- всех коробок в шкафах, где есть спаренные абоненты

88. С целью получения различных отчётных форм и справок, необходимых в работе, должна быть предусмотрена система гибких отчётов.

2.2.1. Интеграция с внешними системами

89. Система учёта ресурсов должна взаимодействовать с внешними системами для обеспечения целостности БП:

- **CRM**

  - По запросам из системы TelCRM по адресным элементам , RI должен возвращать данные по технической возможности по подключению возможных услуг
    - Технология
    - Свободные ресурсы
    - Доступные сервисы

- По запросам из TelCRM система RI должна переводить ресурсы в статусы свободный, рабочий, бронированный , повреждённый, выведен из эксплуатации, в зависимости от БП
- По запросам из ИС **Интерконнект (межоперторские расчеты)** система **RI** должна передавать информацию по номерным диапазонам и транковым группам
- По запросам из ИС **Провижиненга(SPA)** система **RI** должна выдавать информацию по оборудованию сети участвующего в предоставлении услуги, для последующей передачи системой провижининга команд для активации услуги на оборудование сети

3. НЕФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

3.1. Требования к производительности

1. IT-сервис на текущем КТС должен корректно работать при единовременном количестве запросов:
    - общее кол-во запросов - не более 100 000 в день (6000 в час, 200 в минуту),
2. Решение не должно иметь программно-архитектурных ограничений по производительности: максимальная нагрузка может быть увеличена путем горизонтальной масштабируемости (увеличения ресурсов КТС). Методика расчета максимальной нагрузки (количества запросов в единицу времени/ количества активных пользователей) должна передаваться вместе с решением по результатам нагрузочного тестирования.
3. Время обработки пользовательского запроса не должно превышать 5 минут для 100% от общего числа запросов.

3.2. Требования к доступности и надежности

1. Требуется обеспечить возможность работы IT-сервиса в режиме 365(366)x24x7.
2. Максимальное допустимое время простоя IT-сервиса не должно превышать 175 часов в год в год (надежность уровня 98).
3. Время восстановления доступности IT-сервиса в случае сбоя не должно превышать 4 часов.
4. При выходе из строя ПО не должно оказывать влияние на работу не связанных с ним бизнес-логикой IT-сервисов.
5. Действия пользователей не должны приводить к потере информации, «зависанию» ПО.
6. В случае временной недоступности программных систем/подсистем и/или сбоев на сети, корректная работа IT-сервиса должна восстанавливаться по факту устранения «внешней» неполадки.
7. Система должна работать стабильно и быть устойчивой к различным видам сбоев, в том числе аппаратных и сбоев операционной системы.
8. Система должна обладать средствами создания резервных копий, обеспечивающими возможность полного восстановления данных при аварийных сбоях.

3.3. Требования к логированию

1. Механизм протоколирования сбоев/ ошибок в работе IT-сервиса не должен вносить задержек в работу бизнес-процессов.
2. Необходимо обеспечить логирование потоков данных (выгрузка в текстовый файл): как входящих запросов, так и исходящих. Должны логироваться успешные и неуспешные попытки аутентификации пользователя, а также попытки доступа пользователя к данным /ресурсам ИС. Лог-запись должна содержать:
    - дату и время (timestamp) события;
    - идентификатор пользователя;

- источник события (IP-адрес /идентификатор вызывающей подсистемы);
- название или тип операции/выполненного события;
- значения параметров запросов/ответов;
- результат обработки.

3. ПО должно обеспечивать обнаружение и диагностику ошибок с выдачей соответствующих сообщений администратору через лог-запись, недвусмысленно характеризующую причину сбоя. В лог должна попасть информация о всем пути выполнения операции на данной ИС, приведшем к сбою, без необходимости включать другой уровень логирования и ловить ошибку заново.
4. Система должна производить уведомление администраторов обо всех фактах сбоев в том числе в интерактивном режиме.
5. Для использующих БД решений реализовать на содержащей соответствующую логику схеме БД логирование в таблицу СУБД фактов вызова и результатов работы хранимых процедур. При этом лог-записи должны содержать только данные, принятые в запросе (параметры хранимых процедур), и данные, передаваемые в ответе (значения выходных параметров, а также возвращаемые наборы данных (записи курсоров)).
6. Предусмотреть возможность изменения параметров логирования в режиме онлайн (без рестарта сервисов бизнес-логики).
7. Сервисы бизнес-логики могут удерживать файлы логов только в момент записи в них какой-либо информации, в остальных случаях файлы логов должны быть свободны для перемещения/удаления. Необходимо реализовать механизм ротации файлов логирования с присвоением даты/времени к названию файла, ротация должна организовываться по достижению определенного объема файла или периода времени.

