***Проект***

**ЗАДАНИЕ НА ПРОЕКТИРОВАНИЕ**

ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ УСЛУГИ

«ЦИФРОВОЕ РАБОЧЕЕ МЕСТО ГОСУДАРСТВЕННОГО СЛУЖАЩЕГО»

на \_\_\_\_\_\_\_ листах

|  |  |  |
| --- | --- | --- |
|  |  | **СОГЛАСОВАНО** |
| **СОГЛАСОВАНО** |  | **РАЗРАБОТАНО**  |

Оглавление

[1. Общие сведения 7](#_Toc108601126)

[1.1 Цель документа 8](#_Toc108601127)

[1.2. Список принятых сокращений и терминов 8](#_Toc108601128)

[1.3. Нормативные правовые акты 10](#_Toc108601129)

[1.4. Назначение ИК-услуги 12](#_Toc108601130)

[1.5. Цель и задачи создания ИК-услуги 12](#_Toc108601131)

[1.6. Характеристика объекта автоматизации 12](#_Toc108601132)

[1.7. Класс электронного информационного ресурса и прикладного программного обеспечения 13](#_Toc108601133)

[1.8. Механизмы и этапы создания СПП 14](#_Toc108601142)

[2. Предельная стоимость аренды СПП 18](#_Toc108601143)

[3. Предельная стоимость ИК-услуги 18](#_Toc108601144)

[4. Функциональные требования к СПП 18](#_Toc108601145)

[4.1 Общее описание функционала СПП 18](#_Toc108601148)

[4.2. Детальное описание процессов и сценарии использования 22](#_Toc108601149)

[5 Требования и ограничения, связанные с ИК платформой ЭП 33](#_Toc108601150)

[5.1 Общие требования 33](#_Toc108601151)

[5.2 Технологические требования СПП 34](#_Toc108601152)

[5.2.1 Требования к среде тестирования: 35](#_Toc108601153)

[5.2.2. Хранение данных 35](#_Toc108601154)

[5.3 Требования ИК платформы ЭП к СПП 35](#_Toc108601155)

[5.4 Ограничения к вычислительным ресурсам 35](#_Toc108601156)

[6. Требования к интеграции с объектами информатизации «электронного правительства» или другими информационными системами 36](#_Toc108601157)

[6.2. Требования к информационному взаимодействию с УЦ ГО РК 39](#_Toc108601158)

[6.3. Требования к информационному взаимодействию с другими ИС 39](#_Toc108601159)

[7. Требования к надежности, отказоустойчивости, производительности и масштабируемости 39](#_Toc108601160)

[7.1. Требования к отказоустойчивости и бесперебойности 40](#_Toc108601161)

[7.2. Требования к производительности и масштабируемости 40](#_Toc108601162)

[7.3. Требования к надежности 41](#_Toc108601163)

[8. Требования к информационной безопасности 41](#_Toc108601164)

[8.1. Общие требования к информационной безопасности 41](#_Toc108601165)

[8.2. Мониторинг обеспечения безопасного функционирования объектов информатизации ЭП 46](#_Toc108601174)

[8.3. Требование к журналированию 46](#_Toc108601175)

[8.4. Требования к организации защиты информации 47](#_Toc108601176)

[9. Требования к взаимодействию с системой мониторинга 48](#_Toc108601177)

[10. Условия и требования к вводу в эксплуатацию ИК-услуги, СПП и требования к технической документации 49](#_Toc108601178)

[10.1. Требования к документации 49](#_Toc108601179)

[10.2. Требования к порядку и условиям передачи сервисного программного продукта 53](#_Toc108601180)

[10.3. Требование к приемке 53](#_Toc108601181)

[10.4. Требования к развертыванию 54](#_Toc108601182)

[10.5. Порядок конфигурирования и настройки СПП 54](#_Toc108601183)

[10.6. Требование по миграции данных 54](#_Toc108601184)

[10.7. Требования к исходным кодам 55](#_Toc108601185)

[10.8. Требования к пользовательскому интерфейсу 56](#_Toc108601186)

[11. Требования к процессу и материалам обучения пользователей 57](#_Toc108601187)

[11.1. Требование к процессу обучения 57](#_Toc108601188)

[11.2. Требования к материалам обучения пользователей 57](#_Toc108601189)

[12. Требование к прототипу СПП 57](#_Toc108601190)

[13. План коммуникаций и матрица ответственности создания СПП 58](#_Toc108601191)

[14. Дополнительные требования и условия по созданию ИК-услуги, СПП 61](#_Toc108601192)

# Общие сведения

# Цель документа

Настоящий документ разработан в целях описания основных требований по созданию информационно - коммуникационной услуги «Цифровое рабочее место государственного служащего».

В данном документе определяются функциональные и технические требования для потенциальных поставщиков, обеспечивающих реализацию сервисного программного продукта, а также требования и условия для предоставления ИК-услуги Оператором ИК-инфраструктуры для Заказчика ИК-услуги.

Настоящий документ разработан в соответствии с Приказом и.о. Министра по инвестициям развитию Республики Казахстан «Об утверждении Правил реализации сервисной модели информатизации» от 28 января 2016 года № 129.

# Список принятых сокращений и терминов

 Таблица 1. Список принятых терминов

|  |  |
| --- | --- |
| **Принятые термины** | **Полное наименование** |
| SSO | Single Sign-On - схема аутентификации, которая позволяет пользователю войти с одним идентификатором и паролем в любую из нескольких связанных, но независимых программных систем |
| Акционерное общество «Государственная техническая служба» | Юридическое лицо, осуществляющее согласование задания на проектирование ИК-услуги на соответствие требованиям информационной безопасности и испытания ИК-услуги на соответствие требованиям информационной безопасности |
| Аппаратно-программный комплекс  | совокупность программного обеспечения и технических средств, совместно применяемых для решения задач определенного типа |
| Заказчик информационно-коммуникационной услуги (далее – Заказчик ИК - услуги) | Государственный орган, в том числе местный исполнительный орган области, города республиканского значения автоматизирующий деятельность по сервисной модели информатизации, в том числе выступающий как государственный партнер в договоре государственно-частного партнерства по сервисной модели информатизации |
| Информационно-коммуникационная услуга | Услуга или совокупность услуг по имущественному найму (аренде)и (или) размещению вычислительных ресурсов, предоставлению программного обеспечения, программных продуктов, сервисных программных продуктов и технических средств в пользование, включая услуги связи, посредством которых обеспечивается функционирование данных услуг |
| Оператор информационно - коммуникационной инфраструктуры «электронного правительства» (далее - Оператор) | Юридическое лицо, определяемое Правительством Республики Казахстан, на которое возложено обеспечение функционирования закрепленной за ним информационно-коммуникационной инфраструктуры «электронного правительства» |
| Поставщик | Индивидуальный предприниматель, простое товарищество, временное объединение юридических лиц (консорциум) или юридическое лицо, за исключением лиц, выступающих государственными партнерами в соответствии с настоящими Правилами, осуществляющее деятельность в сфере информационно-коммуникационных технологий и претендующий на предоставление в аренду сервисного программного продукта или объекта информационно-коммуникационной инфраструктуры, необходимые для оказания информационно-коммуникационной услуги |
| Потенциальный поставщик | Потенциальный поставщик, определенный конкурсной комиссией по разработке, предоставлению в аренду сервисный программный продукт или объект информационно-коммуникационной инфраструктуры, а также иные услуги, необходимые для оказания информационно-коммуникационной услуги, в том числе выступающий как частный партнер в договоре государственно-частного партнерства по сервисной модели информатизации |
| Программное обеспечение  | совокупность программ, программных кодов, а также программных продуктов с технической документацией, необходимой для их эксплуатации |
| Сервисный интегратор | Юридическое лицо, определенное [постановлением](https://adilet.zan.kz/rus/docs/P1600000207#z1) Правительства Республики Казахстан от 11 апреля 2016 года № 207 "Об определении сервисного интегратора «электронного правительства», на которого возложены функции по разработке задания на проектирование информационно-коммуникационной услуги, организации создания и развития информационно-коммуникационных услуг по сервисной модели информатизации |
| Сервисный программный продукт | Программный продукт, предназначенный для реализации информационно-коммуникационной услуги |
| Средство защиты информации | программное обеспечение, технические и иные средства, предназначенные и используемые для обеспечения защиты информации |
| Токен | вид цифрового актива, являющийся цифровым средством учета, обмена и удостоверения имущественных прав |
| Хостинг  | услуга по аренде вычислительных мощностей |

Таблица 2. Список сокращений

|  |  |
| --- | --- |
| **Принятое сокращение** | **Полное наименование** |
| АО «ГТС» | Акционерное общество «Государственная техническая служба» |
| АО «НИТ» | Акционерное общество «Национальные информационные технологии» |
| АРМ |  Автоматизированное рабочее место |
| БД | База данных |
| ВШЭП | Внешний шлюз «электронного правительства» |
| ГО | Государственный орган |
| ЕСМ | Единая система мониторинга |
| ЕТ | Единые требования |
| ЕТС ГО | Единая транспортная среда государственных органов |
| ЕШДИ | Единый шлюз доступа к Интернету |
| ЗНП | Задание на проектирование |
| ИБ | Информационная безопасность |
| ИКИ | Информационно-коммуникационная инфраструктура |
| ИКП ЭП | Информационно-коммуникационная платформа «электронного правительства» |
| ИПГО | Интранет-портал государственных органов |
| ИС | Информационная система |
| НК ЦИБ | Национальный координационный центр информационной безопасности |
| НПА РК | Нормативно правовые акты Республики Казахстан |
| НСИ | Нормативно справочная информация |
| ПО | Программное обеспечение |
| ППО | Прикладное программное обеспечение |
| ППРК | Постановление Правительства РК |
| СЗИ | Средства защиты информации |
| СПП | Сервисный программный продукт |
| СТП | Структурное подразделение |
| СУБД | Система управления базами данных |
| ТГО | Территориальные государственные органы |
| ТД ИБ | Техническая документация по информационной безопасности |
| УО | Уполномоченный орган в сфере информатизации |
| УРМ | Удаленное рабочее место |
| УЦГО | Удостоверяющий центр государственных органов РК |
| ЦГО | Центральные государственные органы |
| ЦРМ | Цифровое рабочее место государственного служащего |
| ШЭП | Шлюз «электронного правительства» |
| ЭЦП | Электронно-цифровая подпись |
|  |  |

# Нормативные правовые акты

Настоящий документ был разработан в соответствии со следующими нормативными правовыми актами:

1. Закон Республики Казахстан от 10 июня 1996 года «Об авторском праве и смежных правах»[1];
2. Закон Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи» [2];
3. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК [3];
4. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» [4];
5. Приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187 «Об утверждении Правил проверки подлинности электронной цифровой подписи» (далее – Правила проверки) [5];
6. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан «Об утверждении Правил реализации сервисной модели информатизации» от 28 января 2016 года № 129 (в редакции приказа Министра информации и коммуникаций Республики Казахстан от 28 июня 2018 года № 295) [6];
7. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан «Об утверждении Правил классификации объектов информатизации, и классификатор объектов информатизации» от 28 января 2016 года № 135 [7];
8. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан «Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно- коммуникационной инфраструктуры» от 28 марта 2018 года № 52/НҚ [8];
9. Приказ исполняющего обязанности Министра информации и коммуникаций Республики Казахстан от 29 марта 2018 года № 123 «Об утверждении Правил интеграции объектов информатизации «электронного правительства» [9];
10. Приказ Председателя Комитета национальной безопасности Республики Казахстан от 23 октября 2018 года № 86/қе «Об утверждении цен на услуги, реализуемые субъектом государственной монополии в сферах информатизации, обеспечения информационной безопасности» [10];
11. Приказ министра цифрового создания, оборонной и аэрокосмической промышленности Республики Казахстан «Об утверждении методики и правил проведения испытаний объектов информатизации «электронного правительства» и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности» от 3 июня 2019 года № 111/НҚ [11];
12. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан «Об утверждении методики расчета и нормативов затрат на создание, создание и сопровождение объектов информатизации государственных органов» от 27 июня 2019 года № 140/НҚ [12];
13. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29 июня 2019 года «Об утверждении Правил учета и хранения разработанного программного обеспечения, исходных программных кодов (при наличии), комплекса настроек лицензионного программного обеспечения объектов информатизации «электронного правительства» [13];
14. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан «Об утверждении Методики расчета стоимости информационно-коммуникационных услуг для государственных органов» от 12 июля 2019 года № 158/НҚ [14];
15. СТ РК ГОСТ Р 50739-2006 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования [15];
16. СТ РК 1073-2007 «Средства криптографической защиты. Общие технические требования» (далее – СТ РК 1073-2007) [16];
17. СТ РК ISO/IEC 27001-2015 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования [17];
18. СТ РК ISO/IEC 27002-2015 Методы обеспечения защиты. Свод правил по управлению защитой информации [18].

*Далее по тексту указанные документы обозначены в виде аббревиатуры [] в соответствии с их нумерацией*

# Назначение ИК-услуги

Создание ИК-услуги предназначено для оптимизации работы государственных служащих и повышения эффективности деятельности государственных органов. Для реализации ИК-услуги должен быть разработан новый СПП.

#

# Цель и задачи создания ИК-услуги

Целью создания СПП является формирование единой информационной среды для государственных служащих, в виде объединения всех информационных ресурсов ГО в одно окно.

Создание и внедрение СПП способствует достижению следующих результатов:

* упрощение доступов к разнородным информационным ресурсам;
* обеспечение единой точки доступа/входа к сервисам государственных органов;
* оптимизации работы государственных служащих.

Задачи СПП:

* формирование единого интерфейса доступа к различным информационным системам, ресурсам ГО;
* система идентификации пользователя;
* сервисы управления правами и ролями пользователей;
* мониторинг и оценка результатов поручений;
* сервис уведомлений и напоминаний;
* единый справочник работников ГО;
* управление календарем и планирование задач;
* обеспечение взаимодействия пользователей;
* анализ эффективности государственных служащих;
* мобильная версия (планшет) цифрового рабочего места;
* осуществление подачи всех видов заявок.

# Характеристика объекта автоматизации

Количество государственных органов, которые будут пользоваться СПП:

* + - ГО подотчетные Президенту – не менее 9;
		- ЦГО (Комитеты, ТГО) – не менее 1700;
		- МИО – не менее 3 200.

Количество пользователей СПП:

* + - ГО подотчетные Президенту – не менее 3421;
		- ЦГО (Комитеты, ТГО) – не менее 95 846;
		- МИО – не менее 46 293.

 Детальный план внедрения СПП будет предоставлен после ввода СПП в действие.

В процессе эксплуатации количество пользователей может быть увеличено в рамках указанной предельной стоимости аренды СПП, с учетом стоимости доработки СПП и сопровождения кодов СПП.

Разделение прав доступа пользователей к функционалу СПП должно быть проведено в соответствии с пользовательскими ролями, представленными в таблице 3 ниже.

