Система ограничения доступа к ресурсам сети Интернет (URL-фильтрации).

Требования к техническому решению

Москва
2013

Список сокращений встречающихся в данном документе:

АПК - Аппаратно-Программный Комплекс;

БД - База Данных;

ЗИП - обозначение, принятое в технических системах для указания на запасные части, инструменты, принадлежности (по ГОСТ 2.601);

МРФ - Макрорегиональный филиал ОАО "Ростелеком";

МСЭ - Международный Союз Электросвязи;

МЭК - Международная Электротехническая Комиссия;

ОАО - Открытое Акционерное Общество;

ПО - Программное Обеспечение;

ПСОД - Подсистема ограничения доступа;

РФ - Российская Федерация;

СОД - Система ограничения доступа;

СФТ - система фильтрации трафика;

ФЗ - Федеральный Закон;

AS - (англ. Autonomous System, автономная система) — это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с Интернетом;

BGP - (англ. Border Gateway Protocol, протокол граничного шлюза) — основной протокол динамической маршрутизации в Интернете;

CD-ROM (англ. Compact Disc Read-Only Memory, читается: «сиди́-ром») — разновидность компакт-дисков с записанными на них данными, доступными только для чтения;

DPI - (англ. Deep Packet Inspection) — технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому;

GBPS - Объем информации, представленный в единицах - Гигабиты в секунду;

HTTP - (англ. HyperText Transfer Protocol — «протокол передачи гипертекста») — протокол прикладного уровня передачи данных (изначально — в виде гипертекстовых документов в формате HTML);

IBM - Компания, один из крупнейших в мире производителей и поставщиков аппаратного и программного обеспечения, а также ИТ-сервисов и консалтинговых услуг;

IP/MPLS - сеть передачи данных Общества, построенная на технологии коммутации пакетов с использованием меток;

IP - Internet Protocol (IP, досл. «межсетевой протокол») — маршрутизируемый протокол сетевого уровня стека TCP/IP;

IPv6 - (англ. Internet Protocol version 6) — новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при её использовании в интернете, за счёт использования длины адреса 128 бит вместо 32;

LU - англ. Labeled Unicast, однонаправленная маршрутизация пакетов до точки назначения с присвоением метки. Используется как опция в протоколе BGP на сети MPLS;

LSP - Label Switched Path - путь трафика в сети MPLS;

MPPS - Объем информации, представленный в единицах - Миллионы пакетов в секунду;

MTBF - Наработка на отказ (англ. Mean time before failure, MTBF) — технический параметр, характеризующий надёжность восстанавливаемого прибора, устройства или технической системы;

RST - Флаг протокола TCP. Значение - Оборвать соединения, сбросить буфер (очистка буфера) (англ. Reset the connection);

SNMP - (англ. Simple Network Management Protocol — простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур UDP/TCP. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие;

SYSLOG - (англ. system log — системный журнал) — стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания логов), использующийся в компьютерных сетях, работающих по протоколу IP;

SSH - (англ. Secure Shell — «безопасная оболочка»[1]) — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов);

TELNET - (англ. TErminaL NETwork) — сетевой протокол для реализации текстового интерфейса по сети (в современной форме — при помощи транспорта TCP). Название «telnet» имеют также некоторые утилиты, реализующие клиентскую часть протокола;

TCP - Transmission Control Protocol (протокол управления передачей) — один из основных протоколов передачи данных Интернета, предназначенный для управления передачей данных в сетях и подсетях TCP/IP;

URL - Uniform Resourse Locator - Единый указатель ресурсов, определитель местонахождения ресурса сети Internet;

1. ЦЕЛЬ ПРОЕКТА

Реализация на сети ОАО «Ростелеком» системы ограничения доступа к ресурсам сети Интернет (URL-фильтрации) для клиентов B2B, B2C, B2G, B2O.

2. ОБЩИЕ ТРЕБОВАНИЯ К РЕШЕНИЮ

2.1 Для клиентов B2B, B2C, B2G, B2O компании ОАО «Ростелеком» должен обеспечиваться функционал URL-фильтрации ресурсов сети Интернет, перечисленных в БД Единого Реестра zapret-info.gov.ru согласно законодательству РФ:

- Федеральный закон от 07.07.2003 №126-ФЗ «О связи»;
- Федеральный закон от 29 декабря 2010 года №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с учетом №139-ФЗ от 28 июля 2012 года);
- Федеральный Закон от 25 июля 2002 года №114-ФЗ «О противодействии экстремистской деятельности»;
- Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2.2 Механизмы URL-фильтрации для клиентов компании, а также исключения из фильтрации должны обеспечиваться согласно БД Единого Реестра zapret-info.gov.ru, а также по расширенным спискам (см. п.3 данных технических требований).

2.3 Система должна обеспечивать сбор и обработку информации для системы «Спутник» (см. п.4.4.5 данных технических требований).

2.4 Система должна обеспечивать сбор и обработку данных по http запросам Интернет-пользователей сети ОАО «Ростелеком» с возможностью последующей передачи данной статистики потенциальным клиентам - пользователям данной услуги. Для данного функционала должны быть предусмотрены АПК-коллекторы на уровне каждого МРФ. (см. п.4.4.6 данных технических требований).

2.5 Система должна включать в себя

- Централизованную систему управления,

- 2 географически-разнесенные платформы фильтрации, например в гг. Москва, Новосибирск, включающие в себя функционал «Спутник»

- Дополнительные АПК-коллекторы, установленные на уровне каждого МРФ, для обеспечения функционала, указанного в п.2.4.

2.6 В техническом решении должно быть предусмотрено полное резервирование АПК в режиме 1+1, в т.ч. модульное резервирование и резервирование на уровне подключения к сети IP/MPLS ОАО «Ростелеком».

2.7 Система должна иметь централизованную структуру подсистем блокировки, управления и оповещения, при этом иметь возможность разнесения аппаратной части для минимизации задержек и обеспечения резервирования:

- архитектура системы должна предусматривать возможность функционирования системы как на одном, так и на нескольких распределенных узлах;
- при отказе работоспособности аппаратной части на основном узле, обеспечивать функционирование через резервный узел;
- при отказе работоспособности системы в целом - пропускать Интернет-трафик без перерыва действия связи для услуг компании;
- обрабатывать запросы клиентов из других AS (МРФ), с учетом минимизации задержек и возможных петель трафика.

