**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**На проект**

**«ВНЕДРЕНИЕ СИСТЕМЫ АВТОМАТИЗАЦИИ ВНУТРЕННЕГО КОНТРОЛЯ ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ ДОХОДОВ, ПОЛУЧЕННЫХ ОТ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ, ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА И ФИНАНСИРОВАНИЮ РАСПРОСТРАНЕНИЯ ОРУЖИЯ МАССОВОГО УНИЧТОЖЕНИЯ В УЗНАЦБАНКЕ»**

**Заказчик:** АО «Узнацбанк»

Ташкент 2021г.

**ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ, СОКРАЩЕНИЙ И ТЕРМИНОВ**

|  |  |
| --- | --- |
| **Обозначение** | **Пояснение** |
| EAI | Интеграция приложений предприятия (Enterprise Application Integration, EAI) — это технологии и приложения, задача которых - вовлечь несколько приложений, используемых в одной организации, в единый процесс и осуществлять преобразование форматов данных между ними. |
| RBA | risk based approach. подход на основе оценки рисков |
| EDD | Enhanced Due Diligence (углублённая, или расширенная проверка клиента) |
| CDD | Customer Due Diligence (надлежащая проверка клиентов) |
| UBO | Ultimate Beneficial Owner (Конечный бенефициар) – это лицо, по факту владеющее компанией и получающее выгоду от ее деятельности. |
| EDW | Enterprise data warehouse – корпоративное хранилище данных |
| PEP | Politically exposed person (PEP) - Термин в области финансового регулирования. Обозначает физическое лицо, играющее выдающуюся общественную роль как внутри той или иной страны, так и на международном уровне. |
| ODD | Ongoing Customer Due Diligence Постоянная проверка клиентов |
| ПЛПД/ФТ/ФРОМУ | Противодействие легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения |
| ПДЛ | Публичное должностное лицо |
| Перечень | Перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения, формируемый специально уполномоченным государственным органом на основании сведений, представляемых государственными органами, осуществляющими борьбу с терроризмом, распространением оружия массового уничтожения, и другими компетентными органами Республики Узбекистан, а также сведений, полученных по официальным каналам от компетентных органов иностранных государств и международных организаций |
| Ключевой пользователь | Сотрудник Заказчика, обладающий максимальными компетенциями во внутренних процессах Заказчика, имеющий достаточный опыт и знания для последующей передачи знаний и поддержки пользователей |
| АБС | Автоматизированная банковская система |
| IP | Internet Protocol – Маршрутизируемый сетевой протокол |
| RH | Руководящий документ |
| O’z DSt | Государственный стандарт Республики Узбекистан |
| БД | База данных |
| ГОСТ | Государственный стандарт |
| ПАК | Программно-аппаратный комплекс |
| ПО | Программное обеспечение |
| ТЗ | Техническое задание |
| СУГО | Специально уполномоченный государственный орган |

**СОДЕРЖАНИЕ**

1. ОБЩИЕ СВЕДЕНИЯ 5

1.1. Полное наименование проекта и его условное обозначение 5

1.2. Заказчик 5

1.3. Исполнитель 5

1.4. Основание для внедрения 6

1.5. Плановые сроки начала и окончания работ 7

1.6. Источники финансирования 7

1.7. Порядок оформления и предъявления результатов работ 7

2. НАЗНАЧЕНИЕ СИСТЕМЫ И ЦЕЛИ РЕАЛИЗАЦИИ ПРОЕКТА 8

2.1. Назначение системы 8

2.2. Цели реализации проекта 8

3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ 8

3.1. Общие сведения 8

3.2. Архитектура и программно-аппаратный состав ИТ-комплекса 10

3.3. Имеющиеся недостатки текущего процесса 13

3.4. Обоснование выбора аппаратной платформы 16

4. ТРЕБОВАНИЯ К СИСТЕМЕ 19

4.1. Требования к системе в целом 19

4.2. Требования к структуре и функционированию системы 23

4.2.1. Требования к режимам функционирования системы 23

4.2.2. Требования к режимам функционирования системы 23

4.2.3. Перспективы развития, модернизации системы 23

4.2.4. Перечень и описание сценариев использования ИС 24

4.2.5. Требования к диагностированию системы 25

4.2.6. Требования к численности и квалификации пользователей системы и режиму его работы 26

4.2.7. Показатели назначения 30

4.2.8. Требования к надежности 31

4.2.9. Требования к безопасности 32

4.2.10. Требования к эргономике и технической эстетике 33

4.2.11. Требования к транспортабельности 34

4.2.12. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы 34

4.2.13. Требования к защите информации от несанкционированного доступа 35

4.2.14. Требования к разграничению прав доступа 36

4.2.15. Требования по сохранности информации при авариях 37

4.2.16. Требования защите от влияния внешнего воздействия 38

4.2.17. Требования к патентной и лицензионной чистоте 38

4.2.18. Требования по стандартизации и унификации 38

4.3. Требования к функциям (задачам), выполняемым системой 39

4.3.1. Общие требования к функционалу Системы 39

4.3.2. Требования к подсистеме противодействия отмыванию денежных средств (AML) 41

4.3.3. Требования к подсистеме консолидации процесса расследования подозрительной деятельности на единой платформе на уровне Банка (ECM) 43

4.3.4. Требования к подсистеме детального исследования клиентов Банка (KYC) 44

4.3.5. Требования к подсистеме идентификации клиентов, упомянутых в списках особого внимания (CS) 47

4.3.6. Требования к подсистеме фильтрации транзакций (TF) 49

4.3.7. Требования к подсистеме противодействия мошенничеству (Fraud) 55

4.3.8. Требования к подсистеме отчетности 59

4.4. Требования к взаимодействию со сторонними информационными системами 62

4.5. Требования к видам обеспечения 64

4.5.1. Требования к математическому обеспечению 64

4.5.2. Требования к информационному обеспечению 64

4.5.3. Требования к лингвистическому обеспечению 64

4.5.4. Требования к программному обеспечению 64

4.5.5. Требования к техническому обеспечению 65

4.5.6. Требования к метрологическому обеспечению 67

4.5.7. Требования к организационному обеспечению 67

4.5.8. Обучение пользователей 68

4.5.9. Требования к методическому обеспечению 68

4.5.10. Требования к страхованию товаров 69

4.5.11. Требования к объему и/или сроку предоставления гарантий 69

4.5.12. Требования к месту и условиям поставки закупаемого оборудования 69

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО ВВОДУ СИСТЕМЫ 70

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ 77

6.1. Виды, объем и методы испытаний 78

6.1.1. Предварительные испытания 78

6.1.2. Опытно-промышленная эксплуатация 78

6.1.3. Промышленная эксплуатация 78

7. ТРЕБОВАНИЯ ПО СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ СИСТЕМЫ К ВВОДУ В ДЕЙСТВИЕ 78

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ 79

8.1. Проектная документация 79

9. ИСТОЧНИКИ РАЗРАБОТКИ 80

## 1. ОБЩИЕ СВЕДЕНИЯ

## Полное наименование проекта и его условное обозначение

Полное наименование проекта: «Внедрение системы автоматизации внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения» (далее – Система).

## Заказчик

АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан» (далее по тексту «Заказчик»).

**Реквизиты:**

- Юридический адрес: Республика Узбекистан 100047, г. Ташкент, ул. Истикбол, 23;

- Почтовый адрес: Республика Узбекистан 100084, г. Ташкент, проспект А.Темура, 101;

- Р/с No 29802840800000450391 в Межбанковском расчетном центре АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан»;

- МФО 00450;

- ИНН / КПП 200836354;

- ОКОНХ 96120;

- Тел.: (+99878) 147-15-01;

**E-mail:** AMansurov@nbu.uz

## Исполнитель

Исполнитель по данному проекту будет определен на основе результатов тендерного отбора.

Исполнитель должен иметь наличие опыта внедрения систем финансового мониторинга и предотвращения мошеннических операций в банковской сфере не менее 3 лет.

Исполнитель должен предоставить не менее 2 рекомендательных писем от Банков, в которых эксплуатируется предлагаемая Система, включая и банки стран СНГ.

Исполнитель должен иметь в команде не менее 5 сертифицированных специалистов, незадействованных на время реализации проекта в других проектах.

Исполнитель вправе представить свое Техническое предложение по поставке оборудования (в соответствии со всеми требованиями или выше) и программного обеспечения, удовлетворяющие всем требованиям данного документа.

Исполнитель должен предложить решение, которое обеспечит защиту инвестиций Заказчика в течение не менее 3 лет, исключая необходимость полной замены программно-аппаратного комплекса или смены платформы (нового функционала в обозначенный период должна быть реализована только путем обновления программного обеспечения, лицензий и/или расширения аппаратных модулей).

Исполнитель должен иметь статус авторизованного партнера производителей оборудования и программного обеспечения для выполнения требуемых работ в полном объёме с предоставлением MAF (Manufacturer’s Authorization Form) на поставку оригинального оборудования и программного обеспечения с подтверждением гарантийных обязательств на поставляемое оборудование.

Исполнитель должен предоставить:

- сертификаты, подтверждающие наличие сертифицированных специалистов (не менее 3х), не вовлеченных в другие проекты, по предлагаемым решениям;

- информацию по энергоэффективности предлагаемого аппаратно-программных средств (решения) согласно нормативным документам (датащитам) производителя;

- информацию по передаче государственному заказчику исключительных авторских прав на объекты интеллектуальной собственности (при их наличии), возникших в связи с исполнением обязательств исполнителя по выполнению работ и оказанию услуг;

- информацию по условиям лицензирования (порядок взимания платы, срок действия лицензий);

- информацию по порядку лицензирования (объем, добавление функционала, вид предоставляемых лицензий (срочные/бессрочные, по количеству пользователей и/или на неограниченное количество пользователей) и др.);

- в рамках выделенного бюджета должен предоставить полностью укомплектованное и работоспособное оборудование в рамках технический требований настоящего Технического задания, при необходимости предложить дополнительные модули, продукты, и услуги, по каким-либо причинам не учтенные Заказчиком, но обязательные для обеспечения полноты использования запрашиваемой конфигурации;

- информацию по персональному составу проектной команды (подтверждение наличия специалистов (инженеров) в команде Исполнителя, подтвердивших свою квалификацию соответствующими сертификатами);

- информацию по сервисам (подписки и техническая поддержка) и др.;

- информацию по реализации аналогичных проектов, свидетельствующие, что предлагаемое решение зарекомендовало себя в работе и удовлетворительно работало в реальных условиях;

- информацию по рекомендованным требованиям к вычислительным ресурсам аппаратного обеспечения, необходимым для полноценного функционирования программного комплекса без привязки к конкретному производителю оборудования и соответствие предлагаемой аппаратной платформы этим требованиям;

- информацию по уровню защищенности и безопасности программного комплекса от несанкционированного доступа к информации.

Исполнитель гарантирует наступление даты окончания поддержки закупаемого оборудования (всех комплектующих) не ранее чем через 5 лет с момента заключения договора поставки оборудования. Поддержка аппаратного обеспечения подразумевает доступность сервисного обслуживания всех блоков и компонентов аппаратно-программных средств.

При этом, для расширения круга потенциальных участников в тендерных торгах, в рамках выделенного бюджета заказчиком могут быть рассмотрены аналогичные либо превосходящие, указанные в настоящем техническом задании, характеристики к программной платформе. В этой связи, в случае предоставления аналогичного решения Исполнителю необходимо дополнительно предоставить:

• технико-экономическую информацию по результативности и эффективности;

• расчет финансовых затрат по взаимоинтеграции с существующей инфраструктypoй (замена, интеграция и т.д.);

• потенциальные риски по переходу на аналогичное решение и мероприятия по их устранению.

## Основание для внедрения

Основанием для разработки проекта Комплекса является:

1. Закон Республики Узбекистан № 660-II от 26 августа 2004 г. «О противодействии легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения»;

2. Постановление Правления Центрального Банка Республики Узбекистан Департамента по борьбе с налоговыми, валютными преступлениями и легализацией преступных доходов при Генеральной прокуратуре Республики Узбекистан «Об утверждении правил внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения в коммерческих банках», зарегистрированного Министерством юстиции Республики Узбекистан 23 мая 2017 г. Регистрационный № 2886;

3. Положение «О порядке приостановления операций, замораживания денежных средств или иного имущества, предоставления доступа к замороженному имуществу и возобновления операций лиц, включенных в перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения» зарегистрированного Министерством юстиции Республики Узбекистан 11 октября 2016 г. Регистрационный №2833;

4. Положение о порядке предоставления информации, связанной с противодействием легализации доходов, полученных от преступной деятельности, и финансированию терроризма, утвержденного постановлением Кабинета Министров Республики Узбекистан от 12 октября 2009 года №272;

5. Постановление Президента Республики Узбекистан № ПП-1730 от 21.03.2012 г «О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий»;

6. Положение "Об организации защиты электронной информации в банках Республики Узбекистан" №14/13 от 23.06.01г. (Рег. №1047 от 09.07.2001г.);

7. Положение “О защите информации в электронных системах Центрального банка и ответственности должностных лиц” (Рег. № 633 от 17.01.2006);

8. Положение “О защите информации в электронных системах коммерческих банков Республики Узбекистан” (Рег. № 1552 от 13.03.2006);

9. Постановление Президента Республики Узбекистан «О мерах по дальнейшему развитию и повышению устойчивости банковской системы Республики» от 12.09.2017 года № ПП-3270;

10. Постановление Президента Республики Узбекистан «О дополнительных мерах по повышению доступности банковских услуг» от 23.03.2018 года № ПП-3620;

11. №УП-5992 «О стратегии реформирования банковской системы Республики Узбекистан на 2020-2025 годы»

12. Рапорт на имя Председателя Правления от 07.07.2020г.

## Плановые сроки начала и окончания работ

Плановые сроки реализации проекта:

Начало: Май, 2021г.;

Завершение: Май, 2022г.

## Источники финансирования

Источником финансирования работ по проекту являются собственные средства Узнацбанка.

## Порядок оформления и предъявления результатов работ

По завершению отдельных этапов и работы в целом Исполнитель представляет акт сдачи-приемки.

Результаты работ оцениваются приемочной комиссией. Приемочную комиссию в установленном порядке образует Заказчик.

Приемочной комиссии Исполнитель предъявляет документацию, перечень и требования к оформлению которых определяются в соответствии с ГОСТами и иными стандартами, и руководящими документами, действующими на территории Республики Узбекистан, а также по взаимному согласованию Заказчика и Исполнителя.

Датой сдачи – приемки работ считают дату подписания акта приемочной комиссией.

# 2. НАЗНАЧЕНИЕ СИСТЕМЫ И ЦЕЛИ РЕАЛИЗАЦИИ ПРОЕКТА

## 2.1. Назначение системы

Система предназначена для использования работниками Банка, выполняющих свои обязанности по противодействию легализации доходов, полученных от преступной деятельности незаконным путем, и финансирования терроризма, принимающие усиленные меры по надлежащей проверке, выявлению и оценке своих рисков легализации доходов, полученных от преступной деятельности, финансирования терроризма и финансирования распространения оружия массового уничтожения и по выявлению сомнительных и подозрительных операций, в соответствии с Законом Республики Узбекистан от 26.08.2004 г. N 660-II "О противодействии легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения" и других нормативно-правовых документов, касаемо этой области. Как результат - соответствие действующим и появляющимся нормативным актам в сфере противодействия отмыванию денег, с более прозрачным представлением о финансовой деятельности и рисках клиентов.

В ходе реализации проекта должны быть решены следующие задачи:

* анализ и оптимизация методологии механизмов оценки, управления и контроля в отношении ПЛПД/ФТ/ФРОМУ в части сопровождения внедрения Системы
* Развернуть передовую библиотеку предварительно настроенных, нестандартных, индустриальных сценариев Системы по всем направлениям бизнеса, чтобы быстро выполнить нормативные требования;
* Использование проверенных сценариев, которые в настоящее время разрабатываются во всем мире, и которые могут быть легко определены как различные правила, позволяющие бизнес-пользователям применять их без поддержки ИТ департаментов банка;
* Уменьшить ложные срабатывания и уменьшить время и усилия на реализацию с помощью моделей (сценариев), которые будут разработаны с точными параметрами и производительностью;
* Внедрить единую ИТ-платформу на базе передовых специализированных инструментов, которая позволит максимально автоматизировать процесс предотвращения отмывания денег;
* Обеспечить планируемую платформу необходимыми вычислительными ресурсами, и обеспечить надлежащую отказоустойчивость Системы;
* Обучить целевых пользователей Системы внутри Департамента внутреннего контроля Узнацбанка.

## 2.2. Цели реализации проекта

Цель проекта - создать единую платформу, которая позволит автоматизировать процесс внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения.

# 3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

**3.1. Общие сведения**

Национальный банк внешнеэкономической деятельности Республики Узбекистан (Узнацбанк) - универсальный коммерческий банк Узбекистана, создан в сентябре 1991 г.; является крупнейшим банком страны по объёму активов, сочетающим функции проектного финансирования, универсального коммерческого, инвестиционного и сберегательного банков.

Узнацбанк является универсальным коммерческим банком, предоставляющим весь спектр банковских услуг, включая инвестиционный бизнес, проектное и внешнеторговое финансирование, управление активами, расчётно-кассовое обслуживание частных и корпоративных клиентов, ипотечное и потребительское кредитование. Банк обладает разветвлённой филиальной сетью.

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

В миссии Банка заявлены задачи по созданию финансового института, способного на уровне международных стандартов обслуживать внешнеторговые операции отечественных компаний, содействовать повышению экспортного потенциала страны, привлекать в экономику Узбекистана иностранные инвестиции, передовые технологии. По сути, сегодня Узнацбанк является «визитной карточкой» банковской системы страны на международных финансовых рынках. Опираясь на консервативную, взвешенную политику, Банк выработал эффективные механизмы управления, стратегию роста. Это позволило ему уверенно и динамично развиваться, добившись прочной репутации профессионального финансового института, надежного партнера своих клиентов.

Банк стал активным проводником рыночных преобразований. Оптимально сочетая функции банка проектного финансирования, универсального коммерческого, инвестиционного и сберегательного банков, Узнацбанк способствует успешному вхождению Узбекистана в рыночную экономику.

В настоящий момент Банк оперирует развитой филиальной сетью, состоящей из Республиканского аппарата и 73 филиалов. Ниже приведена филиальная структура Банка:

**Таблица 3.1.1.** **Разветвлённая структура филиальной сети Банка**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование подразделения** | **Количество сотрудников** | **Количество филиалов** |
| 1 | Республиканский аппарат | 838 | 1 |
| 2 | ГУ по г. Ташкент | 1617 | 16 |
| 3 | Ташкентское областное отделение | 353 | 6 |
| 4 | Ферганское отделение | 329 | 5 |
| 5 | Бухарское отделение | 361 | 7 |
| 6 | Навоийское отделение | 270 | 5 |
| 7 | Самаркандское отделение | 376 | 6 |
| 8 | Каракалпакское отделение | 211 | 3 |
| 9 | Джизакское отделение | 173 | 3 |
| 10 | Ургенчское отделение | 287 | 6 |
| 11 | Андижанское отделение | 263 | 3 |
| 12 | Наманганское отделение | 265 | 5 |
| 13 | Термезское отделение | 196 | 3 |
| 14 | Сырдарьинское отделение | 65 | 1 |
| 15 | Каршинское отделение | 222 | 4 |
| **ИТОГО:** | | **5826** | **74** |

Ориентировочное количество пользователей Системы составляет 25 пользователей (из которых не менее 15 одновременных сессий пользователей), занимающихся обнаружением, расследованием и сообщением о подозрительных действиях по отмыванию денег и финансированию терроризма.

## 3.2. Архитектура и программно-аппаратный состав ИТ-комплекса

Приобретаемое в рамках проекта оборудование планируется разместить путем встраивания в текущую информационную сеть Узнацбанка, располагающегося по адресу: Республика Узбекистан 100084, г. Ташкент, проспект А. Темура, 101 и имеющую необходимую информационную инфраструктуру: серверные комнаты, информационно-коммуникационную систему, сетевую инфраструктуру, энерго и водоснабжение и пр.

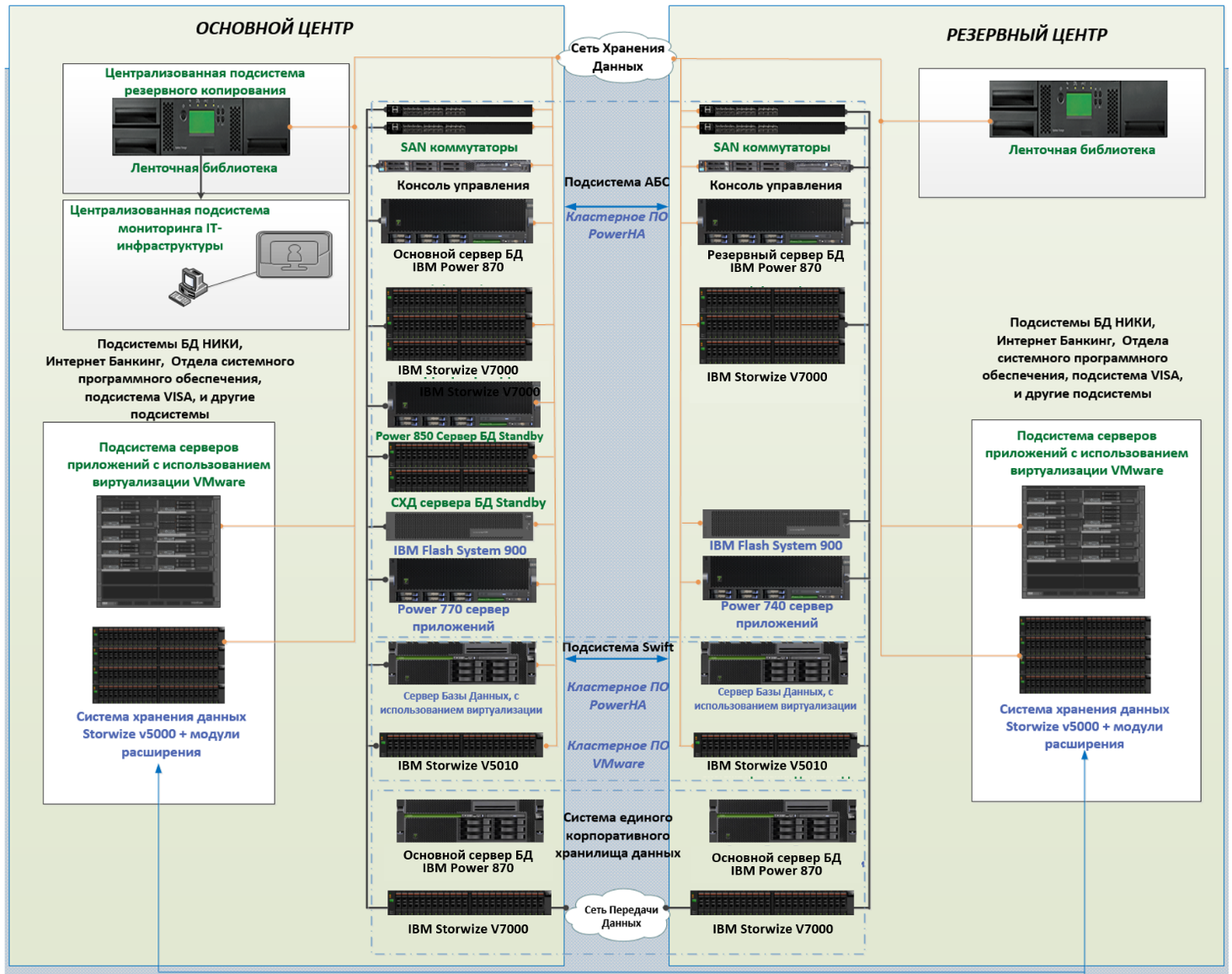
Текущая информационная вычислительная сеть Узнацбанк представляет собой систему из двух географически разнесённых вычислительных центров (ВЦ) - Основной центр (Головной офис) и Резервный Центр (МБРЦ). Каждый ВЦ состоит из серверов баз данных, а также подключенных к ним систем хранения данных. В основном и резервном ВЦ также функционируют сервера приложений, состоящие из Rack и стоечных серверов.

В случае выхода из строя Основного Центра информационной системы банка, включение и перераспределение ресурсов Автоматизированной банковской системы в Резервный Центр производится автоматически, используется кластерное программное обеспечение IBM PowerHA SystemMirror.

Действующая сетевая архитектура Узнацбанка состоит из двух больших подсистем.

Корпоративная сеть, построенная на собственной волоконно-оптической линии связи Узнацбанк - используется для связи между основным центром и МБРЦ, а также филиалами города Ташкента, имеющими собственные волоконно-оптические линии.

Корпоративная сеть передачи данных Узнацбанк с использованием арендованных каналов связи у таких операторов как БТС и Buzton - используется для связи между региональными филиалами банка.