 Таблица 3. Пользователи и их роли

|  |  |  |
| --- | --- | --- |
| № п/п. | **Наименование ролей** | **Характеристика/описание** |
|  | Администратор ЦРМ | * управление ролями;
* управление учетными записями (создание, редактирование и удаление учетных записей);
* мониторинг действий пользователей по логам событий;

- диагностика и устранение программных и аппаратных неисправностей ЦРМ;- мониторинг журнала логирования действий;- резервирование копирование и восстановление БД |
|  | Аналитик бизнес-процессов | * Ведение реестра сервисных услуг государственного органа
* Формализация и управление процессами сервисных услуг;
* Мониторинг реализации сервисных услуг.
 |
|  | Агент первой линии поддержки | Специалисты технической поддержки, которые обрабатывают и мониторят заявки* Консультационые услуги;
* Внесение изменений в НСИ;
* Эскалация заявки в зависимости от типа заявки
 |
|  | Пользователь ЦРМ | * Вход в ИС ГО и работа в системе;
* Настройка уведомлений и напоминаний по приоритетности через личный кабинет;
* Ослеживать статистику своих действий;
* Просмотр НСИ, истории заявок, личных данных;
* Подача заявки через сервис управления услугами;
* Переписка посредсвом сервиса обмена сообщениями;
* Отправка файлов посредством сервиса обмена сообщениями;
* Возможность просмотра информации о пользователе в модуле Журнал входа/выхода в ЦРМ
 |
|  | Руководитель СТП ГО | * Все права Пользователя ЦРМ;
* Возможность просмотра информации о сотрудниках СТП в модуле Журнал входа/выхода в ЦРМ.
 |

Пользователями СПП будут являться сотрудники государственных органов. Администраторами ЦРМ будут являться сотрудники, обеспечивающие бесперебойное функционирование СПП, выполнение настроек, техническую, консультационную и методическую поддержку пользователей.

При необходимости должна быть предоставлена возможность установить Пользователю одновременно несколько ролей. При этом Пользователь будет иметь доступ к функционалу, предусмотренному для данных ролей, и возможность выполнять одновременно функции различных ролей Пользователей.

Права доступа к документам должны назначаться либо для конкретного Пользователя, либо для группы Пользователей.

#  Класс электронного информационного ресурса и прикладного программного обеспечения

Классификация объектов информатизации производится согласно [7]

Результаты классификации объектов информатизации используются для:

1. мониторинга и анализа состояния информатизации;
2. определения требований, применяемых к определенному классу объектов информатизации в соответствии с [4] и обеспечения информационной безопасности, утверждаемыми в соответствии с подпунктом 3) статьи 6 [3]

Класс ЭИР – **третий,** класс ППО – **третий.** Классификации объектов информатизации приведены в таблицах 4, 5

ППО третьего класса характеризуется как: малоприоритетное прикладное программное обеспечение – ведомственные типовые информационные системы, интернет-ресурсы и пользовательские программные продукты, выход из строя которых окажет минимальное влияние на деятельность одного государственного органа или его отдельных структурных подразделений.

Таблица 4. Классификация электронного информационного ресурса.

Уровень классификационных характеристик ППО приведен в таблице 5

Таблица 5. Классификация прикладного программного обеспечения.



1. 1.
	2.
	3.
	4.
	5.
	6.
	7.

## Механизмы и этапы создания СПП

Таблица 6. Механизмы и этапы создания СПП

| **Стадия** | **Этапы создания** | **Форма завершения** | **Ответственный** | **Сроки реализации** |
| --- | --- | --- | --- | --- |
| Публикацияобъявления оначале приемазаявок на участие вразработке СПП |  | Объявление насайте Сервисногоинтегратора | Сервисный интегратор  | В течение 3 (трех) рабочих дней после получения запроса от Заказчика ИК-услуги по утверждению бюджета |
|  | Получение заявок от потенциальных поставщиков | Заявки от потенциальных поставщиков | Потенциальные поставщики, Сервисный интегратор | В течение 15 (пятнадцать) рабочих дней со дня опубликования объявления о начале приема заявок |
|  | Извещение членов Конкурсной Комиссии и подавших заявку на участие в конкурсе потенциальных поставщиков о месте, дате и времени проведения рассмотрения заявок на участие в конкурсе и квалификационного отбора | Официальное письмо | Сервисный интегратор | Не более 3 (трех) рабочих дней со дня истечения срока приема заявок на участие в конкурсе приема заявок |
| Конкурс по определению поставщика | Квалификационный отбор | Документы, представляемые потенциальными поставщиками вподтверждение их соответствия квалификационным требованиям | Потенциальный поставщик |  |
| Протокол допуска потенциальных поставщиков к конкурсному отбору | Комиссия | Не более 3 (трех) рабочих дней |
| Конкурсный отбор | Оценка прототипа СПП | Комиссия | В соответствии с Протоколом допуска |
| Протокол об определении поставщика | Комиссия | Не более 3 (трех) рабочих дней |
| Разработка СПП | Демонстрация СПП | Официальное письмо Поставщика о готовности к демонстрации СПП | Поставщик | От 15 (пятнадцати) до 60 (шестьдесят) календарных дней с момента подписания Протокола допуска |
| Протокол встречи | Сервисный интегратор | Не более 3 (трех) рабочих дней |
| Тестирование СПП | Проверка комплектности ТД, в соответствии с п. 5.2 настоящего документа | Официальное письмо | Сервисный интегратор, Оператор | 5 (пять) рабочих дней со дня получения уведомления поставщика о готовности к тестированию |
| Проверка содержания и оформления ТД | ТД, согласованная Оператором | Оператор, Поставщик | В течение 15 (пятнадцать) рабочих дней после подтверждения комплектности |
| Разработка Плана тестирования | План тестирования | Сервисный интегратор | В сроки согласно протоколу Комиссии |
| Предоставление ИКИ для тестирования СПП | Информация о требуемых ресурсах ИКИ для функционирования СПП в среде эксплуатации | Оператор | Не более 5 (пяти) рабочих дней после запроса Сервисного интегратора |
| Тестирование СПП на работоспособность | Протокол тестирования на работоспособность СПП | Протокол тестирования на работоспособность СПП | В соответствии с Планом тестирования |
| Опытная эксплуатация СПП | Требования пункта 85 ППРК ЕТ | 1. Акт о вводе в опытную эксплуатацию;2. Акт о завершении опытной эксплуатации | ПоставщикОператорКомиссия | В сроки согласно протоколу Комиссии |
| Испытания СПП на соответствие требованиям ИБ | 1. Анализ исходных кодов2. Нагрузочное испытание3. Испытание функций ИБ | 3. Протоколыиспытаний с положительнымирезультатами4. Акт испытаний СППна соответствиетребованиям ИБ сположительнымзаключением | ПоставщикАО «ГТС»КИБ МЦРИАП РК | В соответствии сДоговором поиспытаниям наИБ,УведомлениеПоставщиком опрохождениииспытаний насоответствиетребованиям ИБ |
| Формирование ИК - услуги | Заседание конкурсной комиссии по формированию ИК-услуги | Письмо по заседанию Комиссии | Сервисный интегратор | В течение 5 (пяти) рабочих дней со дня получения уведомления от поставщика или оператора |
| Протокольное решение Комиссии по вводу СПП в опытную эксплуатацию | Комиссия | В течение 3 (трех) рабочих дней |
| Ввод в промышленную эксплуатацию СПП | 1. Обучение2. МатериалыОбучения пользователей,предусмотренные вразделе 5.6 настоящего документа3.Протокол обучения | Поставщик | В соответствии с Протоколом Комиссии |
| 4. Акт ввода СПП в промышленную эксплуатацию | ОператорМЦРИАП РККИБ МЦРИАП РК | В течение 5 (пяти) рабочих дней |
| 5.СПП и техническая документация СПП» 6. «Акт приема-передачи СПП и технической документации СПП» | Поставщик | В соответствии с Протоколом Комиссии |
| Инициация включения СПП в каталог ИК-услуг | Запрос в Уполномоченный орган по включению СПП в каталог ИК - услуг | Сервисный интегратор | Не позднее 5 (пяти) рабочих дней со дня подписания протокола ввода в эксплуатацию СПП или объекта и ИК-услуги по уведомлению оператора |
| Оказание ИК-услуги | Заключение договора СМИ с Заказчиком ИК-услуги | Договор СМИ между Оператором и Заказчиком ИК-услуги | ОператорЗаказчик ИК-услуги |  |
| Заключение договора об аренде СПП с Поставщиком | Договор об аренде СПП между Оператором и Поставщиком | ОператорПоставщик | Не позднее 5 (пяти) рабочих дней со дня заключения договора СМИ с заказчиком ИК-услуги |
| Техническая поддержка СПП |  | 1.Актуализированная техническая документация, предусмотренная в разделе 5.2 настоящего документа, по мере обновления СПП (при необходимости) 2.Актуализированные справочники СПП по запросу Заказчика ИК-услуги (при необходимости) 3.Проведение постоянных (по мере необходимости) консультаций пользователей СПП, обучающих семинаров и тренингов среди пользователей СПП | Поставщик | В течение срока действия Договора об аренде СПП между Оператором и Поставщиком |

# Предельная стоимость аренды СПП

Расчет стоимости аренды СПП производится согласно [12].

Стоимость проведения испытаний на соответствие требованиям информационной безопасности рассчитывается в соответствии с [10] на основе данных Анкеты-вопросника (Приложение к [10]).

**Таблица 7. Предельная стоимость аренды СПП (в тенге, с учетом НДС):**

|  |  |  |
| --- | --- | --- |
| **Аренда СПП** | **Единица измерения** | **Стоимость за 1 ед. изм., тенге** |
| Разработка СПП | 1 год | *В работе* |
| Ежегодное сопровождение кодов СПП | 1 год | *В работе* |

Предельная стоимость аренды СПП приведена в таблице 8.

**Таблица 8. Предельная стоимость аренды СПП, с учетом стоимости разработки СПП и сопровождения кодов СПП (в тенге, с учетом НДС):**

|  |  |  |
| --- | --- | --- |
| **Первый год аренды СПП** | **Второй год аренды СПП** | **Третий год аренды СПП** |
| *В работе* | *В работе* | *В работе* |

# Предельная стоимость ИК-услуги

Годовая стоимость ИК–услуги как инфраструктуры, приведенная к затратам по обеспечению функционирования конкретного объекта ИКИ, рассчитываемая согласно п. 14 [12].

Стоимость ИК-услуги рассчитывается c учетом затрат на услуги аренды ИК-Услуги, услуги аренды ИК-инфраструктуры, с учетом сопровождения ИК-услуги, а также другие услуги, оказанные Оператором, в соответствии с настоящим заданием на проектирование.

**Таблица 9. Предельная стоимость ИК-услуги в тенге, с учетом НДС**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Стоимость ИК-услуги за первый год** | **Стоимость ИК-услуги за первый год** | **Стоимость ИК-услуги за первый год** |
| **Поставщику:** | *В работе* | *В работе* | *В работе* |
| **Оператору:** | *В работе* | *В работе* | *В работе* |
| **ИТОГО:** | *В работе* | *В работе* | *В работе* |

*Примечания:*

*\* В случае увеличения объема работ, увеличения вычислительных ресурсов, использование лицензионных программных обеспечениях стоимость услуг Оператора подлежат перерасчету после ввода СПП в промышленную эксплуатацию по согласованию с Заказчиком.*

# Функциональные требования к СПП

1.
2.

# Общее описание функционала СПП

 СПП планируется реализовать на базе технологий, которые позволяет интегрировать все используемые информационные системы, ресурсы в одно окно, используя SSO-технологии, позволяющие не прибегать к повторной аутентификации пользователя при его переходе по различным ИС. Такая схема обеспечивает упрощенное централизованное управление правами доступа, избавляя от необходимости многократного ввода логинов и паролей, и от множества окон на рабочем столе.

В СПП в отличие от стандартных методов аутентификации при попытках пользователя получить доступ к сервису, запрос пользователя на авторизацию направляется в SSO-приложение и в Единый справочник СПП, и прежде чем получить доступ к СПП, система запрашивает информацию о пользователе, чтобы удостовериться, что у пользователя есть доступ к данному ресурсу.

На главном экране должна отображаются все используемые ИС согласно перечню используемых ИС (Таблица 29). При нажатии на иконку ИС, пользователь должен переходить в выбранную систему, с возможностью переключения между несколькими системами без повторной аутентификации. При переходе в ИС посредством SSO, ИС должна открываться в интерфейсе СПП. Если у пользователя нет доступа к определенной ИС, то СПП оповещает об отсутствии доступа к выбранному ресурсу. Также должна быть возможность настройки интерфейса пользователем и компонентов интерфейса: скрытие, отображение.

В СПП должна быть предусмотрена возможность добавления новых информационных систем и сервисов с помощью API.

Также СПП предполагает взаимодействие с УРМ, который позволял бы госслужащим осуществлять безопасное подключение к ЦРМ в случае подключения пользователя удаленно. Реализовать защиту удаленного рабочего места госслужащего следует на стороне УРМ, согласно утвержденной схеме КИБ МЦРИАП РК.

Рисунок 1. Общая схема СПП.



Также в СПП должна быть возможность размещения гиперссылок на информационные ресурсы ГО (adilet.zan.kz, egov.kz и т.д.)

В состав ЦРМ должны входить следующие компоненты и сервисы:

1. Личный кабинет пользователя
2. Сервис входа пользователей через SSO в другие ИС
3. Единый справочник ГО
4. База знаний
5. Анкетирование
6. Облачный офис
7. Система уведомлений и напоминаний
8. Живая лента
9. Аналитика
10. Сервис обмена сообщениями (чат)
11. Журнал входа/выхода в СПП
12. API SSO
13. Управление календарем
14. Дашборд
15. Сервис поддержки клиентского места
16. Модуль администрирования интерфейса пользователем

В СПП должны быть реализованы бизнес-сервисы, указанные в таблице 10.

