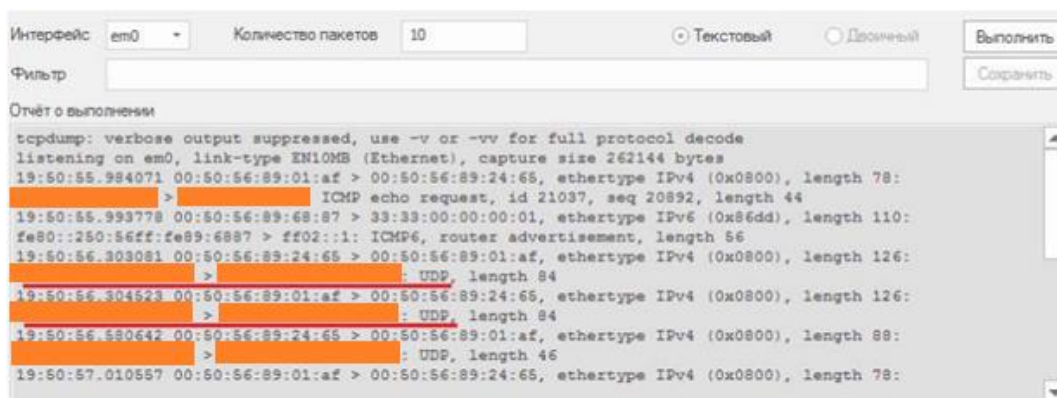


Рисунок 47 – Сформированный отчет em0

Из сформированного отчета можно увидеть, что на внутреннем интерфейсе трафик не шифруется, отображаются IP-адреса отправителя и получателя пакетов. Следует обратить внимание на то, что незашифрованный ICMP-пакет составляет 74 байта, что значит, что при шифровании размер пакета увеличился на 52 байта – это размер дополнительного заголовка зашифрованного пакета.

В результате проделанных действий между АРМ1 и АРМ2, находящимся в защищаемых сетях за разными криптографическими шлюзами, установлено шифрованное соединение (VPN-туннелирование) и протестирована его работа.

### 3.8 Вывод по технологической части

В данном разделе была произведена настройка оборудования, а именно был инициализирован центр управления сетью и сервер доступа, установлена подсистема управления комплексом, произведено конфигурирование базы данных журналов, настроен агент центра управления сетью и сервером доступа. Был инициализирован криптографический шлюз, а также настроены правила фильтрации. Организован L3VPN через сеть общего доступа между пользователями, находящимися в защищаемых сетях с разными в защищаемых сетях за разными криптошлюзами для обмена конфиденциальной информацией.

Также была выполнена задача, поставленная для достижения цели выпускной квалификационной работы, а именно была произведена настройка оборудования, а также система была протестирована на работоспособность.

## 4 Экономическая часть

### 4.1 Обоснование целесообразности разработки проекта

#### 4.1.1 Основание для разработки

Увеличение количества утечек конфиденциальной информации в финансовых организациях России за последний год свидетельствует о необходимости усиления мер по защите конфиденциальной информации, особенно в финансовом секторе.

В современном мире большинство финансовых операций осуществляется посредством электронного обмена данными, а значит финансовым организациям становится критически важно обеспечивать безопасность информации при ее передаче по каналам связи.

Для того, чтобы повысить уровень защищенности информации необходимо внедрение аппаратных и программных средств для организации защищенного соединения между офисами организаций.

#### 4.1.2 Назначение ввода комплекса в эксплуатацию

Цель работы – организация защищенного канала с шифрованием для передачи конфиденциальной информации между главным офисом и филиалом банковской организации.

Назначение ввода комплекса в эксплуатацию заключается в том, чтобы разработать схему сети, согласно которой будет проводиться шифрование, а также настройка выбранного оборудования.

#### 4.1.3 Жизненный цикл проекта

Для проекта была определена каскадная модель жизненного цикла, так как каждый этап разработки наступает последовательно и только после завершения предыдущего. При этом возврат на пройденные стадии не предусматривается.

Каждая стадия завершается выпуском полного комплекта документации. На каждой стадии формируется законченный набор такой документации, отвечающей критериям полноты и согласованности.

Выполняемые в логической последовательности стадии работ позволяют планировать сроки завершения всех работ и соответствующие затраты.

На рисунке 48 представлена диаграмма жизненного цикла проекта:



Рисунок 48 – Жизненный цикл проекта

#### 4.1.4 Реестр заинтересованных лиц

В таблице 7 представлен список заинтересованных в проекте лиц:

Таблица 7 – Реестр заинтересованных лиц

№	Наименование	Описание сторон	Цели и интересы сторон, степень их проявления	Степень влияния/вероятные риски от стороны
1	Руководство банка	Высшее руководящее звено банка, ответственное за стратегическое управление, принятие ключевых решений	Защитить конфиденциальную информацию организации от утечек	Высокая степень влияния  При внедрении комплекса вероятность утечки конфиденциальной информации снизится

