**Функциональные, технические, качественные характеристики и объем выполняемых работ, оказываемых услуг, поставляемого товара, а также товара, используемого при выполнении работ, оказании услуг (рабочий вариант)**

Приложение № 1

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 \_\_\_\_\_

**Общие требования к оказанию комплексной услуги по обеспечению функционирования электронных сервисов РС ЕГИСЗ**

Документ определяет набор гарантируемых параметров качества Услуги, устанавливает соответствующие функциональные требования и описывает порядок взаимодействия Исполнителя, Заказчика, Оператора РС ЕГИСЗ и Получателя Услуги между собой.

Услуга должна быть реализована на базе Облачной платформы исполнителя (далее – Платформа) по принципам облачных технологий и модели **«Программное обеспечение как сервис»** (за исключением Услуги по сопровождению Голосового диалогового сервиса записи на прием к врачу).

Расчёт и выделение вычислительных мощностей, требуемых для организации Услуги и выполнения, устанавливаемых данным документом параметров, производится Исполнителем самостоятельно. Исполнитель гарантирует совместимость не менее чем с двумя разными используемыми Получателями Услуг в работе с РС ЕГИСЗ браузерами. Требования к браузерам должны быть четко описаны Исполнителем в эксплуатационной документации на функциональные компоненты РС ЕГИСЗ.

Оператор РС ЕГИСЗ вправе отказаться от использования того или иного модуля (функции) комплексной услуги в случае его несоответствия ниже приводимых требований. При появлении новых требований к услуге разработчик составляет и согласовывает с Заказчиком частное техническое задание.

Нормативно-правовое и терминологическое обеспечение РС ЕГИСЗ содержится в нижеследующих документах:

- Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;

- Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

- Федеральный закон от 29.11.2010 № 326 «Об обязательном медицинском страховании в Российской Федерации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных»;

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

- Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;

- Федеральный закон Российской Федерации от 29.07.2017 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья»;

- Постановление Правительства Российской Федерации от 6 июля 2015 года № 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»;

- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановление Правительства РФ от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия»;

- Постановление Правительства РФ от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»;

-Постановление Правительства Российской Федерации от 5 мая 2018 г. № 555 «О единой государственной информационной системе в сфере здравоохранения».

* Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
* Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Приказ Роскомнадзора от 5 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

- Приказ Министерства здравоохранения Российской Федерации от 24.12.2018 № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций»;

- Приказ Министерства здравоохранения Российской Федерации от 13.10.2017г. №804н "Об Утверждении номенклатуры медицинских услуг".

-Приказ Министерства здравоохранения Российской Федерации от 28.02.2019г. №108н «Об утверждении Правил обязательного медицинского страхования»

- Приказ Министерства здравоохранения РФ от 13 марта 2019 г. N 124н "Об утверждении порядка проведения профилактического медицинского осмотра и диспансеризации определенных групп взрослого населения"

- Приказ ФФОМС от 07.04.2011 N 79 "Об утверждении Общих принципов построения и функционирования информационных систем и порядка информационного взаимодействия в сфере обязательного медицинского страхования"

- Постановление Правительства Республики Алтай от 03.08.2018 № 247 «Об утверждении государственной программы Республики Алтай «Развитие здравоохранения»

- Приказ Министра здравоохранения Республики Алтай от 27 февраля 2013 г. № 39 «Об операторе информационных систем в сфере здравоохранения Республики Алтай»;

- Приказ Министра здравоохранения Республики Алтай от 12 февраля 2015 года № 42 «О рабочей группе по внедрению современных информационных систем в здравоохранении Республики Алтай»;

- Положение о РС ЕГИСЗ в Республике Алтай, утверждённое приказом министра здравоохранения Республики Алтай от 27 июня 2018 года № 53-од.

Под Услугой подразумевается решение задач по обеспечению достижения показателей развития РС ЕГИСЗ, повышению качества, доступности, эффективности медицинской помощи посредством предоставления медицинским организациям доступа к функциональным компонентам РС ЕГИСЗ.

Исполнитель осуществляет **техническую и организационно-методическую поддержку работы электронных сервисов**, включая:

-проведение аналитики зарегистрированных заявок на доработки ЭС РС ЕГИСЗ;

- консультационную и организационно-методическую поддержку пользователей ЭС РС ЕГИСЗ по бесплатному, выделенному номеру телефона и в режиме обмена электронной почтой. Исполнитель предоставляет доступ специалистов Заказчика к системе регистрации обращений пользователей;

- диагностику работоспособности программного обеспечения ЭС РС ЕГИСЗ;

- поиск и устранение проблем в случае неработоспособности ЭС РС ЕГИСЗ;

- восстановление работоспособности прикладного программного обеспечения ЭС РС ЕГИСЗ при сбоях;

- анализ потребностей в обновлении установленного системного ПО ЭС РС ЕГИСЗ;

- обновление прикладного ПО ЭС РС ЕГИСЗ до новых версий (плановое, внеплановое);

- редактирование проформ электронной медицинской документации, работу с архетипами проформ и пр.

- сопровождение, актуализация и обновление сервисов интеграции ЭС РС ЕГИСЗ.

Исполнитель реализовывает информационное и документарное сопровождение электронных сервисов, подготовку и передачу Заказчику разработанных вебинаров, учебных материалов по соответствующим разделам работы электронных сервисов.

Исполнитель обеспечивает расширенную техническая поддержку ЭС РС ЕГИСЗ, включая: исправление ошибок пользовательского ввода, устранение сбоев, корректировку данных, автоматизированную загрузку и выгрузку данных, изменение административных настроек программного обеспечения, заведение пользователей, перенастройку ролей и полномочий, создание объектов, оказание устных и письменных консультаций по заданиям Оператора РС ЕГИСЗ, либо председателя Рабочей группы.

Исполнитель обеспечивает документационное и информационное обеспечение ЭС РС ЕГИСЗ: обновление руководств, регламентов и инструкций, тестирование и установку обновлений и программных доработок, описание изменений настроек по результатам работ, анализ и оптимизацию алгоритмов информационных систем, реализованных у Заказчика, подготовку частных технических заданий на внесение доработок и модификаций в программное обеспечение информационных систем.

Исполнитель предоставляет Оператору РС ЕГИСЗ визуальный редактор (конструктор) для разработки новых и корректировки сделанных шаблонов экранных и печатных проформ.

**Электронные сервисы**, входящие в состав Услуги, в целях надлежащего функционирования РС ЕГИСЗ **должны отвечать соответствующим требованиям и обеспечивать:**

**А. Полноту функциональной достаточности, исчерпывающую завершенность внедрения, т.е.:**

улучшение качественных и количественных показателей работы организаций в целом, сокращение затрат времени и труда персонала. В том числе за счет повышения уровня оперативности обработки медицинской информации и выполнения принципа однократного ввода информации в систему и её многократного использования;

соблюдение действующих в отрасли правовых и нормативных актов, общепринятых порядков работы, терминологии, принципов документооборота, принципов управления и организации труда учитывая принципы, отраженные в законодательстве РФ, утвержденных методических документах Минздрава России (в том числе «Типовые требования к медицинской информационной системе регионального уровня»), Федерального фонда обязательного медицинского страхования и национальных стандартов по вопросам, связанным с персонифицированным учетом оказания медицинской помощи;

реализацию практически действующих правил, порядков, нормативов, особенностей составления и оформления отчетов и документов в существующей организационной ведомственной структуре в целом и конкретных подведомственных организациях республики.

использование стандартизованных перечня и значений словарей и справочников;

взаимодействие с ЕГИСЗ и другими информационными системами.

**Б. Соответствие практическим потребностям, т.е.:**

соответствие алгоритмов работы практически действующим бизнес-процессам, на основе результатов работ по внедрению электронных сервисов РС ЕГИС выполненных подрядчиком ранее и исчерпывающего документирования бизнес-процессов;

соответствие электронных версий учётных форм документов практически действующим бумажным, на основе исчерпывающего документирования последних;

соответствие электронных версий форм отчетов практически принятым, на основе исчерпывающего документирования последних;

непрерывная актуализация рабочей и эксплуатационной документации на программное обеспечение электронных сервисов РС ЕГИСЗ;

использование положительного опыта эксплуатации электронных сервисов региональных сегментов ЕГИСЗ, наработок других регионов.

**В. Исключение коллизий, т.е.:**

пригодность для адаптации к изменениям в организационной структуре, а также к изменениям правовых и нормативных актов путем изменения настроек;

пригодность для адаптации к текущим изменениям бизнес-процессов, форм отчетов и документов путем изменения настроек.

**Г. Проверяемость параметров пригодности для промышленной эксплуатации, т.е.:**

исчерпывающую полноту, достоверность и непротиворечивость описания устройства и алгоритмов РС ЕГИСЗ, приемов работы пользователей и администраторов в виде разработанной исполнительной, эксплуатационной документации (руководств пользователя, рабочих инструкций и пр.) к РС ЕГИСЗ;

безусловное соответствие исполнительной документации РС ЕГИСЗ устройству и алгоритмам работы электронных сервисов, интерфейсам пользователей и администраторов, применяемым обработкам, документам и отчетам;

содержание в исполнительной документации информации о найденных в ней ошибках, произведенных улучшениях и дополнениях в ходе развития электронных сервисов РС ЕГИСЗ. Данная информация должна предоставляться в обновленных версиях исполнительной и эксплуатационной документации, при этом соблюдается обязательность соответствия исполнительной документации актуальным произведенным изменениям в РС ЕГИСЗ.

**Д. Защиту информации содержащейся в РС ЕГИСЗ, в соответствии с требованиями законодательства Российской Федерации в области информации, информационных технологий и защиты информации, т.е.:**

предотвращение утечки, хищения, утраты, несанкционированного уничтожения, искажения, несанкционированного копирования, блокирования информации, содержащейся в РС ЕГИСЗ, включая, но не ограничиваясь только этим, обновление системного и прикладного программного обеспечения ЭС РС ЕГИСЗ;

предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

обеспечение криптографической защиты таблицы соответствия идентификаторов (для обратного преобразования) пациентов, в соответствии с требованиями ФСБ России;

своевременное обнаружение фактов несанкционированного доступа к информации;

предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

незамедлительное восстановление информации, модифицированной или уничтоженной вследствие несанкционированного доступа;

постоянный и непрерывный контроль за обеспечением уровня защищенности информации.

Для реализации функции квалифицированной электронной подписи Исполнитель должен использовать совместимый с функцией криптопровайдер.

Исполнитель принимает на себя обязательство производить от имени Заказчика обработку конфиденциальной информации (в том числе персональные данные, включающие в себя также и сведения, отнесённые к медицинской, коммерческой и служебной тайне) автоматизированным способом в соответствии с Поручением Оператора и с целями соответствующими исполнению Министерством здравоохранения Республики Алтай своих полномочий.

Исполнитель гарантирует обеспечение условий обработки конфиденциальной информации, установленных ст. 6 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных», принятие исчерпывающих мер по обеспечению её безопасности при обработке и обязан письменно уведомить Заказчика о готовности к обработке конфиденциальной информации с указанием принятых мер, обеспечивающих 1 уровень защищённости, в соответствии со ст. 19 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» и защиту критической информационной инфраструктуры (КИИ).

Данные Заказчика хранятся на инфраструктуре Исполнителя в течение времени исполнения обязательств по Контракту. По окончании этого срока, заранее уведомив Заказчика, Исполнитель удаляет данные с инфраструктуры Исполнителя без возможности последующего восстановления. Данные также могут быть удалены в любое время по письменному требованию Заказчика.

Исполнитель осуществляет резервное копирование в ежемесячном режиме и хранение накопленной в базах данных информации на собственных носителях. По дополнительному запросу Оператора РС ЕГИСЗ предоставляет копию базы данных на носителе согласно требованиям защиты информации на носителе от несанкционированного либо случайного доступа.

**Параметры предоставления Услуг (электронных сервисов РС ЕГИСЗ)**

Параметры предоставления услуги определяют уровень доступности электронных сервисов РС ЕГИСЗ и пригодность к обеспечению персонифицированного учета медицинских услуг, предоставляемой по модели SaaS, а также характеристики, используемые для отчётности.

А. Все электронные сервисы, являясь элементами РС ЕГИСЗ, предназначены для решения комплекса задач, связанного с ведением персонифицированного учета и обработки накапливаемой в электронных сервисах информации в течение календарного года.

Б. Полнота оказания электронного сервиса понимается как признак пригодности или не пригодности данного сервиса в данный момент к обеспечению персонифицированного учета медицинских услуг. При этом сам факт доступности сервиса не является таковым признаком.

В. Таким образом уровень критичности отказа сервисов определяется как отсутствие полноты оказания, достаточной для обеспечения персонифицированного учета медицинских услуг: в данный момент, в течение промежутков времени, в течение календарных периодов.

Г. Регистрация момента и продолжительности отказа осуществляется очно сотрудником медицинской организации и представителем Оператора РС ЕГИСЗ с составлением рукописного акта, в котором устанавливается критичность полноты сервиса и прочие обстоятельства возникновения отказа.

При этом общий уровень доступности должен оставаться в пределах правила 24 часа в сутки, 7 дней в неделю.

**Порядок взаимодействия Исполнителя с Заказчиком и получателями Услуг (электронных сервисов РС ЕГИСЗ)**

На каждую из сторон взаимодействия возложены соответствующие обязанности по информированию других участников взаимодействия при различных режимах работы (оказания и получения Услуги). Порядок информирования сторон приведён в таблице ниже.

Таблица 1 - Информационный обмен

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Субъект | Что передаёт | Кому передаёт |
| Режим повседневной деятельности |
| 1 | Получатель Услуги (МО) | Информационный запрос; Запрос на улучшение электронного сервиса РС ЕГИСЗ; Запрос поддержки; Запрос на доработку электронного сервиса РС ЕГИСЗ. | Оператор РС ЕГИСЗ, СТП  |
| 2 | Оператор РС ЕГИСЗ, МЗ РА | Информационный запрос; Запрос на улучшение, доработку электронного сервиса РС ЕГИСЗ. Запрос информационной безопасности. | Исполнитель либо СТП  |
| 3 | Исполнитель | Ежемесячный отчёт о качестве предоставляемой Услуги. Отчёт о доступности электронного сервиса РС ЕГИСЗ за период (содержит инциденты, регламентные работы). | Оператор РС ЕГИСЗ |
| Режим предстоящего ухудшения параметров Услуги |
| 4 | Исполнитель | Сообщение о предстоящем ухудшении электронного сервиса РС ЕГИСЗ, отключении, обновлении программного обеспечения. | Оператор РС ЕГИСЗ |
| 5 | Получатель Услуги (МО) | Сообщение о предстоящем отключении оборудования Исполнителя на территории МО. | СТП |
| Режим ухудшения параметров Услуги (сбои, неполадки, авария, в том числе неприемлемое для работы увеличение времени отклика Системы) |
| 6 | Исполнитель | Сообщение об ухудшении параметров Услуги, нарушении доступности; сообщение-уточнение времени устранения аварии; сообщение о восстановлении параметров Услуги, устранении аварии и перерасчет стоимости услуги (в случае критичного отказа более 4 часов). | Оператор РС ЕГИСЗ (ответственному лицу) |
| 7 | Получатель Услуги (МО) | Сообщение об ухудшении параметров Услуги (инцидент), нарушении доступности. | Оператор РС ЕГИСЗ, СТП |
| 8 | Оператор РС ЕГИСЗ | Сообщение об ухудшении параметров Услуги (инцидент), нарушении доступности. | СТП, либо Исполнитель |

Приложение № 2

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 \_\_\_\_\_

**Требования к базовому электронному сервису «Медицинская информационная система Республики Алтай»**

Использование электронных сервисов, входящих в состав Услуги, подразумевает автоматизацию следующих рабочих процессов медицинских организаций Заказчика:

1. Учёт обслуживаемых пациентов, включающий в себя регистрацию обслуживаемого населения, определение страховой принадлежности и идентификацию застрахованного, прикрепление к медицинской организации, поликлиническим участкам обслуживания, прикрепление к врачу (реализация права на выбор врача). Ведение регистра прикреплённого к медицинской организации населения;
2. Управление расписанием и записью на обслуживание в поликлинике включающее в себя планирование и обеспечение ресурсов приема пациентов участковыми врачами, специалистами;
3. Управление оказанием амбулаторной помощи включающее в себя персонифицированный учет сведений об оказании медицинской, лечебно-диагностической помощи и профилактических мероприятий в поликлинике участковыми врачами и специалистами, мероприятиях в центрах здоровья, формировании назначений;
4. Управление приёмом в стационаре включающее в себя регистрацию пациентов в приемном отделении, определение страховой принадлежности и идентификацию застрахованного;
5. Управление оказанием стационарной медицинской помощи включающее в себя персонифицированный учет сведений об оказании медицинской, лечебно-диагностической помощи, планирование и обеспечение ресурсов (кроме лекарственного обеспечения, см. п. 17), формирование назначений, выполнение работы и контроль ее качества;
6. Автоматизация коечного фонда стационара;
7. Учёт медицинских работников;
8. Управление взаиморасчётами за медицинскую помощь, включающее в себя: регистрацию тарифного соглашения, план-задания по ОМС, формирование прейскурантов, договоров с корректировкой их состава, формирование реестров счетов, обработку оплаты и отказов, закрытие финансового периода, доступ к сведениям для проведения медико-экономической экспертизы качества медицинской помощи;
9. Формирование внутренней отчётности РС ЕГИСЗ в целях анализа, контроля, аудита и планирования деятельности медицинских организаций;
10. Интеграция и обеспечение взаимодействия с системами ведения классификаторов, справочников, федеральными и региональными сервисами ЕГИСЗ, включая подсистему РЭМД;
11. Управление акушерско-гинекологической службой включающее в себя информационную поддержку процессов наблюдения, ведения и родоразрешения беременных группы высокого и среднего риска и ведение ЭМК. Обмен информацией между акушерско-гинекологической службой и педиатрической службой;
12. Ведение мониторинга пациентов по определённым группам риска;
13. Диспансерное наблюдение. Постановка и снятие с диспансерного учёта. Ведение медицинской документации периодических медицинских осмотров. Планирование профилактических осмотров. Формирование утверждённой статотчётности;
14. Вакцинопрофилактика. Учет фактов выполнения вакцинации, отказов от вакцинации, осложнений от вакцинаций;
15. Формирование и просмотр центрального архива медицинских изображений для приема и хранения ЭКГ с медицинских диагностических аппаратов.
16. Интеграция с ФСС. Интеграция с ИС ТФОМС Республики Алтай в части определения страховой принадлежности, обмена данными о прикреплении пациентов к медицинской организации и получения необходимых сведений страховыми медицинскими организациями.

Автоматизация указанных процессов должна обеспечивать юридическую значимость электронного взаимодействия (интеграции с внешними информационными системами) с применением электронной подписи (изм. в 323).

При появлении в течение контрактного года со стороны МЗ РФ или ФФОМС новых требований к РС ЕГИСЗ разработчик подготавливает и согласовывает с Заказчиком соответствующее частное техническое задание на внесение изменений в сервис/доработку.

Получателям Услуги должен быть предоставлен доступ к следующим, соответствующим практическим потребностям функциям:

**Ф 1. Регистрация пациентов.** Регистрация персональных данных пациентов разных категорий: о проживании, удостоверяющих документах, полисах ОМС/ДМС, прикреплении, занятости (в т.ч. условия труда), социальном статусе (в т.ч. наличии льгот), аллергиях и противопоказаниях, контактной и произвольной информации.

Должна обеспечиваться однозначная идентификация пациентов с использованием собственного идентификатора и идентификаторов внешних систем (паспорт, полис ОМС, УЭК и прочие).

**Ф 2. Работа с картотекой пациентов.** Поиск пациентов, дубликатов записей в картотеке, работа с выборками из картотеки данных на пациентов по разнообразным критериям. Печать штрих-кода на амбулаторной карте. Считывание по штрих-коду для учета месторасположения карты в кабинете/регистратуре (в карточке пациента-раздел "Местонахождение карт").

**Ф 3. Регистр прикреплённого к медицинским организациям населения.**

Управление Регистром. Прикрепление/открепление пациентов к медицинской организации. Выбор вида прикрепления, печать заявлений на прикрепление, присоединение к заявке на прикрепление сканированного документа удостоверяющего личность. Присоединение к электронной карточке пациента в системе сканированных документов (паспорт, ЕНП и пр.) Формирование отчётности по загруженности участков медицинской организации, сортировки по видам прикрепления. Формирование отчётов в ТФОМС, СМО республики. Интеграция Регистра с веб-сервисом ТФОМС для определения страховой принадлежности и проверки полиса ОМС.

Участок. Анализ активности пациентов в разрезе: посещения медицинских организаций, половозрастных признаков, посещения врачей, участков. Реализация функций проведения автоматизированной работы по индексации прикреплённого населения в МИС. То есть создания и ведения красных, белых и зелёных списков на основе признаков относящихся к возрасту пациента, наличии/отсутствии хронических заболеваний, систематической неявки на приём и пр. Ввод сигнальной информации о пациенте и её отображение. Автоматический расчёт и учёт демографических показателей. Регистрация факта смерти пациента. Регистрация вызовов на дом, оформление результата вызова на дом. Отчётность по вызовам врача на дом.

Участковый журнал прикрепленных пациентов. Функция должна обеспечивать учёт прикрепления пациента, как к участку, так и к врачу. Реализованный алгоритм должен позволять корректно закреплять лечащего врача за пациентом, при этом, не изменяя работу принципа участкового обслуживания.

**Ф 4. Ведение расписаний.** Ведение расписания работы медицинских работников, структурных единиц (кабинетов, отделений) и оборудования. Настройка расписаний с учётом приоритетов повторных посещений. Учет фактически отработанного времени. Получение оперативных сводок о планируемой занятости ресурсов. Формирование и вывод на печать расписания. Автоматическое продление и валидации расписаний на заданный период с выводом предупреждений пользователю на экран.

**Ф 5. Запись пациентов на обслуживание в поликлинике.** Выполнение диспетчеризации направлений на прием (предварительная запись).

Учет квартирных вызовов врача (вызовов на дом). Должна быть предусмотрена возможность передачи данных врачу и печать соответствующих отчётных форм.

Должен быть реализован механизм формирования электронных журналов предварительной записи и квартирных вызовов и просмотр пациентов (и их талонов), записанных на прием к врачу.

**Ф 6. Информационная поддержка пациентов. Дистанционная запись пациентов на обслуживание в поликлинике через Интернет и роботизированную систему записи по телефону горячей линии.** Дистанционный доступ пациента к расписаниям работы через интернет, запись на обслуживание. Запись на приём к врачу через оператора колл-центра, а также используя роботизированный сервис.

