ТРЕБОВАНИЯ К РЕШЕНИЯМ ПАРТНЕРОВ

ДОПОЛНЕНИЕ К ПРАВИЛАМ ПАРТНЕРСКОЙ ПРОГРАММЫ

Оглавление

Термины и определения

Авторизация — процесс проверки и подтверждения прав Корпоративного клиента на доступ в систему «Сбербанк Бизнес Онлайн» (СББОЛ), включающий в себя идентификацию и аутентификацию Корпоративного клиента в соответствии с порядком, предусмотренным Договором ДБО.

Аккредитация — комплекс проверочных мероприятий, осуществляемых Оператором в отношении Участника (потенциального Участника), необходимый для присоединения Участника к Программе.

Анкета Участника — форма для внесения сведений об Участнике, направляемая Оператору с целью прохождения Аккредитации и присоединения к Программе.

АС – автоматизированная система**.**

Банк — Публичное акционерное общество «Сбербанк России», ПАО Сбербанк (запись в ЕГРЮЛ внесена Управлением ФНС России по г. Москве 16 августа 2002г., ОГРН 1027700132195, ИНН 7707083893, место нахождения: 117997, г. Москва, ул. Вавилова, д. 19). Генеральная лицензия Банка России на осуществление банковских операций №1481 от 11.08.2015.

БД – база данных.

Договор ДБО — Договор предоставления услуг с использованием системы дистанционного банковского обслуживания ПАО Сбербанк юридическим лицам, индивидуальным предпринимателям и физическим лицам, занимающимся частной практикой в порядке, установленном действующим законодательством Российской Федерации, заключаемый путем присоединения к соответствующим условиям в СББОЛ или путем подписания отдельного договора.

Злоупотребление Правилами — действия Участника, противоречащие Правилам Программы, расцениваемые Банком как недобросовестные, мошеннические, обман и т.п., которые повлекли или могут повлечь возникновение каких-либо убытков Оператора и/или Банка, потерю деловой репутации Оператора и/или Банка и/или Участников.

Корпоративный клиент — юридическое лицо (резидент Российской Федерации), не являющееся кредитной организацией, или индивидуальный предприниматель (резидент Российской Федерации), или физическое лицо, занимающееся частной практикой в соответствии с действующим законодательством РФ, заключившие с Банком договор на расчетно-кассовое обслуживание, Договор ДБО и являющиеся пользователями Системы «Сбербанк Бизнес Онлайн» (СББОЛ).

Оператор — Общество с ограниченной ответственностью «Сбер Бизнес Софт», ООО «Сбер Бизнес Софт» (ОГРН 1217700484814, ИНН 7730269550, место нахождения: 121170, г. Москва, вн.тер.г. муниципальный округ Дорогомилово, пр-кт Кутузовский, д. 32, к. 1, помещ. 7.С.18).

Правила — настоящий документ, определяющий условия и порядок участия в Программе. Правила Программы размещаются на странице в сети «Интернет»:https://sberbp.ru/conditions.

Программа — программа, направленная на стимулирование активности ее Участников в развитии современных информационных технологий, использовании передовых технологических решений, в том числе реализуемых Банком и/или компаниями Экосистемы Сбербанка.

ПСИ – приемо-сдаточные испытания.

Система «Сбербанк Бизнес Онлайн» / «СберБизнес» (СББОЛ) — автоматизированная система дистанционного обслуживания клиентов (комплекс программно-аппаратных средств) Банка через сеть «Интернет», размещенная на официальном ресурсе https: https://www.sberbank.ru/ru/s_m_business/new_sbbol.

Страница Программы — страница в сети «Интернет», размещенная по адресу: https://sberbp.ru.

Уполномоченное лицо Участника — индивидуальный предприниматель или лицо, занимающееся в установленном действующим законодательством РФ порядке частной практикой, действующий(ее) от своего имени, или уполномоченное Корпоративным клиентом физическое лицо (уполномоченный представитель), действующее от имени Клиента, или лицо - единоличный исполнительный орган Корпоративного клиента, обладающее правом, предоставленным на основании уставных документов или наделенное правом Корпоративным клиентом на совершение сделки, направленной на присоединение к Правилам Программы (подключение Программы), осуществление прав и обязанностей в рамках Программы, включая осуществление операций, предусмотренных Правилами, а так же правом прекращения участия в Программе (отключения Программы).

Участник Программы (Участник) — юридическое лицо или индивидуальный предприниматель или физическое лицо, занимающееся частной практикой в соответствии с действующим законодательством РФ, присоединившееся к Программе и прошедшее Аккредитацию в соответствии с Правилами.

Требования к решениям партнеров

1. Требования к взаимодействию

1.1. Общие положения

1.1.1. Услуги

1.1.1.1. Оператор не является Участником программы, не оказывает услуги контрагентам по выполнению их бизнес-требований.

1.1.2. Ответственность

1.1.2.1. Оператор не несет ответственность за качество оказанных услуг Участником Программы контрагенту.

1.2. Защита интересов контрагентов

1.2.1. Формирование коммерческого предложения.

1.2.1.1. В случае невозможности Участника полностью выполнить бизнес-требования потенциального клиента, при отправке коммерческого предложения Участник обязан явно указать отдельные пункты, не соответствующие указанным бизнес-требованиям.

1.2.1.2. Участник обязуется составить коммерческое предложение в течение 10 (десяти) рабочих дней с момента получения бизнес-требований от потенциального клиента.

1.2.2. Изменение возможностей Участников

1.2.2.1. В случае, если Участник вынужден внести изменения в коммерческое предложение до его согласования (начала формирования технического задания) по обстоятельствам, находящимся в его сфере ответственности (например, ошибки в расчетах и т.п.), потенциальные клиенты должны быть уведомлены о таких изменениях в течение 3 (трех) рабочих дней с момента обнаружения указанных обстоятельств.

1.2.2.2. В случае, если Участник вынужден внести изменения в коммерческое предложение до его согласования (начала формирования технического задания) по обстоятельствам, не находящимся в его сфере ответственности (форс-мажор), потенциальные клиенты должны быть уведомлены о таких изменениях в течение 3 (трех) рабочих дней с момента обнаружения указанных обстоятельств.