Таблица 10. Описание бизнес-сервисов

|  |  |  |
| --- | --- | --- |
| **№** | **Наименование****Бизнес-сервиса** | **Назначение** |
|  | Личный кабинет | Сервис предназначен для персональных настроек пользователя СПП. У пользователя должна быть возможность редактировать контактные данные (телефон, кабинет), загрузки фото. Также в личном кабинете должен быть конструктор для изменения интерфейса и настройки модулей (добавление, удаление, упорядочивание). |
|  | Сервис входа пользователей через SSO в другие ИС  | Интеграция всех используемых информационных систем в одно окно, используя SSO, позволяющее не прибегать к повторной аутентификации пользователя при его переходе по различным ИС.При использовании SSO – СПП отправляет запрос в Active Directory/справочник ИС ГО для входа в ИС.  После получения ответа на запрос от ИС ГО предоставляется доступ в ИС ГО в СПП. |
|  | Единый справочник | - отображение у пользователя Справочника государственного органа, где имеется информация о сотрудниках ГО (название организации, должность, ФИО, контактные данные) по иерархии.- актуализация информации о пользователях.Единый справочник будет актуализироваться посредством ИС «Е-қызмет» или других ИС, где имеются актуальные данные пользователей ГО с возможностью группировки пользователей к определенной структуре ГО (департамент, комитет, управление и т.д.). У пользователя должна быть возможность смотреть справочник всех ГО с возможностью сортировки по ГО, В модуле «Единый справочник» реализуется актуализация следующей информации:- данные пользователей (ФИО, организация, должность, контактные данные и т.д.);- статус пользователя (в отпуске, больничный и т.д.). |
|  | База знаний | В данном модуле администратор ЦРМ загружает инструкции по работе ИС ГО для государственных служащих и другие общие документы. У пользователей доступ будет только на чтение. |
|  | Анкетирование | Модуль «Анкетирование» для проведения анкетирования среди сотрудников государственного органа. В данном модуле каждый пользователь с необходимыми ролями, может запустить опрос других пользователей в системе. |
|  | Облачный офис | Модуль предназначен для согласования документов, а также для совместной работы над документами (редактирование) между сотрудниками, руководством государственных органов.  |
|  | Сервис уведомлений и напоминаний  | Сервис предполагает оповещение пользователя о новых сообщениях/письмах/обращениях от ИС.Также сервис предполагает всплывающие уведомления (подсказки) по компонентам системы. |
|  | Живая лента | У пользователей должна быть возможность публикации объявлений, а также оснащающаяся на данных из ИС контрагента. |
|  | Аналитика | Статистический отчет по поступившим документам, формированию различных отчетов. Формы отчетов будут предоставлены после допуска Поставщика к разработке СПП. |
|  | Сервис обмена сообщениями (чат) | Для обмена мгновенными сообщениями между сотрудниками ГО. В сервисе должен быть реализован поиск контакта из Справочника ГО, направление и получение сообщений, направление и получение графического смайла, направление и получение файлов, возможность создания и удаления групп, отображение индикаторов статуса пользователя (в сети, отключен, не беспокоить). В сервисе должно быть реализовано хранение истории сообщений. Также поступление нового сообщения должно сопровождаться звуковым оповещением. |
|  | Журнал входа/выхода в СПП | Предполагается фиксирование времени начала и окончания работы Пользователя в СПП. При неактивной сессии СПП учет времени приостанавливается и при повторном входе в СПП сессия возобновляется. У Пользователя будет доступ на просмотр информации о времени входа/выхода в СПП. У руководителя СТП будет доступ на просмотр информации о времени входа/выхода в СПП сотрудников СТП. |
|  | API «SSO» | - единые требования интеграции со стороны СПП;- универсальный сервис для взаимодействия с другими ИС.Сервис предполагает добавление новых ИС в части единого входа. |
|  | Управление календарем | В данном модуле должно быть реализовано добавление событий (встреча, задача, совещание). Данное событие должно отображаться в календаре по времени и дате, указанным при создании события, а также оповещать о предстоящем событии.  |
|  | Дашборд | Сервис предполагает наличие аналитической панели на главной странице с отображением предстоящих событий, исполненных/неисполненных/просроченных документов, поступивших писем, уведомлений в компактном виде. |
|  | Сервис поддержки клиентского места | Используется для взаимодействия с пользователями СПП. Задача поддержки клиентского места — принимать обращения пользователей, у которых возникают проблемы, фиксировать их и решать.Для решения проблемы пользователя у администраторов ГО будет возможность оперативного ответа на вопрос, в случае если касается проблем ИС, то требуется передать заявку профильному специалисту. Все заявки должны фиксироваться.У аналитика бизнес-процессов системы должна быть возможность производить изменение маршрутов запроса, в том числе добавление/удаление сервисов по типу запроса. У пользователя должна быть возможность подачи заявки по работе СПП, ИС, по административно-хозяйственным вопросам (заявки на настройку рабочих мест, установку телефонии, канцелярские товары и так далее).Консультирование пользователей посредством различных инструментов коммуникаций |
|  | Сервис администрирования интерфейса пользователем | У пользователя должна быть возможность настраивать интерфейс СПП и компонентов интерфейса: скрытие, отображение, упорядочение. Также должен быть сервис интерактивных подсказок. |

# Детальное описание процессов и сценарии использования

В Таблице 11 приведены варианты использования, реализуемые в ЦРМ.

Таблица 11 – Перечень вариантов использования

| **Код ВИ** | **Название варианта использования** |
| --- | --- |
| UC.01 | Личный кабинет |
| UC.02 | Единый вход в ИС посредством SSO |
| UC.03 | Единый справочник |
| UC.04 | База знаний |
| UC.05 | Анкетирование |
| UC.06 | Облачный офис |
| UC.07 | Сервис уведомлений и напоминаний |
| UC.08 | Живая лента |
| UC.09 | Аналитика |
| UC.010 | Сервис обмена сообщениями (чат) |
| UC.011 | Журнал входа/выхода в ЦРМ |
| UC.012 | API «SSO» |
| UC.013 | Управление календарем |
| UC.014 | Дашборд |
| UC.015 | Сервис поддержки клиентского места |
| UC.016 | Сервис администрирования интерфейса пользователем |

* + 1. **Личный кабинет**

Сценарий использования UC.01 описан в таблице.

Таблица 12. Личный кабинет

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Все роли |
| **Предусловия** | Пользователь зарегистрирован в СПП при условии принятия обязательства о конфиденциальности и авторизован |
| **Постусловия** | Пользователь осуществил вход в СПП |
| **Основной сценарий авторизации в Системе**  | 1. При первичной авторизации в СПП пользователь должен авторизоваться посредством ЭЦП и логин-пароля.
2. После этого должно появится окно с соглашением о конфиденциальности.
3. После принятия условий соглашения о конфиденциальности, пользователь получает доступ к функционалу системы согласно настроенных прав доступа.
4. В последующих авторизациях Пользователь авторизуется посредством многофакторной аутентификации.
5. Пользователь выбирает сервис Личный кабинет на главной странице ЦРМ.
6. В Личном кабинете у пользователя должна быть возможность загрузить фото, редактировать контактные данные.
7. В Личном кабинете должен быть конструктор для изменения интерфейса ЦРМ и настройки модулей (добавление, удаление, упорядочивание).
 |
| **Альтернативный** **сценарий 1** | *Сведения по учетной записи не найдены в Едином справочнике ЦРМ:*1. Модуль отображает пользователю сообщение, что не найдены данные по учетной записи.
 |
| **Альтернативный** **сценарий 2** | *Пользователь неправильно указал логин и/или пароль** + - 1. Система выводит информацию об ошибке;
			2. Пользователь выбирает функцию восстановления пароля:

- система отображает окно восстановления пароля;- Пользователь указывает ИИН/логин и адрес электронной почты (указанную при регистрации);- Система направляет новый пароль на указанный электронный адрес. |
| **Альтернативный** **сценарий 3** | *Пользователь неправильно указал логин и/или пароль 3 раза подряд*1. Система выводит информацию о блокировке учетной записи и необходимости обращения к администратору ЦРМ;
2. Администратор ЦРМ после проверки учетных данных отправляет новый пароль на указанный электронный адрес.
 |

* + 1. **Единый вход в ИС посредством SSO**

Сценарий использования UC.02 описан в таблице.

Таблица 13. Единый вход в ИС посредством SSO

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Все роли  |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | Пользователь осуществил вход в информационные системы |
| **Основной сценарий**  | 1. После аутентификации на главной странице СПП отображаются информативные блоки (Живая лента, дашборд, доступные ИС, аналитика и другие компоненты), пользователь выбирает определенную из перечня.
2. С помощью Сервиса входа пользователей через SSO определяются доступы Пользователя в доступные ИС.
3. В случае отсутствия доступа к ИС, система выводит уведомление *«Отсутствует доступ к данной ИС»*
4. Как только Сервис входа пользователей через SSO одобрит доступы пользователя, он подтверждает успешную аутентификацию в ИС.
5. Пользователю предоставляется доступ к ИС.
 |

* + 1. **Единый справочник**

Сценарий варианта использованияUC.03 описан в таблице

Таблица 14. Единый справочник

| **Акторы/Действующие лица** | Все пользователи СПП |
| --- | --- |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | Записи в Справочнике актуализированы |
| **Основной сценарий**  | *Актуализация информации в Едином справочнике*1. Пользователь СПП заходит на главную страницу СПП
2. Справочик будет создаваться и актулизироваться по согласованию кадровика ГО.
3. Единый справочник будет обновляться автоматически с других ИС, где имеется актуальная информация о пользователях.
4. Администратор ЦРМ имеет доступ к редактированию информации о пользователях, созданию новых пользователей и удалению.
5. Администратор ЦРМ в Едином справочнике настраивает доступы к ИС и ресурсам ЦРМ.
6. Все действия по актуализации информации сохраняются в профиле пользователя.
 |
| **Альтернативный сценарий** | *Отображение информации в Справочнике ГО** + - 1. Пользователь открывает модуль «Справочник ГО»
			2. У пользователя будет возможность на просмотр Справочника государственного органа, где имеется информация о сотрудниках ГО (название организации, должность, ФИО, контактные данные) по иерархии.
 |

* + 1. **База знаний**

Сценарий варианта использования UC.04 описан в таблице.

Таблица 15. База знаний

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Администратор ЦРМ |
| **Предусловия** | Администратор авторизован в ЦРМ |
| **Постусловия** | Отображаются инструкции по ИС  |
| **Основной сценарий** | В данном модуле администратор ЦРМ загружает инструкции по работе ИС ГО и других общих документов для государственных служащих.  |

* + 1. **Анкетирование**

Сценарий варианта использования UC.05 описан в таблице.

Таблица 16. Анкетирование

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Все роли |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | Пользователь прошел анкетирование |
| **Основной сценарий** | В модуле «Анкетирование» должны быть 2 роли:- администратор (пользователь, который должен иметь возможность создавать анкетирование для всех ГО);- модератор (пользователь, который должен иметь возможность создавать анкетирование только для своего ГО).Редактировать и удалять анкеты может только автор, создавший анкету (вопросы с несколькими вариантами ответов).При опубликовании анкеты автор должен иметь возможность выбора одного или нескольких ГО, а также определить с какого по какое данная анкета будет активна.Сотрудник ГО, получивший анкету должен видеть период активности анкеты и в указанный срок ответить на данные вопросы. Анкета, по которой срок прошел, не должна быть доступна пользователю.Модуль должен предоставить пользователю возможность при желании не указывать свои персональные данные (ФИО и ГО), т.е. ответить «анонимно».Автор должен иметь возможность просмотреть результаты по проводимому анкетированию, также вывести результаты в текстовом виде (excel-формате). |

* + 1. **Облачный офис**

Сценарий варианта использования UC.06 описан в таблице.

Таблица 17. Облачный офис

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Все роли |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | Документ отредактирован и согласован |
| **Основной сценарий** | Модуль предназначен для согласования документа между сотрудниками государственных органов и предполагает совместную работу над документами с другими пользователями. Модуль включает в себя следующее:- одновременный многопользовательский доступ к редактируемому документу;- мгновенное отображение изменений;- комментарии к редактируемому документу;- просмотр и сравнение версий документа;- создание рабочей группы;- возможность добавления участников рабочей группы;- возможность добавления новой версии документа на повторное рассмотрение. |

* + 1. **Сервис уведомлений и напоминаний**

Сценарий вариантаиспользования UC.07 описан в таблице.

Таблица 18. Сервис уведомлений и напоминаний

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Все роли  |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | Отображаются поступившие сообщения |
| **Основной сценарий**  | 1. На главной странице СПП пользователю доступна вкладка уведомления.
2. Во вкладке уведомления отображаются поступившие запросы/письма/обращения/сообщения с других ИС.
3. С других ИС поступает информация о количестве новых непрочитанных письмах/сообщениях
4. ЦРМ отображает информацию о количестве уведомлений:

- всего уведомлений;- не прочитано (количество).1. ЦРМ предоставляет возможность отметить уведомление как прочитанное.
2. ЦРМ должен отображать уведомления только для:
* приглашенных участников событий (назначение/изменение/отмена событий, задач в календаре),
* пользователей о поступлении новых писем, если пользователь является адресатом и/или находится в списке адресатов (почта ЦРМ),
* пользователей об изменении статусов для событий модулей в которых пользователь является исполнителем, согласующим, подписантом (ИС),
* для пользователей об изменении статусов событий автором которых является пользователь (календарь)
1. ЦРМ должен предоставлять возможность просмотра поступивших уведомлений в модальном окне.
2. Уведомления должны отображаться по дате и времени поступления уведомления (от новых к старым).
3. Все прочитанные уведомления должны отображаться внизу списка после непрочитанных с соблюдением условия (от новых к старым).
4. В модальном окне должна быть предоставлена возможность поиска уведомления по словам или полному наименованию, содержащемуся в уведомлении.
5. В модальном окне пользователю должна быть возможность фильтрации уведомлений по:
* наименованию модуля (выбор из выпадающего списка),
* дате поступления уведомления (поступление в определенную дату, поступление в промежутке от и до).
 |

* + 1. **Живая лента**

Сценарий вариантаиспользования UC.08 описан в таблице.

Таблица 19. Живая лента

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Все роли  |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | Отображается публикация пользователя/ИС  |
| **Основной сценарий**  | 1. На главной странице СПП пользователю доступно информационное табло живая лента.
2. СПП отображает сведения из других ИС, к примеру, назначения на должность вице министра в ГО.
3. У пользователя должна быть возможность публикации новостей/объявлений/запросов. Также у автора публикации должна быть возможность редактирования и удаления публикации.
4. У пользователей СПП должна быть возможность комментировать публикации.
 |

* + 1. **Аналитика**

Сценарий вариантаиспользования UC.09 описан в таблице.

Таблица 20. Аналитика

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | ЦРМ  |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | Отображаются аналитические данные |
| **Основной сценарий**  | 1. На главной странице ЦРМ пользователю доступны аналитические данные по:

- количеству исполненных документов;- среднее время исполнения документов;- просроченным документам;- документам, на особом контроле;- поступившие документы/сообщения;- срочные поручения;- финансовая аналитика по принятым договоровным обязательствам;- исполнение стратегических и операционных планов;- статистика по НПА (сколько рассмотрено, на исполнении, просрочено).1. В СПП аналитические данные, отображаются на основании информации с других ИС.
 |

* + 1. **Сервис обмена сообщениями (чат)**

Сценарий вариантаиспользования UC.10 описан в таблице.