Должно быть реализовано в виде портала пациента с авторизированным доступом к личному кабинету, просмотра медицинских организаций с учётом участкового принципа обслуживания, просмотра расписания и записи на обслуживание.

Через веб портал пациент должен иметь возможность получить на экран сведения о режиме работы ЛПУ и расписании работы врача с информацией о часах приёма, занятых и свободных талонах.

Отображение информации о медицинских организациях, к которым прикреплён пациент, списка прикреплённых к нему врачей, дополнительной информации в личном кабинете на портале пациента.

Поддержка вывода информации о расписании работы МО на информационные табло (мониторы). - Возможность для администраторов МО гибко менять оформление и выводимую информацию, включая автоматический вывод расписания из календарей ЭР на экран. - Бегущая строка с функцией внесения информации регистраторами.

**Ф 7. Поиск и просмотр ЭМК амбулаторного пациента.** Поиск ЭМК пациента по заданным критериям, просмотр ЭМК пациента.

**Ф 8. Ведение ЭПМЗ амбулаторного пациента.** Формирование электронных персональных медицинских записей (ЭПМЗ) в ЭМК амбулаторного пациента в соответствии с требованиями к структуре ЭПМЗ, их жизненному циклу (создание, ведение, подписание, хранение, уничтожение) и организации прав доступа к ним в соответствии с действующими требованиями.

Формирование использующихся типов медицинских карт: взрослая поликлиническая, стоматологическая, и др.

Формирование первичного, повторного приема, консультации с использованием настроенных пользовательских шаблонов ввода данных осмотра пациента. Для оформления повторного приёма пациента в интерфейсе должна быть реализована возможность повторного (в виде подстановки в шаблон) полуавтоматического использования данных введённых в ЭМК на первичном приёме.

Регистрация подробного структурированного диагноза (основное заболевание, осложнения основного и сопутствующие). При этом должна быть возможность ввода предварительного диагноза, а после уточнения заболеваний пациента – уточненного с автоматическим отражением его в листе уточненных (заключительных) диагнозов ЭМК пациента. Должна быть возможность регистрации изменений диагноза. Каждое заболевание должно кодироваться в соответствии с МКБ-10. Возможность указания стадии и фазы заболевания.

Регистрация и просмотр диагностических и лечебных назначений: консультаций специалистов, лабораторных исследований, инструментальных исследований, медикаментозных назначений, процедуры или комплекса процедур.

Должна быть возможность изменения и отмены назначений.

Должна быть возможность одномоментного формирования всего комплекса назначений согласно государственным стандартам оказания медицинской помощи, медико-экономическим стандартам, стандартам, применяемым в МО или личным шаблонам врача, настроенным в Системе.

Стандарты должны быть настроены и актуализироваться в соответствии с требованиями действующих нормативных документов.

Регистрация сведений о проведенных на приеме амбулаторных манипуляциях, процедурах, операциях, исследованиях.

Учет направлений на врачебную комиссию медицинского учреждения и медико-социальную экспертизу (МСЭ), направлений на госпитализацию, назначения санаторно-курортного лечения.

Создание ЭПМЗ типа консультация, лабораторное исследование, инструментальное исследование, процедура на основании диагностических и лечебных назначений врача. Отображение ЭПМЗ указанных типов в списках пациентов, направленных на консультацию, исследования и процедуры в соответствующих журналах.

Присоединение к ЭМК (ЭПМЗ) усиленной квалифицированной электронной подписи.

**Ф 9. Формирование выходных документов ЭМК амбулаторного пациента.** Формирование и вывод на печать выходных документов, разделов ЭМК амбулаторного пациента в традиционной форме, в том числе, но не ограничиваясь:

Титульный лист медицинской карты;

Прием пациента (дневник врача);

Направление на госпитализацию, обследование, консультацию;

Направление на лабораторное исследование (форма направления зависит от вида исследования);

Рецепт;

Памятка пациенту о назначенных медикаментах. Генерация по листам назначений и печать бланков журналов назначений;

Талон амбулаторного пациента;

Ведомость учета врачебных посещений в амбулаторно-поликлинических учреждениях, на дому и др. утверждённые Минздравом России учётные документы.

**Ф 10. Учет приема больных и отказов в госпитализации.** Регистрация поступления пациента в приемное отделение. Идентификация застрахованных, актуализация сведений о страховой компании. Ввод данных первичного осмотра пациента. Печать титульного листа истории болезни и данных врачебного приема. Формирование журналов: учет приема больных, перевод из других корпусов, амбулаторный прием, отказы в госпитализации.

Оформление госпитализации пациента, формирование ЭМК. Оформление отказа в госпитализации или факта оказания амбулаторной помощи. Ведение единого журнала учета приема больных и отказов в госпитализации, а также отдельных журналов госпитализации, отказов в госпитализации и учета амбулаторной помощи со своей нумерацией и печатными шаблонами. Отчеты о поступивших пациентах в приемное отделение.

**Ф 11. Просмотр списка стационарных больных на отделении.**

**Ф 12. Поиск и просмотр ЭМК стационарного больного.** Поиск по заданным критериям и просмотр результатов поиска.

**Ф 13. Ведение ЭПМЗ стационарного больного.** Формирование электронных персональных медицинских записей (ЭПМЗ) в ЭМК стационарного больного в соответствии с требованиями к структуре ЭПМЗ, их жизненному циклу (создание, ведение, подписание, хранение, уничтожение) и организации прав доступа к ним в соответствии с действующими стандартами.

Формирование медицинской карты стационарного больного в соответствии с профилем оказываемой стационарной помощи.

Формирование ЭПМЗ следующих типов: первичных осмотров, дневников, консультаций по направлениям других специалистов, этапных эпикризов, переводных эпикризов, выписных эпикризов, выписок, предоперационных эпикризов, протоколов операций.

При этом должны использоваться настроенные пользовательские шаблоны ввода данных осмотра пациента; предоставляться возможность выбора из БД и включения в ЭПМЗ необходимой информации из ЭМК пациента в соответствие с полномочиями пользователя. Для оформления повторного осмотра пациента в интерфейсе должна быть реализована возможность повторного (в виде подстановки в шаблон) полуавтоматического использования данных введённых в ЭМК на первичном осмотре.

Регистрация структурированного диагноза (основное заболевание, осложнения основного и сопутствующие) при поступлении, клинического диагноза и заключительного клинического диагноза пациента с использованием международного классификатора болезней 10 пересмотра (МКБ-10). Возможность указания стадии и фазы заболевания.

Формирование плана лечения, плана обследования и плана наблюдения пациента.

Должна быть возможность изменения и отмены назначений.

Ведение листов назначений и листов наблюдений: формирование листов назначений и листов наблюдений в соответствии с планом в историях болезней; расчет графика выполнения назначений и измерения показателей состояния здоровья пациента; формирование сводных листов назначений и наблюдений в целом по отделению.

Должна быть возможность одномоментного формирования всего комплекса назначений согласно государственным стандартам оказания медицинской помощи, медико-экономическим стандартам, стандартам, применяемым в МО или личным шаблонам врача, настроенным в Системе.

Стандарты должны быть настроены и актуализироваться в соответствии с требованиями действующих нормативных документов.

Создание ЭПМЗ типа консультация, инструментальное исследование, процедура, оперативное вмешательство на основании листов назначений. Отображение ЭПМЗ указанных типов в списках пациентов, направленных на консультацию, исследования и процедуры в соответствующих журналах.

Присоединение к ЭМК (ЭПМЗ) усиленной квалифицированной электронной подписи.

**Ф 14. Формирование выходных документов ЭМК стационарного больного.** Формирование и вывод на печать учётно-отчётных медицинских документов, разделов ЭМК стационарного пациента в традиционной форме. Просмотр листов назначений (генерация по листам назначений и печать бланков журналов назначений. Оформление статистической карты выбывшего из стационара по данным из медицинской карты пациента.

**Ф 15. Учет индивидуальных направлений на анализы и исследования и учет результатов анализов и исследований.** Печать бланков-заключений. Заполнение дополнительных полей отражающих результат исследования в составе медицинских протоколов.

**Ф 16. Управление взаиморасчетами за оказанные медицинские услуги.** Регистрация договоров на оказание медицинских услуг. Регистрация договоров по ОМС, ДМС, бюджету, на оказание платных услуг, договоров с предприятиями. Регистрация прейскурантов медицинских услуг. Регистрация прейскурантов оказываемых медицинских услуг к договорам на оказание медицинских услуг по ОМС, ДМС, по договорам с предприятиями, договорам на оказание платных услуг.

Ведение счетов с персонифицированными реестрами по оказанным услугам и взаиморасчёты со страховыми медицинскими организациями в соответствии с общими принципами построения и функционирования информационных систем и порядка информационного взаимодействия в сфере ОМС, а также с учетом принятых регламентов на территории республики и сложившейся практики. Учет подтверждений оплаты и причин отказов. Обеспечение связи позиции реестра с ЭПМЗ, первичным учетным документом. Закрытие финансового периода. Формирование реестров-счетов на неотложную медицинскую помощь.

Наличие средств поиска и анализа ошибок Наличие средств регистрации и анализа планов-заданий. Наличие автоматизированных средств печати справок о составе и стоимости оказанных услуг.

Должна поддерживаться история изменений прейскурантов для возможности расчета стоимости лечения на любой момент времени в течение не менее года после оказания услуги.

**Ф 17. Формирование отчетности.** Формирование аналитических отчётов в целях анализа, контроля, аудита и планирования деятельности учреждений здравоохранения. Формирование сведений управленческого характера: объем проведенных лечебных мероприятий, контроль за исполнением обязанностей медицинского персонала, полноты и качества оказания медицинской помощи и т.п.

**Ф 18. Учет медицинских работников.** Регистрация и хранение сведений о медицинских работниках, включая сведения о квалификации, месте работы (до структурного подразделения), регистрация сведений об увольнении.

**Ф 19. Администрирование МИС. Защита информации.** Ролевое управление доступом к данным и функциям. Распределение доступа пользователей на уровне клиентского интерфейса, доступ к открытым механизмам конфигурирования.

В основу распределения прав доступа должны быть положены требования к ведению бумажных медицинских документов, определенные существующими нормативными документами, и принятая технология лечебно-диагностического процесса в медицинских учреждениях в соответствии с их профилем.

Подсистема журналирования, позволяющая фиксировать источник, дату и время внесения изменений, имя пользователя, вносившего изменение, тип операции (создание, изменение, удаление), модель объекта, код объекта, IP адрес, с которого произведены изменения объекта. События должны отображать начальное и конечное значения по измененным полям.

Система выгрузки логов в файл. В данном файле должна фиксироваться следующая информация:

− Внутренний уникальный идентификатор события;

− Дата и время события;

− Типы события;

− Типы объектов;

− Значение измененного объекта;

− Идентификатор пользователя, IP-адрес, с которого произведено событие.

В обязательном порядке для каждого фиксирующегося события должно фиксироваться время события (TimeStamp). Формат даты и времени должен быть следующий ГГГГ-ММ-ДД ЧЧ:ММ:СС.MLS (миллисекунды).

Журналированию должны подлежать типы события (EventType). Фиксируются юридические (lse) и системные (se) события. К юридически значимым событиям относятся записи о совершении операций, изменяющих статус объектов Системы или влекущие иные последствия для участников административных процедур. Системные события – операции, не связанные с изменением статуса участников процедур или с действиями над конкретным объектом Системы (просмотр объектов, печать документов и т.п.).

В журнале изменений должны регистрироваться следующие события (Event): создание (create), чтение (read), обновление (update), удаление данных (delete).

Должен также фиксироваться тип объекта (ObjectType) и значение объекта, который изменился.

Выгруженные данные должны содержать удобно читаемый код (human-readable code), который должен включать наименование пользователя, производящего изменение, наименование события, наименование типа объекта, новое значение объекта. Требование обусловлено в связи с обязанностями Оператора РС ЕГИСЗ представлять справки в судебные органы, в иные инстанции при расследовании инцидентов информационной безопасности.

В журнале изменений должен регистрироваться идентификатор пользователя, который совершил событие, а также IP-адрес, с которого было совершено событие.

В информационной системе должна обеспечиваться защита информации о событиях безопасности и должна иметься возможность просмотра и анализа информации о действиях отдельных пользователей в информационной системе.

Система логического контроля за действиями пользователей в системе должна производить оповещение ответственного пользователя о совершении критичных с точки зрения защиты информации операций и действий путём отправки сигнала на адрес электронной почты и записи в соответствующий журнал аудита.

Формирование отчётов информационной безопасности.

**Ф 20. Поиск ЭМК и просмотр всех ЭПМЗ по пациенту.** Поиск ЭМК и просмотр всех ЭПМЗ по пациенту, включая как амбулаторные ЭПМЗ, так и стационарные ЭПМЗ. Просмотр информации хронологически по всем зарегистрированным госпитализациям, амбулаторным посещениям, результатам анализов/исследований.

**Ф 21. Интеграция с федеральными и региональными сервисами ЕГИСЗ.** Синхронизация справочной информации и информации региональных разделов федеральных регистров и систем;

Обновление (актуализация) информации в отдельных разделах Системы из федерального сегмента ЕГИСЗ;

Интеграция с федеральным сервисом ИЭМК (ИЭМК второй очереди);

Интеграция с сервисом ФЭР (ФЭР второй очереди)

Интеграция с сервисом ФРМП.

Интеграция с сервисом МИС СМП.

**Ф 22. Интеграция с системой ОМС Республики Алтай.** АРМ ТФОМС и сервисы интеграции с региональным сегментом Единого регистра застрахованных, включая просмотр информации о прикреплении и мониторинг коечного фонда медицинских организаций.

*Определение страховой принадлежности.*Идентификация застрахованных, актуализация данных в соответствии с общими принципами построения и функционирования информационных систем и порядка информационного взаимодействия в сфере ОМС, интеграцию с сервисом определения страховой принадлежности Территориального фонда ОМС Республики Алтай.

*Экспертиза качества оказанной медицинской помощи.* Ограниченный доступ специалистов ТФОМС, СМО к первичной медицинской документации, накапливаемой в МИС, к разделам ЭМК, к разделам регистра медицинских работников в целях проведения медико-экономической экспертизы с выполнением соответствующих требований по защите информации.

**Ф 23. Режим минимальной функциональности.** Основные требования к функции см. Функцию 16.Назначение функции режима минимальной функциональности: ввод информации о случаях, созданных в МО, в упрощенном режиме, не формируя случаи из МИС. Ввод данных по поликлиническим случаям ответственным специалистом ЛПУ на основе талона амбулаторного пациента, поиск в БД на основе введенных данных ранее созданного случая с целью контроля его дублирования, настройка кодов ввода информации, клавиатурный ввод данных («горячие клавиши»).

Данная функция расширяет возможности применения функции 16.

**Ф 24. Интегрированный в МИС модуль Перинатального центра.**

Функция должна быть интегрирована с работой основных функций МИС: электронная регистратура, ведение ЭМК, выгрузка отчётности ОМС.

Мониторинг беременных. Постановка беременных на учет. Планирование посещений акушера-гинеколога и врачей-специалистов. Регистрация и внесение результатов осмотров беременной лечащим врачом, врачами-специалистами с сохранением в карте ведения беременности.

Назначение и автоматизированный контроль выполнения необходимых консультаций, инструментальных исследований, лабораторных исследований согласно медицинским показаниям и единым стандартам, в том числе рекомендуемому графику мероприятий по сопровождению беременности.

Автоматический анализ принадлежности беременной к группе риска. Формирование сигнальной информации о здоровье будущей матери. Ведение дневника наблюдения акушера-гинеколога. Регистрация в карте ведения беременности данных функциональных и лабораторных исследований.

Закрепление за пациенткой МО для планового или экстренного приема родов. Закрепление за пациенткой МО для курирования новорожденного. Формирование и оформление эпикриза по случаям госпитализации. Формирование данных медицинской статистики и форм статистической отчетности.

В программе Мониторинга должна быть реализована поисковая система. В программе должна быть предусмотрена возможность консультанта вышестоящей МО, перевести беременную из одной группы риска в другую, если для этого возникает необходимость.

Система должна обеспечивать формирование унифицированных стандартных форм отчетных и учетных документов, в том числе, но не ограничиваясь только этим:

13 Сведения о прерывании беременности (в сроки до 22 недель);

32 Сведения о медицинской помощи беременным, роженицам и родильницам;

096/у История родов;

097/у История развития новорожденного;

111/у Индивидуальная карта беременной и родильницы;

003-1/у Медицинская карта прерывания беременности;

113/у Обменная карта родильного дома, родильного отделения больницы;

097-1/у-95 Карта первичной и реанимационной помощи новорожденному в родильном зале;

103/у-08 Медицинское свидетельство о рождении.

Функциональная компонента «Материнство» должна иметь набор следующих подфункций:

планирование посещений акушера-гинеколога и врачей-специалистов;

регистрацию осмотров беременной лечащим врачом, врачами-специалистами с сохранением в ЭМК региона;

формирование протоколов осмотров беременной с сохранением в ЭМК региона;

назначение выполнения необходимых консультаций, инструментальных исследований, лабораторных исследований согласно медицинским показаниям;

регистрация в ЭМК региона данных функциональных и лабораторных исследований;

формирование эпикризов;

идентификация, сопоставление беременной и её родившегося ребёнка в системе;

формирование истории развития ребёнка на основе данных беременных и данных, полученных в стационаре перинатальной службы (истории родов, истории развития новорожденного).

**Ф 25. Мониторинг пациентов с тяжелыми заболеваниями** **различного профиля.** Функция должна реализовываться в интерфейсе МИС, использовать общую для здравоохранения региона картотеку пациентов.

Функция должна обеспечить автоматизацию деятельности медицинских работников в части внесения данных о факторах мониторинга пациентов кардиологического, педиатрического, травматологического (основных профилей) и других настраиваемых профилей, также интерактивного построения отчетности по этим данным.

Система должна строить список (монитор) пациентов в порядке, определяемом значением интегрального показателя риска. Выборка осуществляется из тех пациентов, которые поступили в приёмные покои медицинских организаций республики за определённый период. Расчёт интегрального показателя риска сводится к подсчёту значений частных показателей риска отдельных факторов и перемножения их вероятностей возникновения.

Для каждой ЭМК пациента должен быть доступен ввод следующего базового набора данных (факторов риска), специфических для каждого мониторинга.

Педиатрический мониторинг: Диагноз по МКБ-10. Сведения о факте госпитализации, который важен для мониторинга. Сведения об образе жизни пациента.

Кардиологический мониторинг: Диагноз по МКБ-10. Сведения о факте госпитализации, который важен для мониторинга. Сведения об образе жизни пациента. Угроза ОКС. Угроза ОКМ. Артериальная гипертензия.

Травматологический мониторинг: Основной диагноз по МКБ-10 (диагноз при поступлении). Сопутствующий диагноз (диагнозы в ЭМК пациента до момента поступления в стационар). Тяжесть общего состояния больного. Ввод значения тяжести состояния должно быть предусмотрено в протоколе осмотра врача приёмного покоя. Сведения о факте госпитализации, который важны для мониторинга. Социальный фактор. Сведения об образе жизни пациента. Значение должно храниться в электронной карточке пациента. Сохранение данных о враче, который заполнил данные и даты внесения сведений.

Настройка для каждого из описанных выше факторов риска значения степени риска (для некоторых пользователей). Значения степеней риска, которые должны быть проставлены для каждого из факторов. Формирование отчетов за выборочный период времени.

Для отдельно выбранного пациента в мониторинге должен быть предусмотрен переход от данных мониторинга к данным в ЭМК выбранного пациента.

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 доступ к основным функциям системы.

Должна быть функция фильтра/сортировки выводимых на экран строк мониторинга по половозрастным признакам и другим критериям.

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

**Ф26. Диспансерное наблюдение и периодические медицинские осмотры.** Учет случаев диспансерного наблюдения (ДН) и профилактических осмотров, регистрация фактов постановки пациента на диспансерное наблюдение и снятия с диспансерного наблюдения. - Внесение информации о явках пациента. - Формирование этапных эпикризов, планов наблюдения. - Формирование списков для углубленного медицинского обследования. Автоматическое планирование мероприятий по диспансеризации и профилактическим осмотрам на основании действующих нормативноправовых актов Минздрава, - Контроль полноты проведения мероприятий и правильности заполнения медицинской документации. - Автоматическое информирование руководителя МО о фактах неисполнения плана диспансерного наблюдения. - Автоматическое напоминание врачу о пропущенных явках пациента по ДН. - Формирование утвержденной статистической отчетности и отчетности ОМС.

Формирование карты периодического медицинского осмотра. - Поддержка различных видов медицинского осмотра, включая выдачу справок на оружие, водительская комиссия, периодические медицинские осмотры лиц, работающих во вредных и опасных условиях труда, осмотры декретированных групп и т.д. Планирование профилактических осмотров, включая формирование списков подлежащих осмотру сотрудников и объема исследований, заполнение карт профилактических осмотров. - Формирование утвержденной статистической отчетности.

**Ф.27. Вакцинопрофилактика.** Учет фактов выполнения вакцинации, отказов от вакцинации, осложнений от вакцинаций. - Учет исследования напряженности иммунитета. - Формирование этапных эпикризов, планов.

Автоматизированное планирование графика вакцинаций на основе настраиваемого справочника календаря вакцинаций (национальный). - Автоматическое информирование руководителя МО о фактах неисполнения плана вакцинаций. - Автоматическое напоминание лечащего врача о пропущенных плановых ревакцинациях и вакцинациях. - Формирование утвержденной статистической отчетности.

**Ф28. Модуль интеграции с ИС ТФОМС. И**сполнитель обеспечивает работу электронных сервисов в части выполнения требований к их пригодности к промышленной эксплуатации. Электронное взаимодействие осуществляется в целях реализации соглашения об информационном взаимодействии между ТФОМС Республики Алтай и Оператором РС ЕГИСЗ.

**Ф29. Модуль интеграции с ИС ФСС совмещенный с функционалом «Документы нетрудоспособности».** Модуль «предназначен для автоматизации деятельности медицинского персонала при работе с листами нетрудоспособности и бланками строгой отчетности. Ведение журналов листов нетрудоспособности и бланков строгой отчетности. Вывод и фильтрация документов нетрудоспособности по различным признакам. Редактирование существующих документов. Настройка параметров журналов и параметров печати бланков. Настройка журналов выдачи и параметров печати бланков. Функция интеграции модуля с электронным сервисом ФСС (при необходимости Заказчик совместно с Исполнителем подготавливает частное техническое задание).

