

Москва,

2018

**Оглавление**

[1 Общие сведения 4](#_Toc529380229)

[1.1 Полное наименование работ 4](#_Toc529380230)

[1.2 Условное обозначение системы 4](#_Toc529380231)

[1.3 Шифр темы 4](#_Toc529380232)

[1.4 Заказчик 4](#_Toc529380233)

[1.5 Пользователь 4](#_Toc529380234)

[1.6 Пользователи Системы 4](#_Toc529380235)

[1.7 Подрядчик 4](#_Toc529380236)

[1.8 Основание для развития Системы 4](#_Toc529380237)

[1.9 Плановые сроки развития Системы 4](#_Toc529380238)

[1.10 Источник финансирования 4](#_Toc529380239)

[1.11 Порядок финансирования 5](#_Toc529380240)

[1.12 Порядок оформления и предъявления Заказчику результатов работ 5](#_Toc529380241)

[1.13 Перечень нормативно-технических документов, методических материалов, регламентирующих развитие Системы 5](#_Toc529380242)

[1.14 Перечень сокращений 6](#_Toc529380243)

[1.15 Термины и определения, используемые в ТЗ 7](#_Toc529380244)

[2 Назначение и цели развития Системы 10](#_Toc529380245)

[2.1 Назначение Системы 10](#_Toc529380246)

[2.2 Цели и задачи выполнения работ 10](#_Toc529380247)

[3 Характеристики объектов автоматизации 12](#_Toc529380248)

[3.1 Краткие сведения об объекте автоматизации 12](#_Toc529380249)

[3.2 Сведения об условиях эксплуатации объекта автоматизации и характеристиках окружающей среды 12](#_Toc529380250)

[3.2.1 Условия эксплуатации комплекса технических средств 12](#_Toc529380251)

[3.2.2 Характеристики окружающей среды 12](#_Toc529380252)

[3.3 Описание места объекта автоматизации в совокупности окружающих автоматизированных информационных систем 12](#_Toc529380253)

[3.3.1 Основные функции взаимодействующих сторон 12](#_Toc529380254)

[3.4 Текущее состояние объекта автоматизации 12](#_Toc529380255)

[4 Требования к Системе 14](#_Toc529380256)

[4.1 Требования к Системе в целом 14](#_Toc529380257)

[4.1.1 Требования к структуре и функционированию Системы 14](#_Toc529380258)

[4.1.2 Требования к численности и квалификации персонала Системы и режиму его работы, требования к квалификации пользователей Системы и режиму их работы 19](#_Toc529380259)

[4.1.3 Показатели назначения 20](#_Toc529380260)

[4.1.4 Требования к надежности 22](#_Toc529380261)

[4.1.5 Требования к безопасности 23](#_Toc529380262)

[4.1.6 Требования к эргономике и технической эстетике 23](#_Toc529380263)

[4.1.7 Требования к транспортабельности для подвижных АС 24](#_Toc529380264)

[4.1.8 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов Системы 24](#_Toc529380265)

[4.1.9 Требования к защите информации от несанкционированного доступа 25](#_Toc529380266)

[4.1.10 Требования по сохранности информации при авариях 32](#_Toc529380267)

[4.1.11 Требования к патентной чистоте 33](#_Toc529380268)

[4.1.12 Требования к вычислительной инфраструктуре 33](#_Toc529380269)

[4.1.13 Требования по стандартизации и унификации 34](#_Toc529380270)

[4.1.14 Дополнительные требования 34](#_Toc529380271)

[4.2 Требования к функциям (задачам), выполняемым Системой 35](#_Toc529380272)

[4.2.1 Требования к сценариям (процессам), автоматизируемым Системой 35](#_Toc529380273)

[4.2.2 Требования к функциям модернизируемой подсистемы сбора данных 38](#_Toc529380274)

[4.2.3 Требования к функциям модернизируемой подсистемы обработки данных 39](#_Toc529380275)

[4.2.4 Требования к функциям модернизируемой подсистемы хранения данных 41](#_Toc529380276)

[4.2.5 Требования к функциям модернизируемой подсистемы статистики и мониторинга 41](#_Toc529380277)

[4.2.6 Требования к функциям разрабатываемой подсистемы предоставления данных 44](#_Toc529380278)

[4.2.7 Требования к подсистеме обеспечения информационной безопасности 45](#_Toc529380279)

[4.3 Требования к видам обеспечения 47](#_Toc529380280)

[4.3.1 Требования к математическому обеспечению 47](#_Toc529380281)

[4.3.2 Требования к информационному обеспечению 47](#_Toc529380282)

[4.3.3 Требования к лингвистическому обеспечению 49](#_Toc529380283)

[4.3.4 Требования к программному обеспечению 49](#_Toc529380284)

[4.3.5 Требования к техническому обеспечению 50](#_Toc529380285)

[4.3.6 Требования к метрологическому обеспечению 50](#_Toc529380286)

[4.3.7 Требования к телекоммуникационному обеспечению системы 50](#_Toc529380287)

[5 Состав и содержание работ по созданию системы 51](#_Toc529380288)

[6 Порядок контроля и приемки системы 57](#_Toc529380289)

[6.1 Виды, состав, объем и методы испытаний системы и ее составных частей 57](#_Toc529380290)

[6.2 Сведения о гарантийном обслуживании Системы 57](#_Toc529380291)

[6.3 Порядок выполнения доработок и устранения допущенных Подрядчиком ошибок, которые выявлены в процессе испытаний и в период гарантийного обслуживания 57](#_Toc529380292)

[6.4 Статус приемочной комиссии 58](#_Toc529380293)

[6.5 Сведения об обслуживании Системы 58](#_Toc529380294)

[7 Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу Системы в действие 59](#_Toc529380295)

[7.1 Развертывание и конфигурирование 59](#_Toc529380296)

[7.2 Приведение поступающей в систему информации к виду, пригодному для обработки с помощью ЭВМ 59](#_Toc529380297)

[7.3 Изменения, которые необходимо осуществить в объекте автоматизации 59](#_Toc529380298)

[7.3.1 Создание условий функционирования объекта автоматизации, при которых гарантируется соответствие создаваемой системы требованиям 59](#_Toc529380299)

[7.3.2 Создание необходимых для функционирования системы подразделений и служб 59](#_Toc529380300)

[7.3.3 Сроки и порядок комплектования штатов и обучения персонала системы 59](#_Toc529380301)

[8 Требования к документированию 60](#_Toc529380302)

[9 Источники развития Системы 61](#_Toc529380303)

[9.1 Нормативно-правовые акты 61](#_Toc529380304)

[9.2 Нормативно-технические документы 61](#_Toc529380305)

**1 Общие сведения**

* 1. **Полное наименование работ**

Выполнение работ по развитию информационной системы мониторинга и анализа интернет активности пользователей.

* 1. **Условное обозначение системы**

ИС СТАТС, Система

* 1. **Шифр темы**

ИС СТАТС.

* 1. **Заказчик**

Департамент информационных технологий города Москвы.

107078, г. Москва, Новая Басманная улица, 10, стр. 1.

* 1. **Пользователь**

Аппарат Мэра и Правительства Москвы.

125032, г. Москва, Тверская улица, д. 13.

* 1. **Пользователи Системы**

Сотрудники органов исполнительной власти города Москвы, включая лица, ответственные за принятие управленческих решений, аналитики, разработчики и владельцы интернет-ресурсов.

* 1. **Подрядчик**

Определяется по результатам проведения конкурсной процедуры в соответствии с Федеральным законом 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

* 1. **Основание для развития Системы**

Основаниями для развития Системы являются:

1. Постановление Правительства Москвы от 21 декабря 2011 г. № 604-ПП «Об утверждении положения об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие органов исполнительной власти города Москвы и организаций при предоставлении государственных услуг и исполнении государственных функций в городе Москве».
2. Государственная программа города Москвы «Информационный город», утвержденная Постановлением Правительства Москвы от 9 августа 2011 г. № 349-ПП.
3. Постановление Правительства Москвы от 15 декабря 2015 г. № 871-ПП «О развитии единого интернет-пространства Правительства Москвы».
	1. **Плановые сроки развития Системы**

Начало работ: с даты заключения государственного контракта на выполнение работ по развитию информационной системы мониторинга и анализа интернет активности пользователей (далее – Контракт).

Окончание работ: не более 620 календарных дней со дня заключения Контракта.

* 1. **Источник финансирования**

Источники финансирования – бюджет города Москвы.

* 1. **Порядок финансирования**

Порядок финансирования определяется действующими нормативными правовыми актами города Москвы, регулирующими вопросы финансирования расходов городского бюджета, и условиями Контракта.

* 1. **Порядок оформления и предъявления Заказчику результатов работ**

Результаты работ передаются Заказчику в порядке, определенном Контрактом в соответствии с Календарным планом на основании Актов сдачи-приемки выполненных работ.

Состав передаваемых на машинных носителях результатов работ оформляется документом «Ведомость машинных носителей информации».

Отчеты и документация передаются на бумажных (по три экземпляра) и на машинных носителях (CD/DVD). Текстовые документы, передаваемые на машинных носителях, должны быть представлены в форматах, поддерживаемых программным обеспечением Microsoft Office. Язык документации – русский. Все материалы передаются с сопроводительными документами Подрядчика.

* 1. **Перечень нормативно-технических документов, методических материалов, регламентирующих развитие Системы**

Выполняемые работы и оформление их результатов должны отвечать требованиям нормативно-правовых актов, а также соответствующих государственных стандартов из числа Комплекса стандартов на автоматизированные системы:

* Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».
* Информационная технология. Комплекс стандартов на автоматизированные системы (класс стандартов ГОСТ 34).
* РД 50-34.698-90. Методические указания. Информационная технология. Автоматизированные системы. Требования к содержанию документов.
* ГОСТ 28806-90. Качество программных средств. Термины и определения.
* ГОСТ 16504-81. Система государственных испытаний продукции. Испытания и контроль качества продукции. Термины и определения.
* ГОСТ Р ИСО/МЭК ТО 12182-2002. Информационная технология. Классификация программных средств.
* ГОСТ Р ИСО/МЭК 12207:1999. Процессы жизненного цикла программных средств.
* ГОСТ Р ИСО/МЭК ТО 15271-2002. Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207.
* ГОСТ Р ИСО/МЭК 9126:93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению.
* ГОСТ Р ИСО/МЭК 15026:1998. Информационная технология. Уровни целостности систем и программных средств.
* ГОСТ Р ИСО/МЭК 14764:2002. Информационная технология. Сопровождение.
* ГОСТ Р ИСО/МЭК ТО 9294:93. Информационная технология. Руководство по управлению документированием программного обеспечения.
* ГОСТ Р ИСО/МЭК 15910-2002. Информационная технология. Процесс создания документации пользователя программного средства.
* ISO 14756: 1999. ИТ. Измерение и оценивание производительности программных средств компьютерных вычислительных систем.
* ГОСТ 2.051-2006. Единая система конструкторской документации. Электронные документы. Общие положения.

Работы в части обеспечения информационной безопасности должны выполняться в соответствии со следующими методическими документам, национальными стандартами и нормативными правовыми документами:

* Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ
«О персональных данных»;
* Постановление Правительства РФ от 6 июля 2015 г. № 676
«О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
* Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
* Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
* Постановление правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Приказ ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
* Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 г. Москва «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
* Проект методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах»;
* Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.;
* «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные ФСБ России 31 марта 2015 г. № 149/7/2/6-432;
* Распоряжение Правительства Москвы от 3 июля 2012 г. № 342-РП «О требованиях к вводу в эксплуатацию информационных систем, создаваемых в городе Москве»;
* ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие положения. ДСП;
* ГОСТ РО 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний. ДСП;
* ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;
* ГОСТ Р 51624-2000 Автоматизированные информационные системы в защищенном исполнении.
	1. **Перечень сокращений**

|  |  |
| --- | --- |
| АС | Автоматизированная система |
| ВМ | Виртуальная машина |
| ГИС | Государственная информационная система |
| ГОСТ | Государственный стандарт |
| ДИТ | Департамент информационных технологий города Москвы |
| ИС | Информационная система |
| НСИ | Нормативно-справочная информация |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| ППО | Прикладное программное обеспечение |
| СЗИ | Система защиты информации |
| СКЗИ | Система криптографической защиты информации |
| СУБД | Система управления базами данных |
| СХД | Система хранения данных |
| ТЗ | Техническое задание |
| ЦОД | Центр обработки данных |
| CD | CompactDisc — Компакт-диск. Оптический носитель информации |
| DVD | DigitalVersatileDisc — цифровой многоцелевой диск |
| SQL | StructuredQueryLanguage — «язык структурированных запросов». Универсальный компьютерный язык, применяемый для создания, модификации и управления данными в реляционных базах данных. |
| TCP/IP | TransmissionControlProtocol/InternetProtocol — протокол управления передачей данных — набор сетевых протоколов разных уровней модели сетевого взаимодействия, используемых в сетях. |

* 1. **Термины и определения, используемые в ТЗ**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| АВТОМАТИЗИРОВАННАЯ СИСТЕМА |  | Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций  |
| АВТОРИЗАЦИЯ |  | От англ. Authorization — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий |
| АУТЕНТИФИКАЦИЯ |  | От англ. Authentication — процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им пароля с паролем в базе данных пользователей |
| ВИТРИНА ДАННЫХ |  | От англ. DataMart — срез хранилища данных, представляющий собой массив тематической, узконаправленной информации, обычно содержащий тематические подмножества заранее агрегированных данных |
| ДОМОХОЗЯЙСТВО  |  | Институциональная социальная единица, которая состоит из относительно небольшой группы граждан, проживающих вместе, в той или иной степени объединяющих свои доходы и ресурсы, а также совместно потребляющие ряд товаров и услуг |
| ИДЕНТИФИКАЦИЯ |  | В информационных системах — присвоение субъектам и объектам идентификатора и / или сравнение идентификатора с перечнем присвоенных идентификаторов |
| ИЗМЕРЕНИЕ |  | Элемент данных, который классифицирует каждый элемент среза данных в непересекающиеся области |
| ИНФОРМАЦИОННЫЙ СЕРВИС |  | Услуга, предполагающая обработку определенной информации из транзакционных информационных систем (получение различных отчетов, аналитических оценок и т. д.) или таких повседневных процедур, как проверка введенной информации, заполнение, исправление или утверждение отчетов о проделанной работе, подача заявок и их утверждение |
| КОНЦЕПТУАЛЬНАЯ АРХИТЕКТУРА СИСТЕМЫ |  | Обобщенная (высокоуровневая) модель приложения корпоративного уровня. Описывает основные прикладные компоненты информационной системы |
| ОПЕРАТОР ДАННЫХ |  | Орган исполнительной власти города Москвы, структурное подразделение органа исполнительной власти города Москвы, подведомственная организация – обеспечивающая контроль за соблюдением стандарта ведения данных |
| ПОКАЗАТЕЛЬ |  | Величина (обычно числового типа), которая является предметом анализа |
| СИСТЕМА |  | Информационная система мониторинга и анализа интернет активности пользователей |
| СЕГМЕНТ ИС |  | Совокупность нескольких компонентов информационной системы, использующих общую (в том числе разделяемую) среду передачи и объединенных для единства решения функциональных задач |
| СЕТЕВЫЕ СЕРВИСЫ |  | Взаимодействие компьютеров между собой, а также с другим активным сетевым оборудованием, в TCP/IP-сетях организовано на основе использования сетевых служб, которые обеспечиваются специальными процессами сетевой операционной системы — демонами в UNIX-подобных операционных системах (далее – ОС), службами в ОС семейства Windows и т. п. |
| СТАНДАРТ ВЕДЕНИЯ ДАННЫХ |  | Единые требования к стандарту ведения данных, утвержденные распоряжением руководителя ДИТ |
| ХРАНИЛИЩЕ ДАННЫХ |  | Предметно-ориентированная информационная база данных, специально разработанная и предназначенная для подготовки отчётов и бизнес-анализа с целью поддержки принятия решений |
| WEB-СЕРВИС |  | От англ. webservice — идентифицируемая веб-адресом программная система со стандартизированными интерфейсами. Веб-службы могут взаимодействовать друг с другом и со сторонними приложениями посредством сообщений, основанных на определённых протоколах. Веб-служба является единицей модульности при использовании сервис-ориентированной архитектуры приложения |

* 1. **Порядок внесения изменений и дополнений**

Изменения настоящего ТЗ не предусмотрены.