**Рисунок 3.2.1. Логическая схема существующих**

**Центров Обработки Данных Узнацбанк**

Аппаратный состав комплекса можно разделить по принципу размещения целевых систем:

**Таблица 3.2.1.** **Автоматизированная банковская система**

|  |  |
| --- | --- |
| **ОСНОВНАЯ ТЕХНОЛОГИЧЕСКАЯ ПЛОЩАДКА** | |
| **НАИМЕНОВАНИЕ ОБОРУДОВАНИЯ** | **ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ** |
| **ОСНОВНАЯ ТЕХНОЛОГИЧЕСКАЯ ПЛОЩАДКА** | |
| Сервер базы данных IBM Power E870C (Основной) | 2x32 core processor Power 8, 4.02 GH, 4096 ГБ, 4x600Gb 15K, AIX 7.2 |
| IBM Standalone Hardware Management Console | Hardware appliance |
| Сервер БД IBM Power E850 (Standby) | 32 core Power 8, 1024 ГБ, AIX 7.1 |
| СХД IBM Storwize V7000 (Основной) | 256 Cache; 72x900GB 15K; 72x2.4TB 10K |
| СХД IBM Storwize V7000 (Standby) | 256 Cache; 120x600GB 15K; 96x1.8TB 10K |
| IBM Flash System 900 | 4.6 TB |
| Сервер приложений IBM Power 770 | 8 core, 64 ГБ, AIX 7.1 |
| Оптические SAN-коммутаторы | 24 из 48 портов активированы 16Гб/с |
| Оптические SAN-коммутаторы | 24 из 48 портов активированы 16Гб/с |
| Сервер базы данных IBM Power 870 (Основной) | 1x32 (12 active) core processor Power 8, 4.02 GH, 1024 ГБ, 6x300Gb 15K, SUSE |
| **РЕЗЕРВНАЯ ТЕХНОЛОГИЧЕСКАЯ ПЛОЩАДКА** | |
| Сервер базы данных IBM Power E870C | 2x32 core processor Power 8, 4.02 GH, 4096 ГБ, 4x600Gb 15K, AIX 7.2 |
| СХД Storwize v5000 | 6.23 TB |
| IBM Flash System 900 | 4.6 TB |
| Сервер приложений IBM Power 740 | 16 core, 128 ГБ, AIX |
| Оптические SAN-коммутаторы | 24 из 48 портов активированы 16Гб/с |
| Оптические SAN-коммутаторы | 24 из 48 портов активированы 16Гб/с |
| Сервер базы данных IBM Power 870 (Резервный) | 1x32 (12 active) core processor Power 8, 4.02 GH, 1024 ГБ, 6x300Gb 15K, SUSE |

**Таблица 3.2.2. Система SWIFT (МБРЦ)**

|  |  |  |
| --- | --- | --- |
| **ОСНОВНАЯ ТЕХНОЛОГИЧЕСКАЯ ПЛОЩАДКА** | | |
| Сервер базы данных IBM Power S914 | 1 | 6 core, 3.8 GH Power 9, 64 ГБ, 4x600Gb 15K, AIX 7.2 |
| IBM Storwize V5010 | 1 | 12x600Gb 15K |
| **РЕЗЕРВНАЯ ТЕХНОЛОГИЧЕСКАЯ ПЛОЩАДКА** | | |
| Сервер базы данных IBM Power S914 | 1 | 6 core, 3.8 GH Power 9, 64 ГБ, 4x600Gb 15K, AIX 7.2 |
| IBM Storwize V5010 | 1 | 12x600Gb 15K |

**Таблица 3.2.3. Подсистемы БД НИКИ, Интернет Банкинг, Отдела системного программного обеспечения, подсистема VISA и другие подсистемы**

|  |  |  |
| --- | --- | --- |
| **ОСНОВНАЯ ТЕХНОЛОГИЧЕСКАЯ ПЛОЩАДКА** | | |
| Сервера подсистемы приложений Lenovo PureFlex | 8 | 18С 2.3GHz 24.75MB Cache/140W, 256GB, 2x600GB 15K |
| Сервера подсистемы приложений Lenovo PureFlex | 2 | 18С 2.3GHz 24.75MB Cache/140W, 1024GB, 2x600GB 15K |
| IBM Storwize V5030 | 1 | 24x900GB 15K; 24x2.4TB 10K |
| **РЕЗЕРВНАЯ ТЕХНОЛОГИЧЕСКАЯ ПЛОЩАДКА** | | |
| Сервера подсистемы приложений Lenovo PureFlex | 8 | 18С 2.3GHz 24.75MB Cache/140W, 256GB, 2x600GB 15K |
| Сервера подсистемы приложений Lenovo PureFlex | 2 | 18С 2.3GHz 24.75MB Cache/140W, 1024GB, 2x600GB 15K |
| IBM Storwize V5030 | 1 | 24x900GB 15K; 24x2.4TB 10K |

**Таблица 3.2.4. Тестовый ЦОД**

|  |  |  |
| --- | --- | --- |
| **НАИМЕНОВАНИЕ ОБОРУДОВАНИЯ** | **КОЛ-ВО** | **ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ** |
| Сервера БД HP HL330 Gen 9 | 2 | 2 CPU E5504 2,00 GHZ, 8 ГБ |
| HP 30 Gen9 | 1 | 2 CPU E5504 2,00 GHZ, 8 ГБ |
| DELL POWER EDGE T630 | 1 | 2.40GHzx16CPU, 32ГБ, HDD(1,2ТБ x8 300ГБ x2 |
| FUJITSU PRIMERGY TX200 | 4 | 2CPUs x 2.00GHz, 8 ГБ, 1 ТБ+146 ГБ |
| FUJITSU PRIMERGY RX | 1 | 2CPUs x 2.40GHz, 80ГБ, 300ГБ+500ГБ+2ТБ |
| DELL POWER EDGE R410 | 2 | 2CPUs x 2.13 GHz, 4ГБ, 500ГБ+2ТБ |
| HP 380E | 8 | Windows 2012 Server  Windows 2003 Server  Windows 2008 Server |
| Fujitsu Primergy RX2520 M1 | 1 | Windows 2008 Server |
| HP Proliant ML 350 G6 | 1 | Windows 2003 Server |
| HP Proliant DL360 G7 | 1 | CPU - 2.4; RAM – 16 GB; HDD -4\*400GB |
| HP Proliant DL 180 G6 | 7 | CPU - 2.4; RAM -16GB; HDD 6\*300 GB |
| Fujitsu PrimeERGY RX2530 MI | 2 | CPU - 2.4; RAM 16 GB; HDD 4\*450 GB |
| HP ProLiant DL 360e Gen8 | 3 | CPU - 2.4; RAM 16 GB; HDD 4\*450GB |

На сегодняшний день в Узнацбанк используются следующие информационные системы: **Таблица 3.2.5. Информационные системы Банка**

|  |  |  |
| --- | --- | --- |
| **№** | **НАЗВАНИЕ СИСТЕМЫ** | **ОПИСАНИЕ** |
|  | **Внутренние системы** | |
| 1. | ИАБС | Автоматизированная банковская система Заказчика |
| 2. | Центр сертификации | Система управления сертификатами безопасности при обмене с расчетно-кассовыми центрами |
| 3. | R-Bank |  |
| 4. | 1С Бухгалтерия | Программа бухгалтерского и налогового учета |
| 5. | 1С Зарплата и кадры | Программа расчета ЗП и кадрового учета |
| 6. | БИС (КХД) |  |
| 7. | Корпоративное хранилище данных на базе SAP HANA | Корпоративное хранилище данных на базе платформы SAP HANA с возможностью гибкого бизнес анализа (BO/BI) |
| 8. | Кредитный конвейер | Кредитный конвейер на базе IBM BPM |
| 9. | Интеграционная шина | Единая интеграционная среда Банка на базе IBM ESB |
|  | **Внешние системы** | |
| 10. | РКЦ ЦБ | Рассчетно-кассовый центр Центрального Банка РУз |
| 11. | SWIFT | Международная межбанковская платежная система |
| 12. | PRIME | Международная межбанковская платежная система |
| 13. | НИББД | Национальная информационная база банковских депозиторов (НИББД) |
| 14. | Система НИКИ | Система Национального Института Кредитной Информации |
| 15. | АСОКИ | Автоматизированная система обмена кредитной историей. База кредитного бюро |
| 16. | Залоговый реестр | Система ГУП Залоговый реестр РУз |
| 17. | ЕПИГУ ГНК | Единый портал интерактивных государственных услуг |
| 18. | ЕИСВО | Единая электронная информационная система внешнеторговых операций |

* 1. Имеющиеся недостатки текущего процесса

В целях регулирования отношений в области противодействия легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения 26 августа 2004 года был принят Закон Республики Узбекистан №660-II «О противодействии легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения».

Действие настоящего Закона распространяется на граждан Республики Узбекистан, иностранных граждан и лиц без гражданства, юридических лиц, их филиалы и представительства, осуществляющие операции с денежными средствами или иным имуществом на территории Республики Узбекистан и за ее пределами в соответствии с международными договорами Республики Узбекистан, а также государственные органы, осуществляющие контроль на территории Республики Узбекистан за проведением операций с денежными средствами или иным имуществом.

Во исполнение данного закона разработаны и утверждены Правила внутреннего контроля для банков (зарегистрированы в МЮ РУз 23.05.2017г. №2886).

В Узнацбанке создано специальное самостоятельное независимое подразделение -Департамент внутреннего контроля (ДВК), осуществляющее свою деятельность в области ПОД/ФТ.

Система внутреннего контроля по ПЛПД/ФТ/ФРОМУ Узнацбанка осуществляет свою деятельность при взаимодействии Департамента внутреннего контроля и других подразделений Банка и включает в себя:

* Департамент внутреннего контроля;
* всех работников Банка.

ДВК определяют порядок организации и осуществления внутреннего контроля, в частности:

* выявление подозрительных и сомнительных операций на основании приведенного перечня критериев сомнительных и подозрительных операций;
* проведения надлежащей проверки клиентов при установлении хозяйственных и гражданско-правовых отношений, при проведении разовых операций, при проведении подозрительных и сомнительных операций;
* выявление уровня риска на основании представленной клиентом информации, с учетом видов деятельности и операций, совершаемых клиентом, критериев, установленных в соответствии Правил внутреннего контроля №2886.

Данная процедура по проведению надлежащей проверки клиентов осуществляется следующим образом:

* проверка личности и полномочий клиента и лиц, от имени которых он действует на основании соответствующих документов, с обязательным условием корректного внесения в АБС «ИАБС» данных о клиенте;
* идентификация бенефициарного собственника клиента, с обязательным условием корректного внесения в АБС «ИАБС» данных о клиенте;
* изучение цели и характера деловых отношений или запланированных операций;
* проведение на постоянной основе изучения деловых отношений и операций, осуществляемых клиентом, в целях проверки их соответствия сведениям о таком клиенте и его деятельности;
* на каждого клиента согласно информация о клиенте, полученная в процессе надлежащей проверки сотрудниками формируется и заполняется анкета (данные берутся из АБС «ИАБС»);
* сведение анкеты должны обновляться при наличии изменений в сведениях клиента, также при установлении клиенту высокий уровень риска согласно критериям Правил внутреннего контроля №2886, не реже одного раза в год, в иных случаях не реже одного раза в 2 года;
* клиенты осуществившего разовую операцию, обновляются при следующем осуществлении операции, по которой требуется принятие мер надлежащей проверки клиента.

На каждого клиента заполняется анкета (данные берутся из АБС «ИАБС») с внесенными информациями по всем совершенным подозрительным операциям по переданным сообщениям в СУГО.

Проводимые работы в области ПОД/ФТ в АО «Узнацбанк»:

Выявление подозрительных и сомнительных операций осуществляется вручную на основе мониторинга банковских операции по поручениям клиентов и операции, осуществляющихся программой по дистанционной услуге «I-Bank», а также через мобильное приложение «Миллий». Отсутствует возможность проведения количественного анализа сомнительных операций по одному и тому же клиенту. В связи с чем, сомнительные операции рассматриваются как подозрительные.

Установление риска клиенту осуществляется вручную на основе критериев Правил внутреннего контроля № 2886, по типам и деятельности клиентов, банковским средствам и услугам, каналам поставок, географическим регионам.

Идентификация клиента проводится в виде сверки с паспортными данными через ЦБ РУз в Государственном центре персонализации, помимо того, что клиент при этом присутствует с документом, подтверждающим его личность. Данные о юридических лицах берутся из «Центра государственных услуг», там же проходит регистрация, и сверка с данными ГНК РУз.

Согласно требованиям Положения о порядке предоставления информации, связанной с противодействием легализации доходов, полученных от преступной деятельности, и финансированию терроризма, утвержденного постановлением Кабинета Министров Республики Узбекистан от 12 октября 2009 года №272, предоставление сообщений в СУГО предусмотрено не позднее одного рабочего дня, с момента выявления подозрительной операции. При этом каждое сообщение формируется в программе «Moneyoper» и в зашифрованном виде передается по каналу Lotus. Информация о каждом сообщении заносится в специальный журнал.

В настоящее время в Банке используется услуга «WORLD CHECK» для определения ПДЛ и в соответствии с этим проставляются уровни рисков. В АБС «ИАБС» интеграция с международными списками реализована при условии полного и точного введения данных клиентов Банка и контрагентов операции ответственными сотрудниками Банка.

Также, используется список лиц, входящий в Перечень - делится на международный и национальный, а также в свою очередь по физическим и юридическим лицам, список Антитеррористического центра (АТЦ), и список «Наемники». Данные списки предоставляются со стороны Департамента по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан.

В настоящий момент приостановка проведения подозрительных операций происходит следующим образом:

* выявление среди участников операции лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения, путем сверки с Перечнем - *на данный момент идет проверка по совпадению со списками (на данный момент ловит при открытии карточки клиента и при проведении денежных переводов отправитель (получатель тестируется));*
* безотлагательное приостановление операции, за исключением операций по зачислению денежных средств, поступивших на счет юридического или физического лица, и (или) замораживание денежных средств или иного имущества лиц, включенных в Перечень, без их предварительного уведомления, в случае установления полного совпадения всех идентификационных данных клиента или одного из участников операции с лицом, включенным в Перечень.

Меры, принимаемые при выявлении операций с участием лиц, включенных в Перечень:

Если во время установления отношений или при проведении операции, сотрудниками Банка будет установлено полное совпадение всех идентификационных данных клиента или одного из участников операции с лицом, включенным в Перечень, Банк безотлагательно и без предварительного уведомления должен приостановить операцию, за исключением операций по зачислению денежных средств, поступивших на счет юридического или физического лица, и (или) заморозить денежные средства или иное имущество лиц, включенных в перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения, а также направить сообщение о подозрительной операции в специально уполномоченный государственный орган.

В свою очередь Департамент внутреннего контроля должен предпринять следующие меры по:

- подробной идентификации личности клиента, бенефициарного собственника клиента либо одного из участников операции.

- выявлению денежных средств или иного имущества по операции, подлежащих замораживанию в соответствии с требованиями законодательства и настоящих Правил;

- подготовке сообщения о подозрительной операции с указанием суммы замороженных денежных средств или иного имущества, и передача сообщения в СУГО в день ее приостановления;

- получению дополнительной информации о клиенте (в том числе род деятельности, размер активов, информация, доступная через открытые базы данных и т. п.);

- определению источника денежных средств или источника финансового состояния клиента, в том числе путем получения от клиента информации;

В случае приостановления операции списание денежных средств со счетов, на основании распоряжения клиента не производится.

Замораживание осуществляется коммерческим банком в отношении денежных средств или иного имущества, которое находится в его непосредственном владении.

Коммерческий банк возобновляет проведение приостановленной операции и предоставляет доступ к замороженному имуществу в порядке, установленном [Положением](http://lex.uz/ru/docs/3042462#3042919) о порядке приостановления операций, замораживания денежных средств или иного имущества, предоставления доступа к замороженному имуществу и возобновления операций лиц, включенных в перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения.

Текущая ситуация по системе AntiFraud:

* данная система в банке не реализована;
* в банке нет подразделения для выявления и анализа мошеннических операций;
* Департамент внутреннего контроля подключается только при выявлении мошенничества;
* отсутствуют отчёты, при проведении операций, которые не имеют экономического смысла и не соответствуют характеру и виду деятельности клиента. Не проводится анализ автоматическим путем с получением данных из ИАБС.

Во исполнение всех требовании Правил внутреннего контроля для банков (зарегистрированы в МЮ РУз 23.05.2017г. №2886) и устранения имеющихся недостатков в текущем процессе, считаем целесообразным, внедрение Системы AntiFraud.

**3.4. Обоснование выбора аппаратной платформы**

### 3.4.1. Модернизация текущих серверов базы данных IBM Power

На текущий момент для нужд Корпоративного хранилища данных Банком эксплуатируются сервера базы данных IBM Power 870, расположенных в территориально разнесенных дата центрах. Данные сервера являются серверами базы данных класса Enterprise с возможностью гибкого наращивания вычислительных мощностей. Ниже приведены данные о текущей загруженности серверов и возможностях дальнейшего наращивания мощностей:

**Таблица 3.4.1.1**

**Возможность модернизации системы хранения данных IBM Power 870**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Оборудование** | **Установленные ресурсы** | **Активированные ресурсы** | **Спящие ресурсы** |
| 1 | Сервер базы данных  IBM Power 870 (Основной) | CPU: 32-core POWER8 processor  RAM: 1024 GB | CPU: 12-core POWER8 processor  RAM: 1024 GB | CPU: 20-core POWER8 processor  RAM: 0 GB (при текущей конфигурации возможно нарастить до 2 Тб) |
| 2 | Сервер базы данных  IBM Power 870 (Резервный) | CPU: 32-core POWER8 processor  RAM: 1024 GB | CPU: 12-core POWER8 processor  RAM: 1024 GB | CPU: 20-core POWER8 processor  RAM: 0 GB (при текущей конфигурации возможно нарастить до 2 Тб) |

Т.е. имеющиеся сервера базы данных имеют запас мощности и возможность для дальнейшей модернизации. Таким образом для обеспечения бесперебойной работы Системы целесообразна модернизация вычислительных мощностей текущих серверов БД IBM Power E870. При этом использование в тендерных документах оборудования компании “IBM” сохраняет инвестиции в:

- Сохранение ресурсов благодаря исключению перехода серверной инфраструктуры на иную аппаратную и программную платформу;

- Сохранение ресурсов на обучение персонала новым технологиям при работе с кардинально новой платформой;

- Продолжение использования всех преимуществ высокотехнологичной платформы;

- Своевременная аналитика и мониторинг аппаратно-программной платформы;

- Гибкое управление серверной инфраструктурой, построенной на базе одного производителя;

- Снижение времени устранения различных неполадок, благодаря своевременным аналитическим данным мониторинга серверного оборудования.

Использование оборудования и программных продуктов других производителей повлечет за собой возможное возникновение несовместимости с текущей серверной архитектурой, переподготовку ИТ специалистов, а это в свою очередь повлечет за собой дополнительные расходы.

Учитывая все вышеперечисленные факты, а также руководствуясь статьей 14 «Антимонопольные требования к конкурсным (тендерным) торгам» Закона Республики Узбекистан №ЗРУ-319 от 06.01.2012г., согласно которой «при проведении конкурсных (тендерных) торгов запрещаются действия, которые приводят или могут привести к ограничению конкуренции, в том числе: указание конкретного производителя товара, за исключением несовместимости товаров и иных случаев, предусмотренных законодательством» можно определить, что для модернизации серверов базы данных Банка, в частности IBM Power E870 является целесообразным использование оборудования и программных продуктов производителя «IBM». Также в соответствии с пунктом 11 Положения о порядке проведения комплексной экспертизы тендерной документации и технического задания на государственную закупку товаров (работ, услуг), утвержденного Постановлением Президента Республики Узбекистан «О мерах по совершенствованию порядка проведения экспертизы предпроектной, проектной, тендерной документации и контрактов» от 20.02.2018 года № ПП-3550 в случае, если в требованиях к товарам (работам, услугам) указаны товарные знаки, знаки обслуживания, патенты, полезные модели, промышленные образцы, наименование места происхождения товара или наименование производителя, должна быть представлена дополнительная информация, раскрывающая обоснованность их указания, в том числе наличие в технической части тендерной документации или техническом задании возможности поставки эквивалента товаров (работ, услуг). Соответственная дополнительная и обосновывающая информация Узнацбанком в подразделе 3.4 настоящего технического задания приведена.

### 3.4.2. Модернизация текущей системы хранения данных

Текущая система хранения данных подсистемы приложений Узнацбанка построена на базе IBM Storwize V5030. Данная система является гибридной и позволяет гибко наращивать объем хранения данных до 760 дисковых накопителей на систему. Ниже приведена текущая конфигурация системы:

**Таблица 3.4.2.1**

**Возможность модернизации системы хранения данных IBM Storwize V5030**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Текущее оборудование** | **Текущая конфигурация** | **Запас модернизации** |
| 1 | IBM Storwize V5030 (Основной СХД) | 64 ГБ кэш памяти  24 х 900 Гб 15К  24 Х 2,4 Тб 10К | Возможность добавления еще 19 полок расширения. |
| 2 | IBM Storwize V5030 (Основной СХД) | 64 ГБ кэш памяти  24 х 900 Гб 15К  24 Х 2,4 Тб 10К | Возможность добавления еще 19 полок расширения. |

При этом следует учесть, что загруженность системы хранения данных подсистемы приложений на сегодняшний день составляет более 96% как для Основного так и для Резервного дата центров, из них:

- накопители SAS 15k – из 15,6Тб занято 15 Тб (перегрузка 96%);

- накопители SAS 10k – из 41,6Тб занято 40 Тб (перегрузка 96%).

Данные объемы хранения используются для нужд среды виртуализации, включающей в себя подсистему приложений критичных сервисов банка, включая систему ИАБС, а также внутренние разработки банка. Объем системы хранения для Системы и подсистемы приложений Банка в рамках проекта приведен с учетом бесперебойной эксплуатации Системы и подсистемы приложений в целом на ближайшие 3 года.

Учитывая, что основная стоимость системы СХД заложена в контроллере (модуле управления), то целесообразно в дальнейшем наращивать объем хранения данных Банка путем добавления полок расширения с необходимым объемом, количеством и скоростью дисковых накопителей. При этом, сотрудники ДИТ Банка на текущий момент эксплуатируют систему хранения данных с подобной архитектурой с 2015 года, и за это время прошли специальное обучение, ознакомлены и специализируются на таком оборудовании, в частности в управлении и мониторинге системы хранения данных. Более того, на протяжении 5 лет эксплуатации подсистемы хранения данных на базе оборудования расширяемой СХД, Банк на сегодняшний день обладает своей внутренней экспертизой, что позволяло обеспечивать бесперебойную работу критичных сервисов Банка.

Исходя из вышеизложенного, работники ДИТ банка проанализировав существующее состояние системы хранения данных и планируемые нагрузки на систему, разработали карту проектов Банка, согласно которому Банк будет строить свою систему хранения данных на базе отказоустойчивых, масштабируемых решений, что позволит:

* Сохранить ресурсы благодаря исключению перехода серверной инфраструктуры на иную аппаратную и программную платформу;
* Сохранить ресурсы на обучение персонала новым технологиям при работе с кардинально новой платформой;
* Продолжить использование всех преимуществ высокотехнологичной платформы;
* Проводить своевременную аналитику и мониторинг аппаратно-программной платформы;
* Сохранить гибкое управление серверной инфраструктурой, построенной на базе одного производителя;
* Снизить время устранения различных неполадок, благодаря своевременным аналитическим данным мониторинга серверного оборудования.

### 3.4.3. Модернизация подсистемы приложений

В Узнацбанкеподсистема приложений построена на базе системы блейд-шасси Lenovo PureFlex. Данное решение подразумевает собой блейд-шасси с предустановленными оптическими и сетевыми коммутаторами, системой охлаждения, питания и централизованным управлением виртуальной средой. Это масштабируемый комплекс высокой доступности, который позволяет гибко наращивать вычислительные мощности путем добавления до 14 серверов-лезвий. На текущий момент в блейд-шасси установлено 10 блейд-серверов (Таблица 3.2.3) на каждый сайт (Основной и Резервный). При этом, вычислительные ресурсы каждого сервера могут быть расширены. Ниже приведена текущая загруженность подсистемы приложений на базе Lenovo PureFlex.

**Таблица 3.4.3.1**

**Возможность модернизации подсистемы приложений Lenovo PureFlex**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Оборудование** | **Установленные ресурсы** | **Эксплуатируемые ресурсы** | **Свободные ресурсы** |
| 1 | Lenovo PureFlex SN550 (Основной) | 7 лезвий, в каждом:  CPU: 36-core Intel Xeon processor  RAM: 256 GB | 7 лезвий, в каждом:  CPU: 36-core Intel Xeon processor  RAM: 256 GB | Свободных ресурсов нет |
| 2 | Lenovo PureFlex SN550 (Резервный) | 7 лезвий, в каждом:  CPU: 36-core Intel Xeon processor  RAM: 256 GB | 7 лезвий, в каждом:  CPU: 36-core Intel Xeon processor  RAM: 256 GB | Свободных ресурсов нет |
| 3 | Lenovo PureFlex SN550 (Основной) | 1 лезвие, в котором:  CPU: 36-core Intel Xeon processor  RAM: 256 GB | 1 лезвие, в котором:  CPU: 18-core Intel Xeon processor  RAM: 256 GB | CPU: 18-core Intel Xeon processor  RAM: свободных ресурсов нет |
| 4 | Lenovo PureFlex SN550 (Резервный) | 1 лезвие, в котором:  CPU: 36-core Intel Xeon processor  RAM: 256 GB | 1 лезвие, в котором:  CPU: 18-core Intel Xeon processor  RAM: 256 GB | CPU: 18-core Intel Xeon processor  RAM: свободных ресурсов нет |
| 5 | Lenovo PureFlex SN550 | 2 лезвия, в каждом:  CPU: 36-core Intel Xeon processor  RAM: 1024 GB | 2 лезвия, в каждом:  CPU: 36-core Intel Xeon processor  RAM: 1024 GB | Свободных ресурсов нет |
| 6 | Lenovo PureFlex SN550 | 2 лезвия, в каждом:  CPU: 36-core Intel Xeon processor  RAM: 1024 GB | 2 лезвия, в каждом:  CPU: 36-core Intel Xeon processor  RAM: 1024 GB | Свободных ресурсов нет |

Как видно из таблицы выше, в текущей подсистеме приложений имеются свободные ресурсы процессора. Недостающие вычислительные ресурсы оперативной памяти могут быть наращены путем добавления дополнительных модулей памяти. При этом текущий программно-аппаратный комплекс имеет централизованное отказоустойчивое управление и систему мониторинга виртуальной среды включаемых в нее серверных-модулей и инструментов виртуализации, а также отказоустойчивый кластер средствами VMWare. Для управления хостами ESXI как единым комплексом, в рамках одного вычислительного центра установлен модуль управления виртуализации.

