16. Методология

Разработка

Единственно приемлемым решением при выборе методологии к текущему проекту, в условиях ограниченного времени на реализацию проекта, для нас является манифест разработки программного обеспечения «**Agile Manifesto**». Мы не можем руководствоваться классическим подходом каскадной модели разработки программного обеспечения «**Waterfall**», где задачи выполняются поточно (последовательно), так как это приведет к неминуемому срыву сроков в условиях большого объема работ и малого времени на исполнение.

Принципы которые мы используем в рамках аналогичных проектов:

- работающий продукт в срок важнее идеального продукта, но с опозданием;
- рабочие группы самоорганизующиеся, это дает зачастую лучшие архитектурные и технические решения;
- поощряем непосредственное общение как наиболее практичный и эффективный способ обмена информацией;
- непрерывная интеграция, релизы выходят часто (от 1 дня до одной недели);
- парное программирование;
- мотивированный персонал, за соблюдение краткосрочных и долгосрочных целей финансовое поощрение и бонусы (дополнительный отпуск, привилегии и тд);
- параллельное выполнение множества задач, даже если задачи смежные и имеют прямую зависимость (достигается за счет согласований интерфейсов на ранней стадии разработки);
- запрет работы в выходные дни, как превентивная мера по эмоциональному выгоранию сотрудников при высокой интенсивности работ.

Для обеспечения соответствия требованиям безопасности приложения будут внедрены следующие меры:

- пользователи получают доступ к интерфейсу приложения, используя end-to-end защиту (**HTTPS**);
- проверка всех входных данных клиента, включая все параметры, URL-адреса, заголовки HTTP (например, **Cookie**, **User Agent**);
- проверка типа данных: (целое число, буква, цифра и т.д)
- проверка корректного синтаксиса и ограничение длины данных;
- фильтрация специальных символов, таких как: <> "'% () & + \ \' \";
- пароли доступа между модулями приложения шифруются в файлах конфигурации;
- учетные данные доступа не передаются в незашифрованном виде между компонентами системы;
- срок жизни сессий имеет конечное фиксированное значение;
- логирование (даты, времени, IP-адреса), которое доступно для анализа системным администратором: успешная/неуспешная аутентификация, запросов к базе данных;
- учетные данные доступа пользователя к приложениям являются уникальными в системе и могут создаваться и управляться только системными администраторами;
- пароли доступа к приложениям шифруются криптографическим алгоритмом **sha256** с примесью соли (добавлению секретного ключа приложения);
- каждый пользователь имеет свой уровень доступа к данным и разделам, и приложение предоставляет/запрещает операции, которые относятся/не относятся к конкретным

действиям пользователя, и разрешать или запрещать операцию на основе конфиденциальной политики;
- в рамках обучающей программы сотрудникам исполкома будут представлены материалы об индивидуальной информационной безопасности;
- система содержит встроенный механизм отслеживания действий связанных с подбором паролей (метод грубой силы) к учетным данным и блокирует такие действия;
- доступ к системе, как на уровне пользователей, так и на уровне администратора, предшествует идентификация, аутентификация и авторизация доступа;
- работа с кодом систем после официального релиза на рабочих серверах будет осуществляться через сетевой протокол **ssh** с доступом по IP адресу головного офиса разработчиков;
- при проектирование и реализации проекта применяется модель «нулевого доверия», при котором происходит сегментация приложений по принципу «не доверяй и проверяй»;
- учетные данные для доступа пользователей будут предназначены исключительно для приложений и не будут использоваться для доступа или изменения конфигурации системы, а также для доступа к ресурсам, специфичным для привилегированных администраторов или пользователей (резервное копирование, доступ к файлам конфигурации, системные файлы, регистры), установки, обновления;
- при работе с документами будет реализована цифровая подпись, которая отвечает за подлинность текущего документа;
- все загруженные документы фиксируются в едином реестре.

Тестирование

Так как мы используем непрерывную интеграцию (частые релизы), это обязывает нас проводить регулярное тестирование написанного кода, что приводит к высокому качеству кода на всем промежутке разработок. Начиная с середины разработки проекта и до его окончательного релиза мы проводим следующие тесты:
- тестирование связку **UI** и бэкенда;
- тесты **API REST** на взаимодействия систем;
- модульное тестирование (юнит-тестирование);
- интеграционное тестирование;
- тестирование на проникновение (пентесты).