**Ф30. Регистр инвалидов. Модуль интеграции с ИС ФБ МСЭ для обработки ИПРА и направлений на МСЭ.**

1. Основные нормативно - правовые документы Федеральный закон от 24 ноября 1995 года № 181-ФЗ «О социальной защите инвалидов в Российской Федерации».
2. Приказ Минтруда России от 31 июля 2015 года № 528н «Об утверждении Порядка разработки и реализации индивидуальной программы реабилитации…».
3. Приказ Минтруда России от 15 ноября 2015 года № 723н.

Описание рабочих процессов, подлежащих автоматизации

1. Направление подведомственными Министерству здравоохранения Республики Алтай учреждениями пациентов на медико-социальную экспертизу.
2. Организация исполнения мероприятий ИПРА подведомственными Министерству здравоохранения Республики Алтай учреждениями, в части медицинской реабилитации.
3. Оказание соответствующих видов помощи, оказываемых инвалиду в преодолении барьеров, мешающих получению им услуг в медицинских организациях Республики Алтай.
4. Сбор, обработка и свод информации об исполнении мероприятий подведомственными Министерству здравоохранения Республики Алтай учреждениями.
5. Предоставление Министерством здравоохранения Республики Алтай сводной информации об исполнении возложенных на него ИПРА мероприятий в ФГУ МСЭ.
6. Ведение реестра инвалидов проходящих медицинскую реабилитацию на территории Республики Алтай, закрепление их за конкретной медицинской организацией.

Общие требования

Информационная поддержка процессов направления на МСЭ, медицинской реабилитации (абилитации) и оказания соответствующих видов помощи в преодолении барьеров должна быть реализована на основе использования технологии SaaS «облачный электронный сервис».

Структурно АРМ ИПРА должно состоять из трёх компонентов:

- АРМ ИПРА уровня медицинской организации;

- АРМ ИПРА уровня ОУЗ;

- компонента загрузки и выгрузки данных (интеграции) с ГИС, формирующей банк данных о гражданах, которым была предоставлена государственная услуга по проведению медико-социальной экспертизы (ГИС ФГУ МСЭ)

Реализуемая ИС должна быть полностью интегрирована с региональным сегментом Единой государственной информационной системой в сфере здравоохранения и ГИС ФГУ МСЭ.

Методы и способы интеграции АРМ ИПРА и ГИС ФГУ МСЭ должны соответствовать разработанным ФГУ МСЭ документам, но не ограничиваясь только этим:

- структура таблиц БД-витрины ОИВ;

- инструкция по созданию базы данных - «витрины» ОИВ и скрипт для создания БД-витрины ОИВ;

- инструкция по настройке клиента для доступа к сведениям МСЭ по защищённому каналу;

- структура XML-файлов со сведениями из ИПРА.

Сводная информация о выполнении мероприятий ИПРА, либо причинах их невыполнения подается медицинскими организациями в Министерство здравоохранения Республики Алтай

В графах таблиц Данные об исполнении мероприятий, предусмотренных ИПРА инвалида (ИПРА ребенка-инвалида)" указываются:

графа 1 - наименование мероприятий, предусмотренных ИПРА инвалида (ИПРА ребенка-инвалида);

графа 2 - исполнитель мероприятия - орган исполнительной власти субъекта Российской Федерации, региональное отделение Фонда, орган местного самоуправления, организация независимо от ее организационно-правовой формы;

графа 3 - дата исполнения реабилитационного или абилитационного мероприятия, предусмотренного ИПРА инвалида (ИПРА ребенка-инвалида).

графа 4 - делается запись "выполнено" и указываются реквизиты контракта (соглашения, государственного задания) на предоставление реабилитационных или абилитационных мероприятий, включая оказание медицинской помощи, обеспечение техническими средствами реабилитации (при его наличии) или делается запись "не выполнено".

Причины неисполнения мероприятий, предусмотренных ИПРА инвалида (ИПРА ребенка-инвалида):

- Инвалид (ребенок-инвалид) либо законный (уполномоченный) представитель не обратился в соответствующий орган государственной власти, орган местного самоуправления, организацию независимо от организационно-правовых форм за предоставлением мероприятий, предусмотренных ИПРА инвалида (ИПРА ребенка-инвалида).

- Инвалид (ребенок-инвалид) либо законный (уполномоченный) представитель отказался от того или иного вида, формы и объема мероприятий, предусмотренных ИПРА инвалида (ИПРА ребенка-инвалида).

- Инвалид (ребенок-инвалид) либо законный (уполномоченный) представитель отказался от реализации ИПРА инвалида (ИПРА ребенка-инвалида) в целом.

- Причины неисполнения мероприятий, предусмотренных ИПРА инвалида (ИПРА ребенка-инвалида), при согласии инвалида (ребенка-инвалида) либо законного (уполномоченного) представителя на их реализацию.

 По каждому невыполненному мероприятию должны указываться причины неисполнения мероприятий, предусмотренных ИПРА инвалида (ИПРА ребенка-инвалида).

Ограничения и валидации

Передача сведений выписки из ИПРА исполнителю ИПРА, с указанием исполнителей, сроков исполнения происходит в 3-дневний срок.

Сводная информация направляется в ГИС ФКУ МСЭ в течение пяти дней с даты исполнения мероприятий, предусмотренных ИПРА инвалида, ИПРА ребенка-инвалида, но не позднее одного месяца до окончания срока действия ИПРА инвалида, ИПРА ребенка-инвалида.

Модернизация отчета по мониторингу выполнения индивидуальных программ реабилитации и абилитации инвалидов.

Реализация доступа ко всем картам индивидуальных программ реабилитации и абилитации инвалида в списке пациентов.

Очистка логов сессий экспорта карт администратором.

Добавление функционала удаления карты и мероприятий администратором системы.

Импорт карт с систему даже при отсутствии СНИЛСа в файлах из витрины МСЭ.

Реализовать частный вариант отнесения импортируемых карт ИПРА для детей-инвалидов направленных Республиканской больницей. (Если импортируемая карта ребенка до 18 лет и в сведениях о направлении стоит Республиканская больница, то такую карту относить к Республиканской детской больнице).

Реализовать частный вариант экспорта карт в витрину МСЭ по набору конкретных пациентов.

# Параметры предоставления **электронного сервиса «Региональная медицинская информационная система Республики Алтай»**

* 1. Общие сведения
		1. Работы (услуги) по эксплуатации Региональной медицинской информационной системы (РМИС) должны выполняться (оказываться) для всех элементов, указанных в настоящем Техническом задании.
		2. Услуги включают в себя:
			1. Оказание операторских услуг (выполняются заказчиком);
			2. Техническую поддержку пользователей РМИС;
1. Подлежащие сопровождению функциональности в составе РМИС, описаны выше.
	* 1. Порядок оказания услуг регламентируется Техническим заданием определяющим состав, объемы и параметры качества оказываемых услуг по обеспечению функционирования Системы.
		2. Услуги по технической поддержке пользователей, описанные в пунктах 2.3 Технического задания оказываются Исполнителем по отношению ко всем функциональностям Системы.
		3. В пункте 2.4 Технического задания описывается порядок проведения регламентных и аварийно-восстановительных работ.
		4. Термины и сокращения

Таблица 1. Термины и сокращения

|  |  |
| --- | --- |
| SLA | Показатели уровня качества оказания услуг |
| Вторая линия технической поддержки (2ЛП) | Служба Исполнителя для обработки Запросов, поступающих от Первой линии технической поддержки, и выполнения регламентных и неотложных работ в рамках сервисного сопровождения |
| Инициатор Обращения  | Пользователь РМИС, инициировавший подачу Обращения |
| Исполнитель  | Организация, предоставляющая услуги второй и третьей линии поддержки по техническому обслуживанию и сопровождению ПО РМИС на основании и в объёме заключенного Контракта |
| МО | Медицинская организация  |
| Обработка Обращения  | Комплекс мероприятий, направленных на предоставление Решения по Обращению |
| Обращение  | Оформленный специалистом 1ЛП запрос на консультацию, модификацию или устранение ошибки, содержащий все необходимые сведения для его обработки |
| Оператор РМИС  | БУЗ РА «Медицинский информационно-аналитический центр» |
| Первая линия технической поддержки (1ЛП) | Служба заказчика для взаимодействия с Пользователями и первичной обработки Обращений в рамках сервисного сопровождения  |
| ПО | Программное обеспечение  |
| Пользователь | Cпециалист МО, допущенный к использованию РМИС в рамках исполнения должностных обязанностей |
| Решение по Обращению | Предоставленная информация или совершённые действия, направленные на устранение причины Обращения |
| РМИС , Система | Региональный медицинская информационная система  |
| СТП | Служба технической поддержки РМИС  |
| Стороны  | Сторона Заказчика и Сторона Исполнителя, указанные по тексту совместно |
| СУЗ  | Система учета запросов Исполнителя  |
| Третья линия технической поддержки (3ЛП) | Служба Исполнителя для обработки Запросов, поступающих от Второй линии технической поддержки, связанных с доработкой программного кода РМИС  |
| ЦОД | Центр обработки данных  |
| УЗ | Учетная запись  |

Оказание операторских услуг по обеспечению функционирования РМИС (выполняется заказчиком)

Требования по порядку оказания услуг

Запросы могут быть отнесены к одному из следующих типов:

Таблица 2. Типы Запросов

|  |  |
| --- | --- |
| **Тип** | **Описание типа** |
| Инцидент  | Любое событие, не являющееся частью нормальной работы услуги/сервиса, ведущее/ способное привести к остановке услуги или снижению уровня ее качества. |
| Информационный запрос  | Обращение, не связанное с возникновением инцидента, содержащее запрос на предоставление информации о работе или документации о РМИС . |
| Запрос на изменение  | Обращение, связанное с необходимостью:- внесения изменений в существующие функциональные возможности РМИС в связи с изменениями федеральных нормативно-правовых актов; - разработки отчетной формы, не требующие доработки (изменения) РМИС ; - разработки протокола осмотра врачей, не требующие доработки (изменения) РМИС ; - загрузки региональных справочников и классификаторов и выполнения других общесистемных региональных настроек. |

Все контакты по вопросам сервисного сопровождения РМИС осуществляются исключительно с сотрудником Первой линии технической поддержки.

В случае, если при обработке Обращения выявилась необходимость привлечения 2-й и последующих линий технической поддержки, оформляется обращение в СУЗ Исполнителя.

В зависимости от типа Запроса, описание должно содержать все данные, необходимые для его решения:

Таблица 3. Требования к описанию Обращения

| Тип  | Описание |
| --- | --- |
| Для всех типов Запросов | * наименование функциональности РМИС .
 |
| Инцидент | * пошаговое перечисление действий, выполнение которых повлекло за собой возникновение ошибки;
* снимок экрана с ошибкой;
* наименование экранной формы и ссылка на страницу, где была зафиксирована ошибка;
* техническую информацию об ошибке (содержимое консоли интернет-браузера на момент возникновения ошибки; текст ошибки, отображаемый Системой)
* дополнительные файлы (в случае необходимости);
* описание желаемого результата исправления ошибки.
 |
| Запрос на изменение | * основание для выполнения модификации;
* описание требуемой модификации;
* описание полей;
* описание порядка отбора данных для формирования отчетов;
 |

Обращение, оформленное по установленной форме, направляется сотрудником 1ЛП в СТП Исполнителя.

Техническая поддержка пользователей РМИС и Заказчика (выполняется исполнителем)

Услуги, описанные в данном пункте, оказываются Исполнителем в рамках сервисного сопровождения РМИС.

* + - Состав услуги

Услуги по технической поддержке включают:

1. обеспечение работоспособности и доступности РМИС, мониторинг работоспособности системы;
2. решение инцидентов по информационным системам РМИС;
3. поиск и устранение проблем в случае неработоспособности ПО РМИС;
4. восстановление работоспособности прикладного ПО РМИС при сбоях;
5. выполнение регламентных работ, направленных на обеспечение заданного уровня надежности и бесперебойности функционирования РМИС
	* + Требования по порядку оказания услуг

Запрос должен проходить через следующие основные состояния: «Назначен», «Выполняется», «Решен», «Закрыт». Дополнительное состояние запроса: «В ожидании».

Перевод Запроса в состояние «Решен» требует подтверждения инициатора Запроса. Подтверждение состояния «Решен» инициатором запроса происходит после изменения статуса и оповещения инициатора запроса об изменении статуса по e-mail. После предоставления решения по Запросу, Инициатор должен проверить решение в течение трех рабочих дней. В случае, если инициатор не согласен с решением, Запрос возвращается в статус «Назначен». Инициатор должен предоставить обоснование несогласия с решением. Если несогласие с решением Запроса не связано с исходным содержанием, то Запрос переводится в статус «Закрыт» и регистрируется новый Запрос.

Перевод Запроса в статус «Закрыт» может происходить либо после подтверждения Инициатором статуса «Решен», либо автоматически через 3 рабочих дня после перевода запроса в статус «Решен» в случае отсутствия подтверждения.

Закрытые Запросы повторному открытию не подлежат.

Время решения – это время, затрачиваемое с момента регистрации Запроса до момента предоставления решения.

Расчет времени решения производится с момента создания Запроса до момента перехода в статус «Решен». В случае перехода запроса в статус «Закрыт» счетчик прекращает свою работу и не подлежит возобновлению. В случае перевода запроса в статус «В ожидании» счетчик приостанавливается. В случае возврата запроса в статус «Назначен» счетчик возобновляет отсчет с места остановки.

В зависимости от необходимости привлечения Третьей линии технической поддержки, нормативное время решения Запросов устанавливается согласно п.2.3.3. Третья линия технической поддержки может быть привлечена Исполнителем в случае необходимости внесения изменений в программный код Системы.

Перевод Запроса в статус «В ожидании» возможен в следующих случаях:

- В случае, если в Запросе отсутствуют сведения, достаточные для его успешного решения;

- для продолжения работ по решению требуется действие со стороны инициатора запроса, либо Заказчика, либо стороннего поставщика системного ПО и оборудования;

- при необходимости проведения обновления Системы, либо выполнения технологических работ;

- в случае отсутствия согласования Заказчика, либо Оператора РМИС на проведение работ, не смотря на техническую готовность их проведения.

Срок подготовки и предоставления дополнительной информации инициатором не может превышать трех рабочих дней, в противном случае Запрос автоматически будет переведен в статус «Закрыт».

При запросе дополнительной информации или требовании выполнения действий со стороны Заказчика, или третьих лиц необходимо указывать:

1. Регистрационный номер Запроса;
2. Перечень дополнительной информации и список действий, которые необходимо проделать.

Все обращения по Запросу, зарегистрированному в СУЗ ранее и переведённому в статус «Закрыт», регистрируются, как вновь поступившие, и обрабатываются согласно требованиям данного технического задания.

* + - Приоритизация запросов

К инцидентам 0 (недопустимого) приоритета относятся отказы компонентов базового функционала: Ф 16. Управление взаиморасчетами за оказанные медицинские услуги, ЭМК, Электронное расписание, обеспечивающим формирование финансового результата медицинских организаций в течении 2 астрономических часов.

Данный уровень приоритета означает непригодность электронного сервиса к эксплуатации в целом на протяжении календарного платежного периода. Время устранения такого отказа - в течение текущих календарных 1 суток с момента отказа.

К инцидентам 1 (критического) приоритета относятся аварийные внештатные ситуации, связанные с полной недоступностью ведения персонифицированного учета вызванной недоступностью информационной системой для всех пользователей. Время решения данных инцидентов 4 астрономических часа или 2 рабочих дня в случае необходимости привлечения 3ЛП для решения.

К инцидентам 2 (высокого) приоритета относятся ситуации, связанные с невозможностью ведений персонифицированного учета в одной или нескольких функциональностях информационной системы для всех пользователей. Время решения данных инцидентов 24 рабочих часа или 7 рабочих дней в случае необходимости привлечения 3ЛП для решения.

К запросам 3 (среднего) приоритета относятся:

1. Ошибки, связанные с ведением персонифицированного учета у отдельных пользователей;
2. Ошибки, не связанные с ведением персонифицированного учета;
3. Информационные запросы;

Время решения данных обращений 10 рабочих дней или 45 рабочих дней в случае необходимости привлечения 3ЛП для решения.

К запросам 4 (низкого) приоритета относятся:

1. запросы на изменение.

Время решения данных обращений 20 рабочих дней или 60 рабочих дней[[1]](#footnote-2) при необходимости привлечения 3ЛП для решения.

По результатам проведённого анализа Запроса специалистами СТП тип и приоритет может быть изменен.

* + - Требования по качеству оказания услуг

Уровень оказания Сервиса определяется качественными и количественными параметрами. Параметры оказания услуги определены в Таблице 6.

Таблица 4. Целевые показатели

|  |  |
| --- | --- |
| Показатель | Целевое значение |
| Временной режим доступности сопровождаемой информационной системы | 24 часа в сутки, 7 дней в неделю, не менее 95% за отчетный период без учета времени простоя при плановых профилактических работах |
| Временной режим регистрации Запросов | круглосуточно (24х7) |
| Временной режим устранения инцидентов 1-го приоритета | круглосуточно (24х7) |
| Временной режим обработки Запросов и устранения инцидентов других приоритетов | с 09:00 до 18:00 часов в рабочие дни (по местному времени Заказчика). |
| Время проведения регламентных работ | Для проведения плановых работ, имеющих риск прерывания работоспособности сервиса, должно выделяться технологическое окно с 20:00 до 07:00 следующего дня (по местному времени Заказчика) |

Исполнение запроса на изменение, требующего внесения изменений в программный код системы, осуществляется в рамках вывода релиза.

Требования к качеству технической поддержки (для не менее указанного процента запросов):

|  |  |  |
| --- | --- | --- |
| Приоритет запроса | Время решения (без 3ЛП) | Время решения (с 3ЛП) |
| 1 | 95% | 90% |
| 2 | 90% | 85% |
| 3 | 80% | 75% |
| 4 | 75% | 70% |

Количественные параметры оказания услуги по технической поддержке, при которых должны быть соблюдены требования по качеству оказания услуг:

1. Максимальное количество обращений типа «Инцидент» - 50 (шт./ месяц.)
2. Максимальное количество обращений типа «Информационный запрос» - 30 (шт./ месяц)
3. Максимальное количество обращений типа «Запрос на изменение» - 20 (шт./ месяц)
4. Время нахождения обращения на 1ЛП не учитывается при расчете времени решения запроса.

При превышении максимального количества обращений, указанного в настоящем ТЗ, Исполнитель оказывает услуги без соблюдения SLA.

 Порядок проведения регламентных и аварийно-восстановительных работ

* + - Услуги по профилактике и предотвращению аварий
		- Состав услуг

Услуга по профилактике и предотвращению аварий состоит из:

- услуг по отслеживанию доступности и работоспособности РМИС для своевременного предотвращения и решения аварий;

Требования по порядку оказания услуг

Исполнитель реализует все необходимые мероприятия для обеспечения функционирования РМИС в соответствии с требованиями настоящего Технического задания.

Исполнитель осуществляет постоянный аудит существующих и выпускаемых версий программных компонент РМИС всех уровней и принимает решение о необходимости обновления ПО РМИС . Исполнитель должен планировать работы по профилактике и предотвращению аварий таким образом, чтобы минимизировать возможность остановок функционирования систем во время указанных работ (постепенное обновление ПО с переключением нагрузки между серверами без прекращения функционирования ИС).

Услуги по сопровождению изменений

Состав услуг

Услуга по сопровождению изменений включает в себя:

- ввод новых версий модулей РМИС , входящих в настоящий Контракт;

- проведение регламентных и аварийно-восстановительных работ для обеспечения устойчивого функционирования РМИС ;

Требования по порядку оказания услуг

Исполнитель обеспечивает полный комплекс мероприятий, необходимых для ввода в эксплуатацию новых версий РМИС .

Изменения могут проводиться:

в рамках оказания услуг по эксплуатации РМИС (такие изменения проводятся в рабочем порядке согласно требованиям Технического задания);

в рамках приемки в эксплуатацию новых версий РМИС .

Исполнитель осуществляет изменения режима функционирования РМИС по запросу Заказчика в случаях, если:

1. требуется проведение финальных испытаний или ввод в эксплуатацию новых версий систем или функций;
2. на режим функционирования влияют изменения законодательства или распоряжения, постановления и приказы органов исполнительной власти РФ;
3. требуется подключение новых систем и участников к РМИС .

Исполнитель проводит экспертную оценку всех технологических изменений и классифицирует на 2 класса:

«а»- изменения с потенциальной опасностью незапланированной остановки/необходимостью остановки сервиса ИС;

«б» - изменения без опасности остановки сервиса.

Изменение класса «а» проводится Исполнителем после оповещения Заказчика во время, указанное в Таблице 4

По изменению класса «а» пользователи уведомляются по электронной почте.

Изменения класса «б» осуществляются в любое время без оповещения заказчика и уведомления пользователей.

В течение 1 часа после завершения выполнения изменения класса «а» Исполнитель информирует уполномоченных и заинтересованных представителей Заказчика по электронной почте.

Информирование заказчика о проведении изменений происходит не позднее чем за 6 часов до начала работ. В случае несогласия с проведением работ, заказчик должен предоставить ответ на электронное письмо не позднее чем за 2 часа до начала работ. Аварийно-восстановительные работы по инцидентам 1 приоритета являются исключением и проводятся оперативно без предварительного оповещения о времени подготовки и проведения работ.

Время проведения изменений, по которым было произведено оповещение Заказчика в установленном порядке не учитывается в итоговых отчетах по доступности систем, затронутых изменениями.

Заказчик может установить мораторий на проведение всех изменений в РМИС на определенное время. На время моратория счетчик времени решения запросов, требующих внесения изменения, приостанавливается. Мораторий не распространяется на проведение изменений в рамках аварийно-восстановительных работ.

**Методика оценки качества оказания услуг**

Контроль за исполнением требований технического задания осуществляется Заказчиком при помощи создания запросов при обнаружении сбоев или несоответствия сервиса заявленным требованиям. Оценка качества услуг производится на основании сроков обработки запросов приоритета «Критический», «Высокий», «Средний» и «Низкий».

На оценку качества услуг не влияют инциденты, произошедшие по следующим причинам:

* отказ электропитания или обрыв абонентской линии связи в помещении Заказчика, либо на участке линии связи;
* нарушение работы оборудования, находящегося вне зоны ответственности Исполнителя;
* проведение Исполнителем в согласованные с Заказчиком сроки планово-профилактических работ, если порядок их согласования и срок выполнения соответствует условиям, указанным в настоящем Техническом задании;
* проведение Заказчиком регламентных либо неотложных ремонтных работ;
* неработоспособность интегрированных с сервисами РФ ЕГИСЗ модулей, функций и информационных систем, обслуживание которых не является предметом настоящего Договора.

