УТДВЕРЖДАЮ
“Ўзсаноатқурилишбанк”
Заместитель председателя
правления АКБ
“Узпромсторбанк” А.Эргашев

_____

«___» _____ 2024 й

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На создание автоматизированной системы по борьбе против мошенничества (Antifraud)

на _____ листах
действует с _____

СОГЛАСОВАНО
Руководитель (должность,
наименование предприятия)

_____ _____
подпись имя, отчество, фамилия

_____
дата

Содержание

I. ОБЩАЯ ИНФОРМАЦИЯ

1.1. Полное наименование информационной системы и ее условное обозначение

Полное название системы – Создание автоматизированной системы по борьбе против мошенничества (Antifraud) в АКБ «Узпромстройбанк»

Условное обозначение системы – «Система мониторинга Антифрод».

1.2. Наименование и реквизиты заказчика и вендора информационной системы.

Организация-заказчик: АТБ « Узсаноаткурилишбанк ».

Адрес: город Ташкент, Юнусабадский район, улица Шахрисабз, дом 3

Телефон: 71-120-45-00

H/R: 19907000000000440600

МФО: 00440

ИНН: 200833707

ОКЭД: 64190

Регистрационный номер НДС: 326030011774

Сайт банка: https://sqb.uz

Почтовый адрес: info@sqb.uz

Вендор информационной системы определяется по результатам тендера (отбора).

1.3. Перечень документов в основу создания ИС

Положение о правилах выпуска и обращения банковских карт на территории Республики Узбекистан (регистрационный номер 3294, 03.04.2021 г.), Указ Президента Республики Узбекистан "О мерах по выводу сектора информационно-коммуникационных технологий на новый уровень в 2022-2023 годах" в целях обеспечения выполнение задач, поставленных в PQ-357 от 22 августа 2022 года.

1.4. Начало и окончание запланированной работы

После подписания соглашения с вендором реализации проекта первоначальный компонент планируется запустить на пробной основе в течение 60 рабочих дней.

1.5. Порядок оформления и представления результатов работ

Система выполняется в виде комплекса, работающего в установленные контрактом сроки.

После выполнения отдельных этапов и завершения работ в целом вендор представляет акт приемки работ, отражающий подробную информацию о работах, поэтапно выполняемых организацией.

Результаты работы оцениваются Рабочей группой, которая организована заказчиком.

Желательно, чтобы система работала с использованием технологии "REST API". Кроме того, при возникновении подозрений в отношении определенных проводимых транзакций система должна сформировать запрос на разъяснение от клиента в "контактный центр банка" и сделать вывод о результате запроса (в котором необходимо

отметить, какой оператор сделал вывод).

Для того чтобы система располагала данными о физическом лице, необходимо, чтобы доступ системы к базе данных строго контролировался. Лог-файлы не должны содержать информацию о банковской карте клиента в полном объеме.

После завершения работ на основании технического задания вендор представляет заказчику акт приемки. Датой подачи и приемки корпусов является дата, подписанная приемочной комиссией.

II. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1. Назначение системы

Система борьбы с мошенничеством имеет несколько этапов для обнаружения и предотвращения мошеннических действий. Система борьбы с мошенничеством выполняет несколько ключевых функций по обнаружению и предотвращению мошеннической деятельности. Основные функции системы:

- Обнаружение аномалий: система защиты от мошенничества анализирует данные и транзакции для обнаружения аномальных и необычных событий. Сюда входят необычные временные интервалы между транзакциями, необычные суммы переводов и другие аномалии, которые могут указывать на мошенническую деятельность.
- Сравнение с прошлыми транзакциями: система сравнивает текущие транзакции с историческими данными и прошлыми моделями поведения, чтобы выявить отклонения и несоответствия. Это помогает выявить необычные изменения в поведении клиентов или внутренних сотрудников.
- Мониторинг сигналов тревоги: система борьбы с мошенничеством отслеживает определенные сигналы тревоги и коэффициенты, которые могут указывать на мошенничество. Сюда входят попытки ложного входа в учетную запись, подозрительные IP-адреса, страны или устройства и другие индикаторы вредоносной активности.
- Анализ рисков: системы борьбы с мошенничеством оценивают уровень риска для каждой транзакции или действия на основе множества факторов, включая историю активности клиентов, объем транзакций, тип транзакции и другие параметры.
- Блокировка и предотвращение: если система обнаруживает высокий риск мошенничества, она может предпринять шаги по блокировке или задержке транзакции, потребовать дополнительной аутентификации, отправить оповещения администраторам или автоматически инициировать процессы расследования.
- Интеграция с другими системами. Системы защиты от мошенничества часто интегрируются с системами биометрической аутентификации MY-ID, АВТ и другими системами безопасности и мониторинга.
- Отчетность и анализ. Системы борьбы с мошенничеством предоставляют отчеты и аналитическую информацию, которые помогают компаниям понять масштаб проблемы и принять меры для повышения безопасности.

