**Техническое задание**

**на разработку программного обеспечения**

«**Система платного отпуска воды»**

**1. Общие положения:**

1.1. Предмет: **разработка программного обеспечения** «**Система платного отпуска воды»**

1.2. Начальная максимальная цена Договора определяется расчетом начальной минимальной цены Договора.

1.3. Срок выполнения работ: в течение 6 (шести) месяцев с момента заключения Договора.

1.4. Место выполнения работ:

- автоматизированная станция приема жидких бытовых отходов в районе снегоплавильной установки по Пр. Победы в Советском районе г. Казани;

- водозаправочная станция на ВНС «Тимирязева» г. Казань;

- комплекс автоматизированных водозаборных колонок в г. Казани.

1.5. В цену работ включены стоимость всех материалов и все расходы, связанные с выполнением работ, транспортные расходы по доставке оборудования и рабочей силы до места выполнения работ, все налоги и обязательные платежи.

1.6. Гарантийный срок – 24 мес.

**Система платного отпуска воды**

1. **Общие сведения**

1.1. Отпуск воды происходит либо при авторизации пользователя, либо при оплате банковской картой.

1.2. На один лицевой счет может быть привязано несколько идентификаторов.

1.3. В качестве идентификаторов должны использоваться карт Mifare.

1.4. Состав программно-аппаратного комплекса (далее ПАК);

* Серверное программное обеспечение (далее ПО);
* Автоматизированные рабочие места операторов (далее АРМ);
* Контроллер платежей (см. п.11.1);
* Терминал (включает контроллер и средства взаимодействия с покупателем) (см. п.11);
* Идентификаторы.

1.5. ПАК имеет географически распределенную структуру, т.е. терминалы могут располагаться на значительном удалении от сервера.

1. **Тарифы и процесс отпуска**

**2.1. Предоплаченный тариф** (отпуск только авторизованным пользователям)

* Пользователь подходит к колонке и прикладывает карту (или смартфон)
* Контроллер колонки ищет пользователя в “белом” и “черном” списках
* Если идентификатор нашелся только в “белом” списке, то разрешается отпуск. Если идентификатор нашел и в “белом” и в “черном” списке, то отпуск запрещается. Если карта не найдена, то отпуск запрещен и фиксируется ошибка.
* Контроллер колонки отправляет запрос на сервер
* Сервер отправляет на контроллер информацию о сумме на лицевом счете
* На лицевом счете блокируется сумма максимальной разовой покупки (устанавливается индивидуально для каждой карты)
* Если денег на лицевом счете недостаточно, то бронируется весь остаток
* Информация отображается на дисплее колонки
* Пользователь нажимает кнопку “старт”
* Контроллер включает насос (если необходимо) и открывает клапан, происходит налив
* Контроллер контролирует количество отпущенного ресурса при помощи счетчика
* Налив прекращается по нажатию кнопки “стоп” или по окончании забронированной суммы
* По окончании налива контроллер передает на сервер данные о фактически отпущенном объеме ресурса
* С лицевого счета списывается сумма за фактически отпущенный объем, снимается бронь с остатка.

**2.2. Тариф с постоплатой** (отпуск только авторизованным пользователям)

* Пользователь подходит к колонке и прикладывает карту (или смартфон)
* Контроллер колонки ищет пользователя в “белом” и “черном” списках
* Если идентификатор нашелся только в “белом” списке, то разрешается отпуск. Если идентификатор нашел и в “белом” и в “черном” списке, то отпуск запрещается. Если карта не найдена, то отпуск запрещен и фиксируется ошибка.
* Информация отображается на дисплее колонки
* Пользователь нажимает кнопку “старт”
* Контроллер включает насос (если требуется) и открывает клапан, происходит налив
* Контроллер контролирует количество отпущенного ресурса при помощи счетчика
* Налив прекращается по нажатию кнопки “стоп”
* По окончании налива контроллер передает на сервер данные о фактически отпущенном объеме ресурса
* С лицевого счета списывается сумма за фактически отпущенный объем, фиксируется долг