1.2.2.3. В случае, если Участник вынужден внести изменения в коммерческое предложение после его согласования (начала формирования технического задания) по обстоятельствам, находящимся в его сфере ответственности (например, ошибки в расчетах и т.п.), потенциальные клиенты должны быть уведомлены о таких изменениях в течение 3 (трех) рабочих дней с момента обнаружения указанных обстоятельств.

1.2.2.4. В случае, если Участник вынужден внести изменения в коммерческое предложение после его согласования (начала формирования технического задания) по обстоятельствам, не находящимся в его сфере ответственности (форс-мажор), потенциальные клиенты должны быть уведомлены о таких изменениях в течение 3 (трех) рабочих дней с момента обнаружения указанных обстоятельств.

1.2.2.5. При неизменности бизнес-требований потенциального клиента или контрагента Участник не вправе изменять стоимостную оценку проекта в течение 1 (одного) месяца с даты направления коммерческого предложения.

1.3. Защита интересов Участников

1.3.1. Изменение бизнес-требований потенциальных клиентов

1.3.1.1. В случае изменения бизнес-требований потенциального клиента или контрагента по истечении 1 (одного) месяца с даты направления коммерческого предложения, Участник вправе изменять стоимостную оценку проекта.

1.3.1.2. Все изменения после начала проекта, датой которого считается подписание Договора Сторонами, требуют заключения дополнительного соглашения и не являются поводом для неприема работы Участника.

1.3.1.3. В случае спора по прямым договорным отношениям спор подлежит рассмотрению в соответствии с Гражданским Кодексом Российской Федерации.

1.4. Требования к осуществлению коммуникаций

1.4.1. Ясность и конкретность

1.4.1.1. Стороны соглашаются, что все требования, сроки, задачи и ожидания должны быть ясно и конкретно сформулированы в письменной форме.

1.4.1.2. В случае неоднозначностей или непонимания, Стороны обязуются обратиться друг к другу для получения уточнений и разъяснений.

1.4.2. Учет языковых и культурных различий

1.4.2.1. В случае, если Стороны представляют разные культуры или говорят на разных языках, они обязуются учитывать эти различия и проявлять взаимное уважение и терпимость.

1.4.2.2. При необходимости, Стороны могут использовать переводчиков или другие специализированные инструменты для облегчения понимания и коммуникации.

1.4.3. Регулярные обновления

1.4.3.1. Исполнители обязуются предоставлять регулярные обновления заказчикам относительно прогресса работы в установленные сроки.

1.4.3.2. Обновления могут осуществляться в форме письменных отчетов, устных презентаций, видеоконференций или других согласованных методов связи.

1.4.4. Каналы коммуникации

1.4.4.1. Стороны имеют право выбирать согласованный между ними канал связи на протяжении выполнения работ по проекту.

1.4.4.2. В случае проведения коммуникации за пределами контура Страницы Программы, Стороны должны направить Оператору по адресу: accred@sberbp.ru разработанный в ходе работы над проектом Договор в срок, не превышающий 1 (один) рабочий день с момента подписания Договора.

1.4.5. Ответственность и своевременность

1.4.5.1. Стороны признают свою ответственность за своевременное и полное предоставление информации и ответов на запросы другой Стороны.

1.4.5.2. В случае возникновения задержек или изменений в планах, Стороны обязуются незамедлительно информировать друг друга и согласовывать соответствующие корректировки.

1.4.6. Документирование

1.4.6.1. Стороны соглашаются на документирование всех соглашений, принятых решений и изменений, связанных с процессом коммуникации.

1.4.6.2. Документирование может осуществляться путем ведения протоколов, составления отчетов или другими согласованными способами.

2. Требования к качеству разработки и интеграции

2.1. Общие положения

2.1.1. Соответствие регуляторным документам и стандартам

2.1.1.1. Участник обязуется разработать программное обеспечение в полном соответствии с применимыми регуляторными документами и стандартами, действующими на момент выполнения работ.

2.1.1.2. Регуляторные документы и стандарты включают, но не ограничиваются следующими:

- национальные и международные нормативно-правовые акты, законы, постановления, директивы, стандарты и другие аналогичные документы, которые применимы к разработке, тестированию, внедрению и эксплуатации программного обеспечения;
- отраслевые и профессиональные стандарты, рекомендации и методы, связанные с программным обеспечением и его функциональностью, безопасностью, качеством и производительностью;
- требования, установленные государственными органами, регуляторами, лицензионными и сертификационными организациями, включая, но не ограничиваясь требованиями безопасности, защиты данных, конфиденциальности и этическими стандартами.

2.1.1.3. Контрагент обязуется предоставить Участнику необходимые и достоверные регуляторные документы и стандарты, которые применимы к проекту, в разумные сроки после заключения договора.

2.1.1.4. Участник вправе просить уточнения или дополнительные материалы, если таковые не были предоставлены или в случае изменения действующих регуляторных документов и стандартов в течение выполнения работ.

2.1.1.5. В случае, если в ходе разработки программного обеспечения выявляются несоответствия между требованиями регуляторных документов и стандартов, Участник и контрагент обязуются провести консультации и принять согласованные решения относительно внесения изменений в программное обеспечение или обновления требований.

2.1.1.6. Участник гарантирует, что разработанное программное обеспечение будет соответствовать применимым регуляторным документам и стандартам на момент его передачи Исполнителю, за исключением случаев, когда контрагент вносит изменения или несогласованные модификации после начала работ.

2.1.1.7. Контрагент имеет право провести проверку программного обеспечения на соответствие регуляторным документам и стандартам до его приемки. В случае выявления несоответствий, Контрагент вправе требовать исправления этих несоответствий Участником без дополнительной оплаты.

2.1.1.8. Все изменения и дополнения к регуляторным документам и стандартам, которые могут повлиять на разработанное программное обеспечение, должны быть внесены посредством дополнительных соглашений между Сторонами.

