

«УТВЕРЖДАЮ»
АКБ «УЗПРОМСТРОЙБАНК»

заместитель
Председателя Правления
А. Эргашев



«20» декабря 2023 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на создание Системы принятия решений для кредитования
физических и юридических лиц

«СОГЛАСОВАНО»
Директор департамента
Риск менеджмента

К.Каримов

«__» _____ 2023 г.

«СОГЛАСОВАНО»
вр.и.о.Директор департамента
информационных технологий

А.Кенжаев

«__» _____ 2023 г.

Ташкент 2023 г.

Оглавление

1.	ОБЩИЕ СВЕДЕНИЯ	4
1.1	Полное наименование ИС и ее условное обозначение	4
1.2	Наименование организаций заказчика и разработчика информационной системы	4
1.3	Перечень документов, на основании которых создается ИС	4
1.4	Плановые сроки начала и окончания работ	4
1.5	Порядок оформления и предъявления результатов работ	4
2	Назначение и цели создания информационной системы	5
2.1	Назначение информационной системы	5
2.2	Цели создания информационной системы	5
3	Характеристики объекта информатизации	5
3.1	Описание и предпосылки к разработке информационной системы	5
3.2	Описание текущего бизнес-процесса кредитного конвейера	5
4	Требования к информационной системе	1
4.1	Требования к информационной системе в целом	1
4.1.1	Требования к структуре и функционированию информационной системы	1
4.1.2	Требования к взаимодействию со сторонними информационными системами	4
4.1.3	Требования к численности и квалификации пользователей	7
4.1.4	Требования к надежности	8
4.1.5	Требования безопасности	8
4.1.6	Требования к защите информации	9
4.1.7	Требования к эргономике и технической эстетике	11
4.1.8	Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов информационной системы	12
4.1.9	Требования к патентной и лицензионной чистоте	13
4.1.10	Требования по стандартизации и унификации	13
4.2	Требования к функциям (задачам), выполняемым ИС	14
4.2.1	Схема бизнес-процесса СПР Физических лиц	14
4.2.2	Схема бизнес-процесса СПР юридических лиц	39
4.2.3	Анкета/Заявка на проверку	56
4.2.4	Продуктовый каталог	116
4.2.5	Модуль скоринга	135
4.2.6	Модуль автоматического андеррайтинга (СПР ФЛ)	194
4.2.7	Модуль управления этапами	197
4.2.8	Модуль визуализации для управления этапами и конструктора вычислений	210
4.2.9	Расчеты	213
4.2.10	Загруженные анкеты	220
4.2.11	История прохождения анкеты	223

4.2.12	Параметры	224
4.2.13	Модуль расчета предварительно одобренных решений (СПР ФЛ)	225
4.3	Требования к видам обеспечения	229
4.3.5	Требования к информационному обеспечению	229
4.3.6	Требования к лингвистическому обеспечению	229
4.3.7	Требования к программному обеспечению	230
4.3.8	Требования к техническому обеспечению	230
4.3.9	Требования к организационному обеспечению	230
4.3.10	Требования к методическому обеспечению	231
5	Состав и содержание работ по созданию ИС	231
6	Порядок контроля и приемки ИС	231
7	Требования к составу и содержанию работ по подготовке ИС к вводу в действие	232
8	Требования к документированию	233
	Приложение 1. Перечень условных обозначений, сокращений и терминов	234
	Приложение 2. Тексты пуш-сообщений	234
	Приложение 3. Справочники	234
	Приложение 4. Ограничения	243

1. ОБЩИЕ СВЕДЕНИЯ

1.1 Полное наименование ИС и ее условное обозначение

Полное наименование информационной системы: Система принятия решений для кредитования физических и юридических лиц

Условное обозначение информационной системы: СПР ФЛ и ЮЛ

1.2 Наименование организаций заказчика и разработчика информационной системы

Заказчик – АКБ “Узпромстройбанк”

Адрес «Заказчика»: Узбекистан г.Ташкент. 100000, улица Шахрисабз, 3 дом

МФО: 00440

ИНН: 200833707

Наименование банка: ОПЕРУ при АКБ “Узпромстройбанк”

Адрес электронной почты: info@sqb.uz

Исполнитель разработки информационной системы будет определен по результатам тендерных (конкурсных) торгов.

1.3 Перечень документов, на основании которых создается ИС

Основанием для разработки являются:

1. Постановление Президента Республики Узбекистан «О мерах по дальнейшему развитию и повышению устойчивости банковской системы Республик» от 12.09.2017 года № ПП-3270;
2. Указ Президента Республики Узбекистан «О стратегии реформирования банковской системы Республики Узбекистан на 2020-2025 годы» от 12.05.2020 г. №УП-5992;
3. Постановление Президента Республики Узбекистан «О дополнительных мерах по переходу на международные стандарты финансовой отчетности» от 24.02.2020 г. № ПП-4611;
4. Решения Правления банка;

1.4 Плановые сроки начала и окончания работ

Плановые сроки начала работ: 01.11.2023

Плановые сроки окончания работ: 30.12.2024

Источники финансирования

Источником финансирования проекта являются – собственные средства

1.5 Порядок оформления и предъявления результатов работ

Работа по данному техническому заданию между Заказчиком и Разработчиком информационной системы должна организовываться удаленно. В случае необходимости, Заказчик должен предоставить удаленный доступ сотрудникам Исполнителя к серверам, которые находятся в контуре Заказчика, на которых установлена ИС с учетом требований политики информационной безопасности Заказчика.

Объем работы для Разработчика информационной системы должен устанавливаться согласно функциональным требованиям, предъявляемым к создаваемой системе (п.4).

