

М.А. Барамидзе

Руководство по созданию безопасного графического интерфейса

(1-е издание, под редакцией Панюковой А.А.)

ООО “ШЭРИКС”

Санкт-Петербург, 2022

Оглавление

Общие положения	4
Персоналии	4
Ответственность	6
Коммуникация	6
Общее описание процесса разработки	9
Стадия планирования	9
Стадия разработки	9
Особенности проектирования GUI	10
Идея	10
Планирование	10
Требования и пожелания к содержанию бизнес-плана	12
1. Резюме/Введение	12
2. Описание компании	13
3. Целевой рынок	13
3.1 Анализ рынка	13
3.2 Описание продукта/продуктов	13
3.3 Характеристики потенциальных покупателей	13

3.4 Уникальное торговое предложение	14
4. Планирование рабочего процесса	14
4.1 Производственный план	14
4.2 Организационное устройство предприятия	14
5. Маркетинговый план	14
6. Устойчивое развитие (стратегия продвижения и продаж)	14
7. Техничко-экономическое обоснование и финансовый план	14
7.1 Финансовый план	14
7.2 Оценка рисков	15
Требования и пожелания к содержанию технического задания	15
1. Общее описание системы	15
2. Глоссарий терминов	15
3. Описание персон (штатное расписание)	16
4. Описание внутренних подсистем	16
5. Бизнес-процессы	18
6. Описание данных	19
7. Список интерфейсов	20
8. Требования и ограничения систем	22

9. Техническое задание на создание прототипа графического интерфейса	23
10. Описание структуры базы данных	25
11. Модель рисков	26
12. Регламент проверки работоспособности	27
13. Тестовая система	28
14. Должностные инструкции	28
15. Регламент разработки	29
16. Регламент запуска	29
17. Регламент разработки дополнительного функционала	29
18. Оценка стоимости простоя	29
Пример чек-листа проверки при тестировании GUI	30

Общие положения

Данный документ является частью Руководства по созданию продуктов компании ООО “ШЭРИКС”.

Цели и задачи документа: Систематизация и упорядочивание процесса разработки безопасного интерфейса для сотрудников компании.

Персоналии

Ниже описаны подразделения компании, а также отделы внутри подразделений.

IT-подразделение

- Отдел проектирования
- Отдел разработки
- Отдел верстки и дизайна
- Отдел тестирования
- Отдел документирования
- Отдел научной разработки
- Отдел системного администрирования
- Отдел информационной безопасности

Продуктовое подразделение

- Отдел бизнес-планирования
- Отдел дизайна продукта
- Отдел формирования продукта

Подразделение маркетинга

- Отдел контента

- Отдел дизайна
- Отдел планирования и прогнозирования
- Отдел организации мероприятий

Финансовое подразделение

- Отдел планирования и прогнозирования
- Отдел контроля финансового прогнозирования
- Отдел финансового развития

Функциональное подразделение

- Бухгалтерия и отдел кадров
- Отдел подготовки кадров
- Отдел снабжения
- Юридический отдел

Внутри каждого отдела предусмотрена следующая структура ролей. На одного человека может быть назначено несколько ролей, также он может иметь отношение к нескольким отделам. Перечень возможных ролей:

- руководитель;
- ответственный за взаимодействие между отделами;
- ответственный по конкретной задаче;
- ментор практикантов;
- рядовой сотрудник;
- практикант;
- руководитель группы;
- линейный контроль выполнения задач.

На дизайнера интерфейсов возлагается решение следующих задач:

1. Контроль качества внедряемых дизайнерских разработок.
2. Разработка дизайнерских проектов в соответствии с заданными критериями.
3. Контроль за производством опытных образцов.
4. Ведение документирования в своей сфере ответственности.
5. Участие в экспертизе сторонних моделей и расчетов, относящихся к дизайну.
6. Участие в подборке материалов для разрабатываемых проектов.
7. Разработка частей технического задания, относящихся к дизайну.
8. Изготовление востребованных макетов, прототипов, эскизов.
9. Проведение необходимых расчетов по своим проектам, а также их обоснование.
10. Отслеживание актуальных трендов в области дизайна.
11. Взаимодействие с коллегами и контрагентами по аспектам, затрагивающим дизайнерскую деятельность.
12. Отслеживание отношений с правообладателями в процессе разработки и утверждения дизайнерских решений.

13. Участие в расчетах экономических параметров дизайнерских проектов.

14. Учет эргономических требований в разрабатываемых проектах.

15. Внесение требуемых коррективов в свои разработки.

16. Соблюдение стандартов трудовой дисциплины, охраны труда и пожарной безопасности.

17. Поддержание порядка на своем рабочем месте.

18. Статус задачи указывается в системе обработки заявок.

Требующие обработки ответственным лицом или линейным контролем:

- **NEW** – новая заявка в системе;
- **REOPENED** – вновь открытая заявка в системе.
- Требующие обработки сотрудниками компании:
- **ASSIGNED** – назначена на конкретного сотрудника для исполнения;
- **IN PROCESS** – конкретный сотрудник взял заявку в работу.
- Требующие обработки инициатором заявки:
- **WONTFIX** – заявка не подлежит исполнению;
- **DONE** – заявка исполнена.
- Не требующие дальнейшей обработки:
- **DUPLICATE** – заявка дублируется;
- **CLOSED** – заявка закрыта.

В тексте заявки может быть обозначена ее срочность.

Срочная/внеплановая задача – задача, поступившая работнику в силу форс-мажора, требующая немедленного реагирования, внесения правок и изменений в проект. Является приоритетной, при наличии нескольких задач с пометкой «срочно» необходимо обратиться к руководителю группы/отдела для уточнения плана выполнения.

Плановая задача – задача, заранее известная и внесённая в план работы. Есть регламентированный срок выполнения задачи.

Ответственность

При разработке продукта применяется концепция Secure by Design.

Действия всех причастных к разработке должны быть направлены на:

- Обеспечение целостности;
- Обеспечение конфиденциальности;
- Обеспечение доступности;
- Обеспечение отслеживаемости.

Ответственность за соответствие продукта перечисленным принципам лежит на руководителях отделов.

Преднамеренное нарушение принципов может быть приравнено к:

- невыполнению должностных функций – в случае, если не соответствующий результат распространяется на

деятельность внутри отдела — в границах, установленных в соответствующих статьях законодательства;

- материальному ущербу – в случае, если не соответствующий результат распространяется на деятельность иных отделов, а также взаимодействие с клиентами — в соответствии с параметрами трудового права.

За нарушения действующих норм и законов, совершенные на рабочем месте, — в порядке, определенном положениями административного, трудового и уголовного законодательства.