Для модернизации подсистемы серверов приложений целесообразно использовать дополнительное наращивание вычислительных мощностей оборудования и программных продуктов Единого производителя, что позволит:

* избежать дополнительных расходов на отдельное коммутационное оборудование для серверов приложений, т.к. в имеющемся комплексе блейд-системы они уже имеются;
* сохранить целостность системы централизованного управления и мониторинга виртуальной средой всего комплекса;
* избежать дополнительных затрат на переобучение персонала, так как работники ДИТ Банка пройдут специальные курсы по эксплуатации, управлению и мониторингу оборудования и ознакомлены с работой программно-аппаратного комплекса.

### 3.4.4. Расширение текущей системы резервного копирования подсистемы приложений

Текущая система резервного копирования подсистемы приложений функционирует на базе программного комплекса Veeam Availability Enterprise Suite с 2018 года. Данная система позволяет осуществлять централизованное управление процессом резервного копирования и восстановления всех критичных сервисов банка, эксплуатируемых на CISC архитектуре. С целью сохранения целостности текущей системы резервного копирования и восстановления, а также для поддержки надежной и бесперебойной работы, минимизации потерь данных, сотрудниками ДИТ было принято решение поддерживать систему на базе ПО Veeam. В связи с этим, Исполнителю необходимо предоставить свое предложение на модернизацию подсистемы приложений с учетом расширения текущей системы резервного копирования и восстановления на базе этого программного продукта.

4. ТРЕБОВАНИЯ К СИСТЕМЕ

## 4.1. Требования к системе в целом

Система, предоставляемая в пользование, должна быть основана на базе готовых пакетов прикладного программного обеспечения, предоставляющих возможность определять наборы модульных компонентов и сервисов.

Система должна иметь возможность обмениваться информацией из/в ИАБС Банка и должна располагаться на серверах Банка.

Система должна иметь возможность дальнейшей модернизации, как программного обеспечения, так и комплекса технических средств. Также необходимо предусмотреть возможность увеличения функциональности системы путем ее модульного расширения и масштабирования.

Система должна иметь возможность предоставить промежуточную область для проверки и отображения данных перед загрузкой в системную базу данных;

Система должна иметь возможность загрузки данных дня несколькими партиями в течение дня и с разными сроками;

Система должна иметь возможность планировать и автоматизировать процесс загрузки данных;

Система должна иметь возможность загрузки основной, клиентской, учетной записи, данных транзакций и т. д.;

Система должна иметь возможность идентифицировать всех клиентов Банка, а также идентифицировать физических лиц при осуществлении разовых операций, в том числе путем совершения одной или нескольких операций, связанных между собой по критериям, предусмотренным в Правилах №2886.

Система должна иметь возможность изменения оценки риска клиента, согласно требованиям Правил №2886 и экспортировать определенный формат файла и поля во внешний файл ежедневно. Например, экспорт клиентов высокого риска для обновления профиля клиента в основной банковской системе (ИАБС) и обеспечить доступный просмотр;

Система должна иметь возможность настроить контроль безопасности данных и функций по ролям и правам доступа (Создать, Читать, Обновить и Удалить);

Система должна иметь возможность настройки матрицы безопасности пользователя и группы;

Система должна иметь возможность предоставить пользовательские интерфейсы для управления загруженным файлом, такие как хранилище для мониторинга, контроль размера файла и т. д.;

Система должна иметь возможность экспорта или передачи данных в другой инструмент отчетности / аналитики.

Система должна иметь возможность обнаружения идентичный / похожий профиль клиента с созданным другим идентификатором.

Система должна иметь возможность предоставления инструмента моделирования для тестирования новых правил обнаружения / пересмотра правил обнаружения.

Система должна иметь возможность формирования отчетов по установленным рискам и выявленным и / или переданным подозрительным операциям.

Система должна иметь возможность хранения информации об операциях, а также хранения идентификационных данных и материалов по надлежащей проверке клиентов в течение сроков, установленных законодательством, но не менее пяти лет после осуществления операций или прекращения деловых отношений с клиентами.

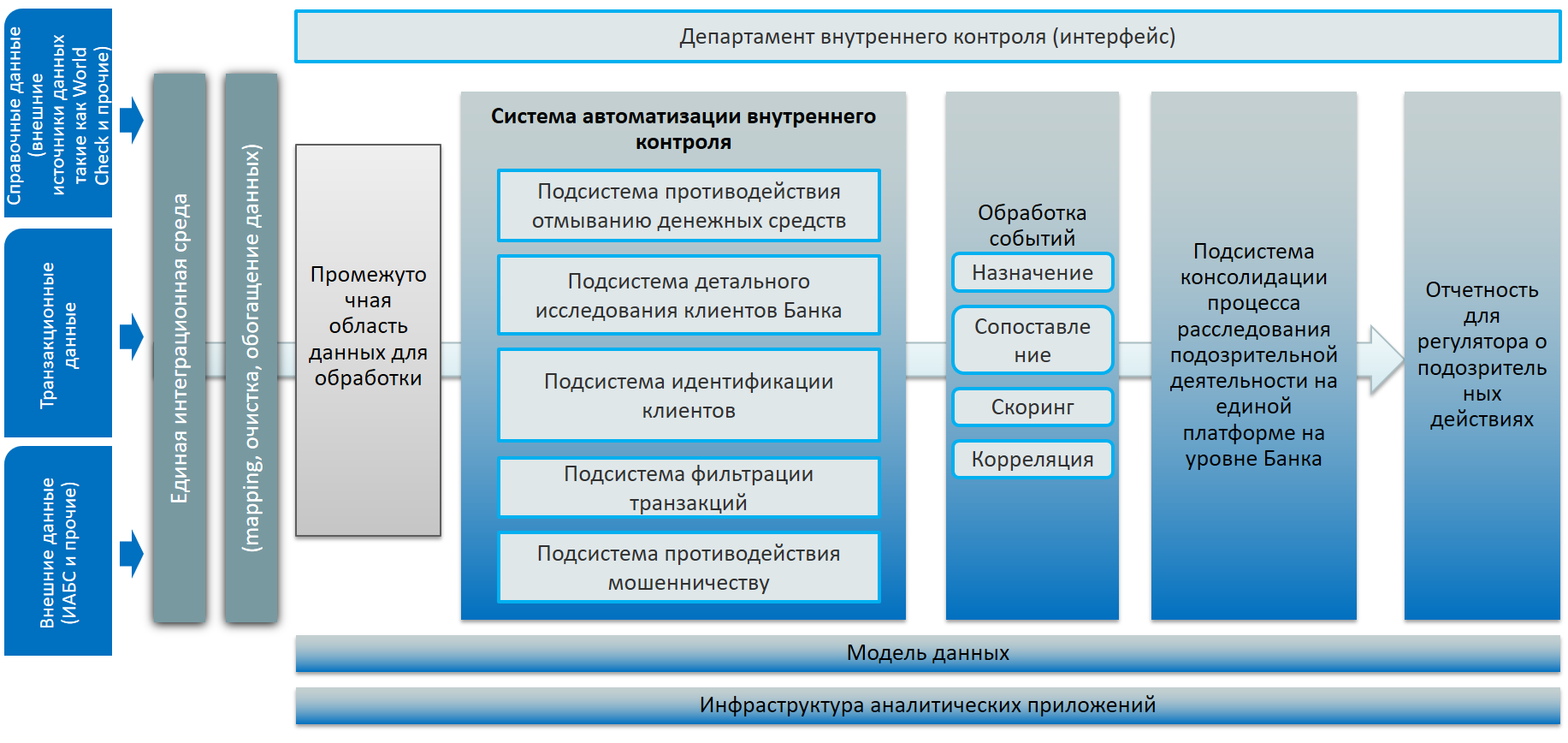
В рамках проекта Исполнителем также должны быть выполнены работы по анализу и оптимизации методологии механизмов оценки, управления и контроля в отношении ПЛПД/ФТ/ФРОМУ в части сопровождения внедрения Системы, в частности:

1. Провести диагностику текущих бизнес процессов, механизмов/подходов, связанных с управлением комплаенс риском в Узнацбанке, в части:

* первичной идентификации клиентов (оn-boarding) и повторной верификации, учитывая степень риска клиентов;
* расширенной проверки клиента;
* надлежащей проверки клиентов;
* постоянной проверки клиентов.

1. Проанализировать эффективность, целостность бизнес процессов верификации транзакций клиентов на предмет сомнительности\подозрительности c учетом триггеров и предпринимаемых превентивных мер Банком по снижению первоначальных\остаточных рисов и соблюдению локального и международного законодательства.
2. Оказать поддержку по оптимизации, устранению выявленных разрывов и внедрению внутренних ключевых регламентов, механизмов/подходов, связанных с управлением комплаенс риском в Банке в отношении аспектов ПЛПД/ФТ/ФРОМУ c учётом внедрения Системы.
3. Сопровождение процесса создания Структурного подразделения с функциями выявления, анализа мошеннических операций и расследования подозрительной деятельности клиентов.

Обучение ключевого пользователей Системы подходам и международным практикам\бенчмаркам по управлению комплаенс риском в части противодействия отмыванию денежных средств (AML). Ниже приведена схема планируемой архитектуры системы автоматизации внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения в Узнацбанке с приведением взаимодействия с внешними системами (Рисунок 4.1.1).



**Рисунок 4.1.1. Схема планируемой архитектуры системы**

### 4.2. Требования к структуре и функционированию системы

**4.2.1. Требования к структуре Системы**

Целевая схема должна включать наличие следующих основных подсистем:

1. Противодействие отмыванию денежных средств (AML)

2. Консолидация процесса расследования подозрительной деятельности на единой платформе на уровне Банка (ECM)

3. Детальное исследование клиентов банка (KYC)

4. идентификация клиентов, упомянутых в списках особого внимания (CS)

5. Фильтрация транзакций (TF)

6. Противодействие мошенничеству (Fraud).

Назначение каждой подсистемы приведено в подразделе 4.2.3.

**4.2.2. Требования к режимам функционирования системы**

Система должна функционировать в круглосуточном режиме и обеспечивать возможность работы в следующих режимах:

1. Штатный режим (непрерывная круглосуточная работа):

Штатный режим обеспечивает выполнение функций системы. Это основной режим работы. В штатном режиме функционирования системы:

* клиентское программное обеспечение на рабочих местах пользователей обеспечивает возможность круглосуточного функционирования с регламентированными перерывами на техническое обслуживание и обновление программного обеспечения;
* серверное программное обеспечение обеспечивает возможность круглосуточного функционирования с регламентированными перерывами на техническое обслуживание и обновление программного обеспечения.

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

1. Сервисный режим (для проведения обслуживания, реконфигурации и пополнения новыми компонентами).

Сервисный режим предназначен для обновления и профилактического обслуживания программно-аппаратных средств, изменения конфигурации компонентов.

Сервисный режим функционирования используется для выполнения операций подготовки и проведения регламентов, испытаний или значительной перестройки системы.

В данном режиме система недоступна для пользователей.

В данном режиме также осуществляется техническое обслуживание, реконфигурация, модернизация и совершенствование системы.

Режим позволяет проводить диагностирование инцидентов или проблем, связанных со сбоями или авариями в работе системы.

Сервисный режим предназначен, прежде всего, для проведения регламентных работ и профилактики системы:

* проведение обслуживания комплекса технических средств системы;
* установка обновлений общесистемного и специального программного обеспечения;
* контроль работоспособности компонентов системы;
* выполнение «холодного» резервного копирования базы данных;
* реконфигурации и замены компонент системы и т.д.).

**4.2.3. Перспективы развития, модернизации системы**

Система должна обеспечивать возможность модернизации и развития при необходимости изменения состава требований к выполняемым функциям и видам обеспечения.

Модернизация и Системы должны проводиться экспертами в предметной области и прикладными программистами.

Порядок Системы уточняется Исполнителем в процессе разработки технического проекта и согласовывается с Заказчиком;

Минимально допустимый срок эксплуатации Системы при этом должен быть не менее 10 лет.

**4.2.4. Перечень и описание сценариев использования ИС**

Система подразумевает следующие возможные сценарии использования:

1. Противодействие отмыванию денежных средств (AML)

Автоматизированное, комплексное и последовательное наблюдение за всеми счетами, клиентами, корреспондентами и третьими сторонами в транзакциях по всем направлениям бизнеса. Ежедневное отслеживание транзакций клиентов с использованием исторической информации о клиентах и профилях счетов, обеспечение целостного представления обо всех транзакциях и действиях с целью:

• обнаружения и расследования случаев предполагаемой деятельности по отмыванию денежных средств;

• предоставления регулятивным органам и ключевым заинтересованным сторонам комплексной информации о финансовой деятельности и рисках клиентов в связи с результатами расследования потенциальных возможностей отмывания денежных средств;

• повышения доверия клиентов и снижения репутационного риска.

2. Консолидация процесса расследования подозрительной деятельности на единой платформе на уровне Банка (ECM)

Повышение эффективности процессов расследования подозрительных событий через выявление корреляции между событиями и объектами. Создание единого интерфейса для изучения множества коррелирующих подозрительных событий на уровне всего Банка.

Процесс корреляции исследует события и объекты, связанные с этими событиями, оценивая их по отдельности и как часть связанной сети, чтобы определить, следует ли их обобщить для совместного исследования ответственным сотрудником Банка. Сети связанных событий и объектов формируются на нескольких уровнях, таких как общие атрибуты, найденные:

– в самих событиях;

– в справочных данных, связанных с этими событиями;

– в любых других внутренних или внешних данных, относимых к процессу исследования.

Оценка должна быть основана как на детерминированных правилах, так и на моделях машинного обучения в зависимости от требуемой сложности.

3. Детальное исследование Клиентов Банка (KYC)

Комплексная оценка каждого Клиента, надежная аналитика рисков и настраиваемые возможности рабочего процесса, интегрированные с решением по Противодействию отмыванию денежных средств.

Использование решения для:

- Оценки рисков, связанных с открытием нового счета, в том числе при совершении разовых операций и внесении данных в «карточку клиента без открытия счета»;

- CDD – Customer Due Diligence (надлежащая проверка);

- EDD – Enhanced Due Diligence (углубленная надлежащая проверка)

- Поддержки услуг по верификации, предоставляемых внешними аналитическими приложениями.

- Мониторинг и анализ состояния Клиентов для предотвращения рискованных транзакций; возможность глубокого исследования всех транзакций клиентов с высокой оценкой степени рисков.

4. Идентификация Клиентов, упомянутых в списках особого внимания (CS)

Идентификация Клиентов, которые могут быть соотнесены с физическими или юридическими лицами, представленными в списках особого внимания:

– Физические и юридические лица, входящие в Перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения;

– Физические и юридические лица участвующие в операции и действующие от имени или по поручению лица, включенного в Перечень;

– Юридическое лицо — участник операции, находящийся в собственности или под контролем лица, включенного в Перечень;

– Публичные должностные лица, члены их семей и лица, близкие к публичным должностным лицам

– Физические лица с участием лиц, включённых в списки Анти Террористического Центра СНГ.

Возможность ручного рассмотрения всех возможных соответствий (Alerts)

Организация рабочего процесса трассировки и управления статусом для каждого возможного соответствия:

– Реальное соответствие,

– Ложное срабатывание,

– Сохранение аудиторского следа для всех решений.

5. Фильтрация транзакций (TF)

Идентификация финансовых транзакций, которые могут включать в качестве фигурантов лиц из списков особого внимания в реальном времени.

Блокировка подозрительных транзакции с предоставлением пользователю возможности ручного рассмотрения этих транзакций.

Минимизация ложных срабатываний, которые могут привести к «засорению»: транзакции повисают в состоянии ожидания до момента принятия решения.

Поддержка аудиторского следа для всех решений.

6. Противодействие мошенничеству (Fraud)

Формирование платформы централизованного управления противодействием мошенничеству, которая позволяет Банку быстро выявлять и предотвращать сложные схемы и изощренные случаи мошенничества, чтобы минимизировать потери, максимизировать доверие клиентов и снизить репутационный риск.

Формирование платформы централизованного управления для определения сделок с участием аффилированных лиц Банка и (или) акционерами Банка или лицами, сделки с которыми осуществляются на льготных условиях с целью выявления мошеннических и (или) коррупционных правонарушений.

Необходимость быстрого предоставления сведений о подозрительном поведении отдельным подразделениям и предупреждения клиентов о любой непредвиденной деятельности.

**4.2.5. Требования к диагностированию системы**

Диагностика программных и технических средств должна осуществляться с помощью стандартных режимов системных операционных систем, операционных систем отдельных рабочих станций, а также путем прогона контрольного примера.

Программные модули должны иметь компоненты по методике испытаний и тестирования, позволяющие провести контроль возможности функционирования основных режимов работы модулей.

При вводе в опытную эксплуатацию отдельных подсистем специалистами Исполнителя совместно с обслуживающим персоналом системы должно быть проведено полное тестирование и диагностика всех вводимых в опытную эксплуатацию элементов системы (активного сетевого оборудования, серверных кластеров, программного обеспечения (ПО) среды электронного взаимодействия, операционных систем серверов, СУБД и специального программного обеспечения (СПО).

В процессе эксплуатации системы, тестирование и диагностика программно-технических комплексов должны осуществляться системным администратором в автоматическом режиме при ее запуске.

В рамках разработки Программы и методики испытаний должен быть сформирован контрольный пример, обеспечивающий проверку работоспособности узлов и подключения взаимодействующих информационных систем как при первоначальной установке и загрузке базы данных, так и в процессе повседневной работы.

### 4.2.6. Требования к численности и квалификации пользователей системы и режиму их работы

Система должна обеспечивать до 15 одновременных сессий и при этом поддерживать работу 25 пользователей. Детальные требования к функциональным группам, составу, квалификации конечных пользователей Системы должны быть определены на этапе разработки Технического проекта в соответствии с организационной структурой, определенной на этапе обследования объекта автоматизации.

Какие-либо специфические квалификационные требования к пользователям Системы не предъявляются. Пользователи должны отвечать следующим квалификационным характеристикам:

* навыки работы с персональной компьютерной техникой и офисными приложениями;
* знание предметной области;
* знание эксплуатационной документации на Систему;
* прохождение на этапе эксплуатации учебных курсов по работе с Системой под руководством организации-поставщика или разработчика;
* наличие допуска для работы с Системой.

Решение о допуске пользователя к работе с Системой принимается руководством или администратором.

На техническую поддержку работоспособности Системы должен быть разработан и согласован с Заказчиком документ, регламентирующий порядок проведения консультаций и допуска к работе администраторов с Системой.

В Системе должны быть предусмотрены следующие роли пользователей (Таблица 4.2.6.1.):

Таблица 4.2.6.1. Описание ролей пользователей Системы

|  |  |
| --- | --- |
| **Роль** | **Описание полномочий в Системе** |
| Исполнитель | * Возможность выявления и сбора сведений и информации об операциях клиентов, подлежащих финансовому мониторингу, согласно Законодательству РУ; * Возможность сбора и анализа данных по операциям клиентов, полученных с помощью отчетов и по информации, переданной сотрудниками филиала, для принятия решения о составлении электронного сообщения в СУГО; * Возможность составления электронного сообщения в СУГО, на основе выявленных сомнительных и подозрительных операций и передача данных на отправку в СУГО; * Возможность составления отчетности переданных сообщении в СУГО, на основе выявленных сомнительных и подозрительных операций; * Возможность работы с данными юридических и физических лиц -клиентов Банка, с целью получения полной информации о клиентах и их деятельности; * Возможность работы, осуществления текущего контроля над формированием анкеты клиентов.(полноты заполнения и обновления) * Возможность установления риска клиентам, на основе представленной клиентом информации с учетом видов деятельности и операций, совершаемых клиентом, критериев, установленных Правилами внутреннего контроля № 2886, результатов надлежащей проверки клиента, факторов риска (по типам и деятельности клиентов, банковским средствам и услугам, каналам поставок, географическим регионам и другие) и составления и составления отчеты по ним * Возможность выявления, оценки, документального фиксирования и снижение рисков юридическим и физическим лицам - клиентам Банка; * Возможность проведения консультаций и разъяснительной работы с сотрудниками по вопросам комплаенса; * Возможность ведения расследований подозрительных, сомнительных операций клиентов филиала и случаев нарушения комплаенс-требований сотрудниками филиала; * Возможность разработки рекомендаций и предложений по устранению и дальнейшему предупреждению выявленных в ходе проверок нарушений и недостатков, осуществление контроля за их исполнением; * Возможность качественного и своевременного составления и предоставления отчетности по проводимым операциям. * Возможность обеспечения надлежащего хранения информации и документации (в том числе конфиденциальной), полученной при проведении проверок деятельности клиентов и сотрудников филиала; * Возможность осуществления текущего контроля над идентификацией клиентов в соответствии с Законодательством РУ и внутренних документов Банка по противодействию легализации (отмыванию) доходов, полученных незаконным путем, и финансированию терроризма в Банке. |
| Контроллер | * Возможность выявления и сбора сведений и информации об операциях клиентов, подлежащим финансовому мониторингу в Банке; * Возможность выявления подозрительных операции клиентов в соответствии с критериями определенными Правилами внутреннего контроля Банка в целях противодействия легализации (отмыванию) доходов, полученных незаконным путем, и финансированию терроризма в Банке; * Возможность осуществления текущего контроля над идентификацией клиентов в соответствии с Законодательством РУ и внутренних документов Банка по противодействию легализации (отмыванию) доходов, полученных незаконным путем, и финансированию терроризма в Банке с формированием отчетов по ним; * Возможность осуществления текущего контроля над идентификацией клиентов в соответствии Законодательства РУ и внутренних документов Банка по противодействию легализации (отмыванию) доходов, полученных незаконным путем, и финансированию терроризма в Банке; * Возможность отправки электронных сообщений в СУГО, получение доп. запросов от СУГО. * Возможность ведения и обновления по требованию Законодательства критериев подозрительных и сомнительных операции, критериев рисков устанавливаемых клиентам, регионов по резолюции ФАТФ (группа разработки финансовых мер по борьбе с отмыванием денег), офшорных зон и зон повышенной террористической активности. * Возможность составления отчетов по сомнительным и подозрительным сообщениям переданными ответственными сотрудниками внутреннего контроля филиалов, отправленные в СУГО. * Возможность ведения расследований подозрительных, сомнительных операций в филиалах и случаев нарушения комплаенс-требований ответственными сотрудниками филиала; * Возможность получения идентификационных данных юридических и физических лиц клиентов Банка, для выявления нарушении требовании Правил, а также с целью получения полной информации о клиентах и их деятельности |
| Администратор | * Возможность административного и системного сопровождения Системы; * Возможность регистрации и деактивации пользователей системы; * Возможность разблокировки и сброс паролей учетных записей пользователей Системы; * Возможность создания групп доступов и выдача прав и ролей пользователям в соответствии с матрицей доступов; * Возможность обеспечения работоспособности Системы и интеграции с другими ИТ-компонентами инфраструктуры и компонентами безопасности Банка |
| Главный контроллер | * Возможность обеспечения своевременности предоставления и полноты сведений по операциям клиентов, подлежащих отправке в СУГО; * Возможность классификации операций клиентов как подозрительные в соответствии с критериями определенными Правилами внутреннего контроля Банка согласно Законодательству РУ; * Возможность приостановления подозрительных операций в случае, если одной стороной (сторонами) является организация или лицо, включенное в Перечень; * Возможность выявления и сбора сведений и информации об операциях клиентов Банка, вызвавших сомнения или подозрения; * Возможность выявления подозрительных операции клиентов в соответствии с критериями определенными Правилами внутреннего контроля Банка в целях противодействия легализации (отмыванию) доходов, полученных незаконным путем, и финансированию терроризма в Банке; * Возможность ведения текущего контроля над идентификацией клиентов в соответствии с Законодательством РУ и внутренних документов Банка по противодействию легализации (отмыванию) доходов, полученных незаконным путем, и финансированию терроризма в Банке и подготовка отчетов по ним; * Возможность осуществления текущего контроля над установлением риска клиентам в соответствии Законодательства РУ и внутренних нормативных документов Банка по противодействию легализации (отмыванию) доходов, полученных незаконным путем, и финансированию терроризма в Банке и подготовки отчетов по ним. |
| Поддержка | * Возможность методологического сопровождения программного обеспечения Системы; * Возможность ведения, обновления Перечня, санкционных и собственных списков Системы, а также справочников НСИ; * Возможность поддержки сценариев Системы по выявлению сомнительных/подозрительных операций в актуальном состоянии; * Возможность регистрации инцидентов на веб-портале Поставщика, связанных с работоспособностью Системы. Участие в разборе и выработке решений по инцидентам; * Возможность тестирования и внедрения доработок по Системе; * Возможность выявления нарушений в работе веб-сервисов Системы; * Возможность анализа журнала обмена информацией с СУГО для устранения ошибок в процессе передачи электронных сообщений. |
| Аудитор | * Возможность просмотра всех данных в разделах меню Системы; * Возможность выгрузки данных из Системы с помощью встроенных отчетов Системы; * Возможность просмотра журнала действий пользователей Системы |
| Сопровождение | * Возможность технической поддержки и функционального сопровождения пользователей Системы; * Возможность диагностики и устранение инцидентов, связанных с использованием Системы; * Возможность выработки решений (или обходного решения) для восстановления и нормализации работоспособности Системы; * Возможность устранения причин сбоя или аномальных поведений Системы; * Устранение ошибок интеграционного взаимодействия; * Возможность взаимодействия с Поставщиком по решению инцидентов и внедрению изменений в Системе |
| Информационная безопасность | * Возможность просмотра журнала действий пользователей (журнал аудита); * Возможность просмотра групп доступов Системы; * Возможность просмотра списка зарегистрированных в Системе пользователей * Возможность просмотра наделенных ролей пользователям |

Архитектура Системы должна иметь возможность обеспечения гибкой настройки прав доступа пользователя к функциям Системы в зависимости от функциональных обязанностей пользователя.