Оценка качества оказания услуги осуществляется в следующем порядке:

Отклонением является превышение фактического времени обработки инцидента приоритета «Критический», «Высокий», «Средний» и «Низкий» от планового срока, приведенного в Таблице 7. Время обработки инцидента, находящегося вне зоны ответственности Исполнителя, не входит в расчет нормативного времени устранения инцидента Исполнителем.

Общим временем отклонения является сумма времени Отклонений по всем запросам приоритета «Критический» за отчетный период оказания услуги.

Для оценки качества оказания услуг применяется Показатель уровня качества (К).

Расчет Показателя уровня качества (К) выполняется Исполнителем по следующей формуле:

,

где

 – Общее время отклонения в часах,

 – Длительность отчетного периода в часах.

В случае, если Показатель уровня качества услуг ниже значения 0.95, Заказчик имеет право на проведение перерасчета стоимости оказание услуги за отчетный период.

Приложение № 3

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

*от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019*

**Техническое задание на оказание услуг по сопровождению электронного сервиса РС ЕГИСЗ «Мониторинг здравоохранения»**

Исполнитель осуществляет техническую поддержку работы ЭС «Мониторинг здравоохранения» (далее – ЭС МЗ) и непрерывно обеспечивает пригодность ЭС к промышленной эксплуатации, в том числе:

* проведение аналитики зарегистрированных заявок на доработки ЭС МЗ;
* консультационную поддержку;
* диагностику работоспособности программного обеспечения ЭС МЗ;
* поиск и устранение проблем в случае невозможности работы ЭС МЗ в промышленном режиме;
* восстановление работоспособности прикладного программного обеспечения ЭС МЗ при сбоях;
* обновление ПО ЭС МЗ до новых версий (плановое, внеплановое);
* предоставление отчетных форм в установленные сроки: федеральных форм установленные в Порядке сроком, утвержденные Минздравом России; региональных и произвольных форм установленные Заказчиком сроком. Заказчик за 10 календарных дней уведомляет Исполнителя об обновлении отчетных форм; за 20 календарных дней уведомляет о реализации новых форм через техническую поддержку в виде заявки. Заказчик предоставляет печатные формы, увязки и аналитику формирования форм. Исполнитель в рамках технического задания реализовывает 10 отчетных форм.

Исполнитель реализовывает информационное и документарное сопровождение ЭС МЗ в виде предоставления на бумажном носителе актуальных руководств пользователя, руководств администратора, подготовку и передачу Заказчику разработанных вебинаров, учебных материалов по соответствующим вопросам работы с ЭС МЗ.

При исполнении требований настоящего технического задания Исполнитель обязан учесть общие требования к оказанию комплексной услуги по обеспечению функционирования электронных сервисов РС ЕГИСЗ.

**Назначение электронного сервиса РС ЕГИСЗ «Мониторинг здравоохранения»**

Система предназначена для оперативного мониторинга статистических и качественных показателей (индикаторов) сферы здравоохранения.

Система обеспечивает возможность сбора первичной информации муниципальными и региональными органами управления в сфере здравоохранения, позволяет получить детализированные статистические сведения как по отдельно взятому медицинскому учреждению, так и любой группе учреждений, автоматизирует и оптимизирует процессы получения справочной статистической информации.

Автоматизация сбора статистической отчетности на уровне учреждений сферы здравоохранения позволяет обеспечить консолидацию информации в нужном объёме на уровне муниципальных районов.

**Цели электронного сервиса РС ЕГИСЗ «Мониторинг здравоохранения»**

Основными целями являются:

* формирование единого информационного пространства для учреждений сферы здравоохранения;
* расширение общественного участия в управлении сферой здравоохранения;
* мониторинг деятельности учреждений сферы здравоохранения в режиме реального времени;
* повышение оперативности, эффективности и качества управления в сфере здравоохранения;
* снижение трудоемкости, как на этапе первичного заполнения данных, так и на этапе обработки информации и формирования аналитических выводов;
* увеличение качества информации и детализации статистических сведений за счет получения информации от первоисточника и ее дальнейшая актуализация;
* сокращение транспортных расходов учреждений сферы здравоохранения;
* повышение информационной открытости и прозрачности сферы здравоохранения;
* создание предпосылок для интеграции информационных ресурсов на уровне региона;
* повышение эффективности взаимодействия ведомственных информационных систем.

**Общие требования к электронному сервису**

Электронный сервис РС ЕГИСЗ «Мониторинг здравоохранения» должен содержать всю необходимую функциональность для работы с иерархией сдачи статистической и экономической отчетности среди списка учреждений.

В электронном сервисе должен быть функционал, позволяющий обеспечить выгрузку данных федеральной отчетности для ИС Медстат Москва в соответствующем формате dbf (всех федеральных форм одним файлом выгрузки и перечня форм по отдельности).

В Системе должно быть реализовано предупреждающее сообщение к запуску операции «Очистить все данные в форме».

Электронный сервис должен обеспечивать контроль целостности данных.

Должна поддерживать функцию подписи отчетных форм электронно -цифровой подписью.

* В электронном сервисе должна быть предусмотрена печать всех отчетных форм по настроенным шаблонам. Должна быть реализована выгрузка печатных форм с использованием офисных пакетов из Единого реестра российских программ.

Электронный сервис должен содержать следующие подсистемы:

* сбора отчетности;
* контроля данных;
* подсистема процедуры утверждения и экспертизы отчетных форм;
* подсистема формирования итоговых (сводных) отчетов;
* подсистема мониторинга и анализа данных;
* подсистема печати;
* подсистема нормативно-справочной информации;
* подсистема ролевого доступа;
* подсистема выгрузки данных в смежные системы;
* подсистема сроков сдачи отчетности;
* подсистема администрирования;
* подсистема журналирования;
* подсистема «Конструктор отчетных форм»;
* подсистема сообщений.

В электронном сервисе должна быть реализована отчетная форма, для контроля достижения показателя назначения сервиса. Основным показателем является количество подписанных электронно-цифровой подписью отчетных форм за отчетные периоды: «за 1 квартал», «за 1 полугодие», «за 9 месяцев», «за год». Формат формы должен быть согласован с Заказчиком в рабочем порядке.

**Состав отчетных форм**

Таблица 1 - Состав федеральных отчетных форм.

|  |  |
| --- | --- |
| **Код формы** | **Наименование формы** |
| 10 | «Сведения о заболеваниях психическими расстройствами и расстройствами поведения (кроме заболеваний, связанных с употреблением психоактивных веществ)» |
| 11 | «Сведения о заболеваниях наркологическими расстройствами» |
| 12 | «Сведения о числе заболеваний, зарегистрированных у больных, проживающих в районе обслуживания лечебного учреждения» |
| 13 | «Сведения о прерывании беременности» |
| 14 | «Сведения о деятельности стационара» |
| 14-ДС | «Сведения о деятельности дневных стационаров лечебно-профилактического учреждения» |
| 15 | «Сведения о медицинском обслуживании лиц, подвергшихся воздействию радиации в связи с аварией на Чернобыльской АЭС и подлежащего включению в российский государственный медико-дозиметрический регистр» |
| 16-ВН | «Сведения о причинах временной нетрудоспособности» |
| 19 | «Сведения о детях - инвалидах» |
| 1-Д | «Сведения о численности беспризорных и безнадзорных несовершеннолетних, помещенных в лечебно-профилактические учреждения» |
| 1-РБ | Сведения об оказании медицинской помощи гражданам республики Беларусь |
| 30 | «Сведения о лечебно-профилактическом учреждении» |
| 31 | «Сведения о медицинской помощи детям и подросткам-школьникам» |
| 32 | «Сведения о медицинской помощи беременным, роженицам и родильницам» |
| 33 | «Сведения о больных туберкулезом» |
| 34 | «Сведения о больных заболеваниями, передаваемыми преимущественно половым путем, грибковыми кожными болезнями и чесоткой» |
| 36 | «Сведения о контингентах психически больных» |
| 36-ПЛ | «Сведения о контингентах больных с психическими расстройствами, находящихся на активном диспансерном наблюдении и принудительном лечении» |
| 37 | «Сведения о больных алкоголизмом, наркоманиями, токсикоманиями» |
| 38 | «Сведения о работе отделений судебно-психиатрической экспертизы» |
| 41 | «Сведения о доме ребенка» |
| 42 | «Отчет врача\бюро судебно-медицинской экспертизы» |
| 45 | «Отчет туберкулезного санатория для взрослых» |
| 47 | «Сведения о сети и деятельности учреждений здравоохранения» |
| 53 | «Отчет о медицинском наблюдении за лицами, занимающимися физкультурой и спортом» |
| 54 | «Отчет врача детского дома, школы-интерната о лечебно-профилактической помощи воспитанникам» |
| 55 | «Сведения о деятельности учреждения здравоохранения (медицинского формирования), принимавшего участие в ликвидации чрезвычайных ситуаций» |
| 56 | «Сведения о сети и кадрах службы медицины катастроф министерства здравоохранения Российской федерации» |
| 57 |  «Сведения о травмах, отравлениях и некоторых других последствиях воздействия внешних причин» |
| 61 | «Сведения о контингентах больных ВИЧ-инфекцией» |
| 68 | Сведения о деятельности центра здоровья |
| 7 | «Сведения о заболеваниях злокачественными новообразованиями» |
| 70 | «Сведения о деятельности центра медицинской профилактики» |
| 7-т | «Сведения о травматизме на производстве и профессиональных заболеваниях» |
| 7-т-приложение | «Сведения о распределении несчастных случаев на производстве» |
| 8 | «Сведения о заболеваниях активным туберкулезом» |
| 9 | «Сведения о заболеваниях, передаваемых преимущественно половым путем, грибковых кожных заболеваниях и чесоткой» |

Таблица 2 - Состав региональных отчетных форм.

|  |  |
| --- | --- |
| **Код формы** | **Наименование формы** |
| МЗ\_БСК | Мониторинг показателей заболеваемости и смертности населения от болезней системы кровообращения (БСК) |
| МЗ\_Кредитор\_задолж | Сведения о кредиторской задолженности |
| МЗ\_Мон\_по\_сниж\_смертности | Мониторинг по снижению смертности |
| МЗ\_Отчет\_ФАПа | Отчет фельдшерско-акушерского пункта(ФАП) |
| МЗ\_Отчет\_о\_дисп\_дет\_от\_0\_17\_лет\_ежекв | Отчет о диспансеризации детей от 0-17 лет (ежеквартально) |
| МЗ\_Отчет\_о\_дисп\_детей\_сирот\_под\_опекой\_ежекв | Отчет о диспансеризации детей-сирот, находящихся под опекой (ежеквартально) |
| МЗ\_Отчет\_о\_пров\_аудиолог\_скрин\_ежемес | Отчет о проведении аудиологического скрининга (ежемесячно) |
| МЗ\_Отчет\_по\_ежемес\_мон\_эфф\_мед\_деят | Отчет по мониторингу эффективности мед. деятельности (ежемесячно) по 86-р |
| МЗ\_Отчет\_по\_еженед\_мон\_эфф\_мед\_деят | Отчет по еженедельному мониторингу эффективности мед. деятельности (еженедельно) по 86-р |
| МЗ\_Отчет\_проведении\_медосмотров\_детей | Отчет о проведении периодических и профилактических мед. осмотров детей (ежемесячно) |
| МЗ\_Платн\_мед\_услуги | Сведения о платных медицинских услугах |
| МЗ\_Пос\_и\_расх\_ден\_ср\_по\_род\_серт | Поступление и расходование денежных средств по родовым сертификатам |
| МЗ\_Профосмотры | Отчет по профосмотрам (ежемесячно,с нарастанием) |
| МЗ\_Сведения\_о\_родившихся | Сведения о родившихся (ежемесячно) |
| МЗ\_Сред\_зп\_ПНП\_Здоровье | Отчет по средней заработной плате ПНП "Здоровье" |
| МЗ\_ТПГГ | Сведения о формировании и выполнении территориальной программы государственных гарантий |
| МЗ\_Цел\_пок\_структ\_преобр\_сети\_мед\_орг | Целевые показатели структурных преобразований сети медицинских организаций |
| Отчет\_о\_заболеваемости\_новорожденных | Отчет о заболеваемости новорожденных (ежемесячно) |
| Форма\_П4 | Сведения о численности, заработной плате и движении работников (Форма П-4) |
| Неонатальный скрининг | Информация об обследовании новорожденных детей в регионе |
| Расшифровка МЗ\_30\_штаты | Расшифровка Таблиц 30 формы |
| Сведения о профилактических медицинских осмотрах несовершеннолетних | Сведения о профилактических медицинских осмотрах несовершеннолетних |
| МЗ\_ЗП\_здрав | Сведения о численности и оплате труда работников сферы здравоохранения по категориям персонала |

|  |  |
| --- | --- |
| От Заказчика: | От Исполнителя: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_ / |

Приложение № 4

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

*от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019*

**Требования к оказанию услуг по сопровождению электронного сервиса РС ЕГИСЗ «АХД»**

**Исполнитель осуществляет техническую поддержку работы ЭС «АХД»** и непрерывно обеспечивает пригодность ЭС к промышленной эксплуатации, в том числе:

* проведение аналитики зарегистрированных заявок на доработки ЭС АХД;
* консультационную поддержку;
* диагностику работоспособности программного обеспечения ЭС АХД;
* поиск и устранение проблем в случае невозможности работы ЭС АХД в промышленном режиме;
* восстановление работоспособности прикладного программного обеспечения ЭС АХД при сбоях;
* обновление прикладного ПО ЭС АХД до новых версий (плановое, внеплановое).

Исполнитель реализовывает информационное и документарное сопровождение ЭС АХД в виде предоставления на бумажном носителе актуальных руководств пользователя, руководств администратора, подготовку и передачу Генеральному Заказчику разработанных вебинаров, учебных материалов по соответствующим вопросам работы с ЭС АХД.

При исполнении требований настоящего технического задания Исполнитель обязан учесть общие требования к оказанию комплексной услуги по обеспечению функционирования электронных сервисов РС ЕГИСЗ.

* Назначение электронного сервиса РС ЕГИСЗ «АХД»
* Сбор данных о результатах административно-хозяйственной деятельности медицинских организаций;
* Хранение данных о результатах административно-хозяйственной деятельности медицинских организаций;
* Выгрузка данных о результатах административно-хозяйственной деятельности медицинских организаций в федеральный сервис ЕГИСЗ АХД;
* Мониторинг данных о результатах административно-хозяйственной деятельности медицинских организаций.
* Требования к подключению организаций к электронному сервису РС ЕГИСЗ «АХД»
* Функциональные требования к электронному сервису.
* Прохождение предусмотренных процедур авторизации и идентификации для начала работы с подсистемой;
* Ведение перечня медицинских организаций, предоставляющих сведения в подсистему;
* Определение отчетного периода, за который медицинские организации предоставляют необходимые сведения (в подсистеме поддерживается месячная дискретность отчетного периода);
* Открытие и закрытие возможности предоставления данных от медицинских организаций по:
* выбранному отчетному периоду;
* выбранным учреждениям;
* Визуализация в журнале загрузок перечня операций загрузки данных от медицинских организаций и их результатах;
* Отмена загрузки данных медицинской организации и удаление загруженных им данных;
* Выгрузка данных о результатах административно-хозяйственной деятельности медицинских организаций в федеральный «облачный» сервис АХД, при этом обеспечивается выгрузка данных за все медицинские организации, которые загружали данные за указанный отчетный период.

При реализации задачи сбора данных для уполномоченного пользователя от медицинской организаций должны быть обеспечены следующие функциональные возможности:

* Прохождение предусмотренных процедур авторизации и идентификации для начала работы с подсистемой;
* Выполнение операции загрузки XML–файлов в подсистему, представляющих собой выгрузку из автоматизированных информационных систем: бухгалтерского учета «ПАРУС» версии 7.\*, 1С версии 8.\*/7.\*, посредством предоставленных Исполнителем средств конвертации данных в необходимый формат загрузки из указанных систем;
* Визуализация сведений по каждой операции выполненной загрузки данных медицинской организации и её результату;
* Неоднократная загрузка данных, при этом ранее загруженные данные медицинской организации за этот отчетный период удаляются;
* Модификация загруженных данных в Веб-интерфейсе подсистемы, при этом ранее загруженные данные медицинской организации за этот отчетный период сохраняются.

В процессе загрузки данных в подсистему должна быть обеспечена проверка загружаемых данных на соответствие значениям словарей подсистемы. Данные, не соответствующие значениям словарей подсистемы, не загружаются. Данные, прошедшие проверку, сохраняются в таблицах подсистемы.

При реализации задачи хранения данных в подсистеме должно обеспечиваться сохранение данных, поступающих от учреждения в виде отдельного «снимка данных», привязанного к отчетному периоду. Не допускается модификация данных одного отчетного периода при загрузке данных другого отчетного периода.

При реализации задачи выгрузки данных о результатах административно-хозяйственной деятельности медицинских организаций в федеральный сервис ЕГИСЗ АХД, при этом обеспечивается выгрузка данных за медицинские организации, которые загружали данные за указанный отчетный период.

При реализации задачи мониторинга данных в подсистеме должно обеспечиваться формирование следующих многомерных отчетов:

* Остатки учреждений. Показатель остатки в разрезе кодов бюджетной классификации и отчетных периодов;
* Обороты учреждений. Показатель обороты в разрезе кодов бюджетной классификации и отчетных периодов;

**Требования к конвертации данных из систем ведения учета**

Должна быть обеспечена возможность конвертации данных из автоматизированных информационных систем «ПАРУС» версии 7.\* и 1С версии 7.\*/8.\*, используемых в медицинских организациях. Данные должны соответствовать действующему регламенту «Описание объема и состава пакета данных, передаваемых в Федеральный сервис АХД от медицинских организаций» в составе:

* Файл данных об остатках на счетах бюджетного учета на задаваемую дату;
* Файл данных об оборотах по счетам бюджетного учета за задаваемый период;

В случае использования в медицинских организациях иных автоматизированных систем, Исполнитель должен провести оценку возможности конвертации данных и необходимости осуществления разработки дополнительных средств конвертации.

**Требование к выгрузке кадровых данных и заработной платы.**

В электронном сервисе должна быть обеспечена возможность заполнения формы ЗП Здрав в ручном режиме. На основанные данных внесенных в форму, должен формироваться XML файл в формате ЕГИСЗ.АХД.

Файл XML формируется на основании статистической формы ЗП здрав - Сведения о численности и оплате труда работников сферы здравоохранения по категориям персонала. Описание формата в Приложении А.

**Требования к техническому обеспечению электронного сервиса**

При работе пользователей с электронным сервисом должна обеспечиваться модель «облачных» технологий.

Все системные компоненты электронного сервиса Исполнитель должен разместить в «облачной» платформе. Электронный сервис должен быть доступен пользователям посредством веб – интерфейсов по модели «Программное обеспечение как услуга».

Для контроля полноты показателя назначения сервиса Исполнитель предоставляет отчетную форму, в котором будет отражена загрузка в ЭС АХД данных из автоматизированных информационных систем медицинских организаций. Формат отчетной формы должен быть согласован с Генеральным Заказчиком в рабочем порядке.

*Приложение А*

*к Приложению №4*

*к Договору №\_\_\_\_\_\_\_\_\_от \_\_\_\_\_\_\_\_\_ 2019 г.*

Описание формата xml-файла

| **Описание значения** | **Вид значения** | **Тип значения** | **xml** | **Обязательность** | **Примечание** |
| --- | --- | --- | --- | --- | --- |
| Запись | Элемент |  | Report | да |  |
|  Код | Атрибут | string | code | нет |   |
| Форма | Атрибут | string | form | нет |  |
| Шифр | Атрибут | string | shifr | да | Фиксировано – q\_p\_zdrav |
| Год | Атрибут | string | year | да | Год периода, за который осуществляется выгрузка |
| Период | Атрибут  | string | period | да | «01»+Номер месяца (два символа), за который с начала года (включая этот месяц) осуществляется выгрузка(например, 0103) |
| Версия | Атрибут | string | version | нет |   |
| Титул | Элемент |  | title | да |   |
| Наименование | Атрибут  | string | name | да | Наименование контрагента |
| Адрес организации | Атрибут | integer | org\_adres | нет |   |
|  ОКПО | Атрибут | string | okpo | нет |  |
|  Тип учреждения | Атрибут | string | Org\_type | да | Значения:АвтономноеБюджетноеКазенное |
| Должность | Атрибут | string | responsible\_post | нет |   |
| ФИО | Атрибут |  | responsible\_fio | нет |  |
| Телефон | Атрибут | string | phone | нет |   |
| Эл почта | Атрибут | string | email | нет |   |
| ИНН | Элемент | string | inn | да |  ИНН контрагента |
| КПП | Элемент | string | kpp | да |  КПП контрагента |
| Секции | Элемент |   |  sections |  да |   |
| Секция | Элемент |   |  section |  да |   |
| Код секции | Атрибут | string | section\_code | да | Фиксировано – «1» |
| Строка | Элемент |   |  row | да |   |
| Код строки  | Атрибут | string | row\_code | да |   |
| Графа | Элемент |   |  code |  да |   |
| Код графы | Атрибут | string |  col\_code | да |   |
| Значение показателя | Атрибут | decimal | Text | да |  |

|  |  |  |
| --- | --- | --- |
| От Исполнителя:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | От Заказчика:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_ / |  |

Приложение № 5

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019

**Техническое задание на оказание услуг по сопровождению работы электронного сервиса РС ЕГИСЗ «ССМП»**

 **Общие положения**

В рамках оказания услуг по настоящему техническому заданию должна быть осуществлена техническая поддержка работы ЭС ССМП.

При исполнении требований настоящего технического задания Исполнитель обязан учесть общие требования к оказанию комплексной услуги по обеспечению функционирования электронных сервисов РС ЕГИСЗ и гарантирует совместимость не менее чем с одним браузером из Единого реестра российских программ для электронных вычислительных машин и баз данных.