2.8 Прогнозируемые объемные показатели системы:

Параметр	Текущее значение	Максимальное значение (экспертная оценка)
Количество записей, в списке ресурсов, подлежащих блокированию шт.	< 1000	< 10 000
Количество Клиентов, шт.	100	< 1 000
Производительность web-сервера (среднее количество запросов в 1 секунду)	180	2 500
Срок хранения статистики блокирования, мес.	36	60
Максимальное количество запросов в 1 секунду по спискам Спутник		5000
Максимальное количество HTTP пакетов в 1 секунду по Иным спискам, Mpps - текущее значение на всей сети	36,108	5 000 URL на 1 платформу
Максимальный объем HTTP трафика в 1 секунду по Иным спискам, Gbps - текущее значение на всей сети	27,643	10 Гбит/с на 1 платформу

2.9 АПК должен быть гибко масштабируемым для увеличения производительности. Поддерживать модульное расширение первоначальных функциональных возможностей без замены ранее установленных основных программных и аппаратных модулей.

2.10 Должна быть обеспечена интеграция с системой управления сети IP/MPLS ОАО «Ростелеком» (на данный момент IBM NetCool для взаимодействия по протоколам snmp, syslog).

2.11 Поддержка протоколов с адресацией формата IPv6.

2.12 Поддержка механизмов резервного копирования и восстановления статистических и информационных данных.

2.13 Поддержка оборудованием АПК возможности доступа и сбора данных по протоколам TELNET, SSH, SNMP.

2.14 Должна быть обеспечена информационная безопасность в процессе предоставления клиентам URL-фильтрации.

2.15 Для разрешения имен в запросах к узлам сети Интернет должно быть предусмотрено использование DNS серверов ОАО «Ростелеком».

2.16 Поддержка ролевой модели предоставления доступа к ресурсам АПК с помощью CLI и web-портала для сотрудников ОАО «Ростелеком».

2.17 Время открытия любой страницы на портале не должно превышать 5 секунд.

3 БАЗОВЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ URL-ФИЛЬТРАЦИИ.

3.1. Автоматическое взаимодействие со списком сайтов из единого реестра zapret-info.gov.ru:

- Обеспечение автоматической выгрузки данных из единого реестра не реже чем 1 раз в час;
- Возможность выгрузки по запросу;

3.2 Автоматическое конфигурирование сетевого оборудования для притягивания на систему блокировки маршрутов на запрещенные ресурсы;

3.3 Проверка соответствия IP и URL при обнаружении запроса к запрещенному сайту из Единого Реестра и блокировку по URL;

3.3.1 Блокировка запрещенных URL из БД Единого Реестра;

3.3.2 При размещении на одном IP нескольких URL система должна осуществлять блокировку только запрещенных URL;

3.3.3 При размещении на одном домене нескольких URL система должна осуществлять блокировку только запрещенных URL;

3.3.4 Решение должно обеспечивать возможность защиты от подставных IP, для случаев когда DNS-сервис отдает СФТ подставной IP-адрес, при этом на остальные запросы выдает действительный IP-адрес.

3.4 Возможность фильтрации, а также исключения из фильтрации запрещенных URL для клиентов ОАО «Ростелеком»:

- по source-IP;
- по BGP community;
- по номеру AS.

3.5 Ведение статистики запросов и блокирования, логирование действий персонала, протоколирование изменений списка ресурсов и настроек с указанием времени внесения изменений;

3.6 Информирование абонента о недоступности URL;

3.7 Наличие системы управления с функциями: общее администрирование, логирование событий, синхронизация с БД Единого Реестра, управление учетными записями, создание групповых политик доступа, автоматическое управление настройками сетевого оборудования в части конфигурирования и обновления маршрутов на запрещенные URL.

3.8 Требования к доставке трафика на сомнительные IP (содержащиеся в БД Единого Реестра) на платформу фильтрации :

- получение маршрутной информации Интернет при помощи BGP LU сессий, связывающих АПК с оборудованием сети IP/MPLS;
- анонсы маршрутов /32 на запрещенные ресурсы на оборудование сети IP/MPLS через next-hop АПК.
- трафик, прошедший обработку на АПК должен уходить с двумя метками по маршруту, полученному по BGP LU в LSP до оборудования IP/MPLS и далее в Интернет.
- в случае, если запрос был адресован на запрещенный URL клиенту должен отправляться TCP RST и http redirect.

3.9 СФТ должна функционировать по следующей схеме:

Рис.1 Схема функционирования системы.

4 РАСШИРЕННЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ URL-ФИЛЬТРАЦИИ.

4.1 Правила обработки Списков Спутник и «Иных списков».

4.1.1 Алгоритм обработки Списков Спутник.

URL поисковых запросов пользователей Интернет в системах Google, Yandex, Mail.Ru, Habrahabr.ru и др. системах, указанных в Списке Спутник, должны :

- направляться на платформу фильтрации для обработки;
- логироваться и передаваться на сервер «Спутник» по протоколу syslog;

4.1.2 Объем данных представлен в п.2.8.

4.1.3 Формат выходных данных для «Спутник» должен соответствовать требованиям, описанным в разделе 4.4.5.

4.1.4. HTTP запросы пользователей Интернет к ресурсам указанным в Иных списках, должны направляться на платформу фильтрации для обработки согласно формату и алгоритму указанному в п. 4.4.6.

4.2 Требования к блокировке:

4.2.1 Система должна обеспечивать фильтрацию трафика магистральной и макрорегиональных сетей Общества.

4.2.2 Возможность фильтрации трафика должна быть осуществима при любом способе доступа: по IP, доменному имени, указателю страницы с доменным именем, указателю страницы с IP адресом.