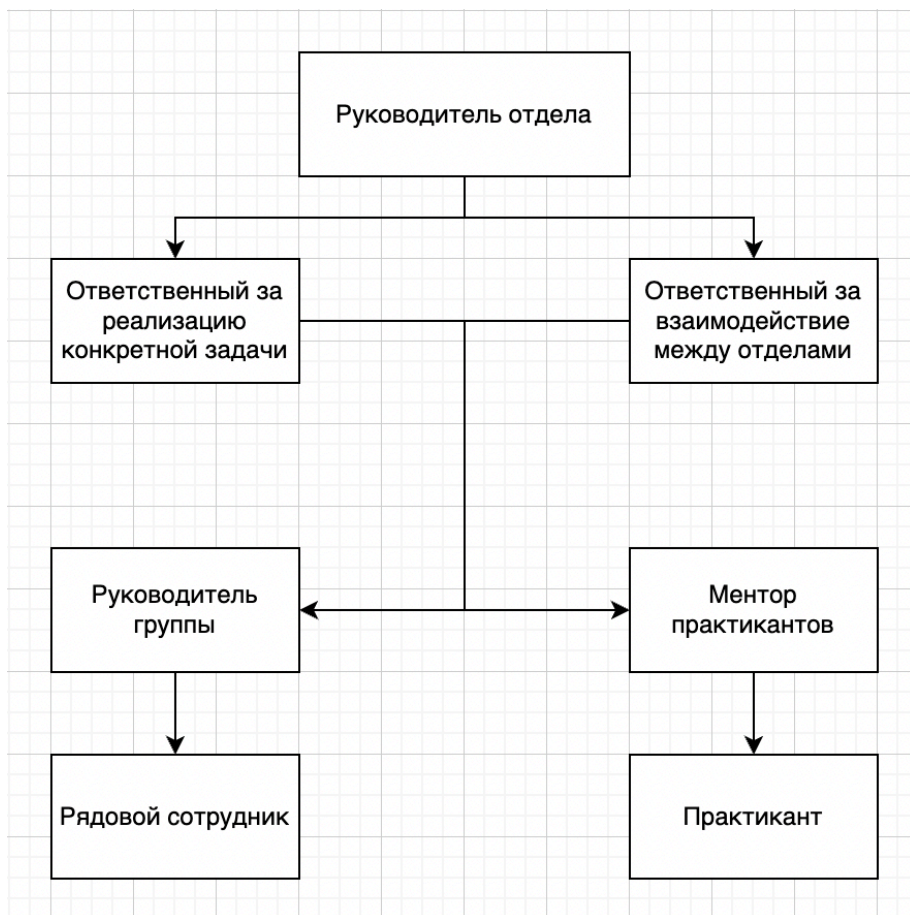
Коммуникация

Иерархия отделов представлена на Рисунке 1.

Руководитель руководит отделом и является наивысшим звеном в отделе, принимающим решение. Он же принимает глобальные задачи по ходу разработки, в том числе от руководителей других отделов.

Ответственный за взаимодействие между отделами обрабатывает заявки от других отделов, распределяя их между ответственными внутри отдела или согласовывая с руководителем, если это необходимо по инструкции.

Ответственный по конкретной задаче выполняет заявки, назначенные на него и сообщает о выполнении своему непосредственному руководителю, отправившему заявку или системе обработки заявок. Ответственный по задаче может передать задачу на исполнение руководителю группы по данному направлению.



Руководитель группы распределяет задачи между назначенными ему простыми сотрудниками и контролирует их выполнение.

Рисунок 1 — Иерархия отделов

Ментор практикантов выполняет задачи руководителя группы для практикантов.

Рядовой сотрудник просто выполняет назначенные задачи.

Практикант просто выполняет поставленные задачи.

Линейный контроль выполнения задач дублирует действия всех звеньев руководителей, отслеживая прогресс выполнения и возникновение затруднений при реализации задач. Составляет для руководителей сводку о положении дел.

Процесс коммуникации внутри отдела при выполнении поставленной задачи представлен на Рисунке 2.

Основные принципы взаимодействия сотрудников описываются в «Корпоративном стандарте компании ООО «ШЭРИКС» по коммуникации внутри информационного пространства с целью обеспечения защиты от атак посредством социальной инженерии».

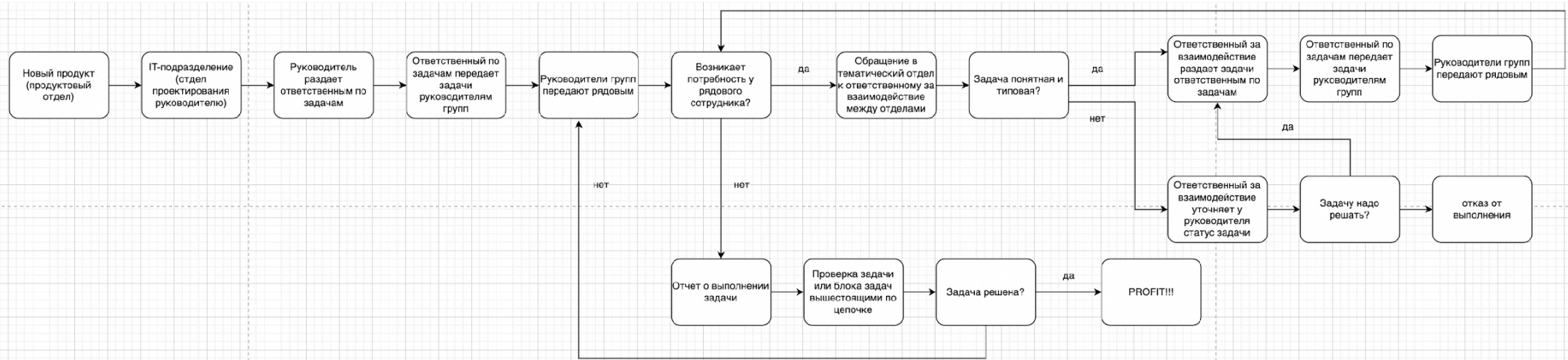


Рисунок 2 — Процесс коммуникации внутри отдела

Общее описание процесса разработки

Путь, пройденный компанией для создания программного продукта от идеи до выпуска продукта на рынок, выглядит следующим образом:

Стадия планирования

- Формулируется и описывается идея. Идея тестируется и проверяется на жизнеспособность командой Маркетингового подразделения, в случае положительного результата тестирования и проверки (идея жизнеспособна), она передается Финансовому и Продуктовому подразделениям.
- В Финансовом подразделении производится планирование и прогнозирование применительно к действующему предприятию. Тем временем, Продуктовое подразделение занимается созданием бизнес-плана (отдел бизнес-планирования), дизайном продукта (отдел дизайна), формированием безопасной среды для передачи и хранения информации (отдел информационной безопасности).

Стадия разработки

- Процессы параллельны.
- Отделы документирования и тестирования занимаются документированием процесса разработки и тестированием решений соответственно. Проводятся на каждом этапе разработки.

- Подразделения и отделы обмениваются необходимой информацией для выполнения задач, через специализированные каналы связи.
- Юридический отдел занимается разработкой необходимой документации (Функциональное подразделение).
- Отдел подготовки кадров занимается написанием стандартов. Созданием и проведением обучающих мероприятий для сотрудников и практикантов компании. (Функциональное подразделение)
- Отдел проектирования создает ТЗ (IT-подразделение).
- Отдел научной разработки занимается научным моделированием (IT-подразделение).
- Отдел разработки на основе составленного ТЗ начинает заниматься разработкой программного продукта (IT-подразделение).
- Отдел верстки и дизайна приступает к созданию графического интерфейса (IT-подразделение).
- Отдел научной разработки занимается созданием и внедрением необходимых решений (IT-подразделение).
- Отдел системного администрирования занимается развертыванием сетевой инфраструктуры (IT-подразделение).
- Только при успешном прохождении каждого этапа начинается стадия запуска продукта.