**Исполнитель осуществляет техническую поддержку работы ЭС ССМП** для МО согласно таблице 2 настоящего приложения и непрерывно обеспечивает пригодность ЭС к промышленной эксплуатации, в том числе:

* проведение аналитики зарегистрированных заявок на доработки ЭС ССМП;
* ведет консультационную поддержку;
* диагностику работоспособности программного обеспечения ЭС ССМП;
* поиск и устранение проблем в случае невозможности работы ЭС ССМП в промышленном режиме;
* восстановление работоспособности прикладного программного обеспечения ЭС ССМП при сбоях;
* поддерживает полноту формирования реестров счетов за оказанную скорую медицинскую помощь из ЭС ССМП в БУЗ РА «Центр медицины катастроф»;
* полноту оформления и передачи в РМИС случая вызова бригады скорой медицинской помощи для районных медицинских организаций;
* полноту ведения журнала регистрации вызовов, полноту оформления и передачи в РМИС сигнальных листков вызовов;
* обновление прикладного ПО ЭС ССМП до новых версий (плановое, внеплановое).

Исполнителем должно быть обеспечено взаимодействие с внешними системами: МИС РС ЕГИСЗ, ИС ТФОМС РА и Унифицированным специальным программным обеспечением системы-112 (далее – УСПО - 112).

В части взаимодействия с МИС РС ЕГИСЗ для всех МО из Таблицы 2 должны быть обеспечена работоспособность сервисов интеграции, обеспечивающих:

* Получение от МИС данных о пациенте;
* Передачу сигнального листа об оказанной помощи от Системы в МИС;
* Передачу информации от Системы в МИС о госпитализации пациента бригадой скорой помощи в приемное отделение в объеме лицевой стороны сопроводительного листа формы 114-у;
* Передачу и обновление информации о результатах госпитализации от МИС в Систему в объеме обратной стороны талона формы 114-у;
* Передачу основных параметров случая вызова бригады скорой медицинской помощи, для формирования реестров счетов в РМИС.

В части взаимодействия с ТФОМС РА для БУЗ РА «Центр медицины катастроф» должны быть обеспечена выгрузка реестров счетов в соответствии с требованиями тарифного соглашения, план-задания и порядка информационного взаимодействия действующего на территории субъекта.

В части взаимодействия с УСПО — 112 должна быть обеспечена работоспособность сервиса автоматизированного межсистемного взаимодействия (интеграции) в процессе повседневной деятельности между УСПО-112 и ЭС ССМП.

Исполнитель реализовывает информационное и документарное сопровождение ЭС ССМП в виде предоставления на бумажном носителе актуальных руководств пользователя, руководств администратора, подготовку и передачу Заказчику учебных материалов по соответствующим вопросам работы с ЭС ССМП.

При возникновении любых технических или методических проблем специалист Заказчика передает техническую проблему в техническую поддержку, по выделенному бесплатному номеру. Техническая поддержка осуществляется с 9:00 до 18:00 (по местному времени Заказчика), должна быть организована на территории Республики Алтай.

**Назначение электронного сервиса РС ЕГИСЗ «ССМП»**

Сервис «ССМП» предназначен для решения следующих задач:

* Принятие быстрых и эффективных решений медицинским персоналом;
* Обеспечение централизованного персонифицированного учета пациентов, при оказании скорой медицинской помощи;
* Формирование единой методологической, информационно-аналитической и управленческой основы для реализации основных направлений и задач скорой медицинской помощи;
* Координация действий и повышение эффективности взаимодействия при оказании скорой медицинской помощи населению.
* Автоматизация и техническое сопровождение процесса формирования и выставления реестров счетов оказанной медицинской помощи.

**Цели электронного сервиса РС ЕГИСЗ «ССМП»**

Основной целью является повышение эффективности работы ССМП за счёт повышения качества и оперативности выезда, диагностики и медицинской помощи благодаря использованию автоматизированной системы, обеспечивающей:

* Долговременное хранение электронных медицинских данных;
* Освобождение сотрудников от рутинной бумажной работы и необходимости дублирования информации в различных журналах;
* Конфиденциальность информации медицинской карты;
* Повышение оперативности и эффективности работы ССМП за счет оперативного приема и обработки вызовов;
* Обеспечения диспетчерского персонала информацией о состоянии выездных бригад на любой текущий момент времени.

**Требования к электронному сервису РС ЕГИСЗ «ССМП»**

Должны быть доступны следующие функциональные возможности сервиса:

Ведение электронной карты вызова скорой медицинской помощи, в том числе:

- ввод данных с заполненных карт вызовов бригадой СМП;

- учет заполненных карт вызовов бригадой СМП;

- просмотр карты вызова скорой помощи;

- сохранение данных о вызове и оказанных услугах.

Формирование регламентированной отчетности ССМП:

- Форма 109/у;

- Форма 110/у;

- Форма 114/у;

- Форма 115/у.

Формирование произвольной аналитической выборки и оперативных отчетов по случаям оказания скорой медицинской помощи. Полнота оформления и передачи в РМИС сигнальных листков вызовов и основных параметров случая вызова бригады скорой медицинской помощи, для формирования реестров счетов в РМИС.

Реализация вышеперечисленных задач подсистемы должна быть доступна пользователям посредством веб – интерфейсов по модели «программное обеспечение как услуга».

Таблица 1 –Требования к функциональным возможностям электронного сервиса ССМП

| **№** | **Функция** | **АРМ Регистратора ССМП** | **АРМ Диспетчера** | **АРМ Старшего смены** | **АРМ статистика** | **АРМ Провизора** | **АРМ Администратора** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Регистрация вызова с заполнением обязательных полей для карты вызова. Возможность оформления вызова к группе пострадавших. Автоматический подбор аналогичных вызовов за период с указанием даты, времени вызова, повода вызова, ФИО, возраста пациента, адреса, статуса вызова. Возможность просмотра истории назначений бригад на аналогичные вызова. | X |  |  |  |  |  |
| 2 | Возможность просмотра вызовов с различными параметрами выборки: за период, по статусам, по приоритетам, по пациентам, по поводам. Вывод на печать списка вызовов. | Х | X |  |  |  |  |
| 3 | Возможность редактирования вызова | X | X |  |  |  |  |
| 4 | Передача вызова на бригаду с возможностью просмотра статусов бригад и составов бригад в разрезе профилей бригад. Возможность установки статуса бригады. | Х | Х |  |  |  |  |
| 5 | Печать карты вызова – форма 110/у. | Х | X |  |  |  |  |
| 6 | Возможность формирования составов бригад из перечня сотрудников станции, по графикам работы. | Х |  | X |  |  |  |
| 7 | Ведение электронной карты вызова скорой медицинской помощи, в том числе:- ввод данных с заполненных карт вызовов бригадой СМП;- учет заполненных карт вызовов бригадой СМП; - просмотр и печать карты вызова скорой помощи; - формирования карточки оказанных услуг с описанием протокола осмотра и оказанных назначений;- сохранение данных о вызове и оказанных услугах. | Х | Х |  | Х |  |  |
| 8 | Персонифицированный учет использованных медикаментов. | Х |  |  |  |  |  |
|  | Учет медикаментов:- учет поступления и расхода медикаментов и перевязочных материалов;- формирование заявок на закупку медикаментов и перевязочных материалов. | Х |  |  |  | Х |  |
| 9 | Формирование регламентированной отчетности ССМП:- Форма 109/у;- Форма 115/у;- Форма 117/у;- Форма 114/у (сопроводительный лист);- Форма 30 (в части относящейся к деятельности скорой медицинской помощи); | Х |  |  | Х |  |  |
| 10 | Формирование произвольной аналитической выборки по пациентам, которым была оказана скорая медицинская помощь. | Х |  | X | X |  |  |
| 11 | Формирование оперативных отчетов:- Отчет по летальности с возможностью формирования посменно;- Сведения об основных целевых показателях деятельности учреждений здравоохранения, участвующих в реализации мероприятий, направленных на совершенствование организации медицинской помощи при дорожно - транспортном происшествии;- Количество вызовов ССМП- Отчет по критериям вызовов скорой медицинской помощи (общее по территории субъекта).  |  |  | X | Х |  | Х |
| 12 | Формирование реестров счетов за оказанную медицинскую помощь в рамках ОМС с заданием параметров выгрузки. |  |  |  | Х |  |  |
| 13 | Выдача справок населению, с функцией регистрации справок. Должна быть реализована возможность просмотра выданных документов. | Х |  | X |  |  |  |
| 14 | Администрирование МО: - регистрация пользователей;- настройка прав доступа;- настройка состава бригад;- настройка соответствия профилей и бригад;- настройка приоритезации вызовов;- настройка графиков работы бригад;- настройка персонифицированного учета медицинских препаратов и перевязочных материалов;- настройка соответствия региональных и федеральных справочников; - настройка формирования нумерации вызовов, в зависимости от параметров окончания смены.  |  |  |  |  |  | Х |

Таблица 2 – Перечень МО для оказания консультационной и организационно-методической поддержки сервиса РС ЕГИСЗ «ССМП»

|  |  |
| --- | --- |
| **№** | **Наименование МО** |
| 1 | БУЗ РА «Акташская больница» |
| 2 | БУЗ РА «Улаганская РБ» |
| 3 | БУЗ РА «Кош-Агачская РБ»» |
| 4 | БУЗ РА «Турочакская РБ» |
| 5 | БУЗ РА «Онгудайская РБ» |
| 6 | БУЗ РА «Усть-Канская РБ» |
| 7 | БУЗ РА «Усть-Коксинская РБ» |
| 8 | БУЗ РА «Чемальская РБ» |
| 9 | БУЗ РА «Чойская РБ» |
| 10 | БУЗ РА «Шебалинская РБ» |
| 11 | БУЗ РА «Центр медицины катастроф» |

|  |  |  |
| --- | --- | --- |
| От Исполнителя:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | От Заказчика:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
|  |  |  |

*Приложение № 6*

*к Контракту от\_\_\_ 2019 г. №\_\_\_*.

**Техническое задание на оказание услуг по сопровождению электронного сервиса РС ЕГИСЗ «СВМД»**

Общие положения

В рамках оказания услуг по настоящему техническому заданию должны быть автоматизированы рабочие процессы выписки медицинских свидетельств о смерти и рождении. При исполнении требований настоящего технического задания Исполнитель обязан учесть общие требования к оказанию комплексной услуги по обеспечению функционирования электронных сервисов РС ЕГИСЗ.

Услуга должна быть реализована на базе платформы Заказчика (далее – Платформа) по принципам облачных технологий и модели «Программное обеспечение как сервис».

Исполнитель гарантирует совместимость не менее чем с двумя разными используемыми получателями Услуг в работе с электронным сервисом браузерами. Требования к браузерам должны быть четко описаны Исполнителем в эксплуатационной документации на электронный сервис.

Исполнитель осуществляет техническую поддержку работы СВМД, включая:

-проведение аналитики зарегистрированных заявок на доработки СВМД;

- консультационную поддержку;

- диагностику работоспособности программного обеспечения СВМД;

- поиск и устранение проблем в случае неработоспособности СВМД;

- восстановление работоспособности прикладного программного обеспечения СВМД при сбоях;

- обновление прикладного ПО СВМД до новых версий (плановое, внеплановое).

Исполнитель реализовывает информационное и документарное сопровождение СВМД в виде предоставления на бумажном носителе актуальных руководств пользователя, руководств администратора, подготовку и передачу Заказчику разработанных вебинаров, учебных материалов по соответствующим вопросам работы в СВМД.

Назначение электронного сервиса СВМД

Сервис предназначен для решения следующих задач:

- построение системы централизованной персонифицированной медицинской статистики рождаемости и смертности;

- получение оперативных данных для мониторинга рождаемости и смертности на территории региона,

- проведение оперативной экспертизы правильности определения причин смерти и оформления медицинских свидетельств.

Цели электронного сервиса СВМД

Основной целью электронного сервиса, является автоматизация выписки медицинских свидетельств о смерти и рождении, осуществление мониторинга естественного движения населения. Улучшение качественных и количественных показателей работы организаций в целом, сокращение затрат времени и труда персонала. В том числе за счет повышения уровня оперативности обработки медицинской информации и выполнения принципа однократного ввода информации в систему и её многократного использования;

Структурно сервис должен включать в себя:

Рабочий функционал медицинской организации с учётом её профиля. Функционал должен обеспечивать формирование и вывод на печать документов, ведение списков умерших и родившихся, создание печатных форм.

Рабочий функционал органа управлением здравоохранения и медицинской статистики. Функционал должен обеспечивать мониторинг смертности и рождаемости.

Рабочий функционал администратора системы: ведение нормативно-справочной информации, техническая и методологическая поддержка, развитие системы.

Рабочий функционал интеграции с внешними информационными системами.

На уровне медицинской организации Web-сервис «Система ведения медицинских документов» должен обеспечивать регистрацию факта живорождения/мертворождения/смерти/перинатальной смерти и автоматизированное создание, редактирование, хранение, печать, удаление учетных медицинских документов, регистрирующих данный факт:

- медицинское свидетельство о рождении;

- медицинское свидетельство о перинатальной смерти (предварительное, окончательное, взамен предварительного, взамен окончательного);

- медицинское свидетельство о смерти (предварительное, окончательное, взамен предварительного, взамен окончательного);

Создание свидетельств о рождении/перинатальной смерти в случае рождения близнецов должно выполняться в неразрывной связи друг с другом.

Медицинские свидетельства о рождении/смерти должны:

- содержать ссылки на все ранее созданные свидетельства о данном факте рождения/смерти (предварительное, взамен предварительного, окончательное, взамен окончательного);

- содержать помимо даты рождения (смерти) и даты выписки документа указание на отчетный период (месяц и год), к которому относится отражаемый в документе факт рождения/смерти. Отчетный период определяется на основании даты рождения/смерти из первоначального свидетельства, но может быть изменен вручную.

Web-сервис «Система ведения медицинских документов» должен обеспечивать удобный поиск документов по комбинации различных критериев:

- серии и номеру медицинского свидетельства;

- дате создания документа;

- отчетному периоду;

- ФИО гражданина, на которого выписан документ;

- ФИО матери (для документов о рождении);

- дате смерти/рождения;

- медицинской организации, выдавшей документ.

В Web-сервисе «Система ведения медицинских документов» должна быть предусмотрена возможность формирования, печати и выгрузки следующих списков:

- родившихся;

- умерших (в различные возрастные периоды);

Web-сервис «Система ведения медицинских документов» должен обеспечивать расчет абсолютных величин, интенсивных, экстенсивных и динамических показателей за любой промежуток времени, измеряемый в днях, формирование и печать соответствующих отчетных форм:

 смертность:

по административно-территориальным образованиям,

по группам административно-территориальных образований,

по группам населенных пунктов,

по возрастным группам умерших,

по возрастным группам матерей в перинатальной и младенческой смертности,

по полу,

по причинам смерти (отдельным диагнозам, группам кодов МКБ-10, категориям причин),

по результатам освидетельствования и экспертизы,

 рождаемость:

по административно-территориальным образованиям,

по группам административно-территориальных образований,

по группам населенных пунктов;

 фертильность:

по административно-территориальным образованиям,

по группам административно-территориальных образований,

по группам населенных пунктов,

по возрастным группам

Формирование отчетных форм должно осуществляться конструктором, позволяющим формировать параметризированные запросы и оформлять их результаты в типовые отчеты.

Web-сервис «Система ведения медицинских документов» должен иметь средства интеграции с другими информационными системами:

- универсальные средства импорта/экспорта свидетельств о рождении (смерти) из/в других информационных систем в режиме онлайн (сервисы) и с помощью выгрузки/загрузки данных из файлов в xml, csv форматах.

Средства администрирования Web-сервиса «Система ведения медицинских документов» должны обеспечивать ограничение прав пользователей при обращении к данным, операциям и отчетам. Управление пользователями должно быть реализовано на основе ролей.

Для дополнительного контроля все действия пользователей и обращения к данным должны регистрироваться в журнале. Должна быть предусмотрена защита журналов логирования от несанкционированного либо случайного доступа и изменения.

Система должна иметь средства восстановления работоспособности после сбоев, средства создания архивных и резервных копий.

Требования к оказанию услуг

Web-сервис «Система ведения медицинских документов» реализован в виде многопользовательской информационной системы, имеющей трехуровневую архитектуру: СУБД – сервер приложений – интерфейс пользователя. В качестве СУБД и сервера приложений должны использоваться программы, распространяемые как свободное программное обеспечение. Интерфейс пользователя должен быть реализован в виде веб-приложения. Эксплуатация серверной и клиентской части не должна требовать использования проприетарного общесистемного программного обеспечения.

Программное обеспечение должно устойчиво функционировать в соответствии с требованиями ГОСТ 28195-89.

Программное обеспечение должно иметь интуитивно-понятный пользовательский интерфейс, вводимые пользователем данные должны подвергаться форматно-логическому контролю и в случае ввода недопустимых данных программа должна выдавать предупреждающее сообщение.

Обязательно наличие пользовательского меню, из которого могут запускаться все основные операции программы. Последовательность объектов в окнах должна соответствовать функциональной последовательности ввода информации.

Информационная система «Система ведения медицинских документов» должна функционировать в режиме 24/7 и обеспечивать одновременную работу не менее 200 пользователей.

Время ответа при вводе и редактировании данных должно быть не более 5 секунд на запрос.

Перечень МО для технической поддержки сервиса

№ Наименование МО

1 БУЗ РА «Акташская больница»

2 БУЗ РА «Улаганская РБ»

3 БУЗ РА «Кош-Агачская РБ»

4 БУЗ РА «Турочакская РБ»

5 БУЗ РА «Онгудайская РБ»

6 БУЗ РА «Усть-Канская РБ»

7 БУЗ РА «Усть-Коксинская РБ»

8 БУЗ РА «Чемальская РБ»

9 БУЗ РА «Чойская РБ»

10 БУЗ РА «Шебалинская РБ»

11 БУЗ РА «Майминская РБ»

12 БУЗ РА «Республиканская больница»

13 БУЗ РА «Перинатальный центр»

14 БУЗ РА «Бюро судебно-медицинской экспертизы»

15 БУЗ РА «Противотуберкулезный диспансер»

16 БУЗ РА «Медицинский информационно-аналитический центр»

Приложение № 7

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019

**Техническая характеристика Услуг по сопровождению Голосового диалогового сервиса записи на прием к врачу**

Программное обеспечение Голосового диалогового сервиса записи на прием к врачу размещается на мощностях Заказчика.

Аппаратное оборудование:

Сервер 1: процессор – IntelCore i7 / Xeon E3 (4C/8T), ОЗУ – не менее 8 ГБ, HDD – не менее 12 ГБ, хранилище - не менее 1 ТБ - для хранения информации об обработанных звонках (один канал должен генерировать не более 3 МБ информации за 1 минуту работы Сервиса), 2 LAN 1 Гб/с, удаленное администрирование (внешний канал не менее 8 Мб/с на прием). Информация об обработанных звонках виртуальной АТС хранится в хранилище не менее 3 месяцев.

Сервер 2: процессор – не менее 4-х ядер, ОЗУ – не менее 8 Гб, HDD – не менее 600 Гб, 3 LAN 1 Гб/с, удаленное администрирование (канал не менее 8 Мб/с на прием). Сервер 2 имеет доступ к защищенной сети передачи данных РА, в т.ч. к НОП.

Программное обеспечение:

На Сервере 1 развернут MS Windows 2008 R2 Standard with IIS 7 & .NET FW 4.0.На Сервере 2 развернута виртуальная АТС Asterisk.

По запросу Исполнителю должен быть предоставлен доступ к программно-аппаратному обеспечению Голосового диалогового сервиса: на программное обеспечение Сервера 1 и Сервера 2 с правами администратора. На период отсутствия доступа Исполнитель не несет ответственности за несоответствие оказываемой услуги требованиям данного Договора.

В рамках сопровождения Голосового диалогового сервиса записи на прием к врачу предоставляются следующие услуги:

1. Поддержка работоспособности голосового диалогового сервиса, включая работу функции обратного вызова для всех получателей услуги;
2. Мониторинг корректности ввода фамилий и имен и устранение возможных неисправностей и неполадок;
3. Добавление лингвистических данных Системы в течение 2 дней с момента обращения Заказчика;
4. Изменение сценариев работы системы поддержки диалога в течение 5 дней с момента обращения Заказчика или обнаружения необходимых изменений Исполнителем и извещения об этом Заказчика;
5. Исправление обнаруженных ошибок в коде в течение 5 рабочих дней с момента обращения Заказчика;
6. Предложение внешних мер по снижению или устранению последствий обнаруженных ошибок в течение 4 часов с момента обращения Заказчика;
7. Производство обновлений программного обеспечения, связанное с изменениями в операционной системе и в средствах защиты, вызванных исправлением обнаруженных в них ошибок в течение одного календарного месяца с момента обращения Заказчика;
8. Предоставление одного оператора для приема звонков и осуществления записи пациентов на прием к врачу. Рабочее время Операторов: 09:00-17:00 нск, с понедельника по пятницу;
9. Оказание консультаций Заказчику, разрешение проблем, связанных с некорректной работой голосового робота с расписанием медицинских организаций;
10. Передача руководств пользователя по настройке расписаний ресурсов в медицинские организации.

Голосовой диалоговый сервис взаимодействует с безопасным облачным сервисом «Медицинская информационная система» (МИС) по протоколу доступа SOAP.

Приём и передачу звонков на виртуальную АТС Заказчика Исполнитель осуществляет самостоятельно в рамках услуги «Бесплатный вызов» с возможностью бесплатного вызова с территории Республики Алтай. Входящий телефонный номер голосового диалогового сервиса согласовывается в рабочем порядке с Заказчиком (согласованный на данное время телефонный номер: 8-800-100-26-99).

Голосовой диалоговый сервис осуществляет запись пациентов на приём к врачу исходя из расписаний врачей, настроенных на работу с сервисом. Сервис осуществляет запись на прием пациентов, зарегистрированных в МИС. Сервис должен позволять одновременно обрабатывать не менее 4 входящих звонков при отсутствии в момент входящего вызова выполняемых заданий на совершение исходящих звонков и не менее 2 входящих звонков при наличии в момент входящего вызова выполняемых заданий на совершение исходящих звонков.

Исполнитель обеспечивает автоматический исходящий обзвон пациентов, записавшихся на приём к врачу, в целях снижения «недохода» (обратный вызов), проведение его настройки и настройки его интеграционных связей с медицинской информационной системой.