- Обучение и адаптация: системы по борьбе с мошенничеством автоматически учатся на новых данных и обновляют свои алгоритмы, чтобы адаптироваться к новым типам мошенничества.

2.2. Цели создания системы

При разработке программного обеспечения ставятся следующие цели:

- Автоматизация методов обнаружения, предотвращения и снижения мошеннических действий в банковской системе;
- использовать сбор данных, аналитические методы и алгоритмы для выявления транзакций или процессов, которые указывают на более высокий, чем обычно, уровень потенциального мошенничества;
- защита от мошенничества за счет быстрого выявления подозрительных событий, остановки определенных операций и обеспечения надежной и безопасной работы информационных систем;
- Программное обеспечение «Антифрод» для оповещения и защиты от потенциального мошенничества с помощью сложных алгоритмов обнаружения;
- программа автоматизирует и упрощает анализ данных в Банке, а также защищает от финансовых потерь и репутационных рисков.

III. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

3.1. Краткая информация о предмете информации или ссылки на документы, содержащие такую информацию.

В настоящее время стратегической целью банка является расширение клиентской базы, качественное улучшение банковских услуг и расширение спектра предлагаемых услуг.

На сегодняшний день процессы анализа практик, связанных со случаями мошенничества, и их выявления занимают длительное время. Это определяется анализом проведенных транзакций. Сейчас практика онлайн-мониторинга транзакций по банковским картам доступна не в полной мере.

Кроме того, отсутствие интегрированной системы, которая в настоящее время выполняет анализ, обобщающий все информационные системы банка, создает потребность во внедрении системы Антифрод.

3.2. Информация об условиях эксплуатации информационного объекта и характеристиках окружающей среды

Поскольку антифрод-система является внутренней системой, такие требования не предъявляются.

IV. ТРЕБОВАНИЯ К СИСТЕМЕ АНТИФРОД

4.1. Требования к системе в целом

4.1.1. Требования к структуре и функционированию ИС

4.1.1.1. Авторизация.

Программа разработана для сотрудников банка с целью улучшения системы мониторинга мошенничества. В этой программе разрабатываются правили для предотвращения случаев мошенничества, и при проведении операций, соответствующих этим правилам, программа выдает сигнал админу или автоматически блокирует транзакцию.

Пользователь должен пройти авторизацию для работы в системе. Пользователь входит в приложение через логин и пароль, созданные администратором для доступа к нему. Каждый пользователь создается администратором. Когда пользователь войдет в программу в первый раз, на его экране появится окно для замены пароля, созданного администратором.

Сложность пароля:

- Минимум одна заглавная буква
- Цыфры
- Знаки

Например “Asd123*-” и админ должен иметь права изменить сложность пароля.

Пользователь автоматически выйдет из системы, если в течение 30 минут после входа в систему не будет выполнено никаких операций. Ограничение по времени такой функции должно иметь свойство изменяться администратором

4.1.1.2. Сценарий и правила

В этом разделе формируется список существующих сценариев и правил.

Идентифицированные кейсы изучаются админом и переводятся в состояние инцидента. (Смотрите разделы кейсы и инцидент)

На верхней части окна должно быть иконка "ФИЛЬТР" который может вызывать сценарии на основе их ID, Домена, Периода, кейсов, идентификаторов и приоритета.

В верхней части списка должна быть иконка "Добавить" для добавления новых сценариев, "Заменить" для изменений и дополнений к введенным сценариям, "Удалить" для отмены регистрации существующих сценариев и "Выйти" из окон, чтобы вернуться в главное меню.