4.2.3 При попытке обращения Пользователя к запрещенному ресурсу должны быть предусмотрены несколько сценариев работы Системы:

- Доступ не ограничивается, поскольку Пользователь не входит в «Зону фильтрации». В случае наличия ресурса в Списке Спутник система должна отработать запросы (URL) в соответствии с Правилами обработки Списков Спутник.
- Доступ не ограничивается, поскольку ресурс входит в «Белый список» (параметр «Разрешение блокирования» не установлен), формируется предупреждение. В случае наличия ресурса в Списке Спутник система должна отработать запросы (URL) в соответствии с Правилами обработки Списков Спутник.
- Доступ ограничивается, ресурс входит в «Белый список» (параметр «Разрешение блокирования» установлен), формируется предупреждение. Описание «Белого списка» и др. списков обработки данных - см. в п. 4.4.3. В случае наличия ресурса в Списке Спутник система должна отработать запросы (URL) в соответствии с Правилами обработки Списков Спутник.
- Доступ ограничивается, Пользователю не демонстрируется страница «заглушка». В случае наличия ресурса в Списке Спутник система должна отработать запросы (URL) в соответствии с Правилами обработки Списков Спутник.
- Доступ ограничивается, Пользователю демонстрируется страница «заглушка» предусмотренного для него варианта. В случае наличия ресурса в Списке Спутник система должна отработать запросы (URL) в соответствии с Правилами обработки Списков Спутник.

4.3 Требования к подсистемам:

Данные требования разбиты на модули по функциональной принадлежности и не накладывают обязательств к реализации Системы на базе отдельных функциональных элементов, т.е. возможно комбинирование функционала.

4.3.1 Подсистема работы с базой данных Единого реестра (БД):

- Взаимодействие с Единым реестром.

- Ведение списка заблокированных ресурсов.
- Протоколирование изменений списка ресурсов и изменения настроек блокировки с указанием времени и источника внесения изменений.
- Протоколирование действий персонала.
- Сбор и хранение статистики блокирования.

4.3.2 Подсистема ограничения доступа (ПСОД).

- Взаимодействие с БД.
- Передачу статистики в БД.
- Анализ поступающего трафика.
- Обнаружение запроса соответствующего условиям фильтрации.
- Перенаправление запроса Пользователя на web-сервер.

4.3.3 Web-сервер

Web-сервер осуществляет:

- Хранение нескольких вариантов Страниц «заглушек».
- Демонстрацию Страницы «заглушки» Пользователю.
- Передачу статистики блокировки в БД.

4.3.4 Графический веб-интерфейс:

Веб-интерфейс дает возможность получить:

- Актуальный список заблокированных ресурсов.
- Состояние блокировки.
- Статистику блокирования по каждому ресурсу.
- Лог изменений списка ресурсов.

4.4 Работа с расширенными списками:

4.4.1 Схема работы системы URL-фильтрации.

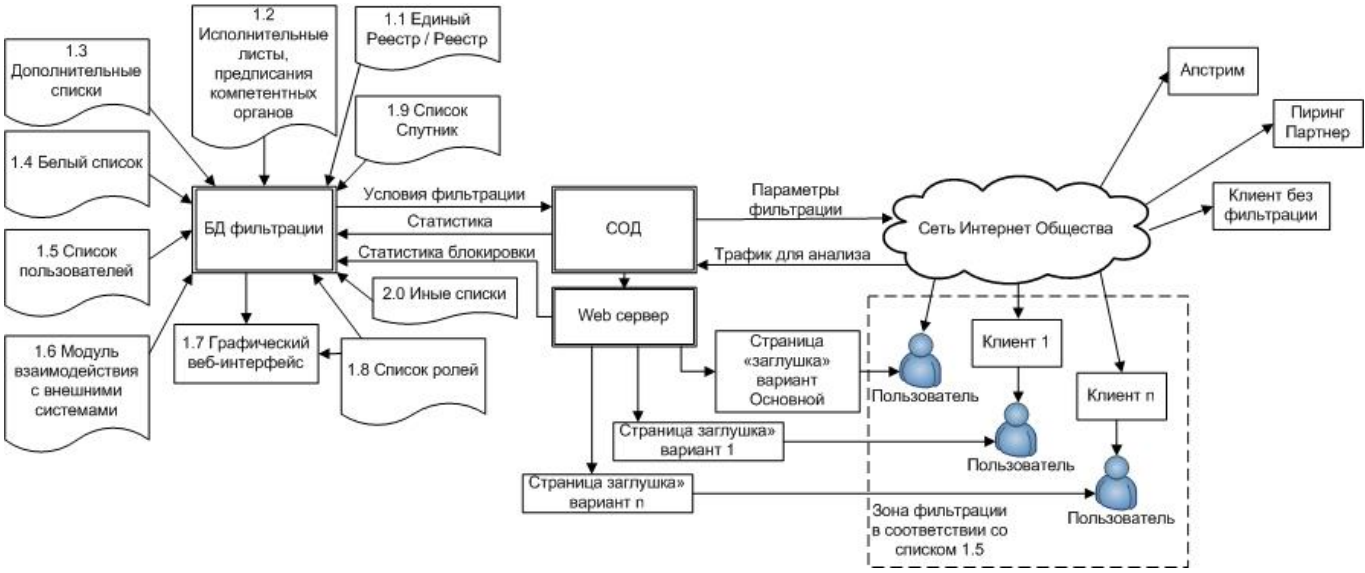

Рис. 2. Общая схема работы системы.

4.4.2 Система состоит из подсистемы ограничения доступа, подсистемы работы с БД фильтрации и web-сервера. БД формирует условия фильтрации посредством которых ПСОД применяет параметры фильтрации на сети Интернет Общества. ПСОД на основании обработки трафика для анализа принимает решение о необходимости блокировки трафика и перенаправления Пользователя на существующий web-сервер. В случае перенаправления запроса Пользователя на web-сервер последний в соответствии с признаком из Списка пользователей (на схеме 1.5) отображает необходимую Страницу «заглушку». Должна быть предусмотрена возможность использования нескольких вариантов таких Страниц:

a. Основной – для всех Пользователей Общества и Пользователей тех Клиентов, для которых не создано специального варианта страницы именно под них.
b. Различные варианты – для Пользователей Клиентов, для которых создан соответствующий вариант страницы.