№	Наименование	Описание сторон	Цели и интересы сторон, степень их проявления	Степень влияния/вероятные риски от стороны
2	ИТ-отдел банка	Отдел, занимающийся выбором, внедрением и поддержкой информационных технологий в организации	Использовать удобные и надежные средства шифрования данных и обеспечить непрерывную работу банковских сервисов	Средняя степень влияния  Успешное внедрение комплекса повлияет на уровень защищенности системы
3	Специалисты по информационной безопасности	Группа специалистов, занимающихся анализом угроз безопасности и разработкой мер по их предотвращению	Обеспечение целостности и конфиденциальности персональных данных, и другой информации ограниченного доступа	Средняя степень влияния  При успешном внедрении комплекса будет необходимо соблюдение требований формуляров
4	Клиенты банка	Непосредственные пользователи услуг банка	Защищенность своих персональных данных и транзакций	Низкая степень влияния  При внедрении комплекса вероятность утечки данных клиентов снизится
5	АО «Компания ТрансТелеКом»	Компания, предоставляющая услугу по организации зашифрованного канала	Предоставление качественной услуги согласно требованиям Заказчика и законодательства	Высокая степень влияния  При успешном внедрении комплекса «ТТК» получает прибыль за предоставляемые услуги



#### 4.1.5 Структура команды проекта

Структура команды проекта состоит из группы инженеров, группы тестирования, группы качества, группы обеспечения информационной безопасности, группа организации обучения сотрудников, группы технической эксплуатации, группы закупок. Структура команды проекта представлена на рисунке 49:

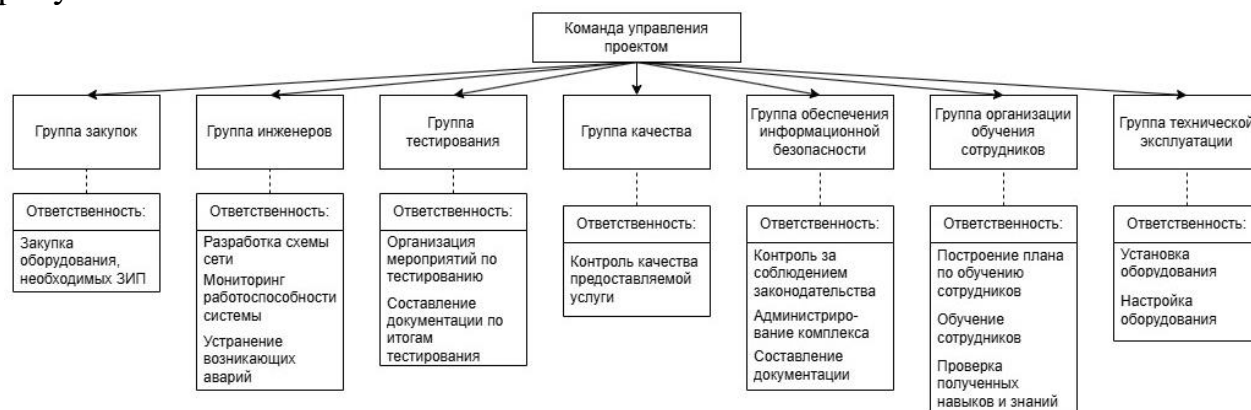


Рисунок 49 – Команда управления проектом

#### 4.2 Описание продукта

В конечном итоге работы, продуктом является организованный с помощью АПКШ «Континент» защищенный канал с шифрованием между главным офисом банка и его филиалом.

#### 4.3 Бизнес-модель проекта

Бизнес-моделью разрабатываемого решения является Pay-per-use, которая заключается в том, что Заказчик сам выбирает набор услуг и время, которое он будет пользоваться предоставляемой услугой.

#### 4.4 Планирование комплекса работ

Весь комплекс работ проекта представлен в таблице 8:

Таблица 8 – Комплекс работ

Содержание работ	Исполнители	Длительность, дни	Загрузка	
			Дни	%
Анализ требований Заказчика и законодательства				
1.1 Предварительный анализ проекта	Специалист ИБ	7	7	11

Содержание работ	Исполнители	Длительность, дни	Загрузка	
			Дни	%
1.2 Анализ технического задания Заказчика	Инженер	4	4	5
1.3 Анализ исходного построения сети	Инженер	3	3	4
1.3 Анализ законодательства	Специалист ИБ	3	3	4
1.4 Подбор необходимого оборудования	Специалист ИБ	4	4	5
Итого по стадии			21	29
2. Проектирование				
2.1 Проектирование модернизированной схемы сети	Инженер	4	4	5,5
2.2 Разработка рабочей технологической документации	Инженер	4	4	5,5
Итого по стадии			8	11
3. Закупка оборудования				
3.1 Расчет стоимости оборудования	Специалист отдела закупок	1	1	1,5
3.2 Закупка оборудования	Специалист отдела закупок	1	1	1,5
3.3 Доставка оборудования на объект заказчика	Специалист отдела технической эксплуатации	11	11	15
Итого по стадии			13	18
4. Обучение сотрудников				
4.1 Составление плана процесса обучения сотрудников	Специалист группы обучения	2	2	3
4.2 Обучение сотрудников	Специалист группы обучения	14	14	19
4.3 Контроль полученных сотрудниками навыками и знаний	Специалист группы обучения	2	2	3
Итого по стадии			18	25
5 Реализация				
5.1 Демонтаж старого оборудования	Специалист отдела	1	1	1,6

