



Техническое задание

350072, г. Краснодар,
ул. Солнечная, 15/5
тел/факс: (861) 210-98-10
www.magnit-info.ru
info@magnit.ru

Касса самообслуживания с возможностью установки на прилавке для МК

Регистрационный номер из 1С: № ТЗ_ОТС_11/25 от 04.02.2025

Срок действия: 1 год.

Сокращения:

КСО - Касса самообслуживания;
ИБП - Источник бесперебойного питания;
АКБ - Аккумуляторная батарея;
AD - Active Directory;
ИС – Информационная система;
ОС – Операционная система;
ПО – Программное обеспечение;
УЧ – Учетная запись;
БД – База данных;

Функциональное предназначение: автоматизация процесса самообслуживания оплаты товара.
Самостоятельное сканирование товаров, сверка списка покупок и оплата товара.

Объекты, на которых используется оборудование:

Магазин Магнит (ММ)	Нет
Магнит Косметик (МК)	Да
Магнит Аптека	Нет
Магнит Семейный	Нет
Магазин Опт	Нет
Распределительный центр	Нет
Автотранспортное предприятие	Нет
Офисы (ГК, Округа, Филиалы)	Нет
Магнит киоск	Нет

Требования:

1. Общие параметры
1.1. С возможностью приема безналичных платежей;
1.2. Наличие сенсорного экрана;
1.3. Наличие встроенного 2D сканера ШК
1.4. С возможностью установки на прилавке;
1.5. Наличие возможности монтажа терминала безналичной оплаты (PIN PAD);
1.6. Диапазон рабочих температур от +15 до 45 градусов Цельсия;
1.7. Поддержка интеграции с кассовыми терминалами на базе ОС Linux.
1.8. Наличие в комплекте ИБП: <ul style="list-style-type: none">• Время автономной работы от АКБ – не менее 15 минут при нагрузке 120 Вт.• Выходные соединения с питанием от батарей – IEC 320 C13 с функционалом «батарея + стабилизатор».

• Не менее одного свободного порта после подключения КСО.
1.9. Диапазон входного напряжения, не менее В - 180-260 В.
1.10. Поддержка сетей: LAN от уровня 100BASE-T и выше;
1.11. Интерфейс взаимодействия КСО с POS: LAN Ethernet.
1.12. Наличие акустомагнитного, бесконтактного деактиватора (рабочая частота 58 кГц) обеспечивающего 100% деактивацию акустомагнитной этикетки на расстоянии не менее 8 см от сканера ШК. Размещение антенны деактивации – скрытая в сканер ШК.
1.13. Возможность последующей установки камеры для фото/видео фиксации лица покупателя. <ul style="list-style-type: none"> • Разрешение камеры не менее 1280x720, автофокус, угол обзора 60 градусов
2. Сканирующий модуль
2.1. Считываемые коды для стационарного сканера: линейные одномерные (EAN-13, EAN13+5, EAN-8, Code 39, Code128, GS1 DataBar, GS1 Expanded, GS1 Stacked, GS1 Expanded Stacked, GS1-128), двумерные штрихкоды (QR Code, PDF417 (алкогольная АМ), DataMatrix Code (табак, алкогольная АМ нового формата, мин 4x4 мм) в условиях искусственного освещения.
2.2. Уверенное распознавание 10 любых ШК (табак, алкоголь, обувь и т. д.) за 10 секунд в условиях минимального размера ШК и искусственного освещения.
2.3. Возможность сканирования кодов с экрана смартфона.
2.4. Дальность считывания: вертикальный модуль – от 0 до 221 мм
2.5. Ширина сканирования — от 4 мм.
2.6. Наличие защитного стекла сканера, устойчивого к механическим воздействиям;
2.7. Защита от пыли и влаги - не менее IP-54;
2.8. Должно быть предоставлено полное описание протокола управления устройством, для всех режимов, поддерживаемых устройством, в том числе по всем пунктам ниже (на русском или английском языке): <ul style="list-style-type: none"> • описание параметров с их ограничениями (тип параметра, список возможных значений, значение по умолчанию, min / max значения). • чтение / запись всех параметров. • перепрошивка устройства. • переключение между всеми доступными для обслуживания режимами.
2.9. В USB HID режиме работы устройство должно уметь отдавать следующую информацию без смены режимов: <ul style="list-style-type: none"> • серийный номер. • название и модель. • версию прошивки (опционально).
. Монитор покупателя.
3.1. Сенсорный, емкостной с поддержкой протокола USB mouse либо наличием открытого драйвера для ядра Linux.
3.2. Диагональ от 15 дюймов;
3.3. Контрастность - не менее 500:1;
3.4. Время отклика - не более 30 мс;
3.5. Ориентация экрана: строго вертикальная.
3.6. Соотношение сторон экрана: строго 9:16.
3.7. Разрешение экрана: не менее 1920x1080 пикселей
3.8. Тип ЖК-матрицы – IPS, *VA.
3.9. Аудио система голосового сопровождения.
4. Система оповещения.
4.1. Лампа индикации - трехцветная;
4.2. Индикация аварийной ситуации;
5. Пин-пад
5.1. Пин-пад должен крепиться на кронштейн (стойку) таким образом, чтобы покупателю были видны все клавиши; В комплекте с кронштейном должен присутствовать крепёж (болты, шайбы, гайки и т.д.) под все используемые в компании модели пинпадов.