2.1.1.9. Все споры и разногласия, возникающие из-за несоответствия разработанного программного обеспечения регуляторным документам и стандартам, будут разрешаться путем переговоров между Сторонами. В случае невозможности достижения согласия, споры подлежат рассмотрению в судебном порядке в соответствии с действующим законодательством.

2.1.2. Процесс разработки и интеграции

Требования к компонентам АС.

- Сервера БД должны быть объединены в отказоустойчивый кластер;
- В АС должна быть реализована возможность георезервирование для всех компонентов решения;
- Система должна обеспечивать возможность резервного копирования данных без остановки и замедления АС или её компонентов;
- В АС должны отсутствовать компоненты, расположенные на одном КТС;
- Все внешние интеграции должны быть реализованы через промежуточный proxy;
- Все интеграции, в том числе и внутренние, должны использовать MTLS1.2, не ниже;
- Стенд ТЕСТ (ИФТ/ПСИ) должен быть точной копией стенда ПРОМ в части архитектуры и набора компонентов. Стенд ТЕСТ может быть меньшей мощности;
- Все программные компоненты должны иметь актуальные на момент публикации версии;
- Компоненты АС должны иметь возможность масштабирования без внесения изменения АС;
- Парольная политика для всех пользователей должна соответствовать требованиям Оператора. Также должна быть организована защита от перебора;
- В АС должны отсутствовать компоненты/библиотеки имеющие известные уязвимости;
- Все входящие данные должны проходить контроль на соответствие разрешенному формату и валидацию на соответствие содержимого и используемым

символам (в частности, должна быть организована защита от SQL-инъекций и атак Cross-site scripting;

- Наличие двухфакторной аутентификации для всех пользователей АС;
- В случае возникновения ошибок в АС, пользователю должна предоставляться только общая информация;
- Поддержка /healtchcheck эндпоинта, 200 – сервис работает, остальные статусы – нет.

Требования к Базам данных

БД должна поддерживать версионность. Новая версия БД должна обеспечивать возможность работы с приложениями предыдущей версии. При этом должны успешно выполняться все функции приложений, успешно выполнявшиеся на БД предыдущей версии. Результаты выполнения функций на текущей и предыдущей версиях БД должны быть идентичны. Наличие и доступность данных в приложениях должны быть обеспечены в том же объеме, что и при работе приложений с БД предыдущей версии.

Должно быть реализовано шифрование критичных данных.

Должна быть реализована ролевая модель.

Требования к бэкапированию и хранению данных

- Хранение бэкапа должно быть реализовано в зашифрованном виде.
- Резервные копии должны быть защищены от изменений.
- Хранение бэкапа должно быть реализовано на отдельном КТС.

Требование к логированию.

Сервисы АС должны обеспечивать отправку логов в logstash (часть стека ELK).

Параметры подключения АС к серверу logstash должны задаваться в переменной окружения logging.proxy.hosts и загружаться в момент старта/перезапуска Бэкенда. Если logstash недоступен для записи логов, это не должно влиять на работу приложения.

Список обязательных полей, отправляемых в logstash:

Поле	Описание
message	Текст сообщения
level	Уровень логирования
logger_name	Название логгера, отправившего событие
service_name	Название сервиса(например saas-sbercrm-dikorosi-service)
@timestamp	Время события
@version	Версия формата сообщения
traceId	Идентификатор трассировки
spanId	Идентификатор отдельных запросов

Все действия пользователей должны логироваться в полном объеме, в соответствии с требованиями к событиям аудита:

- Обеспечить безопасность ведения журнала подсистемы таким образом, чтобы исключить возможность его несанкционированной модификации как путем штатных действий в рамках системы, так и извне.
- Исключить возможность редактирования, отключения и удаления журнала аудита средствами системы, а также его импортирования в систему из какого-либо источника.
- Наличие в журнале аудита чувствительных данных (пароли пользователей, данные платежных карт и т.п.) должно быть исключено.
- Информация в журнале подсистемы аудита должна представляться в структурированном виде.
- При протоколировании событий в журнале аудита АС должно фиксироваться время (в формате UTC с точностью до секунды) прикладного сервера, т.е. сервера приложений.
- Возможность доступа к данным аудита должна предоставляться только уполномоченным пользователям.
- Должен обеспечиваться контроль целостности архивных журналов аудита, в том числе защита от ошибочных или преднамеренных действий администраторов АС.
- При достижении журналом первого порогового значения объема, определенного параметрами системы, администратору системы должно выдаваться соответствующее предупреждение.
- Система должна фиксировать старые и новые значения изменяемых пользовательских атрибутов.
- Должна быть обеспечена передача событий аудита в сторонние системы с поддержкой защищенного авторизованного соединения.

2.1.2.1. Участник обязуется выполнять процесс разработки и интеграции программного обеспечения в соответствии с высокими стандартами качества, с целью достижения оптимальной функциональности, надежности и удовлетворения требований контрагента.

2.1.2.2. Стандарты качества задаются самостоятельно Сторонами договора. В противном случае, регулируются международными стандартами:

- ISO/IEC 9126;
- ISO/IEC 25000;
- ISO/IEC/IEEE 12207:20081;
- ISO/IEC/IEEE 15289:2011.

2.1.2.3. Качество процесса разработки и интеграции программного обеспечения должно соответствовать следующим требованиям:

- документирование требований: Участник обязуется документировать и уточнять требования контрагента к программному обеспечению в течение всего процесса разработки и интеграции. Документация должна быть ясной, полной, точной и удовлетворять согласованным стандартам.
- планирование и управление проектом: Участник должен разработать и соблюдать план работы, включающий определение этапов разработки, установку реалистичных сроков, а также контроль и отчетность о прогрессе выполнения работ. Участник также должен предоставлять контрагенту регулярные отчеты о статусе проекта. Срок передачи отчетов согласовывается Сторонами.
- соблюдение передовых методологий: Участник должен применять передовые методологии разработки, такие как Agile, V-Model, Incremental Model, RAD Model, Iterative

Model, Spiral Model или другие признанные стандарты, в зависимости от характера проекта и согласования с контрагентом;

- тестирование и отладка: Участник должен проводить тестирование программного обеспечения на всех этапах разработки и интеграции, включая модульное тестирование, интеграционное тестирование, системное тестирование и приемочное тестирование. Все выявленные ошибки и дефекты должны быть исправлены и проверены перед передачей программного обеспечения контрагенту;
- безопасность: Участник обязуется уделять особое внимание аспектам безопасности в процессе разработки и интеграции программного обеспечения. Все меры безопасности, необходимые для защиты данных и предотвращения несанкционированного доступа, должны быть учтены и реализованы. Требования по обеспечению безопасности определены в разделе 3 настоящего Документа.