4.4.3 БД должна формироваться из следующих источников:

- Единый реестр (на схеме 1.1). Взаимодействие БД и Единого реестра должно быть автоматизировано. В БД фильтрации должна быть отражена вся информация из Единого реестра. Признаком ресурса должен являться IP, подсеть, доменное имя, URL. При этом в первую очередь фильтрация осуществляется по доменному имени/URL с возможностью корректировки.

- Информация из исполнительных листов, судебных решений в отношении ОАО «Ростелеком» и иных предписаний (на схеме 1.2). Должна быть предусмотрена возможность прикрепления файлов сканированных копий.
- Дополнительные списки – списки ресурсов, формируемые вручную на основании различных критериев. Признаком ресурса должен являться IP, подсеть, доменное имя, URL, AS или комьюнити. Дополнительно должна быть предусмотрена возможность указать следует ли показывать страницу «заглушку» при попытке доступа к ресурсу из данного списка (на схеме 1.3).
- Белый список – список ресурсов, доступ к которым не должен быть ограничен. Признаком ресурса должен являться IP, подсеть, доменное имя, URL, AS или комьюнити. Для каждого ресурса Белого списка необходимо предусмотреть параметр «Разрешение блокирования». Дополнительно должна быть возможность указания адресов эл. почты для отправки уведомлений. В случае если ресурс, содержащийся в «Белом списке» вносится в БД из других источников (на схеме 1.1-1.3) должно быть сформировано соответствующее предупреждение. Предупреждение должно выводиться в графическом интерфейсе (на схеме 1.6), параллельно должны рассылаться соответствующие уведомления на указанные ранее адреса эл. почты. Трафик до ресурса блокироваться не должен (на схеме 1.4), если параметр «Разрешение блокирования» не активен. Если параметр «Разрешения блокирования» активен, трафик должен быть заблокирован.
- Списки Пользователей – список, содержащий Пользователей по отношению к трафику которых фильтрация должна осуществляться в соответствии с прописанными для них правилами. В правилах указывается, какой из вариантов страницы «заглушки» должен быть показан, если показ страницы предусмотрен, должен ли по отношению к Пользователю применяться «Белый список». Признаком Пользователя должен являться IP, подсеть, AS или комьюнити (на схеме 1.5).
- Модуль взаимодействия с внешними системами – интерфейс, позволяющий взаимодействовать с внешними информационными системами, в том числе с CMS Общества (на схеме 1.6).
- Графический интерфейс – веб-интерфейс, позволяющий получить список текущих блокировок, историю изменения списка, протоколирование действий и иную информацию. Количество доступной информации, а также возможные

действия регламентируются учетной записью в соответствии со списком ролей (на схеме 1.7).

- Список ролей – список учетных записей системы, которым доступны различные действия в зависимости от типа.
- Список Спутник – список ресурсов, запросы (URL) на которые должны быть обработаны в соответствии с Правилами обработки Списков Спутник, указанными в п. 4.4.5. Признаком ресурса должен являться IP или доменное имя, URL Наличие какого либо ресурса в Списке Спутник никак не должно влиять на доступ к данному ресурсу.
- Иные списки – списки ресурсов, HTTP запросы на которые должны быть обработаны в соответствии с Правилами обработки Иных списков (на схеме 2.0). Признаком ресурса должен являться IP адрес, диапазоны IP адресов. Обработка данных по этим спискам не должна оказывать влияние на доступность указанных в них ресурсах или приводить к деградации производительности СФТ, влияющей на выполнение основной функции – фильтрации трафика.

4.4.4 Функционирование ПСОД осуществляется на основании следующих данных:

- Трафик для анализа – трафик, направляемый в систему URL-фильтрации для последующего анализа и принятия решения о дальнейших действиях.
- Условия фильтрации – признаки, позволяющие ПСОД принять решение о необходимости ограничения доступа и его порядке.
- Параметры фильтрации – признаки, позволяющие определить «подозрительный» трафик, который должен быть направлен в систему.
- Перенаправление на web-сервер – перенаправление запросов Пользователя на web- сервер для последующей демонстрации Страницы «заглушки».
- Статистика ПСОД – информация о действиях, совершаемых ПСОД. Ресурсы из Списка Спутник не должны включаться в статистику, если они не находятся в других списках.

4.4.5 Требования для функционала «Спутник».

URL поисковых запросов пользователей Интернет в системах Google.ru, Yandex.ru, Mail.Ru, Habrahabr.ru и др. системах, указанных в Списке Спутник, должны :

- направляться на платформу фильтрации для обработки;
- передаваться на сервер «Спутник» по протоколу syslog (протокол TCP), совместимым с принимающим сервером syslog-ng версии 3.2.5;

- в случае недоступности принимающего сервера «Спутник» повторная попытка доставки данных осуществляется в течение 10 секунд. Принимающий сервер считается недоступным, если попытка соединения для отправки данных не была завершена за 10 секунд (таймаут 10 секунд). По истечению этого времени данные удаляются.

На Рисунке 3 показана примерная схема Call Flow взаимодействия пользователя и поисковика. Точки 3,5,7 попадают под правила формирования сообщений в сторону Спутника, и именно из них будут сформированы сообщения по протоколу syslog.

Требования к выходным данным

Выходные данные должны содержать строки следующего формата:
<ts> \t <id> \t <URL> \t <URLReferrer> \t <User Agent>,
где
ts − временная метка в формате unixtime (количество секунд, прошедших с полуночи (00:00:00 UTC) 1 января 1970 года (четверг), например 13 февраля 2009 года, 23:31:30 UTC это 1234567890),
\t – табуляция,
id − идентификатор пользователя, получаемый путем хеширования IP адреса отправителя,
URL − ссылка на интернет-ресурс (URL),
URLReferrer − ссылка на интернет-ресурс (URL) источника запроса,
User Agent − клиентское приложение, использующее определенный сетевой протокол.