Таблица 21. Сервис обмена сообщениями (чат)

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Все роли  |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | Отправка и получение сообщений |
| **Основной сценарий**  | 1. На главной странице СПП пользователю доступна функция обмена мгновенным сообщениями между пользователями.
2. Также имеется возможность поиска контакта из Справочника ГО, направление и получение сообщений, направление и получение графического смайла, направление и получение файлов объемом не более 100 Мб, возможность создания и удаления групп, отображение индикаторов статуса пользователя (в сети, отключен, не беспокоить). В сервисе должно быть реализовано хранение истории сообщений. Также поступление нового сообщения должно сопровождаться звуковым оповещением.
 |

* + 1. **Журнал входа/выхода в ЦРМ**

Сценарий вариантаиспользования UC.11 описан в таблице.

Таблица 22. Журнал входа/выхода в ЦРМ

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Все роли  |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | Информация о времени входа/выхода пользователя в СПП |
| **Основной сценарий**  | 1. На главной странице СПП пользователю доступна функция регистрации входа/выхода в СПП.

Предполагается фиксирование времени начала и окончания работы Пользователя в СПП. При неактивной сессии СПП учет времени приостанавливается и при повторном входе в СПП сессия возобновляется автоматически. 1. У Пользователя будет доступ на просмотр информации о времени входа/выхода в СПП. У руководителя СТП будет доступ на просмотр информации о входе/выходе в ЦРМ сотрудников СТП, в том числе Журнал событий по пользователям.

3. У руководителя СТП будет возможность сформировать Отчетность по сотрудникам. В случае временного отсутствия руководителя (больничный, отпуск, командировка), данная функция делегируется на замещающего сотрудника. |

* + 1. **API «SSO»**

Сценарий варианта использования UC.13 описан в таблице.

Таблица 23. «API»

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Администратор ЦРМ |
| **Предусловия** | Администратор зарегистрирован и авторизован в СПП |
| **Постусловия** | Данные сохранены в ИС контрагента |
| **Основной сценарий**  | С помощью API должна быть возможность добавления новых компонентов и сервисов в СПП |

* + 1. **Управление календарем**

Сценарий варианта использования UC.15 описан в таблице.

Таблица 24. Управление календарем

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Все пользователи СПП |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | Событие запланировано в календаре СПП |
| **Основной сценарий**  | На главной странице СПП пользователю доступен сервис календарь. В данном сервисе должно быть реализовано добавление событий (встреча, задача, совещание) с возможностью добавления/удаления участников события, темы и места проведения. Данное событие должно отображаться в календаре по времени и дате, указанным при создании события, а также оповещать о предстоящем событии.При просмотре модуля «Календарь» Система должна предоставлять возможность пользователю сортировки событий в календаре (по дате; автору; по важности события).При создании события СПП должен автоматически подбирать время проведения события у участников. В случае если на определенное время у одного из участников запланировано другое событие, СПП планирует событие на ближайшее свободное время. Также у Пользователя должна быть возможность ручного ввода даты и времени в поле «Дата и время проведения события». В случае уже запланированного события на это время у одного из участников, СПП предлагает данному участнику принять, либо делегировать участие в событии другому сотруднику, если оно пересекается с другим событием. СПП направляет уведомление пользователю, создавшему событие, о принятии или отклонении/делегировании события приглашенным гостем. При создании события в календаре должна быть возможность добавления описания события, комментария к нему. Также при создании нового события должна указываться степень важности планируемого события.При создании события СПП должен предоставлять возможность выбора списка приглашенных гостей события. Для выбора гостей события у Пользователя должна быть возможность выбора ГО для фильтрации сотрудников. Если не выбрано государственное учреждение, Система должна предоставлять возможность выбора приглашенных гостей из всех пользователей системы.При добавлении гостей события должны отображаться статусы участников, т.е. если один из участников в запланированное время находится в отпуске, то при выборе данного участника должно выходить уведомление о его статусе и информация о замещении.Данные статусы должны автоматически подтягиваться из модуля «Единый справочник ГО».Система должна предоставлять возможность выбора формата проведения встречи (Online/Offline). Если выбран формат Online СПП должен дополнительно отобразить поле «Ссылка» для дополнительного добавления ссылки на проведение события Online.Система должна уведомлять приглашенных гостей о событии. Для выбора уведомления приглашенных гостей пользователю доступны следующие варианты выбора периода уведомления:10 минут - уведомление за 10 минут до начала события,1 час - уведомление за 1 час до начала события,1 день - уведомление производится за 24 часа до начала события.Система направляет приглашение участникам события. Уведомление поступает на почту и в модуль «Уведомления». Система должна отправлять приглашение приглашенным гостям, указанным при создании события, даже если у приглашенного гостя занято время. У пользователя должна быть возможность выбора одного события в случае поступления нескольких приглашений.Также должна быть возможность предоставления доступов Пользователям на просмотр запланированных событий других сотрудников.На главной странице ЦРМ должны отображаться цветом ближайшие запланированные события Пользователя, также внизу Календаря должен отображаться список событий.  |

* + 1. **Сервис Дашборд**

Сценарий варианта использования UC.16 описан в таблице.

Таблица 25. Дашборд

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Все пользователи СПП |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | На главной странице СПП отображены события, письма, уведомления |
| **Основной сценарий для администратора** | На главной странице СПП должна быть аналитическая панель с отображением предстоящих событий, исполненных/неисполненных/просроченных документов, поступивших писем, уведомлений в компактном виде с цветным индикатором:Красный цвет – просроченные/до срока исполнения остается 1 день;Желтый цвет – до окончания срока исполнения осталось менее двух дней;Зеленый цвет – на исполнении. |

* + 1. **Сервис поддержки клиентского места**

Сценарий варианта использования UC.17 описан в таблице.

Таблица 26. Сервис поддержки клиентского места

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Все пользователи СПП |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | Заявка на поддержку клиентского места сохранена в СПП и направлена ответственному исполнителю |
| **Основной сценарий для администратора** | Используется для взаимодействия с пользователями СПП. Задача поддержки клиентского места — принимать обращения пользователей, у которых возникают проблемы, фиксировать их и решать.Для решения проблемы пользователя у администраторов ГО будет возможность оперативного ответа на вопрос, в случае если касается проблем ИС, то требуется передать заявку профильному специалисту. Все заявки должны фиксироваться.У аналитика бизнес-процессов системы должна быть возможность производить изменение маршрутов запроса, в том числе добавление/удаление сервисов по типу запроса. |
| **Альтернативный сценарий пользователя** | На главной странице СПП пользователю доступна функция подачи заявки в поддержку клиентского места. При подаче заявки пользователь выбирает тип запроса (заявка по работе СПП, ИС, по административно-хозяйственным вопросам (заявки на настройку рабочих мест, установку телефонии, канцелярские товары и так далее)). Также у пользователя должна быть возможность отслеживания статуса подданной заявки, по завершению исполнения заявки пользователем проводится оценка работы по 5-ти бальной шкале.При ошибочно поданной заявке, либо при самостоятельном устранении возникшей проблемы пользователем может быть отменена заявка c указанием причины отмены. |

* + 1. **Сервис администрирования интерфейса пользователем**

Сценарий варианта использования UC.17 описан в таблице.

Таблица 27. Сервис администрирования интерфейса пользователем

|  |  |
| --- | --- |
| **Акторы/Действующие лица** | Все пользователи СПП |
| **Предусловия** | Пользователь зарегистрирован и авторизован в СПП |
| **Постусловия** | Изменения интерфейса пользователем сохранена в СПП |
| **Основной сценарий для администратора** | Пользователь настраивает интерфейс СПП и компонентов интерфейса: скрытие, отображение, упорядочение. Также пользователю доступны всплывающие уведомления интерактивных подсказок.  |

# Требования и ограничения, связанные с ИК платформой ЭП

# Общие требования

 При реализации сервисной модели информатизации информационные системы размещаются на информационно-коммуникационной платформе «электронного правительства», находящейся на территории Республики Казахстан.

 Поставщик при построении архитектуры и выбора технологических решений при разработке ЦРМ должен руководствоваться техническими и функциональными параметрами утвержденной архитектуры информационно-коммуникационной платформы «электронного правительства», а именно:

1. Обеспечение возможности независимого масштабирования каждого уровня (на уровне виртуального оборудования, программного, прикладного);
2. Обеспечение автоматической балансировки нагрузки серверов;
3. Обеспечение отказоустойчивости путем кластеризации либо резервирования (горячее или холодное) каждого из компонентов;
4. Поддержка виртуализации, а также развертывания как облачный сервис (тонкий клиент);
5. Обеспечение возможности централизованного резервного копирования;
6. Учитывать имеющиеся ограничения по вычислительным характеристикам виртуального сервера, размещающегося на площадке информационно-коммуникационной инфраструктуры;
7. Обеспечение сервером для хранения файлов резервного копирования и логов;
8. Рекомендуется использовать метод распределения пространства жесткого диска по логическим томам – LVM.

 При построении архитектуры СПП потенциальному поставщику необходимо учесть возможность возникновения следующих рисков:

* обеспечение информационной безопасности;
* обеспечение пропускной способности каналов связи;
* модификация СПП (оптимизация функциональных требований).

Концептуальная архитектура ЦРМ приведена на рисунке 4.



Рисунок 4. Концептуальная схема ИК-услуги.

# Технологические требования СПП

 При построении архитектуры СПП и выборе технологических решений должно учитываться:

* + - 1. Количество ядер на одну виртуальную машину не должно превышать 32 ядер;
			2. Объем оперативной памяти на одну виртуальную машину не должно превышать 48ГБ;
			3. Возможность использования контейнеризации и микросервисной архитектуры.

**Ограничения по используемым ОС, СУБД и ППО:**

1. **Операционные системы (ОС):**

• Linux (RedHat Enterprise Linux, платформа x86\_64, версии не ниже 7 и Ubuntu Server версии не ниже 18, Debian версии не ниже 7)

• Microsoft Windows Server, платформа x86\_64, версии не ниже 2019 (необходимо использовать лицензированное ПО в соответствии с требованием подпункта 4) пункта 78 [3])

1. ***Система управления базами данных (СУБД):***
* Microsoft SQL Server, платформа x86\_64, версии не ниже 2019;
* PostgreSQL, платформа x86\_64, версии не ниже 11;
* Oracle Database, платформа x86\_64, версии не ниже 19c;
* MySQL, платформа x86\_64, версии не ниже 8;
* MariaDB, платформа x86\_64, версии не ниже 10.3;
1. **Сервера приложений и web серверы:**

• Microsoft IIS как часть Microsoft Windows Server;

• Microsoft.NET Framework или ASP.NET;

• PHP-FPM версии не ниже 7;

• RedHat JBoss EAP версии не ниже 7;

• WildFly версии не ниже 13;

• Apache Tomcat версии не ниже 9

• Nginx версии не ниже 1.16.0;

• Apache HTTP Server версии не ниже 2.4

# Требования к среде тестирования:

Тестовая среда предоставляется Оператором согласно «Правилам предоставления
информационно - коммуникационной инфраструктуры для разработки и тестирования сервисных программных продуктов потенциальными поставщиками» разработанными на основании Правил и утверждёнными Председателем правления АО «НИТ» от 4 августа 2016 года.

В соответствии с пп. 3) п. 98 и пп. 8) п. 102 [4] должно быть обеспечено разделение сред опытной или промышленной эксплуатации от сред разработки, тестирования или стендовых испытаний, а также физическое разделение сред эксплуатации от сред разработки и тестирования [4].

# Хранение данных

ПО должно предоставлять возможность:

* Хранения лог-файлов;
* Хранение истории изменения данных;
* Хранение данных пользователей;
* Хранение аналитических данных учета рабочего времени;
* Хранение пересылаемых документов посредством сервиса обмена сообщениями
* новости и тд в согласно вышеуказанным замечаниям

# Требования ИК платформы ЭП к СПП

При разработке СПП применять средства из перечисленного ниже списка ограничений:

* на уровне виртуализации поддерживать гипервизоры VmWareESXi;
* поддержка функционала СПП на вычислительных мощностях на базе чипсетов архитектуры x86\_64;
* при создании/развитии СПП необходимо соблюдать допустимые размеры файлов и томов для файловых систем (не планировать использование RAW-устройств);
* на уровне ОС, ППО, СУБД обеспечивать полнофункциональную поддержку технологии виртуализации упомянутых в настоящем ЗНП;
* поддержка работы с мобильными устройствами (планшеты и смартфоны).

# Ограничения к вычислительным ресурсам

Вычислительные ресурсы ИКП ЭП в рамках создания СПП определены согласно требованиям к производительности, масштабируемости, отказоустойчивости и надежности.

Требования к техническим характеристикам технических средств объекта ИКИ представлены в таблице ниже.

Таблица 28. Требования к техническим средствам в рамках создания СПП.

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Сервер** | **Количество серверов** | **Технические характеристики** |
| **CPU (ядра)** | **RAM, Гб** | **HDD, Гб** |
| 1 | СУБД (основной) | 2 | 32 | 64 | 1000 |
| 2 | СУБД (резервный) | 2 | 32 | 64 | 1000 |
| 3 | Сервер приложений (основной) | 2 | 32 | 64 | 500 |
| 4 | Сервер приложений (резервный) | 2 | 32 | 64 | 500 |
| 5 | Сервер балансировки (основной) | 1 | 16 | 24 | 300 |
| 6 | Сервер балансировки (резервный) | 1 | 16 | 24 | 300 |
| 7 | Файл сервер (основной) | 1 | 16 | 24 | 3000 |
| 8 | Файл сервер (резервный) | 1 | 16 | 24 | 3000 |
| **Итого:** | **12** |  |  |  |

*Примечания:*

По истечению одного года эксплуатации ИК-услуги, допускается перераспределение объемов вычислительных ресурсов в рамках общего объема, определенной в строке 9 таблицы 28 настоящего ЗНП между серверами для их оптимального использования.

В случае недостаточности или увеличения требуемых ресурсов, а также в случае использования ОС, СУБД, ППО, для которых рекомендуется установка лицензированного программного обеспечения предельная стоимость ИК-услуги подлежит пересчету на основании заключения Сервисного интегратора, а также Оператор не несет ответственность за невозможность восстановления данных при отсутствии ресурсов.

# Требования к интеграции с объектами информатизации «электронного правительства» или другими информационными системами

Порядок интеграции СПП с объектами информатизации должен соответствовать [9].