Детализация и уточнение требований настоящего ТЗ возможны на этапе проектировании и могут быть предъявлены в составе частного технического задания (ЧТЗ). ТЗ в совокупности с ЧТЗ должны составлять полную систему требований к развитию Системы. При этом детализация и уточнение требований в составе ЧТЗ не должны противоречить основным требованиям настоящего ТЗ и приводить к существенному изменению объема работ, предусмотренных Контрактом.

**2 Назначение и цели развития Системы**

**2.1 Назначение Системы**

Назначением информационной системы мониторинга и анализа интернет активности пользователей является повышение качества продвижения и популяризация контента информационных систем и ресурсов города Москвы, в том числе определение оптимальных площадок коммуникаций с посетителями и канала продвижения контента согласно определенному сегменту, к которому относится посетитель или интернет-ресурс.

Функциональным назначением Системы является:

* мониторинг посещаемости интернет-ресурсов;
* выявление разделов интернет-ресурсов, требующих оптимизации с точки зрения повышения посещаемости;
* мониторинг изменения аудитории интернет-посетителей;
* сегментация и кластеризация интернет-посетителей с возможностью выявления целевых групп;
* визуализация результатов анализа закономерностей и особенностей поведения интернет-посетителей в достаточном объеме для обеспечения принятия решений интернет-ресурсом относительно направлений развития;
* поиск неявных целевых групп путем построения взаимосвязей интернет-посетителей со схожим поведением;
* предоставление информации о поведенческом векторе интернет-посетителя для персонализации контентных блоков интернет-ресурсов.

**2.2 Цели и задачи выполнения работ**

Основными целями развития Системы являются:

* обеспечение возможности предоставления внешним системам статистических данных по запросу, рассчитанных на основании логов действий интернет-посетителей;
* повышение уровня отказоустойчивости Системы с учетом роста объема поступающих данных в Систему;
* обеспечение возможности выявления причин, которые привели к целевому действию интернет-посетителя для предоставления информации о необходимости оптимизации функций интернет-ресурсов;
* обеспечение возможности выявления уникального интернет-посетителя в условиях отсутствия cookies в браузере интернет-посетителя;
* обеспечение возможности поиска целевых аудиторий через взаимосвязь интернет-посетителей, выявленной с помощью графов-связей по схожему поведению и прогноза поведенческих характеристик на основе логов действий интернет-посетителей;
* обеспечение предоставления своевременной информации о типе пользователя для внешних систем для реализации персонализации контентных компонент интернет-ресурсов.

В ходе работ должна быть создана система защиты информации (СЗИ) ИС СТАТС в соответствии с требованиями законодательства Российской Федерации и нормативными документами в области информационной безопасности и проведена аттестация ИС СТАТС на соответствие требованиям приказа ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Приказ № 17) и законодательства в области защиты персональных данных.

Задачами выполнения работ по обеспечению информационной безопасности ИС СТАТС являются:

* оценка соответствия проектных решений и технологий обработки информации актуальным требованиям о защите информации;
* определение требований к мерам и средствам защиты информации, применяемым в ИС СТАТС на всех технологических уровнях обработки информации;
* определение требований к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями;
* определение требований к встроенным средствам прикладного программного обеспечения (ППО) ИС СТАТС реализующим функционал защиты информации;
* разработка подсистемы информационной безопасности;
* подготовка встроенного функционала к сертификации по требованиям безопасности информации;
* разработка технического проекта на СЗИ ИС СТАТС;
* сертификация ППО ИС СТАТС по требованиям безопасности информации;
* подготовка и проведение аттестации ИС СТАТС по требованиям безопасности информации.

В ходе данных работ должен быть выполнен комплекс мероприятий по обеспечению отказоустойчивости системы и мониторинга ее работы.

Критериями достижения целей развития Системы являются:

* наличие работоспособной системы, реализованной за счет создания подсистем, в соответствии с составом, определенным в пункте 4.2 ТЗ;
* полнота реализации требований к функциональным подсистемам, реализованных за счет создания технологических подсистем, определенных пунктом 4.2 ТЗ;
* полнота реализации требований по информационной безопасности, определенных в разделе 4 ТЗ;
* полное и своевременное проведение работ, определённых в разделе 5 ТЗ.

**3 Характеристики объектов автоматизации**

**3.1 Краткие сведения об объекте автоматизации**

Объектом автоматизации являются процессы подготовки и анализа информации о событиях, связанных с действиями посетителей интернет-ресурсов, в том числе подлежащих журналированию.

Ввиду большого количества обрабатываемых данных и запросов, возникают проблемы со временем их обработки и анализа. С целью решения возникших проблем необходима оптимизация алгоритмов функционирования Системы и доработка механизмов распределения нагрузки.

Доступ пользователя к ИС СТАТС должен осуществляться посредством «тонкого» клиента (web-браузера).

Система, развиваемая в рамках настоящего ТЗ, относится к общегородским информационным системам.

**3.2 Сведения об условиях эксплуатации объекта автоматизации и характеристиках окружающей среды**

* + 1. **Условия эксплуатации комплекса технических средств**

Условия эксплуатации комплекса технических средств Системы соответствуют условиям эксплуатации группы 2 ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортировка, хранение».

Условия эксплуатации персональных компьютеров Системы соответствуют Гигиеническим требованиям к видео дисплейным терминалам, персональным электронно-вычислительным машинам и организации работы (Санитарные правила и нормы. СанПиН 2.2.2/2.4.1340-03).

* + 1. **Характеристики окружающей среды**

Характеристики окружающей среды в местах установки технических средств соответствуют требованиям следующих документов:

* ГОСТ Р ИСО 14001-2007 «Системы экологического менеджмента. Требования и руководство по применению»;
* СанПиН 2.2.24.548-96. Физические факторы производственной среды. Гигиенические требования к микроклимату производственных помещений;
* СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы.

**3.3 Описание места объекта автоматизации в совокупности окружающих автоматизированных информационных систем**

* + 1. **Основные функции взаимодействующих сторон**

В рамках автоматизации происходит взаимодействие следующих сторон:

* внешние системы-источники данных;
* система анализа поступивших данных;
* системы предоставления результатов анализа данных внешним системам-потребителям.

**3.4 Текущее состояние объекта автоматизации**

ИС СТАТС была создана в рамках выполнения работ по государственному контракту от 14 августа 2017 г. № ГК 6401/17-2692 на выполнение работ по разработке информационной системы мониторинга и анализа интернет активности пользователей.

Информационная система мониторинга и анализа интернет активности пользователей автоматизирует процессы, обеспечивающие повышение качества продвижения и популяризации контента информационных систем и ресурсов города Москвы, в том числе определение оптимальных площадок коммуникаций с посетителями и канала продвижения контента согласно определенному сегменту, к которому относится посетитель или интернет-ресурс.

Вместе с тем требуют улучшения следующие процессы:

* увеличение допустимой нагрузки на Систему с учетом увеличения количества интернет-посетителей интернет-ресурсов Правительства Москвы;
* реализация последовательного сохранения записывающихся событий в подсистему хранения данных для обеспечения возможности повторного считывания событий с начала хранимого периода (поддержка историчности хранения информации по событиям);
* реализация возможности выявления уникального интернет-посетителя без использования cookies для увеличения точности сопоставления профилей;
* расширение аналитических функций Системы с учетом наличия потребности анализа текстовой информации в привязке к поведенческому профилю интернет-посетителя таких, как полнотекстовой поиск по адресу интернет-ресурса или по городу/ стране используемого интернет-соединения;
* реализация возможности вывода произвольного набора статистических отчетов из стандартного набора отчетов в пользовательском интерфейсе Системы с учетом различных потребностей в собираемых показателях интернет-аналитики у разных интернет-ресурсов;
* реализация возможности предоставления по запросу внешними системами-потребителями статистической информации и информации по поведенческим сегментам.
1. **Требования к Системе**

**4.1 Требования к Системе в целом**

* + 1. **Требования к структуре и функционированию Системы**
			1. **Требования к архитектуре**

Архитектура ИС СТАТС соответствует трехуровневой клиент-серверной архитектуре и состоит из следующих уровней:

* уровень хранения данных;
* уровень приложений;
* презентационный уровень.

Уровень хранения данных: распределенная файловая система, обеспечивающая хранение и предоставление данных Системы.

Уровень приложений: сервер приложений, регламентирующий правила и ограничения автоматизированных функций Системы (бизнес-логику) и выполнение автоматизированных операций, обеспечивающий передачу данных между презентационным уровнем и уровнем хранения данных.

Презентационный уровень: клиентское приложение («тонкий клиент»), работающее через стандартный веб-браузер, обеспечивающее отображение информации пользователям и прием управляющих воздействий.

Концептуальная схема ИС СТАТС приведена на Рисунке 1.



Рисунок 1 – Концептуальная схема ИС СТАТС

Выполнение работ по развитию ИС СТАТС, предусмотренных в настоящем Техническом задании, должно осуществляться с сохранением всех ранее созданных функций ИС СТАТС.

* + - 1. **Перечень подсистем, их назначение и основные характеристики**

В рамках выполнения работ по развитию ИС СТАТС должны быть разработаны/модернизированы следующие подсистемы/сценарии:

* модернизирована подсистема сбора данных, обеспечивающая проксирование трафика между посетителем и интернет-ресурсом:
	+ разработан модуль определения уникального интернет-посетителя без использования cookies;
	+ разработан механизм фиксации переходов по внешним ссылкам;
	+ разработан модуль загрузки данных из внешних информационных систем в формате csv, json, avro;
* модернизирована подсистема обработки данных, обеспечивающая преобразование форматов и выполнения аналитических операций над данными, полученных от подсистемы сбора. В состав данной подсистемы должны входить следующие модули:
	+ разработан модуль полнотекстового поиска;
	+ разработан модуль сегментирования всех интернет-посетителей с учетом прогнозных значений поведения;
	+ разработан модуль сопоставления интернет-посетителей по уникальному идентификатору, присвоенному механизмом генерации cookies и механизмом генерации по характеристикам устройства;
* разработан модуль сервиса коротких ссылок.
* модернизирована подсистема хранения данных, обеспечивающая управление жизненным циклом данных, полученных от подсистем сбора и обработки;
* модернизирована подсистема статистики и мониторинга, обеспечивающая визуализацию статистических отчетов на базе агрегированных данных:
	+ разработан раздел предоставления результатов кластеризации поисковых запросов с учетом поведения интернет-посетителя;
	+ разработан разделпредоставления результатов сегментирования интернет-посетителей;
	+ разработан раздел предоставления статистики по событиям, получаемым из внешних систем-источников в подсистему сбора данных;
	+ разработан функционал конструирования собственных (кастомных) статистических отчетов;
	+ разработан модуль управления интерфейсом:
	+ создание, редактирование и удаление «Ситуационных панелей»;
	+ управление представлением данных;
	+ добавление, редактирование, удаление наборов данных на «Ситуационную панель»;
	+ разработан модуль выгрузки статистических данных:
	+ выгрузка данных в форматах csv, xls для аналитической обработки;
	+ выгрузка данных в формате pdf для печати, презентаций;
	+ настройка функционала формирования регулярных рассылок со статистическими данными.
* разработана подсистема предоставления данных, обеспечивающая предоставление данных внешним системам-потребителям:
	+ разработан механизм предоставления агрегированной статистики внешним системам-потребителям переходов по внешним ссылкам;
	+ разработан механизм предоставления агрегированной статистики внешним системам-потребителям переходов по внутренним ссылкам;
	+ разработан механизм предоставления профилей внешним системам-потребителям по ключу cookie интернет-посетителя.
* разработана подсистема обеспечения информационной безопасности:
* разработан механизм идентификации и аутентификации субъектов доступа и объектов доступа ППО;
* разработан механизм управление доступом субъектов доступа к объектам доступа ППО;
* разработан механизм регистрация событий безопасности ППО;
* разработан механизм контроля защищенности ППО.

Информационная система мониторинга и анализа интернет активности пользователей должна обеспечивать в том числе процессы аналитической обработки информации на основе построения математических моделей (информационно-аналитическая система).

ИС СТАТС не предусматривает размещение компонентов на мобильных устройствах.

В таблице 1 представлена классификация подсистем ИС СТАТС модернизируемых и создаваемых в рамках данного Технического задания

Таблица 1 – Классификация подсистем ИССТАТС

| **№** | **Подсистема** | **Класс** |
| --- | --- | --- |
|  | Подсистема сбора данных | Информационно-аналитическая |
|  | Подсистема обработки данных | Информационно-аналитическая |
|  | Подсистема хранения данных | Информационно-поисковая |
|  | Подсистема статистики и мониторинга | Информационно-аналитическая |
|  | Подсистема предоставления данных | Обеспечения деятельности ОИВ, портал, прочая |
|  | Подсистема обеспечения информационной безопасности | Обеспечения деятельности ОИВ, портал, прочая |

* + - 1. **Требования к способам и средствам связи для информационного обмена между компонентами Системы**

Взаимодействие между компонентами Системы должно осуществляться путем информационного обмена с использованием стандартных средств СУБД и протоколов передачи данных.

* + - 1. **Требования к взаимодействию с внешними информационными системами**

Взаимодействие между Системой и внешними информационными системами должно осуществляться путем информационного обмена с использованием стандартных протоколов передачи данных.

В Системе должны быть сохранены существующие информационные взаимодействия с интернет-ресурсами в части получения информации о действиях интернет-посетителей и связанных с ними событиях. Для взаимодействия используются веб-сервисы, получающие доступ к информационным системам по HTTP протоколу.

В рамках выполнения работ по развитию Системы должно быть обеспечена возможность предоставления внешним системам-потребителям:

* агрегированной статистики переходов по внешним ссылкам;
* агрегированной статистики переходов по внутренним ссылкам;
* профилей по ключу cookie интернет-посетителя.

Механизмы предоставления данных должны обеспечивать агрегацию и передачу обработанных данных в пакетном режиме, в форме JSON-запросов/ответов.

Должна быть обеспечена возможность взаимодействия Системы не менее, чем с двумя внешними информационными системами с направлением потоков информации в обе стороны(вход/выход):

* Информационная система персональных коммуникаций («ИС ПК»);
* Автоматизированная информационная система «Официальный портал Мэра и Правительства Москвы» (АИС «ОПМПМ»).

Полный перечень внешних информационных систем, с которыми должно быть организовано взаимодействие, и направления потоков информации должен быть определен на этапе проектирования и приведен в документе «Пояснительная записка».

* + - 1. **Требования к режимам функционирования Системы**

Система должна функционировать в следующих режимах:

* штатный режим регулярной работы, при котором обеспечивается выполнение задач в объеме функций, предусмотренных настоящим техническим заданием;
* сервисный режим, необходимый для проведения обслуживания, реконфигурации и пополнения технических и программных средств Системы новыми компонентами;
* аварийный режим работы.

Пускового режима не предусмотрено.

В штатном режиме функционирования Система должна обеспечивать следующий режим работы: доступность функций системы, составляющая не менее 95% в год.

В сервисном режиме Система должна обеспечивать возможность проведения следующих работ:

* техническое обслуживание;
* модернизацияаппаратно-программного комплекса;
* устранение аварийных ситуаций.

Система переходит в аварийный режим при возникновении нештатной ситуации и невозможности штатной работы. В случае перехода Системы в аварийный режим, обслуживающему персоналу необходимо перевести Систему в сервисный режим.

Регламентные работы должны производиться с учётом требований о доступности Системы.

Функционирование Системы при отказах и сбоях серверного общесистемного и специального программного обеспечения и оборудования, в том числе структурных узлов Системы, не предусматривается.

* + - 1. **Требования по диагностированию Системы**

Система должна предоставлять инструменты диагностирования и мониторинга процессов выполнения основных функций подсистем, входящих в ее состав.

Данные инструменты должны обеспечивать ведение журналов диагностических событий, в которых должны автоматически фиксироваться возникшие нештатные ситуации и ошибки. Данные журналы должны позволять сохранять набор информации, необходимой для идентификации и решения проблемы.

Подрядчиком должна быть реализована функциональность, позволяющая информировать заинтересованных лиц о выходе параметров информировать заинтересованных лицо выходе параметров работы Системы за установленные пределы.

* + - 1. **Перспективы развития, модернизации Системы**

В рамках следующей очереди развития Системы планируется расширение функций подсистем сбора, хранения данных и предоставления данных внешним системам-потребителям.

В рамках развития Системы должны быть предусмотрены мероприятия по снижению трудозатрат при использовании ее внутренних технологических процессов.

Технические решения, используемые на этапах проектирования и реализации Системы, должны позволять минимизировать трудозатраты по модернизации, требуемые в связи с выпуском новых нормативных актов, приводящих к изменению технологического процесса.

