

Требования к ИС

Структура Артефакта должна включать оглавление и следующие разделы, пункты и подпункты:

1. Глоссарий
2. Описание
3. Функциональные требования
 - 3.1. Описание процессов / функций
 - 3.2. Описание клиентских путей (User flow)
 - 3.3. Прототипы пользовательских интерфейсов
 - 3.4. Требования к отчетности
 - 3.5. Требования к мониторингу
 - 3.6. Требования к журналированию
4. Нефункциональные требования
 - 4.1. Требования к производительности (быстродействию)
 - 4.2. Требования к нагрузке
 - 4.3. Требования доступности и надежности
 - 4.3.1. Класс критичности
 - 4.3.2. Прочие требования
 - 4.4. Регламенты и стандарты
 - 4.5. Требования к качеству данных
 - 4.6. Прочие нефункциональные требования
5. Требования к информационной безопасности

1. ГЛОССАРИЙ

Термины и сокращения приведены в Таблицах настоящего раздела документа.

Таблица – Термины

№	Термин	Значение
1.		

Таблица – Сокращения

№	Сокращение	Значение
1.	АБС	Автоматизированная банковская система
2.	ИС	Информационная система.
3.	ПС	Подсистема
4.	RPO	Recovery Point Objective - Целевая точка восстановления – максимальный промежуток времени, предшествующий моменту возникновения

№	Сокращение	Значение
		кризисной ситуации, за который допускается потеря данных (глубина хранения данных)
5.	RTO	Recovery Time Objective - Целевое время восстановления – промежуток времени с момента возникновения кризисной ситуации, в течение которого необходимо восстановить функционирование ИС до согласованного уровня

2. ОПИСАНИЕ

Верхнеуровневое описание целей и назначения всей ИС, ПС. Содержит описание назначения и основных функций: 5-10 пунктов.

3. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

3.1. Описание процессов / функций

Описание / схемы элементов функциональности: бизнес-процессов, алгоритмов обработки данных, в виде BPMN диаграммы процессов и/или таблицы функций.

При необходимости, приводятся описания не только to be, но и as is.

3.2. Описание клиентских путей (User flow)

Раздел заполняется, если применимо понятие клиентских путей или user flow.

Карты клиентских путей: основные этапы и шаги клиента, с необходимой степенью проработки – в разрезе персон и каналов, а также сценарии использования в разрезе пользователей с указанием основных ролей участников.

3.3. Прототипы пользовательских интерфейсов

Приводятся прототипы интерфейсов в формате figma.

Ссылка на работающий прототип пользовательских интерфейсов в системе прототипирования.

Эскизы прототипов и/или снимки экранов прототипа с пояснениями, переходами между формами.

3.4. Требования к отчетности

Заполняется по необходимости.

Перечень требуемых отчетов в бизнес-терминах с указанием необходимых параметров, алгоритмов по их формированию, требований к формату запуска (например, возможность формирования списков клиентов в определенном разрезе, периодичность формирования отчетов, форма представления отчетов, и т.п.).

3.5. Требования к мониторингу

Описание необходимых проверок относительно показателей качества функций.
Состав атрибутов в таблице:

- **Показатель качества** – краткое описание / алгоритм проверки с указанием единицы измерения;
- **Объект мониторинга** - Информационный ресурс, сервер, база данных, приложение, очередь; любые объекты за исключением бизнес сервисов и бизнес операций.

Таблица – Показатели качества

№	Показатель качества	Объект мониторинга
1.		

		Метрики (показатели качества)		
№№	Источники данных (объекты мониторинга)	ИС (наименование ИС/Подсистемы)	Наименование метрики	Описание метрики
1	URL		Количество входящих запросов с разбивкой по типам	Количество входящих запросов по типам за 5 минут
2	URL		Количество входящих запросов в разрезе отдельных потребителей	Количество входящих запросов от потребителей за 5 минут
3	URL		Среднее время ответа в разрезе операций	Среднее время ответа поставщиков за 5 минут в разрезе операций
4	URL		Общее количество обрабатываемых операций в сутки	Общее количество обрабатываемых операций в сутки.

5	URL		<i>Общее количество обрабатываемых операций в секунду</i>	<i>Общее количество обрабатываемых операций в секунду.</i>
6	URL		<i>Объем операций на этапе "Подготовка" больше 3 секунд больше 90%</i>	<i>Объем операций на этапе "Подготовка" больше 3 секунд больше 90%.</i>

3.6. Требования к журналированию

Требования к протоколированию, ведению, хранению и удалению журналов (логов) и протоколов работы, как минимум, тех функций, которые описаны в разделе 3.1 настоящего документа, а также требования к протоколированию работы реализующих эти функции внутренних частей, механизмов, элементов системы. Могут включать ведение логов и журналов для целей аудита информационной безопасности, если отдельно не приведено в разделе «Требования к информационной безопасности» ниже.

4. НЕФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

Нефункциональные требования (НФТ) – требования, определяющие показатели производительности, отказоустойчивости, надежности и допустимой нагрузки сервиса на омниканальной платформе. т.е. в каких условиях и как выполняются функциональные требования. Примеры: Целевой уровень доступности ИС - 99,9%, RTO - 8 часов, RPO - 1 день

4.1. Требования к производительности (быстродействию)

Требуемая скорость работы, в том числе скорость отработки различных пользовательские операции с учетом ограничений по потреблению, например: скорость входа, скорость ответа страницы, скорость обработки запроса и т.д.