Базовый сценарий модуля обратного вызова (может подвергаться корректировке в процессе эксплуатации):

1. ГС звонит накануне (те за 1 день) дня приема.
2. ГС озвучивает стандартное приветствие.
3. ГС запрашивает подтверждение, что общается с пациентом или законным представителем пациента и только после этого:
4. Сообщает данные записи:
* место, время,
* специализация врача.
1. ГС запрашивает у пациента подтверждение готовности прийти на прием.
* В случае отказа прийти на прием ГС отменяет запись в расписании МИС и завершает вызов. Отмена записи производится только в случае, если пациент сказал НЕТ. При этом не предлагает ничего, но напоминает о возможности записаться снова.
1. В случае занятости или недоступности адресата ГС попытается перезвонить через 45 минут, но не более 2 раз.
2. Список на обзвон формируется раз в сутки в ночное время. В список попадают записи, назначенные на следующие календарные сутки.
3. Если есть записи с одним номером телефона на одно число, ГС объединит их в один звонок.
4. В случае если ГС не дозвонился до пациента в указанное в п. 8 время, ГС формирует список таких пациентов. Данный список может передаваться оператору для дальнейших действий.

При отмене/переносе приема по инициативе МО в течение дня робот голосового сервиса звонит и сообщает, что талон отменен в связи с отсутствием врача. В этом же звонке робот предлагает пациенту заново записаться на прием к другому врачу.

Поддержка функции обратного вызова включают в себя:

* Корректировку сценария по запросу Заказчика и предоставленных сведений, обязательных для выполнения корректировки;
* Корректировка сценария Исполнителем (согласовывая коррективы) по итогам анализа логов электронного сервиса в целях увеличения производительности его работы.

Приложение №8

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

От «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019

**Технические характеристики на передачу прав на использование операционной системы для автоматизированных рабочих мест с базовым техническим сопровождением**

Операционная система для рабочих станций, права на установку и использование которой передаются в рамках данного государственного контракта, должна отвечать следующим требованиям и обеспечивать:

* возможность задания хешей паролей пользователей в соответствии с ГОСТ Р 34.11-2012;
* возможность создания ssh-тунелей с кодированием передаваемой информации в соответствии с ГОСТ Р 34.12–2015
* возможность создания защищенных VPN-тунелей, использующих контроль целостности заголовков IP-пакетов в соответствии с **ГОСТ** Р 34.12–**2015**
* позволять выполнять защитное преобразование файлов и каталогов по ГОСТ Р 34.12–2015 встроенное в файловый менеджер;
* возможность ограничения полномочий пользователей по использованию консолей;
* возможность ограничения работы с интерпретируемыми языками для непривилегированных пользователей
* возможность блокировки макросов в приложениях
* иметь в составе ядро не ниже 4.15 и актуальный набор драйверов для совместимости с имеющимся периферийным оборудованием и обеспечения корректного функционирования современных средств вычислительной техники.
* графическое средство настройки выделяемых ресурсов памяти пользователям (квоты)
* графическое средство ввода рабочей станции в домены Active Directory и FreeIPA
* графические средства настройки подключения к сетевой файловой системе Samba
* графическое средство настройки сохранения и восстановления сессии пользователя (восстановление при старте запущенных программ и их расположения после полного отключения электропитания АРМ).
* графическое средство настроек потребления электроэнергии (яркость экрана, потухание или выключение монитора, переход в ждущий режим, сон или гибернацию) в случае изменения настроек электропитания (питание от сети, питание от батареи, низкий заряд батареи) с возможностью мгновенного тестирования настроек.
* графические средства запуска работы с удаленными, отдельными или вложенными графическими сессиями
* графические средства настройки планирования времени завершения работы без участия пользователя (завершение сессии, выключение АРМ, перехода в энергосберегающие режимы) с настройкой уведомления о событии.
* возможность автоматического брендирования рабочего стола с графическими инструментами настройки расположения логотипа.
* возможность ввода логина и пароля пользователя как при входе в систему, так и при разблокировке экрана после бездействия, как с физической, так и с виртуальной клавиатуры
* графический инструмент регулировки яркости экрана ноутбука или мобильных устройств
* графические средства запуска приложений с изменением приоритета выполнения, либо от имени другого пользователя без доступа к консоли.
* графический инструмент настройки параметров загрузчика операционной системы(загружаемая операционная система по умолчанию, передаваемые параметры ядра, таймаут для ожидания действий пользователя, выбора источника ввода данных при загрузке, выбор терминала для вывода информации).
* поставляться с интернет-браузером, с поддержкой ГОСТ TLS (при наличии установленного в ОС комплекта программ КриптоПро CSP)

Графический менеджер файлов должен обеспечивать:

* возможность расчета контрольных сумм файлов и их сравнения по алгоритмам ГОСТ Р 34.11-2012, MD5, SHA1, SHA256 без доступа к консоли.
* поиск файлов как по шаблону, так и по содержимому в документах формата ODF, а также по времени создания или изменения, а также размеру файла без доступа к консоли..
* создания из контекстного меню архивации файлов или каталогов с возможностью создания многотомного архива, архива с паролем и выбора степени сжатия данных без доступа к консоли.

Файловый менеджер должен обеспечивать:

* возможность работать с архивами (zip, rar, 7zip, tar, tgz, tar.gz, tar.bz, tar.xz, iso), как с папками (с возможностью как замены файлов так и работы в режиме только чтение) без доступа к консоли.
* поддержку работы с файловыми системами ext2/3/4, fat,ntfs, iso9660.

Операционная система должна поддерживать:

* сетевые протоколы SMB, NFS, FTP, NTP, HTTP(S);
* средства удаленного администрирования и управления конфигурациями;
* средства организации единого пространства пользователей, реализующие централизованное хранение информации об окружении пользователей и сетевую аутентификацию через протоколы ldap и kerberos и совместимое с Active Directory.

Операционная система должна иметь графические средства настройки системы, в том числе:

* + - аутентификации (включая Active Directory и ldap/kerberos);
		- установки и синхронизация времени;
		- управления пользователями;
		- просмотра системных журналов;
		- добавления принтеров.

В состав операционной системы должны входить следующие компоненты:

* ядро Linux не ниже 4.15;
* пакет офисных программ (текстовый редактор, редактор электронных таблиц, редактор презентаций, редактор векторной графики);
* сервер печати, обеспечивающий печать документов;
* набор программ для воспроизведения аудио и видео файлов;
* редактор растровой графики;
* запись оптических дисков;
* программа сканирования;
* программа работы с web-камерой.

Операционная система должна быть включена в Единый реестр российских программ для электронных вычислительных машин и баз данных и совместима с офисным пакетом и браузером из Единого реестра российских программ для электронных вычислительных машин и баз данных. Операционная система должна поставляться с базовой технической поддержкой, включающей право на использование обновлений в течение 12 месяцев.

Приложение № 9

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019

**Технические характеристики на техническое сопровождение и передачу прав на использование защищенного браузера**

Защищенный браузер, права на установку и использование которого передаются в рамках данного государственного контракта, должен отвечать следующим требованиям:

* Выполнение пользователем в интернет-обозревателе стандартных операций (открытие окон, изменение масштаба, просмотр загрузок, истории, настроек и т.д.);
	+ - * Использование «умной» адресной строки (ввод URL-адреса приводит к открытию соответствующего веб-сайта, ввод поискового запроса приводит к открытию страницы с результатами поиска в текущей выбранной поисковой системе);
			* Восстановление последних закрытых вкладок;
			* «Быстрый» доступ к часто посещаемым интернет-сайтам;
			* Поддержка проверки целостности и подлинности установочного пакета интернет-обозревателя.
			* Поддержка установки защищенного соединения с информационным системам и ресурсам по протоколу TLS 1.0 и TLS 1.2 с использованием российских криптографических алгоритмов (хеш-функция - ГОСТ Р 34.11-2012, шифрование – ГОСТ 28147-89, ЭП – ГОСТ Р 34.10-2012).
			* Установка и проверка корневых сертификатов российских Удостоверяющих центров, аккредитованных Министерством связи и массовых коммуникаций Российской Федерации.
			* Отключение всех сервисов, направляющих информацию на сервера иностранных разработчиков.
			* Сохранение метрик интернет-обозревателей пользователей только на корпоративном сервере внутри домена.
			* Поддержка как минимум, двух операционных систем, включенных в Реестр российского ПО, в соответствии с пунктом 11 постановления Правительства Российской Федерации от 23 марта 2017 года № 325.
			* Поддержка 6-ой редакции стандарта ECMAScript (JavaScript).
			* Поддержка Adobe Flash Player.
			* Поддержка технологий HTML5, CSS3.
			* Поддержка работы с компонентами ActiveX и Silverlight в среде Microsoft Windows.
			* Наличие русского языка интерфейса.
			* Поддержка настройки параметров используемого прокси-сервера.
			* Объединение пользователей в группы, для настройки применения групповых политик работы с интернет-обозревателем.
			* Настройка доверенных узлов сети.
			* Настройка разрешенных расширений.
			* Поддержка настройки перечня ресурсов (например, использующих элементы ActiveX или «расширения» стандарта HTML компании Microsoft), которые должны корректно отображаться в интернет-обозревателе, с использованием движка Internet Explorer.
			* Настройка стартовой страницы интернет-обозревателя на рабочих местах пользователей:

• ресурсы (быстрые ссылки), которые должны отображаться на стартовой странице интернет-обозревателя;

• источники новостей, которые должны отображаться на стартовой странице интернет-обозревателя.

• Сбор метрик интернет-обозревателей пользователей:

• посещение внутренних и внешних ресурсов;

• ошибки, возникающие при обращении к тем или иным внутренним и внешним ресурсам;

• установка расширений.

* + - * Поддержка отображения:
			* веб-документов, созданных в соответствии со спецификацией XML;
			* популярных открытых аудио и видео-форматов (Ogv, Ogg, WebM);
			* популярных графических форматов (PNG, JPEG, GIF);
			* документов других форматов (например, PDF) при использовании специально подключаемых модулей (расширений для интернет-обозревателя).

Защищенный браузер должен быть включена в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Должна предоставляться техническая поддержка сроком на 12 месяцев на имеющиеся у Заказчика лицензии защищенного браузера Спутник.

Техническая поддержка должна соответствовать следующим требованиям:

* обеспечивать сопровождение программного обеспечения браузера и его дополнительных программных модулей согласно документации;
* предоставлять обновленное программное обеспечение по запросу Заказчика;
* консультировать Заказчика по вопросам снижения рисков возникновения внештатных ситуаций;
* осуществлять регистрацию на Инциденты.

Техническая поддержка должна осуществляться по будним дням (с понедельника по пятницу) с 10-00 до 19-00 (время московское).

Уровни сервиса технической поддержки должны соответствовать требованиям, указанным в Таблице 1.

Таблица 5

| **Параметр** | **Нормативное значение/ Условие соблюдения (где применимо)** |
| --- | --- |
| Гарантированный уровень доступности Услуг (рассчитывается за отчетный период) | 99,5% |
| Временной режим доступности | круглосуточно (24х7) |
| Временной режим регистрации и обработки обращений | с 10:00 до 19:00 часов (московское время) ежедневно по рабочим дням |
| Временной интервал проведения регламентных работ | регламентные работы подразумевают обновление программного обеспечения и данных в соответствии с релиз-циклами разработки и проводятся без деградации сервисов |
| Регистрация обращений и запросов Пользователей, поступивших по всем каналам коммуникаций, кроме телефонных обращений и запросов | 12 часов |
| Временной режим рассмотрения претензий | с 10:00 до 19:00 часов (московское время) ежедневно по рабочим дням |
| Срок предоставления результатов рассмотрения по обращению, требующему технических работ  | не более 63 рабочих часов (7 рабочих дней) с момента назначения претензии |

Реакция на Инциденты должна включать включает в себя:

* регистрацию Инцидента в журнале;
* определение причины Инцидента;
* составление плана восстановительно-ремонтных работ;
* начало восстановительно-ремонтных работ.

Определение приоритетов возникающих проблем должно осуществляться в соответствии с характеристиками, приведенными в Таблице 2.

Таблица 2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Уровень приоритета** | **Описание** | **Время реакции** | **Время устранения** | **Время на понижение приоритетности устранения** |
| Приоритет 1  | Недоступность браузера и его дополнительных программных модулей, полная потеря работоспособности | В течение четырех часов | В течение 1 дня | Снижение приоритета до «2» в течение 24-х часов |
| Приоритет 2  | Функциональность браузера и его дополнительных программных модулей доступна не полностью, производительность серьезно деградирует | В течение 1 дня | В течение 3-х дней | Снижение приоритета до «3» в течение 24-х часов |
| Приоритет 3  | Сбои в работе отдельных приложений отрываемых в браузере | В течение 1 дня | В течение 14-ти дней |  |

Приведенные нормативы реакции на Инциденты распространяются только на Инциденты, зарегистрированные в Рабочие дни. Для Инцидентов, зарегистрированных в выходные и нерабочие дни, отчет ведется с 10-00 первого Рабочего дня новой рабочей недели.

Приложение № 10

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 \_\_\_\_\_

**Технические характеристики на установку. техническое сопровождение и передачу прав на использование антивирусного программного обеспечения**

**Общие требования**

Антивирусное программное обеспечение **должно быть предоставлено в виде сервиса, построенного** на базе программной клиент-серверной системы антивирусной защиты (далее – система), обеспечивающей централизованное управление антивирусной защитой защищаемых объектов - рабочих станций Заказчика в количестве 1526 шт. Все компоненты Системы должны принадлежать одной торговой марке с единой службой технической поддержки на русском языке. Отдельно стоящие рабочие станции, не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным продуктом, включающим в себя защиту от проникновения и активации всех типов вредоносных программ (антивирус), спама (персональный антиспам) и обеспечивать возможность их включения в единую систему антивирусной защиты. Поставляемые средства защиты должны представлять масштабируемое решение, обеспечивающее устойчивое функционирование в сети (сетях) заказчика.

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке.

Для использования Системы конечными пользователями не должны требоваться серийные номера или ключевые файлы. Право использования компонентов Системы должно определяться выбранной подпиской - бессрочной лицензией с возможностью приостановки ее действия и автопродления, Подписка должна позволять изменять (в том числе расширять) количество защищаемых объектов на лету, без замены подписки или переустановки компонентов защиты и не должна иметь привязку к используемому на защищаемых компьютерах и устройствах аппаратному обеспечению. Пользователь Системы должен иметь в рамках подписки право на перенос системы защиты с одних защищаемых объектов (в том числе рабочих станций и серверов) на иные без необходимости перепривязки или получения дополнительных подписок.

Для создания системы антивирусной защиты на все защищаемые объекты должны быть установлены взаимодействующие компоненты, объединяющие объекты в единую антивирусную сеть, которая обменивается информацией с сервером, используя сетевые протоколы TCP/IP.

Система антивирусной защиты должна включать:

* программные средства защиты рабочих станций и файловых серверов;
* программные средства защиты мобильных устройств, в том числе смартфонов;
* программные средства централизованного управления, мониторинга и обновления;
* обновляемые базы данных сигнатур вредоносных программ всех типов и атак;
* эксплуатационную документацию на русском языке.

Программные средства Системы должны обеспечивать определение угроз следующих типов:

* классических вирусов;
* троянских программ;
* руткитов;
* сетевых червей;
* рекламных программ;
* программ автодозвона на платные сайты;
* потенциально опасных приложений;
* прочих вредоносных программ.
* Антивирусная защита должна обеспечивать:
* обнаружение и удаление вирусов из файлов, упакованных программами типа PKLITE, LZEXE, DIET, COM2EXE, а также аналогичными, используемыми злоумышленниками для упаковки вредоносных файлов;
* обнаружение и удаление вредоносных программ, скрытых под упаковщиками, имеющими неизвестный (неописанный публично) формат, специально создаваемый для сокрытия вредоносных файлов;
* обнаружение вирусов внутри контейнеров и архивных файлов формата ACE (до версии 2.0), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO (включая NRG, образы с нестандартным форматом сектора и не имеющие сигнатур), ZLIB, VCLZIP, VISE, PST, DMG, PDF, GHOST INSTALLER с зашифрованными контейнерами и т.д. без ограничений на уровень вложенности проверяемых объектов;
* обнаружение вирусов внутри контейнеров, не имеющих строгого формата (HTML, MIME);
* обнаружение вирусов внутри контейнеров с нечетким значением размера объекта (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES и т.д.);
* антивирусную проверку файлов и объектов, имеющих формат Smart Install Maker (SIM); DMG, HFS, XAR, Universal Binary (MacOS); SIS (Symbian 9); INNO SETUP (5.3.9 и выше); SETUP FACTORY (линейки 7,8); XENOCODE; TARMA INSTALL (линейка 3); XZ (UNIX); COMPRESS; SQUAHFS; CHILKAT ZIP; пакеты LHA (AWARD BIOS);
* антивирусную проверку в самораспаковывающихся архивах: AppPackager, Astrum Install Wizard, Create Install, Fly Studio, GSFX, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy;
* проверку исполняемых файлов упакованных следующими упаковщиками: PELOCK, ENIGMA Protector, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR, ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, RCRYPTOR, PECRYPT, а также почтовых файлов Mozilla Thunderbird- вне зависимости от их размера;
* разбор неформатированных почтовых баз и обработка писем с высокой вложенностью (например, переписки с большим количеством ответов и пересылок RE/FW), поддержка формата TNEF;
* защиту от вредоносных программ, принадлежащих семействам вредоносных программ, информация о которых имеется в антивирусных базах, созданных после занесения соответствующей информации в антивирусные базы и еще не попавших на анализ в антивирусные лаборатории - как на основе эвристического анализа, так и с помощью технологии поиска похожих вирусов, основанной на анализе расположения участков кода в файле;
* обнаружение вредоносных объектов в HTML- и PDF-документах, включая обфусцированные эксплойты в JavaScript, находящиеся в документах данных типов. Возможность извлечения и анализа «невидимых» IFRAME-элементов. Возможность извлечения для проверки скриптов любой сложности и снятие с них защиты;
* обнаружение угроз по лицензионным данным (ASPROTECT, PEP и ENIGMA);
* обнаружение вредоносных объектов в DEX-файлах (Android).