* + 1. **Требования к численности и квалификации персонала Системы и режиму его работы, требования к квалификации пользователей Системы и режиму их работы**
			1. **Требования к численности персонала Системы**

Персонал Системы разделён на категории:

* обслуживающий персонал:
	+ системный администратор;
	+ администратор баз данных;
	+ администратор информационной безопасности;
	+ специалист по технической поддержке;
* пользователи:
	+ базовые пользователи;
	+ аналитики данных (пользователи, выполняющие произвольные запросы и занимающиеся выявлением трендов).

Роли системного администратора и администратора баз данных могут быть совмещены в одну роль.

Численность персонала должна быть достаточной для обеспечения требований, изложенных в ТЗ.

* + - 1. **Требования к квалификации персонала Системы, порядку его подготовки и контроля знаний и навыков**

Персонал, допущенный к эксплуатации и обслуживанию Системы должен иметь подготовку и квалификацию, необходимую для обеспечения функционирования Системы, а также выполнения требований, определенных в руководстве пользователя Системы.

Обслуживающий персонал Системы должен иметь навыки и знания по администрированию прикладного программного обеспечения Системы и техническому обслуживанию средств вычислительной техники, на которых оно устанавливается, в объеме навыков, определенном в руководстве администратора.

Сотрудники, работающие с Системой должны иметь общую подготовку для работы с прикладным программным обеспечением Системы, а также знания и навыки на уровне пользователя общераспространенного программного обеспечения (Операционная система и офисное программное обеспечение) в объеме навыков, определенных руководством пользователя Системы.

* + - 1. **Требуемый режим работы персонала Системы**

Режим работы персонала Системы должен регулироваться должностными инструкциями.

* + - 1. **Требования к квалификации пользователей Системы**

Пользователи Системы должны обладать квалификацией, обеспечивающей, как минимум:

* базовые навыки работы на персональном компьютере с современными операционными системами (клавиатура, мышь, управление окнами и приложениями, файловая система);
* базовые навыки использования интернет-браузера (настройка типовых конфигураций, установка подключений, доступ к web-сайтам, навигация, формы и другие типовые интерактивные элементы web-интерфейса);
* знание основ информационной безопасности.

Базовые пользователи должны обладать базовыми знаниями в предметной области, для анализа отчетов и отправки запросов к интерфейсной части подсистеме статистики и мониторинга Системы.

Аналитики данных – пользователи, выполняющие произвольные запросы, должны владеть основами языка запросов SQL, Python, ApachePig.Пользователи, занятые выявлением трендов и закономерностей, должны обладать необходимыми знаниями в области математической статистики и теории вероятности.

* + - 1. **Требуемый режим работы пользователей Системы**

Система должна обеспечивать обработку не менее 50 запросов от разных пользователей в час на предоставление регулярных (типовых) отчетов.

Система должна обеспечивать комфортное время реакции на действия пользователя для процессов формирования аналитической отчетности – не более 5 минут.

Нерегламентированные запросы могут потребовать значительно большего времени выполнения. Для исключения негативного влияния нерегламентированных запросов на функционирование Система должна обеспечивать при необходимости прекращение выполнение запросов по требованию пользователя.

* + 1. **Показатели назначения**
			1. **Количество пользователей**

В рамках выполнения работ по развитию Системы, предусмотренных настоящим ТЗ, показатель назначения «Количество пользователей» должен соответствовать значениям, приведенным в данном разделе.

Пояснения по показателям, связанным с количеством пользователей, приведены в таблице 2.

**Таблица 2 — Определения показателей, связанных с количеством пользователей в Системе**

| **№** | **Показатель** | **Определение** |
| --- | --- | --- |
|  | Расчетное количество пользователей | Количество пользователей, работу которых должно обеспечить Система к моменту сдачи Контракта с учетом достижения всех показателей назначения |
|  | Расчетное количество одновременно работающих пользователей | Количество одновременно работающих пользователей, работу которых должна обеспечивать Система к моменту сдачи Контракта с учетом достижения всех показателей назначения |

Значения показателей количества пользователей, достижение которых необходимо обеспечить, представлено в таблице 3.

**Таблица 3 — Значения показателей количества пользователей**

|  |  |  |
| --- | --- | --- |
| **№** | **Показатель** | **Значение** |
|  | Расчетное количество пользователей | 100 |
|  | Расчетное среднее количество одновременно работающих пользователей | 50 |

* + - 1. **Число обрабатываемых объектов**

К показателям числа обрабатываемых объектов относятся:

1. расчетное количество основных объектов предметной области обрабатываемых за секунду (по каждому типу обрабатываемого объекта);
2. расчетное количество основных объектов предметной области обрабатываемых за год (по каждому типу обрабатываемого объекта);
3. максимальное количество основных объектов предметной области обрабатываемых за секунду (по каждому типу обрабатываемого объекта);
4. максимальное количество основных объектов предметной области обрабатываемых за год (по каждому типу обрабатываемого объекта).

Перечень объектов, в отношении которых применяется данный показатель, приведен в таблице 4.

**Таблица 4 — Перечень типов объектов, в отношении которых применяется показатель**

| **№** | **Объект** | **Краткое описание** |
| --- | --- | --- |
| 1 | Запись в журнале действий | Данные, передаваемые о действии посетителя, с информацией по используемому интернет-браузеру |
| 2 | Событие | Json объект с данными о действиях интернет-посетителей с предопределенными параметрами |
| 3 | Сегменты посетителей | Количество стандартных поведенческих профилей (сегментов) посетителей, рассчитываемых и перестраиваемых ежедневно на основе поведения посетителей и сформированных прогнозных значений |

Пояснения по показателям, связанным с количеством объектов в Системе, приведены в таблице 5.

**Таблица 5 — Определения показателей, связанных с числом обрабатываемых Объектов**

| **№** | **Показатель** | **Определение** |
| --- | --- | --- |
|  | Расчетное количество основных объектов предметной области обрабатываемых за секунду (по каждому типу обрабатываемого объекта) | Количество основных объектов предметной области, которое должно обрабатывать приложение за секунду к моменту сдачи Контракта с учетом достижения всех показателей назначения |
|  | Максимальное количество основных объектов предметной области обрабатываемых за секунду (по каждому типу обрабатываемого объекта) | Максимальное количество основных объектов предметной области, обработку которых должна обеспечить архитектура приложения в течение секунды |
|  | Расчетное количество основных объектов предметной области обрабатываемых за год (по каждому типу обрабатываемого объекта) | Количество основных объектов предметной области, которое должно обрабатывать приложение за год к моменту сдачи Контракта с учетом достижения всех показателей назначения |
|  | Максимальное количество основных объектов предметной области обрабатываемых за год (по каждому типу обрабатываемого объекта) | Максимальное количество основных объектов предметной области, обработку которых должна обеспечить архитектура приложения в течение года |

Значения показателей количества объектов Системы, достижение которых необходимо обеспечить, представлено в таблице 6.

Таблица 6 – Значение показателей числа обрабатываемых объектов

| **№** | **Объект** | **Количество объектов предметной области, обрабатываемых Системой** |
| --- | --- | --- |
| **Расчетное** | **Максимальное** |
| **За секунду** | **За год** | **За секунду** | **За год** |
|  | Запись в журнале действий | 10 000 | 5 000 000 000 | 15 000 | 8 000 000 000 |
|  | Событие | 1000 | 50 000 000 | 2000 | 100 000 000 |
|  | Сегменты посетителей | - | 20 | - | 30 |

* + - 1. **Время получения отчетности**

**4.1.3.3.1 Время получения отчетности с заранее определенной структурой**

К показателям времени получения отчетности с заранее определенной структурой относятся:

1. расчетное время получения отчета с заранее определенной структурой (по каждому отчету);
2. максимальное время получения отчета с заранее определенной структурой (по каждому отчету).

**Таблица 7 — Определения показателей, связанных с получением**

**отчетности с заранее определенной структурой**

|  |  |  |
| --- | --- | --- |
| **№** | **Показатель** | **Определение** |
|  | Расчетное время получения отчета с заранее определенной структурой (сек) | 5 сек |
|  | Максимальное время получения отчета с заранее определенной структурой (сек) | 20 сек |

* + 1. **Требования к надежности**
			1. **Показатели доступности/надежности**

К показателям доступности/надежности относятся:

* доступность;
* надежность;
* время сохранности данных;
* время восстановления после сбоя.

Пояснения по показателям, связанным с доступностью/надежностью, приведены в таблице 8.

Таблица 8 – Определение показателей, связанных с доступностью/надежностью

| **№** | **Показатель** | **Определение** |
| --- | --- | --- |
| 1. | Надежность, измеряется в часах | Надежность – мера того, как долго ИС может сохранять непрерывную работоспособность в рамках выполнения согласованных функций |
| 2. | Доступность, измеряется в процентах | Доступность – способность ИС выполнять согласованную функцию в течении оговоренного времени (время работы ИС – время простоя)/время работы ИС \* 100). |
| 3. | Время сохранности данных (RecoveryPointObjective - RPO), измеряемые в часах | Время сохранности данных – допустимый период времени, за который могут быть утрачены данные |
| 4. | Время восстановления после сбоя (RecoveryTimeObjective - RTO), измеряется в часах | Время восстановления после сбоя – допустимое время восстановления работоспособности |

Значения показателей доступности/надежности, достижения которых необходимо обеспечить, представлено в таблице 9.

Таблица 9 – Значения показателей доступности/надежности

| **№** | **Показатель** | **Значение** |
| --- | --- | --- |
| 1. | Надежность, измеряется в часах | 5 000 часов |
| 2. | Доступность, измеряется в процентах | 95% |
| 3. | Время сохранности данных (RecoveryPointObjective - RPO), измеряется в часах | 12 часов |
| 4. | Время восстановления после сбоя (RecoveryTimeObjective - RTO), измеряется в часах | 4 часа |

* + - 1. **Требования к программным мероприятиям по обеспечению надежности**

Надежность Системы должна достигаться комплексом организационных и технических мер, обеспечивающих требуемые уровни безотказности, ремонтопригодности, долговечности и сохранения ресурсов Системы.

Технические меры по обеспечению надежности должны предусматривать:

* резервирование критически важных компонентов и данных Системы и отсутствие единой точки отказа;
* использование технических средств с избыточными компонентами и возможностью их «горячей» замены;
* использование программного резервирования (программной избыточности);
* конфигурирование используемых средств и применение специализированного ПО, обеспечивающего высокую надёжность.

Организационные меры по обеспечению надежности должны быть направлены на минимизацию ошибок пользователей (а также обслуживающего персонала при эксплуатации и проведении работ по обслуживанию), минимизацию времени ремонта или замены вышедших из строя компонентов за счёт:

* обеспечения требуемого уровня квалификации пользователей;
* обеспечения требуемого уровня квалификации обслуживающего персонала;
* регламентации и нормативного обеспечения выполнения работ обслуживающего персонала и пользователей;
* своевременного оповещения пользователей о случаях нештатной работы компонентов Системы;
* своевременной диагностики неисправностей;
* наличия запасных изделий;
* наличия договоров на сервисное обслуживание и поддержку компонентов комплекса технических средств (КТС).
	+ 1. **Требования к безопасности**

Конструкция комплекса технических средств ИС должна обеспечивать безопасность обслуживающего персонала при эксплуатации, техническом обслуживании и ремонте.

В помещениях должны поддерживаться параметры микроклимата в соответствии с требованиями, предъявляемыми поставщиками размещаемого там оборудования.

* + 1. **Требования к эргономике и технической эстетике**

Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав Системы, должно осуществляться посредством визуального графического интерфейса (GUI). Интерфейс Системы должен быть понятным и удобным, не должен быть перегружен графическими элементами. Навигационные элементы должны быть выполнены в удобной для пользователя форме. Ввод-вывод данных, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям Системы.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление Системой должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов. Клавиатурный режим ввода должен использоваться главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм.

Экранные формы должны проектироваться с учетом требований унификации:

* все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;
* для обозначения сходных операций должны использоваться сходные графические значки, кнопки и другие управляющие (навигационные) элементы. Термины, используемые для обозначения типовых операций (добавление информационной сущности, редактирование поля данных), а также последовательности действий пользователя при их выполнении, должны быть унифицированы.

При необходимости Подрядчик этапе проектирования должен разработать и согласовать с Заказчиком макет визуального графического интерфейса.

* + 1. **Требования к транспортабельности для подвижных АС**

Требования к транспортабельности не предъявляются.

* + 1. **Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов Системы**

Обслуживание Системы должно производиться обслуживающим персоналом.

Допускается использование специализированных служб или подразделений на объектах внедрения для обслуживания и ремонта оборудования.

* + - 1. **Условия и регламент (режим) промышленной эксплуатации**

Должно быть предусмотрено ежедневное/еженедельное техническое обслуживание Системы.

* + - 1. **Требования по количеству, квалификации обслуживающего персонала и режимам его работы**

Персонал Системы разделён на категории:

* обслуживающий персонал:
	+ системный администратор;
	+ администратор баз данных;
	+ администратор информационной безопасности;
	+ специалист по техническому обслуживанию. Роли системного администратора и администратора баз данных могут быть совмещены в одну роль.

Численность персонала системы должна быть достаточной для обеспечения требований, изложенных в ТЗ.

* + - 1. **Требования к составу, размещению и условиям хранения комплекта запасных изделий и приборов**

Требования к составу, размещению и условиям хранения комплекса запасных изделий и приборов не предъявляются.

* + - 1. **Требования к регламенту обслуживания**

При промышленной эксплуатации Системы входящее в ее состав системное программное и аппаратное обеспечение должно соответствовать рекомендациям производителя.

Должны соблюдаться правила эксплуатации компонентов Системы, а также производиться своевременная установка обновлений программного обеспечения, рекомендованных производителями.

Подрядчиком должны быть сформулированы требования к ежедневному и еженедельному обслуживанию, а также обслуживанию по возникновению особых (исключительных) ситуаций. Сюда включаются работы по обслуживанию технических средств Системы, данных в постоянных и временных хранилищах (базах данных), потоков сообщений в электронных коммуникациях, паролей и прав доступа.

В частности, в обслуживание входят работы:

* по восстановлению баз данных при порче или разрушении данных;
* по профилактическому контролю состояния дисковых запоминающих устройств и данных на них.

Выполнение указанных требований должно обеспечивать непрерывную работу комплекса. При этом резервное копирование информации может осуществляться в следующих режимах:

* создание полной копии базы данных;
* избыточное хранение в ЦОД Заказчика, при котором выход из строя определенного числа нод (узелов кластера серверов), не приводит к потере данных;
* сохранение изменений, внесенных со времени создания последней архивной копии (архивные копии log-файлов).

Периодичность и очередность этих операций определяются политикой резервного копирования информации площадкой размещения.

Создание полной копии базы данных осуществляется полным копированием всех файлов указанной базы на внешние носители.

При сохранении изменений, внесенных со времени создания последней архивной копии, на внешние носители переносятся только те изменения базы данных, которые были сделаны со времени или после последней операции архивирования (полного или частичного).

При восстановлении информации с архивных копий сначала с архивных носителей восстанавливается состояние базы данных на момент последней операции полного резервного копирования, затем в базу поочередно вносятся изменения со всех частичных архивов, созданных после полного резервирования.

Предпочтительный интервал для технического обслуживания Системы в нерабочие дни, например, с 23:00 до 07:00.

* + 1. **Требования к защите информации от несанкционированного доступа**

Работы по обеспечению информационной безопасности ИС СТАТС должны включать:

* Формирование требований к защите информации, содержащейся в ИС СТАТС;
* Разработку подсистемы обеспечения информационной безопасности;
* Создание СЗИ ИС СТАТС;
* Разработку организационно-распорядительной документации на СЗИ ИС СТАТС;
* Сертификация ППО ИС СТАТС по требованиям безопасности информации;
* Аттестация ИС СТАТС по требованиям безопасности информации.

Результаты работ должны соответствовать требованиям законодательства и подзаконных нормативных актов, действующих на дату сдачи работ.

* + - 1. **Формирование требований к защите информации, содержащейся в информационной системе**

Задачами по реализации данных требований являются:

* оценка соответствия проектных решений ИС СТАТС, состава информационной системы и технологий обработки информации актуальным требованиям по защите информации;
* определение класса ИС СТАТС в соответствии с требованиями по информационной безопасности, определение сегментов ИС СТАТС, участвующих в аттестации по требованиям безопасности информации в качестве типовых сегментов;
* определение угроз безопасности информации ИС СТАТС;
* определение класса СКЗИ;
* определение требований к системе защиты информации ИС СТАТС.
	+ - * 1. **Оценка соответствия проектных решений информационных, состава и технологий обработки информации актуальным требованиям о защите информации**

В ходе реализации данной задачи должны быть проведены следующие мероприятия:

* анализ целей создания ИС СТАТС и задач, решаемых указанной ИС;
* анализ ИС СТАТС на соответствие требованиям нормативных правовых актов, методических документов и национальных стандартов в области защиты информации, указанных в пункте 1.13 ТЗ;
* формирование перечня информации, подлежащей обработке в ИС СТАТС;
* обоснование решения о необходимости создания СЗИ ИС СТАТС, а также определение целей и задач защиты информации в ИС СТАТС.