Разработчик должен организовать работу по созданию информационной системы путем формирования проектной команды.

С целью принятия результатов работ по проекту Заказчик имеет право создать в установленном порядке группу тестирования и приемочную комиссию.

Совместно с предъявлением Группе тестирования Модуля и приёмочной комиссии, производится сдача разработанного Исполнителем комплекта документации, перечня и требований к оформлению по взаимному согласованию Заказчика и Исполнителя с учетом п.8.

По завершению каждого этапа, составляется двусторонний технический акт сдачи и приёмки выполненных работ.

Акт выполненных работ подписывается в течение 10 рабочих дней с момента предоставления указанного акта Заказчику (если не имеется претензии и вопросы).

Датой сдачи – приёмки работ считают дату подписания акта приёма-сдачи (уполномоченного лица).

По каждому реализованному этапу подписываются акты приёмки-сдачи этапа между Исполнителем и Заказчиком.

Уполномоченными лицами подписывается акт сдачи системы в эксплуатацию.

2 Назначение и цели создания информационной системы

2.1 Назначение информационной системы

Система принятия решений на кредитование физических и юридических лиц предназначена для модификации процесса кредитного конвейера для физических и юридических лиц с целью обеспечения оптимального использования результатов обработки заявки, а также преобразования в конкурентоспособный, клиентоориентированный, работающий по рыночным механизмам, привлекательный для инвесторов и клиентов.

2.2 Цели создания информационной системы

- Унификация процесса одобрения для всех кредитных конвейеров и продуктов Банка;
- Максимальная автоматизация процесса одобрения заявки;
- Уменьшение TimeToYes, TimeToNo;
- Уменьшение стоимости рассмотрения заявки;
- Минимизация операционных рисков;
- Внедрение Risk Based Pricing, Risk Based Limits, Portfolio Management Underwriting;
- Возможность конструирования процессов одобрения на базе модулей за счет перестановок этапов, отключения/включения этапов.

Для решения вышеперечисленных задач было принято решение автоматизировать процесс одобрения кредитов посредством системы принятия решений для физических и юридических лиц.

3 Характеристики объекта информатизации

АКБ «Узпромстройбанк» - одно из старейших финансовых учреждений в Республике Узбекистан. История Узпромстройбанка исчисляется с открытия в Ташкенте Среднеазиатской конторы Промышленного банка в 1922 году. Его разветвленная филиальная сеть включает в себя 44 банковские сети, предлагая различные виды банковских услуг.

В настоящий момент, стратегическая цель банка выйти на качественно новый путь развития - банк расширяет свою клиентскую базу, стремится к качественному улучшению банковского сервиса и расширению ассортимента предлагаемых услуг.

В АКБ «Узпромстройбанк» под «региональным управлением» и «минибанком, спецкасса и т.д.» понимается банковское учреждение второго и третьего уровня, выполняющее функции по непосредственному обслуживанию клиентов.

Основные крупнейшие акционеры банка: Фонд реконструкции и развития Республики Узбекистан (82,09%), Министерство финансов Республики Узбекистан (13,58%) и другие (4,33%).

В число крупных акционеров АКБ «Узпромстройбанк» входят: Фонд реконструкции и развития Республики Узбекистан и Министерство финансов Республики Узбекистан».

3.1 Описание и предпосылки к разработке информационной системы

Предпосылками к созданию информационной системы являются необходимость унификации процесса одобрения для всех кредитных конвейеров и продуктов Банка, автоматизация ручного труда, снижение операционных расходов и оптимизация процесса выдачи кредитов клиентам-физическим лицам.

Ключевые недостатки:

- решение бинарное «Одобрить/отказать»;
- изменение условий требует перезапуска или возврата заявки на начальные этапы;
- изменение условий осуществляется посредством экспертного суждения на базе расчетов вне системы;
- отсутствует возможность смены продукта в рамках одной заявки.

3.2 Описание текущего бизнес-процесса кредитного конвейера

Бизнес-процесс кредитного конвейера, реализующий процесс ввода кредитной заявки, ее рассмотрения и одобрения, а также выдачи займа представлен на схемах Рисунков 1 - 3. В рамках проекта внедрения СПР предполагается интеграция внедряемой системы с КК и модификация данного процесса с целью обеспечения оптимального использования результатов обработки заявки СПР. Подпроцессы, которые будут заменены функционалом СПР, выделены на схеме синим цветом. Точки интеграции КК и СПР выделены на схеме красным цветом.