2.1.2.4. Контрагент имеет право провести независимую проверку качества процесса разработки и интеграции программного обеспечения в период времени, согласованный Сторонами. В случае выявления несоответствий требованиям качества, контрагент вправе требовать от Участника принятия корректирующих мер и устранения дефектов без дополнительной оплаты.

2.1.3. Инструменты разработки и интеграции

2.1.3.1. Исполнитель обязуется использовать при разработке и интеграции программного обеспечения передовые методы и инструменты, с целью обеспечения высокого качества и эффективности работ.

2.2. Функциональные требования

2.2.1. Взаимодействие с другими системами или компонентами

2.2.1.1. Разработанный Участником продукт должен обладать совместимостью с операционными системами и оборудованием, указанными в бизнес-требованиях контрагента.

2.2.1.2. Продукт обязан демонстрировать высокую эффективность при обработке указанных в бизнес-требованиях контрагента типов данных и объемов данных.

2.3. Нефункциональные требования

2.3.1. Производительность

2.3.1.1. Участник должен выбирать и реализовывать эффективные алгоритмы и структуры данных, чтобы обеспечить оптимальную производительность программного обеспечения.

2.3.1.2. Участник должен обращать внимание на оптимизацию использования памяти в программном обеспечении: минимизировать использование памяти, устранять утечки памяти и оптимизировать процессы выделения и освобождения памяти.

2.3.1.3. Участник должен проводить тестирование производительности программного обеспечения для выявления узких мест и определения возможных улучшений.

2.3.1.4. Участник должен стремиться к оптимизации использования ресурсов во время работы разрабатываемого в рамках проекта программного обеспечения, таких как процессорное время, память, сетевые ресурсы и дисковое пространство.

2.3.2. Надежность и доступность

2.3.2.1. Участник должен предусмотреть механизмы предотвращения, обработки и восстановления от ошибок и исключительных ситуаций.

2.3.2.2. Участник должен предусмотреть механизмы мониторинга и логирования для отслеживания работы программного обеспечения и выявления проблем.

2.3.2.3. Участник должен предусмотреть механизмы резервного копирования и восстановления данных, чтобы обеспечить их сохранность и доступность.

2.3.3. Безопасность и защита данных

2.3.3.1. Участник должен обеспечить выполнение требований по кибербезопасности разработанного продукта. Полные требования по кибербезопасности приведены в разделе 3 настоящего Документа.

2.3.4. Удобство использования

2.3.4.1. Программное обеспечение должно иметь интуитивно понятный и легко осваиваемый пользовательский интерфейс.

2.3.4.2. Элементы управления и функциональность программы должны быть логически организованы и соответствовать ожиданиям пользователя.

2.3.4.3. Программное обеспечение должно быть разработано с учетом эргономических принципов, обеспечивающих комфортное использование для различных категорий пользователей.

2.3.4.4. Программное обеспечение должно предоставлять возможности настройки и персонализации в соответствии с потребностями пользователя.

2.3.4.5. Участник должен обеспечить удобство установки обновлений программного обеспечения, включая автоматическое обновление, если применимо.

2.3.4.6. Исправление ошибок и устранение дефектов должно осуществляться оперативно и предоставляться в виде патчей или новых версий программы

2.3.5. Сопровождение и расширяемость

2.3.5.1. Программное обеспечение должно быть разработано Участником с учетом принципов модульности и разделения ответственности, чтобы обеспечить возможность легкого внесения изменений и добавления новых функций.

2.3.5.2. Требования по сопровождению и расширяемости программного обеспечения должны соответствовать следующим нормативным документам:

- Статья 1270 ГК РФ;
- Статья 1280 ГК РФ.

2.3.5.3. Участник должен предусмотреть документацию, объясняющую архитектуру, принципы работы и способы расширения системы.

2.4. Требования к тестированию и контролю качества

2.4.1. Планирование тестирования

2.4.1.1. Участник обязан разработать план тестирования, четко определяющий, какие аспекты программного обеспечения будут подвергнуты тестированию. План тестирования должен удовлетворять требованиям:

- план тестирования должен четко определять цели и ожидаемые результаты тестирования;
- план тестирования должен определить критерии, по которым будет оцениваться успешное завершение тестирования и готовность программного обеспечения к принятию;
- цели тестирования могут включать обнаружение дефектов, проверку соответствия требованиям, оценку производительности и надежности программного обеспечения;
- тестирование должно охватывать различные функциональные и нефункциональные требования, а также возможные сценарии использования.

2.4.1.2. Стратегия тестирования может включать модульное тестирование, интеграционное тестирование, системное тестирование, нагрузочное тестирование и другие формы тестирования.

2.4.2. Тестовая документация

2.4.2.1. Участник должен создать необходимую тестовую документацию, такую как тестовые сценарии, тест-кейсы, наборы тестовых данных и описание ожидаемых результатов.

2.4.2.2. Документация должна быть полной, понятной и доступной для всех участников процесса тестирования.

2.4.2.3. Документация должна опираться, но может не ограничиваться нормативными документами:

- IEEE 829-2008;
- ISO/IEC 29119;
- ISO/IEC/IEEE 29119-3:2013.

2.4.3. Исполнение тестов

2.4.3.1. Тестирование должно быть выполнено в соответствии с запланированными методами и процедурами.

2.4.3.2. Разработчик должен проверить функциональность, производительность, надежность и безопасность программного обеспечения.

2.4.4. Регистрация и анализ дефектов

2.4.4.1. Разработчик должен зарегистрировать все найденные дефекты и проблемы в системе отслеживания дефектов.

2.4.4.2. Дефекты должны быть анализированы, классифицированы по приоритету и исправлены в соответствии с процедурами управления дефектами.