Результаты работ должны быть оформлены в виде документа «Аналитическое обоснование необходимости создания системы защиты информации ИС».

* + - * 1. **Определение класса ИС СТАТС в соответствии с требованиями по информационной безопасности и определение сегментов, участвующих в аттестации по требованиям безопасности информации**

Определение класса ИС СТАТС и сегментов ИС (при наличии) должны быть проведены в зависимости от значимости, обрабатываемой в ней информации и масштаба ИС в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17. Также должны быть выполнены работы по определению уровня защищенности персональных данных, обрабатываемых в ИС (при наличии), и его соответствия классу защищенности ГИС.

Класс защищенности должен быть определен для ИС в целом и для каждого ее типового сегмента (при необходимости) и должен быть оформлен в виде документа «Проект акта классификации ИС по требованиям безопасности информации».

В ходе работ также должна быть определена область проведения аттестации для ИС СТАТС, которая должна быть зафиксирована в отчетном документе «Акт определения области проведения аттестации ИС». Должны быть определены сегменты (если таковые имеются), участвующие в аттестации по требованиям безопасности информации в качестве типовых сегментов ИС.

* + - * 1. **Определение угроз безопасности информации ИС СТАТС**

В результате работ для ИС СТАТС должен быть создан документ «Проект модели угроз безопасности информации» с учетом выделенных типовых сегментов.

При этом угрозы безопасности информации должны быть определены (для всех сегментов, если таковые имеются) по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

Для определения угроз безопасности информации и разработки модели угроз безопасности информации должны применяться методические документы, указанные в пункте 1.13 ТЗ, в том числе проект методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах».

При формировании общего перечня угроз безопасности информации информационной системы в качестве исходных данных для определения угроз безопасности информации должен использоваться Банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

В качестве дополнительных источников для формирования общего перечня угроз безопасности информации, в случае обработки в информационной системе персональных данных, должны использоваться:

* Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15 февраля 2008 г. (далее – Базовая модель угроз).

В рамках формирования общего перечня угроз безопасности информации информационной системы перечень угроз Банка данных угроз безопасности информации необходимо дополнить как минимум угрозами, представленными ниже:

* угрозы, связанные с наличием недекларированных возможностей в системном программном обеспечении;
* угрозы, связанные с наличием недекларированных возможностей в прикладном программном обеспечении;
* угрозы утечки информации по каналу побочных электромагнитных излучений и наводок;
* природные угрозы;
* техногенные угрозы;
* угрозы утечки акустической (речевой) информации.

В ходе работ по определению угроз безопасности информации необходимо определить способ размещения информационной системы в вычислительной инфраструктуре ЦОД Заказчика. С учетом типовой модели предоставления вычислительной инфраструктуры ЦОД Заказчика как сервиса возможны следующие способы размещения информационной системы в вычислительной инфраструктуре ЦОД:

* размещение по модели «Colocation» - размещение вычислительного, телекоммуникационного и иного оборудования в ЦОД Заказчика и обеспечение его подключения к каналам связи с высокой пропускной способностью;
* размещение по модели «Инфраструктура как услуга» - обеспечение размещения ИС на виртуальных вычислительных мощностях ЦОД Заказчика, реализуемое в виде организации виртуального сервера с характеристиками по выбору, ограниченными возможностями ЦОД Заказчика, с развернутым эталонным дистрибутивом операционной системы по выбору из перечня ЦОД Заказчика. В рамках данной услуги Заказчик не управляет и не контролирует лежащую в основе инфраструктуру, но имеет контроль над операционной системой и развернутыми приложениями. Размещение по модели «Инфраструктура как услуга» состоит из предоставления в аренду виртуальных вычислительных ресурсов и дискового пространства в составе виртуальной машины; организации сетевого хранилища данных в составе виртуальной машины.
* размещение по модели «Платформа как услуга» - услуга заключается в предоставлении во временное пользование виртуальной платформы исполнения, включающей в себя виртуальную машину, ОС (ОС и СУБД), для развёртывания программного обеспечения, созданного на базе языков программирования и инструментов, поддерживаемых предоставляемой платформой исполнения, реализуемой в виде организации виртуального сервера с предустановленными лицензированными ОС и СУБД по выбору, ограниченному перечнем ЦОД Заказчика. Заказчик не имеет возможности управлять инфраструктурой (сетевое и серверное оборудование, СХД, ПО виртуализации), но имеет контроль над развёрнутыми приложениями и настройками среды исполнения.

Размещение по модели «Платформа как услуга» состоит из:

* подбора (или экспертизы подбора) конфигурации ВМ, исходя из минимальных системных требований необходимых ОС и СУБД и прогноза расчётно-плановых значений потребления ресурсов;
* предоставления в пользование сконфигурированной ВМ, с предустановленными ОС и СУБД;
* предоставления возможности сетевого взаимодействия с информационными системами размещёнными на вычислительных ресурсах ЦОД Заказчика;
* предоставления возможности удалённого администрирования ОС и СУБД по защищённым каналам связи;
* регистрации ВМ в технологическом домене ЦОД Заказчика (если иное не указано в Заявке);
* подключения ВМ к сервису лицензирования;
* подключения ВМ к сервису централизованного управления ППО и инвентаризации;
* подключения ВМ к серверу мониторинга качества;
* централизованного администрирования ОС и СУБД.

В соответствии с определенным способом размещения информационной системы в вычислительной инфраструктуре ЦОД Заказчика необходимо определить соответствующие ему технологические (архитектурные) уровни для каждого сегмента информационной системы.

Для каждого из технологических (архитектурных) уровней характерны соответствующие угрозы безопасности информации. Для технологических (архитектурных) уровней защищенной вычислительной инфраструктуры ЦОД Заказчика актуальные угрозы безопасности информации определены и нейтрализованы (блокированы) системой защиты информации вычислительной инфраструктуры ЦОД Заказчика. При моделировании угроз безопасности информации необходимо учитывать только те объекты воздействия, которые применимы к технологическим (архитектурным) уровням системы защиты информации информационной системы, а также те объекты воздействия, которые не закрываются системой защиты информации вычислительной инфраструктуры ЦОД Заказчика.

Заказчик направляет в уполномоченные органы по сертификации (аттестации) «Проект модели угроз безопасности информации» для ИС СТАТС, разработанный и представленный Подрядчиком по результатам завершения Этапа 1. В период прохождения согласования у уполномоченных органов «Проекта модели угроз безопасности информации» Подрядчик продолжает выполнение работы в сроки, предусмотренные настоящим ТЗ.

В случае если по результатам указанного потребуются доработки «Проекта модели угроз безопасности информации» для ИС СТАТС в соответствии с замечаниями уполномоченных органов, Подрядчик обязан в срок не более 5 (пяти) рабочих дней, провести требуемые доработки, а также при необходимости внести изменения в иные документы и результаты выполнения работ по настоящим ТЗ, не прерывая выполнение работ, предусмотренных настоящим ТЗ.

Результатом согласования является утвержденная ФСБ России и ФСТЭК России версия «Проекта модели угроз безопасности информации» для ИС СТАТС. Данная версия документа должна быть доведена до Подрядчика не позднее 10 (десяти) рабочих дней с момента ей получения от уполномоченных органов.

После получения от Подрядчика доработанной по требованиям ФСБ России и (или) ФСТЭК России «Проекта модели угроз безопасности информации» Заказчик направляет ее на повторное согласование в уполномоченные органы (уполномоченный орган).

Согласованная версия «Проекта модели угроз безопасности информации» должна быть получена Заказчиком за 10 (десять) рабочих дней до начала этапа 7 «Аттестация ИС СТАТС по требованиям безопасности информации». В случае если документ не был получен Заказчиком в установленный срок, к Подрядчику применяются пени в соответствии с положениями Контракта.

Стороны согласились, что процесс согласования «Проекта модели угроз безопасности информации» не влечет за собой невозможность выполнения этапов № 2, 3, 4, 5 и 6. Подрядчик не вправе ссылаться на отсутствие согласованной уполномоченными органами (или органом) «Проекта модели угроз безопасности информации» как причину несвоевременного или некачественного выполнения работ по настоящему ТЗ.

* + - * 1. **Определение класса СКЗИ**

Необходимо выполнить работы по определению требуемого класса СКЗИ. Работы должны выполняться согласно требованиям приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» и методического документа «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденного руководством 8 Центра ФСБ России 31 марта 2015 г. № 149/7/2/6-432.

Результаты работ должны быть отражены в документе «Проект модели угроз безопасности информации».

* + - * 1. **Определение требований к системе защиты ИС СТАТС**

Требования к системе защиты информации, обрабатываемой в ИС СТАТС, должны быть определены в зависимости от класса защищенности ИС СТАТС и их типовых сегментов (при наличии таковых), и угроз безопасности информации, включенных в «Проект модели угроз безопасности информации» (работы, выполненные согласно пунктам 4.1.9.1.1– 4.1.9.1.4 ТЗ).

В зависимости от способа размещения информационной системы в вычислительной инфраструктуре ЦОД Заказчика должен определяться перечень мер защиты информации для каждого из технологических (архитектурных) уровней, реализуемых на базе системы защиты информации информационной системы. При этом, для технологических (архитектурных) уровней вычислительной инфраструктуры ЦОД Заказчика должны учитываться меры защиты информации, предусмотренные пунктом 4.1.12 ТЗ, которые реализованы системой защиты информации вычислительной инфраструктуры ЦОД Заказчика.

Требования к подсистеме обеспечения информационной безопасности ИС СТАТС, которая должна быть проверена в ходе прохождения сертификационных испытаний, должны быть сформулированы на основании приказа ФСТЭК от 11 февраля 2013 г. № 17
«Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Требования к реализации подсистемы обеспечения информационной безопасности ИС СТАТС должны быть включены в **«**Частное техническое задание на создание системы защиты информации». Требования в том числе должны в себе содержать требования на доработку встроенного функционала ППО ИС СТАТС по информационной безопасности. Требования на доработку встроенного функционала ППО ИС СТАТС должны формироваться на основании Требований к подсистеме обеспечения информационной безопасности, приведенных в пункте 4.2.7 ТЗ.

* + - 1. **Создание системы защиты информации ИС СТАТС**

На данном этапе должно быть проведено создание СЗИ ИС СТАТС, которая включает в себя в том числе следующие средства защиты конфиденциальной информации:

* наложенные средства защиты информации;
* подсистему информационной безопасности ППО ИС СТАТС.

Создание ИС СТАТС выполняется в соответствии с Частным техническим заданием на создание системы защиты информации с учетом ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (далее – ГОСТ 34.601), ГОСТ Р 51583-2014 и ГОСТ Р 51624-2000 и в том числе должно включать:

* проектирование систем защиты информации ИС СТАТС;
* разработку (актуализацию) эксплуатационной документации на СЗИ ИС СТАТС.

При этом должна быть разработана следующая документация:

* Технический проект СЗИ ИС СТАТС:
	+ Ведомость технического проекта;
	+ Пояснительная записка к техническому проекту СЗИ;
	+ Описание технологического процесса обработки информации;
	+ Схема размещения комплекса технических средств системы защиты информации;
	+ Схема структурная комплекса технических средств;
	+ Схема функциональной структуры;
	+ Описание настроек средств защиты информации;
	+ Ведомость покупных изделий системы защиты информации.
	+ Руководство администратора информационной безопасности.

При проектировании системы защиты информации ИС СТАТС в зависимости от способа размещения информационной системы в вычислительной инфраструктуре ЦОД Заказчика для технологических (архитектурных) уровней вычислительной инфраструктуры ЦОД должны учитываться меры защиты информации, предусмотренные пунктом 4.1.12 ТЗ, которые реализованы системой защиты информации вычислительной инфраструктуры ЦОД Заказчика.

Поставка и внедрение необходимых наложенных средств защиты информации осуществляется Заказчиком в рамках отдельной закупки и не является предметом выполнения работ по настоящему Контракту, в том числе настоящего ТЗ.

* + - 1. **Разработка организационно-распорядительной документации на СЗИ ИС СТАТС**

Организационно-распорядительная документация разрабатывается в соответствии с требованиями Частного технического задания на создание системы защиты информации и результатами технического проектирования ИС СТАТС и направлена, в том числе, на приведение процессов обработки информации ИС СТАТС в соответствие требованиям законодательства в области информационной безопасности, при этом должны учитываться технологические особенности обработки информации в ИС. Организационно-распорядительная документация включает в себя проекты документов по вопросам обработки и обеспечения безопасности информации, содержащейся в ГИС.

Базовый пакет проектов организационно-распорядительной документации, приведенный в таблице 10. Полный перечень организационно-распорядительной документации будет приведен в составе Частного технического задания на системы защиты информации.

**Таблица 9 - Базовый пакет проектов организационно-распорядительной документации**

| п/п№ | Документ |
| --- | --- |
| 1. | Регламент управления (администрирования) СЗИ (проект) |
| 2. | Регламент выявления инцидентов и реагирования на них (проект) |
| 3. | Регламент управления конфигурацией ИС и ее СЗИ (проект) |
| 4. | Регламент обеспечения защиты информации при выводе ИС из эксплуатации или после принятия решения об окончании обработки информации (проект) |

* + - 1. **Подготовка к сертификации и сертификация ППО ИС СТАТС по требованиям безопасности информации**

Подготовка к сертификации включает в себя:

* оформление требований к встроенному функционалу ППО ИС СТАТС, входящего в область проведения аттестации, с учетом требований, определенных согласно пункту 4.2.7 ТЗ. Требования должны быть оформлены в виде проекта документа «Технические условия», на основе которого будет проводиться сертификация ППО ИС СТАТС. Данные требования должны формироваться на основании требований, приведенных в пункте 4.2.7 к ТЗ;
* подача заявки на сертификацию по требованиям безопасности информации во ФСТЭК России.

Подрядчик обязан устранить замечания к заявке до момента принятия заявки. Подрядчик после подачи заявки на проведение сертификации во ФСТЭК России передает Заказчику копию заявки с отметкой о приеме.

Результатом выполнения сертификации ППО является получение Подрядчиком сертификата соответствия в системе сертификации средств защиты информации ФСТЭК России (средства защиты информации информационных систем) ППО ИС СТАТС.

По результатам выполнения работ по Этапу 6 Подрядчик предоставляет Заказчику следующие документы:

* Технические условия, утвержденные испытательной лабораторией;
* Руководство администратора по комплексу средств защиты;
* Копия сертификата соответствия в системе сертификации средств защиты информации ФСТЭК России (средства защиты информации информационных систем) ППО ИС СТАТС.

* + - 1. **Аттестация ИС СТАТС по требованиям безопасности информации**

В рамках данного этапа проводятся аттестационные испытания выделенных согласно «Акту определения области проведения аттестации» сегментов информационной системы.

В процессе подготовки и проведения аттестационных испытаний должны быть оформлены:

* Программа и методика аттестационных испытаний;
* Протокол аттестационных испытаний;
* Протокол анализа уязвимостей информационной системы;
* Заключение по результатам аттестационных испытаний;
* Аттестат соответствия требованиям безопасности.

Аттестация информационной системы должна проводиться в соответствии с программой и методикой аттестационных испытаний с применением национальных стандартов, а также методических документов, указанных в пункте 1.13 ТЗ.

Аттестация информационной системы должна быть проведена на основе результатов аттестационных испытаний выделенного набора сегментов информационной системы, реализующих полную технологию обработки информации.

Особенности аттестации информационной системы на основе результатов аттестационных испытаний выделенного набора ее сегментов, а также условия и порядок распространения аттестата соответствия на другие сегменты информационной системы должны быть определены в программе и методике аттестационных испытаний, заключении по результатам аттестационных испытаний и аттестате соответствия требованиям безопасности.

При аттестации информационной системы должны использоваться результаты аттестации вычислительной инфраструктуры ЦОД Заказчика, полученные в рамках исполнения гражданско-правового договора бюджетного учреждения от 15.11.2017 № 30/11/17 на оказание услуг по обеспечению информационной безопасности вычислительной инфраструктуры в общегородском Центре обработки данных: копия аттестата, копия модели угроз информационной безопасности, которые будут предоставлены Подрядчику не позже 5 (пяти) рабочих дней после заключения Контракта в рабочем порядке.

