**1.**Предположительно, у заказчика есть несколько информационных систем, которые обеспечивают функциональность его онлайн магазина полного цикла и позволяют ему масштабировать бизнес. Вот описание этих систем и обмена данными между ними в удобной и понятной форме:

1. Веб-сайт заказа товаров:

- Интерфейс для размещения заказов клиентами, включая выбор продуктов, указание доставочных адресов и способов оплаты.

- Отправка заказов на Backend для дальнейшей обработки.

2. CRM:

- Принимает заказы с веб-сайта, выгружает их для обработки отделом продаж.

- Хранит информацию о клиентах, заказах и контактной информации.

3. Backend обработки заказов:

- Получает заказы от CRM и отдела продаж, обрабатывая их для дальнейшего выполнения.

- Координирует работу отдела продаж, отдела закупок, склада и доставки.

4. Отдел продаж:

- Обрабатывает заказы, полученные с сайта и по телефону.

- Оформляет выполненные заказы и передает их в Backend для обработки оплаты и доставки.

5. Отдел закупок:

- Отвечает за закупку товаров под заказ и для хранения на складе.

- Информирует склад о закупках и новом поступлении товаров.

6. Склад:

- Хранение товаров, закупленных отделом закупок.

- Поддерживает свою логистику для обработки поступающих и исходящих товаров.

7. Система доставки:

- Отправляет информацию о выполненных заказах и доставочных адресах курьерам для обеспечения эффективной доставки.

- Получает от курьеров данные о маршрутах доставки, отметках поставок и оплате.

8. Приложение для курьеров:

- Предоставляет курьерам информацию о маршруте доставки и деталях заказов.

- Позволяет курьерам отмечать товары, отданные клиентам, принимать оплату и пробивать чеки.

9. Система оплаты:

- Обрабатывает онлайн-оплату заказов с сайта.

- Поддерживает оплату наличными при доставке заказа.

Обмен данных между информационными системами:

- Веб-сайт заказа товаров отправляет заказы в CRM и Backend для дальнейшей обработки.

- CRM передает заказы отделу продаж и информацию о клиентах в Backend для синхронизации данных.

- Backend взаимодействует с отделом продаж, отделом закупок, складом, системой доставки и системой оплаты для координации и обмена информации.

- Отдел продаж передает выполненные заказы в Backend для обработки оплаты и доставки.

- Отдел закупок информирует склад о новом поступлении товаров.

- Склад передает информацию о поступлении товаров на Backend, чтобы обновить доступные запасы.

- Backend передает информацию о выполненных заказах и доставочных адресах в систему доставки для планирования маршрутов и уведомления курьеров о необходимых доставках.

- Курьерское приложение взаимодействует с системой доставки для получения информации о маршрутах доставки, отметках поставок и оплате.

- Система доставки передает информацию о выполненных заказах и оплате обратно в Backend, чтобы обновить статус доставки и обработать оплату.

- Система оплаты взаимодействует с веб-сайтом заказа товаров для проведения онлайн-оплаты и с Backend для обработки наличных платежей при доставке.

- Backend, в свою очередь, связывается с системой оплаты для проверки и подтверждения платежей, а также передает информацию о статусе оплаты в CRM и другие соответствующие системы для обновления данных о заказе и клиентах.

Это лишь предположения о наличии информационных систем и обмене данными на основе представленной информации о бизнесе. Фактические системы и процессы могут отличаться в реальной ситуации заказчика.

**2.**Функциональные требования к информационным системам магазина могут включать:

1. Управление заказами:

- Возможность размещать заказы через веб-сайт.

- Отслеживание статуса заказа от размещения до доставки.

- Генерация уведомлений о статусе заказа для клиентов.

2. Управление клиентскими данными:

- Создание и обновление профилей клиентов.

- Хранение и отображение истории заказов клиентов.

- Возможность изменения адреса доставки и контактной информации.

3. Управление товарным ассортиментом:

- Добавление, обновление и удаление товаров.

- Управление описаниями, изображениями, ценами и наличием товаров.