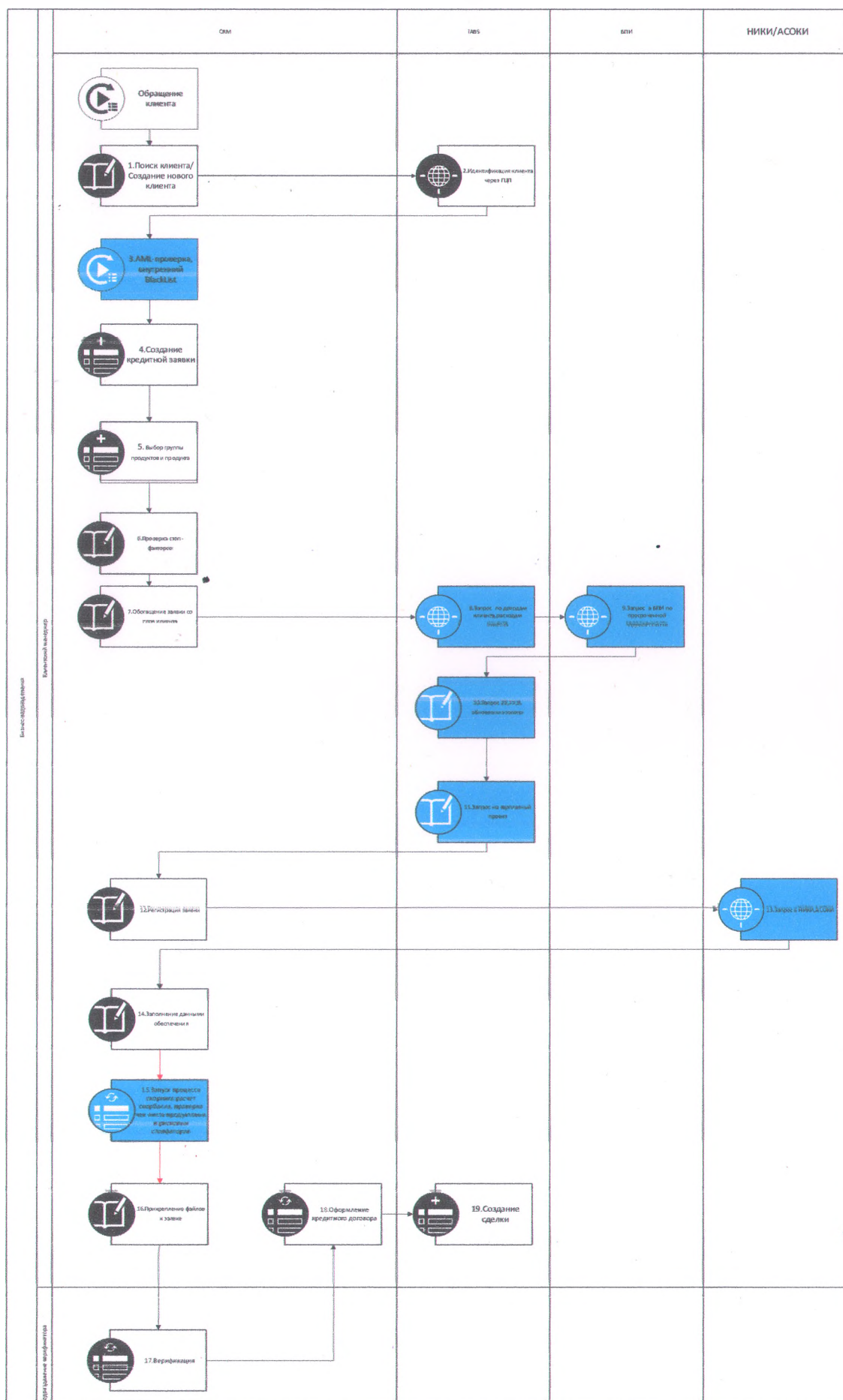


Рисунок 1 Схема текущего процесса кредитного конвейера физических лиц (КК ФЛ)