Подрядчик приступает к выполнению работ, предусмотренных пунктом 4.1.9.5 ТЗ, после предоставления Заказчиком подтверждения выполнения требований, предусмотренных пунктом 4.1.9.1.3 ТЗ и поставки и внедрения необходимых средств защиты информации (за исключением встроенного функционала ППО ИС СТАТС в соответствии с пунктом 4.2.7 ТЗ). В случае, если указанное подтверждение получено Подрядчиком после завершения работ, предусмотренных Этапом 6, датой начала выполнения работ, предусмотренных Этапом 7, является дата, следующая за датой предоставления Заказчиком указанного подтверждения.

* + 1. **Требования по сохранности информации при авариях**

Сохранность информации в Системе должна обеспечиваться:

* при пожарах, затоплениях, землетрясениях и других стихийных бедствиях: организационными и защитными мерами, опирающимися на подготовленность помещений и персонала, обеспечивающими сохранность хранимых копий информации на магнитном носителе;
* при разрушении данных при механических и электронных сбоях и отказах в работе компьютеров: на основе программных процедур восстановления информации с использованием хранимых копий баз данных, файлов журналов изменений в базах данных, копий программного обеспечения.

Для обеспечения сохранности информации в Системе должны быть включены следующие функции:

* резервное копирование баз данных Системы;
* восстановление данных в непротиворечивое состояние при программно-аппаратных сбоях (отключение электрического питания, сбоях операционной Системы и других) вычислительно-операционной среды функционирования;
* восстановление данных в непротиворечивое состояние при сбоях в работе сетевого программного и аппаратного обеспечения.
	+ - 1. **Перечень событий, при которых должна быть обеспечена сохранность информации в Системе**

В Системе должно предусматриваться восстановление обрабатываемой информации в следующих аварийных ситуациях:

* программный сбой при операциях записи-чтения;
* разрыв связи с клиентской программой (терминальным устройством) в ходе редактирования/обновления информации;
* выход из строя одной и более нод вычислительного кластера (допустимое количество одновременно вышедших из строя нод определяется конфигурационными настройками кластера и коэффициентом избыточности при хранении данных).

В Системе должна предусматриваться возможность ручного восстановления обрабатываемой информации из резервной копии в при ошибочных действиях обслуживающего персонала.

В Системе должно предусматриваться автоматическое восстановление работоспособности серверной части Системы в следующих ситуациях:

* штатное и аварийное отключение электропитания серверной части;
* штатная перезагрузка Системы и загрузка после отключения;
* программный сбой общесистемного программного обеспечения, приведший к перезагрузке Системы.

В Системе должно предусматриваться полуавтоматическое восстановление работоспособности серверной части Системы в следующих аварийных ситуациях:

* физический выход из строя любого аппаратного компонента – после замены компонента и восстановления конфигурации общесистемного программного обеспечения;
* аварийная перезагрузка Системы.
	+ - 1. **Требования к регламентам и объемам резервного копирования и архивирования данных**

Резервное копирование информации может осуществляться в двух режимах:

* создание полной копии базы данных;
* сохранение изменений, внесенных со времени создания последней архивной копии.

Периодичность и очередность этих операций определяются отдельным распоряжением, а также политикой резервного копирования информации и положением по категоризации информационных ресурсов.

* + 1. **Требования к патентной чистоте**
			1. **Перечень стран, в отношении которых должна быть обеспечена патентная чистота системы и ее частей**

Патентная чистота программного комплекса и его частей должна быть обеспечена в отношении патентов, действующих на территории Российской Федерации.

Реализация технических, программных, организационных и иных решений, предусмотренных проектом Системы не должна приводить к нарушению авторских и смежных прав третьих лиц.

* + - 1. **Требования к использованию лицензионного программного обеспечения**

При использовании в Системе программ (программных комплексов или компонентов), разработанных третьими лицами, условия, на которых передается право на использование (исполнение) этих программ, не должны накладывать ограничений, препятствующих использованию Системы по ее прямому назначению.

* + 1. **Требования к вычислительной инфраструктуре**

Выполнение требований данного раздела обеспечиваются Заказчиком в рамках иных конкурсных процедур или другим законным способом, за исключением мер защиты, реализуемых средствами ППО ИС СТАТС.

Для сегмента вычислительной инфраструктуры центра обработки данных, в котором размещаются вычислительные ресурсы, должны обеспечиваться следующие технические и организационные меры защиты информации:

* организационные меры и меры физической безопасности вычислительной инфраструктуры ЦОД Заказчика;
* меры и средства защищенного системного и(или) специального программного обеспечения информационной системы и(или) наложенных средств защиты информации от несанкционированного доступа;
* меры и средства обеспечения защиты инфраструктуры виртуализации вычислительной инфраструктуры ЦОД Заказчика;
* меры и средства обеспечения межсетевого экранирования вычислительной инфраструктуры ЦОД Заказчика;
* меры и средства обеспечения обнаружения вторжений вычислительной инфраструктуры ЦОД Заказчика;
* меры и средства обеспечения защиты каналов связи вычислительной инфраструктуры ЦОД Заказчика;
* меры и средства обеспечения анализа защищенности вычислительной инфраструктуры ЦОД Заказчика;
* меры и средства обеспечения удаленного доступа и мониторинга действий привилегированных пользователей вычислительной инфраструктуры ЦОД Заказчика;
* меры и средства обеспечения доступности вычислительной инфраструктуры ЦОД Заказчика;
* защиту информационной системы, ее средств, систем связи и передачи данных (со своей стороны Заказчик обеспечивает возможность использования внешним пользователем, являющимся физическим лицом, СКЗИ на основе web-браузера, не требующем его покупки пользователем, сертифицированного ФСБ России, при условии существования такого решения).
	+ 1. **Требования по стандартизации и унификации**

Взаимодействие пользователей с Системой должно осуществляться посредством визуального графического интерфейса (GUI). Интерфейс Системы должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм. Навигационные элементы должны быть выполнены в удобной для пользователя форме. Средства редактирования информации должны удовлетворять принятым соглашениям в части использования функциональных клавиш, режимов работы, поиска, использования оконной Системы. Ввод-вывод данных Системы, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям Системы.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление Системой должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов. Клавиатурный режим ввода должен использоваться главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм.

Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений) должны быть на русском языке.

Система должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных ранее случаях Система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Клиентская часть Системы должна функционировать на мультиплатформенной основе с использованием наиболее распространённых интернет браузеров (Chrome, Safari, Opera, Firefox,YandexBrowser).

Система должна оборудоваться в соответствии с Санитарными правилами и нормами - СанПиН 2.2.2.542-96 – «Гигиенические требования к видео дисплейным терминалам, персональным электронно-вычислительным машинам и организации работ» (утверждёнными постановлением Госкомсанэпиднадзора РФ от 14 июля 1996 г. № 14).

* + 1. **Дополнительные требования**
			1. **Специальные требования**

При развитии Системы должен применяться итерационный (модульный) подход в зависимости от длительности и сложности разработки.

Технические средства, необходимые для размещения разрабатываемого решения, предоставляются Заказчиком.

Подрядчик должен сформулировать предложение по размещению Системы, исходя из заданных параметров производительности, доступности и информационной безопасности. Предложение по размещению в части требуемых мощностей должно быть описано в документе «Описание архитектуры Системы» и согласовано с Заказчиком.

* + - 1. **Требования к оптимизации и модернизации**

С целью обеспечения поддержания требуемого уровня производительности Системы, подсистема сбора данных должна быть модернизирована в части:

* увеличения допустимой нагрузки на Систему с учетом увеличения количества интернет-посетителей;
* повышение уровня отказоустойчивости Системы с учетом роста объема поступающих данных в Систему.

При модернизации подсистемы в рамках обеспечения требуемого уровня производительности, отказоустойчивости и достижения операционных возможностей требуется обеспечить:

* высокую скорость передачи служебных сообщений между компонентами системы в пространстве распределённой системы больших данных;
* реализацию последовательного сохранения записывающихся событий в подсистему хранения данных для обеспечения возможности повторного считывания событий с начала хранимого периода (поддержка историчности хранения информации по событиям);
* возможность сохранения порядка следования сообщений в очереди сообщений;
* достаточный уровень отказоустойчивости системы при пиковых значениях увеличения нагрузки на систему;
* возможность масштабирования подсистемы для повышения производительности при дальнейшем увеличении нагрузки;
* длительное хранение данных с возможностью поиска на всю глубину хранения.
	+ - 1. **Требования о наличии лицензий**

Для выполнения работ по пункту 4.1.9 ТЗ Подрядчик должен обладать действующей лицензией ФСТЭК России, на деятельность по технической защите конфиденциальной информации, устанавливающей право выполнения следующих работ и услуг:

* аттестационные испытания и аттестация на соответствие требованиям по защите информации средств и систем информатизации;
* проектирование в защищенном исполнении средств и систем информатизации.

Для выполнения работ по пункту 4.2.7 ТЗ Подрядчик должен обладать действующей лицензией ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации, устанавливающей право выполнения следующих работ и услуг: разработка средств защиты конфиденциальной информации, в том числе: программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации.

Для выполнения работ по определению требуемого класса СКЗИ и подготовки документа «Проектмодели угроз безопасности информации» ИС СТАТС (пункт 4.1.9.1.4 ТЗ) Подрядчик должен обладать действующими лицензиями ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), устанавливающими право выполнения следующих работ и услуг: разработка защищенных с использованием шифровальных (криптографических) средств информационных систем.

В случае если у Подрядчика отсутствует данные лицензии он должен привлечь для выполнения данных работ субподрядчика, имеющего действующие лицензии.

* 1. **Требования к функциям (задачам), выполняемым Системой**
		1. **Требования к сценариям (процессам), автоматизируемым Системой**

Данный раздел содержит описание и требования к сценариям (процессам) реализуемым в рамках работ по развитию ИС СТАТС

* + - 1. **Сценарий «Присвоение интернет-посетителю многофакторного статистического идентификатора»**

При выполнении сценария «Присвоение интернет-посетителю многофакторного статистического идентификатора» подсистема сбора данных должна в автоматическом режиме собирать данные необходимые для присвоения посетителю статистического идентификатора и передавать их в подсистему обработки данных.

Подсистема обработки данных должна в автоматическом режиме при получении данных:

* проверять наличие статистического идентификатора в подсистеме хранения данных, соответствующего совокупности полученных признаков;
* присваивать посетителю статистический идентификатор при его отсутствии в системе;
* дополнять идентификатор вновь полученными признаками;
* очищать подсистему хранения данных от задвоенных идентификаторов с целью повышения качества статистических расчётов.

Подсистема хранения данных должна обеспечивать хранение статистических идентификаторов в формате, учитывающем признаки, как полученные с помощью cookies, так и с помощью отпечатка рабочей среды интернет-посетителя.

В целом Система должна в режиме реального времени автоматически:

* + - 1. присваивать статистический идентификатор новому посетителю, как по совокупности признаков идентификации, так и по отдельности полученных признаков:
* cookies;
* отпечаток рабочей среды интернет-посетителя;
	+ - 1. дополнять существующий статистический идентификатор новыми признаками;
			2. унифицировать задвоенные записи определённые по совокупности признаков.

При обращении посетителя к интернет-ресурсу Система должна проверять наличие в подсистеме хранения тождественногостатистического идентификатора. В случае отождествления пользователя со статистическим идентификатором по информации cookies, Система должна проверять наличие в подсистеме хранения признака отпечатка рабочей среды интернет-посетителя. При отсутствии признака, статистический идентификатор должен быть дополнен им.

В случае отсутствия статистического идентификатора, он назначается пользователю по признаку отпечатка рабочей среды интернет-пользователя с идентификационным маркером cookie.

При обнаружении нескольких статистических идентификаторов соответствующих одному отпечатку рабочей среды Система должна унифицировать статистический идентификатор.

В совокупности признаков «cookies-отпечаток» первичным признаком Система должна считать «уникальный отпечаток рабочей среды».

* + - 1. **Сценарий «Представление информации о профиле интернет пользователя»**

Сценарий «Представление информации о профиле интернет пользователя» описывает автоматизируемый процесс представления данных о профиле интернет пользователя.

Данные о профиле интернет пользователя дополнительно должны содержать «историю профиля»:

* Дата/Время первого появления идентификатора в системе;
* Дата/Время объединения идентификаторов (если это происходило);
* История добавления/изменения технических характеристик устройств пользователя.

Статистические данные профиля должны включать в себя все доступные отчеты, настроенные в системе. При добавлениив Систему новых отчетов, предусматривающих работу с профилем, данные отчеты должны автоматически появляться при вызове сценария предоставления информации о профиле интернет пользователя.

* + - 1. **Сценарий «Представление общей статистики по профилям интернет пользователя»**

Сценарий «Представление общей статистики по профилям интернет пользователей» описывает автоматизируемый процесс осуществления просмотра общей статистики по профилям интернет пользователей.

Статистические данные по профилям интернет пользователей должны включать в себя все доступные отчеты, настроенные в системе. Все новые отчеты должны быть доступны для формирования для текущего набора профилей.

* + - 1. **Сценарий «Представление статистики интернет события»**

Сценарий «Представление статистики интернет события» описывает автоматизируемый процесс просмотра статистики события интернет ресурса, передаваемого внешними системами-источниками (функционального назначения события).

При осуществлении функции представления статистики интернет ресурса должны быть представлены следующие сведения:

* распределение количества событий во временном периоде;
* количество уникальных посетителей, совершивших указанное событие;
* среднее количество событий в день;
* сегменты интернет пользователей, совершающих действие, приведшее к получению рассматриваемого события (в разрезе событий схожего функционального назначения).
	+ - 1. **Сценарий «Построение цепочек выполнения целевого действия пользователем на интернет ресурсах»**

Сценарий «Построение цепочек выполнения целевого действия пользователем на интернет ресурсах» описывает автоматизируемый процесс построения цепочек действий пользователя на интернет ресурсах, которые были совершены до осуществления целевого действия.

При выборе целевого действия должны быть доступны следующие типы назначений:

* посещение определенной страницы интернет ресурса;
* отправка поискового запроса на интернет ресурсе;
* выполнение события из списка событий, предоставляемых внешними системами-источниками в подсистему сбора данных;
* переход по внешней ссылке, фиксируемый разрабатываемым компонентом в рамках подсистемы сбора данных.

При осуществлении функции построения цепочек действий пользователя на интернет ресурсах должны выполняться следующие операции:

* фиксация действий пользователей на интернет ресурсах;
* накопление статистических данных для анализа;
* определение сегмента для интернет-пользователя на основе информации о прогнозных значений поведенческого сегмента, к которому имеет отношение посетитель;
* анализ последовательности переходов и действий (событий) интернет посетителя;
* построение цепочек действий пользователя на основании проведенного анализа до реализации целевого действия;
* построение цепочек действий пользователя на основании проведенного анализа после реализации целевого действия;
* выявление поведенческих сегментов интернет посетителей, отправляющих поисковые запросы по схожей тематике/ категории.
	+ - 1. **Сценарий «Построение преднастроенных статистических отчетов»**

Для уменьшения времени реакции системы на действия пользователей в системе должны быть предусмотрены сценарии расчета и подготовки наиболее востребованных отчетов заранее.

Данные сценарий должен применяться ко всем стандартным отчетам и отчетам, построенным с помощью конструктора (при условии, что при построении выбрана опция «регулярное создание отчета»).

* + - 1. **Сценарий «Рассылка статистической информации»**

В случае формирования отчетов в системе должен быть предусмотрен вариант предоставления отчета по электронной почте.

Сценарий должен включать в себя подготовку и отправку отчетов.

* + - 1. **Сценарий «Построение взаимосвязей интернет посетителей»**

Сценарий «Построение взаимосвязей интернет посетителей» описывает результаты анализа сопоставления интернет посетителей по уникальному идентификатору, присвоенному механизмом генерации cookies и механизмом генерации по характеристикам устройства.

Сопоставление должно производиться путем:

* анализа времени присвоения различных id одному интернет посетителю;
* анализа отклонений в количестве различных интернет посетителей, связанных одним id;
* анализа поведения интернет посетителя и поиска схожих по поведению и характеристикам.

Для анализа должны быть использованы графовые методы исследования для визуализации связей и поиска выбросов. Для поиска похожих по поведению интернет посетителей должны быть использованы механизмы look-a-like с использованием таких атрибутов, как частота, время посещений интернет ресурсов, тематики посещаемых интернет ресурсов, выполняемые целевые действия и их последовательность, прогнозные значения поведенческого сегмента.