Содержание работ	Исполнители	Длительность, дни	Загрузка	
			Дни	%
	технической эксплуатации			
5.2 Перепланировка помещения	Специалист отдела технической эксплуатации	1	1	1,6
5.3 Подготовка фундамента под новое оборудование	Специалист отдела технической эксплуатации	1	1	1,6
5.4 Подведение систем энергоснабжения	Специалист отдела технической эксплуатации	1	1	1,6
5.5 Монтаж оборудования	Специалист отдела технической эксплуатации	1	1	1,6
5.6 Наладка и доводка оборудования	Специалист ИБ	1	1	1,6
Итого по стадии			6	8
6 Тестирование				
6.1 Тестирование работоспособности системы	Тестирующий	2	2	3
6.2 Заполнение актов по итогам тестирования	Тестирующий	2	2	3
Итого по стадии			4	6
7 Эксплуатация				
7.1 Ввод и сдача оборудования в эксплуатацию	Специалист ИБ	1	1	1
7.2 Мониторинг работы оборудования	Инженер	1	1	1
7.3 Оценка предоставляемой услуги	Специалист отдела качества	1	1	1
Итого по стадии			3	3
Итого			73	100

## 4.5 Расчет затрат на реализацию проекта

### 4.5.1 Анализ структуры затрат

Затраты на выполнение проекта состоят из затрат на заработную плату исполнителям, затрат на закупку или аренду оборудования, затрат на организацию рабочих мест, и затрат на накладные расходы (1):

$$C = C_{зп} + C_{эл} + C_{об} + C_{орг} + C_{накл} , \quad (1)$$

где

1.  $C_{зп}$  – заработная плата исполнителей;
2.  $C_{эл}$  – затраты на электроэнергию;
3.  $C_{об}$  – затраты на обеспечение необходимым оборудованием;
4.  $C_{орг}$  – затраты на организацию рабочих мест;
5.  $C_{накл}$  – накладные расходы.

Затраты на выплату исполнителям заработной платы определяется следующим соотношением (2):

$$C_{зп} = C_{з.осн} + C_{з.доп} + C_{з.отч} , \quad (2)$$

где

1.  $C_{з.осн}$  – основная заработная плата;
2.  $C_{з.доп}$  – дополнительная заработная плата;
3.  $C_{з.отч}$  – отчисление с заработной платы.

Расчет основной заработной платы при дневной оплате труда исполнителей проводится на основе данных по окладам и графику занятости исполнителей (3):

$$C_{з.осн} = O_{дн} \times T_{зан} , \quad (3)$$

где

1.  $O_{дн}$  – дневной оклад исполнителя;
2.  $T_{зан}$  – число дней, отработанных исполнителем проекта.

При 8-и часовом рабочем дне оклад рассчитывается (4):

$$O_{дн} = (O_{мес} * 8) / F_m \quad (4)$$

где

1.  $O_{мес}$  – месячный оклад;
2.  $F_m$  – месячный фонд рабочего времени (5).

$$F_m = (tp * (Dp - Dв)) / 12 \quad (5)$$

где

1.  $tp$  – продолжительность рабочего дня;
2.  $Dp$  – общее число дней в году;
3.  $Dв$  – число выходных и праздничных дней в году.

При подстановке значений месячный фонд рабочего времени составит:

$$F_m = (8 * (366 - 118)) / 12 = 165 \text{ дней}$$

В таблице 9 можно увидеть расчет заработной платы с перечнем исполнителей и их месячных и дневных окладов, а также времени участия в проекте для каждого исполнителя.

Таблица 9 – Затраты на основную заработную плату

№	Должность	Оклад, руб	Дневной оклад, руб	Трудовые затраты, дни	Заработная плата, руб
1	Специалист ИБ	65 000	3151	15	61029
2	Инженер	60 000	2909	16	60097
3	Тестирующий	45 000	2181	4	11265
4	Специалист отдела качества	45 000	2181	1	2816
5	Специалист отдела обучения	40 000	1939	12	30044
6	Специалист технической эксплуатации	55 000	2666	16	55077
7	Специалист отдела закупок	45 000	2181	2	5632
Итого					225960

Расходы на дополнительную заработную плату учитывают все выплаты непосредственно исполнителям за время, не проработанное, но предусмотренное законодательством, в том числе: оплата очередных отпусков, компенсация за неиспользованный отпуск, и др. Величина этих выплат составляет 20% от размера основной заработной платы (5):

$$C_{з.доп} = 0,2 \times C_{з.осн} \quad (5)$$

Отчисления с заработной платы составят для ИТ-компаний — 7,6% с выплат в пределах 1917000Р на сотрудника. Сверх этой суммы взносы не начисляют (6):

$$C_{з.отч} = (C_{з.осн} + C_{з.доп}) \times 7,6\%, \quad (6)$$

В таблице 10 показан расчет затрат на оплату труда сотрудника вместе с дополнительными выплатами.

Таблица 10 – Расчет затрат на оплату труда сотрудника вместе с дополнительными выплатами

№	Должность	Заработная плата, руб.	Расходы на доп. ЗП.	Отчисления с ЗП.	Итого затраты на оплату труда
1	Специалист ИБ	61029	12206	4311	77546

№	Должность	Заработная плата, руб.	Расходы на доп. ЗП.	Отчисления с ЗП.	Итого затраты на оплату труда
2	Инженер	60097	12019	4245	76311
3	Тестирующий	11265	2253	796	14314
4	Специалист отдела качества	2816	563	199	3578
5	Специалист отдела обучения	30044	6009	2122	38175
6	Специалист отдела технической эксплуатации	55077	11015	3890	69982
7	Специалист отдела закупок	5632	1126	398	7156
Итого					287062

Общую сумму расходов по заработной плате равна сумме основной заработной платы всех исполнителей, дополнительной заработной платы и отчислений в нашем случае фонд оплаты труда исполнителей равен 287062 руб.