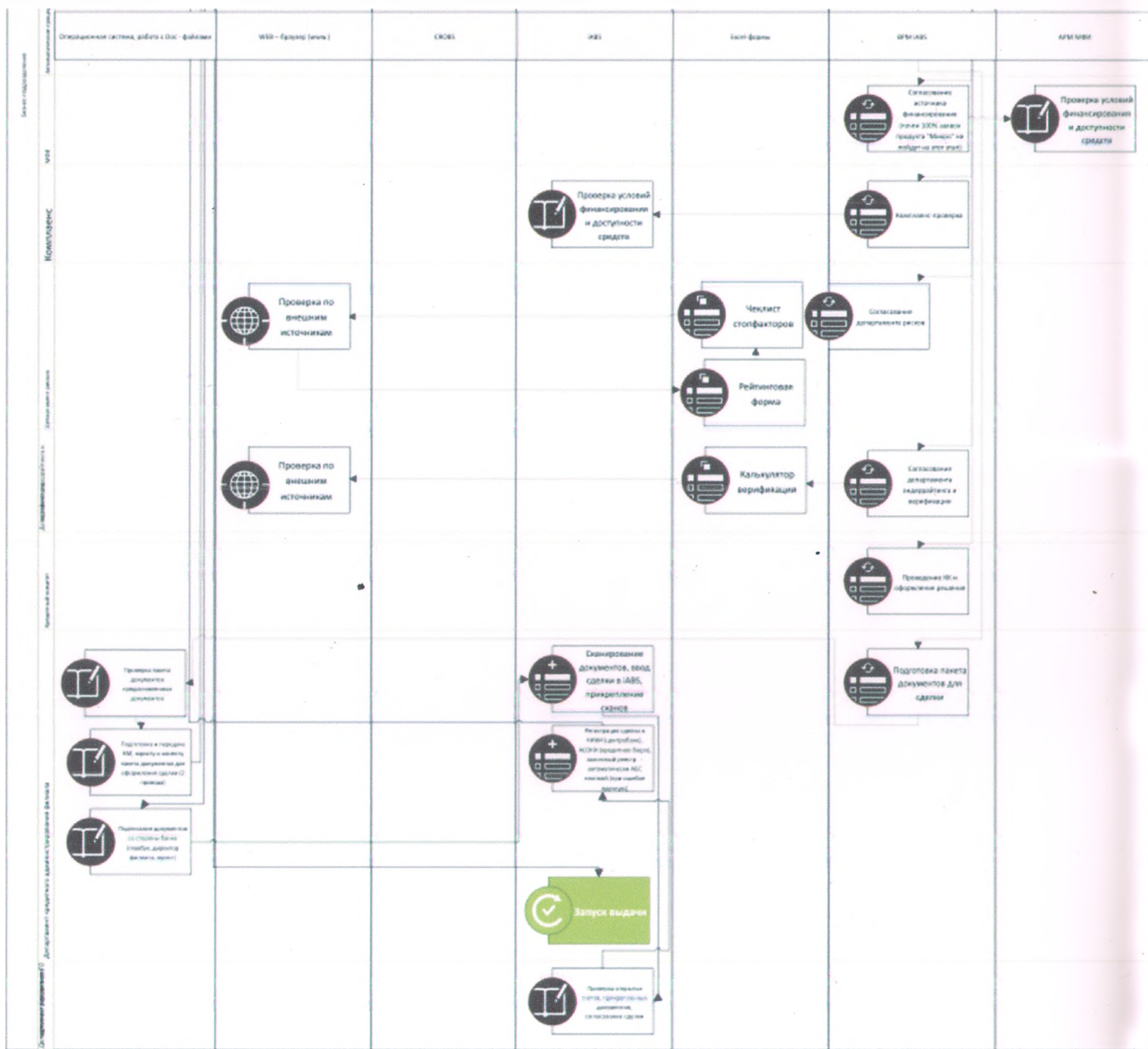


Рисунок 2 Схема текущего процесса кредитного конвейера юридических лиц. Часть 2

4 Требования к информационной системе

4.1 Требования к информационной системе в целом

4.1.1 Требования к структуре и функционированию информационной системы

Основные сценарии использования системы с краткими описаниями перечислены ниже в виде функциональных компонент. Каждый из компонент подробно изложен в отдельных пунктах раздела 4.2 «Требования к функциям (задачам), выполняемым ИС». Ниже изложены компоненты системы:

1. Проверки клиента, поручителей и имущества по списку проверок для продукта заявки (СПР ФЛ):

- 1.1. Проверка во внутреннем черном списке
- 1.2. Проверка в черном списке внутреннего контроля
- 1.3. Проверки в iABS
- 1.4. Проверки в БПИ
- 1.5. Проверки в АСОКИ
- 1.6. Проверки дохода
- 1.7. Проверки в ЧС работодателя
- 1.8. Проверка скорбалла KIATS
- 1.9. Проверка обеспечения займа

2. Проверки клиента, поручителей и имущества по списку проверок для продукта заявки (СПР ЮЛ):

- 1.1. Проверка клиента во внутреннем ЧС
- 1.2. Проверка клиента в ЧС iABS
- 1.3. Проверка Комплаенс-контроля
- 1.4. Проверка в БПИ
- 1.5. Проверка кредитной истории и кредитной нагрузки на все связанные компании (АСОКИ) (кредитное бюро)
- 1.6. Проверка клиента на уровень дохода (CROBS финансовая отчетность и бух. Баланс)
- 1.7. Проверка скорбалла KIATS
- 1.8. Проверка объекта гарантий (залога) на наличие обременений
- 1.9. Проверка в ГНК на наличие задолженностей
- 1.10. Проверка в НИБДД, информация об открытых счетах
- 1.11. Проверка Департамента рисков
- 1.12. Проверка Департамента одобрения кредитов
- 1.13. Расчеты концентрации риска на группу связанных и аффилированных,

ковенанты на сектора экономики

- 1.14. Проверка условий финансирования

3. Модуль скоринга.

Модуль скоринга представляет собой рабочую область системы с пользовательским интерфейсом для создания и редактирования скоркарт. В качестве предикторов могут быть использованы любые данные объектной модели. Все проверки (включая скоринг) оперируют в парадигме коллекции участников сделки. Таким образом СПР позволяет рассматривать заявки с созаемщиками, гарантами точно также, как и займы с одним заемщиком.

4. Модуль автоматического андеррайтинга (СПР ФЛ).

Это отдельный программный продукт, представляющий собой библиотеку алгоритмов, интегрирующийся с любыми кредитными конвейерами, системами принятия решений,

CampaignManagement и иными подобными системам.

Модуль генерирует варианты одобрения заявки согласно продуктовой карты организации используя заложенные алгоритмы:

- Risk Based Pricing – расчет риск-премии по сделке;
- Risk Based Limit – расчет лимита в соответствии с коэффициентом долговой нагрузки;

- Portfolio Management Underwriting – сценарий управления портфелем (на максимизацию портфеля / максимизацию оборачиваемости / приоритизацию конкретных продуктов).

Устанавливается индивидуальная ставка по каждому варианту сделки. Подбираются варианты рефинансирования имеющихся у клиента займов с добором суммы до максимума, рассчитанного через коэффициент долговой нагрузки.

5. Модуль управления этапами.

Модуль управления этапами оперирует атомарными процедурами – «проверками». Каждая проверка возвращает бинарный результат – «Успех/Неуспех». «Успех» - переводит процесс на следующий по очередности этап. «Неуспех» - инициирует отказ и выход из процесса.

6. Модуль визуализации для управления этапами и конструктора вычислений.

Модуль управления проверками позволяет в пользовательском интерфейсе:

- Создавать маршруты процесса одобрения для продуктов;
- Включать/исключать проверки в маршрут рассмотрения;
- Назначать сценарии по результатам проверок.

Это позволяет гибко управлять процессом, минимизировать затраты, обрабатывать заявку при отказе от сервисов.

7. Модуль Расчеты.

Основные сценарии использования системы с краткими описаниями перечислены ниже в виде функциональных компонент. Каждый из компонент подробно изложен в отдельных пунктах раздела 4.2 «Требования к функциям (задачам), выполняемым ИС». Ниже изложены компоненты системы:

4.1.1.1 Требования к режимам функционирования Системы

Информационная система должна функционировать в режиме 5*8: пять рабочих дней в неделю восьмичасовой рабочий день.

Для Системы определены следующие режимы функционирования:

- нормальный режим функционирования;
- аварийный режим функционирования.

Основным режимом функционирования является нормальный режим.