3.4. Требования к мониторингу и контролю показателей качества

1. Должны быть выделены и зафиксированы в предлагаемой реализации ТЗ (документ «Архитектура решения», HLA и т.п.) измеряемые комплексные верхнеуровневые КПЭ здоровья решения, определяющие уровень предоставляемого сервиса.
2. Решение должно обеспечивать возможность измерения КПЭ IT-сервиса. Методика расчета КПЭ должна быть представлена в предлагаемой реализации ТЗ (документ «Архитектура решения», HLA и т.п.).
3. Модель влияния компонентов (КЕ) решения на КПЭ (сервисно-ресурсная модель) должны быть представлены в предлагаемой реализации ТЗ (документ «Архитектура решения», HLA и т.п.).
4. Наборы метрик мониторинга – модели здоровья – для всех типов КЕ (конфигурационных единиц) CPM должны быть представлены в предлагаемой реализации ТЗ (документ «Архитектура решения», HLA и т.п.).
5. Для каждой метрики мониторинга должны быть определены:
   - соответствие модели здоровья;
   - периодичность опроса;
   - тип данных (логический, целое, срока…);
   - единица измерения;

- условия контроля (нарушение которых изменяет статус метрики и формирует сообщение в соответствии с указанной критичностью);
- уровень критичности (согласно спецификации ITU-T X.733);
- инструкция по устранению нештатной ситуации при превышении порогов метрики;

6. В рамках поставки решения должен быть приобретен необходимый пакет лицензий системы мониторинга. При этом от производителя решения должно быть получено официальное заключение о возможности установки и эксплуатации агентов системы мониторинга, используемой в компании.
7. Для случая, если предусмотрена интеграция с системой мониторинга, поставляемой вместе с решением, необходимо выполнение следующих требований:
   - В случае передачи событий по протоколу SNMP требуется предоставить описание формата трапов: MIB-файлы, содержащие описания SNMP трапов NOTIFICATION-TYPE или TRAP-TYPE, в зависимости от версии SNMP.
   - Для каждого события необходимо определить перечень признаков, позволяющих определить принадлежность трапа/события к системе (IP-адрес источника, ключевое значение в одной из переменных трапа, возможно, OID или Enterprise трапа).
   - Требуется предоставить текстовое описание правил дедупликации трапов (подавление большого кол-ва одинаковых или однотипных событий).
8. Требуется предусмотреть возможность мониторинга таких метрик, как:
   - количество запросов по каждой операции в минуту;
   - количество ошибок по каждой операции в минуту (общее и по типам ошибок);
   - количество сессий, установленных с компонентом;
   - количество сессий, установленных с компонентом в минуту;
   - среднее время обработки запроса по типу операции;
   - количество сообщений в очереди на обработку;
   - возраст самого старого объекта в очереди;

3.5. Требования к времени хранения данных и архивации

1. Требуется хранить в оперативной доступности историю произведенных операций за последние 3 года.
2. Необходимо предусмотреть возможность выделения и миграции данных старше 36 месяцев, с целью последующей их архивации на внешних носителях, согласно действующим регламентам Компании.

3.6. Требования к информационной безопасности

3. Система будет иметь возможность идентификации, аутентификации и авторизации пользователей в нескольких экземплярах MS Active Directory без отдельного повторного запроса логина и пароля (SSO).
4. Идентификация и аутентификация внешних систем при предоставлении им данных будет производиться посредством двухсторонней SSL аутентификации.

5. Система будет позволять предоставлять доступ к данным, согласно предварительно настроенным ролям пользователей.
6. Система будет протоколировать все действия пользователей, связанные с изменением данных в системе (аудит).
7. Система будет предоставлять предопределенный набор стандартных ролей с настроенными для них доступами. Данные роли должны быть заведены в MS Active Directory
8. Система должна позволять предоставлять доступ к данным, согласно предварительно настроенным ролям пользователей внутри МГТС с учетом того, что часть информации является коммерческой тайной.
9. Предоставлять доступ системе пользователям за пределами МГТС не предполагается.
10. Система обеспечения безопасности системы должна отвечать требованиям ФЗ-152.

3.7. Требования к пользовательскому интерфейсу системы

1. Требования к рабочим местам пользователей должны соответствовать нормативным документам заказчика:
2. Стандарт "Оснащение автоматизированных рабочих мест" СТ-МГТС-042-2
3. Политики «Обеспечения сотрудников компании ИТ-ресурсами» ПТ-МГТС-022-2.
4. Все интерфейсы пользователей Системы будут выполнены в виде web приложения.
5. Минимальное разрешение экрана для работы web приложение должно быть 1024x768
6. При обновлении пользователем данных на форме, сама форма не будет перерисовываться (то есть должна быть реализована с применением технологии AJAX или её аналогов)
7. Поддерживаемое ПО на клиентских устройствах (браузеры):
    1. Internet Explorer v8.0 и выше
    2. Mozilla Firefox v11 и выше
    3. Google Chrome v18 и выше