**2.3. Отпуск по банковской карте** (не требует авторизации)

* Пользователь подходит к колонке и вставляет/прикладывает карту к pos терминалу, набирает желаемую сумму оплаты
* При удачной оплате POS терминал передает информацию о сумме оплаты на контроллер колонки
* Информация отображается на дисплее колонки
* Пользователь нажимает кнопку “старт”
* Контроллер включает насос (если необходимо) и открывает клапан, происходит налив
* Контроллер контролирует количество отпущенного ресурса при помощи счетчика
* Налив прекращается по окончании уплаченной суммы или по нажатию кнопки “стоп” (в этом случае система должна иметь возможность сделать частичный возврат на карту)
* По окончании налива контроллер передает на сервер данные о фактически отпущенном объеме ресурса, сумме платежа

**2.4. Тариф “фиксированный”**

* Пользователь подходит к колонке и прикладывает карту (или смартфон)
* Контроллер колонки ищет пользователя в “белом” и “черном” списках
* Если идентификатор нашелся только в “белом” списке, то разрешается отпуск. Если идентификатор нашел и в “белом” и в “черном” списке, то отпуск запрещается. Если карта не найдена, то отпуск запрещен и фиксируется ошибка.
* Контроллер колонки отправляет запрос на сервер
* На лицевом счету блокируется фиксированная сумма (устанавливается индивидуально для каждой карты)
* Информация отображается на дисплее колонки
* Пользователь нажимает кнопку “старт”
* Контроллер включает насос и открывает клапан, происходит налив
* Контроллер НЕ контролирует количество отпущенного ресурса
* Налив прекращается по нажатию кнопки “стоп”
* По окончании налива контроллер передает на сервер данные о фактически отпущенном объеме ресурса
* С лицевого счета списывается фиксированная сумма (задается для каждой карты)

**2.5. Тариф “вход”**

* С л/с списывается фиксированная сумма (настраивается для каждого идентификатора) по факту входа пользователя на закрытую территорию
* Данные на сервер о факте входа поступают на сервер от системы контроля доступа

1. **Режим “оффлайн”**

Если контроллер не может выйти на связь с сервером, то отпуск происходит в “оффлайн” режиме, т.е. без проверки платежеспособности. Данные сохраняются в журнал контроллера и передаются “пачкой” при появлении связи.Т.о. у пользователей с предоплаченным тарифом есть возможность “уйти в минус”.

1. **Пополнение лицевого счета**

* С расчетного счета юридического лица
* Через банковский платеж (физическое лицо)
* С банковской карты (в т.ч. автоплатеж)
* Через кассу организации (наличными или банковской картой)
* Через терминал самообслуживания (наличными или банковской картой)

1. **Блокировка пользователя (добавляется в “черный список” контроллера)**

* Если л/с пользователя предоплаченного тарифа имеет нулевой или отрицательный баланс
* Если пользователь постоплатного тарифа не оплатил долг в положенное время
* Если баланс л/с пользователя тарифов “фиксированный” и “вход” меньше суммы фиксированного платежа
* Автоматическая блокировка при подозрении на мошенничество (см. п.11)
* Ручная блокировка владельцем л/с
* Ручная блокировка оператором системы.

1. **Личный кабинет (владельца лицевого счета)**

* Личный кабинет должен быть в виде веб-интерфейса
* История пополнений л/с
* История списаний (по всем идентификаторам привязанным к л/с)
* Отображаются идентификаторы привязанные к л/с
* Настройка индивидуальных ограничений каждого пользователя (идентификатора)
* Возможность сформировать счет на оплату
* Возможность онлайн оплаты (пополнения л/с)
* Настройка уведомлений
* “Обратная связь”.