Интеграционное взаимодействие должно соответствовать положениям п. 90-1 [4]: при реализации функций интеграционного взаимодействия объектов информатизации или компонентов объектов информации посредством шлюза, интеграционной шины, интеграционного компонента или интеграционного модуля обеспечиваются:

      1) регистрация и проверка источников (точек подключений) запросов на легитимность;

      2) проверка легитимности запросов по:

* паролю или ЭЦП;
* точке подключения;
* наличию блокировки соединения;
* разрешенным видам запросов, определенным в регламенте интеграционного взаимодействия;
* разрешенной частоте запросов, определенной в регламенте интеграционного взаимодействия;
* наличию в запросах признаков нарушений информационной безопасности;
* наличию вредоносного кода по сигнатурам;

      3) блокировка соединения при обнаружении нарушений в протоколах обмена сообщениями при:

* отсутствии соединения в течение времени, определенного в регламенте интеграционного взаимодействия;
* превышении разрешенной частоты запросов на время, определенное в регламенте интеграционного взаимодействия;
* наличии в запросах признаков нарушений информационной безопасности;
* превышении количества ошибок аутентификации, определенного в регламенте интеграционного взаимодействия;
* выявлении аномальной активности пользователей;
* выявлении попыток выгрузки массивов данных;

      4) регулярная смена паролей соединения по времени действия, определенного в регламенте интеграционного взаимодействия;

      5) замена логина соединения при выявлении инцидентов ИБ;

      6) сокрытие адресации ЛС внутреннего контура;

      7) журналирование событий, включающее:

* регистрацию событий передачи/приема информационных сообщений;
* регистрацию событий передачи/ получения файлов;
* регистрацию событий передачи/получения служебных сообщений;
* применение системы управления инцидентами и событиями ИБ для мониторинга журналов событий;
* автоматизацию процедур анализа журналов событий на наличие событий ИБ;
* хранение журналов событий на специализированном сервере логов, доступном для администраторов только для просмотра;
* раздельное ведение журналов событий (при необходимости) по:

      а) текущим суткам;

      б) соединению (каналу связи);

      в) государственному органу (юридическому лицу);

      г) интегрируемым объектам информатизации;

      8) предоставление сервиса синхронизации времени для интегрируемых объектов информатизации;

       9) программно-аппаратная криптографическая защита соединений, осуществляемых через сети передачи данных;

       10) хранение и передача паролей соединений в зашифрованном виде;

      11) автоматизация оповещения об инцидентах ИБ ответственных лиц интегрируемых объектов информатизации.

Также в соответствии с подпунктом 10 и 11 пункта 139 [4], для обеспечения ИБ, размещаются ИС субъектов информатизации, реализующие информационное взаимодействие через Интернет, в выделенном сегменте ЛС внешнего контура субъектов информатизации, и осуществляется взаимодействие с ИС субъектов информатизации, размещенными в ЛС внутреннего контура субъектов информатизации, через ВШЭП; осуществляется информационное взаимодействие ИС, размещенных в Интернете, с ИС субъектов информатизации, размещенными в ЛС внутреннего контура субъектов информатизации, только через ВШЭП.

В соответствии с подпунктами 7 и 8 пункта 139 [4], для обеспечения ИБ, исключается подключение ЛС внутреннего контура субъектов информатизации к Интернету;

      9) осуществляется соединение ЛС внешнего контура субъектов информатизации с Интернетом только через ЕШДИ. Подключение к Интернету иным способом не допускается, за исключением специальных и правоохранительных ГО в оперативных целях. Взаимодействие ВШЭП с Интернетом осуществляется через ЕШДИ.

Порядок интеграции ИС Субъекта, ШЭП, СПП должен соответствовать Приложению 6, к [9].

Назначение участников информационного взаимодействия:

1. Субъект – является поставщиком информации;
2. ШЭП и ВШЭП является универсальной транспортной средой обмена электронными сообщениями информационных систем «электронного правительства»;
3. СПП является получателем информации.

Информационный обмен между ИС Субъекта и СПП посредством ШЭП осуществляется посредством электронных сообщений в XML-формате с использованием ЭЦП.

В целях обеспечения безопасности взаимодействия между системами электронный документ должен содержать учетную запись\пароль и транспортную подпись Владельца ИС взаимодействующей системы, при этом, бизнес данные должны быть подписаны цифровым сертификатом владельца ИС, так как сообщения обрабатываются в этих системах без участия пользователей.

Электронные документы подразделяются на следующие два типа: «запрос» и «ответ». Инициализирующим информационный обмен электронным документом является сообщение типа «запрос». На электронный документ типа «запрос» получатель должен выслать отправителю электронный документ типа «ответ». Сообщение типа запрос должно передаваться из ИС Субъекта через ШЭП в ЦРМ, а ответ должен передаваться синхронно из ЦРМ через ШЭП в ИС Субъекта.

Обмен данными производится путем передачи SOAP-сообщений. В качестве транспорта доставки таких сообщений выступает протокол HTTP(S).

В процессе развития взаимодействия структура и формат данных могут изменяться по согласованию взаимодействующих сторон, в зависимости от изменения и дополнения получаемых сведений.

Порядок обработки запроса

1. ИС Субъекта формирует данные (запрос), подписывает системной ЭЦП ИС Субъекта, передает запрос в ШЭП и выполняет запись запроса в журнале событий
2. При отсутствии технических неполадок запрос ИС Субъекта поступает на ШЭП и проходит валидацию на предмет подлинности системной ЭЦП ИС Субъекта.
3. ШЭП выполняет проверку целостности сообщения, валидности ЭЦП ИС Субъекта и выполняет проверку заголовка сообщения, конверта сообщения на соответствие форматам данных в НУЦ РК. Проводит авторизацию инициатора взаимодействия, проверяет права на указанное взаимодействие. В случае не успешного результата проверки возвращает сообщение об ошибке. В случае успешной проверки, снимает ЭЦП передает запрос в ШЭП.
4. ШЭП принимает запрос, записывает в журнал событий факт получения/отправки сообщений, подписывает ЭЦП владельца, передает его в СПП.
5. СПП проверяет целостность сообщения, валидность ЭЦП, проводит авторизацию инициатора взаимодействия. В случае неуспешной проверки подписывает его ЭЦП и возвращает сообщение об ошибке. В случае успешной проверки формирует ответ о получении запроса, подписывает его ЭЦП и отправляет его в ШЭП.

 В СПП должна быть предусмотрена возможность добавления новых информационных систем через единый API.

Взаимодействие с ИC приведено в таблице 29.

После допуска потенциального Поставщика на разработку СПП будет составлен детальный план интеграции с ИС ГО, также будет предоставлен описание форматов взаимодействия.

Таблица 29. Взаимодействие с ИС.

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п:** | **Наименование системы\*** | **ГО владелец** | **Назначение взаимодействия** |
| 1 | ИС ГО  | УО | Авторизация в СПП посредством SSO (ОДО, ЭПС, Е-өтініш, Е-қызмет, Е-лицензирование и другие ИС).  |
| 2 | Облачный документооборот ГО | УО | Уведомления по передачи информации о поступивших письмах/обращениях в ОДО ГО;Информация о просроченных письмах, документах на исполнении и исполненных документах. |
| 3 | Электронный почтовый сервис | АО «НИТ» | Уведомления по передаче информации о поступивших сообщениях |
| 4 | Е-Otinish | НАО «Правительство для граждан» | Уведомления по передаче информации о поступивших обращениях;Информация о просроченных письмах, документах на исполнении и исполненных документах. |
| 5 | Е-қызмет | АДГС РК | - Идентификационные данные пользователей ГО;- Уведомления по передаче данных о временном отсутствии сотрудников, основанные на приказах. |
| 6 | Удостоверяющий центр ГО | МЦРИАП РК | Проверка ЭЦП и регистрационного свидетельства. |
| 7 | Е-лицензирование | УО | Уведомления по передаче информации о поступивших заявках. |

\**по мере необходимости будут добавлены другие ИС*

Каждый модуль интеграции должен представлять собой систему обмена XML-сообщениями, отвечающую за передачу и прием XML-сообщений между системами.

Реализация каждого модуля интеграции должна обеспечить:

- маршрутизацию XML-сообщений;

- журналирование процессов обмена XML-сообщениями в соответствии с [4].

- возможность взаимодействия приложений вне зависимости от аппаратных платформ и операционных сред;

- защищенный обмен данных путем сочетания следующих элементов: использование подписание ЭЦП ИС.

Обмен данными между системами должен соответствовать следующим форматам:

1) расширенный транспортный протокол HTTPS, с применением регистрационных свидетельств SSL, выданных НУЦ РК;

2) протокол взаимодействия SOAP (SimpleObjectAccessProtocol) в качестве протокола взаимодействия;

3) язык описания WSDL;

4) язык XSD для описания структур данных, подписываемых ЭЦП;

5) формат передаваемых данных XML для веб-методов и их параметров;

6) структура подписанного ЭЦП XML-файла должна соответствовать спецификации консорциума W3C «XML - Signature Syntax and Processing» (Синтаксис и обработка подписи XML).

7) в рамках взаимодействия по протоколу SOAP, использовать ЭЦП владельца объекта информатизации, выданной НУЦ РК, в соответствии со спецификацией WS-security.

* 1. **Требования к информационному взаимодействию с УЦ ГО РК**

Взаимодействие с УЦ ГО РК должно выполняться при проверке регистрационного свидетельства УЦ ГО РК (на отозванность), и при формировании метки времени. Инициатором информационного обмена при проверке регистрационного свидетельства УЦ ГО РК (на отозванность) является запрос от ЦРМ в УЦ ГО РК.

Порядок проверки подлинности регистрационного свидетельства УЦ ГО РК осуществляется в соответствии с [5].

* 1. **Требования к информационному взаимодействию с другими ИС**

Взаимодействие с ИС ГО в части получения информации, уведомлений должно проходить через ШЭП согласно ст. 43 [3]. Взаимодействие с ИС, находящимися вне ЕТС ГО, должно проходить через ВШЭП. Взаимодействие с внешними пользователями в Интернете должно проходить через единый шлюз доступа к Интернету, согласно [4].

# Требования к надежности, отказоустойчивости, производительности и масштабируемости

# Требования к отказоустойчивости и бесперебойности

При выборе архитектурного решения по обеспечению отказоустойчивости должно обеспечиваться:

* равномерное распределение запросов между программно-прикладными обеспечениями СПП;
* доступность СПП при сбоях одного из узлов базы данных.

СПП должен сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

* при отказе или выходе из строя по любым причинам одного из компонентов СПП;
* при отказе одного из компонентов не зависимо от его назначения, с последующим восстановлением работоспособности СПП после завершения всех необходимых ремонтных и восстановительных работ;
* СПП должен поддерживать автоматическое переключение на резервный сервер СПП в случае выхода из строя основного сервера.

# Требования к производительности и масштабируемости

Поставщиком должно быть обеспечено горизонтальное масштабирование серверных компонентов СПП по мощности, путем наращивания комплекса дополнительными виртуальными серверами и распределяя задачи между ними.

Для обеспечения надежности и отказоустойчивости должен быть реализован активный кластер, состоящий из дублируемых компонентов в точках отказа.

Используемая СУБД в СПП должна обеспечивать масштабируемость и резервное копирование данных.

Для планирования масштабируемости должны быть предусмотрены риски при каких условиях может быть увеличение ресурсов на СУБД и ППО.

При передаче ИК-услуга в эксплуатацию поставщик должен предоставить схему масштабируемости с учетом требуемой ИКИ, для увеличения ресурсов СУБД и ППО.

А также, обязательно должно быть предусмотрено:

* увеличение запросов учтенные в ЗНП;
* выход из строя компонентов ИК-услуга;
* увеличение записей в БД;
* увеличение объема журнала событий.

Для обеспечения производительности и масштабируемости ИК-услуга должно удовлетворять следующим показателям:

* среднее время обработки запроса в СПП - 3 сек;
* пиковая нагрузка - 50 000 транзакций в минуту;
* номинальная нагрузка - 25 000 транзакций в минуту.
* согласно пп 1) п) 49 [4] наличие резервного собственного или арендованного серверного помещения для объектов информатизации ЭП первого и второго классов в соответствии с классификатором;
* согласно пп 2) п) 49 [4] резервирование аппаратно-программных средств обработки данных, систем хранения данных, компонентов сетей хранения данных и каналов передачи данных, в том числе для объектов информатизации ЭП: второго класса в соответствии с классификатором – не нагруженное (холодное) в резервном серверном помещении;
* обеспечение безопасности хранения государственных электронных информационных ресурсов при оказании информационно-коммуникационных услуг, согласно пп.6 статьи 13 [3].

СПП должен функционировать при следующей пропускной способности канала связи (ЕТС ГО) от 512 кбит/сек до 4 Мбит/сек в зависимости от технических условий подключения ГО.

# Требования к надежности

Для обеспечения отказоустойчивости и надежности функционирования СПП Поставщик в рамках предоставления ИК-услуги должен обеспечивать время однократного простоя не более 30 минут, и обеспечения бесперебойной и отказоустойчивой работы 98,7% в режиме 365/7/24 без учета плановых работ и непредвиденных ситуаций, связанные с внешним воздействием (отсутствие электроэнергии, каналов связи и т.д.).

СПП должен поддерживать автоматическое переключение на резервный сервер СПП в случае выхода из строя основного.

При передаче СПП Поставщик и Заказчик предоставляют Оператору информацию о периодичности резервного копирования ОС, ППО, БД, о сроках хранения резервных копий и RPO (допустимый уровень потери данных).

Максимальное время восстановления (recovery time objective (RTO)) – 3 часа.

Обеспечение требований пп 3) п. 114 [3] в части обеспечения ИБ, надежного хранения и возможности восстановления данных посредством обеспечения записи и испытаний резервных копий в соответствии с регламентом резервного копирования, определенным в ТД ИБ.

Также должны быть учтены требования подпункта 2) пункта 114 [4] в части использования выделенного сервера для защищенного хранения ключей шифрования по уровню безопасности не ниже уровня безопасности, используемых СКЗИ.

Требования к информационной безопасности в соответствии с классом объекта информатизации и описание взаимодействия с системами мониторинга, контроля и журналирования событий.

# Требования к информационной безопасности

# Общие требования к информационной безопасности

Создание СПП осуществляется с учетом требований нормативных правовых актов и стандартов Республики Казахстан в сфере информатизации и обеспечения информационной безопасности Республики Казахстан:

* Закон «Об информатизации» от 24 ноября 2015 года № 418-VЗРК.
* Постановление Правительства Республики Казахстан «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» от 20 декабря 2016 года №832.
* СТ РК 2199-2012 «Информационные технологии. Требования к безопасности веб-приложений в государственных органах».
* СТ РК ГОСТ 50739-2006 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».
* СТ РК ISO/IEC 27001-2015 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
* СТ РК ISO/IEC 27002-2015 Государственный стандарт РК «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации».
* СТ РК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». (Части 1-3).
* Объекты информатизации ЭП в соответствии с классификатором объектов информатизации, утвержденным уполномоченным органом, подключаются к системе мониторинга обеспечения ИБ, защиты и безопасного функционирования.

Также необходимо выполнение следующих основных условий:

− объекты информатизации ЭП в соответствии с классификатором объектов информатизации, утвержденным уполномоченным органом, подключаются к системе мониторинга обеспечения ИБ, защиты и безопасного функционирования.