#### 4.5.2 Затраты на оборудование и программное обеспечение

Затраты, связанные с обеспечением работ оборудованием и программным обеспечением, следует начать с определения состава оборудования и определения необходимости его закупки или аренды. Оборудованием, необходимым для работы, является персональный компьютер и периферийные устройства, которые были приобретены.

В данном случае величина годовых амортизационных отчислений рассчитывается по следующей формуле (7):

$$A_{\Gamma} = C_{\text{бал}} \times H_{\text{ам}}, \quad (7)$$

где

- $A_{\Gamma}$  – сумма годовых амортизационных отчислений, руб;
- $C_{\text{бал}}$  – балансовая стоимость компьютера, руб./шт.;
- $H_{\text{ам}}$  – норма амортизации, %.

$$A_{\Pi} = A_{\Gamma} / 365 \times T_{\text{к}}, \quad (8)$$

где

- $A_{\Pi}$  – сумма амортизационных отчислений за период создания программы дней, руб.;
- $T_{\text{к}}$  – время эксплуатации компьютера при создании программы.

Согласно данным проекта на реализацию требуется 73 дней, при этом время эксплуатации компьютера при создании программы составило 56 дней.

Амортизационные отчисления на компьютер и программное обеспечение производятся линейным методом с учетом срока эксплуатации.

Балансовая стоимость ПЭВМ включает отпускную цену, расходы на транспортировку, монтаж оборудования и его наладку и вычисляется по формуле (9):

$$C_{\text{бал}} = C_{\text{рын}} \times Z_{\text{уст}}, \quad (9)$$

где

- $C_{\text{бал}}$  – балансовая стоимость ПЭВМ, руб.;
- $C_{\text{рын}}$  – рыночная стоимость компьютера, руб./шт.;
- $Z_{\text{уст}}$  – затраты на доставку и установку компьютера, %.

Для проведения работ использовался ПК, который способен проводить емкие вычисления с оптимальной скоростью, со следующими основными характеристиками:

- Intel Core i5-10400F, 6 x 2.9 ГГц;
- GeForce GTX 1650 4GB;
- Память ОЗУ 8 ГБ;
- 512 GB 2.5" SATA;

Стоимость данного ПК на момент проведения работ составляет 50000 рублей, с учетом затрат на доставку.

Стоимость периферийных устройств для работы с данным ПК не учитывается, т.к. они были приобретены еще до возникновения необходимости разработки.

Общая амортизация за время эксплуатации компьютера и программного обеспечения при создании программы вычисляется по формуле (10):

$$A_0 = A_{\text{ЭВМ}} + A_{\text{ПО}}, \quad (10)$$

где

1.  $A_{\text{ЭВМ}}$  – амортизационные отчисления на компьютер за время его эксплуатации;
2.  $A_{\text{ПО}}$  – амортизационные отчисления на программное обеспечение за время его эксплуатации.

Отсюда следует (предполагается, что срок полезного использования составляет 2 года):

$$A_0 = ((50\,000 \times 0,5)/365) \times 56 = 3835,6 \text{ руб.};$$

Расчеты проводились для 1 персонального компьютера, а для работы сотрудников использовалось в общей сложности 7 одинаковых ПК, а значит:

$$A_{\text{П}} = 26\,849,2 \text{ руб.}$$

#### 4.5.3 Расчет затрат на содержание и эксплуатацию оборудования

Затраты на содержание и эксплуатацию оборудования принимаем на уровне 5% от стоимости объектов (11):

$$З_{тр} = C_{бал} \times P_p \times T_k / 365, \quad (11)$$

где

–  $P_p$  – затраты на содержание и эксплуатацию оборудования, %.

При подстановке в формулу (11):

$$З_{тр} = 50\,000 \times 0,05 \times 56 \times 7 + 950216 \times 0,05 / 365 = 50\,195,8 \text{ руб.}$$

#### 4.5.4 Затраты на электроэнергию

Стоимость электроэнергии, потребляемой за год, определяется по формуле (12):

$$З_{эл} = P_{эвм} \times T_{эвм} \times C_{эл} \quad (12),$$

где

1.  $P_{эвм}$  – суммарная мощность ЭВМ, кВт;
2.  $T_{эвм}$  – время работы компьютера, часов;
3.  $C_{эл}$  – стоимость 1 кВт/ч электроэнергии, руб.

Согласно техническому паспорту ЭВМ  $P_{эвм} = 0,4$  кВт/ч электроэнергии, а стоимость 1 кВт/ч электроэнергии в г. Ярославль компании на первое полугодие 2024 года  $C_{эл} = 5,62$  руб. Тогда расчетное значение затрат на электроэнергию равна:

$$З_{эл} = 0,4 \times 56 \times 8 \times 5,62 \times 7 = 8812,16 \text{ руб.}$$

#### 4.5.5 Затраты на внедрение

Затраты на внедрение рассчитываются на основе заработной платы исполнителей, и количества дней на внедрения.