- Стадия финального тестирования. Любая неисправность или ошибка документируется и передается в соответствующий отдел для исправления.
- Выпуск продукта.

После выпуска продукт переходит в стадию поддержки. Жизненный цикл продукта в данной стадии описывается в Руководстве по созданию продуктов.

Особенности проектирования GUI

Разработка GUI — часть общего процесса разработки. Специалисты, занимающиеся разработкой GUI, участвуют в стадиях разработки, выделенными желтым цветом на схеме, представленной на Рисунке 3.

Идея

Идея поступает первоначально в отдел маркетинга, где проходит тестирование. Отдел маркетинга после тестирования при целесообразности создания продукта предоставляет на стадию Планирования в Продуктовое подразделение текстовый документ, содержащий ответы на как минимум перечисленные ниже вопросы и раскрывающий перечисленные ниже темы.

- Какая проблема решается?
- Каковы конкуренты проекта/сервиса (аналогичные, похожие или контент-смежные приложения/сайты)?
- Что будет делать приложение/сайт/интерфейс?
- Название приложения, слоган и миссия.
- Краткое описание целевой аудитории.

Планирование

В стадию планирования входят процессы бизнес-планирования, дизайна продукта и формирования безопасной среды для информации. Этим занимается Продуктовое подразделение на основании данных подразделения маркетинга, а также IT-подразделение.

Результат этапа планирования — подробное техническое задание на продукт и подробный бизнес-план.

Это самый важный этап в процессе разработки безопасного пользовательского интерфейса. В бизнес-плане должен быть корректно оценен фронт работ специалистов по дизайну при реализации запланированного в техническом задании. В техническом задании формируются основные требования к интерфейсу и создаются предварительные макеты.

В описаниях требований к техническому заданию и бизнес-плану будут отдельно отмечены особо важные для дизайна безопасного пользовательского интерфейса положения, которые могут оказывать влияние на выбранные решения при разработке.

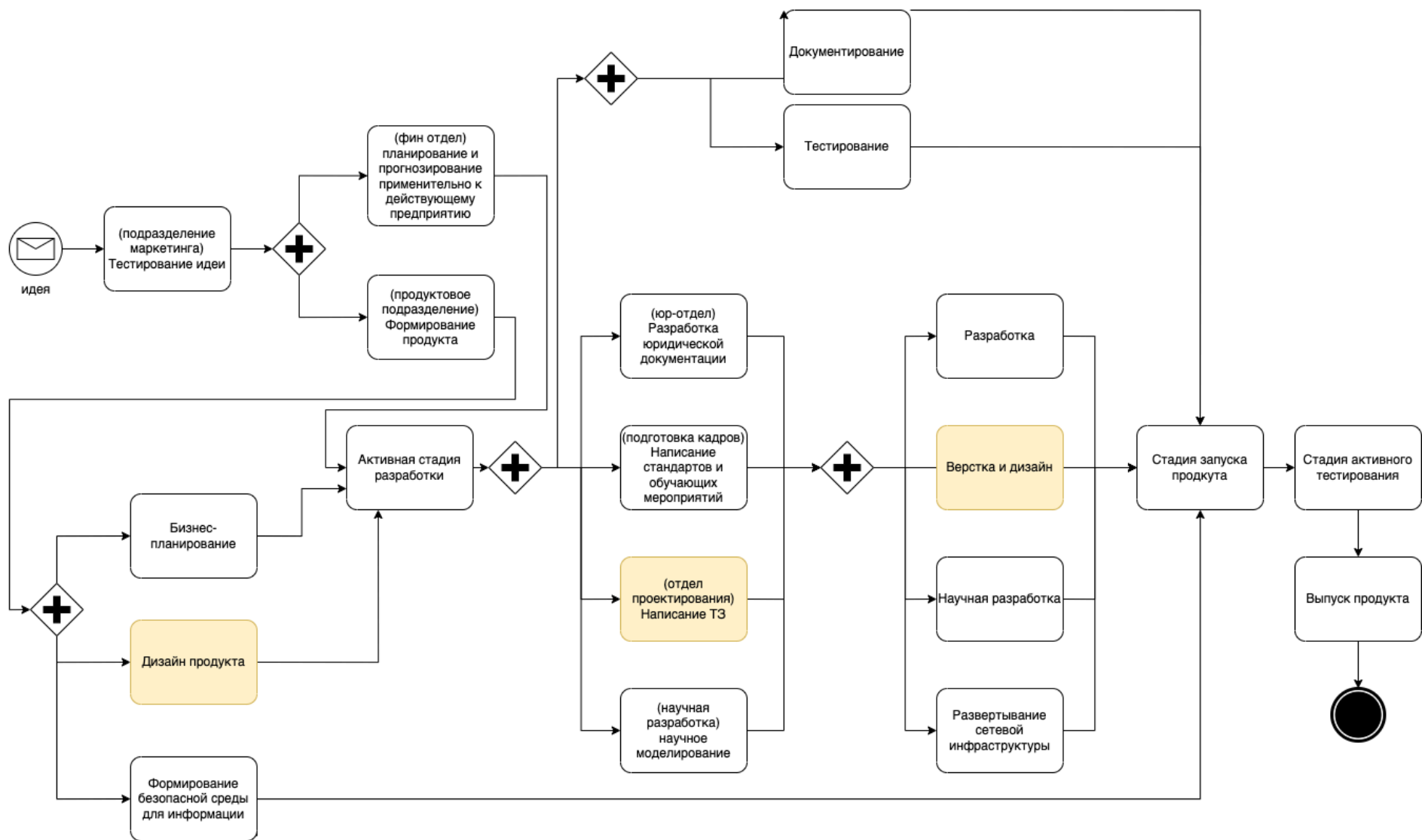


Рисунок 3 — Описание процесса разработки проекта

Требования и пожелания к содержанию бизнес-плана

Полная информация о содержимом раздела находится в Шаблоне бизнес-плана.

1. Резюме/Введение

Резюме стоит в начале бизнес-плана, но пишут его в самом конце. Это краткое содержание всего документа — выводы, которые сделаете на основе детальных расчетов.

Ниже приведены вопросы, на которые должен отвечать текст.

- Какой необходимый стартовый капитал?
- Каковы сроки окупаемости?
- Каковы ключевые этапы развития проекта?
- Какова планируемая прибыльность?

Этот пункт включает краткое описание проекта и его конкурентных преимуществ, информацию о потенциальных потребителях и партнерах. В резюме должна содержаться информация о том, как компания собирается продавать свой товар или услугу и как их рекламировать. Нужно указать, какой стартовый капитал необходим и где планируется его взять. Нужно описать ключевые этапы развития проекта и обязательно привести сроки его окупаемости и планируемую прибыльность.