В нормальном режиме функционирования системы:

- технические средства пользователей и администратора системы обеспечивают возможность круглосуточного функционирования с перерывами на обслуживание;
- серверное программное обеспечение и технические средства обеспечивают возможность круглосуточного функционирования с перерывами на обслуживание;
- исправно работает оборудование, составляющее комплекс технических средств;
- исправно функционирует системное, базовое и прикладное программное обеспечение системы.

Для обеспечения нормального режима функционирования системы необходимо выполнять требования и выдерживать условия эксплуатации программного обеспечения и комплекса технических средств системы, указанные в соответствующих технических документах (техническая документация, инструкции по эксплуатации и т.д.).

Аварийный режим функционирования системы характеризуется отказом одного или нескольких компонентов программного и (или) технического обеспечения.

В случае перехода в аварийный режим ИС Платежи должна обеспечивать возможность завершения работы всех приложений с сохранением данных.

4.1.1.2 Перспективы развития, модернизации Системы

Система должна иметь возможность дальнейшей модернизации. Также необходимо предусмотреть возможность увеличения производительности системы путем её масштабирования.

Система должна быть спроектирована таким образом, чтобы была возможность увеличения функциональности системы. Функциональность системы увеличивается в целях повышения эффективности Системы и удовлетворения потребности пользователей. Модернизация и развитие















системы должны осуществляться с учетом факторов, обеспечивающих их экономическую обоснованность.

Система должна допускать перенос программного обеспечения на новые аппаратные средства без доработки программного кода.

Развитие ИС должно быть возможно силами Заказчика бизнес-подразделениями без участия программистов и Разработчика.

4.1.2 Требования к взаимодействию со сторонними информационными системами

Таблица 1 Интеграции (СПР ФЛ)

№	Источник	Описание	Реализация	Запрос	Ответ
1	АСОКИ (КИАЦ)	Кредитная история и кредитная нагрузки, на всех связанные компании (но не на физлицо), регистрацию заявки для ФЛ, поручительство (022, 025, 008, 077)	через шину Rabbit.	 АСОКИ_req.txt	 АСОКИ_res.txt
2	БПИ, https://www.mib.uz/home	Проверка на наличие задолженности	через шину Rabbit	 MIB_req.txt	 MIB_res.txt
3	iABS	проверки физ.лица в ЧС, получение зарплатной истории	через шину Rabbit	 iABS_ЧС_req.txt  iABS_ЗП_req.txt	 iABS_ЧС_res.txt  iABS_ЗП_res.txt
4	ELMA	Проверка задолженности по кредитам у физ.лица в банке	через шину Rabbit.	 ELMA_req.txt	 ELMA_res.txt
5	HUMO	Кредитная история ФЛ	через шину Rabbit.	 HUMO_req.txt	 HUMO_res.txt
6	UzCard	Кредитная история ФЛ по картам	через шину Rabbit.	 UzCard_req.txt	 UzCard_res.txt











7	МИСОКИ	Регистрация заявки для ФЛ и проверка скорбалла KIATS	через шину Rabbit.	 МИСОКИ_req.txt	 МИСОКИ_res.txt
8	ИНПС	Паспорт, серия, номер, pin	через шину Rabbit.	 Inps_getData_res.zip	 Inps_getData_req.zip
9	https://www.garov.uz/	Проверка ареста и обременения на залог.	.		
10	НИБДД	Сервис центрального банка по информации об открытых счетах ФЛ и ЮЛ.			
11	Программа CROBS	Сведения о месячной заработной плате физических лиц			
12	SOLIQ.UZ	Паспорт, серия, номер, pin, ИНН			
13	Министерство юстиций				

Таблица 2 Интеграции СПР ЮЛ

№	Источник	Описание	Реализация	Запрос	Ответ
1	https://www.e-baholash.uz/ru	Предварительная оценка залога и сравнивает с независимой оценкой от клиента.			
2	https://orginfo.uz/ru/	Единая база предпринимателей. Информация о ЮЛ, связанных с клиентом и учредителем.			
3	https://www.garov.uz/	Проверка ареста и обременения на залог.	.		
4	https://davreestr.uz/	Проверка принадлежности недвижимости: кому принадлежит, адрес, кв.м.			
5	АСОКИ (КИАЦ)	Кредитная история и кредитная нагрузка, на все связанные компании	через шину Rabbit.	 АСОКИ_req.txt	 АСОКИ_res.txt

6	БПИ, https://www.mib.uz/home	Проверка на наличие задолженности	через шину Rabbit	 MIB_req.txt	 MIB_req.txt
7	https://my.sud.uz/	Проверка наличия судопроизводства в отношении компаний и учредителей.			
8	ЕЭИСВО	Единая электронная информационная система внешнеторговых операций	через шину Rabbit.		
9	https://license.gov.uz/	Фактические лицензии на ведение определенного типа деятельности.			
10	Гос центр персонализации	Информация о физлицах (для ИП)	через шину Rabbit.		
11	Программа CROBS (по ИНН запрос Ф1, Ф2 в налоговую)	Финансовая отчетность (Форма №-2) и бухгалтерский баланс (Форма №-1).		да	
12	НИБДД	Сервис центрального банка по информации об открытых счетах ФЛ и ЮЛ.		да	
13	iABS	Проверки в ЧС Банка	через шину Rabbit	 iABS_ЧС_req.txt	 iABS_ЧС_res.txt
14	МИСОКИ	Проверка скорбалла KIATS	через шину Rabbit.	да	
15	ГНК	Государственный налоговый комитет, данные о наличии задолженности у ЮЛ перед государством.		да	
16	Министерство Юстиций	Информация учредителя			

Все данные, полученные из источников интеграции, должны сохраняться в формате бинарного файла.