2.4.5. Проверка качества

2.4.5.1. Участник должен осуществить проверку качества программного продукта перед его поставкой.

2.4.5.2. Верификация и валидация программного обеспечения должны быть проведены для проверки соответствия требованиям и корректности его работы.

2.4.6. Документация и отчетность

2.4.6.1. Участник должен подготовить отчет о результатах тестирования, включая информацию о проведенных тестах, найденных дефектах, исправлениях и итоговой оценке качества программного обеспечения.

2.4.6.2. Участник должен подготовить документацию, описывающую процесс тестирования и контроля качества, чтобы обеспечить прозрачность и повторяемость процесса.

2.5. Документация и обучение

По результатам реализации проекта Участник обязуется сформировать следующую сопроводительную документацию:

- Краткую и полную инструкцию по автоматической и ручной установке (в разрезе ролей участников установки и содержать строгий порядок действий).
- Архитектура сервиса (включая описание технического долга, если есть).
- Архитектура АС, включая модель БД с описанием (физическая и логическая схемы).
- Руководство Администратора.
- Руководство пользователя.
- Руководство Бизнес-Администратора
- Описание доработок (фичи/истории)

2.5.1. Требования к документации

2.5.1.1. Разработчик программного обеспечения должен составить полную документацию, которая описывает все функции, возможности и настройки программного обеспечения.

2.5.1.2. Документация должна удовлетворять требованиям:

- должна быть понятной для пользователей с различным уровнем технической подготовки и предоставлять подробные инструкции по установке, настройке и использованию программы;
- должна быть логически структурирована и иметь четкое оглавление и навигацию, чтобы пользователи могли быстро найти нужную информацию;
- должна быть разбита на разделы, такие как введение, установка, настройка, руководство пользователя и т. д., помогает организовать информацию и улучшить ее доступность;
- должна содержать информативные примеры использования программного обеспечения и реальные сценарии работы;

и прочим, предусмотренным в Договоре Сторон.

2.5.2. Обучение пользователей и администраторов

2.5.2.1. Разработчик программного обеспечения должен предоставить обучающие материалы, такие как видеоуроки, учебные курсы или онлайн-документацию, чтобы помочь пользователям освоить программу.

2.5.2.2. Обучающие материалы должны быть структурированы, информативны и доступны для пользователей с разным уровнем знаний и навыков.

2.5.2.3. Участник должен предоставить каналы поддержки и консультаций, где пользователи могут задавать вопросы, сообщать об ошибках и получать помощь в использовании программного обеспечения.

2.5.2.4. Участник должен обеспечить актуализацию документации при выпуске новых версий программы или внесении значительных изменений.

2.5.2.5. Участник должен провести оценку понятности документации, например, путем тестирования на представителях целевой аудитории, чтобы убедиться, что она ясна и понятна для пользователей.

2.5.2.6. В случае изменений или дополнений к программе Участником должна быть обновлена соответствующая документация.

2.6. Оценка качества и приемка

2.6.1. Процедуры контроля качества

2.6.1.1. Участник должен разработать план контроля качества, который определяет методы, инструменты и ресурсы, необходимые для контроля качества программного обеспечения.

2.6.1.2. Программное обеспечение должно быть протестировано на соответствие функциональным требованиям.

2.6.2. Процедуры приемки

2.6.2.1. Участник должен предоставить полную и понятную документацию по программному обеспечению, включая описание функциональности, руководства пользователя, инструкции по установке и настройке, требования к системе и другие необходимые материалы.

2.6.2.2. При приемке программного обеспечения должна проводиться проверка его функциональности в соответствии с требованиями и спецификациями.

2.6.2.3. Контрагент полностью берет на себя ответственность по приемке разработанного программного обеспечения.

2.6.2.4. В случае обнаружения недостатков в программном обеспечении, которые противоречат требованиям, изложенным в Договоре, Участник обязан устранить такие недостатки без дополнительной оплаты в установленный срок, определенный при заключении дополнительного соглашения.

2.6.2.5. В случае выявления недостатков в программном обеспечении, которые не противоречат требованиям, изложенным в Договоре, Участник обязан устранить такие недостатки в установленный срок и в соответствии с оплатой, определенной при заключении дополнительного соглашения.

2.7. Гарантии и поддержка

2.7.1. Гарантийные обязательства

2.7.1.1. Участник должен гарантировать, что программное обеспечение будет функционировать в соответствии с описанными функциональными требованиями и спецификациями.

2.7.1.2. Участник должен гарантировать, что программное обеспечение соответствует установленным стандартам, нормам и регулятивным требованиям.

2.7.1.3. Участник должен гарантировать, что программное обеспечение будет иметь высокое качество и работать без существенных дефектов.

2.7.1.4. Участник должен гарантировать обеспечение регулярных обновлений и патчей для программного обеспечения, чтобы исправлять ошибки, улучшать функциональность и обеспечивать совместимость с новыми окружениями.

2.7.1.5. Участник должен гарантировать безопасность программного обеспечения, включая защиту от внешних угроз, уязвимостей и несанкционированного доступа.

2.7.1.6. Участник должен гарантировать выполнение работ в установленные сроки и согласно договору или соглашению между сторонами.

2.7.2. Техническая поддержка

2.7.2.1. Участник должен обеспечить доступность технической поддержки для пользователей программного обеспечения.

2.7.2.2. Участник быть отзывчивым и оперативно отвечать на запросы пользователей.

2.7.2.3. Участник должен предоставить полную и понятную документацию и руководства пользователя для программного обеспечения.

2.7.2.4. Участник должен предоставить систему регистрации и отслеживания запросов на поддержку, чтобы обеспечить структурированное и системное решение проблем пользователей.

2.7.2.5. Участник может предлагать разные уровни технической поддержки в зависимости от потребностей пользователей и их условий обслуживания.

3. Требования к обеспечению кибербезопасности

3.1. Идентификация и аутентификация

3.1.1.1. Участник обязуется внедрить механизмы идентификации и аутентификации для контроля доступа к системе и ограничения прав пользователей в рамках выполняемого проекта, если иное не оговорено с контрагентом.