А также уточнение информации относительно идеи в целом:

- краткая история бизнеса (если есть);
- короткое описание бизнес-идеи и продукта;
- краткий портрет целевой аудитории;
- цели и миссию компании/проекта/сервиса;
- основные бизнес-показатели.

Если резюме будет показываться инвестору, необходимо также в этот раздел включить финансовые показатели, графики и другую визуальную информацию, которая укажет на финансовые перспективы бизнеса и суть бизнес-идеи.

У нового бизнеса нет бизнес-показателей, вместо них нужно указать предстоящие затраты, объём собственных и кредитных средств и срок окупаемости. Уже существующему бизнесу стоит отразить в резюме размер выручки и чистой прибыли за последние 2-3 года, а также другие показатели, иллюстрирующие финансовую стабильность. Или нестабильность, если цель бизнес-плана — улучшить положение компании.

Сюда включается график прогноза продаж и анализа денежных потоков, несколько выводов из анализа рынка и отрасли, антирисковые стратегии. Цели обязательно выразить в цифрах или других измеримых показателях. Например: годовой доход — 15 млн рублей. Миссия компании должна быть сформулирована лаконично, она должна выражать причину существования бизнеса и характер взаимодействия с потребителями и обществом.

Важное для проектирования безопасного GUI: целевая аудитория, миссия, примерный бюджет, примерные сроки реализации проекта.

2. Описание компании

В этом разделе должна содержаться информация об:

- организационно-правовой форме предприятия;
- именах управленцев и владельцев бизнеса, их вкладе в проект;
- расположении и оснащении предприятия;
- текущих финансовых показателях и необходимых инвестициях.

Полная информация о содержимом раздела находится в Шаблоне бизнес-плана.

Важное для проектирования безопасного GUI: расположение и оснащение предприятия, организационно-правовая форма предприятия (возможно).

3. Целевой рынок

3.1 Анализ рынка

В данном разделе выделяется целевой сегмент аудитории и прогнозируется его рост.

Полная информация о содержимом раздела находится в Шаблоне бизнес-плана.

Важное для проектирования безопасного GUI: возможные стратегии привлечения клиентов (разрабатываемые решения должны корректно принимать привлеченных клиентов), конкуренты.

3.2 Описание продукта/продуктов

Раздел с описанием продукта содержит информацию о том, что:

- производится или продается;
- в чём особенности товара или услуги;
- какие выгоды это сулит потребителю;
- каков путь продукта до клиента из каждого сегмента;
- каков планируемый доход от каждого сегмента;
- какая инфраструктура необходима.

Полная информация о содержимом раздела находится в Шаблоне бизнес-плана.

Важное для проектирования безопасного GUI: особенности продукта, путь продукта до клиента.

3.3 Характеристики потенциальных покупателей

В данном разделе содержится описание потенциального покупателя — особенности поведения, привычки, портрет в целом.

Важное для проектирования безопасного GUI: подробное описание целевой аудитории решения.

3.4 Уникальное торговое предложение

Важное для проектирования безопасного GUI: из данного раздела можно почерпнуть информацию, на которую могут обращать внимание потенциальные пользователи, так как они могут выбирать решение на основе указанной уникальности.

4. Планирование рабочего процесса

4.1 Производственный план

Важное для проектирования безопасного GUI: сроки и ресурсы на реализацию графических интерфейсов.

4.2 Организационное устройство предприятия

В данном разделе, среди прочего, должна содержаться следующая информация:

- иерархия компании/сервиса;
- зоны ответственности сотрудников;
- состав управленческой команды;
- категории персонала.

Важное для проектирования безопасного GUI: возможные роли людей, взаимодействующих с системой, возможные уровни доступа, способ передачи прав доступа.

5. Маркетинговый план

Что должно быть прописано в разделе из того, что может понадобиться при составлении дизайна:

- краткая характеристика целевой аудитории;
- оценка платёжеспособности целевой аудитории;
- конкурентные преимущества продукта;
- стратегия ценообразования;
- рекламная тактика.

Важное для проектирования безопасного GUI: конкурентные преимущества (если они затрагивают графическое представление), рекламная тактика (продукт должен быть способен принять привлеченную аудиторию).

6. Устойчивое развитие (стратегия продвижения и продаж)

Стратегия продаж должна определять, как предприятие будет позиционироваться на рынке, и какой комплекс интегрированных маркетинговых коммуникаций будет использоваться для продвижения товаров и услуг.

Важное для проектирования безопасного GUI: способы привлечения клиентов, которые могут оказать влияние на внешний вид приложения, а также тактики продаж.

7. Техничко-экономическое обоснование и финансовый план

7.1 Финансовый план

Важное для проектирования безопасного GUI: информация о доступных ресурсах в разные моменты времени для разработки и дальнейшей поддержки разрабатываемого решения.

7.2 Оценка рисков

Если на риск предполагается воздействие посредством чего-либо, что может быть отражено в интерфейсе приложения, то это указывается.

Учёт негативных сценариев — тоже важная часть планирования. В этом разделе перечислены типичные факторы риска, а также сильные и слабые стороны самой компании/сервиса, и выработаны стратегии на случай нежелательного развития событий.

Необходимо описать:

- внутренние и внешние риски;
- индикаторы риска;
- программу действий для каждого индикатора.

Риски нестабильны, поэтому, когда ситуация на рынке меняется, их необходимо пересматривать заново. Определите конкретные зоны риска. Потом устанавливаются индикаторы риска — показатели, которые сообщают, что ситуация выходит из-под контроля.

Важное для проектирования безопасного GUI: возможные сценарии смягчения рисков с использованием графического интерфейса, возможные риски взаимодействия с графическим интерфейсом, угрозы, реализуемые через графический интерфейс и способы их нейтрализации.

Требования и пожелания к содержанию технического задания

1. Общее описание системы

Описание технологий и инструментов для реализации продуктов.

Составить краткое описание – что за система, зачем, что делает, какова ее цель существования и решаемые ею задачи. Ее целевая аудитория и краткое описание технического представления решения для целевой аудитории.

Важное для проектирования безопасного GUI: предварительный перечень возможных подсистем. Данный перечень позволяет примерно оценить фронт работ по созданию графических интерфейсов, так как для большинства подсистем он необходим.

Зона ответственности специалиста по проектированию безопасного GUI: корректность описания на основе бизнес-плана, так как дальнейшая разработка технического задания опирается на данное представление.

2. Глоссарий терминов

Зона ответственности специалиста по проектированию безопасного GUI: обеспечить наличие корректной расшифровки всех используемых терминов при составлении фрагментов технического задания, связанных с проектированием безопасных пользовательских интерфейсов.

3. Описание персон (штатное расписание)

- перечисление всех персоналий, которые могут взаимодействовать с системой. Полезно разделить их на группы:
- сотрудники;
- клиенты;
- внешние системы (тут могут быть перечислены не только люди).