**Требования к системе управления антивирусной защитой (далее - Сервер управления)**

* Система управления должна быть построена по клиент-серверной архитектуре с возможностью построения иерархической системы серверов – с возможностью использования в системе антивирусного управления как главных, так подчиненных серверов.
* Система управления должна быть реализована на основе Web-интерфейса, поддерживающего Web-браузеры, используемые как в корпоративной сети, так и Web-браузеры, используемые на устройствах и компьютерах, имеющих доступ к сервисам управления антивирусной защитой извне корпоративной сети - в том числе Mozilla Firefox или Internet Explorer, Google Chrome, Opera, Safari. Управление через данные браузеры должно быть доступно с любых ОС, имеющих возможность их установки и запуска.
* Система должна включать поддержку кластерного протокола, с помощью которого координируются действия над агентами защиты с разных антивирусных серверов
* Система управления должна быть доступной с любой операционной системы, поддерживающей браузеры вышеперечисленные браузеры (в том числе с ОС Microsoft Windows и ОС типа UNIX (Linux, FreeBSD, Solaris)), без ограничений на использование последних версий браузеров и без доустановки какого-либо программного обеспечения как на стороне сервера управления, так и на стороне администратора Системы. Контроль работы Системы должен быть также возможен консоли управлеия, функционирующей на мобильных устройствах iPhone
* В целях безопасности все программное обеспечение, входящее в состав антивирусного сервера (в том числе необходимое для доступа с помощью браузера) должно поставляться в виде единого дистрибутива и принадлежать одной торговой марке.
* Система управления должна включать систему управления лицензиями, позволяющую распределять между серверами в рамках иерархической сети необходимое количество лицензий
* Установка антивирусного сервера Системы, должна быть возможна на:
* Microsoft Windows Server 2008;
* Microsoft Windows Server 2012;
* Microsoft Windows Server 2016;
* Linux glibc2.12 и выше;
* FreeBSD 9.3 и выше;
* Sun Solaris 10/11 (x86/ Sparc).
* Установка агента управления антивирусной защиты должна быть возможна на:
* Linux glibc 2.13 и выше для платформ Intel x86/amd64;
* Microsoft Windows XP Professional SP2 и выше;
* Microsoft Windows Server 2003 SP2;
* Microsoft Windows Vista (также с SP1 и выше) ;
* Microsoft Windows Server 2008 (также с SP1 и выше) ;
* Microsoft Windows 7;
* Microsoft Windows Server 2012 (также с R2);
* Microsoft Windows 8/8.1;
* Microsoft Windows 10;
* ОС Android 4.0 и выше;
* Mac OS X 10.7 и выше.
* Система управления должна иметь возможность:
* просмотра и сравнения состава аппаратно-программного обеспечения на станциях антивирусной сети
* контроля неактивных станций антивирусной сети
* просмотра сессий пользователей антивирусной сети
* замены системного DNS
* использования как внутренней СУБД (поставляемой в составе дистрибутива антивирусного сервера), так и внешней (устанавливаемой отдельно до или после развертывания антивирусного сервера). При использовании внешней СУБД Система должна иметь возможность работы с ней как без установки дополнительное ПО(с СУБД MS SQL, Oracle), так и с помощью драйверов ODBC для операционных систем Windows и Linux (в том числе с СУБД PostgreSQL). Система должна иметь возможность замены типа используемой СУБД после установки серверной части – без необходимости переустановки серверной части Системы
* управления базой данных средствами системы управления, в том числе возможности очистки базы данных, ее анализа, выполнения произвольных SQL-запросов
* экспорта и импорта базы данных антивирусного сервера в XML-файл.
* создания иерархической сети антивирусных серверов. Антивирусные сервера должны иметь возможность установки как внутри локальной сети, так и на удаленных серверах. В случае реализации иерархической сети
* объединения информации от нескольких серверов на одном;
* распределения рабочих станций между серверами для получения обновлений в целях снижения общей нагрузки на сеть;
* обмена статистикой в рамках одной иерархической сети между антивирусными серверами различных версий;
* контроля отсутствия связанных серверов в расписании антивирусного сервера.
* резервирования информации, хранящейся на антивирусных серверах путем создания равноправных серверов (кластера серверов) и синхронизации информации между ними. Сервера кластера должны иметь возможность установки как внутри локальной сети, так и на удаленных серверах. Антивирусные агенты должны иметь возможность переподключения к серверам кластера в случае падения одного из них;
* построения многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне;
* установки антивирусных агентов в сети, не использующей единого пароля доступа к рабочим станциям;
* централизованной настройки параметров защиты, уникальных для различных групп, в том числе для рабочих станций, находящихся в режиме off-line.
* централизованного сбора и просмотра статистической информации и создания (автоматического и ручного) отчетов о состоянии антивирусной защиты, установленных и запущенных компонентах антивирусной защиты, наличии станций сети, не состоящих ни в одной организации, неактивных станциях сети, консолидации отчетов;
* интеграции в системы управления и информационные системы с помощью встроенного в систему API
* наличия множественных путей уведомления пользователей и администраторов путем посылки почтового сообщения, всплывающего окна, записи в журнал событий, SNMP-trap;
* оповещения о возникновении эпидемий (множественных инфекций)
* оповещения о наличии обновлений сервера
* отправки информационных сообщений пользователям по сети в режиме реального времени через Web-интерфейс Системы;
* обеспечения связи антивирусного сервера и клиентских частей через встроенный модуль в случае, когда они расположены в различных сетях, работающих по протоколам TCP/IP (в т.ч. IPv6), между которыми отсутствует маршрутизация пакетов
* самостоятельного написания обработчиков событий на языке программирования, имеющего встроенную систему очистки мусора (удаления неиспользуемых данных), а также не требующего для своей работы установки дополнительных компонент (Lua), а также выполнения произвольных Lua-скриптов с помощью средств системы управления.
* В случае интеграции с внешними подсистемами с помощью встроенного Web API, должна иметься возможность аудита действий, произведенных с помощью функций данного Web API
* Вне зависимости от типа антивирусного агента и защищаемой системы, Система должна обеспечивать реализацию следующих функциональных возможностей:
* экспорта, импорта и распространения конфигураций групп, станций антивирусной сети или компонентов антивирусной защиты на другие группы, станции и компоненты, в том числе в целях изменения политик, применения их к определенным группам;
* скачивания конфигурационных файлов с настройками подключения антивирусных агентов для ОС Android, Mac OS X и ОС семейства UNIX;
* восстановления рабочих станций, случайно удаленных из системы защиты;
* централизованного обновления антивирусных баз на всех защищенных рабочих станциях, в том числе мобильных и находящихся в режиме off-line. Доставки обновлений на рабочие места пользователей как по расписанию, так сразу после их получения;
* обновления программных средств и антивирусных баз из разных источников, доставляемые как автоматически по каналам связи в пределах антивирусной сети, так и путем ручной синхронизации информации между серверами и рабочими станциями;
* управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера, включая откат обновлений;
* контроля результатов обновления антивирусного ПО на станциях антивирусной сети;
* организации межсерверного обмена согласно расписанию;
* ограничения канала связи по группам;
* наличия возможности групповых обновлений;
* обновлений по защищенному каналу с использованием SSL-сертификатов;
* организации отложенного обновления;
* автоматического перехода установленного ПО на более новые версии, в том числе с возможностью выбора обновляемых компонентов.
* Программные средства управления для всех защищаемых ресурсов, реализованных на платформах ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:
* централизованной удаленной установки и деинсталляции программных средств, антивирусных баз и антивирусного ядра на защищаемые узлы сети – в том числе на станции, находящиеся в разных доменах;
* создания инсталляционных пакетов для конкретных защищаемых рабочих станций;
* выбора и настройки устанавливаемых компонентов до начала установки антивирусного пакета на клиентские части.
* Система управления должна поддерживать возможность:
* создания точки восстановления перед установкой антивирусного пакета на защищаемые рабочие станции и сервера;
* восстановления удаленных станций.
* запрета останова компонентов защиты и их деинсталляции:
* контроля выполнения назначенных заданий:
* Система должна поддерживать множественную возможность установки своих компонентов на защищаемые рабочие станции – в том числе с помощью:
* прямого их указания в системе управления в результате сканирования локальной сети, Microsoft Active Directory,
* политик Microsoft Active Directory
* установки с помощью дистрибутива, содержащего все компоненты защиты
* рассылки инсталляционных файлов из системы управления по электронной почте
* возможностей службы распределенной файловой системы (DFS).
* Система должна поддерживать возможность настройки правил автоматического распределения станций по пользовательским группам, а также возможность изменения первичной группы при автоматическом подтверждении доступа станций к антивирусному серверу.
* Система должна иметь возможность минимизации трафика:
* за счет применения специальных алгоритмов сжатия;
* ограничения трафика по пропускной способности и по времени в определенных IP-подсетях.
* Система должна иметь возможность интеграции с платформой Microsoft® Network Access Protection (NAP), обеспечивающей автоматическую систему реагирования на инциденты безопасности.
* Система должна иметь возможность выбора уровня подробности протоколирования своих компонентов.
* Cистема управления должна иметь возможность загрузки архивированных файлов журнала работы всех антивирусных серверов иерархической сети.
* В целях ограничения использования серверного пространства должна иметься возможность ротации файлов журнала антивирусного сервера по времени (час, день, неделя).
* Система управления должна обеспечивать защиту от несанкционированного доступа. Авторизация должна обеспечиваться парой логин/пароль.
* Администраторы Системы должны иметь возможность авторизации с помощью ActiveDirectory, LDAP, RADIUS, PAM. Система управления должна иметь возможность предварительного тестирования настроек авторизации внешних администраторов Active Directory, LDAP и RADIUS.
* Система должна иметь журнал аудита действий администраторов Системы, позволяющий просматривать журнал событий и изменений, осуществленных администраторами при помощи системы управления.
* Система должна обеспечивать:
* возможность экспорта выбранных файлов из карантина рабочей станции и/или файлового сервера на антивирусный сервер для дальнейшего анализа;
* возможность задания групповых политик в зависимости от группы IP-адресов, имени станции, организации, идентификатора пользователя, операционной системы и иных параметров;
* возможность просмотра новостей безопасности, в том числе информирующих об актуальных угрозах.
* Система должна обеспечивать реализацию следующих функциональных возможностей по обновлению:
* получения ежедневных обновлений вирусных баз не менее 10 раз в сутки независимо от того, рабочий, либо выходной день, что должно подтверждаться созданным Системой отчетом (файлом протокола). Система также должна поддерживать возможность получения экстренных обновлений, связанных с выходом новых типов вредоносного ПО, а также возможность мгновенного распространения этих обновлений;
* возможность множественности путей обновления, в том числе, в случае установки в закрытой локальной сети - с помощью специальной утилиты загрузки обновлений;
* возможность обновления через прокси-серверы, в том числе прокси-серверы MS ISA/TMG.
* проверка целостности и подлинности обновлений средствами электронной цифровой подписи.
* обновления компонентов и вирусных баз по защищенному каналу, с использованием протокола HTTPS.
* в случае размещения антивирусных серверов во внутренней сети без доступа к сети Интернет получение обновлений должно быть возможно с помощью специальной утилиты автономной загрузки репозитория.
* Система должна иметь возможность перезагрузки защищаемой станции через систему управления
* Система должна иметь возможность шифрования трафика между серверами и защищаемыми рабочими станциями в целях предотвращения утечки конфиденциальной информации.
* В комплект поставки должна входить утилита дистанционной диагностики работы антивирусного сервера

**Требования к программным средствам антивирусной защиты ОС семейства Microsoft Windows**

* Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
* осуществление антивирусной (включая постоянную защиту от руткит-технологий) и антиспам защиты на рабочих станциях;
* создание резервных копий папок, указанных пользователем, а также восстановление данных из хранилища - в том числе самим пользователем.
* В целях противодействия вредоносным программам, блокирующим запуск известного ПО - для установки системы защиты не должна требоваться установка стороннего инсталлятора - включая Microsoft Windows Installer, либо использование служб, дополнительных к ранее используемым.
* В связи с необходимостью автоматизации развертывания системы защиты установка должна быть возможна в том числе в режиме командной строки - указанием необходимых параметров установки. В том числе установки в фоновом режиме, состава устанавливаемых компонент;
* В связи с возможными ограничениями канала доступа в сеть Интернет, установка системы защиты должна быть возможной без доступа в сеть Интернет - полный дистрибутив должен содержать все компоненты системы защиты, а также базы данных признаков вредоносных программ и вредоносных ресурсов сети Интернет, доступ к которым может регулироваться системой защиты.
* Для работы системы защиты не должны использоваться внешние библиотеки, а также среда .Net Framework, целостность которых не находится под контролем системы самозащиты и компрометация которых может привести к ошибкам отображения информации системы защиты или иным проблемам, связанным с интерфейсом системы защиты
* Система установки должна поддерживать импорт настроек, содержания карантина и хранилища резервных копий папок, сохраненных после удаления ранее установленной версии Системы - в случае наличия совместимости версий.
* Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.
* Система, используя актуальную на момент проведения тендера версию программного обеспечения, должна обеспечивать защиту рабочих станций под управлением операционных систем:
* Microsoft Windows XP Professional;
* Microsoft Windows 7;
* Microsoft Windows Vista;
* Microsoft Windows 8/8.1;
* Microsoft Windows 10.
* Система должна обеспечивать защиту серверов под управлением операционных систем:
* Microsoft Windows Server 2003;
* Microsoft Windows Server 2008.
* Microsoft Windows Server 2012
* Microsoft Windows Server 2000;
* Microsoft Windows Server 2016.
* Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки.
* Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых «на чтение», а также использования особенностей современных архитектур.
* Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов.
* Права доступа к настройкам компонентов антивирусного пакета для пользователей должны определяться администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав и без применения пароля.
* В случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек пользователями и администраторами Системы в рамках имеющихся у них прав.
* В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
* В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
* Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы.
* По умолчанию система защиты должна работать в так называемом пользовательском (ограниченном) режиме. Пользователю системы, не являющемуся администратором защиты, не должны быть доступны настройки компонентов системы защиты, а также возможность отключения системы защиты. При работе в данном режиме в интерфейсе системы защиты не должны показываться пункт меню или иконка, нажатие на которые открывает окно или раздел интерфейса с настройками системы защиты. Администратор должен иметь возможность ограничить доступ к настройкам с помощью пароля;
* Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях:
* поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
* непрерывное фоновое сканирование в целях нейтрализации активных угроз
* обнаружение вредоносных программ, не обнаруживаемых средствами антивирусного ядра, с помощью превентивной защиты, отслеживающей поведение запущенных процессов, а также вредоносных объектов, внедренных в запущенные процессы;
* проверки ссылок на видоизменение, скрипты и фреймы;
* проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора;
* выявления вредоносных объектов в HTML- и PDF-документах;
* выявления и анализа «невидимых» IFRAME-элементов на страницах сайтов и HTML-документах;
* проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
* блокировку опасных макросов VBA в реальном времени;
* защиту от вредоносных сценариев, загружаемых с Web-страниц;
* защиту от проникновения вредоносных программ и использования уязвимостей за счет использования персонального межсетевого экрана;
* проверку трафика как до получения его программными клиентами, так и после, с целью исключения использования уязвимостей прикладного ПО;
* защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам. В том числе отдельным типам сменных носителей информации, локальным файлам и каталогам, сайтам в сети Интернет;
* ограничения доступа к сети Интернет или к компьютеру в определенный момент времени по расписанию
* помещение найденных зараженных файлов, а также резервных копий объектов, к которым были применены действия, отличные от «Поместить в карантин», в специальное место на жестком диске -«карантин»;
* просмотр местоположения станций и серверов на карте, если заданы географические координаты станции
* автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке.
* защиту возникновения претензий от правообладателей контента путем использования специальной базы данных признаков ресурсов, доступ к которым ограничен по требованию правообладателей.
* Администратор системы должен иметь возможность:
* настройки правил защиты от намеренных/непреднамеренных действий посредством блокировки доступа к локальным и сетевым ресурсам (локальным файлам и каталогам, сайтам в сети Интернет) для конкретных пользователей;
* копировать настройки между учетными записями пользователей;
* запрещать возможность отправки заданий на печать;
* запрещать возможность передачи данных по сети;
* запрещать возможность **изменения системного времени и часового пояса**;
* отключать ранее заданные ограничения для конкретной учетной записи;
* назначать месторасположения карантина при обнаружении зараженных файлов на съемных носителей;
* используя возможности менеджера карантина, осуществлять повторную проверку объектов, помещенных в карантин;
* иметь возможность очистки карантина для отдельного диска.
* Система защиты рабочих станций должна обеспечивать проверку протоколов:
* HTTP, независимо от используемого браузера или иного приложения, получающего трафик;
* IMAP, SMTP, POP3 независимо от используемого почтового клиента;
* NNTP (только проверка на вирусы), независимо от почтового клиента.
* Система защиты рабочих станций должна обеспечивать проверку почтовых сообщений, передаваемых по протоколу MAPI для Microsoft Outlook 2000 (Outlook 9)/2002 (Outlook 10 или Outlook XP)/2003 (Outlook 11)/2007/2010/2013.
* Система защиты рабочих станций должна автоматически обеспечивать проверку трафика передаваемого по поддерживаемым системой защиты протоколам:
* вне зависимости от порта, через который передается трафик - без необходимости указания списка проверяемых портов для конкретных протоколов;
* включая проверку трафика, передаваемого по зашифрованному соединению SSL.
* Система защиты рабочих станций должна обеспечивать фильтрацию трафика в мгновенных сообщениях Mail.Ru Agent, ICQ, Jabber, QIP и другие, включая антивирусную проверку пересылаемых вложений, а также автоматическое удаление из сообщений ссылок, ведущих на вредоносные и фишинговые сайты.
* Система защиты рабочих станций должна обеспечивать фильтрацию выдачи результатов поисковых систем Google, Yandex, Yahoo!, Bing, Rambler с показом только безопасных с точки зрения поисковых систем и системы защиты ресурсов.
* Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макро-вирусов, опасных Java-апплетов, ActiveX и др.) посредством:
* антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
* проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы;
* непрерывного фонового сканирования и нейтрализации активных угроз. В том числе в критических областях Windows, оперативной памяти, запущенных процессах, MBR/VBR дисков, BIOS;
* проверки ссылок и файлов с помощью репутационного сервиса облачной защиты - в том числе с помощью базы данных алгоритмов работы вредоносных программ.
* В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.
* Система должна обеспечивать защиту от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе шифровальщиков, а также блокировщиков экрана) с помощью превентивной защиты, отслеживающей попытки внедрения вредоносных файлов.
* С целью защиты от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе шифровальщиков, а также блокировщиков экрана) Система должна обеспечивать защиту критически важных частей системы (в том числе папок и ветвей реестра) от модификаций вредоносными программами, в том числе блокировать попытки:
* изменения вредоносными программами загрузочных областей диска;
* изменения нежелательным образом пользовательских файлов (в том числе действия троянцев-шифровальщиков) ;
* изменения файла HOSTS;
* добавления новых задач в логику работы операционной системы;
* изменения правил запуска ранее установленных программ;
* измения параметров работы системных служб, в том числе процесса создания резервных копий файлов;
* загрузки новых или неизвестных драйверов без ведома пользователя, установки новых виртуальных устройств, загрузки в браузер вредоносных плагинов, в том числе блокировщиков браузера;
* автозапуска вредоносных программ;
* получения низкоуровневого доступа к диску;
* регистрации вредоносных программ в реестре для последующего запуска;
* отключения безопасного режима Windows путем блокировки изменения реестра;
* сокрытия присутствия троянской программы в контролируемой системе в виде руткита.
* блокировать попытки установления каналов связи между вредоносным ПО, ранее установленным на компьютер и удаленными серверами злоумышленников;
* с помощью превентивной защиты, отслеживающей работу всех процессов системы в поисках действий, характерных для процессов вредоносных программ и не позволяющей вредоносным объектам внедриться в процессы других программ или каким-либо способом разместить вредоносные файлы в защищаемой системе, выявлять и прекращать работу вредоносных, подозрительных или ненадежных сценариев и процессов;
* обеспечивать защиту от эксплойтов (программ, эксплуатирующих как уже известные, так и еще неизвестные уязвимости) путем внедрения специального модуля защиты в контролируемые процессы;
* ограничивать время работы конкретного сотрудника на защищаемом компьютере - с целью исключения доступа к компьютеру в остальное время неопределенного круга лиц.
* Система ограничения доступа должна позволять:
* задавать время работы на компьютере для выходных и будних дней для каждого сотрудника, а также ограничения по доступу в сеть Интернет;
* задавать суммарное время работы на компьютере для конкретного сотрудника;
* автоматически блокировать доступ к защищаемому компьютеру в ночное время.
* ограничивать доступ к определенным ресурсам сети Интернет - согласно белым и черным спискам ресурсов сети, предопределенным группам ресурсов;
* ограничивать доступ к определенным файлам и папкам - с указанием типа доступа объектам (блокировать доступ или разрешать только чтение);
* обеспечивать возможность использования на защищаемом компьютере только устройств, входящих список разрешенных.
* Администратор Системы должен иметь возможность:
* контроля доступа к таким типам устройств, как дисковые накопители, приводы DVD/CD-ROM, клавиатуры, компьютерные мыши, сетевые карты, игровые устройства, USB-устройства;
* импорта и экспорта правил использования устройств (в том числе с помощью функционала управления удаленными компьютерами антивирусной сети), а также формирования правил блокировки шин и классов устройств, создания списка разрешенных устройств для заблокированных шин и классов устройств;
* задать уровень доступа к устройству осуществляется в форме полного запрета доступа всем процессам операционной системы или в форме интерактивного режима, в котором пользователю выводится оповещение о попытке доступа к устройству. Для устройств. с файловой системой администратор Системы должен иметь возможность задать тип доступа - разрешать полный доступ к устройству или доступ только на чтение;
* обеспечивать возможность полного запрета использования USB-устройств и CD/DVD-приводов;
* обеспечивать создание резервных копий папок, указанных пользователем, а также восстановление данных из хранилища как системой защиты, так и самим пользователем в любой момент времени.
* Модуль превентивной защиты должен поддерживать возможность создания профилей - групп настроек, применяемых пользователем или администратором защищаемой системы - как для системы превентивной защиты в целом, так и для конкретных приложений с целью исключения потенциальных конфликтов при их работе.
* Система создания резервных копий папок должна поддерживать возможность:
* выбора защищаемых каталогов;
* выбора диска для хранения защищаемых копий;
* настройки расписаний копирования;
* создания защищенных копий по требованию.
* С целью ускорения проверки Система должна поддерживать возможность исключения из проверки различными компонентами системы защиты:
* данных, передаваемых по защищенным протоколам (в том числе HTTPS), а также трафика доверенных приложений (имеющих валидную цифровую подпись) ;
* файлов и папок;
* ресурсов сети Интернет;
* почтовых адресов;
* доверенных программ;
* С целью ускорения проверки Брандмауэр (файрвол) должен поддерживать **базу доверенных приложений, а также позволять создавать правила работы для приложений.**
* В случае отсутствия централизованного управления системой защиты Система защиты рабочей станции должна поддерживать возможность удаленного управления Системами защиты, установленными на компьютерах в пределах одной локальной сети.
* Подсистема показа статистики Системы защиты должна:
* отображать время возникновения (детектирования) угроз;
* отображать списки запрещенных сайтов, доступ к которым был запрошен с защищаемого компьютера.
* Подсистема статистики должна иметь возможность отображения только необходимых для анализа сообщений - в том числе создания выборки сообщений отдельных компонентов системы защиты, сообщений с определенными кодами
* В случае использования в Системе модуля хранения информации в защищенных файловых контейнерах Система должна обеспечивать:
* безопасную работу с зашифрованной информацией как на отдельно стоящем компьютере, так и при его подключении к сети, в том числе за счет ограничения доступа по сети к защищенной информации;
* создание криптодисков в том числе для съемных носителей;
* шифрование информации, находящейся в файловых контейнерах с помощью стойких алгоритмов шифрования, в том числе AES, Blowfish;
* защиту доступа к контейнерам с помощью пароля;
* гарантированное удаление ненужных файлов без возможности восстановления содержавшейся в них информации.
* В Системе должна быть реализована защита работы собственных модулей от сбоев и случайного изменения.

**Требования к программным средствам антивирусной защиты рабочих станций Linux**

* Система должна обеспечивать проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.
* Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.
* Система, используя актуальную версию программного обеспечения, должна обеспечивать защиту ресурсов рабочих станций функционирующих под управлением операционных систем Linux, имеющих версию ядра 2.6.37 и выше.
* Автоматически создаваемый дистрибутив, предназначенный для установки на защищаемую станцию, должен включать параметры доступа к антивирусному серверу.
* Система установки должна включать возможность автоматической установки модулей, необходимых для компонентов Системы.
* В случае необходимости внесения изменений, Система должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователями в рамках имеющихся у них прав.
* Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции без их предварительного лечения с последующим лечением заданных файловых областей.
* Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
* поиск и удаление вирусов всех известных типов в файлах;
* антивирусного сканирования ресурсов компьютера как по команде администратора, так и по расписанию, заключающегося в однократной полной или выборочной проверке на наличие угроз объектов;
* контроля доступа в сеть интернет, в том числе согласно наличию адресов ресурсов в базе категорий нерекомендованных интернет-ресурсов и черных списках пользователей;
* проверки загружаемых по сети файлов (в том числе с веб-серверов, доступ к которым был разрешен), и блокировки их загрузки, в случае если они содержат угрозы;
* проверки адресов сети Интернет с помощью сервиса облачной проверки;
* помещения найденных зараженных и подозрительных файлов в карантин для дальнейшего анализа;
* автоматического запуска антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой операционной системы;
* запуска задач по расписанию и/или сразу после загрузки операционной системы;
* настройки расписания сканирования с указанием параметров запуска.
* Управление программой должно осуществляться как непосредственно через конфигурационные файлы, так и через графический интерфейс, реализованный для операционных систем типа Linux. Система управления должна поддерживать возможность настройки параметров антивирусного сканирования с указанием файлов и каталогов, подлежащих антивирусной проверке, действий по отношению к вредоносным объектам различных типов.
* Администратор системы должен иметь возможность:
* определять необходимый уровень анализа, в том числе путем отключения эвристического анализа, ограничения размера файла и глубины проверки;
* определять типы проверяемых файлов, в том числе с использованием масок;
* задавать различные действия по отношению к различным типам вредоносных объектов в случае их обнаружения;
* управлять детализацией протоколов антивирусной проверки;
* просматривать информацию об используемом ключевом файле и его владельце;
* запускать периодическую проверку в приоритетном или в фоновом режиме.

**Требования по комплектности поставке**

В состав Системы должны входить:

* программные средства антивирусной защиты, необходимые для выполнения требований данного технического задания;
* программные средства защиты пользователей от нежелательных массовых почтовых рассылок – спама;
* программные средства централизованного управления, мониторинга и обновления;
* обновляемые базы данных сигнатур всевозможных вредоносных программ.