3.1.1.2. Участник обязуется довести до сведения контрагента важность использования сильных паролей и многофакторной аутентификации для защиты учетных записей в рамках выполняемого проекта.

3.2. Управление доступом

3.2.1.1. Участник обязуется реализовать систему управления доступом, обеспечивающей назначение прав доступа в соответствии с ролевой моделью и принципом наименьших привилегий в рамках выполняемого проекта, если иное не оговорено с контрагентом.

3.2.1.2. Участник обязуется проводить постоянный мониторинг и аудит доступа к системе для выявления и реагирования на подозрительные активности в рамках выполняемого проекта, если иное не оговорено с контрагентом.

3.3. Защита данных

3.3.1.1. Участник обязуется обеспечить шифрование конфиденциальных данных при их передаче и хранении в рамках выполняемого проекта, если иное не оговорено с контрагентом.

3.3.1.2. Участник обязуется проводить регулярное создание резервных копий данных для предотвращения потери информации и возможности восстановления системы в случае сбоя в рамках выполняемого проекта, если иное не оговорено с контрагентом.

3.4. Мониторинг и обнаружение инцидентов

3.4.1.1. Участник обязуется внедрить системы мониторинга, которые отслеживающих и анализирующих активности в сети с целью обнаружения и предотвращения инцидентов безопасности в рамках выполняемого проекта, если иное не оговорено с контрагентом.

3.4.1.2. Участник обязуется создать процедуры реагирования на инциденты и планов континуитета бизнеса для эффективного управления и быстрого реагирования на угрозы в рамках выполняемого проекта, если иное не оговорено с контрагентом.

Требования к ИТ мониторингу в АС.

ИТ мониторинг должен быть предназначен для контроля работоспособности АС администраторами АС и администраторами из состава дежурной смены.

Полнота мониторинга определяется покрытием метриками всех межкомпонентных (внутри АС) и межсистемных (со смежными АС) взаимодействий.

Визуальные представления должны быть реализованы в виде схемы всех межкомпонентных (внутри АС) и межсистемных (со смежными АС) взаимодействий со светофорами работоспособности (красный, желтый, зеленый)

Сигнализация о проблемах должна производиться красным светофором на визуальном представлении, направлять СМС и почтовое сообщение.

Метрики должны быть реализованы в разрезе каналов поступления информации – потребителей и АПИ, в противном случае неработоспособность одной АПИ или одного потребителя может быть не заметна на общем фоне работы АС.

Вывод нового функционала в эксплуатацию должен быть синхронизирован с разработкой и визуализацией метрик по новому функционалу в разных типах представлений (ИТ мониторинг и Бизнес мониторинг).

Требования к Бизнес-мониторингу АС.

Необходимо реализовать инструменты, позволяющие владельцу продукта или ответственному в бизнес-подразделении в режиме on-line следить за работой процесса/сервиса. Для этого одновременно с реализацией бизнес функционала реализуются метрики, позволяющие в режиме on-line контролировать все этапы работы процесса/сервиса и представление для отображения метрик на экране владельца продукта или ответственного в бизнес-подразделении.

Сигнализация о проблемах должна производиться красным светофором на визуальном представлении, направлять СМС и почтовое сообщение.

Вывод нового функционала в эксплуатацию должен быть синхронизирован с разработкой и визуализацией метрик по новому функционалу в разных типах представлений (ИТ мониторинг и Бизнес мониторинг).

3.5. Обновления и патчи

3.5.1.1. Участник обязуется проводить регулярное обновление и установку патчей для операционной системы, прикладного программного обеспечения и других компонентов системы для устранения известных уязвимостей и обеспечения безопасности в рамках выполняемого проекта, если иное не оговорено с контрагентом.

3.6. Тестирование на проникновение

3.6.1.1. Участник обязуется проводить регулярные тесты на проникновение для выявления уязвимостей и проверки эффективности мер безопасности в рамках выполняемого проекта, если иное не оговорено с контрагентом.

3.6.1.2. Участник обязуется выполнять аудит систем и процессов с целью выявления и исправления слабых мест в области безопасности в рамках выполняемого проекта, если иное не оговорено с контрагентом.

3.7. Соблюдение регулятивных требований

3.7.1.1. Участник обязуется соблюдать требования соответствующих регуляторных органов и стандартов безопасности, таких как:

- ГОСТ Р ИСО/МЭК 15408 "Информационная технология. Оценка соответствия. Критерии оценки безопасности информационных технологий";
- ГОСТ Р ИСО/МЭК 27034 "Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке безопасного программного обеспечения";
- ГОСТ Р ИСО/МЭК 27035 "Информационная технология. Методы и средства обеспечения безопасности. Управление информационной безопасностью событий";
- ГОСТ Р ИСО/МЭК 30111 "Информационная технология. Методы и средства обеспечения безопасности. Уязвимость информационной технологии";
- ГОСТ Р ИСО/МЭК 15446 "Информационная технология. Технология защиты информации. Методы и средства разработки и оценки стойкости к воздействию угроз информационных технологий"

и других, в зависимости от применимости.

3.7.1.2. Участник обязуется проводить регулярный аудит соответствия требованиям безопасности и внедрять необходимые меры для соблюдения стандартов.

В рамках реализованного функционала АС категорически запрещается передача:

- Данных без валидации и проверки корректности по схемам валидации;
- Сообщений или вложений, содержащих вирус, архив с паролем или исполняемый файл;
- Состав передаваемой информации должен контролироваться АС-источником.»

- Использование разных кодировок для разных источников входных данных должно быть исключено. Необходимо использовать директивы в заголовках сообщений HTTP, определяющие применяемую кодировку.
- «Для защиты приложения от SQL-инъекций необходимо реализовать валидацию входящих данных. Валидация входящих данных может быть реализована эшелонированной защитой. Для этого необходимо:
- На frontend использовать валидацию данных с помощью регулярных выражений (regexp), например, набора правил OWASP Core Rules. В том числе валидировать данные по ожидаемому формату, например, если ожидалось натуральное число, то проверять это, и не принимать запросы со строкой, нулем или отрицательными числами;
- Интегрировать приложение с WAF (например, ModSecurity);

Требования к передаче данных на backend:

- Использовать параметризированные запросы, при обращении к БД;
- Правильно использовать технологию ORM. Например, в ORM Hibernate нужно использовать именованные параметры вместо конкатенации строк Java.
- Если принять все меры по защите принять невозможно, то стоит рассмотреть их по приоритетам. Важнее и надежнее использовать защиту на backend, далее идет WAF и последним фронт.»