В таблице 11 представлены расчет затрат зарплаты сотрудников на внедрение:

Таблица 11 – Расчет затрат на зарплаты сотрудников на внедрение

№	Должность	Оклад, руб	Дневной оклад, руб	Трудовые затраты, ч.-дн.	Заработная плата, руб
1	Отдел ИБ	65 000	3151	1	3151
2	Инженер	60 000	2909	1	2909
3	Отдел качества	45 000	2181	1	2181
Итого					8241

Накладные расходы, связанные с внедрением проекта, вычисляются, ориентируясь на расходы по основной заработной плате на внедрение. Обычно они составляют от 60% до 100% расходов на основную заработную плату. При



расчётах использовалось значение в 60%. В таблице 12 показаны общие затраты на внедрение проекта.

Таблица 12 – Затраты на внедрение проекта

№	Должность	Основная зар. плата, руб	Дополнительная заработная плата, руб	Отчисления с заработной платы, руб	Накладные расходы, руб	Итого, руб
1	Отдел ИБ	3 151	218	4 311	1 891	9 471
2	Инженер	2 909	215	4 245	1 745	9 114
3	Отдел качества	2 181	10	199	1 309	3 699
Итого						22 284

#### 4.5.6 Накладные расходы

Накладные расходы, связанные с выполнением проекта, вычисляются, ориентируясь на расходы по основной заработной плате. Обычно они составляют от 60% до 100% расходов на основную заработную плату. В данном случае было принято, что данный показатель составляет 60%. Накладные расходы вычисляются по следующей формуле (13)

$$C_{\text{накл}} = 0,6 \times C_{\text{з осн}} \quad (13).$$

Накладные расходы составят:

$$C_{\text{накл}} = 0,6 \times 225960 = 135\,576 \text{ руб.}$$

#### 4.5.7 Прочие расходы

В прочие расходы включаются затраты на покупку необходимого оборудования. Стоимость закупаемого оборудования представлены в таблице 13:

Таблица 13 – Расходы на закупку оборудования

Наименование	Цена, руб. с НДС	Кол-во	Стоимость, руб. с НДС	Описание
АПКШ "Континент" 3.9. ЦУС. Платформа IPС10. КС3	82 373	2	164 746	ЦУС АПКШ "Континент" 3.9 в корпусе Mini-ITX, лицензия ЦУС для 1 ЦУС + 4 КШ.
				3x1000BASE-T RJ45.
				Сертификация: ФСБ (КС3, МСЭ4), ФСТЭК (МЭ А3, СОВ3, УД3).
				ТП уровня Базовый, срок 1 год + Техническая гарантия, срок 1 год.

Наименование	Цена, руб. с НДС	Кол-во	Стоимость, руб. с НДС	Описание
Ключ активации сервиса прямой технической поддержки уровня "Стандартный" для АПКШ "Континент"	32 949	2	65 898	ТП уровня Стандартный, срок 1 год + Техническая гарантия, срок 1 год. В цену включен НДС (20%)
АПКШ "Континент" 3.9. Криптошлюз. Платформа IPC10. КСЗ	71 663	4	286 652	КШ АПКШ "Континент" 3.9 в корпусе Mini-ITX.
				3x1000BASE-T RJ45.
				Сертификация: ФСБ (КСЗ, МСЭ4), ФСТЭК (МЭ АЗ, СОВЗ, УДЗ).
				ТП уровня Базовый, срок 1 год + Техническая гарантия, срок 1 год.
Ключ активации сервиса прямой технической поддержки уровня "Стандартный" для АПКШ "Континент",	57 330	1	229 320	ТП уровня Стандартный, срок 1 год + Техническая гарантия, срок 1 год. В цену включен НДС (20%)
Монтажный комплект на 1 или 2 устройства для АПКШ "Континент"	23 100	3	69 300	Монтажный комплект, для установки на 1 или 2 платформы IPC50 или IPC10 в серверную стойку
Услуга интеграции для внедрения решения	134 300	1	134 300	Настройка двух отказоустойчивых кластеров криптошлюзов IPC-10 и отказоустойчивого кластера ЦУС IPC-10, технический надзор и консультирование в процессе установки и подключения криптошлюзов на объектах в части обеспечения соответствия требованиям регулятора
Итого			950 216	

#### 4.5.8 Общие затраты на разработку

В таблице 14 приведены все итоговые значения на реализацию проекта после ранее проведенных расчетов.

Таблица 14 – Общие затраты на разработку

Статьи затрат	Затраты на проект, руб.	Удельный вес, %
Расходы по заработной плате	287 062	19,4
Амортизационные отчисления	26 849,2	1,8
Затраты на электроэнергию	8 812,16	0,6
Затраты на содержание и эксплуатацию оборудования	50 195,8	3,3
Затраты на внедрение	22 284	1,5
Накладные расходы	135 576	9,2
Прочие расходы	950 216	64,2
Итого	1 480 995,16	100

#### 4.6 Оценка эффекта

Экономическая целесообразность внедрения АПКШ «Континент» обоснована с точки зрения обеспечения безопасности передаваемых данных и заключается в следующем:

1. Соответствие законодательству;
2. Снижение риска утечки и несанкционированного доступа к конфиденциальной информации.

#### 4.7 Вывод по экономической части

В данном разделе выпускной квалификационной работы были рассмотрены экономические аспекты, связанные с организацией работ по внедрению АПКШ «Континент» для создания защищенного канала с шифрованием. Была рассчитана стоимость данного решения и обоснована его целесообразность с экономической точки зрения.