Список сервисов может сократиться после уточнения наличия у сервисов API.

4.1.3 Требования к численности и квалификации пользователей

Требования к функциональным группам, составу, численности и квалификации персонала со стороны Заказчика могут быть определены в соответствии с организационной структурой Заказчика на этапе разработки Системы и согласованы с Заказчиком.

Система должна включать следующие пользовательские роли:

Таблица 3 Ролевая модель СПР

Роль	Описание
Аналитик	Настройка матрицы проверок для продуктов. Работа в конструкторе приложений. АРМ Аналитика описан в подразделе «АРМ Аналитика»

4.1.3.1 АРМ Аналитика

Таблица 4 Интерфейсные формы АРМ Аналитика

Форма	Описание
Настройка скоркарты	<p>Работа с модулем «Скоринг» :</p> <ul style="list-style-type: none"> -Создание новых скоркарт (копированием уже имеющихся скоркарт, создание скоркарты «с нуля») - Редактирование скоркарт. Настройка предикторов в скоринговых картах: <ul style="list-style-type: none"> -добавление/удаление предикторов в карте. -Изменение значения предикторов в карте, -изменение значения балла предиктора в карте. -Нельзя добавлять новые предикторы, а только выбирать из заранее преднастроенных.
Настройка продуктов	<p>Работа с модулем «Продуктовый каталог»:</p> <ul style="list-style-type: none"> - Изменение значений полей - Добавление новых продуктов, устанавливать продуктам признак «неактивный» - добавление/удаление скоркарты у продукта (Из таблицы «Продукты» можно открыть таблицу всех скоркарт этого продукта). <p>Работа с модулем управления этапами:</p> <ul style="list-style-type: none"> -Добавление/удаление проверки у продукта. -Настройка последовательности проверок продукта. <p>Из таблицы «Продукты» можно открыть таблицу всех проверок этого продукта.</p>
Справочники ФЛ	<ol style="list-style-type: none"> 1. Справочник регионов, районов, подразделений, департаментов, валюта (Приложение 3). Добавление в справочник новых значений, установка признака активности/неактивности значения справочника. 2. Причины отказа ФЛ. Добавление в справочник новых значений, установка признака активности/неактивности значения справочника. 3. Стоп-факторы. Изменение значений стоп-факторов, нельзя добавлять новые стоп-факторы. 4. Параметры. Изменение значений параметров, нельзя добавлять новые параметры. Параметры системы описаны в п.4.2.11
Справочники ЮЛ	<ol style="list-style-type: none"> 1. Справочник типов клиентов ЮЛ, типов продуктов, валют и другие. Полный перечень указан в «Приложение 3. Справочники». Добавление в справочник новых значений, установка признака активности/неактивности значения справочника. 2. Причины отказа ЮЛ. Добавление в справочник новых значений, установка признака активности/неактивности значения справочника. 3. Стоп-факторы. Изменение значений стоп-факторов, нельзя добавлять новые стоп-факторы. 4. Параметры. Изменение значений параметров, нельзя добавлять новые параметры. Параметры системы описаны в п.4.2.11
Истории прохождения анкеты	<p>Просмотр истории прохождения анкеты по проверкам: проверка, дата проверки, результат проверки, ФИО выполнившего проверку, комментарий к проверке, выполненные запросы во внешние сервисы и</p>

	<p>результат ответов, рассчитанные значения: скорбаллы, все значения по алгоритмам.</p> <p>Возможность перейти к форме с самой проверкой.</p> <p>Поиск записей в истории по id клиента, id анкеты, дате расчета.</p>
--	--

4.1.4 Требования к надежности

Показатели надежности должны обеспечиваться при условии соблюдения требований к надежности оборудования и электроснабжения, а также за счет выполнения следующих организационных мероприятий:

- предварительного обучения пользователей и обслуживающего персонала;
- своевременного выполнения процессов администрирования;
- соблюдения правил эксплуатации и технического обслуживания;
- своевременного выполнения процедур резервного копирования данных.

Показатели надежности должны определяться прогнозируемой частотой возникновения аварийных ситуаций. Для Системы регламентируются показатели надежности для следующих видов аварийных ситуаций:

- Общесистемный отказ - выражается в недоступности всех или большинства пользовательских интерфейсов Системы вне зависимости от причин, вызвавших этот отказ (отказы средств технического обеспечения, телекоммуникационных средств, общесистемного программного обеспечения, неверная работа специализированных программ, ошибки персонала, сбой электропитания и т.п.), кроме причин катастрофического характера (форс- мажорных обстоятельств): не больше 5% рабочего времени, не чаще 2 раз в месяц.

- Частный сбой - выражается в недоступности одного из интерфейсов какого-либо функционального компонента или его некорректной работе (отклонении от порядка функционирования, установленного в требованиях ТЗ, проектной или рабочей документацией на Систему): не чаще 4 раз в месяц, не больше 10% рабочего времени.

Сохранение работоспособности обеспечивается при возникновении локальных отказов компонентов системы:

- отказ автоматизированного рабочего места;
- отказ линии связи или сегмента ЛВС;
- отказ центрального сервера.

Сохранность информации в Системе должна обеспечиваться при следующих аварийных ситуациях:

- нарушения электропитания (кратковременные понижения при резком увеличении нагрузки в электрической сети, кратковременные значительные увеличения напряжения, полное отключение электроэнергии вследствие аварий, перегрузок);

- нарушение или выход из строя каналов связи локальной сети Заказчика;
- полный или частичный отказ технических средств системы, включая сбой и отказы накопителей на жестких магнитных дисках;
- сбой общего или специального программного обеспечения системы;
- ошибки в работе управляющего или технического персонала;
- выход из строя комплекса технических средств за счет аварий техногенного характера - повреждение внешних каналов связи, нарушение системы электропитания здания;
- выход из строя элемента сетевой инфраструктуры системы.