В целях организации контроля и качества обработки данных Система должна иметь возможность ведения двойного контроля в следующих функциях:

- Введение новых клиентов Банка;

- Редактирование информации существующих клиентов Банка;

- Утверждение изменений или отправка на доработку электронных сообщений;

- Создание пользователей, распределение полномочий, редактирование сценариев, настройка параметров отображения пользовательских интерфейсов

- Проверка и подтверждение действий администратора Системы;

- Подтверждение корректности отправки подозрительных операций в архив и исключения из обработки.

### 4.2.7. Показатели назначения

Степень приспособляемости системы к изменению процессов и методов управления:

* Меню программного комплекса должны быть сгруппированы в соответствии с тематикой информации, функциональными задачами и технологией работы с возможностью изменения состава.
* Администратор безопасности должен иметь возможность изменять права доступа пользователей к данным и меню при изменении организационной структуры, технологии работы или других факторов, влияющих на права доступа к информации.
* В целях реализации требований законодательства и нормативных актов в банковской системе должна быть обеспечена возможность изменения состава форматов данных, используемых при работе программного обеспечения. Вновь применяемые форматы данных должны быть описаны и утверждены Заказчиком.
* В случае изменений нормативно-правовой базы банковской системы, влекущих за собой изменения в структуре и составе баз данных, его функциональности, все доработки системы проводятся в рамках его модернизации по отдельным договорам.

Производительность системы:

* Система должна отвечать требованиям масштабируемости, то есть входящее в ее состав аппаратное обеспечение ПО должно обеспечивать одновременную работу необходимого числа пользователей путем наращивания вычислительных ресурсов соответствующих ЦОД.
* Недоступность какого-либо информационного ресурса системы не должна оказывать влияния на производительность системы в целом.
* Время обмена данными между информационными ресурсами центрального и регионального уровней системы определяется техническими возможностями аппаратного обеспечения, на которых размещены ресурсы, и пропускной способностью каналов сети передачи данных между ресурсом и потребителем информации.

Показатели назначения, характеризующие степень соответствия Системы предъявляемым к ней требованиям для организационно-экономических Систем информатизации, в которых управленческое решение и его реализация зависят от человека, трудно формализуются.

Поэтому для Системы степень соответствия назначению будет определяться выполнением требований настоящего технического задания, особенно, в части состава (и содержания) автоматизированных функций и задач, решаемых в подсистемах и отдельных модулях (например, в процентах от запланированных), точности и достоверности исходной и расчетной информации и получаемых решений, возможности их непосредственного использования (таблица 4.2.7).

### Таблица 4.2.7.1. Показатели степени соответствия Системы назначению

|  |  |  |
| --- | --- | --- |
| **№** | **Наименование показателей назначения** | **Пояснение** |
| 1 | Показатели надежности | Характеризуют функциональное соответствие Системы заявленным целям и способность Системы выполнять заданные функции в различных условиях |
| 1.1 | Валидность | Система должна соответствовать заявленным целям и функциональным требованиям технического задания |
| 1.2 | Защищенность | Система должна иметь возможность предотвращать несанкционированный доступ к данным |
| 1.3 | Работоспособность | Система должна функционировать в заданных режимах при отсутствии дестабилизирующих воздействий |
| 1.4 | Согласованность | Система и документация должны иметь однозначные, непротиворечивые описания для одинаковых объектов, функций, терминов, определений и т.д. |
| 1.5 | Устойчивость | Система должна иметь способность, обеспечивающую продолжение работы Системы после возникновения отклонений, вызванных дестабилизирующими воздействиями |
| 2 | Показатели эффективности | Характеризуют степень удовлетворения потребности пользователя в получении информации с учетом экономических, временных и других ресурсов Системы |
| 2.1 | Быстродействие | Система должна быть способной выполнять действия в интервале времени, отвечающем заданным требованиям |
| 2.2 | Экономичность | Система должна иметь возможность работы на минимальных ресурсах Системы |
| 3 | Показатели технологичности | Характеризуют технологические аспекты, обеспечивающие простоту устранения ошибок в Системе |
| 3.1 | Модифицируемость | Система должна иметь возможность, обеспечивающую простоту внесения необходимых изменений и доработок в Систему в процессе эксплуатации |
| 3.2 | Повторяемость | В Системе должно быть использованы типовые проектные решения или компоненты |
| 3.3 | Структурность | Система должна состоять из комплексов, выполняющих взаимосвязанные функции |

### 4.2.8. Требования к надежности

Показатели надежности для системы должны определяться действующими требованиями по надежности автоматизированных информационных систем для органов власти и управления и могут быть уточнены в техническом проекте. Также в техническом проекте должны быть определены методы и средства выполнения работ в случае сбоев системы.

К надежности ***оборудования*** предъявляются следующие требования:

* в качестве аппаратных платформ должны использоваться средства с повышенной надежностью (RISC архитектура, UNIX-подобная ОС);
* применение технических средств, соответствующих классу решаемых задач;
* аппаратно-программный комплекс Системы должен иметь возможность восстановления в случаях сбоев.

К надежности ***электроснабжения*** предъявляются следующие требования:

* система должна быть укомплектована подсистемой оповещения Администраторов о переходе на автономный режим работы;
* система должна быть укомплектована агентами автоматической остановки операционной системы в случае, если перебой электропитания превышает 15 минут;
* должно быть обеспечено бесперебойное питание активного сетевого оборудования.

Надежность ***аппаратных и программных средств*** должна обеспечиваться за счет следующих организационных мероприятий:

* предварительного обучения пользователей и обслуживающего персонала;
* своевременного выполнения процессов администрирования;
* соблюдения правил эксплуатации и технического обслуживания программно-аппаратных средств;
* своевременное выполнение процедур резервного копирования данных.

Надежность программного обеспечения подсистем должна обеспечиваться за счет:

* надежности общесистемного ПО и ПО Разработчика;
* проведением комплекса мероприятий отладки, поиска и исключения ошибок.
* ведением журналов системных сообщений и ошибок по подсистемам для последующего анализа и изменения конфигурации.

Надежность создаваемой системы обеспечивается:

* высокой технологичностью внедряемых программных средств и организационного обеспечения, позволяющего сохранять циркулирующую в системе информацию при сбоях и других ситуациях, нарушающих или разрушающих устойчивость функционирования системы;
* выбором отказоустойчивого оборудования и его структурным резервированием;
* горячим резервированием наиболее важных узлов Системы, к которым относятся серверы базы данных, серверы приложений, компоненты сети хранения данных, оборудование, обеспечивающее связь подсистем, а также связь пользователей каждой подсистемы с серверами БД;
* использованием источников бесперебойного питания;
* выбором топологии телекоммуникационной и локальных вычислительных сетей, обеспечивающих вариантность маршрутизации потоков информации;
* дублированием носителей информации;
* высоким уровнем квалификации и организации работы обслуживающего персонала;
* организацией технического обслуживания, использованием современных методов и средств диагностики;
* использованием только лицензионных программных продуктов;
* отладкой и тестированием модулей всех подсистем;
* наличием исчерпывающих комплектов технической документации, обеспечивающих надежную эксплуатацию всех модулей подсистем;
* работой модулей подсистем, которые не должны вызывать разрушение, искажение и/или утрату сведений, хранящихся в прикладных автоматизированных информационных системах субъектов взаимодействия Системы.

### 4.2.9. Требования к безопасности

Необходимый уровень безопасности должен обеспечиваться Заказчиком путем строгого соблюдения правил эксплуатации и технического обслуживания оборудования, рекомендованных Исполнителями и разработчиками средств информатизации.

Работы по монтажу и наладке системы, а также последующее ее техническое обслуживание не должны быть сопряжены с воздействием на персонал опасных значений электрического тока, электромагнитных полей, акустических шумов, вибраций и т.д., при этом безопасность работы персонала обеспечивается Заказчиком.

Конструкция технических средств должна обеспечивать защиту обслуживающего персонала от поражения электрическим током в соответствии с требованиями ГОСТ 12.2.003 и ГОСТ 12.2.007.0.

Все внешние элементы технических средств Системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь зануление или защитное заземление в соответствии с ГОСТ 12.1.030-81;

Система электропитания должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в целях нагрузки, а также аварийное ручное отключение, и обеспечивается Заказчиком.

Конструкция технических средств должна обеспечивать свободный доступ к отдельным узлам и элементам для их технического обслуживания и ремонта, удобное подключение силовых кабелей.

Безопасность помещений, в которых будут размещаться технические средства Комплекса должна обеспечиваться соответствующей рабочей группой при банке, ответственной как за эксплуатацию системы в целом, так и за реализацию настоящего Технического задания и обеспечивается силами Заказчика.

В Системе должны быть предусмотрены средства защиты информации от несанкционированного доступа неавторизованных пользователей. Cистема 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 Системы.

### 4.2.10. Требования к эргономике и технической эстетике

Обслуживающий персонал системы при работе с системой не должен испытывать неудобств, связанных с неправильной организацией рабочего места или взаимодействия человека с элементами системы.

Смонтированные элементы системы не должны портить внешний вид помещений, где они будут установлены.

Оборудование рабочих мест административного персонала подсистемы должно обеспечивать в штатном режиме непрерывный работы (без необходимости покидания рабочего места для осуществления производственных операций) цикл работы в соответствии с эксплуатационной и технологической документацией.

Эргономические решения должны быть едиными для всех компонентов комплекса.

В системе должны быть предусмотрены необходимые виды интерфейсов для всех категорий административного персонала. Интерфейсы могут реализовываться в виде веб приложений, графических оболочек или командной строки.

Пользовательский интерфейс Системы должен отвечать следующим требованиям:

1. Дизайн экранных форм должен быть стандартным и подвергаться изменению только в случае невозможности решить задачу стандартной формой;
2. Система должна быть удобна и понятна;
3. Эргономические решения должны быть едиными для всех компонентов и модулей Системы;
4. Пользователь должен иметь возможность доступа к контекстно-зависимой справке по стандартному компоненту Системы и руководству пользователя;
5. Интерфейс пользователей должен способствовать уменьшению вероятности совершения случайных ошибочных действий;
6. Интерфейс должен быть оптимизирован для выполнения типовых и часто используемых прикладных операций.

Объем и представление информации, предоставляемые пользователю клиентскими интерфейсами Системы должны соответствовать возможностям человека по восприятию и переработке информации.

При ошибках в действиях пользователя должно выдаваться сообщение, содержащее информацию, достаточную для понимания причин возникновения ошибки.

Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав Системы должно осуществляться посредством визуального графического интерфейса.

Интерфейс Системы не должен быть перегружен графическими элементами. Навигационные элементы должны быть выполнены в удобной для пользователя форме.

Ввод-вывод данных Системы, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление системой должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов.

Клавиатурный режим ввода должен используется главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм.

Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений) должны быть на русском языке.

Система должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях Система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Экранные формы Системы должны проектироваться с учетом требований унификации:

* все экранные формы должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;
* для обозначения сходных операций должны использоваться сходные графические значки, кнопки и другие управляющие (навигационные) элементы. Термины, используемые для обозначения типовых операций, а также последовательности действий пользователя при их выполнении, должны быть унифицированы;
* внешнее поведение сходных элементов интерфейса должны реализовываться одинаково для однотипных элементов.

### 4.2.11. Требования к транспортабельности

Все оборудование в рамках проекта должно быть упаковано. Упаковка должна защищать аппаратуру от повреждений и обеспечивать ее хранение в течение 1 года в складских не отапливаемых помещениях при температуре от -30°С до +70°С, среднемесячном значении относительной влажности 90% при +25°С.

Аппаратура в упакованном виде должна выдерживать транспортирование любым видом транспорта при температуре от -30°С до +70°С и относительной влажности до 90% при+25°С.

### 4.2.12. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов 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.

Должна быть обеспечена возможность функционирования Системы в круглосуточном режиме.

Инсталляционные комплекты Системы должны храниться у администраторов систем в помещениях с ограниченным контролируемым доступом.

Для хранения и восстановления данных в системе должны использоваться средства СУБД или внутренние программные инструменты Системы. Реализация этих требований должна быть обеспечена соответствующими организационными мерами – регламентным обслуживанием системы.

Требования к эксплуатации и регламент обслуживания технических средств (оборудования) системы определяются соответствующими эксплуатационными документами и инструкциями от производителя соответствующего оборудования.

Требования к эксплуатации и регламент обслуживания, необходимого для функционирования Системы, системно-программного обеспечения (операционная система, база данных и т.д.) определяются соответствующими эксплуатационными документами и инструкциями от производителя программного обеспечения.

Требования к допустимым площадям для размещения обслуживающего персонала Системы определяются в соответствии с требованиями норм охраны труда и техники безопасности, установленными в Республике Узбекистан.

Требования к размещению технических средств, параметрам сетей энергоснабжения и условиям эксплуатации разрабатываются на основе соответствующих технических условий, предъявляемых к развертываемым средствам аппаратного обеспечения.

### 4.2.13. Требования к защите информации от несанкционированного доступа

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 Комплекса будут предприняты организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий.

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

* 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 шифрованного канала;
* Обеспечения передачи файлов между узлами участников системы путём создания закрытого файлообмена (Головной банк, областной и районный филиал);
* Возможность обеспечения формирования и передачи сообщении по подозрительным операциям, составленным в форме электронного документа с помощью автоматизированного комплекса программных средств по вводу, обработке и передаче информации с возможностью применения средств криптографической защиты информации согласно Положения «О порядке предоставления информации, связанной с противодействием легализации доходов, полученных от преступной деятельности, и финансированию терроризма» №272 от 12.10.2009 г.
* 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 соответствовать требованиям действующих стандартов и нормативных документов Республики Узбекистан.

Система защиты информации системы в части защиты локальных вычислительных сетей и автоматизированных рабочих мест должна соответствовать требованиям национальных стандартов:

* O'z DSt 2927:2015 «Информационная технология. Информационная безопасность. Термины и определения»;
* O‘z DSt ISO/IEC 27001:2016 Информационные технологии. Методы обеспечения безопасности системы управления информационной безопасностью. Требования;
* O‘z DSt ISO/IEC 27002:2016 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью.

**4.2.14. Требования к разграничению прав доступа**

Система должна отвечать следующим требованиям для управления правами доступа к данным внутри системы:

* Возможность ограничить пользователям системы доступ только к тому уровню информации и данных, который необходим им для выполнения своих рабочих функций, настраиваемым системным администратором;
* Возможность организации доступа к приложению по HTTPS;
* Возможность настраивать внутри системы иерархическую структуру департаментов организации, и добавлять пользователей в различные департаменты, согласно организационной структуре;
* Возможность настраивать внутри системы иерархическую организационную структуру сотрудников, и назначать доступы к данным в зависимости от позиции внутри данной структуры (например, руководитель 1-го уровня имеет доступ к данным своих подчиненных 2-го уровня, менеджеры 2-го уровня имеют доступ к своим подчиненным 3-го уровня). Возможность настраивать глубину доступа внутри иерархии (количество уровней вниз) для руководителей;
* Возможность визуального древовидного отображения настроенной иерархии пользователей и структуры подчиненности в организации;
* Возможность присваивать пользователям определенные роли, и ограничивать доступ к данным в зависимости от роли;
* Возможность настраивать внутри роли права отдельно для каждого объекта/реестра системы, в разрезе следующих привилегий:
* Создание;
* Чтение;
* Изменение;
* Удаление;
* Предоставление индивидуального доступа;
* Связывание других дочерних записей с данной записью, например, иметь возможность управлять правом создания проекта, связанного с чужим клиентом, или можно только к своим;
* Привязка данной дочерней записи к родительской записи.
* Возможность указывать в каждой записи ответственного, и настраивать каждый вид привилегий (создание, чтение, изменение, удаление, предоставление индивидуального доступа, связывание других дочерних записей с данной записью, привязка данной дочерней записи к родительской записи) в разрезе следующих областей действия:
* Только свои;
* Свои записи и записи коллег из своего департамента;
* Свои записи, записи коллег из своего департамента и записи коллег из всех подчиненных (нижестоящих) департаментов;
* Все записи организации независимо от права собственности.
* Возможность настраивать доступ на уровне отдельных полей объекта, в разрезе:
* Полный доступ к полю;
* Просмотр поля без права изменения;
* Поле заблокировано для просмотра и изменения.
* Возможность настраивать команды пользователей внутри системы, и назначать выбранные роли для всей команды, а не только для отдельных пользователей.
* Возможность предоставления индивидуального доступа к записям, так чтобы пользователи без доступа ко всем записям объекта выбранного типа, могли участвовать в совместной работе над отдельными записями, если разрешение на конкретную одну запись им было предоставлено индивидуально.
* Предотвращать доступ пользователей к данным, к которым они не должны иметь доступ согласно назначенной роли или индивидуально назначенному доступу.
* Возможность предоставления доступа к данным аналитики, согласно ролевому уровню пользователя.

### 4.2.15. Требования по сохранности информации при авариях

Сохранность информации Системы обеспечивается Заказчиком и должна обеспечиваться при следующих аварийных ситуациях:

* нарушения электропитания;
* полный или частичный отказ технических средств системы, включая сбои и отказы накопителей на жестких магнитных дисках;
* сбой общего или специального программного обеспечения системы;
* ошибки в работе персонала;
* выход 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 обеспечивается:

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

В случаях отказа технических средств из-за потери электропитания в целях сохранности информации и обеспечения бесперебойного функционирования системы должны быть предусмотрены:

* кратковременная (до 20-30 минут) поддержка электроснабжения путем автоматического включения устройств бесперебойного питания;
* обеспечение постоянного электроснабжения путем включения дизель-генераторных систем.

### 4.2.16. Требования защите от влияния внешнего воздействия

Все аппаратные компоненты Системы должны быть размещены в специальных помещениях, оборудованных и защищенных в соответствии с требованиями стандарта Республики Узбекистан O‘z DSt 2875:2014 «Информационная технология. Требования к дата центрам. Инфраструктура и обеспечение информационной безопасности», нормативно-технической документации (Руководящий документ RH 45-201:2011 Технические требования к зданиям и сооружениям для установки средств вычислительной техники») и документации производителей оборудования.

Непроизводственный характер аппаратных компонентов Системы определяет ограниченность возможных внешних воздействий – агрессивные газы и пары, запыленность, радиационное излучение, мощные электромагнитные, электрические и тепловые поля, вибрация и прочее.

Защита аппаратных компонентов Системы от воздействий внешних электрических и магнитных полей, а также помех по цепям питания должна быть достаточной для эффективного выполнения техническими средствами своего назначения при функционировании аппаратных компонентов и обеспечивается Банком.

Средства защиты информации Системы от внешних воздействий должны обеспечивать:

* стабильность электропитания технических средств в соответствии с требованиями, определяемыми техническими условиями эксплуатации;
* исключение влияния сильных электрических и магнитных полей;
* уровень вибрации в пределах установленных норм;
* пожарную безопасность;
* требуемые микроклиматические условия в помещениях.

### 4.2.17. Требования к патентной и лицензионной чистоте

Реализация Системы должна отвечать требованиям патентной частоты согласно действующему законодательству и регламентирующих распорядительных документов.

### 4.2.18. Требования по стандартизации и унификации

При внедрении Системы необходимо соблюдать принцип унификации используемых средств.

Данные, загружаемые, вводимые и обрабатываемые в Систему, должны отвечать основным принципам единообразия, непротиворечивости, однократности ввода, полноты и достоверности информации.

Все службы должны работать в Инфраструктуре TCP/IP;

Взаимодействие клиентских устройств с серверной частью системы должно осуществляться по стандартным протоколам обмена, определенных документами RFC в среде TCP/IP.

Система должна соответствовать следующим показателям, устанавливающим требуемую степень использования стандартных, унифицированных методов реализации функций (задач), поставляемых программных средств:

* Поддержка форматов электронных документов для распространения данных, CSV, DOC, EXL, PDF;
* Поддержка автоматического преобразования форматов данных в формат HTML, для обеспечения просмотра информации без установки специальных программных средств;
* Возможность функционирования на различных аппаратных платформах.

## 4.3. Требования к функциям (задачам), выполняемым системой

**4.3.1. Общие требования к функционалу Системы**

Система должна иметь возможность выполнения следующих функций:

- Возможность получения необходимого набора данных, необходимых для управления процессами ПОД/ФТ в Банке из ИАБС, а также хранение всех полученных данных в системе;

- Возможность аавтоматического выявления операций, в отношении которых есть подозрения, что они связаны с легализацией доходов, полученных незаконным путем и финансированием терроризма, а также операций, подлежащих финансовому мониторингу, на основе разработанных сценариев. Каждая операция должна проверяться по всем существующим сценариям. Каждый сработавший сценарий должен добавлять расшифровку в поле комментария. Одна операция может быть определена как сомнительная и так подозрительная одновременно;

- Возможность сохранения информации по сомнительным/подозрительным операциям в течение срока, требуемого Законодательством РУ (не менее пяти лет после осуществления таких операций или прекращения деловых отношений с клиентами);

- Возможность формирования и получения сообщений в формате обмена с информационной системой СУГО, связанное с предоставлением данных о сомнительных/подозрительных операциях и получением санкций на выполнение отдельных категорий операций в соответствии с требованиями Законодательства РУ;

- Возможность предоставления пользовательского веб-интерфейса для запуска и расчета отчетов, создания новых и изменения существующих на основе данных, содержащихся в хранилище системы;

- Возможность предоставления пользовательского веб-интерфейса для обеспечения возможности корректировки сценариев, логики их работы и установочных параметров (КНП, суммы, категории операций и т.д.) по выявлению сомнительных/подозрительных операций;

- Возможность генерации отчетности о пользователях, их ролях и истории действий в Системе.

Система должна иметь возможность автоматически блокировать учетные записи пользователей, которые не использовались на протяжении длительного времени - более 180 дней. Условие не распространяется на учетные записи администраторов системы;

Система не должна иметь возможность незадекларированных функций, позволяющих обойти механизмы контроля;

Для минимизации пользовательских ошибок ввода данных в Систему, Система должна иметь возможность автоматического контроля ввода на уровне интерфейсных форм, а именно обязательность заполнения реквизитов, а также форматный контроль.

Система должна включать основные понятия по процедурам «Знай своего клиента»

Процедуры включают в себя следующие:

* надлежащая проверка клиента – возможность проверки личности и полномочий клиента и лиц, от имени которых он действует, идентификация бенефициарного собственника клиента, а также проведение на постоянной основе изучения деловых отношений и операций, осуществляемых клиентом, в целях проверки их соответствия сведениям о таком клиенте и его деятельности;
* идентификация клиента - возможность определения коммерческим банком данных о клиентах на основе предоставленных ими документов, дополнительно подтвержденных сведений, доступных в открытых источниках и базах данных в целях осуществления надлежащей проверки клиента;
* идентификация бенефициарного собственника клиента - возможность определения коммерческим банком юридического лица собственника, в том числе лица контролирующего клиента путем изучения структуры собственности и управления на основании учредительных документов, определенных законодательством (устава и (или) учредительного договора, положения).

Процедуры по НПК (надлежащая проверка клиента):

* возможность осуществления процедур идентификации и мер по надлежащей проверке клиентов, в том числе верификации и регулярного обновления данных о клиенте и их бенефициарных собственниках;
* возможность обеспечения хранения информации об операциях, а также идентификационных данных и материалов по надлежащей проверке клиентов в течение сроков, установленных законодательством;
* процедуры обмена данными, необходимыми для управления рисками, связанными с легализацией доходов, полученных от преступной деятельности, финансированием терроризма и (или) финансированием распространения оружия массового уничтожения, и надлежащей проверки клиентов.

Система должна включать основные понятия по процедурам углубленного мониторинга «Публичных должностных лиц»:

* публичные должностные лица - лица, назначаемые или избираемые постоянно, временно или по специальному полномочию, выполняющие организационно-распорядительные функции и уполномоченные на совершение юридически значимых действий в законодательном, исполнительном, административном или судебном органе иностранного государства либо в международной организации, а также высокопоставленные руководители предприятий иностранных государств, известные политики и известные члены политических партий иностранных государств.

Процедуры по ПДЛ (публичные должностные лица)

* возможность осуществления углубленного мониторинга операций, проводимых публичными должностными лицами, членами их семей и лицами, близкими к публичным должностным лицам;
* порядок установления деловых отношений с публичными должностными лицами, членами их семей и лицами, близкими к публичным должностным лицам и осуществления углубленного мониторинга ими проводимых операций;
* возможность применять разумные меры для проверки сведений о статусе публичного должностного лица и определения источника денежных средств или иного имущества по операции;
* возможность устанавливать (или продолжать для существующих клиентов) деловые отношения с публичным должностным лицом только с разрешения председателя правления банка или его уполномоченного заместителя;
* возможность осуществлять постоянный углубленный мониторинг деловых отношений.