- Категоризация товаров для удобства навигации клиентов по сайту или приложению.

4. Управление складскими запасами:

- Отслеживание доступных запасов товаров на складе.

- Генерация уведомлений о необходимости пополнения запасов.

- Связь с отделом закупок для автоматического заказа недостающих товаров.

5. Управление доставкой:

- Планирование доставок и определение оптимальных маршрутов для курьеров.

- Уведомления клиентов об ожидаемом времени доставки.

- Отслеживание статуса доставки и подтверждение доставки клиентами.

Нефункциональные требования могут включать:

1. Производительность:

- Быстрый и отзывчивый интерфейс для пользователей.

- Обработка большого числа одновременных запросов с минимальной задержкой.

2. Безопасность:

- Защита данных клиентов и их конфиденциальности.

- Защита от несанкционированного доступа и взлома.

3. Масштабируемость:

- Возможность расширения системы для поддержки большого числа товаров, клиентов и заказов.

4. Надежность:

- Непрерывная работа системы без сбоев и вылетов.

- Резервное копирование данных и восстановление в случае сбоев.

Для удовлетворения требований могут потребоваться следующие доработки текущих информационных систем:

1. Внедрение онлайн-оплаты на веб-сайте и интеграция с системой оплаты для обработки онлайн-платежей.

2. Расширение функциональности CRM и Backend для обработки заказов, передачи информации отделам продаж и закупок, а также синхронизации данных с веб-сайтом.

3. Интеграция системы доставки с Backend для обмена информацией о заказах, статусе доставки и оплате.

4. Улучшение интерфейса и производительности информационных систем для удобства пользователей и обеспечения отзывчивости в системе.

5. Обеспечение безопасности данных и внедрение механизмов защиты, таких как шифрование данных и двухфакторная аутентификация

7. Мониторинг и обнаружение инцидентов безопасности: Реализация системы мониторинга и обнаружения инцидентов безопасности поможет своевременно обнаруживать необычную активность или попытки несанкционированного доступа. Использование специализированных инструментов и технологий, таких как системы обнаружения вторжений (IDS) и системы информационной безопасности (SIEM), поможет сканировать и анализировать логи и события в режиме реального времени, с целью выявления потенциальных угроз.

8. Управление рисками и оценка уязвимостей: Проведение регулярной оценки уязвимостей и управление рисками помогут выявить и устранить слабые места в сети и информационных системах. Критический анализ системы, сканирование на наличие уязвимостей и план действий по их устранению позволят улучшить общую безопасность.

9. Четкие политики безопасности и согласование: Разработка и использование четких политик безопасности, которые определяют стандарты и процедуры обеспечения безопасности, является важным шагом. Политики должны быть согласованы с регулирующими органами и установленными стандартами безопасности, чтобы гарантировать соответствие и минимизацию рисков.

10. Внутренний контроль и авторизация: Внедрение механизмов внутреннего контроля и авторизации помогает ограничить доступ к критическим системам и данным только необходимым сотрудникам. Уровень доступа должен быть в соответствии с ролью и обязанностями каждого пользователя, с минимальными привилегиями, необходимыми для выполнения конкретных задач.

11. Внешний аудит безопасности: Проведение регулярных внешних аудитов безопасности позволяет получить независимую оценку системы и идентифицировать потенциальные уязвимости или слабые места. Аудит безопасности должен проводиться профессиональными фирмами, имеющими опыт в области информационной безопасности.

12. Резилиентность и планы реагирования на инциденты: Разработка планов реагирования на инциденты безопасности поможет обеспечить эффективное реагирование на возможные нарушения безопасности. Эти планы должны включать в себя процедуры для быстрого и эффективного восстановления после инцидента, коммуникацию с заинтересованными сторонами и сдержанный подход к восстановлению нормальной работы.