5.2. Список пин-падов, эксплуатируемых в компании:

- Терминал безналичной оплаты ingenico iPP320;
- Терминал безналичной оплаты ingenico iPP350.
- Терминал безналичной оплаты Castles vega 3000
- Терминал безналичной оплаты PAX SP30.
- Терминал безналичной оплаты PAX Q25.
- Терминал безналичной оплаты PAX S300.

6. Фискальный регистратор (ФР)

6.1. Расположение фискального регистратора снаружи или внутри корпуса КСО, с надежной фиксацией, без препятствий для печати и отрыва чека.

6.2. Список ФР, эксплуатируемых в компании:

	Модель	Габариты оборудования, мм
	Retail-01ФМ	152x220x150,5
	АТОЛ FPrint-22ПТК	140x140x200
	АТОЛ 27Ф	156x200x150
	Атол 22в2Ф	200x156x150

7. Мониторинг КСО, который позволит:

7.1. Определить состояние основных компонентов (Системный блок, сканер);

7.2. Определить заводской номер КСО;

7.3. Обязательно наличие возможности удаленного получения:

- модели
- версии ПО
- серийного номера
- неработоспособность КСО (информирование о поломке в соответствии с кодом ошибки)
- Наличие собственной системы мониторинга, ПО для централизованного мониторинга работы КСО или готовый SDK мониторинга для интеграции.

8. Требования к информационной безопасности.

8.1. Все используемые дистрибутивы для работы ИС должны быть последней стабильной версии, поддерживаться вендором и не содержать известные уязвимости.

8.2. Используются стойкие защищенные протоколы как на промежутке между ИС и пользователем, так и между ИС/серверами.

8.3. Реализовано ограничение доступа к конфигурационным файлам, содержащим конфиденциальную информацию, файлам закрытых ключей.

8.4. Взаимодействие с другими ИС (поток данных) должно осуществляться с использованием сервисных доменных УЗ.

8.5. На всех пользовательских и служебных интерфейсах ИС должна присутствовать аутентификация, а механизм выполнения её не должен передавать данные в открытом виде.

8.6. Отключены неиспользуемые службы, веб-сайты и веб-приложения по умолчанию (Default Web Site).

8.7. На серверах отсутствуют тестовые данные, данные других серверов и сервисов, а также другие данные (к примеру SQL-дампы, дебаг логи), не относящиеся к ИС.

8.8. Сервис должен работать под ограниченной УЗ с набором минимальных прав, необходимых для работы.

8.9. Должно присутствовать разграничение прав доступа, в том числе и для административных действий.

8.10. Сервис поддерживает работу через прокси-сервер с авторизацией для доступа к ресурсам в интернете.

8.11. Сервис имеет систему журналирования событий в стандартизованных видах, позволяющую осуществлять анализ работы сервиса, действия пользователей, выявлять отклонения и нарушения, проводить аудит использования сервиса пользователями, а также администраторами.

8.12. Система ведения журналов имеет возможность передачи сообщений стороннему серверу хранения журналов стандартизованным способом.