В целях организации контроля и качества обработки данных Система должна иметь возможность ведения двойного контроля в следующих функциях:

* + - * + возможность просмотра, корректировки реквизитов электронных сообщений о сомнительных и/или подозрительных операциях, подлежащих отправке в СУГО и сформированных в автоматическом режиме, а также создание в ручном режиме электронных сообщений, подлежащих отправке в СУГО. Указание клиентов - участников операции (выбор из списка доступных) с последующей отправкой на утверждение или исключение из обработки (архив).
        + возможность проверки и отправки электронных сообщений о сомнительных и/или подозрительных операций, подлежащих отправке в СУГО, на доработку предыдущему исполнителю, а также в архив с целью исключения из обработки. Контроль обмена информационными сообщениями с СУГО.
        + возможность введения новых клиентов Банка;
        + возможность редактирования информации существующих клиентов Банка;
        + возможность утверждения изменений или отправка на доработку электронных сообщений;
        + возможность актуализации списков и справочников в Системе;
        + возможность создания пользователей, распределение полномочий, редактирование сценариев, настройка параметров отображения пользовательских интерфейсов;
        + возможность проверки и подтверждения действий администратора Системы;
        + возможность подтверждения корректности отправки подозрительных операций в архив и исключения из обработки.

Система должна иметь возможность выполнения следующих функций:

* Вход в систему разрешен только авторизованным пользователям с обязательным вводом логина и пароля доменной учетной записи Active Directory;
* Длина пароля должна быть не менее 8 символов и обязательно содержать специальные символы или числа;
* Система должна требовать смены пароля пользователя каждые 45 дней, и новый пароль не должен совпадать с одним из 12 предыдущих паролей;
* Пароль пользователя может быть изменен только 1 раз в течение суток;
* Шифрование пароля пользователя должно быть обеспечено алгоритмом AES-256;
* В случае неверного ввода пароля 3 раза подряд должна быть выполнена блокировка пользователя;
* Необходимо предусмотреть проставление статуса «Системный пользователь», на которого блокировка и требования к смене пароля не распространяются;
* Создание пользователей и распределение полномочий должно осуществляться через пользовательский веб-интерфейс.

**4.3.2. Требования к подсистеме противодействия отмыванию денежных средств (AML)**

Система должна иметь возможность предоставить диаграмму / анализ отношений с клиентами, включая скрытые отношения (например, связь одного и того же работодателя, адрес, мобильный телефон и т. д.), социальные сети (Facebook, LinkedIn) и т. д.;

Система должна иметь возможность предоставить пользовательский интерфейс для настройки и обслуживания правил обнаружения;

Система должна иметь возможность выполнять конвертацию валюты из иностранной валюты в национальную валюту и генерировать оповещения, когда превышается пороговое значение, установленное в национальной валюте;

Система должна иметь возможность определения правил обнаружения, специально предназначенных для профиля клиента (например, род занятий и / или юрисдикции) и схемы транзакций (например, быстрое перемещение средств);

Система должна иметь возможность предоставить специальное правило обнаружения для мониторинга списка клиентов высокого риска;

Система должна иметь возможность обнаруживать сомнительную транзакцию на основе порога / параметра, определенного сегментацией.

Система должна иметь возможность получать все данные СВИФТ операций, сравнивая данные отправителей и получателей (контрагентов) с Санкционными списками FATF (Группа по разработке финансовых мер борьбы с отмыванием денег) и с оффшорными зонами;

Система должна иметь возможность обнаруживать отклонения в поведении транзакции на основе профиля клиента, сравнивая его с группой сверстников и оповещая / внося оценку в профиль риска клиента;

Система должна иметь возможность обнаруживать изменение поведения транзакции клиента и оповещать / вносить оценку в профиль риска клиента;

Система должна иметь возможность включать и выключать правила обнаружения только для конкретного объекта / страны;

Система должна иметь возможность предоставить диаграмму / анализ сетевой ссылки для соответствующего предупреждения / транзакции и клиента;

Система должна иметь возможность внесения в белый список клиента / аккаунта с датой истечения срока действия (с напоминанием до и после истечения срока действия) и применима только к определенным правилам обнаружения;

Система должна иметь возможность автоматического скрининга белого списка в базе данных полного списка наблюдения и внутреннего списка и автоматического обновления, если не обнаружено изменений в профиле клиента и поведении транзакции;

Система должна иметь возможность настройки порогов для нескольких стран с использованием внутренней валюты для одного и того же правила обнаружения;

Система должна иметь возможность просмотра «периодичности» с типами транзакций «международные платежи», «положительное сальдо кредита», «отток кредитной линии» и сопоставление соответствующих платежных отношений (например, «1-я сторона», «третья сторона») и оповещение при обнаружении подозрительной транзакции;

Система должна иметь возможность настройки, чтобы избежать повторения оповещения для одного и того же профиля клиента, который попал туда из того же правила обнаружения;

Система должна иметь возможность обнаруживать и предупреждать данные о неполноте, которые требуются правилами обнаружения, чтобы избежать создания ложного положительного предупреждения из-за неполных данных;

Система должна иметь возможность предложить оптимизированный порог и сегментацию для оптимизации правила обнаружения и, таким образом, генерировать более истинное положительное предупреждение;

Система должна иметь возможность указать высокую вероятность / частоту для предупреждений о подозрительных транзакциях на основе закрытия истории предупреждений;

Система должна иметь возможность прогнозировать тренд транзакции клиента и сигнализировать о возможной подозрительной транзакции;

Система должна иметь возможность включения результатов машинного обучения / оптимизации в мониторинг транзакций и профилирование рисков клиентов;

Система должна иметь возможность выполнять массовое закрытие оповещения для определенных случаев;

Система должна иметь возможность вывода внешних отчетных файлов для электронной подачи в регулирующие органы;

Система должна иметь возможность автоматического сопоставления профиля клиента на основе конфигурации и выбора подозрительных транзакций для отчетов о подозрительных транзакциях;

Система должна иметь возможность настроить несколько форматов отчетов о подозрительных транзакциях для представления регулирующим органам;

Система должна иметь возможность настроить отчет о подозрительных транзакциях;

Система должна иметь возможность подготовки отчетов о идентифицированных клиентах (юридических лиц, ИП и физических лиц).

Система должна иметь возможность подготовки отчетов об установленных рисках клиентов (юридических лиц, ИП и физических лиц).

Система должна иметь возможность подготовки в нескольких форматах отчетов по странам и регионам, с зонами Повышенной Террористическим активности, Офшорами и странами не участвующим в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма.

**4.3.3. Требования к подсистеме консолидации процесса расследования подозрительной деятельности на единой платформе на уровне Банка (ECM)**

Система должна иметь возможность обеспечить функциональность обеспечения качества (quality assurance QA) (чтобы снова открыть кейс, редактировать комментарии / открыть кейс даже после закрытия кейса) и выполнить выборку для рассмотрения кейса;

Система должна иметь возможность эскалации и переназначения кейса автоматически, если кейс / предупреждение не было получено / обновлено по истечении срока;

Система должна иметь возможность импортировать случаи из различных источников данных и метки для клиента / учетной записи;

Система должна иметь возможность настроить поля, необходимые для другого типа кейса;

Система должна иметь возможность предоставить пользовательский интерфейс для управления и мониторинга при назначении события:

- Уметь назначать события

- Отслеживание даты наступления сроков рассмотрения

- Контролировать ежедневную производительность аналитика / сотрудника

- Возможность экспортировать список событий в файл MS Excel.

Система должна иметь возможность предоставить инструмент для совместной работы;

Система должна иметь возможность загрузить поясняющий документ в событие;

Система должна иметь возможность отправки напоминания через систему и по электронной почте автоматически, чтобы запросить ответ на основе установленного срока;

Система должна иметь возможность импорта и экспорта для массового закрытия событий с комментариями и аудиторским следом и возможность указать при этом тип закрытия события;

Система должна иметь возможность назначать и корректировать приоритет оповещения на основе старения события и других факторов;

Система должна иметь возможность выполнять поиск документа, загруженного в систему.

**4.3.4. Требования к подсистеме детального исследования клиентов Банка (KYC)**

**4.3.4.1. Требования к подсистеме в целом**

Система должна иметь возможность предоставить пользовательский интерфейс для поддержки полей профиля клиента для дополнительной информации без настройки;

Система должна иметь возможность реализации подхода, основанного на оценке риска (risk based approach RBA), на основе профиля клиента, основанного на нескольких факторах риска. Например, род деятельности, характер бизнеса, юрисдикция, отсутствие сообщений о подозрительных операциях, поведение при совершении сделки, продукт и т.д.;

Система должна иметь возможность пометить утвержденную отправку расширенной проверки клиента (EDD) автоматически и вручную с зарегистрированным клиентом и предупредить клиента с высоким риском без одобрения расширенной проверки клиента (EDD);

Система должна иметь возможность загрузки информации о клиенте, включая вспомогательный документ;

Система должна иметь возможность создать корректировочную запись для изменения оценки риска клиента;

Система должна иметь возможность выполнения скрининга и профилирования рисков для конечного бенефициара (UBO);

Система должна иметь возможность отслеживания контрольного журнала для предыдущего профилирования рисков клиентов;

Система должна иметь возможность работы в качестве отдельного модуля, который позволяет бизнес-подразделению представлять EDD на утверждение перед тем, как подключить клиента, и помечать EDD, утвержденный данными клиента, как только клиент вошел в систему;

Система должна иметь возможность автоматически создавать новую запись EDD после процесса скрининга / оценки риска для профиля клиента с высоким уровнем риска;

Система должна иметь возможность проверки данных клиента из встроенного хранилища данных (EDW);

Система должна иметь возможность предоставить инструмент моделирования тестирования на основе исторических данных результата изменения оценки риска / внедрения нового фактора для оценки риска;

Система должна иметь возможность идентифицировать изменения профиля клиента и выполнить восстановление всякий раз, когда это необходимо;

Система должна иметь возможность настройки периода проверки и события / уведомления до и после даты наступления срока проверки на основе уровня риска и т. д.

Система должна иметь возможность вручную вызвать необходимость проверки на одного или нескольких клиентов с контролем прав доступа пользователей;

Система должна иметь возможность классифицировать тип генерируемых специальных предупреждений (ODD). Например, изменения данных поведения, периодический обзор и т. д.;

Система должна иметь возможность изменения всех клиентов при изменении оценки рисков (в режиме реального времени) и оповещение о новых клиентах с высоким риском;

Система должна иметь возможность настроить контрольный список проверки специальных событий;

Система должна иметь возможность интеграции с внешними источниками данных.

**4.3.4.2. Подсистема «Клиенты»**

Подсистема должна иметь возможность формирования и редактирования данных в карточках клиентов, находящихся в Системе.

Подсистема «Клиенты» должна иметь возможность обеспечивать выполнение следующих функций:

- возможность редактирования данных в карточках клиентов, полученных из ИАБС, а также создание новых;

- при обновлении данных в карточке клиентов в ИАБС Система должна иметь возможность обновления информации в Системе с учетом следующего условия: если из ИАБС получено нулевое значение поля, то информация в Системе в данном поле сохраняется.

- при обновлении данных Система должна иметь возможность опционального использования двойного контроля при изменении данных в карточках клиентов через пользовательский веб-интерфейс.

**4.3.4.3. Подсистема «Онлайн»**

Подсистема должна иметь возможность проверки в режиме реального времени определенного набора данных при заведении карточки клиента в ИАБС, в том числе при изменении данных в карточке клиента по клиентам, бенефициарным собственникам, учредителям (акционерам) клиентов и руководителям; а также при проведении операций в ИАБС - проверки данных по клиентам, бенефициарным собственникам, операциям и участникам операций, передаваемого из ИАБС посредством использования веб-сервисов, по заданным условиям проверки. Кроме того, при выявлении совпадений клиентов и/или бенефициарных собственников клиентов по спискам в режиме онлайн существует возможность автоматической приостановки операций открытия счета (-ов) таких клиентов и бенефициарных собственников клиентов.

Подсистема должна иметь возможность выполнения следующих функций:

- просмотр операций, совершаемых клиентами, совпавшими со списками (Перечнем, санкционные списки и собственные списки) Системы;

- проверка клиентской базы на совпадения со списками Системы.

- анализ поступивших результатов совпадения и принятие решения по достижению предельных пороговых значений параметров по каждому из участников;

- формирование сообщения в ИАБС с решением о разрешении или запрете проведения операции.

- ручное редактирование списков Системы;

- двойной контроль изменений данных в списках Системы.

- уведомление пользователей Системы о совпадении со списками Системы.

Система должна иметь возможность обеспечения работы с функциями подсистемы через пользовательский веб-интерфейс.

**4.3.4.4. Подсистема «Управление рисками»**

Подсистема должна иметь возможность обеспечения исполнения требований «Правил внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения в коммерческих банках» в части оценки клиентов и их операций степени подверженности рискам ОД/ФТ путем выполнения следующих процедур:

- возможность отметки основных объектов Системы признаком «уровень риска»: клиент, операция.

- возможность разработки модели автоматического расчета уровня риска для основных объектов Системы на основании экспертных заключений и результатов статистического анализа. При анализе также должна учитывается статистика отправляемых электронных сообщений в СУГО по каждому клиенту.

- возможность гибкой настройки уровней риска основных объектов системы, используя пользовательский веб- интерфейс.

- возможность присвоения уровня риска клиенту в режиме онлайн при заведении карточки клиента в ИАБС. Система также предоставляет возможность принятия решения по клиенту комплаенс-сотруднику внутреннего контроля через веб-интерфейс;

- возможность ведения настроечных таблиц, с помощью которых настраивается расчет по оценочным показателям;

- возможность расчета рисков необходимо производить по шкале, например по 2-х уровневой шкале: 1-низкий; 2-высокий риск.

Подсистема должна иметь возможность изучения, анализа, выявления, оценки, мониторинга, управления, документирования и снижения уровня риска согласно Правилам №2886.

Согласно Правилам №2886 к категории высокого уровня риска относятся клиенты, отвечающих изначально следующим критериям, в отношении которых должны проявлять повышенное внимание:

1) лица, включенные в Перечень либо находящиеся в собственности или под контролем лица, включенного в Перечень, либо прямо или косвенно являющиеся собственником или контролирующие организацию, включенную в Перечень;

2) лица, постоянно проживающие, находящиеся или зарегистрированные в государстве, не участвующем в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма

3) представительства иностранных компаний и нерезиденты — физические лица Республики Узбекистан;

4) лица, постоянно проживающие, находящиеся или зарегистрированные в оффшорной зоне;

5) резиденты и нерезиденты, имеющие счета в оффшорных зонах; 45

6) организации и индивидуальные предприниматели, фактическое местонахождение которых не соответствует сведениям, указанным в учредительных или регистрационных документах;

7) организации и индивидуальные предприниматели, период деятельности которых не превышает одного квартала финансового года;

8) организации, бенефициарным собственником которых являются «лица включенные в Перечень либо находящиеся в собственности или под контролем лица, включенного в Перечень, либо прямо или косвенно являющиеся собственником или контролирующие организацию, включенную в Перечень» и «Лица, постоянно проживающие, находящиеся или зарегистрированные в государстве, не участвующем в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма»;

9) клиенты, осуществляющие подозрительные или сомнительные операции на систематической основе (например, в течение 3 месяцев подряд);

10) клиенты, использующие программные комплексы, исключающие возможность осуществления надлежащей проверки клиента;

11) публичные должностные лица, члены их семей и лица, близкие к публичным должностным лицам;

12) Иные лица, определяемые внутренними правилами (с возможностью указания причины):

- операции с драгоценными металлами, драгоценными камнями, а также ювелирными изделиями, содержащими драгоценные металлы и драгоценные камни, за исключением таких операций, проводимых самими коммерческими банками;

- операции, связанные с переводами денежных средств, в которых сведения об отправителе (фамилия, имя, отчество физических лиц, полное наименование юридических лиц, местонахождение (почтовый адрес) и номер счета отправителя) представлены не в полном объеме;

13) Прочие (с возможностью указания причины) например:

Операции, участниками которых являются лица, указанные в подпунктах

«1 Лица, включенные в Перечень либо находящиеся в собственности или под контролем лица, включенного в Перечень, либо прямо или косвенно являющиеся собственником или контролирующие организацию, включенную в Перечень»;,

«2 Лица, постоянно проживающие, находящиеся или зарегистрированные в государстве, не участвующем в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма»

«8 Организации, бенефициарным собственником которых является «лицо включенные в Перечень либо находящиеся в собственности или под контролем лица, включенного в Перечень, либо прямо или косвенно являющиеся собственником или контролирующие организацию, включенную в Перечень» и «Лица, постоянно проживающие, находящиеся или зарегистрированные в государстве, не участвующем в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма»;

«11 Публичные должностные лица, члены их семей и лица, близкие к публичным должностным лицам;

- операции, осуществляемые через счета, открытые в оффшорных зонах;

- иные операции, определяемые внутренними правилами.

Подсистема должна иметь возможность выполнения следующих функций:

- возможность формирования отчетов, для контроля и управления рисками ОД/ФТ;

- возможность выполнения функционала по пересчету значений риска, обеспечивающий возможность как автоматического расчета по заданному расписанию, так и проведения ручного пересчета уровня рисков как по каждому клиенту отдельно, так и по всем карточкам клиента;

- возможность ведения журнала изменений уровней риска, для учета исторических данных по расчету/пересчету уровней риска;

Система должна иметь возможность обеспечения работы с функциями подсистемы через пользовательский веб-интерфейс.

**4.3.5. Требования к подсистеме идентификации клиентов, упомянутых в списках особого внимания (CS)**

Система должна иметь возможность выполнять пакетный скрининг по базе данных наблюдения и по внутреннему списку клиентов;

Система должна иметь возможность выполнять скрининг в режиме реального времени и профилирование рисков по базе данных наблюдения и внутреннему списку при подключении клиента через EAI;

Система должна иметь возможность повторного скрининга всех профилей клиентов или определенного списка клиентов из базы данных контрольных списков, а также внутреннего списка;

Система должна иметь возможность указать новое совпадение при повторном просмотре клиента с последними списками наблюдения;

Система должна иметь возможность предоставить инструмент моделирования для тестирования на основе исторических данных новых правил проверки / пересмотра правил проверки;

Система должна иметь возможность интеграции со сторонними списками наблюдения, такими как WorldCheck, Factiva, World Compliance и т.д.;

Система должна иметь возможность интеграции со списками, получаемыми от Регулятора (Перечень международный и национальный, список лиц Антитеррористического центра);

Система должна иметь возможность классифицировать тип совпадения;

Система должна иметь возможность изменения / добавления дополнительных источников баз данных наблюдения, таких как worldcheck, Factiva и т. д., а также внутреннего списка;

Система должна иметь возможность скрининга определенных полей для оплаты (адрес / имя / банк и т.д.);

Система должна иметь возможность импортировать несколько внутренних списков;

Система должна иметь возможность импортировать и экспортировать список исключений / белый список и применять список исключений;

Система должна иметь возможность включать и выключать правила проверки, а также список исключений;

Система должна иметь возможность определения алгоритма сопоставления по полям для проверки платежей;

Система должна иметь возможность предоставить пользовательский интерфейс для произвольного скрининга, который пользователь может выполнять на основе списка наблюдения и внутреннего списка;

Система должна иметь возможность обеспечить печатный и экспортируемый формат отчета;

Система должна иметь возможность автоматического переэкранирования в белом списке с полной базой данных и внутренним списком;

Система должна иметь возможность настройки нескольких алгоритмов сопоставления с несколькими идентификаторами, включая Юникод и родные языки для проверки имени, даты рождения и т. д.

Система должна иметь возможность обеспечения периодического обновления на ежедневной основе.

В Таблице 4.3.5.1 приведены списки и способы их загрузки в Систему.

Таблица 4.3.5.1. Списки Системы

|  |  |
| --- | --- |
| **Наименование списка** | **Ссылка на обновление** |
| Список ООН | <http://www.un.org/> sc/committees/1267/AQLi st.xml |
| <http://www.un.org/> sc/committees/ 1988/1988Li st.xml |
| Список ОФАК | <http://www.treasury.gov/ofac/downloads/sdn.xml>  <http://www.treasury.gov/ofac/downloads/fse/fse.xml> |
| Списки ИПДЛ | Будет предоставлено Заказчиком при согласовании ТЗ |
| Перечень | Будет предоставлено Заказчиком при согласовании ТЗ |
| Список АТЦ и наёмников | Будет предоставлено Заказчиком при согласовании ТЗ |
| Собственный список Банка | Будет предоставлено Заказчиком при согласовании ТЗ |

***\*)*** *Окончательный перечень списков будет определен на этапе разработки проектной документации.*

Система должна иметь возможность фиксации в журнале аудита действий пользователей Системы и обеспечивать выполнение следующих функций:

- возможность ведения аудита изменений данных по сомнительным и/или подозрительным клиентам;

- возможность ведения аудита изменений данных клиентов и их учредителей;

- возможность логирования входа пользователей через веб-интерфейс в журнал логов Системы;

- возможность просмотра и фильтрации записей в журнале аудита.

**4.3.6. Требования к подсистеме фильтрации транзакций (TF)**

**4.3.6.1. Подсистема «Проведенные операции»**

Подсистема должна иметь возможность просмотра и отображения всех операций, полученных из ИАБС с возможностью фильтрации и последующей отправкой в сомнительные или подозрительные операции.

Подсистема должна иметь возможность выполнения следующих функций:

- возможность получения, накопления в едином хранилище Системы данных о проведенных операциях из ИАБС;

- возможность поиска и просмотра операций в базе данных Системы через визуальный веб-интерфейс;

- возможность фильтрации всех операций по диапазону дат по реквизиту «Дата время совершения операции»;

- возможность ручного переноса пользователем операций в категории сомнительные и/или подозрительные с указанием кода типа подозрения;

- возможность просмотра операций в виде списка, а также детального просмотра всей полученной информации в расширенном виде;

- возможность выполнения проверки и выявления сомнительных и/или подозрительных операций, на основе сценариев в автоматическом режиме без участия пользователя.

- в случае выявления факта срабатывания сценария по операции, подсистема должна иметь возможность формирования и заполнения имеющимися реквизитами электронное сообщение в СУГО;

- возможность передачи в СУГО электронных сообщений о подозрительных операциях или факты совпадений с Перечнем должна осуществляться с учетом контроля процесса отправки и ограничения доступа к информации;

Система должна иметь возможность обеспечения работы с функциями подсистемы через пользовательский веб-интерфейс.

Алгоритмы работы сценариев должны быть построены на основе критериев и признаков по выявлению сомнительных и подозрительных операций, в соответствии с «Правилами внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения в коммерческих банках».

Для управления работой сценариев Система должна иметь возможность выполнения следующего функционала:

- Указание порядка выполнения сценария;

- Активация и деактивация сценария;

- Удаление сценария.

Перечень и описание критериев и признаков для выявления сомнительных и подозрительных операций, определенных в Правилах внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения в коммерческих банках (Утверждены Постановлением от 17.04.2017 г. Правления ЦБ N 343-В, Департамента по борьбе с НВП и ЛПД N 14, зарегистрированным МЮ 23.05.2017 г. N 2886).

**4.3.6.2. Подсистемы «Сомнительные операции» и «Подозрительные операции»**

Подсистема должна иметь возможность просмотра, редактирования данных о сомнительных и/или подозрительных операциях, с последующей передачей для отправки в СУГО.

**Система должна иметь возможность признания операции сомнительной при наличии одного из нижеследующих критериев и признаков:**

* операции или клиенту, ее осуществляющему, коммерческим банком присвоен высокий уровень риска;
* систематически осуществляемый возврат клиентом-резидентом ранее полученной суммы в пользу нерезидента по договору поставки товаров (выполнения работ, оказания услуг);
* предоставленные документы на проведение операции вызывают сомнение в их подлинности (достоверности), и (или) сведения об операции, в том числе о какой-либо из ее сторон, не соответствуют имеющейся у коммерческого банка информации;
* необычность в поведении клиента при обращении с заявлением (поручением, ходатайством) о совершении операции, например: нервозность, неуверенность, агрессия с одновременным присутствием лиц, руководящих действиями клиента, либо его обращением по телефону к другим лицам за советом по незначительному поводу;
* необычная озабоченность клиента вопросами конфиденциальности или необоснованный отказ либо неоправданные задержки в представлении клиентом информации об операции, запрашиваемой коммерческим банком;
* невозможность установления партнеров клиента по проводимой операции;
* операция не имеет явного экономического смысла и не соответствует характеру и виду деятельности клиента;
* необоснованное увеличение оборота денежных средств по счету клиента, не связанное с характером его деятельности и (или) произошедшее после более, чем трехмесячного периода низкой активности либо отсутствия признаков активности на счетах данного клиента;
* необоснованное и (или) досрочное прекращение деловых отношений по инициативе клиента, сопровождаемое снятием или переводом всех средств в другие коммерческие банки;
* немедленное прекращение деловых отношений по инициативе клиента после обоснованного применения коммерческим банком мер, предусмотренных настоящими Правилами;
* явное несоответствие операций, проводимых клиентом с участием коммерческого банка, общепринятой практике совершения операций;
* необоснованное дробление сумм аналогичных операций, совершаемых клиентом на общую сумму, равную или превышающую 500-кратный размер базовой расчетной величины на день осуществления операции;
* порядок проведения расчетов содержит нестандартные или необычно сложные схемы, отличающиеся от обычной деятельности клиента;
* обмен банкнот одного достоинства на банкноты другого достоинства физическим лицом на сумму, равную или превышающую 500-кратный размер базовой расчетной величины, установленный на день обмена;
* внесение физическим лицом в наличной форме денежных средств на сумму, равную или превышающую 500-кратный размер базовой расчетной величины на день осуществления операции, на банковский счет юридического лица или индивидуального предпринимателя в качестве займов, финансовой помощи, вклада в уставный фонд (капитал) либо оборотных средств в целях пополнения;
* перечисление со счетов юридических лиц или индивидуальных предпринимателей денежных средств на сумму, равную или превышающую 1000-кратный размер базовой расчетной величины на день осуществления операции, в качестве финансовой помощи или займа;
* перечисление со счетов юридических лиц и/или индивидуальных предпринимателей в пользу физических лиц денежных средств на сумму, равную или превышающую 1000- кратный размер базовой расчетной величины на день осуществления операции, в качестве дивидендов или прибыли;
* снятие со счета физического лица денежных средств в наличной форме на сумму, равную или превышающую 500-кратный размер базовой расчетной величины на день осуществления операции;
* осуществление операций (оплата или снятие наличности) с пяти и более международных платежных карт в течение одного дня по терминалу одного контрагента, когда сумма операций с каждой картой равна или превышает 25-кратный размер базовой расчетной величины;
* перечисление денежных средств, сумма которых равна или превышает 500-кратный размер базовой расчетной величины, за пределы Республики Узбекистан на счет получателя, открытый в банке, местонахождение которого отличается от места регистрации получателя.