Важное для проектирования безопасного GUI: перечень возможных пользователей всех систем – а значит это перечень всех персон, которые могут осуществлять взаимодействие с интерфейсами того или иного вида.

Зона ответственности специалиста по проектированию безопасного GUI: корректность описания на основе бизнес-плана, так как дальнейшая разработка технического задания опирается на данное представление.

Перечень действий, которые необходимо выполнить специалисту по проектированию безопасного GUI на данном этапе:

- проверить корректность описания персон на соответствие бизнес-плану;
- выписать возможные мотивы каждой роли использования информационной системы в целом;
- выписать возможные ожидания каждой роли от использования информационной системы в целом.

Требования к результату работы специалиста по проектированию безопасного GUI:

- результат выполнения всех вспомогательных операций должен быть доступен другим сотрудникам, принимающим участие в разработке технического задания;
- до окончания работы над техническим заданием необходимо регулярно актуализировать информацию на предмет возможных изменений как в основном файле, так и во вспомогательных;
- ответственным за принятие окончательного решения по списку персон и ролей является руководитель команды (отдела) разработки по данному проекту. В случае расхождения мнений со специалистом по проектированию интерфейсов последнему необходимо аргументированно обосновать позицию или принять мнение руководителя разработки.

4. Описание внутренних подсистем

Тут надо перечислить все системы, которые будут в проекте. Это могут быть:

- конкретные программные и иные технологические продукты (1 продукт — 1 система, например — мобильное приложение для клиента, мобильное приложение для исполнителя, админка для исполнителя и так далее);

- внутренние решения (например – почтовый сервер, система эшелонированных бэкапов, система внутреннего документооборота);
- системы для обеспечения законной деятельности (часто – это взаимодействие с внешними структурами, например – система отправки отчетности в госорганы (скорее всего – это несколько разных систем – изучите), платежная система, виртуальный кассовый принтер);
- инфраструктурные решения (какие-то системы внутри офиса, серверной и так далее).

К каждой выделенной системе надо дать короткое описание, которое содержит следующую информацию:

- название системы;
- тип системы (внутренняя или есть взаимодействие с внешними системами);
- программные продукты, имеющие отношение к реализации системы, предлагаемые языки программирования в случае, если система требует разработки, предполагаемые библиотеки для разработки (перечисление);
- оборудование, необходимое для реализации системы (перечисление);
- какая информация на входе (какую информацию система получает для обработки);

- какая информация на выходе (какую информацию система может предоставить в результате работы и кому).

Важное для проектирования безопасного GUI: возможность подготовить основу для выделения списка графических интерфейсов, так как каждый графический интерфейс имеет отношение к какой-то одной подсистеме, его способ реализации и особенности зависят от того, к какой подсистеме они принадлежат.

Зона ответственности специалиста по проектированию безопасного GUI: корректность описания на основе бизнес-плана, так как дальнейшая разработка технического задания опирается на данное представление. Для каждого графического интерфейса, предполагаемого при описании идеи продукта – должна быть одна подсистема.

Перечень действий, которые необходимо выполнить специалисту по проектированию безопасного GUI на данном этапе:

- проверить корректность описания систем на соответствие бизнес-плану;
- составить список отношений потенциальных пользователей и подсистем;
- описать причины и процессы использования и взаимодействия внутренних систем различными потенциальными пользователями;
- выписать возможные ожидания потенциальных пользователей от каждой системы.

Требования к результату работы специалиста по проектированию безопасного GUI:

- результат выполнения всех вспомогательных операций должен быть доступен другим сотрудникам, принимающим участие в разработке технического задания;
- до окончания работы над техническим заданием необходимо регулярно актуализировать информацию на предмет возможных изменений как в основном файле, так и во вспомогательных;
- допускается схематическое изображение отношений пользователей и подсистем;
- ответственным за принятие окончательного решения по списку систем является руководитель команды (отдела) разработки по данному проекту. В случае расхождения мнений со специалистом по проектированию интерфейсов последнему необходимо аргументированно обосновать позицию или принять мнение руководителя разработки.

5. Бизнес-процессы

В данном разделе должно содержаться:

- перечень всех процессов, которые должны быть;
- графическое представление разработанных процессов и пояснения-описания.

В процессах (или описаниях к ним) нужно сделать пометки — какие персоналии используют те или иные процессы.

Важное для проектирования безопасного GUI: в процессах должно быть отмечено взаимодействие с пользовательским интерфейсом, где и в какой момент пользователь каждого вида начинает взаимодействие с интерфейсом.

Зона ответственности специалиста по проектированию безопасного GUI: корректность описания на основе бизнес-плана, так как дальнейшая разработка технического задания опирается на данное представление.

Перечень действий, которые необходимо выполнить специалисту по проектированию безопасного GUI на данном этапе:

- для каждой пользовательской роли выделить возможные точки входа в интерфейсы, основанные на их причинах использования продуктов;
- предварительно подготовить текстовое описание user stories для каждой точки входа и передать их лицам, участвующим в разработке bpmn;
- проверить корректность описания и составления бизнес-процессов на соответствие бизнес-плану;
- выделить в процессах фрагменты, при которых пользователь взаимодействует с интерфейсом.

Требования к результату работы специалиста по проектированию безопасного GUI:

- результат выполнения всех вспомогательных операций должен быть доступен другим сотрудникам, принимающим участие в разработке технического задания;
- допускается написание user stories как в виде текста, так и в виде схем или bpmn;
- до окончания работы над техническим заданием необходимо регулярно актуализировать информацию на предмет возможных изменений как в основном файле, так и во вспомогательных;
- ответственным за принятие окончательного решения по списку персон и ролей является руководитель команды (отдела) разработки по данному проекту. В случае расхождения мнений со специалистом по проектированию интерфейсов последнему необходимо аргументированно обосновать позицию или принять мнение руководителя разработки.

6. Описание данных

Составить перечень данных, которые участвуют в функционировании системы:

- хранятся внутри системы;
- получаются от внешних участников;
- обрабатываются системой;
- передаются внешним участникам.

Можно сделать в виде таблицы с колонками: тип данных — форма представления — источник получения — хранение — обработка — передача.

Важное для проектирования безопасного GUI: распределение данных между персоналиями. Что, кому и как должно передаваться или предоставляться, в какой форме оно может отображаться для пользователя.

Зона ответственности специалиста по проектированию безопасного GUI: корректность описания на основе бизнес-плана, так как дальнейшая разработка технического задания опирается на данное представление. Специалисту важно предположить, какие данные в какой форме какими пользователями будут восприниматься наиболее корректно.

Перечень действий, которые необходимо выполнить специалисту по проектированию безопасного GUI на данном этапе:

- проверить корректность описания персон на соответствие бизнес-плану;
- определить какие данные отображаются в интерфейсе и каким способом, дополнить информацию при необходимости;
- определить необходимую длину вводимых данных (например для фамилии, имени, комментария, пароля);
- написать возможные виды предоставления информация (список, таблица, уведомление и т.д., а также форматы дат, валюты, графического или текстового представления и так далее), а также выделить предпочтительные форматы

представления информации с точки зрения восприятия различными группами пользователей.