Пример выходных данных:

1325376000 1417374768 http://www.odnoklassniki.ru/ http://yandex.ru/yandsearch?lr=213&text=%D0%BE%D0%B4%D0%BD%D0%BE%D0%BA%D0%BB%D0%B0%D1%81%D1%81%D0%BD%D0%B8%D0%BA%D0%B8 Mozilla/5.0 (Windows NT 5.0; rv:8.0) Gecko/20100101 Firefox/8.0
1325376000 1536658436 http://m.odnoklassniki.ru/dk?st.cmd=userMain&tkn=2435 http://yandex.ru/yandsearch?text=%D0%BE%D0%B4%D0%BD%D0%BE%D0%BA%D0%BB%D0%B0%D1%81%D1%81%D0%BD%D0%B8%D0%BA%D0%B8%20%D0%BC%D0%BE%D0%B1%D0%B8%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F%20%D0%B2%D0

%B5%D1%80%D1%81%D0%B8%D1%8F&lr=213 SonyEricssonW880i/R1JC Browser/NetFront/3.3 Profile/MIDP-2.0 Configuration/CLDC-1.1

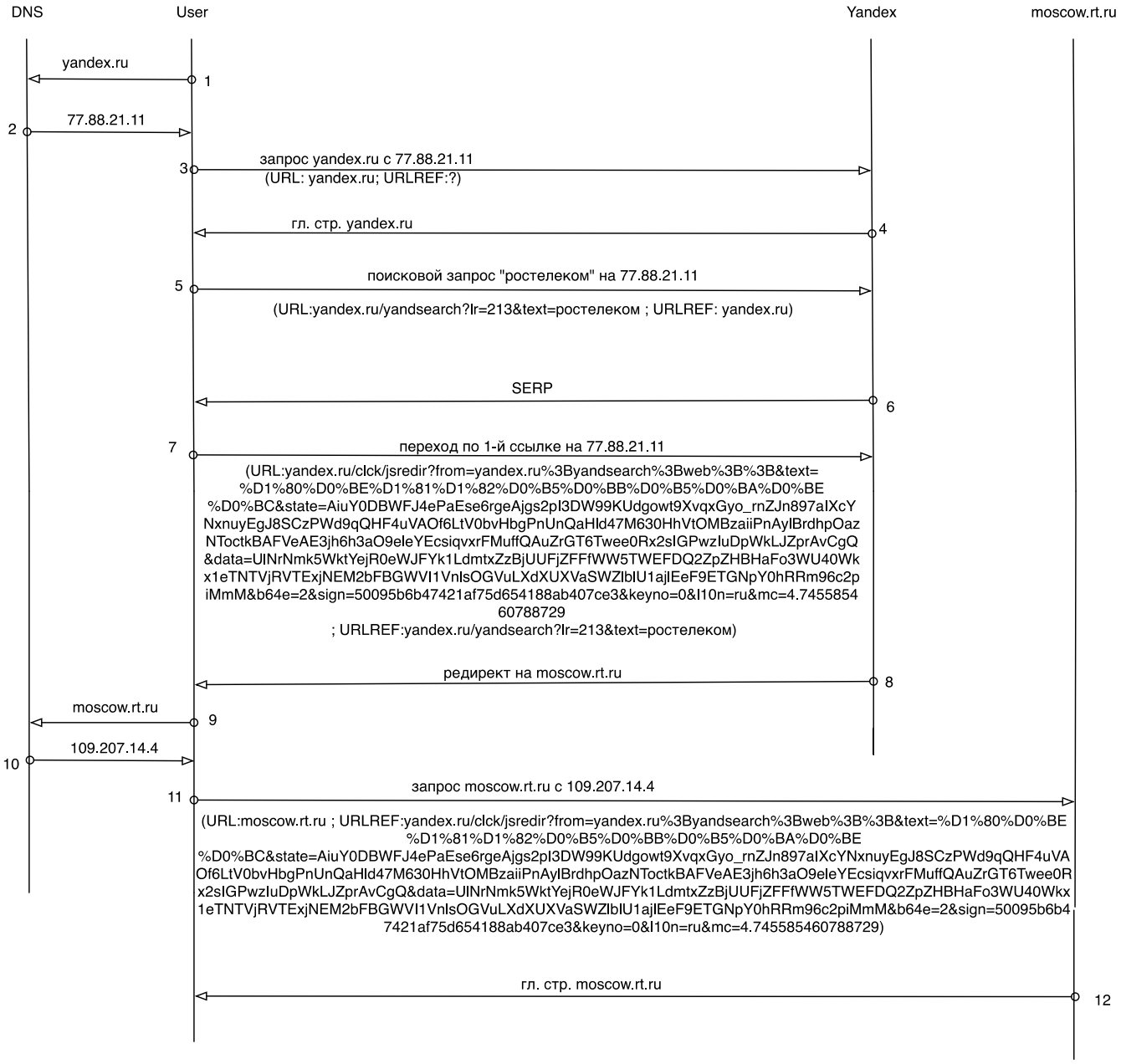

Рис. 3 Call-Flow.

4.4.6 Правила обработки «Иных списков».

HTTP запросы пользователей Интернет к ресурсам указанным в Иных списках, должны :

- направляться на платформу фильтрации для обработки;
- из запросов должна выделяться следующая информация

- хэшированный (анонимизированный) идентификатор;
- HTTP GET URL
- IP адрес
- USER Agent
- Referer
- Timestamp

- для некоторых ограниченных списков помимо информации перечисленной в предыдущем пункте собираются значения Cookie
- данная информация в режиме «реального времени» передается и в СТФ не хранится

5 СОСТАВ РЕШЕНИЯ

Необходимо предоставить следующую информацию:

5.1 Стоимость оборудования (заказные спецификации) на условиях поставки DDP. Стоимость указывается в рублях РФ с учетом всех налогов, таможенных пошлин и сборов) и стоимость работ и услуг (в рублях РФ). Отдельно указывается курс пересчета стоимостей с долларов США в рубли РФ.

5.2 Стоимость монтажных и пуско-наладочных работ при условии, что работы выполняются Поставщиком (партнером поставщика) полностью под ключ.

5.3 Стоимость обучения обслуживающего персонала (с указанием программы и сроков обучения по каждому курсу, присваиваемого уровня квалификации и типа операций с оборудованием, разрешенного после этого курса) и подтверждение соответствия требованиям, указанным в «Требованиях к обучению».