**Система должна иметь возможность признания операции подозрительной при наличии одного из нижеследующих критериев и признаков:**

* одной из сторон операции является лицо, постоянно проживающее, находящееся или зарегистрированное в государстве, не участвующем в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма;
* получение отправленных из-за рубежа или отправление за рубеж физическими лицами (в том числе несколькими физическими лицами на имя одного контрагента) денежных средств в иностранной валюте, в том числе через системы денежных переводов, на общую сумму, равную или превышающую 500-кратный размер базовой расчетной величины, единовременно или многократно в течение срока, не превышающего 1 месяца;
* продажа или покупка, а также снятие с международных платежных карт физическими лицами и/или индивидуальными предпринимателями денежных средств в иностранной валюте на сумму, равную или превышающую 500-кратный размер базовой расчетной величины, единовременно или многократно в течение срока, не превышающего 1 месяца;
* перечисление денежных средств за пределы Республики Узбекистан на счет, открытый на анонимного владельца, и поступление денежных средств в Республику Узбекистан со счета, открытого на анонимного владельца или при отсутствии сведений об отправителе;
* перечисление денежных средств за пределы Республики Узбекистан на счет получателя, открытого в банке, зарегистрированном в оффшорной зоне, отличающейся от места регистрации получателя;
* денежные средства переводятся за пределы Республики Узбекистан на счета или в пользу лиц, постоянно проживающих или зарегистрированных в оффшорных зонах, либо поступают в Республику Узбекистан со счетов таких лиц единовременно или многократно в течение 30 дней, на общую сумму, равную или превышающую 500-кратный размер базовой расчетной величины, установленный на день последнего перевода (поступления);
* операции с клиентами-нерезидентами, информация об учредителях которых отсутствует и получить ее всеми доступными методами невозможно;
* операция, связанная с использованием денежных средств или иного имущества, к которым предоставлен доступ, включая попытку ее проведения;
* другие операции, не имеющие критериев и признаков, предусмотренных в данном пункте, установленных настоящими Правилами и внутренними правилами коммерческого банка, в отношении которых у коммерческого банка имеются подозрения в причастности к легализации доходов, полученных от преступной деятельности, и (или) финансированию терроризма;
* передача нерезидентом резиденту денежных средств в качестве грантов, финансовой помощи, займов или безвозмездной помощи;
* отправка и получение денежных средств через системы международных денежных переводов гражданами Республики Узбекистан, находящимися в зонах с повышенной террористической активностью (список стран и территорий предоставляется специально уполномоченным государственным органом);
* операции лиц, которые находятся в межгосударственном розыске за совершение преступления террористического характера (перечень лиц предоставляется специально уполномоченным государственным органом);
* денежный оборот юридического лица - клиента равен или превышает 20000-кратный размер базовой расчетной величины в течение срока, не превышающего 3 месяцев с момента создания данного юридического лица, и осуществляется с целями, не соответствующими характеру его деятельности;
* покупка физическими лицами монет Центрального банка из драгоценных металлов на сумму, равную или превышающую 500-кратный размер базовой расчетной величины, единовременно или многократно в течение срока, не превышающего 1 месяца.

Внутренними правилами могут быть установлены дополнительные критерии и признаки сомнительных и подозрительных операций, согласовываемые с Исполнителем в ходе реализации проекта.

Подсистема «Сомнительные/Подозрительные операции» должна иметь возможность выполнения следующих функций:

- возможность просмотра и редактирования реквизитов операции со статусом «Необработанные»;

- возможность просмотра данных по участникам операции и их учредителям;

- возможность создания новой операции с пустыми значениями реквизитов для заполнения данных пользователей и подготовки к отправке в СУГО;

- возможность поиска и просмотра операций в базе данных Системы через визуальный веб-интерфейс с фильтрацией по статусу операции и диапазону дат;

- возможность перевода выбранных операций в статус «На отправку в СУГО»;

- возможность перевода выбранных операций в статус «Архив» с обязательным проставлением комментария. Перевод операции в статус «Архив» должен быть авторизован;

- возможность просмотра списка операций - источников, на основании которых данная операция признана сомнительной или подозрительной;

Система должна иметь возможность обеспечения работы с функциями подсистемы через пользовательский веб-интерфейс.

Система должна иметь возможность просмотра заблокированного платежа и платежа, основанного на историческом совпадении для предложения возможности истинного совпадения или автоматически блокировать / деблокировать платеж на основе журнала логов и комментариев;

Система должна иметь возможность поддержки интеграции с SWIFT Alliance Access (SAA) и RENTAS.

**Таблица 4.3.6.2.1. Примеры кодов подозрительных операций, проводимых в национальной и в иностранной валюте для перевода в статус «На отправку в СУГО»**

|  |  |
| --- | --- |
| **КОДЫ СПО** | **Описание операции** |
| 101 | Одной из сторон операции является лицо, постоянно проживающее, находящееся или зарегистрированное в государстве, не участвующем в международном сотрудничестве в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма |
| 102 | Получение отправленных из-за рубежа или отправление за рубеж физическими лицами (в том числе несколькими физическими лицами на имя одного контрагента) денежных средств в иностранной валюте, в том числе через системы денежных переводов, на общую сумму, равную или превышающую 500-кратный размер минимальной заработной платы, единовременно или многократно в течение срока, не превышающего 1 месяца |
| 103 | Продажа или покупка, а также снятие с международных платежных карт физическими лицами и/или индивидуальными предпринимателями денежных средств в иностранной валюте на сумму, равную или превышающую 500-кратный размер минимальной заработной платы, единовременно или многократно в течение срока, не превышающего 1 месяца |
| 104 | Перечисление денежных средств за пределы Республики Узбекистан на счет, открытый на анонимного владельца, и поступление денежных средств в Республику Узбекистан со счета, открытого на анонимного владельца или при отсутствии сведений об отправителе |
| 527 | Перечисление денежных средств за пределы Республики Узбекистан на счет получателя, открытого в банке, зарегистрированном в оффшорной зоне, отличающейся от места регистрации получателя |
| 106 | Денежные средства переводятся за пределы Республики Узбекистан на счета или в пользу лиц, постоянно проживающих или зарегистрированных в оффшорных зонах, либо поступают в Республику Узбекистан со счетов таких лиц единовременно или многократно в течение 30 дней, на общую сумму, равную или превышающую 500-кратный размер минимальной заработной платы, установленный на день последнего перевода (поступления) |
| 522 | Операции с клиентами-нерезидентами, информация об учредителях которых отсутствует и получить ее всеми доступными методами невозможно |
| 526 | Операция, связанная с использованием денежных средств или иного имущества, к которым предоставлен доступ, включая попытку ее проведения |
| 516 | Передача нерезидентом резиденту денежных средств в качестве грантов, финансовой помощи, займов или безвозмездной помощи |
| 530 | Денежный оборот юридического лица — клиента равен или превышает 20000-кратный размер минимальной заработной платы в течение срока, не превышающего 3 месяцев с момента создания данного юридического лица, и осуществляется с целями, не соответствующими характеру его деятельности |
| 531 | Покупка физическими лицами монет Центрального банка из драгоценных металлов на сумму, равную или превышающую 500-кратный размер минимальной заработной платы, единовременно или многократно в течение срока, не превышающего 1 месяца |
| 601 | Юридическое или физическое лицо, которое участвует или подозревается в участии в террористической деятельности |
| 602 | Юридическое или физическое лицо, которое прямо или косвенно является собственником или контролирует организацию, осуществляющую или подозреваемую в осуществлении террористической деятельности |
| 603 | Юридическое лицо, которое находится в собственности или под контролем физического лица либо организации, осуществляющих или подозреваемых в осуществлении террористической деятельности |
| 604 | Операции лиц, которые находятся в межгосударственном розыске за совершение преступлении террористического характера |
| 605 | Одной из сторон операции является лицо, постоянно проживающее, находящееся или зарегистрированное в зонах с повышенной террористической активностью(из зон ПТА) |
| 606 | Одной из сторон операции является лицо, постоянно проживающее, находящееся или зарегистрированное в зонах с повышенной террористической активностью(в зоны ПТА) |
| 999 | Прочие виды операций |

**Таблица 4.3.6.2.2. Примеры кодов сомнительных операций, проводимых в национальной и иностранной валюте для перевода в статус «На отправку в СУГО»**

|  |  |
| --- | --- |
| **КОДЫ СПО** | **Описание операции** |
| 501 | Операции или клиенту, ее осуществляющему, коммерческим банком присвоен высокий уровень риска |
| 503 | Систематически осуществляемый возврат клиентом-резидентом ранее полученной суммы в пользу нерезидента по договору поставки товаров (выполнения работ, оказания услуг) |
| 508 | Операция не имеет явного экономического смысла и не соответствует характеру и виду деятельности клиента |
| 511 | Необоснованное дробление сумм аналогичных операций, совершаемых клиентом на общую сумму, равную или превышающую 500-кратный размер минимальной заработной платы на день осуществления операции |
| 515 | Внесение физическим лицом в наличной форме денежных средств на сумму, равную или превышающую 500-кратный размер минимальной заработной платы на день осуществления операции, на банковский счет юридического лица или индивидуального предпринимателя в качестве займов, финансовой помощи, вклада в уставный фонд (капитал) либо оборотных средств в целях пополнения |
| 520 | Снятие со счета физического лица денежных средств в наличной форме на сумму, равную или превышающую 500-кратный размер минимальной заработной платы на день осуществления операции |
| 519 | Осуществление операций (оплата или снятие наличности) с пяти и более международных платежных карт в течение одного дня по терминалу одного контрагента, когда сумма операций с каждой картой равна или превышает 25-кратный размер минимальной заработной платы |
| 528 | Перечисление денежных средств за пределы Республики Узбекистан на счет получателя, открытый в банке, местонахождение которого отличается от места регистрации получателя |

**4.3.6.3. Подсистема «Отправка в СУГО»**

Подсистема должна иметь возможность отправки подготовленной операции в СУГО, возврат на доработку формирование сообщений и последующая отправка сообщений в СУГО.

Подсистема «Отправка в СУГО» должна иметь возможность выполнения следующих функций:

- возможность просмотра реквизитов операции перед отправкой в табличном и карточном виде без возможности редактирования;

- возможность поиска и просмотра операций в базе данных Системы через визуальный веб- интерфейс с фильтрацией по статусу операции и диапазону дат;

- возможность отправки операций в СУГО. Инициируется процесс формирования электронного сообщения с последующей отправкой в СУГО на специальный защищенный от несанкционированного доступа электронный почтовый адрес.

- возможность возврата на доработку без отправки в СУГО;

- возможность просмотра всех отправленных операций в СУГО с указанием текущего статуса;

- возможность просмотра сообщения, отправленного в СУГО;

- возможность просмотра сообщения-подтверждения, полученного из СУГО;

- возможность визуального отображения статусов операций: например «Полученные СУГО», «Отправленные», «Ошибки», «Отклоненные СУГО»;

Система должна иметь возможность обеспечения работы с функциями подсистемы через пользовательский веб-интерфейс.

Подсистема должна иметь возможность предоставления Пользователю возможности просмотра сообщения в виде XML и виде печатной формы. Подтверждения о получении сообщений в СУГО должны выводиться в виде XML и печатной формы в виде документа формата XLS.

Система должна иметь возможность открытия отдельной страницы для получения сообщений из СУГО на предоставление дополнительной информации для формирования ответа и мониторинга доставки.

**4.3.7. Требования к подсистеме противодействия мошенничеству (Fraud)**

Система должна иметь возможность обеспечения централизованного представления информации о подозрительных событиях во всех продуктах и каналах для обнаружения новых схем мошенничества и точек входа.

Система должна иметь возможность наличия механизмов оповещения и корреляции событий, чтобы выявить скрытые связи и тенденции.

Система должна иметь возможность поддержки мониторинг в режиме реального времени, а также возможность приостановки транзакций.

Система должна иметь возможность наличия интерфейсов для расследования подозрительных событий в режиме реального времени.

Система должна иметь возможность наличия механизмов продвинутой оценки рисков для определения приоритетов в расследовании подозрительных событий.

Система должна иметь возможность наличия широкого набора готовых сценариев мошенничества и методов их обнаружения, включая кражу личных данных; захват аккаунта; мошенничество сотрудников/инсайдеров; мошенничество с электронными платежами; мошенничество в Интернете; мошенничества с чеками и депозитами; мошенничество с банкоматами и дебетовыми картами.

Система должна иметь возможность наличия инструментария для комплексного управления инцидентами, включая организацию рабочего процесса, документирование, данные об убытках, репутационных потерях и их восстановлении, а также контрольный журнал всех событий, обеспечивающий возможность тщательного аудита.

Система должна иметь возможность получения необходимого набора данных, необходимых для управления процессами Antifraud в Банке из ИАБС, а также хранение всех полученных данных в системе;

Система должна иметь возможность автоматического выявления операций, в отношении которых есть подозрения, что они связаны с мошенничеством, на основе разработанных сценариев выявления подозрительных операций. Каждая операция должна проверяться по всем существующим сценариям. Каждый сработавший сценарий должен добавлять расшифровку в поле комментария;

Система должна иметь возможность сохранения информации по подозрительным операциям в течение срока, требуемого Законодательством РУ (не менее пяти лет после осуществления таких операций или прекращения деловых отношений с клиентами);

Система должна иметь возможность предоставления пользовательского веб-интерфейса для запуска и расчета отчетов, создания новых и изменения существующих на основе данных, содержащихся в хранилище системы;

Система должна иметь возможность предоставления пользовательского веб-интерфейса для обеспечения возможности корректировки сценариев, логики их работы и установочных параметров (КНП, суммы, категории операций и т.д.) по выявлению подозрительных операций;

Система должна иметь возможность генерация отчетности о пользователях, их ролях и истории действий в Системе либо через существующему аналитическую платформу Банка.

Система должна иметь возможность автоматически блокировать учетные записи пользователей, которые не использовались на протяжении длительного времени – более 180 дней. Условие не распространяется на учетные записи администраторов системы;

Система не должна иметь незадекларированных функций, позволяющих обойти механизмы контроля;

Для минимизации пользовательских ошибок ввода данных Система должна иметь возможность автоматического контроля ввода на уровне интерфейсных форм, а именно обязательность заполнения реквизитов, а также форматный контроль.

**4.3.7.1. Подсистема «Проведенные операции»**

Подсистема должна иметь возможность просмотра и отображения всех операций, полученных из ИАБС с возможностью фильтрации и последующей отправкой в сомнительные или подозрительные операции.

Подсистема должна иметь возможность выполнения следующих функций:

- возможность получения, накопления в едином хранилище Системы данных о проведенных операциях из ИАБС;

- возможность поиска и просмотра операций в базе данных Системы через визуальный веб-интерфейс;

- возможность фильтрации всех операций по диапазону дат по реквизиту «Дата время совершения операции»;

- возможность ручного переноса пользователем операций в категории сомнительные и/или подозрительные с указанием кода типа подозрения;

- возможность просмотра операций в виде списка, а также детального просмотра всей полученной информации в расширенном виде;

- возможность выполнения проверки и выявления сомнительных и/или подозрительных операций, на основе сценариев в автоматическом режиме без участия пользователя.

Система должна иметь возможность обеспечения работы с функциями подсистемы через пользовательский веб-интерфейс.

Алгоритмы работы сценариев должны быть построены на основе критериев и признаков по выявлению сомнительных и подозрительных операций, в соответствии с «Правилами внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения в коммерческих банках».

Для управления работой сценариев Система должна иметь возможность выполнения следующего функционала:

- Указание порядка выполнения сценария;

- Активация и деактивация сценария;

- Удаление сценария.

Ниже приведены примеры сценариев:

1. При выходе сотрудника в трудовой отпуск - блокирование доступа в систему. При попытке входа логином и паролем данного сотрудника, Система оповещает Пользователя с указанием IP-адреса компьютера, с которого совершена попытка входа в Систему.

- необходима интеграция с кадровой службой ИАБС

2. При входе в Систему в позднее вечернее время сотрудником банка, Система сообщает об этом Исполнителю с указанием счетов, транзакций и IP-адреса компьютера, с которого осуществлен вход и оповещает Пользователя.

3. При совершении хищения денежных средств или мошенничества, Пользователь анализирует данный факт и вводит в Систему счета, механизм и алгоритм нарушения. Текстовая аналитика, которая выполняется с помощью технологий поиска, категоризации контента и извлечения сущностей. Система обязана выявить аналогичные факты в других филиалах банка.

4. При получении chargeback от Компании VISA необходимость установления прокси-серверов, IP-адресов по международным картам VISA.

5. Оплата в российском интернет-магазине осуществляется картой VISA, выпущенной в Узбекистане, а плательщик находится в Испании. Система анализирует и автоматически присваивает транзакциям высокий уровень риска совершения мошеннических операций.

6. Анализ транзакций по картам, которым присваивается «метка», характеризующая способ обработки транзакции и разделение на три типа меток:

• «Зеленая» отмечает транзакции с низкой вероятностью возникновения мошеннической операции.

• «Желтой» меткой отмечаются транзакции, в которых шанс возникновения мошеннической операции выше среднего, и для проведения платежа потребуются дополнительного внимания.

• «Красной» отмечаются транзакции, которые с наибольшей вероятностью могут оказаться мошенническими, и при их проведении потребуется документальное подтверждение аутентичности владельца карты.

7. Трассировка операций – учет местонахождения объектов в привязке к месту и времени.

**4.3.7.2. Подсистема «Подозрительные операции»**

Подсистема должна иметь возможность просмотра, редактирования данных о подозрительных операциях.

Подсистема «Подозрительные операции» должна иметь возможность выполнения следующих функций:

- возможность просмотра и редактирования реквизитов операции со статусом «Необработанные»;

- возможность просмотра данных по участникам операции;

- возможность поиска и просмотра операций в базе данных Системы через визуальный веб-интерфейс с фильтрацией по статусу операции и диапазону дат;

- возможность перевода выбранных операций в статус «Архив» с обязательным проставлением комментария. Перевод операции в статус «Архив» должен быть авторизован;

- возможность просмотра списка операций - источников, на основании которых данная операция признана сомнительной или подозрительной;

Система должна иметь возможность обеспечения работы с функциями подсистемы через пользовательский веб-интерфейс.

**4.3.7.3. Подсистема «Клиенты»**

Подсистема должна иметь возможность формирования и редактирования данных в карточках клиентов, находящихся в Системе.

Подсистема «Клиенты» должна иметь возможность обеспечивать выполнение следующих функций:

- возможность редактирования данных в карточках клиентов, полученных из ИАБС, а также создание новых;

- при обновлении данных в карточке клиентов в ИАБС Система должна иметь возможность обновления информации в Системе с учетом следующего условия: если из ИАБС получено нулевое значение поля, то информация в Системе в данном поле сохраняется.

- при обновлении данных Система должна иметь возможность опционального использования двойного контроля при изменении данных в карточках клиентов через пользовательский веб-интерфейс.

**4.3.7.4. Подсистема «Онлайн»**

Подсистема должна иметь возможность проверки в режиме реального времени определенного набора данных при заведении карточки клиента в ИАБС, в том числе при изменении данных в карточке клиента по клиентам, бенефициарным собственникам, учредителям (акционерам) клиентов и руководителям; а также при проведении операций в ИАБС - проверки данных по клиентам, бенефициарным собственникам, операциям и участникам операций, передаваемого из ИАБС посредством использования веб-сервисов, по заданным условиям проверки. Кроме того, при выявлении совпадений клиентов и/или бенефициарных собственников клиентов по спискам в режиме онлайн существует возможность автоматической приостановки операций открытия счета (-ов) таких клиентов.

Подсистема должна иметь возможность выполнения следующих функций:

- просмотр операций, совершаемых клиентами, совпавшими со списками (Перечнем и иные собственные списки) Системы;

- проверка клиентской базы на совпадения со списками Системы.

- анализ поступивших результатов совпадения и принятие решения по достижению предельных пороговых значений параметров по каждому из участников;

- формирование сообщения в ИАБС с решением о разрешении или запрете проведения операции.

- ручное редактирование списков Системы;

- двойной контроль изменений данных в списках Системы.

- уведомление пользователей Системы о совпадении со списками Системы.

Система должна иметь возможность обеспечения работы с функциями подсистемы через пользовательский веб-интерфейс.

**4.3.7.5. Подсистема «Управление рисками»**

Подсистема должна иметь возможность обеспечения оценка уровня риска мошенничества клиента путем выполнения следующих процедур:

- возможность отметки основных объектов Системы признаком «уровень риска»: клиент, операция.

- возможность разработки модели автоматического расчета уровня риска для основных объектов Системы на основании экспертных заключений и результатов статистического анализа.

- возможность гибкой настройки уровней риска основных объектов системы, используя пользовательский веб- интерфейс.

- возможность расчета балла и присвоения уровня риска клиенту в режиме онлайн при заведении карточки клиента в ИАБС. Система также предоставляет возможность принятия решения по клиенту комплаенс- контроллеру через веб-интерфейс.

Подсистема должна иметь возможность выполнения следующих функций

- возможность ведения настроечных таблиц, с помощью которых настраивается расчет по оценочным показателям

- возможность расчета рисков необходимо производить по шкале, например по 2-х уровневой шкале: 1-низкий; 2-высокий риск.

- возможность формирования отчетов, для контроля и управления рисками ОД/ФТ;

- возможность ведения пересчета значений риска, обеспечивающий возможность как автоматического расчета по заданному расписанию, так и проведения ручного пересчета уровня рисков как по каждому клиенту отдельно, так и по всем карточкам клиента;

- возможность ведения журнала изменений уровней риска, для учета исторических данных по расчету/пересчету уровней риска;

Система должна иметь возможность обеспечения работы с функциями подсистемы через пользовательский веб-интерфейс.

**4.3.8. Требования к подсистеме отчетности**

Подсистема отчетности должна иметь возможность предоставления возможности запуска, получения результата, хранения рассчитанных отчетов, создания новых отчетов и редактирования существующих. При этом Исполнителем для реализации необходимого перечня отчетности Системы может быть реализовано на базе эксплуатируемых банком инструментов формирования отчетности.

Подсистема должна обеспечивать выполнение следующих функций:

- Возможность запуска отчетов с указанием входящих параметров и/или критериев отбора информации либо формирование отчетов через корпоративной портал отчетности Банка;

- Возможность просмотра результата в форматах XML и XLS;

- Возможность хранения ранее сформированных отчетов с указанием даты формирования, пользователя и входящих параметров;

Система должна иметь возможность обеспечения работы с функциями подсистемы через пользовательский веб-интерфейс.

В Система должна иметь возможность формирования следующих видов отчетов:

* **Детальные отчеты по операциям:**
* Операции, отправленные в СУГО;
* Операции, по которым получен запрос от СУГО;
* Не отправленные в СУГО операции (архивные);
* Подозрительные операции;
* Сомнительные операции;
* Отчет «Полученные из ИАБС»;
* Отчеты, предоставляемые в СУГО;
* Отчет о приостановленных операциях и (или) замороженных денежных средствах или иного имущества лиц, включенных в Перечень;
* Отчет о совершенных операциях по купле иностранной валюты физическими лицами через электронный кошелек по приложению «Миллий» с деталями. (Пример шаблона приведен в Таблице 4.3.8.1).
* Аналитический отчет по запрашиваемым счетам клиентов, дебетовым и кредитовым оборотам с выписки счета по деталям платежа.
* **Статистические отчеты:**
* Отчет «Количество операций, выгруженных из ИАБС» (статистический);
* Подозрительные операции в разрезе дней;
* Подозрительные операции в разрезе месяцев;
* Сомнительные операции в разрезе дней;
* Сомнительные операции в разрезе месяцев;
* **Отчеты по рискам:**
* Отчеты клиентов высокого уровня риска в разрезе дней (юр,ИП и физ);
* Отчеты клиентов высокого уровня риска в разрезе месяцев(юр,ИП и физ);
* Отчет по странам (с данными контрагентов);
* Отчет по странам и регионам денежных переводов с данными контрогентами;
* Отчет по странам и регионам по Свифту с данными контрогентами;
* Отчеты по ПТА и АТЦ;
* Отчет по странам (с данными контрагентов)
* Отчет статистический по продуктам/услугам;
* Отчет статистический по клиентам;
* Отчет расширенный по клиенту;
* Отчет статистический по уровням рисков в разрезе по типам клиентов;
* Отчет статистический по уровням рисков в разрезе по бизнес-блокам;
* **Отчеты по идентификации:**
* Отчет об идентифицированных юридических лицах, по дате и в разрезе месяца
* Отчет об идентифицированных индивидуальных предпринимателях, по дате и в разрезе месяца
* Отчет об идентифицированных физических лицах по дате и в разрезе месяца;
* Отчет о не идентифицированных юридических лицах по дате и в разрезе месяца
* Отчет об не идентифицированных индивидуальных предпринимателях, по дате и в разрезе месяца;
* Отчет о не идентифицированных физических лицах по дате и в разрезе месяца;
* **Административные отчеты**
* Пользователи и роли системы;
* Журнал аудита действий.