1. **Возможности для оператора системы (АРМ)**

* АРМ должен быть в виде веб-интерфейса
* Настройка системы
* Отчеты и статистика (финансы, отпущенные ресурсы и т.п.)
* Разграничение прав пользователей (сотрудники оператора системы)
* Система тревог
* Импорт списков
* Экспорт БД и отчетов
* Ручное пополнение баланса л/с
* Настройка ограничений вместо владельца л/с
* Отправка сообщений (sms, email) пользователям
* Выставление счетов.

1. **Дополнительные возможности**

* Гибкая настройка системы лояльности (скидки, накопительные баллы)
* Автоматическое выставление счетов (по email)
* Автоматическое напоминание пользователям о критическом балансе (sms, email)
* Автоматическое начисление пени
* Автоматические сообщения пользователям (sms, email)
* Интеграция с 1С
* Интеграция с ОФД и “Облачными кассами”
* Интеграция с СКУД (в т.ч. шлагбаумами).

1. **Варианты взаимодействия контроллера с периферийными устройствами и системами**

**9.1. Варианты управления исполнительными устройствами (клапаны, насосы и т.п.)**

* Прямое управление - “открытый коллектор”;
* Управление через промежуточные устройства (устройства плавного пуска, реле и т.п.) - “открытый коллектор”/”сухой контакт”;
* Управление по протоколу ModBus.

**9.2. Варианты получения данных от приборов учета**

* Импульсный (прямое подключение к контроллеру);
* По протоколу ModBus.

**9.3. Варианты взаимодействия со сторонними системами КИПиА и АСУ**

* По протоколу ModBus.

1. **Минимальные требования к терминалу**

**10.1. Минимальные требования к контроллеру**

* Входы для: кнопок управления, подключения датчиков (“сухой контакт”), подключения приборов учета (счетчик импульсов), подключения считывателя карт, питания.
* Выходы для: подключения дисплея, управления исполнительными устройствами (см. п.12), управление моторизированным считывателем карт
* Связь: RS-485 (ModBus см. п.10), Ethernet, GSM (GPRS/3G/LTE)
* Программируемая логика работа (в т.ч. отработка внештатных ситуаций)
* Контроллер должен иметь возможность работать как режиме “сервер” (ожидая подключения “клиента”), так и в режиме “клиент” (самостоятельно подключаясь к “серверу”).

**10.2. Минимальные требования к корпусу**

* Уличное исполнение;
* Вандалоустойчивость;
* Система подогрева, должна обеспечивать работу до -50оС;
* Защита от осадков;
* Монтаж на бетонное основание в земле;
* Высота должна обеспечивать удобство работы с терминалом.

**10.3. Минимальные требования к интерфейсу**

* Наличие дисплея не менее 5”;
* Наличие бесконтактного считывателя карт;
* Наличие возможности подключения моторизированного считывателя карт;
* Наличие кнопок “старт” и “стоп”;
* Наличие возможности подключения устройства для связи с оператором;
* Наличие возможности подключения POS терминала для оплаты банковской картой;

**10.4. Функциональные требования**

* Терминал должен обеспечивать взаимодействие покупателя с системой платного отпуска воды (приема стоков);
* Покупатель должен получать инструкции и предупреждения, посредством вывода на дисплей текстовой информации на русском языке;
* Покупатель может управлять процессом, путем нажатия кнопок “старт” и “стоп”;
* На дисплее должен отображаться ход процесса отпуска услуги;
* Наличие возможности “изъятия” карты (в случае применения моторизированного считывателя) по команде контроллера;
* Наличие возможности голосовой связи с оператором (опция);
* Наличие блока бесперебойного питания (автономная работа терминала (с отключенной системой обогрева) не менее 15 минут).