Должно быть реализовано представление на основании проведенного анализа по взаимосвязям интернет посетителей в рамках одного интернет ресурса, с распределением по следующим группам:

* одиночные интернет посетители;
* интернет посетители, схожие по устройствам в качестве домохозяйств;
* интернет посетители, схожие по поведению в качестве домохозяйств;
* интернет посетители, схожие по устройствам различной по категориям функционального действия социальной группы (категория должна быть определена в зависимости от выявленных особенностей группы – устройства в образовательных учреждениях, устройства в городских центрах предоставления государственных услуг);
* интернет посетители, схожие по поведению различной по категориям функционального действия социальной группы (категория должна быть определена в зависимости от выявленных особенностей группы – устройства в образовательных учреждениях, устройства в городских центрах предоставления государственных услуг).
	+ 1. **Требования к функциям модернизируемой подсистемы сбора данных**

В рамках выполняемых работ по развитию ИС СТАТС должны быть разработаны следующие функции модернизируемой подсистемы сбора:

* модуль определения уникального интернет-посетителя без использования cookies:
	+ функция получения специфичных настроек браузера и пользовательского устройства;
	+ функция обработки полученных параметров и генерации уникального идентификатора;
	+ функция присвоения уникального идентификатора интернет-посетителю с учетом алгоритма сопоставления и проверки на уникальность;
* механизм фиксации переходов по внешним ссылкам:
	+ функция получения информации о переходе интернет-посетителя по внешней ссылке;
* модуль загрузки данных из внешних информационных систем в формате csv, json, avro:
	+ функция взаимодействия со внешними ИС посредством не менее 5 протоколов и форматов передачи и хранения данных.

По итогам модернизации механизма генерации статистического идентификатора, являющегося модулем определения уникального интернет-посетителя без использования cookies, необходимо обеспечить:

* реализацию механизма получения Системой совокупного «отпечатка рабочей среды статистического идентификатора» без внедрения программного обеспечения или иной информации на жёсткий диск посетителя;
* разработку алгоритма составления статистического идентификатора по полученному ранее «отпечатку рабочей среды».

Полный перечень параметров, участвующих в формировании статистического идентификатора без использования cookies, должен быть определен Подрядчиком и согласован с Заказчиком на этапе проектирования и приведен в документе «Пояснительная записка».

В части обеспечения надёжности предоставления собранной информации и повышения уровня её структурированности для подсистемы сбора данных должны быть предусмотрены механизмы:

* буферизации очереди сообщений;
* сохранения порядка записи сообщений.

В рамках модернизации подсистемы сбора данных должен быть разработан механизм фиксации переходов интернет-пользователей по внешним и внутренним ссылкам информационных ресурсов, с последующей инициализацией обработки параметров этого перехода и передачи в агрегированном виде во внешние системы-потребители, а также модуль загрузки данных из внешних систем в форматах csv, json, avro.

* + 1. **Требования к функциям модернизируемой подсистемы обработки данных**

В рамках выполняемых работ по развитию ИС СТАТС должны быть разработаны следующие модули модернизируемой подсистемы обработки данных:

* модуль полнотекстового поиска;
* модуль сегментирования всех интернет-посетителей с учетом прогнозных значений поведения;
* модуль сопоставления интернет-посетителей по уникальному идентификатору;
* модуль сервиса коротких ссылок.

В рамках модулей подсистемы обработки данных должны быть реализованы следующие функции:

* модуль полнотекстового поиска:
	+ получение информации не менее, чем из 6 различных по составу и типу данных справочников, хранящихся в реляционных и нереляционных СУБД;
	+ формирование наборов данных для предоставления по интернет-ресурсу по свободному вводу наименования ресурса;
	+ формирование наборов данных для предоставления по целевому действию обращения к поисковому сервису;
	+ формирование наборов данных для предоставления по страновой принадлежности интернет-соединения;
	+ формирование наборов данных для предоставление данных по любому доступному текстовому полю лога действия интернет-посетителя;
* модуль сегментирования всех интернет-посетителей с учетом прогнозных значений поведения:
	+ функция построения поведенческих групп интернет-посетителей при помощи не менее 3 внутренних и не менее 9 внешних справочников;
	+ функция настройки частоты перестроения поведенческих групп;
* модуль сопоставления интернет-посетителей по уникальному идентификатору:
	+ функция сопоставления интернет-посетителей по уникальному идентификатору с возможностью анализа статистических выбросов по запросу;
	+ функция настройки частоты обновления данных о сопоставленных статистических идентификаторах;
* модуль сервиса коротких ссылок:
	+ интеграция с входным контуром Системы;
	+ функция генерации коротких ссылок с учетом количества уникальных кампаний и не менее 2 каналов их использования;
	+ хранение сопоставлений между целевыми и короткими ссылками.

Модуль полнотекстового поиска должен обеспечивать:

* фильтрацию данных для предоставления статистической информации по интернет-ресурсу как по полному, так и по частичному вводу адреса интернет-ресурса;
* фильтрацию данных для предоставления статистической информации по целевому действию обращения к поисковому сервису как по полному, так и по частичному вводу поисковой фразы;
* фильтрации данных для предоставления статистики по страновой принадлежности интернет-соединения, используемого интернет-посетителем;
* фильтрация данных по любому доступному текстовому полю лога действия интернет-посетителя.

Модуль сегментирования всех интернет-посетителей с учетом прогнозных значений поведения должен предоставлять возможность построения математических и прогнозных моделей вероятностных значений, характеризующих интернет-посетителя, на основе:

* частоты посещения интернет-ресурсов;
* категории интересов, определенной с использованием категории посещенных интернет-ресурсов;
* выявленных закономерностей в поведении на интернет-ресурсах сформированных групп интернет посетителей.

Модуль сегментирования всех интернет-посетителей с учетом прогнозных значений поведения должен обеспечивать построение поведенческих групп интернет-посетителей и перестраивать их на основе поступающих непрерывно новых данных. В рамках данного модуля должны быть определены временные критерии необходимой частоты перестроения сегментов с учетом типа и назначения рассчитываемой характеристики. Критерии должны быть определены на этапе проектирования и приведены в документе «Пояснительная записка».

Модуль сопоставления интернет-посетителей по уникальному идентификатору должен обеспечивать сопоставление хранящихся статистических идентификаторов, сформированных с использованием cookies и идентификаторов, сформированных разработанным механизмом генерации статистических идентификаторов по «отпечатку рабочей среды» с целью обеспечения сбора статистических данных.

Модуль сервиса коротких ссылок должен обеспечивать:

* подготовку коротких ссылок для целевых ссылок на интернет-ресурсы города Москвы;
* хранение сопоставлений между короткими ссылками и целевыми ссылками. Короткие ссылки должны иметь однозначное сопоставление с целевыми и должны быть уникальными;
* интеграцию с входным контуром ИС СТАТС;
* API для генерации и получения статистики от клиентских систем;
* трансляцию коротких ссылок обратно в целевые вместе с собранными по ним при переходе пользователей статистическими данными.

При формировании коротких ссылок модуль сервиса коротких ссылок должен «маркировать» их ID пользователей с сокрытием референтных окончаний ссылок, содержащих ID пользователя, с целью сбора статистики при переходе по ссылке из sms-оповещений.

Формируемые модулем короткие ссылки должны иметь физическую возможность быть корректно интегрированными в социальные сети.

В модуле сервиса коротких ссылок должна быть обеспечена интеграция с существующим циклом сбора и обработки данных.

* + 1. **Требования к функциям модернизируемой подсистемы хранения данных**

В рамках выполняемых работ по развитию ИС СТАТС должна быть модернизирована подсистема хранения данных. Подсистема должна обеспечить выполнение функций ИС СТАТС при любом изменении в процессе модернизации формата и объёма данных, участвующих в жизненном цикле Системы.

В рамках модернизации подсистемы хранения данных должна быть реализована функция хранения не менее 6 новых справочников и иных источников данных в файловой системе с учетом возможного изменения их объема и формата хранения.

* + 1. **Требования к функциям модернизируемой подсистемы статистики и мониторинга**

В рамках выполняемых работ по развитию ИС СТАТС должна быть модернизирована подсистемы статистики и мониторинга. В процессе модернизации подсистемы статистики и мониторинга должны быть реализованы следующие функции модулей и разделов подсистемы:

* раздел предоставления результатов кластеризации поисковых запросов с учетом поведения интернет-посетителя:
	+ функция получения данных о кластеризации поисковых запросов;
	+ функция обработки и визуализации результатов кластеризации поисковых запросов;
* раздел предоставления результатов сегментирования интернет-посетителей:
	+ функция получения данных о сегментировании интернет-посетителей;
	+ функция обработки и визуализации результатов сегментирования интернет-посетителей;
* раздел предоставления статистики по событиям, получаемым из внешних систем-источников в подсистему сбора данных:
	+ функция получения статистических данных по событиям, получаемым из внешних систем-источников;
	+ функция обработки и визуализации статистики по событиям;
* функционал конструирования собственных (кастомных) статистических отчетов:
	+ функция настройки кастомного отчета по набору атрибутов на основании предрасчитанных срезов данных в интерактивном режиме;
	+ функция сохранения настроек отчета и дополнительных опций;
* модуль управления интерфейсом:
	+ функция создания, редактирования, удаления ситуационных панелей;
	+ функция наполнения ситуационных панелей информационными блоками;
* модуль выгрузки статистических данных:
	+ функция настройки выгружаемого статистического отчета;
	+ функция выгрузки отчета с использованием не менее 2 протоколов передачи данных.

В рамках данной подсистемы должна быть реализована витрина данных в оптимальном для потребителей виде.

Подсистема должна обеспечивать графический пользовательский интерфейс для формирования отчетности. В подсистеме должна быть предоставлена возможность мониторинга показателей интернет-аналитики на основании графиков и отчетов, сформированных на базе агрегированных параметров подсистемы обработки данных.

В рамках подсистемы статистики и мониторинга должна быть реализована возможность построения статистических отчетов с возможностью задания следующих параметров:

* дата начала;
* дата окончания;
* агрегированные показатели;
* срезы данных;
* адрес сайта;
* организация (орган исполнительной власти, к которому относится интернет ресурс);
* категория, тематический раздел ресурса;
* поведенческие сегменты посетителей интернет-ресурсов, рассчитанных с использованием модуля сегментирования интернет-посетителя с учетом прогнозных значений модернизируемой подсистемы обработки данных.
	+ - 1. **Функционал «Предоставление результатов кластеризации поисковых запросов с учетом поведения интернет-посетителя»**

В рамках раздела предоставления результатов кластеризации поисковых запросов должен быть реализован функционал обработки данных поисковых запросов с последующим формированием отчетов, визуализирующих цепочки действий интернет-посетителей до и после обращения к поисковому сервису и отправки поискового запроса. Отчеты должны предоставлять информацию как по отдельным поисковым запросам, так и по их группам, объединенным по тематикам. В рамках отчетов должна быть реализована возможность просмотра наиболее популярных цепочек действий до и после совершения целевого действия и цепочек действий в рамках сформированных поведенческих сегментов всех интернет-посетителей.

Раздел кластеризации поисковых запросов должен предоставлять необходимую информацию для реализации сценария «Построение цепочек выполнения целевого действия пользователем на интернет ресурсах» в части анализа поисковых запросов интернет-посетителей.

* + - 1. **Функционал «Предоставление результатов сегментирования интернет-посетителей»**

Раздел, предоставляющий информацию о поведенческих сегментах посетителей интернет-ресурсов, должен включать в себя функционал обработки данных с последюущим формированием как типовых отчетов для всех интернет-ресурсов, так и индивидуальных, построенные на основании выявленных поведенческих сегментов интернет пользователей рассматриваемого ресурса.

* + - 1. **Функционал «Предоставление статистики по событиям, получаемым из внешних систем-источников в подсистему сбора данных»**

В рамках раздела предоставления статистики по событиям, получаемым из внешних систем-источников в подсистему сбора данных, должен быть реализован функционал обработки данных с последующим формированием отчетов учета основных статистических показателей – таких, как:

* распределение количества событий во временном периоде;
* количество уникальных посетителей, совершивших указанное событие;
* среднее количество событий в день по типу события.

Предоставляемые статистические показатели должны быть достаточными для реализации сценария «Представление статистики интернет события». Полный перечень интернет событий, по которым необходимо рассчитывать статистические показатели, и перечень статистических показателей должны быть определены на этапе проектирования и приведены в документе «Пояснительная записка». Полный перечень требований и параметров модернизируемой подсистемы статистики и мониторинга должен быть определен Подрядчиком и согласован с Заказчиком на этапе проектирования и приведен в документе «Пояснительная записка».

* + - 1. **Функционал «Конструирование собственных (кастомных) статистических отчетов»**

Функционал «Конструирование статистистических отчетов» позволяет пользователям системы формировать собственные (кастомные) статистические отчеты на основании данных,собранных системой, по предоставленному набору допустимых атрибутов и готовых временных срезов.

Кастомные отчеты доступны в списке кастомных отчетов только тому пользователю, который их создал.

Администратор системы с соответствующими правами может создавать кастомные отчеты доступные всем пользователям.

При формировании кастомного статистического отчета конструктор предлагает:

* выбор наборов данных, доступные данному пользователю, из перечня подготовленных и рассчитанных агрегатов;
* выбор временного промежутка для построение отчета из перечня подготовленных и рассчитанных временных срезов;
* выбор графического представления отчета из предлагаемого перечня отчетов, доступных для выбранных данных;
* дополнительный набор опций: «разовое формирование отчета», «регулярное создание отчета», «формирование файла для выгрузки без формирование графического представления»;
* название кастомного отчета (если на задано, формируется автоматически на основании даты/времени/имени пользователя).

При формировании кастомных отчетов возможны временные задержки в зависимости от объема данных. В случае задержек более 30 секунд должен быть предусмотрен механизм отправки оповещения пользователю о том, что его отчет готов.

Создание кастомного отчета не предполагает создание произвольного поведенческого сегмента, отсутствующего в задаваемых фильтрах Системы.

* + - 1. **Функционал модуля управления интерфейсом**

Модуль управления интерфейсом должен поддерживать следующие функции:

* Создание ситуационных панелей;
* Управление наполнением ситуационной панели данными.

«Ситуационная панель» должна представлять из себя отдельный раздел в подсистеме статистики и мониторинга, данные которого формируются выборочно из всего набора данных доступных в системе.

«Ситуационная панель по умолчанию» - это первая страница СТАТС, доступная сразу после входа в систему и отображающая все основные статистические данные, интересные большинству пользователей.

Доступ к ситуационным панелям осуществляется из специального подраздела со списком всех доступных панелей.

При реализации функции «создание ситуационных панелей» должны быть доступны следующие операции:

* создание, редактирование, удаление ситуационной панели;
* управление названием ситуационной панели;
* управление порядковым номером ситуационной панели в списке.

Управление наполнением ситуационной панели должно осуществляться с помощью графического интерфейса с гибкими возможностями по формату, объему и набору данных.

Интерфейс наполнения данными должен реализовывать следующий функционал:

* добавление, редактирование, удаление информационного блока;
* выбор статистического отчета и его представления в информационном блоке;
* изменение размера, положения информационного блока;
* создание, редактирование заголовков и подзаголовков информационных блоков;
* управление дополнительными информационными блоками, которые могут содержать: картинку, заголовок, текст.
	+ - 1. **Функционал модуля выгрузки статистических данных**

У пользователей системы должна быть возможность выгрузки любого стандартного статистического, либо собственного (кастомного) отчета для дальнейшей работы.

Подсистема выгрузки должна позволять:

* при работе с отчетами выгрузить отчет именно в тех настройках, которые заданы пользователем (с тем же набором дат, за тот же промежуток времени, что и в веб-представлении);
* выбрать формат выгрузки отчета (csv, xls, pdf);
* настроить отправку отчета на электронный адрес пользователя (адрес, указанный в системе при заведении пользователей).

Помимо выгрузки отчетов должен быть реализован функционал формирования регулярных рассылок со статистическими данными:

* регулярность формирования рассылки (разово, ежедневно, еженедельно, ежемесячно);
* набор стандартных и собственных (кастомных) отчетов для включения в рассылку.
	+ 1. **Требования к функциям разрабатываемой подсистемы предоставления данных**

В рамках выполняемых работ по развитию ИС СТАТС должна быть разработана подсистема предоставления данных. Подсистема предоставления данных должна обеспечивать передачу внешним системам-потребителям агрегированной информации по переходам пользователей по внутренним и внешним ссылкам информационных ресурсов, а так же профилей интернет-посетителей с использованием ключа cookie.