Окончательный перечень отчетности и шаблоны форм отчетов будут представлены Банком Поставщику при разработке проектной документации и согласовано с Исполнителем. При этом Исполнителем для реализации необходимого перечня отчетности Системы может быть реализовано на базе эксплуатируемых банком инструментов формирования отчетности.

**Таблица 4.3.8.1. Пример шаблона отчетности**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| МФО Банка | Наименование клиента | Номер паспорта и серия | ИНН | Сумма купленной иностранной валюты с начала года | Эквивалент в сумах | Счет оприходованной иностранной валюты | Расходы на обмен валюты (эквивалент в долларах США) | | | | | | | |
| Снято наличными | | Снято безналичными через терминалы за товары и услуги за рубежом | Оплата через инвойс за товары и услуги | Предмет инвойса (товары или услуги) | Обратная конверсия | Остаток суммы |
|
|
| На территории республики | За рубежом |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |  | 15 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

*продолжение*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Источник (в сумах) | | | | | | | | | | | | | | | | | | | | | | |
| Сумовой счет клиента для приобретения ин.валюты  (20206000/22618000) | Общие поступления на счета клиента в сумах для приобретения ин.валюты | Источник средств, поступивших на банковский счет | | | | | | | | | | | | | | | | | Поступления с банковских карт других банков | | | |
| Наличными | Поступления от физ. лиц | | | Поступления от частных предпринимателей | | | | | | Поступления от юр. лиц | | | | | | | Сумма | Банк эмитент банковской карты | Счет или владелец Ф.И.О. | Номер банковской карты |
| Переводы от физ. лиц | В том числе | | Сумма поступления со счетов частных предпринимателей | В том числе | | | | | Сумма поступления со счетов юр. лиц | В том числе | | | | | |
| Кредитные средства физ. лиц | Собственные средства | Сумма поступления кредитных средств частных предпринимателей | Торговая выручка | Финансовая помощь или займ | За предоставленные услуги или товары от физ. лиц | Другие цели | Сумма поступления кредитных средств юр. лиц | Финансовая помощь или займ | дивиденд | Сумма уменьшения Устава | За предоставленные услуги или товары от физ. лиц | Другие цели |
| 23 | 17=18+19+22+28+35 | 18 | 19=20+21 | 20 | 21 | 22=23+24+25+26+27 | 23 | 24 | 25 | 26 | 27 | 28=29+30+31+32+33+34 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Система должна иметь возможность предоставить ежедневный сводный и подробный отчет для отчетности о результатах и ходе закрытия кейса;

Система должна иметь возможность предоставления настраиваемого отчета о транзакциях для оповещения, созданного правилами обнаружения. Отчет должен быть отсортирован по дате и времени транзакции и показан в столбцах кредита и дебета;

Система должна иметь возможность обеспечить просмотр клиентом всех сгенерированных оповещений, включая закрытые;

Система должна иметь возможность интеграции с другими инструментами отчетности, такими как Qlik View и т. д.;

Система должна иметь возможность предоставления ежедневного, еженедельного и ежемесячного отчета о рисках для профилирования рисков клиентов и мониторинга транзакций.

Система должна иметь возможность развернуть отчет / дэшборд для разбивки отчета.

Система должна иметь возможность предоставить пользователю настроить для собственной панели инструментов / домашней страницы;

Система должна иметь возможность предоставить удобный интерфейс для настройки панели инструментов и отчета;

Система должна иметь возможность интеграции со сторонними инструментами отчетности.

**4.4. Требования к взаимодействию со сторонними информационными системами**

Система должна иметь возможность интеграции с Enterprise Application Interface (EAI) через веб-сервисы / API.

Информационный обмен между компонентами системы должен осуществляться в режиме on-line через единую базу данных.

Использование вышеописанной схемы должно обеспечить оперативную передачу данных.

Система должна иметь возможность интеграции с информационными системами:

* + - * + Режим «Оффлайн»
        + Интеграция c ИАБС. Выгрузка проведенных операций.
        + Принципы и алгоритмы интеграции:

В режиме «Оффлайн» осуществляется проверка проведенных банковских операций по сценариям, для выявления, анализа и отправки в СУГО данных о подозрительных операциях. В этом режиме Система не участвует в документообороте ИАБС, а должна иметь возможность получения проведенных банковских операций из ИАБС в виде выгрузок данных в формате XML через веб-сервис. Запуск проверки по сценариям должен осуществляется автоматически через заданный промежуток времени.

Обмен данными может быть предусмотреть в одном или нескольких следующих форматов XML/JSON/CSV. Формат будет определен при согласовании проектной документации.

Интеграция c ИАБС. Получение карточек клиентов из ИАБС

Для формирования сообщения в СУГО со сведениями об участнике операции Система должна иметь возможность получения карточек клиентов из ИАБС. Для уменьшения объема передаваемых данных при выгрузке операций с систему ПОД/ФТ передается только минимальный набор данных по участникам операции. В случае необходимости формирования сообщения в СУГО Система должна иметь возможность производить запрос в веб-сервис Банка на получение карточки клиента по уникальному номеру клиента.

Интеграция c СУГО. Отправка электронных сообщений

Интеграция Банка с СУГО должна быть реализована посредством обмена электронными почтовыми сообщениями. Отправка сообщений в СУГО должна производится со специально-выделенного электронного почтового адреса Банка через Почтовый сервер Банка.

Для получения сообщений от Банка СУГО предоставляет специальный защищенный от несанкционированного доступа электронный почтовый адрес. Все сообщения, отправляемые и получаемые из СУГО должны сохраняться в Системе в формате передачи XML.

Режим «Онлайн»

* + - * + Интеграция c ИАБС. Проверка онлайн операций.

В режиме «Онлайн» осуществляется включение Системы в документооборот ИАБС, для выполнения проверок на принадлежность отправителя, получателя и их учредителей со списками Системы с возможностью приостановки банковской операции в автоматическом режиме, до решения пользователя в Системе. В данном режиме Система должна иметь возможность отправки в ИАБС сообщения об отсутствии совпадений, если не достигнуто пороговое значение при проверке по спискам Системы. При совпадении свыше порогового значения выводится сообщение пользователю Системы о найденном совпадении и отправляется в ИАБС сообщение о приостановлении проводки, до того момента, пока пользователь Системы не примет решение о проведении.

В функции анализатора должны входить:

Просмотр операций, совершаемых клиентами, совпавшими со списками (Перечнем, санкционные списки и собственные списки) Системы;

- Проверка совпадений по спискам Системы;

- Анализ поступивших результатов и принятие решения по достижению предельных пороговых значений параметров по каждому из участников;

- Формирование сообщения в ИАБС с решением о разрешении или запрете проведения операции.

- Блок транслитерации и конвертации и выявления совпадения должен быть предназначен для:

- Выполнение транслитерации поступающих из ИАБС данных в латиницу для осуществления проверки по спискам Системы;

Так как источниками списков являются различные источники, то существует вероятность неполного написания имени или порядка слов. Аналогичная ситуация и с данными из ИАБС. Для увеличения вероятности совпадения должны выполняться следующие преобразования данных, поступающих из ИАБС:

Производится транслитерация и приведение букв к одному регистр: (Иванов Иван Иванович -> IVANOV IVAN IVANOVICH);

Каждое поступившее наименование или ФИО участника операции для повышения вероятности соответствия спискам приводится во всех различных написаниях.

Осуществляется проверка по алгоритму нечеткого сравнения строк по спискам Системы всех различных написаний участников и учредителей и выбирается максимальный процент совпадения.

В случае, если процент совпадения равен или превышает пороговое значение, то автоматически отправляется сообщение ответ в ИАБС о запрете на проведение данной операции и пользователю в Системе выводится сообщение, в котором необходимо подтвердить возможность проведения данной операции. Операция будет находиться в статусе «Необработанные» в Системе до принятия решения пользователем.

Хранилище онлайн операций предназначено для хранения всех данных, когда-либо попадавших на анализ в Систему, а также результаты проверки и максимальный процент совпадения.

Обмен данными с другими информационными системами должен осуществляться по согласованным форматам и протоколам передачи данных. Система должна также иметь возможность построения интеграционных потоков со всеми информационными системами, эксплуатируемыми в Узнацбанке, посредством единой интеграционной шины на базе IBM ESB. Исполнителем могут быть предложены другие форматы, протоколы и сценарии интеграции информационных систем Банка с Системой на базе эксплуатируемой банком интеграционной шины данных IBM ESB.

## 4.5. Требования к видам обеспечения

### 4.5.1. Требования к математическому обеспечению

Не предъявляются.

### 4.5.2. Требования к информационному обеспечению

* Для кодирования информации должны использоваться принятые у Заказчика классификаторы;
* Должна быть обеспечена совместимость с информационным обеспечением систем, взаимодействующих с внедряемой Системой;
* Формы документов должны отвечать требованиям корпоративных стандартов Заказчика (или унифицированной системы документации);
* Структура документов и экранных форм должна соответствовать характеристикам терминалов на рабочих местах конечных пользователей;
* Графики формирования и содержание информационных сообщений, а также используемые аббревиатуры должны быть общеприняты в этой предметной области и согласованы с Заказчиком;
* В Системе должны быть предусмотрены средства контроля входной и результатной информации, обновления данных в информационных массивах, контроля целостности информационной базы, защиты от несанкционированного доступа;
* Доступ к данным должен быть предоставлен только авторизированным пользователям с учетом их служебных полномочий, а также с учетом категории запрашиваемой информации;
* Необходимо предусмотреть возможность экстренного отключения доступа к Системе в случаях внештатных ситуаций.

### 4.5.3. Требования к лингвистическому обеспечению

Необходимо, чтобы Система обеспечивала эффективную возможность ввода информации и работу интернационального офиса с помощью инструментов мультиязычности, которые должны обеспечить возможность использовать несколько языков в одном интерфейсе. При этом название полей в экранных формах должно быть на английском или русском языке.

Мультиязычность не подразумевает перевод служебных сообщений на государственный язык;

Мультиязычность будет использоваться в рамках стандартных возможностей Системы по выводу информации на разных языках.

### 4.5.4. Требования к программному обеспечению

ПО должно поставляться с комплектами лицензий, соответствующими числу рабочих мест, на которых его предполагается устанавливать, и иметь наиболее позднюю по времени выпуска версию производителя.

Лицензии на программное обеспечение системы должно быть представлено следующими категориями:

|  |  |
| --- | --- |
| **№** | **КАТЕГОРИЯ ЛИЦЕНЗИЙ НА СИСТЕМУ** |
| 1 | Лицензии ядра Системы |
| 2 | Лицензии СУБД |
| 3 | Лицензии операционной системы серверов |
| 4 | Лицензии программных компонентов обеспечения отказоустойчивости (кластерного ПО) |
| 5 | Общесистемное программное обеспечение |
| 6 | Программное обеспечение для резервного копирования в виртуальной среде |

ПО Системы должно обладать следующими характеристиками:

* выполнять весь перечень алгоритмов математического обеспечения;
* обеспечивать устойчивость к ошибочным ситуациям, в том числе при неверных и противоречивых данных; сбои в работе программ, отказы части вычислительных средств, ошибки персонала должны диагностироваться, сопровождаться сообщениями, и не должны вызывать нарушений в работе системы;
* обеспечивать автоматический перезапуск при восстановлении электрического питания после его отключения без выдачи ложных сигналов и управляющих воздействий;
* давать правильные результаты при всех комбинациях исходных данных, допустимых в рамках постановки задачи;
* иметь возможность оперативного конфигурирования в процессе функционирования Системы.

Должна иметься возможность задания паролей и установления границ санкционированного доступа при внесении изменений в прикладное ПО.

### 4.5.5. Требования к техническому обеспечению

Проект подразумевает поставку «под ключ», что включает в себя обеспечение доставки при условии всех требований по поставке, установке, монтажу, настройки и документирования Системы, пуско-наладки вычислительной системы, обучения, тестирования работоспособности поставляемого оборудования и программного обеспечения (проведения приемочных испытаний) и ввод в действие всего комплекса и начала полноценного функционирования.

Аппаратно-программная архитектура должна удовлетворять следующим требованиям:

Решение должно быть открытой системой, построенной в соответствии с модульной сервис-ориентированной многозвенной архитектурой с выделением следующих уровней:

- централизованный сбор, хранение и обработка данных;

- масштабируемый сервер приложений, где сосредоточена вся логика бизнес- процессов и основная вычислительная нагрузка;

- пользовательский веб-интерфейс.

Пользовательский веб-интерфейс Системы должен быть реализован в виде веб-приложения с работой пользователя посредством веб-браузера.

Предлагаемое и поставляемое оборудование и программное обеспечение должно иметь технические характеристики не ниже требований, указанных в таблицах ниже. Схема планируемой архитектуры ИТ-инфраструктуры Системы приведена на рисунке 4.5.5.1.

**1. Технические требования к модернизации серверов базы данных IBM Power 870 Model 9080-MME, SN 7831B08, 7831B18 – 2 комплекта**

|  |  |  |
| --- | --- | --- |
| **№** | **Параметры** | **Требования** |
| 1 | Производитель | IBM |
| 2 | Модель Сервера Базы Данных | 9119 Model MME |
| 3 | Активация имеющихся установленных процессоров | 16 ядер |
| 4 | Количество активированных / установленных ядер в итоге | 28/32 ядра |
| 5 | Тип оперативной памяти | DDR4 |
| 6 | Емкость модуля DIMM | 256 GB DDR4 Memory (4x64GB CDIMMs) |
| 7 | Количество дополнительных модулей к установке | 4 |
| 8 | Активация оперативной памяти | Не менее 512 Гб |
| 9 | Объем активированной / установленной оперативной памяти в итоге | 1536/2048 Гб |
| 10 | Активация операционной системы | Обязательно |
| 11 | Активация кластерного программного обеспечения | Обязательно |
| 12 | Активация программного обеспечения виртуализации | Обязательно |

**2.** **Технические требования к модернизации текущих систем хранения данных**

**IBM Storwize V5030 (Model 2078-324, SN 781CN46, 781CT93)**

**(полки расширения) – 2 комплекта**

|  |  |  |
| --- | --- | --- |
| **№** | **Параметры** | **Требования** |
| 1 | Производитель | IBM |
| 2 | Модель системы хранения данных | Model 2078-324 |
| 3 | Модель полки расширения | Model 2078-24G/12G |
| 4 | Количество дисков с объемом не менее 800 ГБ, форм фактора не менее SAS флэш диски | Не менее 48 |
| 5 | Количество дисков с объемом не менее 16 ТБ, форм фактора не менее HDD со скоростью вращения не менее 7К RPM | Не менее 12 |
| 6 | Поддержка компрессии в реальном времени | Обязательно |
| 7 | Поддержка функций катастрофоустойчивой репликации данных между несколькими системами | Обязательно |
| 8 | Возможность удаленного зеркалирования | Да |

**3.** **Технические требования к модернизации текущих блейд-шасси подсистемы приложений Lenovo PureFlex (Model SN550, PN 7X16A02TEA) - 2 комплекта**

|  |  |  |
| --- | --- | --- |
| **№** | **Параметры** | **Требования** |
| 1 | Производитель | Lenovo |
| 2 | Модель сервера | ThinkSystem SN550 |
| 3 | Тип оперативной памяти | DDR4 2666 MHz (2Rx4 1.2V) RDIMM |
| 4 | Емкость модуля DIMM | Не менее 32GB |
| 5 | Количество дополнительных модулей к установке | 16 |
| 6 | Объем дополнительной оперативной памяти к установке | Не менее 512 Гб |
| 7 | Активация 12 портов оптического коммутатора в шасси | Не менее 1 |
| 8 | Операционная система | Обязательно |

**4.** **Технические требования к системе управления базами данных**

Для обеспечения полноценной работы Cистемы Узнацбанку требуется наличие следующий лицензируемых программных продуктов корпорации Oracle. Лицензируемые продукты Oracle и их опции должны быть лицензированы на количество процессоров, т.е. по метрике «CPU» в следующих количествах:

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование продукта** | **Метрика** | **Кол-во лицензий** |
| 1 | Oracle Database Enterprise Edition - Processor Perpetual | CPU | 8 |
| 2 | Oracle Partitioning - Processor Perpetual | CPU | 8 |
| 3 | Oracle WebLogic Server Enterprise Edition - Processor Perpetual | CPU | 4 |

***Примечания:***

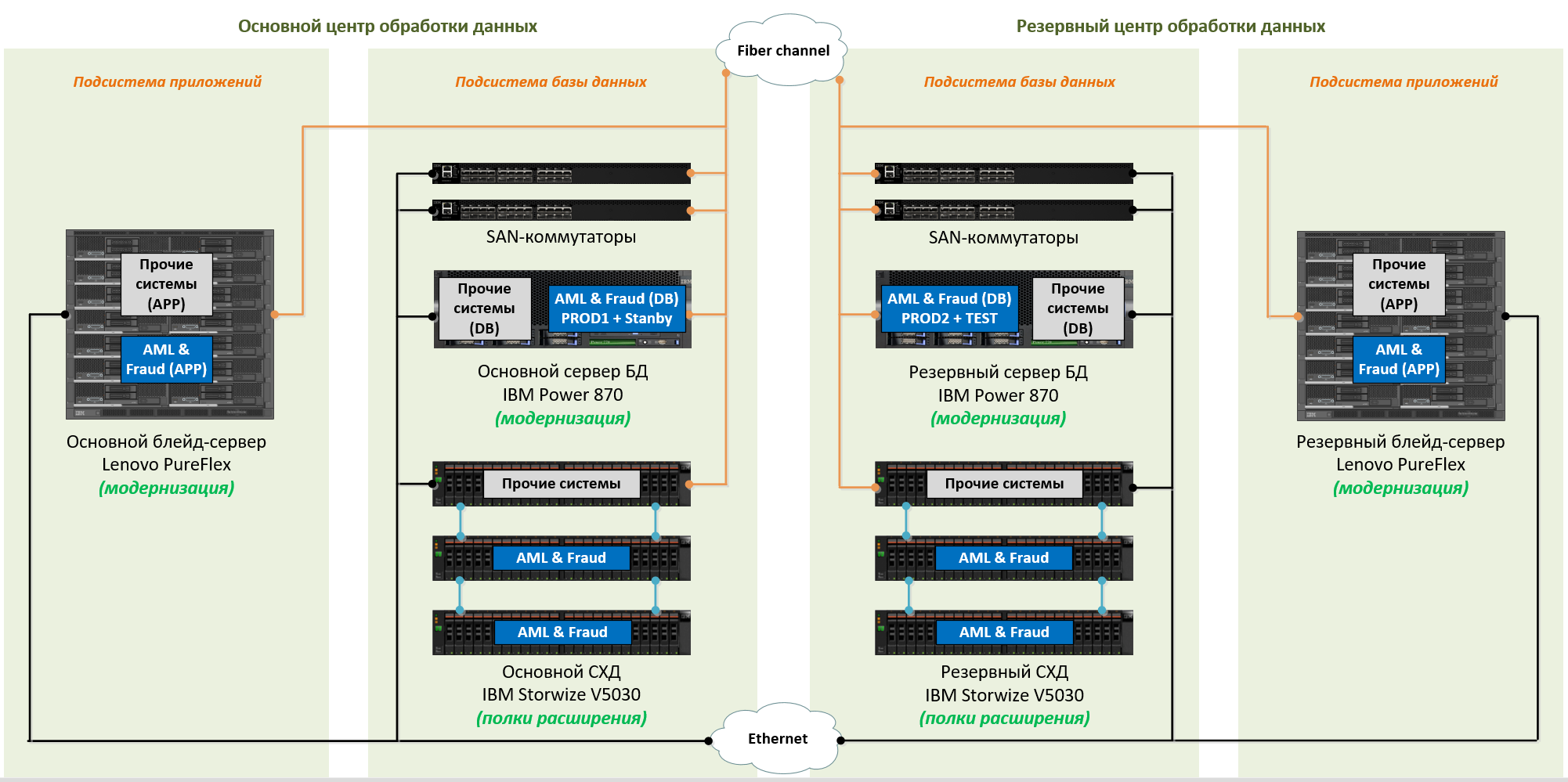
1. комплект лицензий СУБД должен включать трехлетнюю поддержку Oracle;

2. в случае несовместимости предлагаемой программной платформы Системы с СУБД Oracle, Исполнителем должно быть учтено в предложении соответствующее ПО СУБД.

**5. Требования к системе резервного копирования и восстановления**

Для модернизации текущей системы резервного копирования и восстановления на базе Veeam Availability Enterprise Plus необходимы дополнительные лицензии под сервера приложений на базе Lenovo PureFlex. Перечень и лицензий:

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование и описание лицензий** | **Метрика** | **Кол-во лицензий** |
| 1 | Veeam Availability Suite Enterprise Plus (includes Backup & Replication Enterprise Plus + Veeam ONE) | Socket | Не менее 2 |



**Рисунок 4.5.5.1. Схема планируемой ИТ-инфраструктуры Системы**

### 4.5.6. Требования к метрологическому обеспечению

Система должна поддерживать мультивалютность (источником актуального курса валют будет финансовая система Заказчика).

Отсутствие ошибки округления при расчетах денежных единиц.

Отсутствие ошибок округления и отсутствие накопления ошибок расчетов при расчетах по процентному содержанию.

Дополнительных требований к метрологическому обеспечению не предъявляется.

### 4.5.7. Требования к организационному обеспечению

Помимо гарантийной поддержки оборудования, Исполнитель в течение действия гарантийных обязательств должен обеспечить необходимую информационно-консультационную помощь специалистам Заказчика.

Вместе с оборудованием, Исполнителем должна быть представлена эксплуатационная документация и руководства пользователя в бумажном и электронном виде.

Гарантийное сервисное обслуживания всего оборудования должно осуществляться по месту эксплуатации, специалистами авторизованного производителем сервис-центра в Республике Узбекистан.

Производитель оборудования, предложенный исполнителем, должен иметь в Республике Узбекистан признанный сервисный центр для обеспечения гарантийного ремонта поставляемого оборудования.

Сервисный центр должен иметь сертификаты авторизации от производителей поставляемого Исполнителем оборудования.

Гарантийное сервисное обслуживание всего представленного оборудования должно производиться в следующем порядке:

Уполномоченный представитель Исполнителя или сервис центра после вызова уполномоченного представителя Заказчика выполняет следующие процедуры:

* Оформление акта о наличии дефекта оборудования;
* Замену (при наличии) или ремонт неисправного оборудования;
* Оформление акта выполненных работ (после выполнения работ). При этом срок реакции на заявку о техническом обслуживании оборудования не должен превышать 8 часов.

В случае отсутствия в наличии запасных частей у уполномоченного представителя Исполнителя или сервис центра, неисправное оборудование или его неисправная часть, после оформления акта о наличии дефекта оборудования, может быть отправлена для ремонта или замены в сервис центр, указанный Исполнителем в контракте.

**4.5.8.** **Обучение пользователей**

Исполнитель проводит обучение Системы для пользователей в объеме не более 10 человек (ключевых пользователей системы включая конечных пользователей и администраторов). Обучение проводится в г. Ташкент на материально технической базе Заказчика.

Заказчик обеспечивает обучающихся:

* Помещением удовлетворяющем требованиям для обучения соответствующего количества слушателей;
* Наличие компьютерного оборудования в помещении для обучения в нужном количестве и соответствующего требованиям работы в Системе;
* Презентационное оборудование.

### 4.5.9. Требования к методическому обеспечению

Методики расчётов, используемых при решении задач Системы, а также, при необходимости, иные специфические требования к реализации задач, детализируются Исполнителем на стадии разработки Технического проекта и согласовываются с Заказчиком.

Система должна внедряться на основании действующих нормативных правовых актов и организационно-распорядительных документов.

Должны быть разработаны и утверждены в установленном порядке методики и инструкции выполнения пользователями операций в Системе.

В состав методического обеспечения входит:

* нормативные правовые документы;
* должностные инструкции персонала, выполняющего работы с использованием Системы.

Состав методического обеспечения может уточняться в процессе техно-рабочего проектирования и согласовывается с заказчиком.

Нормативно-техническая документация должна соответствовать требованиям нормативных правовых актов и разрабатываться согласно следующих стандартов:

* O‘z DSt 1986:2018 Государственный стандарт Узбекистана Информационная технология. Информационные системы. Стадии создания
* O‘z DSt 1987:2018 Государственный стандарт Узбекистана «Информационная технология. Техническое задание на создание информационной системы».
* O'z DSt 1985:2018 Виды, комплектность и обозначение доку­ментов при создании информационной системы (ИС),
* O‘z DSt 3243:2017 Информационная технология. Локальные и корпоративные вычислительные сети. Общие технические требования
* Т 45-194:2007 Рекомендации по применению программно-аппаратных средств, обеспечивающих предотвращение актов незаконного проникновения в информационные системы.

### 4.5.10. Требования к страхованию товаров

Товары, поставляемые в рамках проекта, должны быть полностью застрахованы с момента погрузки производителем оборудования до их получения Заказчиком согласно условиям доставки Товара. Товары должны быть застрахованы Поставщиком от всех рисков потери или повреждения случайных для производства или приобретения, транспортировки, хранения до момента передачи Заказчику.

### 4.5.11. Требования к объему и/или сроку предоставления гарантий

Предлагаемое оборудование и программное обеспечение должно быть новым (не бывшим в употреблении, неотремонтированным, не рекламным), производства не ранее 2021 г. и соответствовать мировым стандартам.