1. **Мониторинг мошенничества**

**11.1. Общее описание мониторинга мошенничества**

* Обнаружение мошеннических операций до момента совершения авторизации;
* Выявление различных типов мошенничества, как в части эквайринга, так и в части эмиссии;
* Возможность осуществления мониторинга транзакционной активности;
* Немедленное ограничение активности фродовых или подозрительных карт/ЭК, за счет помещения в “черный список” (см. п.5);
* Блокировка точек совершения транзакций в режиме on-line.
* Проведение расследований мошеннических операций (построение сводных отчетов);
* Формирование предупреждений (Тревог) для аналитиков по настроенным событиям и формировать уведомления (E-mail) по заранее настроенным правилам.

**11.2. Настройка блокирующих и разрешающих листов**

Система должна обеспечивать возможность помещения любого атрибута операции в блокирующий или разрешающий лист. При наличии атрибутов пришедшей транзакции в разрешающем листе, транзакция должна признаваться легальной. При наличии атрибутов пришедшей транзакции в запрещающем листе, транзакция должна признаваться мошеннической.

**11.3. Настройка обработки транзакций**

Система должна предоставлять возможность задавать любую последовательность проверок под требования Заказчика:

* проверка по разрешающим листам;
* проверка по запрещающим листам.

1. **Системный мониторинг**

Системный мониторинг используется для отслеживания актуального состояния процессов системы, а также для рассылки оповещений по критическим событиям (тревогам). Система мониторинга позволяет:

* отслеживать статус Системы,
* управлять (останавливать, запускать) процессами Системы,
* останавливать и перезапускать всю Систему;
* настраивать оповещения по заданным событиям Системы указанным получателям посредством рассылки E-mail и SMS;
* отслеживать системные события, записываемые в лог журнала.

1. **Требования к программному обеспечению Системы**

**13.1. Требования к качеству программных средств, способам его обеспечения и контроля**

Система должна предоставлять возможность выбора необходимых методик и средств, предлагаемых базовым ПО и оборудованием.

Основные сценарии:

1) Использование отказоустойчивого кластер (active-passive) . Приложение исполняется на платформе, состояние которой контролируется ПО кластера. В случае недостаточности тех или иных ресурсов (объема памяти, производительности процессора) или недоступности сервисов, прикладная задача (по возможности корректно) останавливается на существующем узле и перезагружается на другом, имеющемся в распоряжении кластерного софта. Тем самым обеспечивается доступность прикладной задачи и некий заданный уровень Quality of Service. Конкретное приложение в каждый конкретный момент времени исполняется на какой-то одной конкретной платформе (сервере).

2) Создание удаленных резервных центров, для реализации катастрофоустойчивого решения. Должна быть обеспечена совместимость с ОС Linux.

**13.2. Требования к техническому обеспечению Системы**

Общими требованиями к техническому обеспечению являются:

 – однородность, базирующаяся на единой платформе устройств с одинаковыми функциями;

 – высокая надежность и отказоустойчивость системообразующих элементов;

– быстродействие;

– масштабируемость системообразующих элементов;

– перспективность с возможностью модификации применяемых технологий без изменения архитектуры Системы.

Техническое оборудование должно обеспечивать выполнение указанных в настоящем документе функций и задач Системы.

**13.3. Требования к серверам**

Сервера БД и сервера приложений системы должны функционировать на оборудовании с архитектурой x86, x64. Конфигурация промышленных серверов должна быть определена в рамках предварительного этапа.

**13.4. Требования к рабочим станциям**

Пользовательское рабочее место иметь возможность быть развернуто на любой конфигурации рабочей станции, операционная система которой поддерживает работу веб-браузера. Браузер должен поддерживать Transport Layer Security (TLS v. 1.1, RFC5246), с использованием российских криптографических стандартов:  Mozilla / Firefox (версия 3.5 и выше);  Google Chrome (последние версии);  Microsoft Internet Explorer (начиная с версии 9.0).

**13.5. Требования к организационному обеспечению Системы**

Для организационного обеспечения эксплуатации Системы необходимо разработать эксплуатационную документацию и обучить технический персонал, а также разработать пользовательскую документацию и обучить ключевых пользователей системы.