Передача должна осуществляться по стандартным сетевым протоколам.

В рамках данной подсистемы должны быть разработаны:

* механизмы предоставления агрегированной статистики внешним системам-потребителям переходов по внешним ссылкам;
* механизмы предоставления агрегированной статистики внешним системам потребителям переходов по внутренним ссылкам;
* механизмы предоставления профилей внешним системам-потребителям по ключу cookie интернет-посетителя.

В рамках разрабатываемых механизмов подсистемы предоставления данных должны быть реализованы следующие функции:

* механизм предоставления агрегированной статистики внешним системам-потребителям переходов по внешним ссылкам:
	+ функция трансляции не менее, чем 2 внешним системам-потребителям данных о переходах по внешним ссылкам посредством не менее 8 протоколов и форматов передачи данных;
	+ функция настройки регулярности передачи данных внешним системам-потребителям;
* механизм предоставления агрегированной статистики внешним системам-потребителям переходов по внутренним ссылкам:
	+ функция трансляции не менее, чем 1 внешней системе-потребителю данных о переходах по внутренним ссылкам посредством не менее 8 протоколов и форматов передачи данных;
	+ функция настройки регулярности передачи данных внешним системам-потребителям;
* механизм предоставления профилей внешним системам-потребителям по ключу cookie интернет-посетителя:
	+ функция трансляции не менее, чем 2 внешним системам-потребителям данных о профилях интернет-посетителей посредством не менее 8 протоколов и форматов передачи данных;
	+ функция настройки регулярности передачи данных внешним системам-потребителям.

Подсистема должна обеспечивать передачу информации внешним системам-потребителям при нагрузке не менее 4 млн. уникальных и 20 млн. общих посещений пользователями в месяц.

* + - 1. **Требования к функционалу механизмов предоставления агрегированной статистики внешним системам-потребителям переходов по внешним ссылкам**

Механизмы предоставления агрегированной статистики внешним системам-потребителям по переходам пользователей по внешним ссылкам должны обеспечивать агрегацию и передачу обработанных данных в пакетном режиме, в форме JSON-запросов/ответов.

* + - 1. **Требования к функционалу механизмов предоставления агрегированной статистики внешним системам потребителям переходов по внутренним ссылкам**

Механизмы предоставления агрегированной статистики внешним системам-потребителям по переходам пользователей по внутренним ссылкам должны обеспечивать агрегацию и передачу обработанных данных в пакетном режиме, в форме JSON-запросов/ответов.

* + - 1. **Требования к функционалу механизмов предоставления профилей внешним системам-потребителям по ключу cookie интернет-посетителя**

Механизмы предоставления профилей пользователей внешним системам-потребителям по ключу cookie интернет-посетителя должны обеспечивать агрегацию и передачу обработанных данных, как в пакетном, так и on-line режиме, в форме JSON-запросов/ответов.

* + 1. **Требования к подсистеме обеспечения информационной безопасности**

В рамках выполняемых работ по развитию ИС СТАТС должна быть реализована подсистема обеспечения информационной безопасности. Подсистема обеспечения информационной безопасности ППО ИС СТАТС является средством защиты конфиденциальной информации и должна удовлетворять следующим требованиям.

В части обеспечения механизмов идентификации и аутентификации субъектов доступа и объектов доступа должны быть реализованы следующие требования:

* аутентификация пользователя должна осуществляться с использованием паролей;
* должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования не более 90 календарных дней;
* должны быть установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей в информационной системе:
* установление характеристик пароля:

а) задание минимальной сложности пароля с определяемыми ниже требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

б) задание минимального количества измененных символов при создании новых паролей;

в) задание максимального времени действия пароля;

г) задание минимального времени действия пароля;

д) запрет на использование пользователями определенного числа последних использованных паролей при создании новых паролей;

* назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);
* обновление аутентификационной информации (замена средств аутентификации) с установленной периодичностью;

Характеристики паролей должны быть следующими:

* длина пароля не менее шести символов, алфавит пароля не менее 60 символов;
* максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки - 3 попытки;
* блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации на время 5 минут;
* смена паролей не более чем через 120 календарных дней;
* должно быть установлено ограничение на продолжительность сессии по времени с последующим переходом на страницу авторизации либо определено время простоя с последующей обязательной авторизацией пользователя.

В части управления доступом субъектов доступа к объектам доступа должно быть реализовано:

* разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
* должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями). Данное разделение должно быть описано в виде матрицы ролей и полномочий;
* принцип назначения минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы должен быть документирован;
* должно быть установлено ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за установленный период времени.

В части регистраций событий безопасности должны быть реализованы следующие требования:

* все события безопасности должны быть доступны для просмотра из графического интерфейса администратора, наделенного необходимыми полномочиями;
* мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации;
* защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий;
* доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только администратору, наделенному необходимыми полномочиями.

В части контроля (анализа) защищенности должны быть реализованы следующие требования:

* контроль правил генерации и смены паролей пользователей;
* контроль заведения и удаления учетных записей пользователей;
* контроль реализации правил разграничения доступом;
* контроль реализации полномочий пользователей.
	1. **Требования к видам обеспечения**
		1. **Требования к математическому обеспечению**

Разрабатываемое программное обеспечение должно реализовывать типовые алгоритмы анализа данных.

* + 1. **Требования к информационному обеспечению**
			1. **Требования к составу, структуре и способам организации данных в системе**

Информационное обеспечение представляет собой совокупность всех необходимых для функционирования системы данных и систем обеспечения. В состав информационного обеспечения входят:

* нормативно-справочная информация;
* информационные объекты;
* входные и выходные данные;
* структура управления базами данных.

Состав, структура и способы организации данных на разрабатываемые/модернизированные подсистемы должны быть определены на этапе проектирования и приведены в документе «Пояснительная записка».

* + - 1. **Требования к организации ввода данных в Систему**

Система должна обеспечивать однократный ввод данных вне зависимости от того, в каких информационных массивах или базах данных они будут храниться и какими функциональными подсистемами использоваться.

Ввод данных осуществляется путем загрузки данных существующих электронных хранилищ данных, по разработанной исполнителем методике. Ввод данных осуществляется с обязательной последующей проверкой и сопоставлением введенных данных, подтверждением их корректности и отсутствия неправильных, дублетных и неполных записей. После проверки данные меняют статус на проверенные и предоставляются для использования.

Начальная загрузка данных производится в соответствии с мероприятиями по вводу Системы в эксплуатацию. В дальнейшем производится синхронизация данных имеющихся в Системе и данных во внешних хранилищах (если выявлена такая необходимость на этапе проектирования).

* + - 1. **Требования к информационному обмену между компонентами Системы**

Информационный обмен между компонентами Системы должен осуществляться без вмешательства пользователя и без повторного ручного ввода информации.

Информационный обмен между компонентами Системы и клиентскими приложениями должен осуществляться по локальной сети и по сети Интернет.

* + - 1. **Требования по использованию общегородских и других зарегистрированных классификаторов, унифицированных документов и др.**

В рамках выполнения работ по развитию ИС СТАТС в случае такой потребности необходимо использовать общегородские справочники и классификаторы, зарегистрированные в системе «Единая система ведения и управления реестрами, регистрами, справочниками и классификаторами» (АС УР).

В части межведомственного взаимодействия, при передаче данных, входящих в группу НСИ (в случае их централизованного ведения и использования), должны передаваться только коды справочных данных, но не смысловые значения справочников, что обеспечит сокращение объема данных, передаваемых по сетям связи.

Состав и назначение общегородских и других зарегистрированных классификаторов, унифицированных документов, должны быть определены на этапе проектирования и приведены в документе «Пояснительная записка».

* + - 1. **Назначение справочников и классификаторов и информации, хранящейся в них**

Состав и назначение справочников, классификаторов и информации, хранящейся в них, должны быть определены на этапе проектирования и приведены в документе «Пояснительная записка».

* + - 1. **Объем и состав информации, получаемой из классификаторов**

Объем и состав информации, получаемой из классификаторов, должны быть определены на этапе проектирования.

* + - 1. **Требования к структуре процесса сбора, обработки, передачи данных в системе и представлению данных**

Состав данных должен быть достаточным для выполнения всех функций Системы и отвечать требованиям полноты, достоверности, однозначной идентификации, непротиворечивости и необходимой точности представления.

При взаимодействии информационных систем и ресурсов Система должна обеспечивать предоставление данных в соответствии с требованиями, описанными в Приложении 1 «Навигатор атрибутов» к Стандарту ведения данных, утвержденному распоряжением Департамента информационных технологий города Москвы от 01.11.2016 № 64-16-549/16 «Об утверждении Единых требований к стандарту ведения данных» (далее - Стандарт). Данные требования относятся к тем информационным объектам, которые описаны в Стандарте и создаются, изменяются или удаляются в системе (далее – информационные объекты).

Контроль соответствия указанных данных требованиям Стандарта в части форматов и используемой нормативно-справочной информации осуществляет Оператор данных. В случае выявления отклонений от требований и выявления проблем с качеством этих данных – отклонения должны исправляться в системе в течение 5 рабочих дней.

С целью контроля соответствия обрабатываемых в системе данных Стандарту должен быть реализован механизм предоставления Оператору данных наборов атрибутов, описанных в Приложении 1 «Навигатор атрибутов» к Стандарту, без привязки к экземплярам сущностей, хранящихся и обрабатываемых в системе. Предоставление указанных данных Оператору данных должно быть обеспечено на регулярной основе, в соответствии с форматом, заданным в Стандарте, и должно предусматривать инкрементальный режим предоставления данных и режим предоставления полного набора данных по информационным объектам.

Инкрементальное предоставление данных должно осуществляться не реже 1 раза в месяц.

Полное предоставление данных должно осуществляться не реже 1 раза в год.

В системе необходимо предусмотреть режим предоставления данных «по запросу» вне рамок вышеописанного расписания. Предоставление данных «по запросу» осуществляется не чаще 10 календарных дней.

* + - 1. **Требования к защите данных от разрушений при авариях и сбоях в электропитании Системы**

В Системе должна быть обеспечена защита данных от утраты или нарушения целостности в следующих случаях:

* при сбоях в электропитании серверного оборудования;
* при авариях, приведших к невозможности восстановления данных— использованием процедур резервного копирования Системы и хранения резервных копий.

Дополнительные требования к защите данных от разрушений при авариях и сбоях в электропитании Системы не предъявляются.

* + - 1. **Требования к контролю, хранению, обновлению и восстановлению данных**

Система должна обеспечивать первичный контроль вводимых данных на соответствие формальным правилам: проверка типов, размерности, допустимости значений.

Система должна сохранять имеющиеся данные, достаточные для полного восстановления работоспособности, в удаленном хранилище в сертифицированном центре обработки данных, находящемся на территории России.

* + - 1. **Требования к процедуре придания юридической силы документам, продуцируемым техническими средствами АС**

Придание документам, продуцируемым Системой, юридической силы должно производиться в соответствии с рекомендациями ГОСТ 6.10.4-84. В случае выявления на этапе проектирования целесообразности использования ЭП для придания юридической силы документам, продуцируемым системой, в системе должны быть предусмотрены соответствующие механизмы.

* + 1. **Требования к лингвистическому обеспечению**

Все пользовательские выходные формы, инструкции по работе, вся документация должны быть выполнены на русском языке. Исключения могут составлять системные сообщения, не подлежащие русификации.

При разработке программных решений должно быть предусмотрено использование языков программирования высокого уровня.

* + 1. **Требования к программному обеспечению**

Используемые при разработке языки высокого уровня должны обеспечивать решение всех задач по реализации функций Системы.

Прикладное программное обеспечение должно отвечать следующим требованиям:

* работа программного обеспечения должна быть основана на использовании трехзвенной технологии «сервер БД – сервер приложений – «тонкий» клиент»;
* клиентская часть Системы должна функционировать на мультиплатформенной основе с использованием наиболее распространённых интернет браузеров (Chrome, Safari, Opera, Firefox,YandexBrowser);
* серверная часть должна функционировать на основе систем типа UNIX/Linux/FreeBSD;
* управление базами данных Системы должно осуществляться с использованием СУБД Hive, HBase, Solr или аналогичных по своим характеристикам СУБД.

В качестве инструментов, обеспечивающих сбор данных, должен использоваться распределённый брокер сообщений (например, Kafka) и сервис управления потоками данных (например,Flume).

Подрядчик при проектировании Системы должен использовать:

* кроссплатформенные языки программирования;
* визуальные средства проектирования;
* другие языки высокого уровня по выбору Подрядчика.
	+ 1. **Требования к техническому обеспечению**

Требования к техническому обеспечению должны быть сформированы на этапе проектирования и приведены в документе «Пояснительная записка».

* + 1. **Требования к метрологическому обеспечению**

Требования к метрологическому обеспечению не предъявляется.

* + 1. **Требования к телекоммуникационному обеспечению системы**
			1. **Необходимые линии и каналы связи**

Связь между компонентами Системы должна осуществляться с использованием проводных и беспроводных каналов связи.

* + - 1. **Среда передачи**

Связь между компонентами Системы должна осуществляться с использованием локальной сети и Интернет.

* + - 1. **Технические параметры каналов связи**

Специальные требования не предъявляются.

* + - 1. **Пропускная способность, интерфейсы, топология и т.п.**

Пропускная способность каналов связи должна быть не ниже 10 Мбит/с для пользовательских соединений и не ниже 100 Мбит/с для рабочих

* + - 1. **Необходимость организации новых каналов связи либо возможность использования существующей телекоммуникационной инфраструктуры Правительства Москвы**

Требования к организации новых каналов не предъявляются.

* + - 1. **Требования к другим видам обеспечения**

Требования к другим видам обеспечения не предъявляются.

**5 Состав и содержание работ по созданию системы**

Этапы выполнения работ по развитию информационной системы мониторинга и анализа интернет активности пользователей представлены в таблице 11.