5.4 Относительный план-график реализации проекта.

5.5 Гарантийные обязательства по поставляемому оборудованию и программному обеспечению, продолжительность периода гарантийного обслуживания оборудования описаны в Приложении А: Требования к составу услуг гарантийной и постгарантийной поддержки.

5.6 Система должна включать в своем составе расширенную техническую поддержку системы сроком на 3 года. Расширенная поддержка системы должна включать возможные доработки системы под нужны ОАО «Ростелеком», в рамках функционала описанного в данных Технических требованиях, с учетом развития сети IP/MPLS.

6 ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Требования к информационной безопасности при разработке тех задания на систему:

6.1 Разрабатываемый АПК должен отвечать требованиям Федерального закона «Об информации, информационных технологиях и о защите информации»;

6.2 Требования к защите информации от несанкционированного доступа:

6.3 Выполнение всех функций АПК должно осуществляться штатными средствами самой системы и таким образом, что это не приведет к возможности запуска на рабочих местах нештатных программных средств;

6.4 АПК должен обеспечивать доступ к системе только авторизованных пользователей;

6.5 АПК должен обеспечивать защиту от несанкционированного доступа к информации;

6.6 АПК должен обеспечивать информирование администратора о попытке НСД, регистрацию данного события в журнале аудита; регистрацию в журнале аудита любого неправильного набора пароля.

6.7 АПК должен обеспечивать отсутствие возможности выполнения администраторами и любыми пользователями прямого соединения с базой данных в обход подсистемы администрирования.

6.8 АПК должен обеспечивать выполнение административных функций системы, в том числе управление правами пользователей на прикладном уровне в виде отдельной роли.

6.9 Территориальная распределенность АПК может потребовать реализации иерархического администрирования с возможностью делегирования прав нижестоящим администраторам.

6.10 В системе допускается использование внешних программных средств только в том случае, если их вызов не создает предпосылок к нарушению защиты (расширенные возможности по работе с файловой системой, возможность создания исполняемого/интерпретируемого программного кода, возможность запуска из данных средств нештатных программ и т.д.);

6.11 Требования к идентификации и аутентификации.

6.11.1 Система должна обеспечивать пользователю возможность предоставления закрепленных за ним прав доступа к информации, экранным формам и функциям АПК.

6.11.2 АПК должен обеспечивать возможность предоставления пользователю доступа к информации, экранным формам и функциям АПК только после предъявления уникального персонифицированного идентификатора (имени) пользователя и проведения процедуры аутентификации на основе некоторой вводимой пользователем информации (пароль, ключи).

6.11.3 АПК должен обеспечивать возможность регистрации действий пользователя средствами подсистемы аудита.

6.11.4 АПК должен обеспечивать возможность определения авторства каждой операции в системе АПК и отсутствие неавторизованных операций на основе уникальных персонифицированных идентификаторов каждого пользователя, процедуры аутентификации и протоколирования действий пользователей в журналах аудита.

6.11.5 АПК должен обеспечивать наличие развитой системы управления аутентификационной информацией пользователей (паролями, ключами) и механизмов контроля за ее качеством и использованием, обладающие следующими характеристиками:

a. Длина пароля не менее восьми символов;
b. Периодическая принудительная смена паролей не реже, чем раз в месяц;
c. Возможность установки администратором признака принудительной смены пароля пользователя при следующем входе пользователя в систему АПК;
d. Возможность самостоятельного изменения пользователями своего пароля в любое время;
e. Автоматическая установка новому пользователю пароля, задаваемого администратором системы АПК;
f. Предоставление доступа к информации при первом входе пользователя в системе АПК только после смены им пароля, установленного администратором, на его личный пароль;
g. Хранение парольной «истории» пользователя, т.е. списка контрольных значений (сумм) нескольких предыдущих паролей пользователя (рекомендуется хранить пять паролей), и невозможность при смене пароля выбора пароля из этого списка;
h. Выполнение анализа качества выбираемых пользователями паролей;

i. При вводе пароля пользователем на запрос системы символы пароля на экране не отображаются (отображается только число введенных символов);
j. Хранение паролей в системе и передача по каналу связи от клиента серверу таким образом, чтобы исключить возможность восстановления пароля пользователя (кроме как методом полного перебора) по хранящейся в системе или перехваченной в канале связи информации;
k. Перехваченная передаваемая по каналу связи аутентифицирующая информация не должна позволять осуществлять вход в систему через прикладную систему.

6.12 Требования к разграничению прав доступа.

- Права пользователей в системе должны определяться согласно модели ролевых групп;
- Права доступа в системе должны назначаться как отдельному пользователю, так и группе пользователей;
- Пользователи, отнесенные к группе должны получать права, назначенные на группу;
- Система должна обеспечивать наличие механизма разграничения прав доступа, обеспечивающего возможность просмотра сотрудником только разрешенных ему данных.
- Система должна обеспечивать возможность удаления пользователей из системы путем перевода их в разряд заблокированных без возможности совершения операций под их именами и без возможности отмены этого статуса.

Система должна обеспечивать возможность блокирования работы отдельных пользователей с возможностью снятия блокировки:

a. На некоторый промежуток времени;
b. Начиная с некоторого момента времени;
c. Автоматически после превышения задаваемого настройкой системы периода неактивности пользователя (отсутствия успешных входов в систему).

- Система должна обеспечивать отсутствие возможности удаления информации о пользователях, зарегистрированных в системе, в том числе заблокированных.

- Система должна обеспечивать исключение возможности доступа администратора системы к «боевым» паролям пользователей.
- Система должна обеспечивать возможность предоставления доступа к спискам пользователей, а также их правам (группы, к которым принадлежит пользователь, роли, назначенные пользователю (т.е. выполнение им ролевых функций), объектам, доступным пользователю) из единого дерева прав по единым непротиворечивым правилам.

6.13 Система должна иметь возможность интеграции с внешними серверами аутентификации и авторизации.

6.14 Система должна иметь возможность разграничения доступа к серверам не сетевом уровне.

6.15 Система должна осуществлять проверку и фильтрацию вводимых данных пользователем системы через формы веб-интерфейса.