Под составом эксплуатационной документации понимается перечень документов:

– Руководство администратора;

– Руководство пользователя;

Структура и функции подразделений, участвующих в функционировании Системы или обеспечивающих ее эксплуатацию, должны соответствовать составу ролевых задач, решаемых в Системе и выполняемых при этом функций.

1. **Требования к надежности**

**14.1. Состав и количественные значения показателей надежности для Системы в целом или ее подсистем**

Система должна относиться к обслуживаемым восстанавливаемым изделиям общего назначения многократного циклического применения.

Основными показателями надежности Системы устанавливаются:

 - среднее время наработки на отказ;

- среднее время восстановления работоспособности.

Оборудование, выбранное для технических средств, должно отвечать требованиям ГОСТ 24.701 и иметь следующие значения показателей надежности:

– среднее время наработки на отказ в целом – не менее 250 часов;

– среднее время восстановления при отказах и сбоях ПО – не более 30 минут;

 – коэффициент готовности в целом – 0,998-0,999.

Надежность сохранения данных должна осуществляется за счет обеспечения баз данных техническими и программными средствами резервного копирования и восстановления в случае возникновения внештатных ситуаций.

Система должна обеспечивать работоспособность системы в рамках Проекта в режиме 24х7 с коэффициентом отказоустойчивости 99,9%.

Система должна поддерживать необходимые технологии для реализации доступности на уровне 99.9% (три девятки).

В системе должно быть обеспечено профилирование нагрузки. Процессы реального времени, такие как маршрутизация операций и авторизация, отделяются от процессов обработки данных. Сбой на уровне клиентского места не должен приводить к сбоям на серверах и остальных клиентах

В системе должны присутствовать встроенные средства мониторинга работоспособности внутренних процессов и модулей, авторизационных каналов, средства уведомления при сбоях в работе.

**14.2. Перечень аварийных ситуаций, по которым должны быть регламентированы требования к надежности, и значения соответствующих показателей**

Система должна сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих ситуаций:

– при сбоях в системе электроснабжения аппаратной части, приводящих к перезагрузке операционной системы (ОС), восстановление программы должно происходить после перезапуска ОС, СУБД и сервера приложений;

– при ошибках в работе аппаратных средств (кроме носителей данных и программ) восстановление функций системы возлагается на ОС;

– при ошибках, связанных с программным обеспечением (ОС и драйверы устройств), восстановление работоспособности возлагается на ОС;

– для защиты аппаратуры от бросков напряжения и коммутационных помех должны применяться устройства бесперебойного питания.

Аварийные ситуации, по которым регламентируются требования к показателям надежности Системы:

– отказ Системы в результате сбоя или выхода из строя технических средств, входящих в ее состав;

– отказ Системы в результате сбоя общего или специального ПО, входящих в ее состав;

– сбой или отказ Системы в результате ошибки в прикладном ПО; – отказ единичного канала связи Системы;

– сбой или отказ Системы в результате ошибки в работе персонала.

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

Для нормальной эксплуатации разрабатываемой системы должно быть обеспечено бесперебойное питание комплекса терминала, серверов.

Периодическое техническое обслуживание используемых технических средств должно проводиться в соответствии с графиком планово-предупредительного ремонта.

Периодическое техническое обслуживание и тестирование технических средств должны включать в себя обслуживание и тестирование всех используемых средств, включая рабочие станции, серверы, кабельные системы и сетевое оборудование, устройства бесперебойного питания, терминалы и контроллеры. В процессе проведения периодического технического обслуживания должны проводиться внешний и внутренний осмотр и чистка технических средств, проверка контактных соединений, проверка параметров настроек работоспособности технических средств и тестирование их взаимодействия. На основании результатов тестирования технических средств должны проводиться анализ причин возникновения обнаруженных дефектов и приниматься меры по их ликвидации. Восстановление работоспособности технических средств должно проводиться в соответствии с инструкциями разработчика и поставщика технических средств и документами по восстановлению работоспособности технических средств и завершаться проведением их тестирования. При вводе системы в опытную эксплуатацию должен быть разработан план выполнения резервного копирования программного обеспечения и обрабатываемой информации. Во время эксплуатации системы персонал, ответственный за эксплуатацию системы должен выполнять разработанный план.