## Заключение

В заключение выпускной квалификационной работы необходимо отметить, что организация зашифрованных каналов для передачи конфиденциальной информации необходима финансовым организациям, в том числе банкам, так как такие компании очень часто становятся жертвами злоумышленников, которые каким-либо образом способны получить доступ к конфиденциальной информации и тем или иным образом использовать ее для получения собственной выгоды.

В ходе выполнения дипломной работы была проведена аналитическая часть, в рамках которой были изучены и описаны существующие решения и выбрано средство реализации VPN при построении защищенной сети. Также была выполнена проектная часть, в результате которой была спроектирована схема построения сети после внедрения АПКШ «Континент», после чего было настроено необходимое оборудование и описана экономическая характеристика разработки.

В целом, данная работа позволяет повысить уровень защищенности информации при ее передаче по открытым каналам связи, а также сохранить конфиденциальность данных клиентов и сотрудников организации, а также проводимых банком транзакций.

## Список использованной литературы

1. Постановление Правительства РФ от 16 апреля 2012 г. N 313;
2. Приказ ФАПСИ от 13 июня 2001 г. N 152;
3. Утечки информации в финансовом секторе за три года | Мир Россия. [Электронный ресурс], - <https://www.infowatch.ru/analytics/analitika/utechki-informatsii-v-finansovom-sektore-za-tri-goda-mir-rossiya> (Дата обращения: 29.02.2024);
4. «Компания ТрансТелеКом» [Электронный ресурс], - <https://company.ttk.ru/?ysclid=lrpflzwwg6206451411> – сайт в Интернете (Дата обращения 03.12.2023);
5. Код безопасности. Континент. [Электронный ресурс], - <https://www.securitycode.ru/> - статья в Интернете (дата обращения 13.11.2023);
6. Государственный реестр сертифицированных средств защиты информации [Электронный ресурс], - <http://fstec.ru/> - сайт в Интернете (дата обращения 12.12.2023);
7. АПКШ Континент 3.9 Формуляр RU.88338853.501430.022 30. [Электронный ресурс], <https://www.securitycode.ru/upload/iblock/> (дата обращения 05.11.2023);
8. АПКШ Континент 3.9 Правила пользования RU.88338853.501430.022 99. [Электронный ресурс], <https://www.securitycode.ru/upload/iblock/> (дата обращения 05.11.2023);
9. ТТК: VPN-ГОСТ. [Электронный ресурс], [https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:%D0%A2%D0%A2%D0%9A:\\_VPN-%D0%93%D0%9E%D0%A1%D0%A2?ysclid=lrqbqznzll916508658](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:%D0%A2%D0%A2%D0%9A:_VPN-%D0%93%D0%9E%D0%A1%D0%A2?ysclid=lrqbqznzll916508658) - статья в Интернете (Дата обращения 15.12.2023);
10. VPN протоколы / Хабр (habr.com). [Электронный ресурс], <https://habr.com/ru/companies/dsec/articles/499718/> (Дата обращения 02.04.2024);
11. Описание MPLS/VPN. [Электронный ресурс], <https://www.opennet.ru/docs/RUS/mpls/mplsvpn.html> (Дата обращения 12.04.2024);
12. MPLS L3VPN / Хабр (habr.com). [Электронный ресурс], <https://habr.com/ru/articles/273679/> (Дата обращения 13.04.2024);
13. АПКШ "Континент". Клиент аутентификации. [Электронный ресурс], <https://www.securitycode.ru/upload/iblock/86b/cdw1412sbfzk7ayb4ejcg6lvjuym19tk/Continent%20-%20AU%20-%20Admin%20Guide.pdf?ysclid=lrpbfjz3zh434117725> (Дата обращения: 14.04.2024);
14. Challenge Handshake Authentication Protocol (CHAP) - GeeksforGeeks (turbopages.org). [Электронный ресурс], [https://translated.turbopages.org/proxy\\_u/en-ru.ru.e7e4e4aa-6654cb24-001d62d0-74722d776562/https/www.geeksforgeeks.org/challenge-handshake-authentication-protocol-chap/](https://translated.turbopages.org/proxy_u/en-ru.ru.e7e4e4aa-6654cb24-001d62d0-74722d776562/https/www.geeksforgeeks.org/challenge-handshake-authentication-protocol-chap/) (Дата обращения 15.04.2024);

15. Описание стенда АПКШ "Континент" 3.9 (securitycode.ru). [Электронный ресурс], [https://www.securitycode.ru/upload/stands/continent39\\_stand.pdf](https://www.securitycode.ru/upload/stands/continent39_stand.pdf) (Дата обращения 14.05.2024);

## Приложение А

Требования из нормативно-правовых актов в области защиты информации при передаче ее по каналам связи и выполнении работ, оказанию услуг в области шифрования информации, техническому обслуживанию, ограничению по развертыванию СКЗИ на стороне ТТК и с использованием площади Заказчика

Требования из нормативно-правовых актов представлены в таблице 1:

Таблица 1 - Лицензионные ограничения ФСБ России

Требование из нормативных документов	Возможные реализуемые меры
<b>Постановление Правительства РФ от 16 апреля 2012 г. N 313</b>	
П.6 а) наличие у соискателя лицензии (лицензиата) права собственности или иного законного основания на владение и использование помещений, сооружений, технологического, испытательного, контрольно-измерительного оборудования и иных объектов, необходимых для осуществления лицензируемой деятельности;	Лицензиат должен иметь права собственности на помещения, необходимые для осуществления лицензируемой деятельности
П.6 в) наличие у соискателя лицензии (лицензиата) условий для соблюдения конфиденциальности информации, необходимых для выполнения работ и оказания услуг, составляющих лицензируемую деятельность, в соответствии с требованиями о соблюдении конфиденциальности информации, установленными ФЗ «Об информации, информационных технологиях и о защите информации»	Аттестация объекта информатизации
П.6 д) наличие в штате у соискателя лицензии (лицензиата) следующего квалифицированного персонала: · руководитель и (или) лицо, уполномоченное руководить работами в рамках лицензируемой деятельности, имеющие высшее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет; · руководитель и (или) лицо, уполномоченное руководить работами в рамках лицензируемой деятельности, имеющие высшее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или)	Наличие сотрудников с необходимой квалификацией

Требование из нормативных документов	Возможные реализуемые меры
<b>Постановление Правительства РФ от 16 апреля 2012 г. N 313</b>	
<p>прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 500 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 3 лет;</p> <ul style="list-style-type: none"> <li>· руководитель и (или) лицо, уполномоченное руководить работами в рамках лицензируемой деятельности, имеющие высшее или среднее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 100 аудиторных часов);</li> <li>· инженерно-технические работники (минимум 2 человека), имеющие высшее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет;</li> <li>· инженерно-технический работник (минимум 1 человек), имеющий высшее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедший переподготовку по одной из специальностей этого направления (нормативный срок - свыше 500 аудиторных часов), а также имеющий стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 3 лет;</li> <li>· инженерно-технический работник, имеющий высшее или среднее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей;</li> </ul>	



Ограничения на развертывание и эксплуатацию СКЗИ на стороне ТТК представлены в таблице 2:

Таблица №2 - Ограничения на развертывание и эксплуатацию СКЗИ на стороне ТТК

<b>Ограничения на развертывание и эксплуатацию СКЗИ на стороне ТТК</b>	
<b>Требование из нормативных документов и формуляров, эксплуатационной документации</b>	<b>Возможные реализуемые меры</b>
<b>Приказ ФАПСИ от 13 июня 2001 г. N 152</b>	
П.6: Для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации лицензиат ФАПСИ создает один или несколько органов криптографической защиты, о чем письменно уведомляет ФАПСИ.	Создание органа криптографической защиты информации для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ
П.7: Орган криптографической защиты осуществляет: <ul style="list-style-type: none"> <li>· проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров используемых СКЗИ, номеров аппаратных, программных и аппаратных-программных средств, где установлены или к которым подключены СКЗИ, с указанием также номеров печатей (пломбиров), которыми опечатаны (опломбированы) технические средства, включая СКЗИ, и результатов проверки функционирования СКЗИ);</li> <li>· разработку мероприятий по обеспечению функционирования и безопасности применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;</li> <li>· обучение лиц, использующих СКЗИ, правилам работы с ними;</li> <li>· поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;</li> </ul>	Регламентация работы органа криптографической защиты в соответствии с указанными требованиями

Ограничения на развертывание и эксплуатацию СКЗИ на стороне ТТК	
Требование из нормативных документов и формуляров, эксплуатационной документации	Возможные реализуемые меры
Приказ ФАПСИ от 13 июня 2001 г. N 152	
<ul style="list-style-type: none"> <li>· учет обслуживаемых обладателей конфиденциальной информации, а также физических лиц, непосредственно допущенных к работе с СКЗИ;</li> <li>· подачу заявок в ФАПСИ или лицензиату, имеющему лицензию ФАПСИ на деятельность по изготовлению ключевых документов для СКЗИ, на изготовление ключевых документов или исходной ключевой информации. Изготовление из исходной ключевой информации ключевых документов, их распределение, рассылку и учет;</li> <li>· контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФАПСИ и настоящей Инструкцией;</li> <li>· расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации; разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;</li> <li>· разработку схемы организации криптографической защиты конфиденциальной информации (с указанием наименования и размещения нижестоящих органов криптографической защиты, если таковые имеются, обладателей конфиденциальной информации, реквизитов договоров на оказание услуг по криптографической защите конфиденциальной информации, а также с указанием типов применяемых СКЗИ и ключевых документов к ним, видов защищаемой информации, используемых совместно с СКЗИ технических средств связи, прикладного и общесистемного программного обеспечения и средств вычислительной техники). Указанную схему утверждает лицензиат ФАПСИ.</li> </ul>	

<b>Ограничения на развертывание и эксплуатацию СКЗИ на стороне ТТК</b>	
<b>Требование из нормативных документов и формуляров, эксплуатационной документации</b>	<b>Возможные реализуемые меры</b>
<b>Приказ ФАПСИ от 13 июня 2001 г. N 152</b>	
<p>П.26: Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземпляроному учету по установленным формам в соответствии с требованиями Положения ПКЗ-99. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно - программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.</p> <p>Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.</p> <p>Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведут органы криптографической защиты и обладатели конфиденциальной информации.</p>	<p>Поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним</p>
<p>П.27: Все полученные обладателем конфиденциальной информации экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.</p> <p>Органы криптографической защиты заводят и ведут на каждого пользователя СКЗИ лицевой счет, в котором регистрируют</p>	<p>Ведение журнала Поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним</p> <p>Ведение Лицевого счета на каждого пользователя СКЗИ</p>