Оператор в рамках обеспечения безопасности функционирования СПП на ИКП ЭП обеспечивает реализацию норм подпункта 3) пункта 53 и подпункта 6) пункта 102 [4]:

1) События ИБ, идентифицированные как критические для конфиденциальности, доступности и целостности, по результатам анализа мониторинга событий ИБ и анализа журнала событий регистрируются в службе реагирования на компьютерные инциденты государственной технической службы.

2) Для обеспечения ИБ при использовании технологии виртуализации реализуются управление инцидентами ИБ, требующее:

* определения формального процесса обнаружения, выявления, оценки и порядка реагирования на инциденты ИБ с актуализацией раз в полугодие;
* составления отчетов с периодичностью, определенной в ТД ИБ, по результатам обнаружения, выявления, оценки и реагирования на инциденты ИБ;
* уведомления ответственных лиц ГО, МИО или организации об инцидентах ИБ;
* регистрации инцидентов ИБ в Службе реагирования на компьютерные инциденты Государственной технической службы.

**С целью обеспечения ИБ:**

* на этапе разработки СПП должны применяться рекомендации [15] в частности защищенность должна соответствовать трем группам требований к средствам защиты Оператора и потенциального поставщика:
* требования к разграничению доступа;
* требования к учету, предусматривающие то, что СПП должны поддерживать регистрацию событий, имеющих отношение к защищенности информации;
* требования к гарантиям, предусматривающие необходимость наличия в составе программных механизмов, позволяющих получить гарантии того, что ИК-услуга обеспечивает выполнение требований к разграничению доступа и к учету.

Должны быть учтены требования пункт 78 [4]:

 1) на этапе разработки ПО учитываются рекомендации [15];

2) требования к разрабатываемому или приобретаемому прикладному ПО предусматривают применение средств:

− идентификации и аутентификации пользователей, при необходимости ЭЦП и регистрационных свидетельств;

− управления доступом;

− контроля целостности;

− журналирования действий пользователей, влияющих на ИБ;

− защиты онлайновых транзакций;

− криптографической защиты информации с использованием СКЗИ конфиденциальных ИС при хранении, обработке;

− журналирования критичных событий ПО;

3) в ТД ИБ определяются и применяются при эксплуатации:

* правила установки, обновления и удаления ПО на серверах и рабочих станциях;
* процедуры управления изменениями и анализа прикладного ПО, в случае изменения системного ПО;

4) лицензируемое ПО используется и приобретается только при условии наличия лицензии.

2. Разрабатываемый СПП должен предусматривать:

* использование ЭЦП (пользовательской и системной) для подписания запросов внутри СПП, а также при взаимодействии с другими информационными системами;
* проверка ЭЦП и регистрационного свидетельства осуществляется в соответствии с [5];
* при формировании и проверке электронной цифровой подписи должны использоваться средства криптографической защиты информации;
* криптографическое шифрование служебной информации ограниченного распространения при хранении, обработке и передаче по сети в соответствии с требованиями п. 48 [4] с использованием в соответствии со стандартом [4];
* системное предупреждение об истечении срока действия ЭЦП за месяц до истечения.

2.1. Модуль идентификации и аутентификации пользователей:

* Процесс «Аутентификации» предназначен для проверки подлинности пользователя при входе в СПП. При внедрении процедур многофакторной аутентификации и авторизации для систем 2-класса, удовлетворяющие всем требованиям пункта 47 [4], необходимо применить два из пяти нижеперечисленных видов аутентификаций:
1. логин и пароль;
2. использование ЭЦП;
3. одноразовый пароль;
4. Digital-ID (биометрические данные);
5. QR – код.
* Модуль идентификации должен включать в себя алгоритм защиты от перебора паролей, с возможностью настройки количества неудачных попыток авторизации за определенный промежуток времени с последующей блокировкой пользователя.
	1. Модуль управления доступом должен включать в себя:

− идентификацию пользователя на основе проверки логина, пароля или ЭЦП пользователя;

− определение прав пользователей на ввод, корректировку, просмотр данных.

* 1. Модуль журналирования событий ИК-услуга (критичных событий, событий действий пользователей и т.д.).
		1. Журналирование всех событий должен соответствовать следующим требованием:
1. журналирование должно вестись в соответствии с требованиями стандарта [17].
2. СПП должен обеспечивать возможность взаимодействия с системами SIEM по протоколу и в формате syslog (RFC 5424).
3. Внешние интерфейсы взаимодействия ИС/ИК-услуга должны быть реализованы посредством технологии WebServices с использованием протокола HTTPS.
4. доступ к журналу информационного обмена должен иметь только пользователь с правами Администратора.

События ИК-услуги, подлежащие обязательному журналированию:

* + авторизация (вход и выход) пользователей, успешные и неуспешные попытки авторизации;
	+ создание, копирование, перемещение, удаление, модификация локальных учетных записей и конфигурационных файлов;
	+ неудавшиеся или отвергнутые действия пользователя;
	+ получение пользователем доступа к объектам доступа;
	+ все действия администраторов СПП;
	+ все действия пользователей в СПП.

 f) Требования к формату файла журнала событий:

− журнал событий должен быть в текстовом формате (нельзя использовать журнал событий в бинарном формате);

− журнал событий должен иметь расширения следующих видов: \*.txt, \*.log;

− расположение файлов журналов событий должны быть в отдельной папке в корневой директории ИС/ПО/СПО/СПП;

− наименование папки с файлами журналов событий должно описывать информацию о хранении журналов событий;

− уровень журналирования событий должен соответствовать Единым требованиям в области информационной безопасности.

g) Журнал СПП в обязательном порядке должен содержать следующие поля:

* дата и время (формат) даты: ДД: ММ: ГГГГ, формат времени: ЧЧ: ММ: СС). Временная метка должна располагаться вначале строки. Необходимо использовать часовой пояс, в формате GMT/UTC с указанием часового пояса.

Необходимо обеспечить синхронизацию времени журналов регистрации событий с инфраструктурой источника времени.

* Наименование источника события (сервис/служба);
* Имя учетной записи/ID пользователя;
* IP-адрес клиента;
* Время начала операции;
* Время окончания операции;
* Уровень события;
* Категория события;
* Описание события
	+ 1. Требования к формату журналов событий:
* для событий, фиксируемых в журналах событий необходимо определять формат записи. Значения полей необходимо разделять символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применять символыограничители полей;
* журналы событий должны быть в текстовом формате, каждое событие должно содержать всю информацию в одной строке. В дополнение, допускается хранение журналов в формате XML, а также в табличной форме в БД;
* для журналов событий должна использоваться кодировка UTF-8;
* в один файл журнала событий не допускается запись событий, имеющих разные форматы данных;
* в журналах событий необходимо использовать пары ключ-значение. Если значение содержит пробелы, их необходимо поместить в кавычки;
* в журналах событий необходимо использовать уникальные идентификаторы (ID). Не изменять уникальные идентификаторы (Идентификаторы транзакций, идентификаторы пользователя), и их формат, на всем пути следования транзакции;
* уровень событий должен быть расширенным. Необходимо добавлять информацию о входах и выходах пользователя, действия пользователя, транзакции, информацию о времени и так далее;
* в журналах событий необходимо установить категории события, следующие значения:
* INFO;

• WARN;

• ERROR;

• DEBUG.

Поставщик на этапе разработки СПП при настройке журналирования событий учитывает необходимость аудита действий пользователей СУБД с администраторскими привилегиями.

2.3.2. Журналы регистрации событий хранятся в течение срока, указанного в ТД ИБ, но не менее трех лет и находятся в оперативном доступе не менее трех месяцев;

2.3.3. При журналировании событий необходимо обеспечивать синхронизацию времени с инфраструктурой источника времени.

* 1. Модуль управления парольной защитой (длина, сложность, периодичность смены, разблокировка и т.д.):
1. пользователь (с правами – администратор) ИК-услуга на основании предоставленных заявочных документов, регистрирует нового пользователя и активирует учетные записи. При первом входе в ИК-услуга, пользователь должен в принудительном порядке сменить пароль;
2. модуль должен в принудительном порядке обеспечивать выбор пароля учетной записи с учетом выполнения следующих требований:
	* + длина пароля должна быть не менее 8 символов;
		+ в числе символов пароля обязательно должны присутствовать буквенные символы (необходимо использовать буквы в верхнем и нижнем регистре), цифры и (или) специальные символы (#, $, @ и др.);
		+ запрещается использовать в качестве пароля «пустой» пароль;
		+ пароль не должен включать в себя легко вычисляемые сочетания символов, а также стандартное расположение букв на клавиатуре (zyxwvuts, 123, 123321, qwerty и т.д.);
		+ в СПП должно быть установлено принудительная смена пароля 1 раз в полгода. Вместе с этим, пользователи должны иметь возможность смены пароля в любое время. Запрещено использование ранее применявшихся паролей - новый пароль должен отличаться от старого не менее чем на 3 позиции, не должен совпадать как минимум с двумя предыдущими паролями и с именем учетной записи пользователя. Пароли для административных учетных записей должны соответствовать минимальным требованиям к парольной защите. Новый пароль администратора не должен совпадать как минимум с тремя предыдущими паролями, не должен совпадать с именем учетной записи пользователя;
		+ пароли на доступ к различным ресурсам должны различаться, не допускается использование универсальных паролей для административных учетных записей;
		+ случаи неудавшихся попыток авторизации должны фиксироваться в журнале логирования, с выводом соответствующего сообщения пользователю.
	1. Модуль управления учетными записями:

В модуле управления учетными записями должна быть предусмотрена распределенная система администрирования. На центральном уровне, Администратором должны осуществляться следующие действия:

− регистрация пользователей;

− создание учетной записи для пользователей;

− назначение и управления ролями;

− корректировка учетных записей пользователей;

− аннулирование регистрационных данных пользователей и учетной записи;

− создание отдельных учетных записей на уровне операционных систем, прикладного ПО и систем управления базами данных для запуска, подключения, работы с минимальными привилегиями с обеспечением штатной работоспособности

На центральном уровне администратором должны осуществлять действия:

* + 1. регистрация пользователя с ролью администратор;
		2. корректировка пользователей с ролью администратор;
		3. назначение и управления ролями. Регистрация пользователей:
		4. в модуле управления учетными записями у пользователя (с ролью – администратор) ИК-услуга должна быть возможность на основании предоставленных заявочных документов регистрировать новых пользователей (при необходимости) и включить пользователя в группу. Группы создаются соответственно организационной структуре ведомства в соответствии предоставляемыми им ролей. У пользователя (с ролью - администратор) должна быть возможность активировать учетные записи.

Корректировка регистрационных данных пользователей:

* у пользователя (с ролью – администратор) должна быть возможность корректировки учетных записей.

Аннулирование регистрационных данных пользователей:

* у пользователя (с ролью – администратор) должна быть возможность аннулировать учетные записи.

При использовании ЭЦП:

Для обеспечения подтверждения принадлежности и действительности открытого ключа ЭЦП и регистрационного свидетельства лица, подписавшего электронный документ, прикладное ПО должно осуществлять проверки:

* + подлинности ЭЦП;
	+ построения корректной цепочки от проверяемого регистрационного свидетельства до доверенного корневого регистрационного свидетельства удостоверяющего центра, с учетом промежуточных регистрационных свидетельств удостоверяющих центров;
	+ срока действия регистрационного свидетельства от проверяемого регистрационного свидетельства до доверенного корневого регистрационного свидетельства удостоверяющего центра, с учетом промежуточных регистрационных свидетельств удостоверяющих центров;
	+ регистрационного свидетельства на аннулирование одним из методов:

− на основе списка отозванных регистрационных свидетельств;

− онлайн-проверка регистрационного свидетельства на аннулирование;

− на основе дополнительного списка отозванных регистрационных свидетельств;

* + области использования ключа ЭЦП;
	+ номера политики регистрационного свидетельства и разрешенных способах его использования;
	+ метки времени при необходимости;
	+ полномочий лица, подписавшего электронный документ;
	+ серийный номер регистрационного свидетельства.
1.
2.
3.
4.
5.
6.
7. 1.

### **Мониторинг обеспечения безопасного функционирования объектов информатизации ЭП**

С целью реализации мониторинга обеспечения информационной безопасности «электронного правительства» Оператор должен обеспечить сбор журналов регистрации событий ИК-услуга в единую систему сбора журналов регистрации событий Оператора для передачи в систему управления событиями информационной безопасности АО «ГТС», согласно пункту 12 [8].

### **Требование к журналированию**

Журналы необходимо хранить в течение срока, указанного в нормативно-технической документации в сфере обеспечения информационной безопасности, но не менее трех лет, а также быть в оперативном доступе не менее трех месяцев; При журналировании событий необходимо обеспечивать синхронизацию времени с инфраструктурой источника времени.

Модуль журналирования событий должен обеспечивать взаимодействие с системами SIEM по протоколу syslog. (RFC 5424).

Расположения директорий базы данных отдельно от ОС (на разных дисках).

Требования к формату журналов событий:

− для событий, фиксируемых в журналах необходимо определять формат записи. Значения полей необходимо разделять символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применять символы-ограничители полей;

− журналом событий является текстовый файл, на каждой строчке которого записывается одно событие;

− для журналов должна использоваться кодировка UTF-8;

− в один файл журнала не допускается запись событий, имеющих разные форматы данных;

− в журнале событий необходимо использовать пары ключ-значение. Если значение содержит пробелы, их необходимо поместить в кавычки;

− расположение файлов журналов событий должны быть в отдельной папке в корневой директории СПП;

− наименование папки с файлами журналов событий должно отражать содержание.

События СПП подлежащие обязательному журналированию:

− создание, копирование, перемещение, блокирование, модификация локальных учетных записей;

− неудавшиеся или отвергнутые действия пользователя;

− все действия пользователей в СПП; − получение пользователем доступа к объектам доступа;

− все действия администраторов системы.

Журнал ПО в обязательном порядке должен содержать следующие поля:

− дата и время (формат даты: ДД: ММ: ГГГГ, формат времени: ЧЧ: ММ: СС). Временная метка должна располагаться вначале строки. Необходимо использовать часовой пояс, в формате GMT/UTC с указанием часового пояса. Время должно быть показано в миллисекундах в каждом событии.

Необходимо обеспечить синхронизацию времени журналов регистрации событий с инфраструктурой источника времени.

− наименование источника события (сервис/служба);

− логин/ имя учетной записи/ID пользователя;

− IP-адрес клиента;

− время начала операции;

− время окончания операции.

Уровень события (необходимо установить следующие уровни события):

− Alerts - необходимо срочное вмешательство;

− Critical - критические события;

− Errors - сообщения о ошибках;

− Warning - всевозможные предупреждения;

− Notifications - различные важные уведомления;

− Informational - информационные сообщения;

− Debug - для отладки приложений;

− категория события;

 − описание события.

### **Требования к организации защиты информации**

Защита информации при информационном взаимодействии должна обеспечиваться за счет мероприятий технического и организационного характера в соответствии [3] и [4].