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

Каждый субъект доступа Системы должен иметь уникальный идентификатор в системе.

Каждый субъект доступа Системы должен использовать аутентификационную информацию при каждом сеансе работы. Ни один субъект доступа Системы не должен иметь возможности осуществлять доступ в обход подсистемы обеспечения безопасности (аутентификация пользователя на системном уровне осуществляется средствами ОС и СУБД). Данная подсистема должна предусматривать:  идентификацию и аутентификацию всех субъектов доступа;  использование сквозной аутентификации, т.е. в журнальных файлах СУБД должны регистрироваться учетные данные реальных пользователей.

Встраивание аутентификационной информации в АС или ее элементы запрещается. Элементы аутентификации (пароли) не должны передаваться по каналам связи и храниться в памяти Системы.

Взаимодействие элементов сервера приложений и сервера БД должно происходить посредством программно-аппаратных решений, не имеющих физического подключения к общедоступным коммуникационным каналам.

Все данные передаваемые и получаемые в процессе работы через интерфейс пользователя автоматически должны шифроваться без дополнительных программных или аппаратных средств

Система должна обеспечивать доступ только для зарегистрированных пользователей, прошедших процедуру аутентификации и авторизации.

Защита информации должна обеспечиваться:  необходимостью ввода пароля на рабочем месте;  разграничением доступа пользователей;  запрещением несанкционированного доступа для изменений ПО, НСИ.

При создании и функционировании информационных баз необходимо проводить ряд контролирующих действий с целью исключения ввода и последующей обработки ошибочных данных. Должны быть обеспечены виды контроля:  контроль заполнения обязательных полей и НСИ;  контроль диапазона вводимых значений;  контроль логических соответствий заполнения полей и справочников.

Все модули системы должны иметь полное логирование активностей, шифрование необходимых данных, разграничение доступов на всех уровнях.

Система должна позволять логировать все события:  действия пользователей через любой интерфейс;  выполнение операций в БД;  выполнение операция на серверах приложений;  выполнение операций на системах передачи данных; Логирование должно фиксировать время действия, объект, субъект, действие, результат; Должна быть возможность изменять уровень логирования; Время хранения лог-файлов должно быть настраиваемым, но не менее 3 месяцев; Должен существовать интерфейс просмотра лог-файлов, обеспечивающий задания различных фильтров для отображения необходимой информации из лог-файлов.

1. **Требования по сохранности информации**

Система должна обеспечивать восстановление при сбоях и авариях технических средств, включая полное восстановление данных и связей между ними. Сохранность информации при авариях в процессе эксплуатации должна обеспечиваться резервным копированием данных. Сохранность информации должна обеспечиваться архивированием и дублированием БД на разных уровнях.

Точные параметры необходимой мощности устройства бесперебойного питания, а также иные требования к помещению для размещения серверов системы должны быть уточнены на основе информации производителя сервера о технических условиях эксплуатации конкретной модели сервера.

**18.** **Требования к сдаче программного продукта**

В результате разработки программного комплекса исполнитель передаёт заказчику полностью настроенную и рабочую систему, производит обучение ответственного специалиста Заказчика по работе в программном комплексе.

После выполнения всех работ исполнителем заказчик осуществляет тестирование программного комплекса в течение 60 дней со дня сдачи программного комплекса.

Перед сдачей программного комплекса Исполнитель передает Заказчику всю исполнительную документацию и исходный код программного обеспечения(проект) по проекту.

Все права на программный продукт (программное обеспечение) после подписания акта приема-передачи принадлежат Заказчику.