<b>Ограничения на развертывание и эксплуатацию СКЗИ на стороне ТТК</b>	
<b>Требование из нормативных документов и формуляров, эксплуатационной документации</b>	<b>Возможные реализуемые меры</b>
<b>Приказ ФАПСИ от 13 июня 2001 г. N 152</b>	
числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы.	
П.31: Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно - программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища	Опломбировать каждое СКЗИ по отдельности с помощью одноразовых наклеек с уникальным идентификационным признаком, выдать эти наклейки по журналу ответственным лицам, вести журнал «Плановых и внеплановых работ на оборудовании», в котором отражать факт вскрытия наклейки, когда и для чего; Опечатать стойку одноразовыми наклейками с уникальным идентификационным признаком, выдать эти наклейки ответственным лицам, вести журнал «Плановых и внеплановых работ на оборудовании», в котором отражать факт вскрытия наклейки, когда и для чего; Установить на стойку средство СКУД, ограничить перечень лиц, которые могут вскрывать эту стойку средствами СКУД.
П.33: Для пересылки СКЗИ, ключевые документы должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. СКЗИ пересылают отдельно от ключевых документов к ним. На упаковках указывают орган криптографической защиты или пользователя СКЗИ, для которых эти упаковки предназначены. На упаковках для пользователя СКЗИ делают пометку "Лично". Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати. Оформленную таким образом упаковку, при предъявлении фельдсвязью дополнительных требований, помещают во внешнюю упаковку, оформленную согласно предъявляемым требованиям. До первоначальной высылки (или возвращения)	Транспортировка СКЗИ, ключевых документов только фельдсвязью

<b>Ограничения на развертывание и эксплуатацию СКЗИ на стороне ТТК</b>	
<b>Требование из нормативных документов и формуляров, эксплуатационной документации</b>	<b>Возможные реализуемые меры</b>
<b>Приказ ФАПСИ от 13 июня 2001 г. N 152</b>	
адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.	
П.52: Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.	Оборудовать двери замками, утвердить перечень лиц, которые могут находиться в данном помещении, ключ выдавать под подпись; Оборудовать двери помещения системой СКУД. Оборудовать окна первых и последних этажей металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещение.
П.54: Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции (прим. Инструкции ФАПСИ 152).	Должен быть документ (инструкция, регламент, приказ), который определяет периодичность контроля за состоянием средств охраны и саму процедуру (кто и что проверяет). Проверяет руководитель органа криптографической защиты или по его поручению другому сотруднику этого органа совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах. Завести журнал периодической проверки состояния технических средств охраны
П.62: Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в специальных помещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптографических ключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.	Меры из п. 31, 52, 54 Утвердить внутренний документ, в котором отразить, что техническое обслуживание средств СКЗИ и смена криптографических ключей должно производиться в отсутствие лиц, не допущенных к работе с данными СКЗИ.

Ограничения на развертывание и эксплуатацию СКЗИ, размещенного на сторонней площадке представлены в таблице 3:

Таблица 3 – Ограничения на развертывание и эксплуатацию СКЗИ “Компанией ТТК”, размещенного на сторонней площадке

Требование из нормативных документов и формуляров, эксплуатационной документации	Возможные реализуемые меры
<b>Ограничения на развертывание и эксплуатацию СКЗИ Исполнителем, размещенного на сторонней площадке (включая площадку Заказчика)</b>	
<b>Приказ ФАПСИ от 13 июня 2001 г. N 152</b>	
<p>П.20: Пользователи СКЗИ обязаны:</p> <ul style="list-style-type: none"> <li>· не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключях;</li> <li>· соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;</li> <li>· сообщать в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;</li> <li>· сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;</li> <li>· немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.</li> </ul>	<p>Указать в договоре об обязанностях пользователей СКЗИ</p>
<p>П.26: Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету по установленным формам в соответствии с требованиями Положения ПКЗ-99. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное</p>	<p>Ведение Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов</p>

Требование из нормативных документов и формуляров, эксплуатационной документации	Возможные реализуемые меры
<b>Ограничения на развертывание и эксплуатацию СКЗИ Исполнителем, размещенного на сторонней площадке (включая площадку Заказчика)</b>	
<b>Приказ ФАПСИ от 13 июня 2001 г. N 152</b>	
<p>функционирование. Если аппаратные или аппаратно - программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.</p> <p>Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.</p> <p>Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (приложения 1, 2 к Инструкции) ведут органы криптографической защиты и обладатели конфиденциальной информации.</p>	
<p>П.27: Все полученные обладателем конфиденциальной информации экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.</p>	<p>Ведение Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов</p>
<p>П.31: Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно- программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища</p>	<p>Проверка пломб каждого СКЗИ по отдельности с помощью одноразовых наклеек с уникальным идентификационным признаком, выдать эти наклейки по журналу ответственным лицам, вести журнал «Плановых и внеплановых работ на оборудовании», в котором отражать факт вскрытия наклейки, когда и для чего;</p>