Внедрение всех вышеуказанных мер поможет создать надежную и устойчивую систему защиты данных, обес

13. Обучение и осведомленность сотрудников о безопасности: Одним из важнейших моментов в обеспечении безопасности информации является обучение и осведомленность сотрудников. Необходимо проводить регулярные обучающие программы, где сотрудники ознакамливаются с правилами безопасного обращения с данными, угрозами информационной безопасности, а также получают инструкции по распознаванию и предотвращению атак.

14. Физическая безопасность: Помимо мер информационной безопасности, важно также уделять внимание физической безопасности. Ограничение доступа к серверным помещениям, контроль доступа к критическим оборудованиям, установка физических барьеров и систем видеонаблюдения - все это меры, направленные на предотвращение физического вторжения и несанкционированного доступа к системам.

15. Регулярное резервное копирование и восстановление: Регулярное создание резервных копий данных и их надежное хранение помогает обеспечить возможность восстановления информации в случае инцидента. Необходимо установить процедуры резервного копирования, проверять работоспособность резервных копий и проводить регулярные тесты восстановления, чтобы быть готовым к непредвиденным сбоям или атакам.

16. Обновление и патчи безопасности: Систематическое обновление программного обеспечения и применение патчей безопасности помогают заполнять известные уязвимости и предотвращать атаки, связанные с ними. Регулярный мониторинг обновлений программного обеспечения и реагирование на уязвимости помогут обеспечить защиту системы от новых угроз.

17. Сотрудничество с внешними организациями: Важно устанавливать партнерские отношения с внешними организациями, специализирующимися на обеспечении информационной безопасности. Консультации с экспертами и сотрудничество с другими компаниями позволят получить доступ к передовым методам и рекомендациям по обеспечению безопасности информации.

18. Систематическое испытание и улучшение безопасности: Безопасность - это непрерывный процесс, который требует постоянного испытания и улучшения. Проведение пенетрационного тестирования, аудитов безопасности и анализа угроз поможет идентифицировать слабые места и принимать меры для их устранения, а также обновления стратегий безопасности.

Важно помнить, что информационная безопасность является постоянным процессом, требующим постоянного внимания и обновления. Непрерывная инновация в сфере информационных технологий может привести к появлению новых угроз и методов атак. Поэтому организации должны оставаться внимательными и готовыми к изменениям, постоянно совершенствуя свои методы защиты информации.

Кроме того, необходимо уделять внимание юридическим аспектам информационной безопасности. Установление соответствующих политик и процедур, а также соблюдение законодательных требований и регуляций, помогут организации соблюдать принятые стандарты безопасности и предотвращать правовые последствия.

Наконец, важно понимать, что информационная безопасность должна стать частью корпоративной культуры организации. Сотрудники должны осознавать свою ответственность за безопасность данных и информации, быть вовлеченными в процессы обучения и осведомленности, а также принимать активное участие в обеспечении безопасности в своей рабочей среде.

В итоге, реализация этих мер поможет организации обеспечить надежную защиту своей информации, минимизировать риски инцидентов и сохранить доверие своих клиентов и партнеров. Также регулярное обновление и применение передовых методов защиты информации поможет организации быть на шаг впереди потенциальных угроз и обеспечить непрерывную безопасность в быстро меняющемся информационном мире.

**3.**Схемы:

<https://app.diagrams.net/#G1ETK-NT0-86FmfUjXQN8VUMUCL0ILPLDI>

**4.**Дополнение:

Исключительные ситуации:

1. Если товар отсутствует на складе:

[Проверка наличия товара на складе] -> [Закупка товара] -> [Хранение на складе] -> ...

2. Если доставка не может быть выполнена:

[Подготовка к доставке] -> [Проверка возможности доставки] -> [Информирование клиента о задержке доставки] -> ...

3. Если клиент отказывается от заказа:

[Обработка заказа отделом продаж] -> [Отказ клиента от заказа] -> [Возврат товара на склад] -> [Возврат средств клиенту] -> [Завершение заказа]

4. Исключительные ситуации с оплатой:

[Оплата заказа] -> [Проверка метода оплаты и суммы] -> [Неправильный метод оплаты] -> [Обратная связь с клиентом] -> ...