Документирование

Согласно пункту **NFR09** приложения 2 и 3, мы подготовим следующие документы:
- инструкция по развертыванию системы;
- инструкции администратора – всех ролей;
- план и алгоритм обучения администраторов системы.

Вся документация будет предоставлена в электронном и бумажном виде на русском языке. Согласно графику разработки начало подготовки документации назначено на середину августа 2019 года.

Обучение

Опираясь на пункты NFR10 - NFR20 мы подготовим подробную учебную программу, включая учебные материалы, для обучения целевых групп на русском языке в электронном и печатном виде. Учебные материалы будут представлены в виде учебников для каждой целевой группы. Учебная программа для администратора системы содержит в себе все компоненты и контрольные точки, которые используются для конфигурации, а также теоретические уроки и лабораторные.

Наша компания осуществляет подготовку как минимум одного сотрудника Исполнительного Комитета АТО Гагаузии в качестве администратора информационной системы.

В курс обучения входят курсы, связанные с технологиями, положенными в основу разработки информационной системы и описанием административных инструментов.

Целевые показатели обучения:

- объем изученных учебных материалов;
- тест на понимание функций и терминологии системы;
- тестирование работы с базовыми функциями системы;
- тестирование работы с отдельными функциями системы;
- тестирование работы с всеми функциями системы;
- количество реализованных задач с помощью системы в процессе обучении;
- количество реализованных задач с помощью системы после обучения;
- количество реализованных задач с помощью системы по истечению месяца после обучения.

В рамках обучения будут подготовлены несколько тренеров/координаторов для подготовки других пользовательских групп и практическое обучение специалистов целевой группы. Обучение направлено на подготовку навыков для будущего обслуживания системы.

Будет разработана учебная программа для формального обучения, включающая актуальные вопросы по обслуживанию портала и освещены аспекты организации технической поддержки в электронном и печатном виде.

Курс обучения включает в себя изучение терминологии, функционала, возможностей системы, взаимодействия между пользователями и ролями, работу с отчетностью, примеры практического применения использования информационной системы. Предусмотрены обучения в рамках подразделений, групп и в индивидуальном формате.

Обучение всех групп проводится на русском языке в течении 12 месяцев. Учебные материалы предоставляются на русском языке. Техническая поддержка портала в течении одного года, после его запуска. Консультационная поддержка администраторов в течении одного года, после запуска проекта.

Внедрение

Процесс внедрения осуществляется поэтапно. Следует учитывать, что первоначальная публикация программного продукта на серверах заказчика производиться с ограничением доступа третьим лицам до момента полной готовности всех узлом систем. Этапы работ:

- установка и подготовка общесистемного ПО сервера;
- инсталляция и наладка компонентов и функций серверной платформы;
- создание таблиц баз данных, загрузка информации и интеграция;
- интеграция и адаптация с уже имеющимися системами и платформами;
- проверка работоспособности всей системы, тестирование функционирования комплекса программного обеспечения;
- окончательная настройка по результатам тестирования с целью получения максимальной производительности и оптимизации работы;
- предоставление доступа систем конечному потребителю.

После окончания пуско-наладочных работ, далее следует обучающая программа сотрудников комитета (проведение тренингов, выдача учебных материалов, консультации), а также плановое техническое обслуживание всех разработанных систем с оперативным реагированием на любые непредвиденные осложнения.

Сопровождение

Под сопровождением программных продуктов мы подразумеваем:

- оперативное реагирование на входящие запросы со стороны заказчика;
- проведение пентестов систем дважды в год по методологии OWASP (Open Web Applications Security Project);
- предоставление заказчику приоритетных прямых каналов связи для взаимодействий (почта, мессенджеры, телефонные номера);
- отслеживание серверных нагрузок и стабильности работы систем;
- при необходимости, корректировку архитектуры приложений для обеспечения стабильной работы в постоянно меняющихся внешних взаимодействий, не зависящих от нашей компании (нестандартные запросы пользователей, попытки несанкционированного доступа);
- проведение консультаций по использованию систем;
- предоставление консультаций в смежных вопросах касательно взаимодействия других продуктов с нашими разработками.

Срок предоставления услуг по сопровождению всех четырех программных продуктов составляет 2-а года с момента внедрения (с 29 ноября 2019 года по 29 ноября 2021 года).