Для обеспечения защиты информации необходимо обеспечить:

- внедрение процедур аутентификации и авторизации;

- использование ЭЦП;

- обеспечение доступности и отказоустойчивости;

- контроль событий нарушения ИБ;

- регистрацию событий.

С целью контроля событий нарушений ИБ должны быть соблюдены требования подпунктов 1)-7) пункта 38 [4]:

1) проводится мониторинг событий, связанных с нарушением ИБ, и анализ результатов мониторинга;

2) регистрируются события, связанные с состоянием ИБ, и выявляются нарушения путем анализа журналов событий:

− журналов событий операционных систем;

− журналов событий систем управления базами данных;

− журналов событий антивирусной защиты;

− журналов событий прикладного ПО;

− журналов событий телекоммуникационного оборудования;

− журналов событий систем обнаружения и предотвращения атак;

 − журналов событий системы управления контентом.

3) обеспечивается синхронизация времени журналов регистрации событий с инфраструктурой источника времени;

4) журналы регистрации событий хранятся в течение срока, указанного в ТД ИБ, но не менее трех лет и находятся в оперативном доступе не менее двух месяцев;

5) ведутся журналы регистрации событий создаваемого ПО в соответствии с форматами и типами записей, определенными в Правилах проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры, утверждаемых уполномоченным органом;

6) обеспечивается защита журналов регистрации событий от вмешательства и неавторизированного доступа. Не допускается наличие у системных администраторов полномочий на изменение, удаление и отключение журналов. Для конфиденциальных ИС требуются создание и ведение резервного хранилища журналов;

7) обеспечивается внедрение формализованной процедуры информирования об инцидентах ИБ и реагирования на инциденты ИБ.

Также, должны быть соблюдены требования пункта 1) статьи 30 [3] и подпункта 9) п. 139 [4] касательно подключения к Интернету через единый шлюз доступа к Интернету.

Оператором должно быть обеспечено:

* журналирование событий операционных систем, систем управления базами данных, антивирусной защиты, прикладного ПО, телекоммуникационного оборудования, систем обнаружения и предотвращения атак, системы управления контентом, согласно нормам подпункта 2) пункта 38 [4].
* регистрация в службе реагирования на компьютерные инциденты АО «ГТС» события ИБ, идентифицированные Оператором как критические для конфиденциальности, доступности и целостности, по результатам анализа мониторинга событий ИБ и анализа журнала событий.

Для обеспечения ИБ при использовании технологии виртуализации управление инцидентами ИБ, требующее:

− определения формального процесса обнаружения, выявления, оценки и порядка реагирования на инциденты ИБ с актуализацией раз в полугодие;

− составления отчетов с периодичностью, определенной в ТД ИБ, по результатам обнаружения, выявления, оценки и реагирования на инциденты ИБ;

− уведомления ответственных лиц ГО, МИО или организации об инцидентах ИБ;

− регистрации инцидентов ИБ в Службе реагирования на компьютерные инциденты Государственной технической службы.

# Требования к взаимодействию с системой мониторинга

Поставщиком должна обеспечиваться передача данных (журналирование лог-файлов или иные методы) с содержанием следующих статистических параметров:

Уровень СУБД:

* информация по сессиям;
* информация о состоянии базы данных/ службы СУБД;
* информация по системным ошибкам СУБД;
* информация о размере файлов системной и пользовательской базы данных, о размере резервной копии БД;
* информация по ошибкам СУБД;
* информация по блокировкам;
* информация по транзакциям (если имеются) (успешные, зависшие, откатанные);
* информация по использованию табличных пространств;
* информация по запросам.

Уровень ППО:

* информацию по статусам системных и сервисных служб ППО;
* информация о статусе состояния модулей приложения;
* информация о состоянии и количестве транзакций (если имеются) - (успешные, зависшие, текущие, откатанные);
* информация по объему JMX памяти, объем заполнения JMX памяти;
* информация о количестве и лимите подключения к серверу приложения.

В случае наличия взаимосвязи с сервисами или компонентами необходимо обязательное логирование их состояния.

Уровень сервиса:

* информация о доступности сервисов по протоколам НТТР, НТТPS;
* информация о времени обработки сервисов по URL.

СПП должен обеспечивать интерфейс подключения для забора данных по следующему
статистическому параметру:

Уровень ППО:

- информация о доступности приложения по порту.

При этом должен быть обеспечен режим круглосуточного мониторинга устройств ИК-услуги посредством ЕСМ с обеспечением оповещения при сбоях/ восстановлениях посредством звонков или электронной почты.

# Условия и требования к вводу в эксплуатацию ИК-услуги, СПП и требования к технической документации

* 1. **Требования к документации**

Поставщиком должна быть разработана техническая документация, представленная в таблице ниже (Таблица 30).

Техническая документация должна быть представлена в редактируемом формате Microsoft Word на русском и казахском языках в трех экземплярах на электронных и бумажных носителях.

Техническая документация должна быть согласована с Оператором в сроки, определенные Протоколом комиссии.

Поставщик в рамках договора аренды СПП должен по требованию Заказчика ИК-услуги и Оператора актуализировать материалы, указанные в Таблице 30.

Таблица 30. Перечень документов, разрабатываемых Поставщиком.

| **№ п/п** | **Наименование документа** | **Требования к документу** |
| --- | --- | --- |
| 1 | Текст программы | ГОСТ 19.401-2000. ЕСПД. Текст программы. Требования к содержанию, оформлению и контролю качества |
| 2 | Описание программы | ГОСТ 19.402-2000. ЕСПД. Описание программы. Требования к содержанию, оформлению и контролю качества |
| 3 | Общее описание системы | Документ должен содержать разделы:1) назначение системы;2) описание системы;3) описание взаимосвязей с другими системами;4) описание подсистем, компонентов (при необходимости).1. В разделе "Назначение системы" указывают:1) вид деятельности, для автоматизации которой предназначена система;2) перечень объектов автоматизации, на которых используется система;3) перечень функций, реализуемых системой.2. В разделе "Описание системы" указывают:1) структуру системы и назначение ее частей (с приложением локальной схемы ИК, IP-адресов и портов);2) сведения об ИС в целом и ее частях, необходимые для обеспечения эксплуатации системы;3) описание функционирования системы и ее частей.3. В разделе "Описание подсистем" указывают:1) структуру подсистем и назначение ее частей;2) сведения об подсистемах и их частях, необходимые для обеспечения их функционирования;3) описание функционирования подсистем и их частей. |
| 4 | Руководство администратора | РД 50-34.698-90. Руководящий документ по стандартизации (Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов)Руководство администратора должно быть предназначено для администратора ИС, администратора СУБД, ППО и ОС.ГОСТ 19.503-79.ЕСПД. Руководство системного программиста. Требования к содержанию и оформлению.Руководство должно быть предназначено для администратора СУБД, ППО, ОС и должны содержать дополнительные требования:1. Основные требования по администрированию и восстановлению ОС:1. Установка ОС.
2. Настройка ОС.
3. Ошибки в ОС и отказ системы.
4. Восстановление ОС (в случае потери сервера приложений, базы данных, сервера балансировки).
5. Создание резервной копии ОС.
6. Периодичность резервного копирования ОС и сроки хранения резервных копий.
7. Инструкция по восстановлению ОС с резервных копий.
8. Настройка firewall (80,443,88,8443,).
9. Настройки NTP.
10. Настройки автозагрузки служб и сервисов.
11. Настройки планировщика(crontab).
12. Обоснование каждой учетной записи.
13. Ротация логов.
14. Состояние заполняемости дисков.
15. Системные лимиты.
16. Лицензии на ОС.

17) Подключения к мониторингу (zabbix, splunk).2. Основные требования по администрированию СУБД:1. Какая СУБД используется (Версию СУБД, редакцию и т.п.). Ссылка на логические/функциональные/архитектурные схемы.
2. Описание установки СУБД / кластера СУБД (если Поставщик сам установил либо переустанавливал).
3. Настройка СУБД (на основном и резервном сервере БД) с описанием измененных параметров и параметров по умолчанию.
4. Описание кластерных решении или других решении для обеспечения отказоустойчивости (если используется). Описание реализации этих решении.
5. Создание пользователей СУБД и их привилегии.
6. Описание шифрования (если используется). Например, описать шифрование паролей, шифрование соединении, шифрование данных и использование сертификатов.
7. Журналирование событий СУБД и действии пользователей, настройка аудита согласно ЕТ.
8. Описание отказоустойчивости серверов БД и настройку резервной БД (репликация)
9. Инструкция и требования для резервного копирования БД СПП
10. Инструкция и требования для восстановления БД ОДО
11. RTO и RPO. Регламент Резервного копирования.
12. Описание возможности масштабирования и реализации при необходимости.
13. Задачи (джобы) которые запускаются через планировщика (если есть).

3. Основные требования по администрированию и восстановлению ППО:3.1. Установка ППО (пошаговая установка ППО на каждом компоненте СПП, с указанием используемых портов и их назначений);3.2. Настройка ППО (Описание настройки ППО на каждом компоненте ОДО, с описанием изменяемых параметров по умолчанию; описание дополнительно установленных/настроенных служб, сервисов, портов; описание проводимых действий при масштабировании ОДО; описание настройки ППО для отказоустойчивости ОДО);3.3. Обновление приложений на серверах ППО;3.4. Ошибки на ППО и примеры их решения;3.5. Отказ системы, причины (как пример: зависания вследствие выгружаемых пользователями отчетов или выходных документов и т.д.);3.6. Восстановление работоспособности ППО (Инструкция по остановке и запуску ППО ОДО);3.7. Резервное копирование ППО.\* После проведения обучения администраторов СУБД, ППО, ОС, возможно внесение дополнений к руководству администратора СУБД, ОС и ППО. |
| 5 | Программа и методика испытаний | Требования к документу: ГОСТ 19.301-2000 ЕСПД. Программа и методика испытаний. Требования к содержанию, оформлению и контролю качества. Требования к плану тестирования: СТ РК 1089-2002 ЕСПД. Программа и методика испытаний. Планирование проведения испытаний программного обеспечения. |
| 6 | Руководство пользователя | СТ РК ISO/IEC 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности свод правил по средствам управления защитой информации»;СТ РК ISO/IEC 27001-2015 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования; |
| 7 | Руководство пользователя. Администратора ОДО | СТ РК 1087 - 2002. Единая система программной документации. Руководство пользователя. Требования к составу, содержанию и оформлению.  |
| 8 | Обучающие материалы | * + - 1. Инструкция по работе в ОДО по ролям пользователей;
			2. Инструкция по настройкам рабочих станций на местах пользователей (технические требования к ПК, ПО, локальные вычислительные сети, единая транспортная среда государственных органов и т.д.).
			3. Инструкция по работе АРМ Администратора.
			4. Обучающий видеоролики для пользователей.
			5. Презентации по ОДО.
 |
| 10 | Функциональная и логическая схема ОДО  | СТ РК 34.006-2002 Информационная технология. Базы данных. Основные термины и определения;СТ РК 34.007-2002 Информационная технология. Телекоммуникационные сети. Основные термины и определения;СТ РК ISO/IEC 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности свод правил по средствам управления защитой информации»;требования пункта 4 Анкеты-вопросника Приложения № 2 к Правилам проведения испытаний объектов информатизации "электронного правительства" и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности, утвержденные Приказом Министра цифрового развития, оборонной и аэрокосмической промышленности РК от 3 июня 2019 года № 111/НҚ– в этом пункте приводится требования к составу функциональной схемы и схемы сети телекоммуникаций. |
| 11 | Паспорт СПП с приложениями | Паспорт СПП с приложениями разрабатывается согласно внутренней документации Оператора (Требования к Паспорту и технической документации на сопровождение сервисного программного продукта Утвержденный Заместителем Председателя Правления от 9 июля 2018 года). |
| 12 | Соглашение по реализации интеграции объектов информатизации | Приказ и.о. Министра информации и коммуникаций Республики Казахстан от 29 марта 2018 года № 123 «Об утверждении Правил интеграции объектов информатизации «электронного правительства» |
| 13 | Иные документы | Полное описание структуры базы данных (имя БД, предназначение БД, диаграмма или описание связи между объектами, описание следующих объектов: таблицы, столбцы, представления, триггеры, хранимые процедуры, функции и т.п.).После заключения договора на аренду СПП по запросу Заказчика необходимо предоставить план-график по разработке СПП ОДО в MS Project с приложением диаграммы Ганта.  |

### **Требования к порядку и условиям передачи сервисного программного продукта**

В соответствии со статьей 47 [3] Поставщик должен обеспечить передачу Оператору компонентов и модулей объекта СПП с библиотеками и файлами на компакт-диске в трех экземплярах.

Передача СПП должна быть оформлена актом приема-передачи между Поставщиком и Оператором на государственном и русском языках.

По требованию Заказчика нормативно-техническая документация должна передаваться на государственном языке.

### **Требование к приемке**

Поставщик должен пройти квалификационный и конкурсный отбор в соответствии с п. 5 Статьи 45-1 [3].

В случае необходимости Поставщику для разработки и (или) тестирования СПП Оператором по запросу Сервисного интегратора в срок не более 5 (пяти) рабочих дней должна быть предоставлена информационно-коммуникационная инфраструктура.

По итогам создания СПП Поставщиком должно быть направлено в адрес Сервисного интегратора уведомление о готовности к тестированию, в сроки, установленные протоколом об определении Поставщика, сформированным в соответствии с п. 64 [6] Комиссией по результатам конкурсного отбора.

В соответствии с пп. 3) п. 98 и пп. 8) п. 102 [4] должно быть обеспечено разделение сред опытной или промышленной эксплуатации от сред разработки, тестирования или стендовых испытаний, а также физическое разделение сред эксплуатации от сред разработки и тестирования.

Тестирование готового решения потенциального поставщика проводится на ИК-инфраструктуре Оператора для разработки и тестирования объекта ИКИ в соответствии с Планом тестирования, разработанным Сервисным интегратором.

По результатам проведения тестирования СПП и испытаний на соответствие требованиям информационной безопасности комиссия формирует протокол с решением по выбору поставщика или поставщиков с приложением стоимости на сервисный программный продукт заявленной потенциальным поставщиком, и вводу СПП в эксплуатацию. На основании данного протокола Сервисный интегратор инициирует включение ИК-услуги в Каталог ИК-услуг.

Испытания на соответствие требованиям ИБ проводятся АО «ГТС» в соответствии с [17].

КИБ МЦРИАП РК выдает акт на соответствие требованиям информационной безопасности, либо мотивированный отказ.

В случае отрицательного результата испытаний СПП на соответствие требованиям информационной безопасности, потенциальный поставщик в течение пятнадцати дней после получения протокола устраняет выявленные замечания и проходит испытания повторно (но не более одного раза).

Испытания признаются положительными при наличии Акта испытаний с положительным заключением, выдаваемого после проведения всех видов работ, входящих в испытания, и наличия по ним протоколов с положительными результатами.