Гарантия на всё оборудование должна быть не менее 3-х лет. Гарантия на всё программное обеспечение должна быть не менее 1-го года.

С целью комплексной оценки совокупной стоимости владения Системой (TCO - Total Cost of Ownership), Исполнитель должен предоставить информацию по затратам на профессиональные решения/услуги, необходимые для эксплуатации Системы в последующие 5 лет после запуска в промышленную эксплуатацию (техническая поддержка, продление официальной гарантии, лицензирование и пр.).

Исполнитель может учесть в стоимости предложения стоимость пост гарантийного обслуживания (после окончания срока официальной гарантии от производителей) и технической поддержки за 1 год.

### 4.5.12. Требования к месту и условиям поставки закупаемого оборудования

Исполнитель должен обеспечить доставку закупаемого в рамках проекта оборудования:

- для отечественных поставщиков: по адресу Республика Узбекистан 100084, г. Ташкент, проспект А.Темура, 101.

- для иностранных поставщиков: DAP г. Ташкент (ИНКОТЕРМС 2020).

Поставка и погрузочно-разгрузочные работы товаров осуществляется автомобильным транспортом, воздушным транспортом либо любым иным способом за счет средств поставщика до места поставки.

Исполнитель вместе с поставляемым оборудованием и программным обеспечением должен предоставить следующий перечень документов:

- счет-фактуру (инвойс) Исполнителя с описанием поставляемого программного-аппаратного комплекса, с указанием количества и цены, стоимости с указанием 100% суммы отгружаемого комплекса;

- техническая документация на поставляемое оборудование (датащиты);

- сертификат качества (копия);

- упаковочный лист;

- сертификат происхождения;

- авианакладная.

Оформление сертификата происхождения международного образца и сертификата качества на поставляемое оборудование осуществляется на основании письменной заявки от Заказчика, с указанием перечня поставляемого оборудования, для которого необходимы документы.

# 5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО ВВОДУ СИСТЕМЫ

Реализация требований настоящего ТЗ должна проводиться в несколько этапов. Состав и содержание работ по этапам приведено в таблице ниже. Перечень стадий и этапов выполненных работ по внедрению автоматизированной системы указан в соответствии с O‘z DSt 1986:2018 Информационная технология. Информационные системы. Стадии создания. Работы спроектированы с учетом того, что конечная Система должны быть сдана Заказчику Исполнителем «под ключ». Работы будут выполняться Исполнителем, который будет определяться после проведения мероприятий по отбору Исполнителя в рамках реализации данного проекта в целом и в частности её отдельных подсистем на территории расположения дата центров Заказчика (Основной и Резервный).

Методология выполнения проекта должна базироваться на методологии Waterfall.

**Таблица 5. 1. RASCI-матрица (распределение обязанностей**

**между участниками проекта)**

|  |  |  |
| --- | --- | --- |
| **R** | **Responsible** (Ответственный) | Участник проекта, выполняющий Работу для достижения Результата проекта. Ответственный за достижение Результата. |
| **A** | **Approver** (Утверждающий) | Участник проекта, утверждающий корректность и полноту выполнения Работ. Принимает Результаты Работ. |
| **S** | **Support** (Соисполнитель) | Участник проекта, оказывающий поддержку в рамках своей компетенции для Ответственного. |
| **C** | **Consulted**  (Консультирующий) | Участник проекта, чье мнение (ресурсы) учитывается для создания Результатов проекта. Эксперты по предметным областям. |
| **I** | **Informed** (Информируемый) | Участник проекта, которого информируют о ходе выполнения Работ по созданию Результатов проекта. |

**Таблица 5.2. Перечень работ по проекту в разрезе ответственности сторон**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Блок работ** | **Наименование работ** | **Продолжи-**  **тельность, дней** | **Ответственный** | | **Результирующий документ/Комментарии** |
| **Исполнитель** | **Заказчик** |
| ***Этап 1. Подготовка проекта*** | | | | | | |
| Управление проектом | Подготовка Устава проекта | 30 дней | R | A, C | Устав проекта, в т.ч.:  - процедуры управления проектом, включая процедуру управления рисками проекта  - структуру проектной команды  - укрупненный план-график проекта |
| Формирование проектной команды со стороны Исполнителя | R | A, С |
| Формирование проектной команды со стороны Заказчика | I | R, A |
| Организация проектного офиса | C | R, A, С |
| Проведение стартового совещания по проекту | C | R, A |
| Формирование шаблонов и стандартов проекта | С | R, A | Шаблоны проектных документов  Стандарты моделирования бизнес-процессов предоставляются Заказчиком |
| Общее управление и координация работ по проекту | R | R, A | 1. Подготовка презентаций УК - ответственные в рамках своих задач; 2. Протоколы РМО - Заказчик, протоколы рабочих встреч консультанты по направлениям; 3. Ведение общего высокоуровневого плана работ -Заказчик, планирование на уровне групп - Руководители групп. |
| Эксплуатация и начальная поддержка | Разработка концепции организации Центра компетенции Заказчика | C | R, A, С | Концепция организации ЦК |
| Управление орг. изменениями | Выявление заинтересованных сторон Проекта | C | R, A, С | Реестр заинтересованных сторон |
| Формирование рекомендаций по обучению проектной команды Заказчика | R | A, С | Рекомендации по обучению проектной команды |
| Обучение проектной команды Заказчика | I | R, A |  |
| Подготовка дорожной карты по управлению организационными изменениями | R | A, С | Дорожная карта по управлению организационными изменениями |
| ***Этап 2. Проектирование*** | | | | | | |
| Управление проектом | Общее управление и координация работ по проекту | 60 дней | R | R, A |  |
| Процессы | Моделирование и описание целевых бизнес-процессов | R | A, C | Схемы целевых бизнес-процессов, Матрица контролей |
| Разработка реестр рисков и дизайн бизнес-контролей для целевых бизнес-процессов на основе лучших практик | R | A, C | Матрица рисков и бизнес-контролей |
| Предоставление методологической документации | C | R, A, I | Методологическая документация |
| Функционал | Выявление, уточнение и анализ функциональных требований к системе | R | A, C |  |
| Подготовка сценариев бизнес-операций для функционального тестирования системы | R | A, C | Сценарии бизнес-операций |
| Проектирование функциональной архитектуры решения | R | A, C | Функциональная архитектура решения |
| Подготовка и демонстрация прототипов решений на базе стандартного функционала и лучших практик, заложенных в концепции стандартной функциональности Системы | R | A, C | Протоколы демонстрации прототипа |
| Разработка проектных решений | R | A, С | Проектные решения |
| Формирование реестра функциональных разработок | R | A, С | Реестр разработок |
| Разработка концепции комплексного приемочного тестирования | R | A, С | Концепция комплексного приемочного тестирования |
| Роли и полномочия | Разработка концепции полномочий | R | A, С | Концепция полномочий |
| Формирование реестра ролей и полномочий | C | R, A, С | Реестр ролей и полномочий |
| Управление орг. изменениями | Разработка концепции обучения, оценка требуемой инфраструктуры для обучения | R | R, A, С | Концепция обучения, описывающая подход к обучению ключевых и конечных пользователей |
| Разработка плана коммуникации | R | R, A, С | План коммуникации |
| Мобилизация Ключевых пользователей и тренеров | I | R, A |  |
| НСИ и миграция данных | Разработка стратегии и подхода к миграции данных | R | A, C | Концепция миграции данных |
| Разработка регламентов ведения справочников и методик нормализации НСИ | R | A, C | Регламенты ведения справочников, Методики нормализации НСИ |
| Программно-аппаратная платформа | Поставка программного обеспечения и лицензий | R | A, C | Акт приема передачи оборудования и лицензий |
| Поставка оборудования для инсталляции системы разработки и системы тестирования | I | R, A |  |
| Описание системной и технической архитектуры решения | C | R, A | Документация, описывающая архитектуру решения |
| Техническая поддержка системы | I | R, А |  |
| Уточнение требований к производительности и разработка концепции нагрузочного тестирования | R | R, A, С | Концепция нагрузочного тестирования |
| Интеграция с внешними системами | Формирование реестра интеграционных потоков | R | R, A, С | Реестр интеграционных потоков |
| Подготовка сценариев тестирования интеграционных потоков | R | R, A | Сценарии тестирования интеграционных потоков |
| Проектирование интеграционных потоков | R | R, A | Спецификации интеграционных потоков |
| ***Этап 3. Реализация и тестирование*** | | | | | | |
| Управление проектом | Общее управление и координация работ по проекту | 100 дней | R | R, А, С |  |
| Процессы | Разработка регламентной документации | C | R, A, I | Регламентная документация |
| Разработка регламентной документации по ИТ | I | R, A, C | Регламентная документация по ИТ |
| Функционал | Детальное проектирование алгоритмов функциональных разработок (очередями итерационно) | R | A, R | Спецификация на функциональную разработку |
| Подготовка сценариев тестирования функциональных разработок (очередями итерационно) | R | A, R | Сценарии тестирования функциональных разработок |
| Реализация функциональных разработок (очередями итерационно) | R | A, R | Спецификация на функциональную разработку |
| Предварительное тестирование функциональных разработок (очередями итерационно) | C | R, А | Протоколы тестирования функциональных разработок |
| Настройка конфигурации системы | R | R, A | Описание настроек |
| Разработка пользовательских инструкций | C | R, A | Пользовательские инструкции |
| Разработка сценариев комплексного приемочного тестирования | С | R, A | План и Сценарии комплексного приемочного тестирования |
| Подготовка комплексного приемочного тестирования (интеграционный тест) | C | R, A, C |  |
| Проведение комплексного приемочного тестирования (интеграционный тест) | C | R, A, С | Протоколы комплексного приемочного тестирования (реестр замечаний) |
| Устранение критичных дефектов, выявленных в результате комплексного приемочного тестирования | R | A | Протоколы устранения дефектов |
| Роли и полномочия | Настройка ролей и полномочий | C | R, A |  |
| Тестирование ролей и полномочий | I | R, A, C |  |
| Интеграция с внешними системами | Детальное проектирование алгоритмов интеграционных разработок на стороне системы | R | A, R | Спецификация на интеграционную разработку |
| Подготовка сценариев тестирования интеграционных разработок на стороне системы | R | R, A, C | Сценарии тестирования интеграционных разработок |
| Реализация интеграционных разработок, настроек | R | R, A | Спецификация на интеграционную разработку |
| Тестирование интеграционных разработок | R | R, A | Протоколы тестирования интеграционных разработок |
| Доработки внешних систем, необходимые для реализации интеграционных потоков | I | R, A |  |
| Проведение комплексного тестирования интеграционных потоков | R | R, A | Протоколы тестирования интеграционных потоков |
| Устранение критичных дефектов на стороне Системы, выявленных в результате комплексного тестирования интеграционных потоков | R | A, R | Протоколы устранения дефектов |
| Устранение критичных дефектов на стороне внешних систем и интеграционной шины, выявленных в результате комплексного тестирования интеграционных потоков | I | R, A |  |
| Управление орг. изменениями | Реализация плана коммуникации | C | R, A |  |
| Оценка влияния изменений, оценка готовности к изменениям | C | R, A, C | Реестр основных рисков изменений, планы управления рисками |
| Планирование и выполнение мероприятий по минимизации рисков изменений | C | R, A, C |  |
| Проектирование изменений организационной структуры | I | R, A, C | Рекомендации по изменению организационной структуры |
| Актуализация должностных инструкций | I | R, A |
| Планирование и управление организационным переходом | I | R, A |
| Мобилизация Ключевых пользователей и тренеров | I | R, A |  |
| Разработка программы и план-графика обучения ключевых пользователей и тренеров | R | R, A | Программа и план-график обучения ключевых пользователей и тренеров |
| Организационная подготовка обучения ключевых пользователей и тренеров | I | R, A |  |
| Проведение обучения ключевых пользователей и тренеров | I | R, A | Протоколы обучения ключевых пользователей |
| Организационная подготовка обучения конечных пользователей | I | R, A |  |
| НСИ и миграция данных | Разработка шаблонов миграции данных | R | A, C | Шаблоны миграции |
| Разработка инструментов обогащения и загрузки данных на стороне системы | R | A, C |  |
| Разработка инструментов обогащения и выгрузки данных на стороне внешних систем | C | R, A |  |
| Подготовка данных для тестовой миграции, заполнение шаблонов миграции | C | R, A |  |
| Выполнение тестовой миграции НСИ и начальных данных | C | R, A | Протоколы тестовой миграции |
| Подготовка и нормализация НСИ | C | R, A, C |  |
| Инсталляция продуктивной системы | C | R, A | Протокол инсталляции продуктивной системы |
| Техническая поддержка системы | I | R, A |  |
| Нагрузочное тестирование наиболее критичных операций | C | R, A | Протокол нагрузочного тестирования |
| Эксплуатация и начальная поддержка | Разработка концепции запуска системы в эксплуатацию | R | R, A, C | Концепция запуска системы в эксплуатацию |
| Разработка плана-графика запуска системы в эксплуатацию | C | R, A, C | План-график запуска системы в эксплуатацию |
| ***Этап 4. Подготовка к запуску*** | | | | | | |
| Управление проектом | Общее управление и координация работ по проекту | 40 дней | R | R, A, C |  |
| Функционал | Устранение некритичных дефектов, выявленных в результате комплексного приемочного тестирования | R | R, A | Протоколы устранения дефектов |
| Интеграция с внешними системами | Устранение некритичных дефектов, выявленных в результате тестирования интеграционных потоков | R | R, A | Протоколы устранения дефектов |
| Управление орг. изменениями | Реализация плана коммуникации | C | R, A |  |
| Планирование и выполнение мероприятий по минимизации рисков изменений | C | R, A, C |  |
| Планирование и управление организационным переходом | I | R, A |  |
| Разработка программы и плана-графика обучения конечных пользователей | C | R, A | Программа и план-график обучения конечных пользователей |
| Организационная подготовка обучения конечных пользователей | I | R, A |  |
| Проведение обучения конечных пользователей | I | R, A | Протоколы обучения конечных пользователей |
| НСИ и миграция данных | Разработка плана-графика продуктивной миграции данных | C | R, A, C | План-график продуктивной миграции |
| Подготовка и нормализация НСИ | C | R, A |  |
| Подготовка данных для продуктивной миграции, заполнение шаблонов миграции | C | R, A |  |
| Выполнение продуктивной миграции НСИ | C | R, A | Протоколы продуктивной миграции |
| Эксплуатация и начальная поддержка | Организация сопровождения системы | C | R, A |  |
| Подготовка рабочих мест конечных пользователей | I | R, A |  |
| Выпуск приказа о запуске системы в эксплуатацию | I | R, A, C |  |
| Роли и полномочия | Создание записей пользователей и присвоение ролей и полномочий пользователям | I | R, A |  |
| Программно-аппаратная платформа | Техническая поддержка системы | I | R, A |  |
| ***Этап 5. Опытно-Промышленная эксплуатация и сопровождение*** | | | | | | |
| Управление проектом | Общее управление и координация работ по проекту | 40 дней | R | R, A, C |  |
| НСИ и миграция данных | Завершение продуктивной миграции НСИ | C | R, A | Протоколы продуктивной миграции |
| Выполнение продуктивной миграции начальных данных | C | R, A | Протоколы продуктивной миграции |
| Эксплуатация и начальная поддержка | Ввод и обработка реальных данных конечными пользователями | I | R, A, C |  |
| 1-ая линия поддержки. Прием обращение и инцидентов от пользователей. Решение обращений и типовых инцидентов | I | R, A |  |
| 2-ая линия поддержки. Решение нетиповых инцидентов, не требующих доработки ПО | I | R, A |  |
| 3-я линия поддержки. Решение нетиповых инцидентов, требующих доработки ПО, устранение дефектов | R | R, A | Протоколы устранения дефектов |
| Функционал | Актуализация и передача документации на решение | R | R, A | Актуализированная документация на решение |
| Приемка документации на решение | I | R, A |  |
| Подписание акта приема-передачи решения | I | R, A, C | Акт приема-передачи |
| Управление орг. изменениями | Реализация плана коммуникации | C | R, A |  |
| Планирование и выполнение мероприятий по минимизации рисков изменений | C | R, A, C |  |
| Планирование и управление организационным переходом | I | R, A |  |
| Оценка готовности конечных пользователей «после Запуска» | I | R, A |  |
| Подготовка материалов для дообучения конечных пользователей «после Запуска» | I | R, A |  |
| Сдача Системы в эксплуатацию | Подписание Акта выполненных работ с Заказчиком | I | R, A |  |
| Программно-аппаратная платформа | Техническая поддержка системы | R | R, A, C |  |

# 6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

Контроль и приемка Системы должны проводиться в соответствии с требованиями O‘z DSt 1986:2018 Информационная технология. Информационные системы. Стадии создания.

Контролю, испытаниям и приемке могут подвергаться как Система в целом, так и ее отдельные очереди (пусковые комплексы), подсистемы и отдельные задачи.

Для Системы устанавливают следующие основные виды испытаний:

* предварительные испытания;
* опытно-промышленная эксплуатация;
* промышленная эксплуатация.

Для планирования проведения всех видов испытаний разрабатываются документы «Программа и методика испытаний» соответствующих видов испытаний, которые должны устанавливать необходимый и достаточный объем и сроки испытаний, обеспечивающие заданную достоверность получаемых результатов. Программа и методика испытаний может разрабатываться на Систему в целом и (или) ее части. В качестве приложения могут включаться тесты (контрольные примеры).

При проведении испытаний Системы должно быть проверено и установлено соответствие Техническому заданию (ТЗ) на создание Системы следующего:

* качество выполнения комплексом программных и технических средств автоматизированных функций во всех режимах функционирования Системы;
* знание персоналом эксплуатационной документации и наличие у него навыков, необходимых для выполнения установленных функций во всех режимах функционирования Системы;
* полнота содержащихся в эксплуатационной документации указаний персоналу по выполнению им функций во всех режимах функционирования Системы;
* количественные и (или) качественные характеристики выполнения автоматических и автоматизированных функций Системы;
* другие свойства Системы, которым она должна соответствовать согласно требованиям Технического задания.

Испытания Системы проводятся на объекте Заказчика. По согласованию между Заказчиком и Поставщиком предварительные испытания и приемку программных средств Системы допускается проводить на технических средствах Поставщика при создании условий получения достоверных результатов испытаний.

Статус и состав приемочной комиссии определяется Заказчиком.

По результатам испытаний составляются протоколы проведения с перечнем замечаний и акты завершения испытаний, на основании которых принимается решение о возможности (или невозможности) перехода к следующему виду испытания или приемки Системы в постоянную эксплуатацию. Виды испытаний могут повторяться до устранения всех замечаний к Системе и соответствующей корректировки эксплуатационной документации.

Испытания Системы выполняются после проведения отладки и тестирования, поставляемых программных и технических средств Системы и представления Исполнителем соответствующих документов об их готовности к испытаниям, а также после ознакомления технических специалистов Заказчика с эксплуатационной документацией Системы.

В процессе эксплуатации и испытаний проводится проверка готовности отдельных частей, комплексов и задач Системы, а также предъявленной документации к функционированию в реальных условиях. Эксплуатация Системы и ее частей начинается с момента утверждения акта приемки в эксплуатацию.

## 6.1. Виды, объем и методы испытаний

На первом этапе проверка должна производиться согласно программе и методике предварительных испытаний опытного сегмента, разработанной Исполнителем работ и утвержденной Заказчиком.

На этапе опытной эксплуатации опытного сегмента должно производиться оценка полноты принятых проектных решений, и могут быть сформулированы требования по доработке до типового тиражируемого решения.

### 6.1.1. Предварительные испытания

Предварительные испытания Системы проводятся для определения ее работоспособности и решения вопроса о возможности передачи Системы в эксплуатацию.

Предварительные испытания проводятся на специально оборудованном стенде.

Укрупнённо, предварительные испытания включают 2 стадии:

### 6.1.2. Опытно-промышленная эксплуатация

Опытно-промышленная эксплуатация Системы проводится для определения правильности принятых проектных решений и построенной информационной модели, для определения степени соответствия функциональности Системы требованиям пользователей и степени удобства работы с пользовательским графическим интерфейсом.

Работы по организации эксплуатации включают:

* определение подразделений Заказчика, в которых будет проводиться эксплуатация;
* определение ответственных лиц Заказчика за проведение эксплуатации;
* определение сотрудников Заказчика участвующих в эксплуатации;
* определение предварительных требований к бумажным формам учетно-отчетной документации и утверждение временного регламента ведения учета в организациях, участвующих в эксплуатации;
* развертывание Системы;
* консультация сотрудников Заказчика правилам работы с Системой.

Информация, вводимая в Систему на этапе тестовой эксплуатации, должна быть удалена из хранилища данных при переходе к этапу эксплуатации и не может быть использована для формирования каких бы то ни было официальных отчетных форм.

### 6.1.3. Промышленная эксплуатация

Эксплуатация Системы, принятой в эксплуатацию в установленном порядке, в соответствие проекту и безопасность которой подтверждены испытаниями на стадии опытно-промышленной эксплуатации.

7. ТРЕБОВАНИЯ ПО СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ СИсТЕМЫ К ВВОДУ В ДЕЙСТВИЕ

К моменту проведения приемо-сдаточных испытаний все замечания к работе инженерных систем, обеспечивающих функционирование ЦОД, Заказчиком должны быть устранены.

К моменту окончания периода опытной эксплуатации обслуживающий персонал системы должен полностью овладеть практическими навыками работы с программно-техническим комплексом.

Для подготовки объекта к вводу Системы Заказчику необходимо выполнить следующие работы:

* внедрить и реализовать, совместно с организацией - исполнителем, план мероприятий по подготовке объекта модернизации к внедрению Системы (подсистем);
* внедрить, совместно с организацией-разработчиком, и утвердить дополнения и изменения в должностных инструкциях, определяющих работу персонала в условиях функционирования Системы;
* при необходимости внести изменения в организационную структуру предприятия с целью обеспечения необходимого количества сотрудников и технического персонала, обеспечивающего эксплуатацию Системы в соответствии с требованиями к персоналу, изложенными в разделе 4 настоящего документа;
* утвердить нормативные документы, разработанные в рамках проекта по внедрению Системы;
* приобрести, установить и протестировать технические средства, обеспечивающие функционирование Системы (подсистем), с проведением соответствующих мероприятий по защите технических средств от внешних воздействий и несанкционированного доступа;
* подготовить и оформить необходимую организационно-распорядительную документацию;
* обеспечить решение организационных вопросов по консультации и повышению квалификации сотрудников, которые будут работать с Системой;
* организовать изучение пользовательской документации Системы всеми отделами и подразделениями уполномоченного органа;
* обеспечить изучение пользователями эксплуатационной документации;
* подготовить нормативно-справочную и иную информацию и занести ее в соответствующие базы данных;
* провести контрольные испытания Системы (подсистем) совместно с исполнителем на рабочем месте администратора Системы.

Для подготовки объекта к вводу Системы организация-исполнитель обязана:

* разработать и реализовать совместно с организацией-заказчиком, план мероприятий по подготовке объекта к внедрению Системы (подсистем);
* разработать и обеспечить пользователей необходимой эксплуатационной документацией для работы с прикладным программным обеспечением Системы;
* провести контрольные испытания Системы (подсистем, задач) совместно с Заказчиком на рабочем месте администратора Системы;
* провести консультацию ключевых пользователей Системы.

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

## 8.1. Проектная документация

Перечень подлежащих разработке комплектов и видов документов, соответствующих требованиям O'z DSt 1985:2018, Исполнитель согласовывает с Заказчиком на основании протоколов.

Передаваемая Заказчику документация должна быть выполнена в бумажном и электронном виде на носителе.

Поставка Системы должна сопровождаться представлением комплекта документации следующего состава на русском языке:

* Руководства пользователя (в т.ч. должны быть описаны операции загрузки и ручного ввода данных, работа с отчетными формами, другими средствами отображения данных и др.);
* Руководство администратора (в т.ч. должны быть описаны порядок установки и настройки Системы - клиентской части и СУБД, порядок разграничения прав доступа и управления учетными записями пользователей, восстановления работоспособности ПО в случае сбоев, аудит и др.).
* Техническое описание произведенной кастомизации модулей Системы (инструкция по подготовке данных и настроек системы, инструкция по заполнению и ведению НСИ, инструкция по работе с объектами системы, инструкция по работе с отчетами, описание пользовательского интерфейса и прочие);
* Техническое описание настроенных интеграций;
* Инструкции по настройке бизнес-процессов для администратора и продвинутого бизнес-пользователя (инструменты администрирования, заведение пользователей в системе, распределение ролей пользователей, администрирование групп доступов, управление задачами системы и прочие).

9. Источники разработки

Источниками разработки настоящего технического задания являются, руководящие и методические материалы, научно-техническая литература.

1. O‘z DSt 1986:2018 Государственный стандарт Узбекистана. Информационная технология. Информационные системы. Стадии создания
2. O‘z DSt 1987:2018 Государственный стандарт Узбекистана «Информационная технология. Техническое задание на создание информационной системы».
3. O'z DSt 1985:2018 Виды, комплектность и обозначение доку­ментов при создании информационной системы (ИС),
4. Т 45-194:2007 Рекомендации по применению программно-аппаратных средств, обеспечивающих предотвращение актов незаконного проникновения в информационные системы.
5. O‘z DSt 2875:2014 Государственный стандарт Узбекистана. «Информационная технология. Требования к датацентрам. Инфраструктура и обеспечение информационной безопасности»,
6. RH 45-201:2011 Руководящий документ. Технические требования к зданиям и сооружениям для установки средств вычислительной техники».