**Требования по технической поддержке Системы**

* Техническая поддержка должна предоставляться на русском языке, круглосуточно без праздников и выходных по электронной почте и через Интернет, а также должна включать прием обращений по телефону в будние дни с 8 до 17 часов по часовому поясу Заказчика, в том числе:
* консультирование по вопросам функционирования системы;
* восстановление работоспособности системы при необходимости посредством подключения;
* обновление версий дистрибутивов программного обеспечения в случае выхода новых версий;
* обновление вирусных баз системы.
* Техническая поддержка должна включать возможность проведения расследования компьютерных инцидентов.
* Техническая поддержка должна включать возможность написания специального программного обеспечения, предназначенного для устранения последствий воздействия вредоносного программного обеспечения на зараженную систему. В том числе утилит расшифровки файлов, если данная операция является возможной.
* Web-сайт производителя Системы должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке, пополняемую базу знаний, а также форум пользователей программных продуктов производителя.
* Срок действия технической поддержки должен составлять не менее 12 месяцев.

Приложение № 11

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019

СОГЛАШЕНИЕ
О КОНФИДЕНЦИАЛЬНОСТИ

Статья 1

1.1. Термины и определения:

В настоящем Соглашении указанные ниже термины имеют следующие значения:

«Принимающая сторона»:

в отношении Конфиденциальной информации, принимаемой Заказчиком от Исполнителя - Заказчик;

в отношении Конфиденциальной информации, принимаемой Исполнителем от Заказчика - Исполнитель.

«Раскрывающая сторона»:

в отношении Конфиденциальной информации, раскрываемой Заказчиком - Заказчик;

в отношении Конфиденциальной информации, раскрываемой Исполнителем - Исполнитель.

«Конфиденциальная информация» - сведения любого характера (производственного, технического, экономического, организационного и другого), которыми обладает Раскрывающая сторона, в том числе о результатах интеллектуальной деятельности, а также сведения о способах осуществления профессиональной деятельности к которым у третьих лиц нет свободного доступа на законном основании и которые отнесены Раскрывающей стороной к сведениям ограниченного распространения.

«Разглашение Конфиденциальной информации» - действие или бездействие Принимающей стороны, в результате которых Конфиденциальная информация, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия Раскрывающей стороны, либо вопреки настоящему Соглашению или иным договорам, заключенным между Сторонами, в т.ч. раскрытие сведений о факте сотрудничества Сторон и тематике такого сотрудничества.

1.2. Стороны договорились, что информация, полученная Принимающей Стороной в процессе заключения, исполнения, изменения, расторжения или окончания срока действия Договора и совместных проектов, а так же в процессе переговоров, консультаций, обмена сведениями и документами и т.п. будет являться Конфиденциальной информацией при соблюдении нижеуказанных условий:

а. Конфиденциальная информация предоставляется в документарной форме или на электронном носителе, и эта информация или ее носитель содержат гриф «Конфиденциально» или «Для служебного пользования» с указанием обладателя информации;

б. Конфиденциальная информация, которая предоставляется визуально, устно или в другой бездокументарной форме, ясно определена Стороной как Конфиденциальная.

Информация не может быть признана Конфиденциальной если:

а. на дату раскрытия информация является общедоступной, то есть:

* Раскрывающая сторона не принимает мер к охране ее конфиденциальности; или
* информация не относится к сведениям ограниченного распространения (Конфиденциальной информации) в силу требований действующего законодательства или нормативно-правовых актов Российской Федерации; или
* информация является публично известной в результате действий и решений самой Раскрывающей стороны;

б. информация находилась в законном владении у Принимающей стороны до момента заключения настоящего Соглашения (как следует из письменных записей или иных свидетельств), и на нее не распространялись какие-либо ограничения на использование до ее раскрытия;

в. информация получена Принимающей стороной (как следует из письменных записей или иных свидетельств) от третьих лиц, которые не связаны обязательством конфиденциальности с Раскрывающей стороной в отношении указанной информации;

г. информация изменила статус в результате заключенных впоследствии Сторонами соглашений.

Статья 2

2.1. Принимающая сторона должна обеспечить хранение Конфиденциальной информации в тайне и не раскрывать ее любым другим лицам, за исключением случаев, указанных в настоящем Соглашении, и не использовать эту информацию для своей собственной выгоды или выгоды третьих лиц, кроме как в рамках исполнения обязательств и предоставления услуг Раскрывающей стороне.

2.2. Принимающая сторона самостоятельно определяет список сотрудников, которым раскрывается Конфиденциальная информация, при условии, что указанные лица примут на себя обязательство сохранять в тайне известную им Конфиденциальную информацию в течение срока, указанного в п. 3.5 Соглашения. Раскрывающая сторона вправе запросить, а Принимающая сторона предоставить список сотрудников, допущенных к Конфиденциальной информации.

2.3. Принимающая сторона обязуется принимать необходимые меры по предотвращению утечки, хищения, утраты, искажения, подделки Конфиденциальной информации, а так же по предотвращению несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию Конфиденциальной информации.

Для защиты Конфиденциальной информации Принимающая сторона обязуется принимать меры предосторожности необходимые и достаточные для защиты такого рода информации.

2.4. Принимающая сторона гарантирует, что она:

будет использовать любую Конфиденциальную информацию, полученную от Раскрывающей стороны, исключительно для целей реализации работ необходимых для исполнения обязательств по Договору, предварительно согласованных Сторонами;

в случае передачи с письменного согласия Раскрывающей стороны Конфиденциальной информации о проводимых совместных работах и реализуемых проектах, включая идеологические и технические решения, планы и сроки реализации, третьим лицам - своим партнёрам (клиентам), Принимающая сторона обязана обеспечить выполнение этими третьими лицами требований о конфиденциальности, установленных настоящим Соглашением, и нести ответственность за публичное разглашение Конфиденциальной информации такими третьими лицами;

не будет в течение срока действия настоящего Соглашения раскрывать и/или передавать Конфиденциальную информацию какой-либо третьей Стороне, а также осуществлять действий (или бездействий), результатом которых может быть раскрытие или передача Конфиденциальной информации третьим лицам. Конфиденциальная информация может быть раскрыта только сотрудникам Принимающей стороны, имеющим непосредственное отношение к работам проводимым в рамках Договора с соблюдением условий п.2.2 Соглашения;

проинформирует своих сотрудников, которым Конфиденциальная информация раскрывается в соответствии с предыдущим подпунктом, об обязанностях, возникающих у Принимающей стороны по настоящему Соглашению, и проведет необходимое обучение таких сотрудников способам обеспечения конфиденциальности;

будет снимать с любых материальных носителей, на которых хранится переданная ей Конфиденциальная информация, только такое количество копий, которое обусловлено необходимостью надлежащего исполнения своих обязательств в рамках Мероприятий;

по требованию Раскрывающей стороны и в сроки, указанные ей, уничтожит всю Конфиденциальную информацию, которую будет невозможно передать Раскрывающей стороне в соответствии с пунктом 2.5 Соглашения, и, которая будет находиться на технических средствах Принимающей стороны.

2.5. Все материальные носители, на которых Конфиденциальная информация была передана, Принимающей стороне в соответствии с Соглашением, договорами, указанными в п. 1.2 Соглашения, Мероприятиями, а так же любые снятые с них копии являются собственностью Раскрывающей стороны и подлежат возврату Раскрывающей стороне по ее первому требованию.

Статья 3

3.1. В случае возникновения угрозы разглашения Конфиденциальной информации, а так же в случае разглашения (раскрытия Конфиденциальной информации в нарушение условий настоящего Соглашения), Принимающая сторона обязуется немедленно уведомить об этом Раскрывающую сторону, обеспечить ей содействие, которое потребует Раскрывающая сторона для предотвращения разглашения (раскрытия) Конфиденциальной информации, и оказать ей необходимое и достаточное содействие для предотвращения раскрытия Конфиденциальной информации.

3.2. Раскрывающая сторона вправе в любое время по своему усмотрению давать распоряжения Принимающей стороне о возврате/передаче Конфиденциальной информации, полученной от Раскрывающей стороны, включая ее носители, а так же иных документов, содержащих Конфиденциальную информацию, об уничтожении всей, либо части Конфиденциальной информации, а Принимающая сторона обязуется в течение 5 (пяти) рабочих дней (если иной срок не указан Раскрывающей стороной) исполнять такие распоряжения и сообщать Раскрывающей стороне о результатах.

3.3. Принимающая сторона в полном объёме возмещает Раскрывающей стороне документально подтвержденные убытки, понесённые ею в случае совершения Принимающей стороной действий, повлекших за собой разглашение (в т.ч. утечку, хищение, утрату, иное несанкционированное раскрытие), а также искажение, подделку, модификацию, копирование, блокирование, раскрытие Конфиденциальной информации, равно как и все убытки, понесенные Раскрывающей стороной, в случае нарушения Принимающей стороной своих обязательств по настоящему Соглашению. Возмещение убытков, в данном случае, осуществляется Принимающей стороной в течение 15 (пятнадцати) календарных дней с даты предъявления Раскрывающей стороной обоснованного и документально подтвержденного требования.

3.4. Передача информации по настоящему Соглашению третьим лицам осуществляется только при наличии предварительного письменного согласия Раскрывающей стороны.

3.5. Настоящее Соглашение вступает в силу с момента его подписания и прекращает действие по истечении 5 (пяти) лет с момента завершения работ по Договору и окончания срока действия, (расторжения) соглашений, указанных в абзаце 1 пункта 1.2 Соглашения.

3.6. Все приложения, изменения и дополнения к настоящему Соглашению действительны при условии, что они совершены в письменной форме, подписаны обеими Сторонами и скреплены печатями. Приложения, изменения и дополнения, оформленные надлежащим образом, являются неотъемлемой частью настоящего Соглашения.

3.7. Во всем, что не урегулировано настоящим Соглашением, Стороны руководствуются действующим законодательством Российской Федерации.

3.8. Настоящее Соглашение регулируется и толкуется в соответствии с действующим законодательством Российской Федерации. Все споры, разногласия или требования, возникающие из настоящего Соглашения или в связи с ним, в том числе касающиеся его исполнения, нарушения, прекращения или недействительности, подлежат разрешению в Арбитражном суде Республики Алтай в соответствии с действующим законодательством Российской Федерации.

3.9. Любое уведомление, запрос или иное сообщение по настоящему Соглашению должно быть передано персонально с курьером по адресу, указанному ниже:

В отношении Заказчика:

649000, Республика Алтай, г. Горно-Алтайск, пр-кт Коммунистический, 54

В отношении Исполнителя:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

При этом каждая из Сторон вправе изменить указанные выше реквизиты, уведомив при этом другую Сторону, в письменном виде, не менее чем за 5 (пять) рабочих дней.

3.10. Настоящее Соглашение подписано в 2 (двух) экземплярах, каждый из которых обладает равной юридической силой.

|  |  |
| --- | --- |
| От Заказчика: | От Исполнителя: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_ / |

Приложение № 12

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019

Лицензионное соглашение о предоставлении права использования программного обеспечения

|  |  |
| --- | --- |
| г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  | «\_\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 \_\_\_\_ г. |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Лицензиар», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Лицензиат», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании Устава, с другой стороны, в дальнейшем совместно именуемые «Стороны», заключили настоящий лицензионное соглашение (далее по тексту – «Соглашение») о нижеследующем:

1. Термины и определения

1.1. Используемые в настоящем Соглашении следующие термины понимаются Сторонами в указанных ниже значениях:

1.2. «Лицензия» – простая (неисключительная) лицензия на право использования ПО, предоставляемая Лицензиаром Лицензиату на условиях настоящего Соглашения.

1.3. «ПО» – программное обеспечение, включающее модули, указанные в Приложении № 2 к настоящему Соглашению, Лицензию на право использования которого Лицензиар предоставляет Лицензиату на условиях настоящего Соглашения.

1.4. «Правообладатель ПО» – лицо, которому принадлежит исключительное право на ПО.

1.5. «Контракт» - государственный контракт № \_\_\_ заключенный Сторонами \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_г.,

1. Предмет Соглашения
	1. Лицензиар во исполнение Контракта предоставляет Лицензиату Лицензию на право использования ПО на условиях, указанных в настоящем Соглашении и Контракте.
	2. Лицензия передается Лицензиату на срок предоставления услуг по Контракту для использования на территории \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Субъект РФ).
	3. Лицензиату предоставляются права использования ПО следующими способами:
		1. право использования ПО для собственных нужд с целью автоматизации функций, выполняемых пользователями в рамках их должностных обязанностей.
	4. Стороны настоящим соглашаются, что Лицензиат вправе использовать в соответствии с условиями Соглашения отдельные его элементы – модули, перечисленные в таблице 1 Приложения 2 Контракта.
		1. Лицензиат не вправе:
		2. передавать Лицензии на использование ПО иным лицам, кроме указанных в настоящем Соглашении.
		3. модифицировать, дополнять, декомпилировать, подвергать инженерному анализу, разбирать, переводить, реорганизовывать, исправлять ошибки или производить какие-либо иные изменения в ПО или Документации к нему.
		4. удалять, изменять или скрывать любые уведомления об авторских правах, товарные знаки или другие уведомления об имущественных правах Лицензиара, содержащиеся в ПО.
2. Гарантии лицензиара
	1. Настоящим Лицензиар заверяет и гарантирует, что:
		1. он вправе предоставлять Лицензию на использование ПО в объеме, предусмотренном Соглашением;
		2. ПО соответствует требованиям действующего законодательства, а также что никакая часть и никакие элементы ПО не нарушают чьих-либо законных прав;
		3. использование ПО Лицензиатом в соответствии с условиями настоящего Соглашения не будет нарушать или каким-либо образом ущемлять любые законные права третьих лиц;
		4. право на использование ПО не состоит под арестом, не находится в залоге, в отношении прав использования ПО не ведётся судебного разбирательства, что право использования ПО не является предметом иных имущественных прав и притязаний третьих лиц, в результате которых Лицензиат может утратить право на предоставление Лицензии, предусмотренной Соглашением.
3. Порядок предоставления лицензий
	1. Предоставление ПО для использования осуществляется посредством предоставления удаленного доступа к ПО, размещенному на технических средствах \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Лицензия считается переданной с момента подписания настоящего Лицензионного соглашения.
	2. В случае, если ПО снабжено техническими средствами защиты информации, Лицензиат обязуется одновременно с передачей Лицензии предоставить Лицензиару ключи, коды и иные подобные сведения, необходимые для использования ПО способами, указанными в настоящем Соглашении.
4. Ответственность сторон
	1. В случае предъявления Лицензиату каких-либо претензий (включая претензии, иски и иные требования) со стороны третьих лиц в связи с нарушением интеллектуальных прав на ПО, Исполнитель обязуется самостоятельно урегулировать все претензии, обеспечить судебную защиту и возместить Лицензиату реально причиненный ущерб, связанный с предъявлением таких претензий. В случае предъявления указанных претензий, требований и/или исков Лицензиат обязан незамедлительно письменно уведомить об этом Лицензиара и передать ему все материалы, касающиеся указанных требований, а также оказать разумное содействие Лицензиару для урегулирования споров. Лицензиар самостоятельно определяет способы защиты интересов, включая судебное разбирательство либо урегулирование спора мирным путем, урегулирует споры своими силами и за свой счет.

|  |  |
| --- | --- |
| От Лицензиата:Должность подписывающего | От Лицензиара:Должность подписывающего |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Фамилия И.О. / | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Фамилия И.О. / |

Приложение № 13

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019

ПОРУЧЕНИЕ
 ОПЕРАТОРА РС ЕГИСЗ РЕСПУБЛИКИ АЛТАЙ НА ОБРАБОТКУ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1. В соответствии с Контрактом Исполнитель (далее Обработчик), по поручению Заказчика, осуществляет обработку информации (персональных данных) о пациентах, сотрудниках медицинских организаций Республики Алтай и другую информацию на своей технологической площадке и технологическом оборудовании соблюдая конфиденциальность и обеспечивая целостность и доступность обрабатываемой информации.

2. Обработчик обязан осуществлять обработку следующей информации (сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение) по поручению Заказчика:

2.1. Информация о пациентах (персональные данные, факты обращения в медицинские организации, принадлежность к группе, диагнозы, анамнезы, назначения и рекомендации, состояние и ход лечения пациента, себестоимость, способы оплаты, обезличенные агрегированные данные, входящие в статистическую информацию и составляющие служебную информацию).

2.2. Информация сотрудников медицинских организаций Республики Алтай (персональные данные, специализации сотрудников учреждений здравоохранения, кадровая информация, графики работы).

2.3. Справочная информация, описывающая медицинские организации (физическая структура учреждения здравоохранения, функциональная структура, территориальные участки, штатное заполнение, ресурсы, услуги).

2.4. Справочная информация, описывающая предметную область (справочники услуг, МКБ-10, схемы наблюдения диспансерного учёта и т.п.). К данной информации предъявляются требования к обеспечению целостности и доступности.

2.5. Финансовая и другие виды информации конфиденциального характера, отнесённые к данной категории Оператором.

3. Исполнитель обязан соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», а также другими нормативными правовыми актами Российской Федерации в области защиты персональных данных и безопасности информации.

4. В рамках реализации настоящего Поручения Оператор (Заказчик) имеет право требовать от Обработчика представления надлежащим образом оформленной отчётной документации и материалов, подтверждающих исполнение обязательств по настоящему Контракту (описание актуальных угроз, модель нарушителя и т.п.), а также проводить проверку качества оказания услуги на предмет соответствия её действующему законодательству в области защиты информации.

5. Обработчик обязуется:

5.1. Соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006г. №152-ФЗ «О персональных данных».

5.2. Осуществлять обработку конфиденциальной информации только в целях определённых Контрактом.

5.3. Осуществлять хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

5.4. Принять надлежащие технические, организационные и правовые меры по обеспечению безопасности обработки конфиденциальной информации в соответствии с требованиями действующего законодательства в области защиты информации КСИИ. Выполнять предписания Оператора по защите информации.

5.5. Обеспечивать конфиденциальность обрабатываемой информации, а также применять меры по её защите.

5.6. Провести оценку эффективности принимаемых мер (аттестацию) по обеспечению безопасности обрабатываемой информации до момента предоставления Услуги;

5.7. Следить за тем, чтобы его сотрудники строго выполняли условия конфиденциальности и требования по защите информации.

5.8. Проследить, чтобы любая третья сторона, которой были раскрыты персональные данные, соблюдала условия конфиденциальности.

5.9. По письменному требованию Оператора подтвердить в письменной форме, что он соблюдает обязательства по настоящему Контракту в части обработки и защиты информации.

5.10. По письменному требованию Оператора блокировать неправомерную обработку информации.

5.11. Предоставлять Оператору необходимую информацию для подготовки ответа на запросы субъектов персональных данных об обрабатываемых персональных данных.

5.12. Проводить резервирование программ и данных электронных сервисов РС ЕГИСЗ в режиме реального времени с возможностью обеспечить восстановление программ и актуальных данных в случае сбоя.

5.13. Осуществлять обработку информации от имени Оператора, исключительно в соответствии с указаниями Оператора и совместно с Оператором.

5.14. Нести ответственность перед Оператором согласно ст. 6 п.5 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», в том числе за утечку или разглашение обрабатываемой информации третьим лицам.

5.14. Исполнять иные обязательства, предусмотренные действующим законодательством и Контрактом.

6. В случае реорганизации или ликвидации одной из Сторон, Обработчик обязуется незамедлительно прекратить осуществление обработки информации, передать её в защищённом виде Заказчику и затем уничтожить без возможности последующего восстановления.

7. Обеспечение защиты информации при её обработке в комплексной республиканской информационной системе должно быть достигнуто Обработчиком:

- определением угроз безопасности персональных данных при их обработке в информационных системах;

- формированием требований к системе защиты информации информационной системы и разработкой системы защиты информации информационной системы;

- реализацией системы защиты информации информационной системы и аттестацией информационной системы на соответствие требованиям о защите информации и ввод ее в действие;

- эксплуатацией системы защиты информации информационной системы. Обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

- обеспечением регистрации и учёта всех действий, совершаемых с персональными данными в информационной системе;

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного или случайного доступа к ним и защиту информации при выводе из эксплуатации информационной системы или после окончания обработки информации.

Приложение № 14

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019

ФОРМА

г. Горно-Алтайск «\_\_»\_\_\_\_\_\_\_ 20\_\_ г.

Акт сдачи-приемки оказанных услуг

Заказчик: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Исполнитель: \_\_\_\_\_\_\_\_\_\_\_

Договор: №\_\_\_\_от «\_\_\_» \_\_\_\_\_\_ 2015 г.

Наименование Услуг: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Мы, нижеподписавшиеся, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с одной стороны и, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ именуемое в дальнейшем «Исполнитель», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_, с другой стороны, составили настоящий акт в том, что:

1. Исполнителем оказаны Услуги в соответствии с Договором №\_\_ от «\_\_\_» \_\_\_\_\_ 2015 г., полностью и надлежащим образом оформлены.

2. Стоимость оказанных Услуг составляет: \_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_) рублей \_\_ копеек, в том числе НДС 18% в размере \_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_) рублей \_\_\_ копеек.

3. Сумма, подлежащая оплате, составляет: \_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_) рублей \_\_ копеек, в том числе НДС 18% в размере \_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_) рублей \_\_\_\_ копеек.

4. Настоящий акт является неотъемлемой частью Договора №\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_ 2015 г. и основанием для расчетов между Заказчиком и Исполнителем.

5. Настоящий акт составлен в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой стороны.

|  |  |
| --- | --- |
| От Заказчика: | От Исполнителя: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_/м.п. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_ /м.п. |

ФОРМА акта утверждена

|  |  |
| --- | --- |
| От Заказчика: | От Исполнителя: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_/м.п. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_ /м.п. |

ФОРМА

Отчет об оказанных услугах за период (наименование периода)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Отчет по инцидентам с критичностью отказа более 4 часов |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| Код инцидента | Наименование инцидента | Приоритет | Статус | Дата создания | Дата закрытия | Задетые инцидентом МО | Отклонение, часов |  |
|   |   |   |   |   |   |  |   |  |
|   |   |   |   |   |   |  |   |  |
| Итого |  |  |  | Итого отклонение, часов: |  |   |  |
|  |  |  |  |  |  |  |  |  |  |
| 2. Отчет по проведению регламентных работ |  |  |  |  |
| № п/п | Наименование работ | Дата уведомления | Начало работ | Окончание работ | Задетые работами МО |  |  |  |  |
|   |   |   |   |   |  |  |  |  |  |
|   |   |   |   |   |  |  |  |  |  |

Форма квартального отчета утверждена:

|  |  |
| --- | --- |
| От Заказчика: | От Исполнителя: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_/м.п. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_\_ /м.п. |

Приложение № 15

к Контракту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 \_\_\_\_\_

Список лиц выполняющих работы и их непосредственных руководителей

1. В случае, если иные сроки не согласованы сторонами [↑](#footnote-ref-2)