Таблица 11 - Этапы проведения работ по развитию Системы

| **№ этапа** | **Наименование и содержание выполняемых работ** | **Сроки выполнения** | **Отчетная документация** | **Стоимость работ, % от Цены Контракта** |
| --- | --- | --- | --- | --- |
| **Начало** | **Окончание** |
| **1.** | **Этап 1. Проектирование** | **С даты заключения Контракта** | **60 календарных дней со дня начала Этапа 1** |  | 17,00% |
| 1.1 | Техническое проектирование |  |  | * Описание архитектуры Системы
* Пояснительная записка
* Аналитическое обоснование необходимости создания системы защиты информации ИС
* Проект акта классификации ИС по требованиям безопасности информации
* Частное техническое задание на создание системы защиты информации
* Проект модели угроз информационной безопасности
* Акт определения области проведения аттестации ИС
* Акт сдачи-приемки выполненных работ по этапу
* Акт приема передачи отчетной документации
* Ведомость машинных носителей информации
 |  |
| 1.2 | Формирование требований к защите информации |  |  |
| **2.** | **Этап 2. Разработка ПО Системы** | **Следующий календарный день со дня окончания Этапа 1** | **200 календарных дней со дня начала Этапа 2** |  | 59,70% |
| 2.1 | Рабочее проектирование / развитие системы в составе:* модернизируемая подсистема сбора данных;
* модернизируемая подсистема обработки данных;
* модернизируемая подсистема хранения данных;
* модернизируемая подсистема статистики и мониторинга;
* разрабатываемая подсистема предоставления данных;
* разрабатываемая подсистема обеспечения информационной безопасности.
 |  |  | * Программное обеспечение Системы
* Программа и методика предварительных испытаний (с приложением Проекта протокола предварительных испытаний и Проекта акта приемки в опытную эксплуатацию)
* Руководство администратора
* Руководство пользователя
* План-программа подготовки персонала (с приложением формы Отчета о подготовке персонала)
* Описание программного обеспечения
* Описание комплекса технических средств
* Регламент технического обслуживания системы
* Акт выполнения пуско-наладочных работ
* Ведомость машинных носителей информации
* Акт сдачи-приемки выполненных работ по этапу
* Акт приема-передачи отчетной документации
 |  |
| **3.** | **Этап 3. Проведение испытаний** | **Следующий календарный день со дня окончания Этапа 2** | **40 календарных дней со дня начала Этапа 3** |  | 10,00% |
| 3.1 | Проведение предварительных испытаний |  |  | * Протокол предварительных испытаний
* Акт приемки в опытную эксплуатацию
* Программа и методика опытной эксплуатации (с приложением формы Отчета о проведении опытной эксплуатации и формы Журнала опытной эксплуатации)
 |  |
| 3.2 | Подготовка персонала Системы |  |  | * Отчет о подготовке персонала Системы с приложением Протокола подготовки персонала Системы
 |  |
| 3.3 | Проведение опытной эксплуатации |  |  | * Отчет о проведении опытной эксплуатации с приложением Журнала опытной эксплуатации
* Актуализированное описание архитектуры системы
* Акт о завершении опытной эксплуатации и допуске системы к приемочным испытаниям
* Программа и методика приемочных испытаний
* Проект протокола проведения приемочных испытаний
 |  |
| 3.4 | Проведение приемочных испытаний |  |  | * Актуализированное программное обеспечение Системы
* Протокол проведения приемочных испытаний
* Акт о готовности системы к промышленной эксплуатации
* Акт сдачи-приемки выполненных работ по этапу
* Акт приема-передачи отчетной документации
* Ведомость машинных носителей информации
 |  |
| **4** | **Этап 4. Создание системы защиты информации ИС СТАТС** | **Следующий календарный день со дня окончания Этапа 2** | **30 календарных дней со дня начала Этапа 4** | * Технический проект СЗИ ИС в составе:
* Пояснительная записка к техническому проекту СЗИ;
* Ведомость технического проекта
* Описание технологического процесса обработки информации;
* Схема размещения комплекса технических средств системы защиты информации;
* Схема структурная комплекса технических средств;
* Схема функциональной структуры;
* Описание настроек средств защиты информации;
* Ведомость покупных изделий системы защиты информации;
* Руководство администратора
* Акт сдачи-приемки выполненных работ по этапу
* Акт приема-передачи отчетной документации
* Ведомость машинных носителей информации
 | 7,30% |
| **5.** | **Этап 5. Разработка организационно-распорядительной документации на СЗИ ИС СТАТС** | **10-й календарный день со дня начала Этапа 4** | **30 календарных дней со дня начала Этапа 5** | * Проект Регламента управления (администрирования) СЗИ
* Проект Регламента выявления инцидентов и реагирования на них
* Проект Регламента управления конфигурацией ИС и ее СЗИ
* Проект Регламента обеспечения защиты информации при выводе ИС из эксплуатации или после принятия решения об окончании обработки информации
* Акт сдачи-приемки выполненных работ по этапу
* Акт приема-передачи отчетной документации
* Ведомость машинных носителей информации.
 | 1,00% |
| **6** | **Этап 6. Подготовка к сертификации и сертификация ППО ИС СТАТС по требованиям безопасности информации** | **Следующий календарный день со дня окончания Этапа 3** | **270 календарных дней со дня начала Этапа 6** | * Копия сертификата соответствия в системе сертификации средств защиты информации ФСТЭК России
* Технические условия
* Руководство администратора по комплексу средств защиты
* Акт сдачи-приемки выполненных работ по этапу
* Акт приема-передачи отчетной документации
* Ведомость машинных носителей информации
 | 2,30% |
| **7.** | **Этап 7. Аттестация ИС СТАТС по требованиям безопасности информации** | **Следующий календарный день со дня окончания Этапа 6** | **50 календарных дней со дня начала Этапа 7** | * Программа и методика аттестационных испытаний
* Протокол аттестационных испытаний
* Протокол анализа уязвимостей информационной системы.
* Заключение по результатам аттестационных испытаний
* Аттестат соответствия требованиям безопасности.
* Акт сдачи-приемки выполненных работ по этапу
* Акт приема-передачи отчетной документации
* Ведомость машинных носителей информации
 | 2,70% |

**6 Порядок контроля и приемки системы**

**6.1 Виды, состав, объем и методы испытаний системы и ее составных частей**

Должны быть проведены следующие виды испытаний:

* предварительные испытания;
* опытная эксплуатация;
* приемочные испытания.

Отдельные виды испытаний – предварительные испытания, опытная эксплуатация, приемочные испытания – проводятся в сроки, установленные Календарным планом.

Объем и методы предварительных и приемочных испытаний определяются соответствующей «Программой и методикой испытаний».

* 1. **Сведения о гарантийном обслуживании Системы**

Гарантийный срок на выполняемые по настоящему Контракту работы составляет 12 (двенадцать) месяцев с даты подписания сторонами Акта об исполнении обязательств.

Подрядчик должен гарантировать, что разработанное программное обеспечение Системы будет функционировать в соответствии со своим назначением не менее 1 (одного) года. При этом возможны незначительные отклонения его технических и потребительских характеристик, а также отдельные ошибки, не создающие препятствий для получения положительных результатов от эксплуатации Системы.

Подрядчик не гарантирует отсутствие недостатков или сбоев в процессе работы, возникающих по причине несоответствия оборудования или установленного на рабочем месте программного обеспечения конечного пользователя требованиям, предъявляемым к характеристикам клиентских мест (см. пункт «Требования к программному обеспечению»).

Подрядчик обязуется обеспечить консультирование специалистов эксплуатирующей организации в течение всего периода гарантийного обслуживания.

Подрядчик гарантирует обеспечение соответствия сертифицированного ППО Системы требованиям по безопасности информации, а также устранение недостатков и дефектов сертифицированного ППО, в том числе устранение уязвимостей и недекларированных возможностей сертифицированного ППО, информирование Заказчика об обновлении сертифицированного ППО, доведение до Заказчика обновлений сертифицированного ППО, а также изменений в эксплуатационную документацию (далее – техническая поддержка сертифицированного ППО). Обеспечение данной технической поддержки сертифицированного ППО должно гарантироваться на протяжении всего срока действия сертификата соответствия на ППО.

* 1. **Порядок выполнения доработок и устранения допущенных Подрядчиком ошибок, которые выявлены в процессе испытаний и в период гарантийного обслуживания**

Недостатки и ошибки в реализации Системы, выявленные в ходе проведения испытаний, должны быть устранены Подрядчиком в рамках выполнения работ по Государственному контракту. Порядок устранения замечаний и реализации рекомендаций комиссии должен быть определен в документах «Программа и методика испытаний» и «Программа и методика опытной эксплуатации (с приложением формы Отчета о проведении опытной эксплуатации и формы Журнала опытной эксплуатации)». Сроки устранения замечаний и рекомендаций, данных приемочной комиссией в ходе испытаний, определяются в «Акте о готовности Системы к промышленной эксплуатации».

Недостатки и ошибки в реализации Системы, выявленные в период гарантийного обслуживания, устраняются Подрядчиком в рамках очередного обновления Системы или в рамках внеочередного экстренного обновления в случае, если обнаруженные ошибки препятствуют или ограничивают эксплуатацию Системы в штатном режиме.

Подрядчиком должны быть внесены соответствующие актуализирующие исправления в техническую и рабочую документацию, связанные с устранением замечаний к работе Системы, и предъявлены Заказчику на приемо-сдаточные испытания или до завершения срока гарантийного обслуживания для замечаний опытной эксплуатации или гарантийного обслуживания соответственно.

* 1. **Статус приемочной комиссии**

Статус приемочной комиссии: межведомственная.

* 1. **Сведения об обслуживании Системы**

Эксплуатация Системы производится в соответствии с Положением об эксплуатации автоматизированных информационных систем и ресурсов города Москвы[[1]](#footnote-1).

Состав работ по эксплуатации Системы, а также их периодичность и требования к составу и квалификации обслуживающего персонала, определяются в эксплуатационной документации на Систему. При этом требования к эксплуатации компьютерного оборудования, системного и прикладного программного обеспечения, входящего в состав Системы, указываемые в эксплуатационной документации, должны соответствовать требованиям к эксплуатации соответствующего оборудования и программного обеспечения, изложенным в документации, поставляемой вместе с данным оборудованием и программным обеспечением при его приобретении.

Системное и прикладное сопровождение, техническое сопровождение аппаратного обеспечения, системное сопровождение средств защиты информации, организация подготовки персонала системы и другие работы производятся на основании Государственных контрактов на выполнение соответствующих работ.

**7 Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу Системы в действие**

* 1. **Развертывание и конфигурирование**

Система должна быть обновлена Подрядчиком. Должен быть установлен передаваемый на машинных носителях дистрибутив и предварительная конфигурация.

Дальнейшее конфигурирование должно быть выполнено Подрядчиком (сервисным оператором) в соответствии с документом «Руководство администратора».

В случае необходимости Подрядчиком должны быть установлены обновления, выпущенные по итогам испытаний, если эти обновления не включены в состав Дистрибутива программного обеспечения Системы.

* 1. **Приведение поступающей в систему информации к виду, пригодному для обработки с помощью ЭВМ**

Для приведения поступающей в Систему информации к виду, пригодному для обработки с помощью ЭВМ, должны быть проведены системно-аналитические мероприятия по формализации, категоризации, описанию атрибутивного состава документов и форм аналитического и статистического учета.

Должны быть описаны и утверждены вновь вводимые справочники и классификаторы.

В случае необходимости Подрядчик должен обеспечить ручной ввод исходных данных в систему в случае отсутствия этих данных в электронном виде на машинных носителях.

* 1. **Изменения, которые необходимо осуществить в объекте автоматизации**
		1. **Создание условий функционирования объекта автоматизации, при которых гарантируется соответствие создаваемой системы требованиям**

Подрядчик должен сформировать описание системы в установленном формате и предоставить заявки на выделение ресурсов.

* + 1. **Создание необходимых для функционирования системы подразделений и служб**

Дополнительный перечень мероприятий, который необходимо осуществить в объекте автоматизации выявляется и уточняется на стадии «Рабочее проектирование».

* + 1. **Сроки и порядок комплектования штатов и обучения персонала системы**

Комплектование штатов и подразделений, необходимых для функционирования Системы, а также подготовка обслуживающего персонала и пользователей Системы должны быть завершены до начала промышленной эксплуатации Системы.

Подготовка обслуживающего персонала и пользователей Системы должна проводиться Подрядчиком в соответствии с документом «План-программа подготовки персонала Системы». По завершении подготовки должен быть оформлен отчет о подготовке персонала Системы.

1. **Требования к документированию**

Техническая и эксплуатационная документация на Систему (далее – документы на Систему) должна быть разработана в составе, указанном в разделе 5 ТЗ, и должна удовлетворять требованиям комплекса стандартов и руководящих документов на автоматизированные системы:

* + ГОСТ 34.003-90 – в части терминологии;
	+ ГОСТ 34.201-89, ГОСТ 19.101-77-82, 19.103-77 – в части наименования и обозначения документов;
	+ ГОСТ 34.601-90 – в части определения стадий и этапов работ;
	+ ГОСТ 34.602-89 – в части состава, содержания и правил оформления документов «Техническое задание»;
	+ ГОСТ 34.603-92 – в части определения видов испытаний;
	+ РД 50-34.698-90 – в части структуры и содержания документов.

Документы на Систему должны оформляться в соответствии с требованиями ГОСТ 2.105-95 на листах формата А4 по ГОСТ 2.301-68 без рамки, основной надписи и дополнительных граф к ней. Допускается для размещения рисунков и таблиц использование листов формата А3 с подшивкой по короткой стороне листа. Документы объемом более 25 листов должны содержать информационную часть, состоящую из аннотации и содержания.

Комплект эксплуатационной документации на Систему должен содержать сведения, достаточные для эксплуатации Системы в соответствии с Положением об эксплуатации автоматизированных информационных систем и ресурсов города Москвы[[2]](#footnote-2), а также:

* в части ПО Системы должен содержать исчерпывающее описание ПО в соответствии с классом стандартов ГОСТ 19, обеспечивающее его установку, настройку, эксплуатацию и сопровождение;
* в части комплекса технических средств (КТС) Системы должен содержать исчерпывающее описание КТС в соответствии с классом стандартов ГОСТ 34, обеспечивающее развертывание ПО Системы, а также сопровождение КТС ИС.

Формальное полное соответствие документов на Систему требованиям РД 50-34.698-90 и классам стандартов ГОСТ по составу и структуре разделов не требуется. При этом должно быть достигнуто адекватное описание всех видов обеспечения АС, достаточное для подготовки персонала, развертывания, эксплуатации и сопровождения АС по всем позициям, определяемым РД 50-34.698-90 и классами стандартов ГОСТ 19 для отдельных документов.

Документам на Систему должны в обязательном порядке присваиваться уникальные децимальные номера в соответствии с порядком, установленном в ГОСТ 34.201-89.

Дополнительные требования к составу, структуре и содержанию документов (кроме приведенных выше и отличные от содержащихся в указанных в данном разделе ГОСТ) должны быть подготовлены Заказчиком и переданы Подрядчику на этапе проектирования (раздел 5 ТЗ). Дополнительные требования оформляются протоколом или дополнением к данному ТЗ. Дополнение или указанный протокол являются неотъемлемой частью ТЗ и должны быть утверждены в установленном порядке.

1. **Источники развития Системы**

В настоящем документе использованы следующие нормативные документы:

* 1. **Нормативно-правовые акты**
* Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
* Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Федеральный закон от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд;
* Государственная программа города Москвы «Информационный город», утвержденная Постановлением Правительства Москвы от 9 августа 2011 г.
№ 349-ПП;
* Постановление Правительства Москвы от 21.12.2011 № 604-ПП «Об утверждении положения об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие органов исполнительной власти города Москвы и организаций при предоставлении государственных услуг и исполнении государственных функций в городе Москве»;
* Распоряжение Департамента информационных технологий города Москвы от 01.11.2016 № 64-16-549/16 «Об утверждении Единых требований к стандарту ведения данных»;
* Постановление Правительства Москвы от 15.12.2015 № 871-ПП «О развитии единого интернет-пространства Правительства Москвы».
	1. **Нормативно-технические документы**
* Информационная технология. Комплекс стандартов на автоматизированные системы (класс стандартов ГОСТ 34);
* РД 50-34.698-90. Методические указания. Информационная технология. Автоматизированные системы. Требования к содержанию документов;
* ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортировка, хранение»;
* ГОСТ 28806-90. Качество программных средств. Термины и определения;
* ГОСТ 16504-81. Система государственных испытаний продукции. Испытания и контроль качества продукции. Термины и определения;
* ГОСТ Р ИСО/МЭК ТО 12182-2002. Информационная технология. Классификация программных средств;
* ГОСТ Р ИСО/МЭК 12207:1999. Процессы жизненного цикла программных средств;
* ГОСТ Р ИСО/МЭК ТО 15271-2002. Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207;
* ГОСТ Р ИСО/МЭК 9126:93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению;
* ГОСТ Р ИСО/МЭК 15026:1998. Информационная технология. Уровни целостности систем и программных средств;
* ГОСТ Р ИСО/МЭК 14764:2002. Информационная технология. Сопровождение;
* ГОСТ Р ИСО/МЭК ТО 9294:93. Информационная технология. Руководство по управлению документированием программного обеспечения;
* ГОСТ Р ИСО/МЭК 15910-2002. Информационная технология. Процесс создания документации пользователя программного средства;
* ISO 14756: 1999. ИТ. Измерение и оценивание производительности программных средств компьютерных вычислительных систем;
* ГОСТ 2.051-2006. Единая система конструкторской документации. Электронные документы. Общие положения;
* ГОСТ 2.105-95 Единая система конструкторской документации. Общие требования к текстовым документам;
* ГОСТ 2.301-68. Единая система конструкторской документации. Форматы;
* ГОСТ 6.10.4-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения;
* ГОСТ 19.004-80-82. Единая система программной документации. Термины и определения;
* ГОСТ 19.101-77. Единая система программной документации. Виды программ и программных документов;
* ГОСТ 19.102-77. Единая система программной документации. Стадии разработки;
* ГОСТ 19.201-78-82. Единая система программной документации. Техническое задание. Требования к содержанию и оформлению;
* ГОСТ 27.001-95. Система стандартов "Надежность в технике". Основные положения;
* ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения;
* ГОСТ 34.201-89. Виды, комплектность и обозначения документов при создании автоматизированных систем;
* ГОСТ 34.601-90. Автоматизированные системы. Стадии создания;
* ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем;
* СанПиН 2.2.24.548-96. Физические факторы производственной среды. Гигиенические требования к микроклимату производственных помещений;
* СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы.
1. Приложение к постановлению Правительства Москвы от 07.02.2012 № 26-ПП «Об утверждении Положения об эксплуатации автоматизированных информационных систем и ресурсов города Москвы». [↑](#footnote-ref-1)
2. Приложение к постановлению Правительства Москвы от 07.02.2012 № 26-ПП «Об утверждении Положения об эксплуатации автоматизированных информационных систем и ресурсов города Москвы» [↑](#footnote-ref-2)