Результаты прохождения испытания СПП на соответствие требованиям информационной безопасности подтверждаются Актом, формируемым КИБ МЦРИАП РК.

###  **Требования к развертыванию**

В инструкции по развертыванию должны быть приведены следующие сведения:

* описание возможных (типовых) конфигураций СПП, прикладного и системного ПО на базе ИКП ЭП;
* пошаговый порядок (алгоритм) развертывания каждой типовой конфигурации;
* порядок проверки работоспособности системы, полученной после установки.

При внедрении СПП необходимо провести миграции данных (документов) из текущей ИС с сохранением полной иерархии (истории, хода исполнения, ссылок на документы) документов, а также должен позволять выгружать реквизиты документов и вложения в xml-формате.

### **Порядок конфигурирования и настройки СПП**

После этапа развёртывания Поставщик согласно Плану внедрения СПП в ГО должен провести следующие работы по конфигурированию и настройки СПП:

1. Создание пользователей и групп пользователей.
2. Определение прав пользователей и групп пользователей.
3. Общая настройка бизнес-процессов под нужды ГО.

*При необходимости дополнительной настройки.*

Кроме того, Поставщик должен предоставить видеоролик по настройке СПП.

### **Требования к исходным кодам**

Требования к исходным кодам должна производиться, согласно [13].

Поставщик должен предоставить исходные коды СПП, включая компоненты и модули СПП, необходимыми для успешной компиляции СПП, в целях обеспечения взаимодействия с другими ИК-услугами или ИС ГО для СИ, а также для прохождения испытаний ИК-услуги в АО «ГТС» согласно [13].

Поставщик обязуется передать Заказчику информационно-коммуникационной услуги имущественные (исключительные) права на СПП путем заключения договора на условиях Заказчика сервисного программного продукта с предоставлением оригинала или нотариально заверенной копии авторского договора, заключенного между Поставщиком и автором(ми) и свидетельства о внесении сведений в государственный реестр прав на объекты, охраняемые авторским правом. Договор на передачу исключительных прав заключаемый между Поставщиком и Заказчиком информационно-коммуникационной услуги должен быть заключен по истечению 3 лет с момента включения СПП в каталог информационно-коммуникационных услуг и содержать условия права пользования без выплаты вознаграждений автору (-ам) и с указанием всех передаваемых имущественных прав согласно ст.16 [1].

### **Требования к пользовательскому интерфейсу**

Разрабатываемый интерфейс СПП должен быть WEB-ориентированным, понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое (максимальное время отображение – 5 секунд) отображение экранных форм. Навигационные элементы должны быть выполнены в удобной для пользователя форме. Средства редактирования информации, ввод-вывод данных СПП должны обеспечивать функциональную симметрию с офисными приложениями или соответствовать аналогичным сокращениям операционной системы, привычные для пользователя.

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

Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений) должны быть на государственном и русском языках в зависимости от выбора интерфейса пользователем.

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

Экранные формы должны проектироваться с учетом требований унификации:

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

«мыши», переключение фокуса, нажатие кнопки) должны реализовываться одинаково для однотипных элементов;

* при выполнении сложных запросов, требующих длительное время на выполнение пользователь должен получить сообщение о выполнении запроса;
* все пиктограммы, присутствующие на рабочих окнах модулей, должны в обязательном порядке быть снабжены надписями, поясняющими их назначение и разворачивающимися на экране при установке курсора в центр пиктограммы;
* при работе с модулями должно быть предусмотрено наличие режима «Помощь».

Эргономические решения пользовательского интерфейса должны быть едиными для всех модулей ИК-услуга.

Интерфейс программного продукта должен обеспечивать просмотр прикрепленных файлов следующих форматов:

1. PDF
2. TIFF, JPEG - графический форматы;
3. RTF, DOC, DOCX - текстовый форматы;
4. XLS, XLSX - табличный формат;
5. PPT - презентации;
6. Должна быть реализована функция просмотра файла скан - образа документа, как в отдельном окне, так и в основном окне программы, вместе с отображением классификатора архива, списка документов и карточки описания документа.

### **Требования к процессу и материалам обучения пользователей**

### **Требование к процессу обучения**

В соответствии со статьей 47 [4] Поставщик должен обеспечить проведение обучения персонала Оператора по эксплуатации и сопровождению СПП.

Поставщик должен обеспечить проведение обучения пользователей Заказчика ИК-услуги по работе с СПП.

Состав участников обучения должен определяться Оператором. По итогам проведения обучения Поставщиком должен быть оформлен и подписан Оператором протокол обучения.

Протокол обучения должен содержать следующую информацию:

1) объект обучения;

2) основание проведения обучения;

3) цель обучения;

4) документация, предоставляемая на обучении;

5) объем обучения (сценарий обучения);

6) список лиц, присутствовавших на обучении;

7) список лиц, проводивших обучение;

8) список лиц, прошедших обучение;

9) место и продолжительность обучения (место обучения, начало обучения, окончание обучения);

10) результаты обучения.

Поставщик должен обеспечить обучение сотрудников операторов Единого контакт центра Кроме того, Поставщик должен обучить сотрудников Оператора, осуществляющих сопровождение СПП и сотрудников Заказчика, осуществляющих внедрение и сопровождение СПП.

База знаний по вопросам 1-линии поддержки для сотрудников Единого контакт-центра. База знаний по вопросам 2-линии поддержки для сотрудников по сопровождению на 2 линии поддержки.

В случае необходимости Поставщик актуализирует обучающие материалы по запросу от Заказчика или Оператора.

### **Требования к материалам обучения пользователей**

Документация должна быть разработана на казахском и русском языках и предоставлена Комиссии:

* На бумажном носителе в формате А4 в 3 (трех) экземплярах;
* На CD-диске (в не редактируемом формате (.pdf) и в редактируемом формате (.doc)) в 3 (трех) экземплярах.
* Инструкции по работе в СПП по ролям пользователей.
* Инструкции по настройкам рабочих станций на местах пользователей (технические требования к ПК, ПО, локальные вычислительные сети, единая транспортная среда государственных органов и т.д.).
* Инструкции по настройке ПО;
* Презентации по СПП;
* Обучающий ролик по работе СПП.

### **Требование к прототипу СПП**

Прототип должен включать в себя основной функционал бизнес-процессов, описанных в ЗНП.

На демонстрацию прототипа потенциальные поставщики должны предоставить информационные материалы со следующим содержанием:

* описание архитектуры и технологий решения;
* основные преимущества планируемого к реализации сервисного программного продукта;
* условия технической поддержки и обучения (при необходимости);
* опыт работы компании (с приложением подтверждающих документов к заявке, в случае если критерий указан в форме объявления).

**Таблица 32. Критерии оценки прототипа и архитектуры решения:**

|  |  |
| --- | --- |
| **Критерии** | **Балл** |
|  | **0** | **1** | **2** | **3** |
| **Не реализовано или не представлено** | **Частично соответствует требованиям** | **Полностью соответствует требованиям** | **Превосходит требования** |
| Реализация основных заданных функций/функционала/бизнес кейса |  |  |  |  |
| Архитектура предлагаемого решения |  |  |  |  |

### **План коммуникаций и матрица ответственности создания СПП**

**Таблица 33. План коммуникаций и матрица ответственности**

| **№ п/п** | **Наименование мероприятия** | **Длительность** | **Ответственный** | **Соисполнитель** | **Форма****завершения** |
| --- | --- | --- | --- | --- | --- |
|  | Разработка задания на проектирование ИК-услуги | Не более 25 рабочих дней со дня получения официального заключения о целесообразности реализации СПП | Сервисный интегратор | МЦРИАП РК  | Проект ЗНП |
|  | Согласование задания на проектирование ИК-услуги | Не более десяти рабочих дней со дня поступления официального запроса на согласование от СИ | Сервисный интегратор | АО ГТС,Оператор,МЦРИАП РК, МЦРИАП РК, | Согласованное ЗНП |
|  | Публикация проекта ЗНП для обсуждения | в течении семи рабочих дней со дня опубликования проекта ЗНП | Сервисный интегратор | МЦРИАП РК | Замечания и (или) предложения к проекту ЗНП |
|  | Утверждение задания на проектирование ИК-услуги | Не более пяти рабочих дней со дня поступления официального запроса на согласование от СИ | МЦРИАП РК | Сервисный интегратор | Утвержденное ЗНП |
|  | Создание конкурсной комиссии по определению поставщика СПП  | Не более пяти рабочих дней | Сервисный интегратор | Сервисный интегратор, Оператор, МЦРИАП РК |  |
|  | Публикация объявление о начале приема заявок на участие в разработке  | В течении 22 рабочих дней | Сервисный интегратор | МЦРИАП РК | Заявки на разработку СПП |
|  | Решение о допуске к конкурсному отбору  | Не более пяти рабочих дней | Комиссия по созданию СПП | Сервисный интегратор | Протокол допуска потенциальных поставщиков к конкурсному отбору |
|  | Разработка прототипа СПП | В соответствии с Протоколом квалификационного отбора Комиссии | Потенциальный поставщик | Сервисный интегратор | Прототип СПП |
|  | Конкурсный отбор потенциального поставщика | В соответствии с Протоколом квалификационного отбора Комиссии | Комиссия по созданию СПП | Сервисный интегратор | Протокол об определении потенциального поставщика |
|  | Предоставление ИК - инфраструктуры для тестирования (при необходимости) | Не более пяти рабочих дней | Оператор | Поставщик,Сервисный интегратор | Письмо о предоставлении ИК - инфраструктуры для тестирования от Оператора в адрес СИ |
|  | Разработка СПП и технической документации к СПП | Не более двух календарных месяца | Потенциальный поставщик | Сервисный интегратор | Разработанный СПП, в том числе техническая документация к СПП |
|  | Разработка Плана тестирования | Во время разработки СПП | Сервисный интегратор |  | План тестирования |
|  | Направление в СИ уведомление о готовности к тестированию | После одного месяца с момента начала разработки СПП | Потенциальный поставщик | Сервисный интегратор | Уведомление, техническая документация, официально направленная в СИ  |
|  | Тестирование на работоспособность СПП | Согласно Плану тестирования СПП | Комиссия по созданию СПП | Оператор,Сервисный интегратор,Потенциальный поставщик | Протокола тестирований |
|  | Опытная эксплуатация | По завершению необходимых испытаний и экспертиз | Поставщик | Оператор,Сервисный интегратор,Комиссия по созданию СПП | Акт о вводе в опытную эксплуатацию, Акт о завершении опытной эксплуатации |
|  | Испытание СПП на соответствие требованиям ИБ  | Согласно договору на проведение испытаний между АО ГТС и потенциальным поставщиком | Потенциальный поставщик АО ГТС | Сервисный интегратор, Оператор | Акт испытаний, протокола испытаний |
|  | Выдача акта по результатам испытаний на соответствие требованиям ИБ | 10 рабочих дней осуществляется  | КИБ МЦРИАП РК | Потенциальный поставщик | Акт испытаний |
|  | Решение о формировании ИК-услуги. | Не более пяти рабочих дней | Комиссия по созданию СПП | Сервисный интегратор | Протокол комиссии по решению о формировании ИК-услуги   |
|  | Ввод ИК-услуги в промышленную эксплуатацию  | Один месяц | Поставщик, Оператор | МЦРИАП РК, Сервисный интегратор Поставщик, Оператор | Протокол, Акты ввода в эксплуатацию |
|  | Инициация включения ИК-услуг в Каталог ИК-услуг. | Не позднее 5 (пяти) рабочих дней со дня подписания протокола ввода в эксплуатацию СПП или объекта и ИК-услуги по уведомлению оператора | МЦРИАП РК | Сервисный интегратор | Письмо, Приказ |

### **Дополнительные требования и условия по созданию ИК-услуги, СПП**

* 1. **Требования к включению ИК-услуги в Каталог ИК-услуг**

Сервисный интегратор в срок не позднее 5 (пяти) рабочих дней со дня подписания протокола ввода в эксплуатацию сервисного программного продукта или объекта и ИК-услуги по уведомлению оператора инициирует включение ИК-услуг в Каталог ИК-услуг.

Каталог с описанием ИК-услуг, оказываемых государственным органам, и информация об их стоимости размещаются на интернет-ресурсе Оператора.

* 1. **Требования к оказанию ИК-услуги**

Обязанности, размер, срок и условия финансирования оказании ИК-услуг и ответственность сторон устанавливаются договором СМИ.

Оператор в срок не позднее 5 (пяти) рабочих дней со дня заключения договора СМИ с заказчиком ИК-услуги, заключает договор об аренде сервисного программного продукта или объекта ИКИ с выбранным поставщиком согласно пункту 105 [14].

* 1. **Требования к технической поддержке СПП**

Взаимодействие Оператора и Поставщика при оказании информационно-коммуникационных услуг регулируется Соглашением согласно п.1 статьи 47 [6].

В соответствии с пунктом 106 [6] в рамках предоставления аренды СПП Поставщик должен обеспечить техническую поддержку СПП в соответствии с договором аренды СПП между Оператором и Поставщиком.

Поставщик должен обеспечить функционирование 3 линии поддержки для осуществления технической поддержки программного кода СПП, а также для осуществления консультационного сопровождения по вопросам оказываемой ИК-услуги, на время действия договора аренды ИК-услуги.

Поставщик должен обеспечить первичное наполнение справочников и реестров СПП данными, необходимыми для функционирования СПП, а также в случае наличия исторических данных осуществлять их миграцию в СПП.

Поставщик в рамках технической поддержки программного кода СПП должен осуществлять следующие работы:

1) прием и своевременное устранение программных ошибок и сбоев, вызванных в процессе эксплуатации СПП в режиме 24/7/365;

2) консультация и помощь в разрешении всех видов запросов по работе в СПП по электронной почте или по телефону в режиме 24/7/365;

3) обновление СПП новыми версиями при необходимости;

4) осуществление миграции данных, предоставленных Заказчиком ИК-услуги;

5) обновление технической документации по мере обновления СПП при необходимости;

6) актуализация справочников СПП по запросу Заказчика ИК-услуги;

7) при необходимости и по согласованию с Заказчиком ИК-услуги, Оператором внесение изменений в СПП;

8) разрабатывать новые формы отчетов по запросу ГО и Оператора по мере поступления;

9) актуализация базы знаний по мере обновления СПП при необходимости;

10) обучение сотрудников Оператора с демонстрацией СПП при необходимости;

11) режим предоставления услуги 24/7/365;

12) выполнение требуемых доработок и функции, указанных в ЗНП.

Запросы по вопросам оказания ИК-услуг разрешаются в порядке и сроки, установленные Регламентом обработки запросов от пользователей информационно- коммуникационных услуг, утвержденным Единым контакт-центром по согласованию с Оператором и поставщиком.

*Также, Поставщик в рамках технической поддержки СПП должен обеспечить первичное наполнение данным справочников, а также настроить конфигураторы для формирования типовых отчетных форм, шаблонов документов.*