6.16 Система должна иметь возможность установку патчей/обновлений локально со сменного носителя, либо по сети с доверительного сервера расположенного в технологической сети Ростелеком с использованием протоколов ftp/scp.

6.17 Система не должна осуществлять подключений к внешним серверам не указанным в ТЗ и расположенным в сети Интернет.

7 ТРЕБОВАНИЯ К ЭЛЕКТРОПИТАНИЮ

7.1 Поставщик должен представить данные о потребности по электропитанию по каждому типу оборудования, допустимых отклонениях параметров первичных источников электропитания постоянного тока;

7.2 Оборудование не должно повреждаться при понижении напряжения ниже нижнего предела и восстанавливать свою работоспособность при восстановлении напряжения до допустимого значения. Поставщик должен предоставить данные о времени полного восстановления параметров аппаратуры во всех случаях занижения или пропадания напряжения первичного источника на вводах питания после восстановления напряжения без вмешательства персонала;

7.3 Если электропитание осуществляется от сети переменного тока с номинальным напряжением 220 В, то Поставщик должен представить

данные о потребности по электропитанию от сети переменного тока по каждому типу оборудования.

8 ТРЕБОВАНИЯ К УСЛОВИЯМ ЭКСПЛУАТАЦИИ

8.1 Оборудование АПК должно обеспечивать непрерывный круглосуточный режим работы;

8.2 Диапазон рабочих температур, при котором должны гарантироваться параметры оборудования АПК: +5 ˚С до +40 ˚С;

8.3 Нижнее допустимое атмосферное давление: 60 кПа (450 мм рт. ст.);

8.4 Относительная влажность: 80 % при +25 ˚С;

8.5 Механические удары, обычные при эксплуатации, такие как срабатывание переключателей, соединение или разъединение жгутов, закрывание створок стоек и т.п. не должны вызывать микрофонного эффекта в цепи любого из передаваемых сигналов;

8.6 Механический резонанс должен отсутствовать в диапазоне частот до 25 Гц;

8.7 Оборудование должно быть работоспособным и сохранять параметры после воздействия вибрации с амплитудой виброускорения 2 g в течение 30 мин на частоте 25 Гц.

9 ТРЕБОВАНИЯ К НАДЁЖНОСТИ

9.1 Поставщик должен представить данные о среднем времени наработки на отказ (MTBF) каждого типа оборудования, блоков, плат и модулей входящих в его состав;

9.2 Поставщик должен представить данные о среднем времени восстановления оборудования после отказа;

9.3 Блоки и субблоки без резервирования должны быть заложены в ЗИП, рассчитанный с учетом MTBF и оптимизации по стоимости;

9.4 Срок службы оборудования (включая ПО) при круглосуточном режиме работы должен быть не менее 10 лет.

10 ТРЕБОВАНИЯ К УРОВНЮ ЗВУКА, СОЗДАВАЕМОМУ АППАРАТУРОЙ

10.1 Уровень звука и эквивалентный уровень звука, создаваемые аппаратурой на рабочем месте в соответствии с ГОСТ 12.0.003-83 не должны превышать 65 дБ А.

11 ТРЕБОВАНИЯ К СОСТАВУ ПОСТАВЛЯЕМОЙ ДОКУМЕНТАЦИИ

11.1 Поставщиком должны быть представлены данные о предлагаемой к поставке эксплуатационно-технической документации в составе и объеме достаточном для ввода в эксплуатацию и технического обслуживания (включая технические описания, инструкции по эксплуатации, руководства по шеф-монтажу и вводу в эксплуатацию, руководства оператора и администратора всех подсистем, руководства по инсталляции ПО, полное описание всех реализованных протокольных стеков интерфейсов, описание программ и методик испытаний) оборудования АПК, включая входящие в состав покупные (у третьих сторон) аппаратно-программные средства;

11.2 Документация должна также включать системный том с описанием работы (взаимодействия) всего комплекса технических средств АПК и описание всей конфигурации проекта;

11.3 Вся документация должна соответствовать принятым стандартам. По возможности, должны быть использованы стандартизированные символы и термины, рекомендованные МСЭ и МЭК;

11.4 Допускается поставка схем и спецификаций на английском языке;

11.5 Документация на русском языке должна поставляться как в отпечатанном виде, так и в электронном виде (на CD-ROM в формате Adobe Acrobat или MS OFFICE). Использование другого программного обеспечения должно быть согласовано с Заказчиком дополнительно.

12 ТРЕБОВАНИЯ К ГАРАНТИЙНЫМ ОБЯЗАТЕЛЬСТВАМ

12.1 Поставщик должен гарантировать соответствие качества оборудования требованиям настоящих технических требований;

12.2 Гарантийный срок должен быть не менее 36 месяцев с момента ввода в эксплуатацию аппаратуры;

12.3 В течение гарантийного срока Поставщик должен производить безвозмездную замену или ремонт аппаратуры. Гарантии не распространяются на дефекты, возникающие вследствие некомпетентного обращения, обслуживания, хранения и транспортирования;

12.4 После истечения гарантийного срока Поставщик должен обеспечить по дополнительному договору о послегарантийном обслуживании платную поставку запасного имущества и принадлежностей (ЗИП) в течение всего срока службы аппаратуры. Состав послегарантийного ЗИП и условия поставки должны оговариваться дополнительно.

13 ТРЕБОВАНИЯ К ЗИП

В связи с предъявлением требований по полному резервированию (1+1) требования к ЗИП не предъявляются.

14 ТРЕБОВАНИЯ К РЕМОНТУ

14.1 Должна обеспечиваться возможность быстрой замены поврежденного оборудования и исправления несъемного оборудования;

14.2 Замена съемных элементов и однотипных блоков, не содержащих элементов эксплуатационной регулировки, должна выполняться без подстройки оборудования;

14.3 Замена съемных элементов должна обеспечиваться без выключения электропитания;

14.4 Поставщик в течение срока службы оборудования обеспечивает его ремонт;

14.5 После истечения гарантийного периода по требованию Заказчика Поставщик выполняет необходимый ремонт (предпочтительно в России в сервисном центре фирмы за дополнительную плату или в организованном Заказчиком при содействии Поставщика);

14.6 Время ремонта должно составлять не более 30 рабочих дней плюс 30 дней на транспортировку и таможенные оформления. Время ремонта исчисляется с момента передачи оборудования Поставщику до момента его возврата Заказчику;

14.7 Поставщик представляет Заказчику отчет о каждом проведенном ремонте, указывает причину повреждения и описание выполненной работы, а также ежегодно общую сводную статистическую информацию о проведенных ремонтах.