4.1.5 Требования безопасности

Все технические решения, использованные в системе, должны соответствовать общим требованиям безопасности программных комплексов при работе информационных систем, включая требования по наладке, эксплуатации и обслуживанию.

Эксплуатация системы персоналом должна вестись с соблюдением общих правил техники безопасности.

Используемые при разработке технологии должны обеспечить безопасность доступа к данным за счет аутентификации, идентификации и ролевых прав пользователей.

В системе должно быть автоматическое ведение журнала аудита, обеспечивающего возможность мониторинга наиболее критичных (уникальных) данных, хранящихся в БД и регистрации всех происходящих событий.

Все системы должны эксплуатироваться внутри банка.

До начала разработки системы Заказчик предоставляет требования политики Информационной Безопасности, действующие в объекте информационной безопасности. Предоставленные требования должны быть учтены при разработке Системы, чтобы избежать конфликтных ситуаций при проведении мероприятий и по обеспечению информационной безопасности.

Необходимо предусмотреть возможность экстренного отключения доступа к системе в случаях внештатных ситуаций.

В системе должны быть предусмотрены средства защиты информации от несанкционированного доступа неавторизованных пользователей.

Программная платформа должна предоставлять возможность гибкого разделения полномочий по ее администрированию и использованию. Требуется наличие ролевой модели предоставления прав на доступ к конкретным разделам пользовательского графического интерфейса и определенные действия по администрированию платформы.

Комплекс средств защиты системы должен включать:

- Средства аутентификации пользователей и элементов платформы (рабочих станций, задач, элементов баз данных и т.п.).
- Средства разграничения доступа пользователей на уровне задач и информационных массивов согласно ролевой матрицы доступа к системе (логин / пароль).
- Удаленный доступ к хранилищу данных должен обеспечиваться только средствами разрабатываемой платформы, за исключением случаев, когда сотрудники Заказчика имеют прямой доступ к БД системы. Разрешение доступа к БД системы выдается Заказчиком, в соответствии с внутренними регламентами, и таким образом, чтобы эти разрешения не нарушали требования политики информационной безопасности.
- Доступ к служебной и системной информации должен осуществляться только локально администратором платформы.
- Платформа должна соответствовать требованиям законодательства Узбекистана в области защиты персональных данных, в той части, в которой это описано в настоящем Техническом Задании.

4.1.6 Требования к защите информации

С целью защиты информации и программных средств от несанкционированного доступа и действия вредоносных программ (компьютерных вирусов и вредоносных скриптов) при модернизации существующего комплекса Заказчика и эксплуатации системы силами Заказчика должны быть приняты организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий группой информационной безопасности банка.

С целью предотвращения несанкционированного доступа к информационным ресурсам автоматизированной банковской системы должно быть обеспечено выполнение следующих требований:

- Защита информации от атак извне;
- Защита информации от несанкционированного доступа пользователей;
- Обеспечение целостности информации (при хранении, передаче и обработке данных);
- Обеспечения защиты передаваемой информации между узлами участников системы (Головной банк, областной и районный филиал) путём создания закрытого и зашифрованного канала;
- Обеспечения передачи файлов между узлами участников системы путём создания, закрытого файлообмена (Головной банк, областной и районный филиал);

Протоколирование и аудит систем безопасности;

Протоколирование (работы межсетевых экранов, обработки защищенных данных на всех участках) должно производиться в читаемой форме;

Применение ключевых приложений и услуг в режиме реального времени (Online) при режиме работе отделения – республика.

Все системы в части безопасности должны разрабатываться с учетом требований действующих стандартов и нормативных документов Республики Узбекистан, которые были согласованы между Заказчиком и Исполнителем до начала разработки.

Информационная безопасность в системе должна достигаться за счет комплексного использования:

- средств защиты информации от несанкционированного доступа для рабочих станций, серверов и сетевого телекоммуникационного оборудования;
- межсетевых экранов (Firewall);
- средств анализа защищенности, обнаружения и предотвращения вторжений;
- средств антивирусной защиты информации;
- средств аутентификации и управления доступом, а также протоколирования действий пользователей.

4.1.6.1 Требования к сохранности информации при авариях

Сохранность информации системы должна обеспечиваться при следующих аварийных ситуациях ответственными сотрудниками соответствующих подразделений банка:

- нарушения электропитания;
- полного или частичного отказа технических средств системы, включая сбои и отказы накопителей на жестких магнитных дисках;
- сбоя общего или специального программного обеспечения системы;
- ошибки в работе персонала;
- выхода из строя:
 - комплекса технических средств из-за аварий техногенного характера – повреждение внешних каналов связи, нарушение системы электропитания зданий и т.д.;
 - элемента сетевой инфраструктуры системы;
 - одиночного сервера;
 - одиночного дискового массива сервера;
 - диска сервера;
 - процессора сервера;
 - сетевого адаптера сервера;
 - внутреннего источника питания сервера;
- нарушение логической целостности информации, хранящейся на диске сервера.

В целях сохранности информации при авариях и сбоях средствами операционной системы и СУБД должны обеспечиваться:

- возможность полного или частичного восстановления программ в результате сбойных ситуаций;
- наличие системы дублирования информации на резервные устройства хранения с последующим восстановлением.