Исполнитель, в целях защиты от Cross-site scripting атак обязуется реализовать следующие требования:

- Передаваемые данные должны быть представлены исключительно как текст;
- После получения от пользователя передаваемых данных и параметров приложения необходимо предварительно привести их к каноническому виду;
- Осуществлять преобразование HTML-кода входного потока данных следующим образом:
  - заменить < > на &lt и >
  - заменить ( ) на &#40 и)
  - заменить # на #
  - заменить & на &
  - В качестве дополнительного метода защиты от Cross-site scripting атак может осуществляться вставка данных в свойство innerText, которое обрабатывает любую информацию как текст (пассивная информация), этот метод можно использовать для построения выходных данных на основе входной информации от пользователя. При этом использование свойства innerHTML является недопустимым, так как данное свойство возвращает текст в виде HTML-кода.
- Также, в качестве дополнительного метода защиты от Cross-site scripting-атак может осуществляться использование метода ValidateRequest, который осуществляет проверку записи HTML кода или сценариев в cookie-файлы (HttpRequest.Cookies), строки запросов (HttpRequest.QueryString) и HTML-формы (HttpRequest.Form);.»
- «Должна выполняться проверка корректности вводимых пользователем данных, причем не только на стороне клиента (с использованием сценариев, исполняемых веб-браузерам), но и на стороне сервера.
- Необходимо запретить пользователю ввод данных, в которых допустимы HTML-теги, например: <IMG>, или <TABLE>, <SCRIPT>, <IFRAME>, <FORM>».
- В случае реализации UI, подразумевающих ввод со стороны не авторизованного пользователя данных, необходимо применение сервиса капчи или сервиса ограничивающий кол-во запросов по цифровому слепку устройства.

- В случаях, если в рамках бизнес-процесса предусмотрен ввод со стороны пользователя строковых данных, эти данные должны быть представлены как текст. Получения данных и параметров приложением необходимо предварительно привести их к каноническому виду, а затем в случае обнаружения в них HTML-тегов, запрещенных символов и т.д. выполнить санитизацию.
- Использование при обработке данных в формате XML внешних сущностей (External Entity), внешних параметров сущностей (External Parameter Entity) и внешних описаний типа документа (External Doctype) должно быть исключено.
- Запрещено сохранять внешние файлы в корневую директорию веб-приложения.

Общие требования:

- Если используется административная панель (например, для управления сайтом), то она должны быть вынесена на отдельный url с возможностью подключения только из внутренней сети или из под VPN.
- Парольная политика для всех пользователей должна соответствовать требованиям, принятым в организации.
- При обработке в АС информации категории конфиденциальности К-2, аутентификация пользователей должна осуществляться с использованием 2 и более надежных факторов аутентификации.
- Настройка TLS должна включать в себя обязательную аутентификацию, шифрование, хэш-функцию с использованием криптостойких алгоритмов.
- Регистрация отдельных событий только составными частями АС, потенциально доступными нарушителю (например, АРМ пользователя, общедоступные веб-серверы), должна быть исключена.
- Событие аудита обязательно должно содержать следующий минимальный набор атрибутов:
  - Дата и время, с точностью до секунды;
  - Идентификатор пользователя;
  - Идентификатор ФП/АС;
  - Идентификатор действия, которое привело к возникновению этого события;
  - Наименование события;
  - Результат (успешный/неуспешный);
  - Старое и новое значение (для событий изменения объекта);
  - Идентификатор (IP-адрес и FQDN (полное доменное имя)) системного компонента (компьютера), используемого для доступа к системе.
- Должна быть обеспечена неизменность данных аудита в хранилище
- Должна отсутствовать возможность отключения фиксации событий в журнал аудита.
- При невозможности фиксации событий в аудите (например, в случае недоступности централизованного аудита/подсистемы аудита) должны быть реализованы механизмы локальной буферизации событий аудита и механизмы их последующей передачи в подсистему аудита. Необходимость реализации данных механизмов зависит от критичности выполняемых операции. В случае, если локальный буфер переполнен, то выполнение бизнес операции должно быть приостановлено.
- При локальной буферизации, события аудита должны быть защищены от ознакомления. Необходимо производить очистку локального буфера после передачи событий в сервис аудита.
- Подлежащие аудиту события должны фиксироваться независимо от того, была ли вызвавшая их операция успешно завершена.