4.2. Требования к нагрузке

Ожидаемые показатели нагрузки, при которых работа должна быть стабильной, например: число одновременно работающих пользователей, объем транзакций, объем передаваемых данных и т.д.

4.3. Требования доступности и надежности

4.3.1. Класс критичности

Mission Critical System (MC) – критически важная ИС - ИС, обеспечивающая функционирование критически важных (Mission Critical) бизнес-сервисов (процессов) Организации, прерывание которых в краткосрочном промежутке времени (до 8 часов) может привести к существенному (вплоть до фатального) финансовому и/или репутационному и/или регуляторно-правовому ущербу для Организации.

Business Critical System (BC) – основная ИС – ИС, обеспечивающая функционирование основных (Business Critical) бизнес-сервисов (процессов) Организации прерывание которых в среднесрочном периоде (от 8 до 24 часов) может привести к существенному (вплоть до фатального) финансовому и/или репутационному и/или регуляторно-правовому ущербу для Организации, однако в кратковременном промежутке (до 8 часов) Организации может выполнять свои обязательства перед клиентами с незначительным снижением качества бизнес-сервиса.

Business Operational System (BO) - обеспечивающая ИС - ИС, обеспечивающая функционирование обеспечивающих (Business Operational) бизнес-сервисов (процессов) Банка, прерывание которых на срок от 24 часов до 2-х недель создает значительные неудобства пользователям, при этом внутренние процессы Банка, поддерживаемые данной ИС, не направленные на обслуживание клиентов, могут быть заблокированы, при этом простой обеспечивающих (Business Operational) бизнес-сервисов (процессов) Банка в среднесрочном периоде (от 8 до 24 часов) не влечет за собой финансовый и/или репутационный и/или регуляторно-правовой ущерб для Банка.

Указать класс критичности ИС/ПС: Mission Critical, Business Critical, Business Operational, Other (Office Productivity)

4.3.2. Прочие требования

Иные требования к доступности и/или надежности.

Использовать формулировку "В соответствии с классом критичности" или перечислить и обосновать список конкретных выдвигаемых требований (целевая доступность в %, RTO/RPO, автомасштабирование, георезервирование, Stand-In, шардирование, симметричность контуров и др.)

4.4. Регламенты и стандарты

Требования от внутренних и внешних регламентов, стандартов, которые должны быть учтены. Рекомендуется указывать не только ссылку на документ, но и что именно / какой раздел из документа должен быть учтён.

4.5. Требования к качеству данных

Заполняется по необходимости.

- Качество данных определяется степенью соответствия следующим критериям:
- точность и достоверность данных: отсутствие синтаксических и семантических ошибок в данных, а также их соответствие реальным и статистически наиболее вероятным значениям свойств, характеристик и параметров, зафиксированных в данных;
- полнота данных - достаточность:
 - объема данных (количества записей),
 - глубины данных (периода данных, необходимого для целей бухгалтерского, аналитического и/или управленческого учета и применяемого в моделях оценки риска, а также для формирования и направления отчетности в надзорные органы)
 - широты данных (охвата данными всех разрезов, свойств и характеристик сущностей, которые используются в бухгалтерском,

аналитическом и/ или управленческом учете и применяются в моделях оценки риска, а также для формирования и направления отчетности в надзорные органы);

- актуальность данных: обязательность фиксирования данных на дату для использования в целях бухгалтерского, аналитического и/ или управленческого учета, и/ или применения в моделях оценки риска, а также для формирования и направления отчетности в надзорные органы;
- своевременность данных: доступность актуальных данных в нужное Потребителю данных время, в соответствии с выполняемыми им функциями;
- согласованность данных: взаимная непротиворечивость данных, хранящихся во всех внутренних ИС Банка, в том числе обеспечивающих бухгалтерский учет, и во всех доступных Банку внешних ИС и иных источниках информации, в том числе в документах на бумажных носителях, а также целостность соответствующих идентификационных ссылок в структурах баз данных;
- доступность данных: возможность использования данных в существующей форме представления.

4.6. Прочие нефункциональные требования

В данный раздел могут быть добавлены, при их наличии, прочие нефункциональные требования (такие, как рекомендации / ограничения по архитектуре, протоколирование, совместимость, API / квоты, целостность, масштабируемость и др.).

5. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Требования, направленные на защиту от несанкционированного доступа, вредоносного кода, атак злоумышленников и т.п., например, требования по идентификации, аутентификации и авторизации пользователей. Описываются в табличном формате и должны содержать, если применимо:

- Аудиту (в том числе, если требуется дополнение к разделу «Требования к журналированию»);
- Программно-аппаратному комплексу для обеспечения безопасности;
- Идентификации / аутентификации / авторизации;
- защите от несанкционированного доступа;
- Антивирусной защите;
- Тестированию безопасности;
- защите от вредоносного кода;
- Паролям;
- Электронным подписям / сертификатам;
- Мониторингу безопасности;
- Управлению сессиями;
- Входным / выходным данным;
- Криптографии;

- Защищённым портам и протоколам.