8.13. Система журналирования не записывает в журналы пароли учетных данных пользователей и другую конфиденциальную информацию.
8.14. Система журналирования имеет возможность регулировать "глубину" журнала, при необходимости включать расширенные журналы аудита.
8.15. Система журналирования имеет возможность архивировать журналы и удалять журналы по заданному сроку устаревания.
8.16. Сервис должен быть независим от обновлений ОС и прикладного ПО, при обновлениях сервис должен продолжать работать, работа используемых агентов не должна препятствовать корректной работе сервиса.
8.17. При работе сервиса с СУБД - доступ в нее должен осуществляться под выделенной УЗ с минимальными правами, необходимых для работы.
8.18. Запрещается использование служебной административной УЗ (sa,postgres,sysdba и др.) для подключения к СУБД сервисами ИС.
8.19. При обработке конфиденциальной информации средства защиты информации должны соответствовать уровню информационной безопасности ИС для конфиденциальной информации.
8.20. ИС для корпоративного использования должна поддерживать доменную аутентификацию с разграничением прав доступа пользователей по доменным группам.
8.21. ИС должна проверять наличие УЗ в домене, совпадение пароля пользователя, состояние блокировки УЗ, требование смены пароля и других ограничивающих атрибутов.
8.22. Сервис контролирует сложность пароля при его изменении, запрещая устанавливать пользователям простейшие пароли.
8.23. Сервис предотвращает попытки подбора пароля, устанавливая увеличивающийся таймаут последующей авторизации при неверном вводе пароля более 5 раз.
8.24. Сервис автоматически завершает сеанс пользователя при бездействии (тайм-аут сессии).
8.25. ОС обновлена до актуального состояния, может быть настроено автоматическое периодическое обновление с корпоративного сервера обновлений.
8.26. На сервере установлены и запущены только те службы и открыты сетевые порты, которые необходимы для работы.
8.27. Отсутствует анонимный доступ к файлам и файловой системе сервера.
8.28. На ОС может быть установлен корпоративный антивирус с актуальными обновлениями и подключенный к корпоративному серверу обновлений.
8.29. Не используемые интерфейсы должны быть по умолчанию выключены или должна быть возможность отключать их самостоятельно.
8.29.1. При наличии интерфейса Wi-Fi, должна быть возможность работы по защищенным протоколам (WPA2-Enterprise/WPA3-Enterprise и протоколы аутентификации EAP-TLS, PEAP). Либо возможность его отключения
8.30. Конструкция КСО должна исключать беспрепятственный доступ посторонних лиц к кнопкам питания (включения/выключения/перезагрузки) устройства. Кнопка питания должна быть визуально незаметна, а также находиться в труднодоступном месте. Пример — расположение за запирающим механизмом (замком) в основном корпусе КСО.
8.31. На КСО должна быть ограничена возможность доступа к управлению ОС КСО со стороны покупателей.
9. Условия гарантии – Не менее 24 месяцев.
10. Центральный компьютер: <ul style="list-style-type: none"> • Возможность установки ОС Linux с поддержкой протокола UEFI, а также ОС Debian Desktop актуальной версии • Процессорная архитектура x86_64. Не менее Intel Celeron J6412. • ОЗУ не менее 8 ГБ с возможностью расширения путем установки доп. модуля памяти. • ПЗУ объёмом не менее 120 GB. • Видеоадаптер OpenGL с поддержкой версии 4.5, OpenCL с поддержкой версии 3.0, Vulkan с поддержкой версии 1.2. • Подключение периферии по USB.

<ul style="list-style-type: none"> Звуковая система, поддерживаемая актуальными версиями свободных дистрибутивов Linux. В BIOS должна присутствовать информация о вендоре, модели КСО, серийном номере КСО (как на шильдике). Пример записи данной информации в BIOS AMIDEEFIx64.EFI - SM "VendorName" -SP "ModelName" -SS "SN"
11. Поддержка возможности загрузки по сети (PXE или аналог).
<p>12. Драйвера для управления устройствами:</p> <p>12.1. Готовность предоставить драйвера/SDK (и их исходники на C/C++) для управления устройствами (сканера, весов, сканер весов, светофора и других устройств) и их перепрошивки (при наличии возможности) для актуального дистрибутива OS Linux сборки Магнит. В случае отсутствия драйверов (и их исходников на C/C++) предоставить описание протоколов для управления устройствами для всех режимов, поддерживаемых устройствами, в том числе по всем пунктам ниже (на русском или английском языке):</p> <ul style="list-style-type: none"> описание параметров с их ограничениями (тип параметра, список возможных значений, значение по умолчанию, min / max значения); чтение / запись всех параметров; перепрошивка устройства (при наличии возможности); переключение между всеми доступными для обслуживания режимами. <p>12.2. Готовность предоставить примеры использования драйверов/SDK для C/C++ для сканера, весов, сканер весов, светофора и других устройств. Примеры должны компилироваться и работать на актуальном дистрибутиве OS Linux сборки Магнит.</p> <p>12.3. Готовность предоставить сервисные утилиты для оборудования (мониторинги, тестовые и т. д.) для актуального дистрибутива OS Linux сборки Магнит.</p> <p>12.4. Готовность доработать драйвера для актуального дистрибутива OS Linux сборки Магнит.</p> <p>12.5. Готовность выделить специалиста по настройке драйверов/SDK на актуальном дистрибутиве OS Linux сборки Магнит.</p> <p>Требования к бинарным библиотекам будут предоставлены по запросу.</p>

Ответственные за согласования

Согласование	ФИО	Пункты
Отдел учета и тестирования оборудования	Цой В. Ю.	все
Управление по ИТ-сопровождению регионов	Шаранов Д.С.	п. 1.8, 1.9, 2.6, 2.7, 5, 6, 9.
Отдел сопровождения оборудования продаж	Ростовский-Сериков К. С.	п. 1.7–1.11, 2, 5-7.
Группа противодействия мошенничеству	Лалаев О. В.	п. 8
Отдел сопровождения категории ИТ оборудование\ПО и персонала	Власюк И. А.	Все
Команда развития КСО	Ефремов А. В.	п. 1.13, 2.8, 2.9, 3.1, 10-12
Направление системного администрирования	Голубев А. О.	11
Направление по проектам	Салихова Р. П.	все

Управление по развитию внутренних продуктов	Устинов Е. И.	все
Направление по проектам	Шафорост Е. С.	все