Требования к результату работы специалиста по проектированию безопасного GUI:

- результат выполнения всех вспомогательных операций должен быть доступен другим сотрудникам, принимающим участие в разработке технического задания;
- дополнительные (помимо ТЗ) создаваемые материалы в рамках данного раздела могут иметь форму текстовых документов с таблицами;
- до окончания работы над техническим заданием необходимо регулярно актуализировать информацию на предмет возможных изменений как в основном файле, так и во вспомогательных;
- ответственным за принятие окончательного решения по списку персон и ролей является руководитель команды (отдела) разработки по данному проекту. В случае расхождения мнений со специалистом по проектированию интерфейсов последнему необходимо аргументированно обосновать позицию или принять мнение руководителя разработки.

7. Список интерфейсов

Перечислить программные интерфейсы, которые нужно будет реализовать для обеспечения взаимодействия систем между собой. Опираясь на информацию о данных, попробовать

составить описание (посмотрите, как обычно описывается API тех или иных систем).

Интерфейсы могут быть 2 видов: программные и пользовательские. Пользовательские интерфейсы могут быть текстовыми и графическими.

В данном разделе должны быть перечислены все возможные виды интерфейсов и их описание.

Важное для проектирования безопасного GUI: перечисление всех графических интерфейсов, с обозначенным отношением к конкретным системам, а также с перечисленными свойствами, необходимыми для реализации, в том числе с требованиями к безопасности данных при взаимодействии с пользователем.

Зона ответственности специалиста по проектированию безопасного GUI: корректность описания на основе бизнес-плана, так как дальнейшая разработка технического задания опирается на данное представление.

Корректность описания по отношению к созданным ранее разделам.

Корректный выбор решений для реализации программной части графического интерфейса.

Обеспечение корректного описания безопасного представления данных.

Перечень действий, которые необходимо выполнить специалисту по проектированию безопасного GUI на данном этапе:

- на основе данных из предыдущих этапов составить список необходимых интерфейсов;
- к каждому интерфейсу выбрать продукт для проектирования и для реализации, выписать требования и ограничения, которые возникают в результате такого выбора;
- составить таблицу с описанием свойств интерфейсов — важно отметить интерфейсы, содержащие конфиденциальную информацию, отметить такие свойства, как привлекательность, функциональность, удобство;
- на основе bpm выделить список экранов для каждого интерфейса;
- для каждого экрана указывается набор информации и способы ее отображения;
- создать общие элементы сайта/приложения (хэдер, футер, меню, боковая/ нижняя панель, контент);
- задать общие элементы формы (фио, телефон, согласие на обработку, кнопки)
- только после этого можно приступить к разработке предварительных макетов, первоначально для какого-то

одного формата устройств (должна быть таблица, где указано соответствие разработанного формату устройства);

- производится предварительное тестирование юзабилити макетов с учетом потенциальных ожиданий пользователей, их целей использования решения, на основе этого создаются рекомендации к графическим интерфейсам, размещаемые в дальнейшем в техническом задании;
- с использованием предварительных макетов составляется техническое задание на разработку полноценных макетов графического интерфейса для всех форматов устройств.

Требования к результату работы специалиста по проектированию безопасного GUI:

- результат выполнения всех вспомогательных операций должен быть доступен другим сотрудникам, принимающим участие в разработке технического задания;
- макеты создаются в выбранных средствах макетирования для каждого интерфейса;
- описания к макетам и иная вспомогательная информация должна содержаться в текстовом виде или в виде схем или таблиц в текстовом файле;
- до окончания работы над техническим заданием необходимо регулярно актуализировать информацию на предмет возможных изменений как в основном файле, так и во вспомогательных;

- ответственным за принятие окончательного решения по списку персон и ролей является руководитель команды (отдела) разработки по данному проекту. В случае расхождения мнений со специалистом по проектированию интерфейсов последнему необходимо аргументированно обосновать позицию или принять мнение руководителя разработки.

8. Требования и ограничения систем

Возможные требования:

- доступность;
- отказоустойчивость;
- требования, связанные с особенностями данных — по типу, объему, способу хранения, скорости передачи.

Ограничения могут быть связаны также с особенностями данных и процессов, например, какие-то данные могут быть актуальны или получаемы только в какой-то конкретный промежуток времени и так далее.

Также в этом разделе указывается размер и особенности технологических окон для обслуживания системы (например, для обновления, для бэкапов и так далее).

Важное для проектирования безопасного GUI: информация, которая может быть актуальна или получаемая только в какой-то определенный промежуток времени, актуальная информация, которая должна соответствовать действительности (дата, валюта и т.д.).

Зона ответственности специалиста по проектированию безопасного GUI: корректность описания на основе бизнес-плана, так как дальнейшая разработка технического задания опирается на данное представление.

Перечень действий, которые необходимо выполнить специалисту по проектированию безопасного GUI на данном этапе:

- выделить те случаи, при которых информация может предоставляться только в конкретный промежуток времени;
- описать обстоятельства при которых, предоставляется информация.
- типизировать информацию (данные, которые могут изменяться, данные которые просто предоставляются, информация необходимая для осуществления какого-либо действия (например: повторная отправка смс-кода подтверждения)
- написать список интерфейсов, в которых может быть необходимо оповещать пользователя о технических работах;
- подготовить полное описание таких интерфейсов для каждой подсистемы, если оно в ней актуально.

Требования к результату работы специалиста по проектированию безопасного GUI:

- результат выполнения всех вспомогательных операций должен быть доступен другим сотрудникам, принимающим участие в разработке технического задания;
- макеты интерфейсов могут быть составлены в выбранных средах для макетирования;
- описания к макетам и иная вспомогательная информация должна содержаться в текстовом виде или в виде схем или таблиц в текстовом файле;
- до окончания работы над техническим заданием необходимо регулярно актуализировать информацию на предмет возможных изменений как в основном файле, так и во вспомогательных;
- ответственным за принятие окончательного решения по списку персон и ролей является руководитель команды (отдела) разработки по данному проекту. В случае расхождения мнений со специалистом по проектированию интерфейсов последнему необходимо аргументированно обосновать позицию или принять мнение руководителя разработки.

9. Техническое задание на создание прототипа графического интерфейса

С учетом информации в пунктах 7 и 8, а также опираясь на технологии и особенности, указанные в пункте 4 составляется прототип приложения.

Важное для проектирования безопасного GUI: использование простых и понятных форм, которые будут направлять пользователя, а не путать или пугать. Обеспечение целостности логики взаимодействия пользователь-приложение. Использование правильных цветовых решений для создания активных элементов. Ясность языка приложения (единая стилистика для обозначения форм ввода данных, кнопок, уведомлений)

Зона ответственности специалиста по проектированию безопасного GUI: корректность описания на основе бизнес-плана, так как дальнейшая разработка технического задания опирается на данное представление.

Корректность описания по отношению к созданным ранее разделам.

Корректный выбор решений для реализации графической части GUI.