15 ТРЕБОВАНИЯ К КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНОЙ АППАРАТУРЕ

15.1 Поставщик должен предоставить рекомендованный список приборов, необходимых для проведения нормальной эксплуатации оборудования АПК (локализации неисправностей и их устранения, а также проверки соответствия параметров установленным нормам);

15.2 Заказчик решает вопрос о целесообразности приобретения приборов для эксплуатационных целей у Поставщика оборудования АПК, либо непосредственно у фирм-поставщиков измерительного оборудования на основании анализа технических и стоимостных данных. Заказчик производит закупку измерительных приборов для технической эксплуатации по отдельным контрактам;

15.3 Контрольное и измерительное оборудование, используемое при пуско-наладочных работах, должно поставляться Поставщиком. Контрольное и измерительное оборудование должно быть укомплектовано шнурами, переходниками и приспособлениями для подключения к испытуемому оборудованию;

15.4 Приемо-сдаточные испытания должны производиться с использованием приборов, имеющих сертификат об утверждении типа Госстандарта РФ, сертификат соответствия Минсвязи России, калибровочные сертификаты и быть проверены в специальных аттестованных метрологических лабораториях Поставщика.

16 ТРЕБОВАНИЯ К УЧЕБНО-ТРЕНИРОВОЧНЫМ СРЕДСТВАМ

a. Базовый курс подготовки специалистов Заказчика проводится специалистами Поставщика в учебных центрах Поставщика и/или Заказчика. Базовый курс подготовки должен охватывать обучение по работам (шеф-монтажа, настройка, эксплуатация, инсталляция ПО) со всем требуемым оборудованием и приборами;

b. В технико-коммерческом предложении Поставщик должен представить подробные программы курсов обучения специалистов, включая обучение работе с аппаратурой, а также те аспекты, которые связаны с обслуживанием аппаратуры, согласовать их с Заказчиком до подписания контракта.

c. Контрольный комплект учебных материалов должен быть передан не позднее двух месяцев до начала учебы;

d. Поставщик вначале обучения должен обеспечить каждого слушателя личным комплектом учебной документации на бумаге и магнитных (или оптических) носителях на русском языке;

e. Поставщик должен предоставить Заказчику копию учебного программного обеспечения и право (лицензию) на его использование в учебном центре Заказчика для повышения квалификации своих специалистов;

f. Поставщик должен предоставить Заказчику предложение о стоимости курсов обучения, включая учебную документацию на русском языке.

17 НЕОБХОДИМЫЕ УСЛУГИ ПОСТАВЩИКА

a. Поставщик должен представить условия оказания следующих услуг:

– Планирование (включая график выполнения работ), инжиниринг данного проекта;

- Технический проект;
- Руководство проектом в части работ, осуществляемых Поставщиком;
- Рабочий проект;
- Эксплуатационная документация, включая типовые конфигурации
- Обучение эксплуатационного персонала Заказчика;
- Доставка оборудования (включая страхование, получение разрешения на ввоз, транспортировку, растаможивание, разгрузку, размещение на площадках Заказчика);
- Монтаж оборудования;
- Пуско-наладочные работы (инсталляция);
- Испытания (тестирование, приемо-сдаточные испытания);
- Гарантийное обслуживание;
- Послегарантийное обслуживание.

b. Поставщик несет ответственность за выполнение выше указанных услуг, а также за качественные показатели АПК. Поставщик отвечает за хранение, доставку, разгрузку, размещение, монтаж, испытание оборудования до получения Акта о приемке. Если во время монтажа, испытания и приемосдаточных испытаний будет повреждена какая-либо часть контрактных материалов по вине Заказчика, за исключением тех случаев, когда это может быть неправильным обращением со стороны Поставщика, Заказчик несет все расходы и издержки по замене поврежденных материалов, если необходимо.

c. В случае, если указания Поставщика, выполненные в точности персоналом Заказчика, потребовали переделок или замены оборудования, дополнительные работы выполняются за счет Поставщика.

18 ТРЕБОВАНИЯ К ИСПЫТАНИЯМ

a. Поставщик должен предложить график и методику проведения испытаний (заводских/стендовых* и/или системных/приемочных), конкретизирующие предлагаемые им испытания с целью демонстрации Заказчику того, что поставленное оборудование установлено и функционирует в соответствии с Техническими требованиями. Испытания должны быть проведены и для всего комплекта запасных частей;

b. Проект программы приемочных испытаний должен быть представлен фирмой не позднее, чем за 2 месяца до начала испытаний;

c. Заказчик имеет право включить в испытания любой дополнительный тест, необходимый, чтобы убедиться, что работа поставленного оборудование во всех отношениях соответствует Техническим требованиям;

d. Обеспечение поставки любого оборудования, необходимого для проведения испытаний и не входящего в список поставляемого оборудования Заказчику для функционирования/обслуживания АПК, является обязательством Поставщика;

e. Тестирование (рабочие испытания) должны проводить представители Исполнителя с участием представителей Заказчика. Результаты должны быть зарегистрированы протоколом, заверены и переданы Заказчику;

f. Приемочные испытания должны проводить представители Заказчика под наблюдением представителей Поставщика. Результаты должны быть зафиксированы Актом приёмки, либо протоколом разногласий, заверены и переданы сторонам (Заказчику и Исполнителю);

g. В случае выявления на испытаниях невозможности выполнения Поставщиком данных Технических требований Заказчика Поставщик должен предложить на согласование приемлемое решение о скидке, допоставке или замене необходимого оборудования за свой счет. В противном случае Поставщик должен осуществить демонтаж, вывоз оборудования и возврат Заказчику всех платежей.