4.1.6.2 Требования к резервному копированию и восстановлению

ПО резервные копирования должно удовлетворять следующим требованиям:

- Обеспечивать возможность копирования только изменившихся блоков на хранилище, для уменьшения объема передаваемых данных;
- Эффективно использовать ресурсы хранения, за счет минимизации избыточности хранимых данных;
- Обеспечивать возможность увеличения производительности комплекса резервного копирования путем масштабирования;

- Поддерживать передачу резервных копий, как по сети передачи, так и по сети хранения данных;
- Разворачивать специализированное программное обеспечение для резервного копирования внутрь ОС, защищаемого физической системы;
- Интегрироваться и использовать программные интерфейсы, которые предоставляет ОС данного компьютера или сервера.

Резервное копирование настраивается Администратором СУБД Заказчика, в соответствии с внутренними регламентами и с вышеперечисленными требованиями.

Доступ к данным в Системе должен быть предоставлен только авторизованным пользователям с учётом их полномочий, а также с учётом категории запрашиваемой информации.

Авторизация будет проводиться посредством ввода логина и пароля пользователя. Необходимо предусмотреть возможность экстренного отключения доступа к системе в случаях внештатных ситуаций.

Комплекс средств защиты связи между сервером системы и пользователем должен включать:

- Шифрование данных (применение протокола HTTPS);
- Средства аутентификации пользователей и элементов платформы;
- Средства разграничения доступа пользователей (логин / пароль);
- Ведение журнала событий;
- Обучение пользователей.

Доступ к служебной и системной информации должен осуществляться только локально администратором Системы.

Система должна соответствовать требованиям законодательства Узбекистана в области защиты персональных данных.

Сессионное время пользователей должно быть настроено с включением фиксации бездействия пользователя.

Пароли пользователей должны отвечать требованиям внутренних норм Банка на предмет сложности в целях предотвращения попыток взлома методом перебора. Количество неудачных попыток входа должно быть ограничено и при его превышении сеанс должен блокироваться на определенный промежуток времени.

Пароли должны храниться в защищенном виде. При вводе паролей они должны быть замаскированы. Все действия пользователей должны записываться в соответствующих журналах. Доступ к данным журналам должен иметь только администратор(ы). Никто (даже администратор) не должен иметь права на изменение и удаление записей журналов.

В Системе должна вестись регистрация событий, относящихся к обращению пользователей к объектам. Журнал зарегистрированных событий должен храниться в течение 2 лет и должен быть защищен от несанкционированного изменения и удаления данных, в том числе от модификаций администраторами Системы.

4.1.7 Требования к эргономике и технической эстетике

Система должна обеспечивать удобный и однозначный интерфейс для работы со всем предоставляемым функционалом, разработанный с учетом достижений современной эргономики и дизайна:

- экранные формы и меню должны иметь простую логическую организацию, пункты меню должны быть сгруппированы в соответствии с функциональными задачами и тематикой информации, каждому пункту меню должна соответствовать только одна выполняемая функция;
- дизайн экранных форм должен быть стандартным и подвергаться изменению только в случае невозможности решить задачу стандартной формой;
- состав полей в экранной форме должен определяться Исполнителем совместно с Заказчиком;
- эргономические решения должны быть едиными для всех компонентов и модулей системы;

- интерфейс пользователей должен способствовать уменьшению вероятности совершения им случайных ошибочных действий;
- интерфейс должен быть оптимизирован для выполнения типовых и часто используемых прикладных операций.
- все справочники в рамках отдельной Подсистемы должны открываться в процессе работы пользователя стандартным образом;
- интерфейс системы должен обеспечивать отображение на экране только тех функциональных возможностей, которые доступны конкретному пользователю;
- интерфейс системы должен обеспечивать визуальное отображение на экране хода длительных процессов обработки.

Система должна требовать подтверждение по важным операциям, например, изменениям и удалениям данных. Пользовательский интерфейс должен иметь информативные описания ошибок. Система должна обеспечивать встроенные удобные механизмы для контроля при вводе пользователем значений полей:

- на соответствие допустимым значениям;
- на соответствие значениям справочников и классификаторов
- на соответствие допустимым размерам.

4.1.8 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов информационной системы

Система должна быть рассчитана на эксплуатацию в составе программно-технического комплекса Заказчика. Техническая и физическая защита аппаратных компонентов системы, носителей данных, бесперебойное энергоснабжение, резервирование ресурсов, текущее обслуживание реализуется техническими и организационными средствами, предусмотренными в ИТ инфраструктуре Заказчика в соответствии с эксплуатационными документами и инструкциями от производителя программного обеспечения.

Должна быть обеспечена возможность функционирования системы в круглосуточном режиме.

Инсталляционные комплекты ПО должны храниться у администраторов системы в помещениях с ограниченным контролируемым доступом.

Для хранения и восстановления данных в системе должны использоваться средства СУБД. Реализация этих требований должна быть обеспечена соответствующими организационными мерами по регламентному обслуживанию системы.

Для нормальной эксплуатации разрабатываемой системы должно быть обеспечено бесперебойное питание ЭВМ. Климатические условия эксплуатации, при которых должны обеспечиваться заданные характеристики, должны удовлетворять требованиям, предъявляемым к техническим средствам в части условий их эксплуатации. Периодическое техническое обслуживание должно проводиться в соответствии с требованиями технической документации изготовителей.

Периодическое техническое обслуживание должно проводиться не реже одного раза в год.

Периодическое техническое обслуживание и тестирование технических средств должны включать в себя обслуживание и тестирование всех используемых средств, включая рабочие станции, серверы, кабельные системы и сетевое оборудование, устройства бесперебойного питания. На основании результатов тестирования технических средств должны проводиться анализ причин возникновения обнаруженных дефектов и приниматься меры по их ликвидации.

Размещение помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств.

Все пользователи системы должны соблюдать правила эксплуатации электронной вычислительной техники.