Перечень действий, которые необходимо выполнить специалисту по проектированию безопасного GUI на данном этапе:

- на основе данных из предыдущих этапов создать дизайн-систему приложения, согласующуюся с правилами оформления бренда (создание Mood board, фундаментальных элементов UI, изображения, типографика, иконки и символы не вызывающие лишних ассоциаций, стиль UI, библиотеки шаблонов, навигации, элементов взаимодействия);

- к каждому элементу выбрать и определить правила визуального представления в интерфейсе, выписать требования и ограничения, которые возникают в результате такого выбора;
- в интерфейсах, содержащих конфиденциальную информацию, должно быть придумано каким образом ее можно скрыть (кружочки при вводе пароля, блюр окна приложения во время просмотра запущенных приложений, частичное скрытие номера телефона, блюр для фотографии паспорта и т.д.) снова отметить такие свойства, как привлекательность, функциональность, удобство;
- на основе списка экранов и использованием созданной дизайн-системы для каждого интерфейса описать, создать и добавить готовые графические элементы на экраны;
- использовать анимацию, не нарушающую логику восприятия приложения (например – если стрелочка обозначающая действие “назад” направлена влево, возврат к предыдущему окну не должен быть осуществлен с использованием анимации перелистывания экранов сверху вниз);
- согласовать с руководителем отдела/группы, с отделом маркетинга, руководителем проекта;
- только после этого можно приступать к разработке прототипов, первоначально для какого-то одного формата устройств (должна быть таблица, где указано соответствие разработанного формату устройства);

- производится полное тестирование GUI (частично описано ниже). Тестирование прототипов на соответствие экранов ТЗ с использованием предварительных макетов. Составляется техническое задание на разработку полноценных макетов графического интерфейса для всех форматов устройств.
- в случае, нахождения ошибки – документирование, внесение правок.

Требования к результату работы специалиста по проектированию безопасного GUI:

- результат выполнения всех вспомогательных операций должен быть доступен другим сотрудникам, принимающим участие в разработке технического задания;
- прототипы GUI создаются в выбранных средствах прототипирования для каждого интерфейса;
- описания к прототипам и иная вспомогательная информация должна содержаться в текстовом виде или в виде схем или таблиц в текстовом файле;
- до окончания работы над техническим заданием необходимо регулярно актуализировать информацию на предмет возможных изменений как в основном файле, так и во вспомогательных;
- ответственным за принятие окончательного решения по списку персон и ролей является руководитель команды (отдела) разработки по данному проекту. В случае

расхождения мнений со специалистом по проектированию интерфейсов последнему необходимо аргументированно обосновать позицию или принять мнение руководителя разработки.

10. Описание структуры базы данных

Схемы, текстовое пояснение и типы данных. Также сюда надо будет добавить технические особенности для реализации.

Если данные в БД хранятся в одном виде, а пользователю показываются в другом — необходимо все такие данные перечислить и описать требования к изменению представления

Важное для проектирования безопасного GUI: вид представленной информации в графическом интерфейсе, взятой из базы данных.

Зона ответственности специалиста по проектированию безопасного GUI: корректность описания на основе предыдущих разделов, так как дальнейшая разработка технического задания опирается на данное представление.

Предоставление корректной информации, предоставляемой из БД.

Корректный выбор решений для обеспечения безопасности графического интерфейса.

Обеспечение корректного описания безопасного представления данных.

Перечень действий, которые необходимо выполнить специалисту по проектированию безопасного GUI на данном этапе:

- перечислить все данные, которые должны браться из базы данных;
- определить какие данные должны будут видоизменяться, а какие нет;
- описать требования к изменению представления данных;
- согласовать с руководителем отдела и разработчиками.
- составить сценарии для снижения/страхования представленных рисков.
- переделать то, что описано ранее, в случае необходимости (согласуется с руководством).

Требования к результату работы специалиста по проектированию безопасного GUI:

- результат выполнения всех вспомогательных операций должен быть доступен другим сотрудникам, принимающим участие в разработке технического задания;
- информация предоставляется в виде таблицы и текстом, в текстовом документе.
- до окончания работы над техническим заданием необходимо регулярно актуализировать информацию на предмет возможных изменений как в основном файле, так и во вспомогательных;

- ответственным за принятие окончательного решения по списку персон и ролей является руководитель команды (отдела) разработки по данному проекту. В случае расхождения мнений со специалистом по проектированию интерфейсов последнему необходимо аргументированно обосновать позицию или принять мнение руководителя разработки.

Если можно хранить данные сразу как надо — надо настоять, чтобы разработчики так и делали, но если они протестуют — не возникать.

11. Модель рисков

В этом разделе упоминаются только технические риски (а не риски, связанные с персоналом).

Можно оформить в виде таблицы со следующими колонками:

- название риска (или аварийной ситуации);
- системы, на которые он влияет;
- описание возможных последствий наступления риска;
- описание сценариев для снижения/страхования.

Также в этом разделе описывается модель угроз (кто злоумышленник, что может сделать, на какую систему это влияет, как можно защитить и так далее).

Важное для проектирования безопасного GUI: риски, связанные со взаимодействием пользователя с интерфейсом.

Зона ответственности специалиста по проектированию безопасного GUI: корректность описания на основе предыдущих разделов, так как дальнейшая разработка технического задания опирается на данное представление.

Корректный выбор решений для обеспечения безопасности графического интерфейса.

Обеспечение корректного описания безопасного представления данных.

Обеспечение эксплуатации графических интерфейсов.

Перечень действий, которые необходимо выполнить специалисту по проектированию безопасного GUI на данном этапе:

- выделить риски при взаимодействия пользователя с приложением;
- описать возможные последствия наступления риска;
- при возможности полностью избавиться от риска, в ином случае – минимизировать;
- составить сценарии для снижения/страхования представленных рисков.
- переделать то, что описано ранее, в случае необходимости (согласуется с руководством).

Требования к результату работы специалиста по проектированию безопасного GUI:

- результат выполнения всех вспомогательных операций должен быть доступен другим сотрудникам, принимающим участие в разработке технического задания;
- информация должна быть представлена в текстовом документе (в виде текста или таблицы).
- до окончания работы над техническим заданием необходимо регулярно актуализировать информацию на предмет возможных изменений как в основном файле, так и во вспомогательных;
- ответственным за принятие окончательного решения по списку персон и ролей является руководитель команды (отдела) разработки по данному проекту. В случае расхождения мнений со специалистом по проектированию интерфейсов последнему необходимо аргументированно обосновать позицию или принять мнение руководителя разработки.

12. Регламент проверки работоспособности

Тут надо перечислить какие конкретно регламенты проверки и каких конкретно систем должны быть написаны. Учитывайте, что должны быть и регламенты действия в аварийных ситуациях.

В качестве примера распишите какой-то один регламент (в идеале — той системы, которую вы будете пытаться реализовать для демонстрации).

Важное для проектирования безопасного GUI: регламенты, связанные с проверкой работоспособности и взаимодействием пользователя с интерфейсом.

Зона ответственности специалиста по проектированию безопасного GUI: корректность описания на основе предыдущих разделов.

Перечень действий, которые необходимо выполнить специалисту по проектированию безопасного GUI на данном этапе:

- выделить системы, связанные с GUI, к которым необходим регламент;
- провести проверку работоспособности устройства.