- Срок хранения данных должен быть настраиваемым параметром.
- Доступ к данным аудита посредством технологических интерфейсов Web-серверов, СУБД, серверов приложений должен быть исключён.
- Администратору АС должны быть недоступны:
  - Возможность управлять настройками клиента аудита.
  - Записи событий аудита.
- Выполнение функций, возлагаемых на АС, должно осуществляться штатными средствами самой АС (т. Е. без необходимости запуска программ типа файловых менеджеров, внешних текстовых редакторов и т.д.). Использование внешних программных средств допускается только в том случае, если их вызов не создает предпосылок к нарушению функциональной замкнутости среды.
- Автоматизированные системы на платформе ОС UNIX не должны осуществлять запись в системные директории (\bin, \sbin, \boot, \opt, mp, \usr, \var, \etc, \lib, \lib64, \root, \sbin, \selinux, \srv, \sys).
- Для полей ввода, обрабатывающих секретную информацию, должна быть отключена функция Auto Correction и Autosuggestion (автозаполнение).
- Для обеспечения защиты от восстановления паролей путем перебора должна быть реализована автоматическая временная блокировка пользователя с прогрессирующим таймаутом при многократных последовательных неудачных попытках аутентификации.
- Необходимо проверять, что в проекте используются последние версии библиотек.
- Необходимо проверять, что в используемых библиотеках нет известных уязвимостей (https://nvd.nist.gov/vuln/search).
- Перед использованием на web-ресурсах JavaScript, подгружаемых со сторонних ресурсов, необходимо осуществлять их проверку на предмет вредоносного воздействия на отображаемую в браузерах пользователя информацию и возможность кражи аутентификационных данных и файлов-cookie пользователей.
- Должно гарантироваться отсутствие неавторизованных операций.
- Все операции по редактированию данных, их вводу и удалению, независимо от категорий их конфиденциальности и целостности должны осуществляться на основе аутентификации с использованием уникальных персонифицированных идентификаторов каждого пользователя.
- Исключением является контент, который АС предоставляют в публичный доступ исключительно для просмотра, не требующий аутентификации и авторизации, не содержащий информации категории конфиденциальности К1-К3 и категории целостности И1-И3.
- Передачу аутентификационных данных на web-сервер осуществлять методом POST.
- «Приложение должно обрабатывать все сообщения об ошибках, полученные от сервера, и возвращать клиенту минимальное количество информации об ошибочных ситуациях, возникающих на сервере.
- При возникновении ошибки пользователю должна предоставляться только общая информация и идентификатор записи в журнале аудита с расшифровкой ошибки. В противном случае злоумышленник, используя подробную информацию о системных ошибках, может восстановить логику работы приложения, что является одним из ключевых факторов при проведении ряда атак.»
- «Полный текст сообщения об ошибке, включая системные сообщения, должен сохраняться в журнале аудита так, чтобы администратор АС мог найти его по:
- Идентификатору записи, сообщенной пользователю.
- Указания комбинации учетной записи пользователя (выполнявшего операции) и интервала времени возникновения ошибки.

- В случае нарушения работоспособности приложения, пользователю не должны предоставляться:
- Данные о структуре файловой системы (информация о версии операционной системы, директориях с системными файлами и системным программным обеспечением, включая пути к директориям и файлам);
- Фрагменты программного или конфигурационного кода;
- Сообщения об ошибках при передаче запросов в СУБД;
- SQL-выражения, используемые при доступе к базе данных.

- В случае выявления в приложении критичной ошибки, рекомендуется перенаправлять пользователя на HTML-страницу с ее описанием. Статус HTTP-ответа Web-сервера должен соответствовать 200, что существенно усложнит применение злоумышленником инструментальных средств поиска уязвимостей в Web-приложениях.

- В случае ошибочных действий клиента или пользователя АС не должна предоставлять дополнительное описание причин и места ошибки.
- Ошибки валидации/верификации не должны передаваться внешним клиентам и пользователям – для передачи ошибок должны использоваться стандартные значения, которые не позволят злоумышленнику обнаружить уязвимые места в процедуре валидации/верификации.
- Ошибки валидации и верификации в обязательном порядке должны попадать в журнал аудита с атрибутами, не прошедшими валидацию и верификацию и комментариями по каждой ошибке.
- Разрешено использование только легальных данных. Легальность данных в АС должна быть подтверждена (выполнены условия: известны и зафиксированы происхождение, состав и структура данных, присвоен КЭ, пройдены ПСИ, установлена категория информации (КИ).
- Загрузка данных должна осуществляться через интеграции, которые прошли процедуру ПСИ.
- Обработка персональных данных должна вестись только на законных основаниях. Обработка ПДн должна производиться с согласия субъекта персональных данных, в т.ч. в части касающейся обогащения данных о нем, матчинга и т.п. Обработка без согласия запрещена.
- Запись ПДн в АС, сбор которых осуществляется на основании согласия Субъекта ПДн, должна осуществляться после получения такого согласия. В АС должна быть реализована функция проверки наличия согласия.
  - Функционал удаления конкретных ПДн и Роль по использованию данного функционала.

Требования к пользовательским взаимодействиям:

- Необходимо исключить возможность прямого обращения неавторизованного пользователя к защищенным ресурсам по известному URL. Доступ к защищенным ресурсам должен быть возможен только после проведения процедуры аутентификации.
- Данные, вводимые на веб-формах UI пользователем, и/или информация выше категории К-3 не должны сохраняться в АС Web сайт BackBase.
- В форме ввода НМТ должен быть фильтр по формату данных (+7-***-***-**-**). Необходимо проверять, что введённый номер не принадлежит следующим группам:
  - Номера телефонов других стран (коды отличные от +7). Исключение составляют НМТ Абхазии и Южной Осетии (начинаются на +7) актуальные маски валидации у операторов.

- Спутниковые телефоны 7(954) и др.
- Платные номера 7(809), 7(803) и др.
- Короткие номера. Эти проверки рекомендованы для всех форм ввода НМТ.

Требования к OTP:

- Генерируемые OTP коды должны быть одноразовыми и с ограниченным сроком жизни (до 5 минут). Рекомендованная длина от 6 символов, генератор должен обладать высокой степенью энтропии.
- После генерации нового OTP кода старый код должен быть деактивирован.
- Количество попыток ввода неправильных (в т.ч. устаревших) OTP-кодов должно быть ограничено (рекомендация: 3 попытки ввода для одного OTP кода);
- Число генерируемых одноразовых OTP-кодов, отправляемых на один и тот же НМТ должно быть ограничено. Пример: если пользователь ошибся 9 раз (3 попытки ввода на каждый OTP код из 3х СМС), то блокировать отправку OTP-кодов на час. После часа еще одна СМС с OTP кодом и 3 попытки ввода. Ошибка – блокируем отправку СМС на сутки.
- Необходимо ограничить число запросов на редактирование\добавление НМТ с одного IP адреса с разными вводимыми номерами телефонов. При превышении лимита необходимо отправлять код «CAPTCHA».
- События, связанные с проверкой OTP должны фиксироваться в журнале аудита с привязкой к НМТ.
- Для регистрации и подтверждения критичных операций рекомендовано использовать СМС для отправки OTP кодов. Это позволит подтвердить факт владения НМТ и обеспечит альтернативный канал связи, если интернет-соединение клиента скомпрометировано (атака MITM). Отправка OTP кодов через PUSH уязвимо к атакам MITM.