Требования к результату работы специалиста по проектированию безопасного GUI:

- результат выполнения всех вспомогательных операций должен быть доступен другим сотрудникам, принимающим участие в разработке технического задания;
- отчет в виде текстового документа;
- до окончания работы над техническим заданием необходимо регулярно актуализировать информацию на предмет возможных изменений как в основном файле, так и во вспомогательных;
- ответственным за принятие окончательного решения по списку персон и ролей является руководитель команды

(отдела) разработки по данному проекту. В случае расхождения мнений со специалистом по проектированию интерфейсов последнему необходимо аргументированно обосновать позицию или принять мнение руководителя разработки.

13. Тестовая система

Опишите, какие тестовые системы должны быть внутри проекта:

- название;
- какой проект она тестирует;
- какие технические средства нужны для ее реализации, это какие-то готовые программные продукты или создаются свои – надо указать;
- формат результата работы тестовой системы (кто оповещается, каким образом, с каким интервалом).

Важное для проектирования безопасного GUI: описание тестовых систем для приложений на соответствие ТЗ и обеспечению безопасности интерфейсов.

Зона ответственности специалиста по проектированию безопасного GUI: корректность описания на предыдущих разделах.

Перечень действий, которые необходимо выполнить специалисту по проектированию безопасного GUI на данном этапе:

- выделить системы для тестирования GUI;
- описать системы для тестирования GUI;

- составить карту тестирования интерфейса;
- согласовать системы с руководством отдела/проекта;
- составить отчет о результатах тестирования.

Требования к результату работы специалиста по проектированию безопасного GUI:

- результат выполнения всех вспомогательных операций должен быть доступен другим сотрудникам, принимающим участие в разработке технического задания;
- информация предоставляется в текстовом документе (список, таблицы, при необходимости блок-схема)
- до окончания работы над техническим заданием необходимо регулярно актуализировать информацию на предмет возможных изменений как в основном файле, так и во вспомогательных;
- ответственным за принятие окончательного решения по списку персон и ролей является руководитель команды (отдела) разработки по данному проекту. В случае расхождения мнений со специалистом по проектированию интерфейсов последнему необходимо аргументированно обосновать позицию или принять мнение руководителя разработки.

14. Должностные инструкции

В этом разделе необходимо перечислить весь штатный персонал проекта и все дополнения к уже принятым в компании должностным инструкциям.

Важное для проектирования безопасного GUI: должностные инструкции не должны противоречить процессам взаимодействия с интерфейсом. Интерфейс не должен способствовать нарушению персоналом должностных инструкций, в том числе связанных с безопасностью.

15. Регламент разработки

В данном разделе описывается разграничение задач и данных между сотрудниками компании.

Способ передачи задач в процессе разработки показан на Рисунке 2 данного Руководства.

16. Регламент запуска

Необходимо создать описание ввода разрабатываемого приложения в эксплуатацию. Помимо тестировщиков приложений, необходим GUI-тестировщик.

Важное для проектирования безопасного GUI: необходимо протестировать по заранее составленным схемам все элементы интерфейса. Схемы могут проверяться как человеком, так и автоматически.

Требования к результату работы специалиста по проектированию безопасного GUI:

- список тестов для каждого интерфейса с описанием тестируемого и иных особенностей проведения тестов;
- подробное описание каждого теста;
- протоколы тестирования;
- рекомендации к обработке результатов тестов.

17. Регламент разработки дополнительного функционала

В данном разделе описывается порядок внедрения дополнительного функционала:

- Описание необходимого функционала;
- Процесс согласования с основной системой;
- Проверка по всем этапам разработки;
- Внесение правок.

Для разработчика интерфейса данный регламент аналогичен регламентам разработки в целом.

18. Оценка стоимости простоя

В данном разделе оцениваются возможный материальный ущерб от ошибок/некачественной работы команды.

Важное для проектирования безопасного GUI: важно учитывать потери от:

- невозможности пользователем достигать результата;
- нежелания использовать систему в результате личного негативного восприятия дизайна;
- возможных утечек данных в результате выбора неудачных интерфейсных решений.

Пример чек-листа проверки при тестировании GUI

- ☐ Проверить на соответствие ТЗ.
- ☐ Проверить приложение на наличие элементов, способных выдать повышенный уровень доступа.
- ☐ Проверить на соответствие состояния кнопок (active/disabled/hover) и действий пользователя.
- ☐ Расположение, размер, цвет, ширина, длина элементов; возможность ввода букв или цифр.
- ☐ Реализуется ли функционал приложения с помощью графических элементов.
- ☐ Размещение всех сообщений об ошибках, уведомлений (а также шрифт, цвет, размер, расположение и орфография и пунктуация в тексте).
- ☐ Читабелен ли использованный шрифт.
- ☐ Переходит ли курсор из текстового в поинтер при наведении на активные элементы, выделяются ли выбранные элементы.
- ☐ Выравнивание текста и форм.
- ☐ Качество изображений.

- ☐ Проверить расположение и отображение всех элементов при различных разрешениях экрана, а также при изменении размера окна браузера для сайтов (проверить, появляется ли скролл).
- ☐ Проверить текст на орфографические, пунктуационные ошибки.
- ☐ Появляются ли тултипы (если есть необходимость).
- ☐ Верный ли тип данных используется. Нужно убедиться, что для определенных типов данных, таких как валюта и даты и т.д., можно вводить только допустимые значения.
- ☐ Указана ли ширина поля. Если определенное текстовое поле предназначено для определенного количества символов, укажите в пользовательском интерфейсе, что введенные данные не должны превышать границу по количеству символов. (Например, поле, которое позволяет использовать 50 символов в базе данных приложения, не должно позволять пользователям вводить более 50 символов в интерфейсе).
- ☐ Правильно ли работают элементы навигации.
- ☐ Все ли необходимые индикаторы прогресса присутствуют.
- ☐ Проверить на корректность работы все индикаторы прогресса.
- ☐ Подсказки ввода. В выпадающем меню с сотнями элементов при вводе первой буквы должны остаться только те элементы, которые начинаются с этой буквы, таким

образом можно уберечь пользователей от просмотра лишней и потенциально опасной информации.

- ☐ Скролл таблиц. Когда данные из таблицы перетекают на следующую страницу, функция прокрутки должна позволять пользователям прокручивать данные, но не трогать все заголовки.
- ☐ Ведение журнала ошибок. Когда в системе возникает фатальная ошибка, нужно убедиться, что приложение записывает сведения об ошибке в специальный файл журнала для последующего просмотра.
- ☐ Пункты меню и режим. Убедитесь, что приложение отображает только те пункты меню, которые доступны в определенном режиме.
- ☐ Комбинации клавиш. Проверьте комбинации клавиш, правильно ли они работают, независимо от браузера, платформы или устройства.
- ☐ Кнопки подтверждения действий. Убедитесь, что пользовательский интерфейс имеет работающую кнопку подтверждения каждый раз, когда пользователь хочет сохранить или удалить элемент.