В течение периода проверки транзакции необходимо учитывать ip-адрес клиента, идентификационный номер устройства, тип транзакции, время регистрации или перерегистрации клиента.

4.1.1.3. Уведомления и текущее состояние

Раздел уведомления и текущего состояния будут состоять из списка подозрительных случаев, выявленных с помощью созданных сценариев и правил, а также их анализа. **(рисунок-18)**

4.1.1.4. Кейсы

В разделе кейсы формируется список выявленных случаев по сценарию и правилам. При нажатии на кейсы формируется вся информация об этом клиенте.

Этот список не является окончательным, администратор может ввести дополнительный тип события. Но типы принимаемых решений не ограничиваются этим списком. У администратора должна быть возможность вносить изменения в решения или принимать новое решение.

4.1.1.5. Инцидент

Информация об инцидентах формируется как в разделе “кейсы”. Разница в том, что, после анализирования кейсов обнаруживается фрод, этот кейс переводится в раздел инциденеты.

4.1.1.6. Лимиты и настройки

Раздел Настройки и лимитов позволяет вам устанавливать ограничения на операции. В случае превышения лимита можно сообщить или блокировать клиента и применить другие меры.

4.1.1.7. Черный список

Черный список может содержать номера телефонов, IP-адреса, имена хостов и другую информацию, подтвержденную при мошенничестве. Кроме того, в этом окне формируются направление, приоритет объекта, внесенного в черный список, количество кейсов ссылок на него и количество связанных с ним инсайдеров. Любые запросы с этих адресов будут обрабатываться и расследоваться как кейсы.

4.1.1.8. Белый список

В процессе, в котором работают сценарии, номера телефонов, IP-адреса, имена хостов, которые включены в белый список, не учитываются. Эта фильтрация выполняется перед любой обработкой в соответствии с любым правилом.

4.1.1.9. Специальные правила по списку

Отдельный раздел правил по спискам состоит из 2 подразделов: управление белыми списками и управление черными списками. Эти подразделы аналогичны разделам 4.1.1.7 и 4.1.1.8, в отличие от этого, в этом разделе также можно установить параметры **Ratelimit** и **Redirect** по белому и черному спискам.

4.1.1.10. Тестинг

В этом разделе все настройки для вновь добавленного сценария, лимита, черного и белого списка изначально будут запущены в тестовом режиме. При этом формируется информация об операциях, соответствующих включенному сценарию. Но в реальности клиенты не блокируются и сообщение не отправляется.

Как только сценарии будут использованы в тестовом режиме, они могут быть реализованы или отменены на практике.

4.1.1.11. Импорт / Экспорт

Раздел Импорт/ экспорт предназначен для загрузки доступных данных в программу или скачивания данных в программе. Для загрузки файлов поддерживаются все типы файлов (excel, json, xml, csv...).

4.1.1.12. Отчеты / Аудит

Отчеты / аудит состоят из подразделов "Уведомление", "кейсы и инциденты" и "визуализация".

Раздел "Уведомление", "кейсы и инциденты" отражают список, статистику и анализ случаев, определенных сценариями, правилами и инцидентом

4.1.1.13. Пользователь

В разделе "Пользователь" формируется информация о версии приложения "входы" для обычных пользователей, чтобы изменить свои личные данные, данные или пароль

Этот раздел позволяет администратору формировать свои собственные данные, как обычному пользователю, и управлять основными пользователями. Админ сможет прикреплять или удалять определенный модуль к пользователю, и новый пользовательский вид будет доступен только в пределах полномочий администратора

4.1.1.14. Системные настройки

Страница настроек системы позволяет настраивать сценарии, настраивать уведомления, создавать черные списки, белые списки, ограничения скорости, перенаправления, списки импорта/экспорта и автоматические списки, необходимые для успешной работы мониторинга мошенничества.

4.1.1.15. Внутреннее мошенничество

Что касается внутреннего мошенничества, то в головных системах банка формируется таблица о подозрительных действиях, совершаемых банковскими сотрудниками.

4.1.2. Требования к взаимодействию со сторонними информационными системами

Данное техническое задание предусматривает интеграцию до 10 информационных систем (в режиме реального времени).

- Обработка местных банковских карт (Uzcard, Humo)
- Обработка международных банковских карт (Visa, Mastercard, UPI и т.д.
- Автоматизированная банковская система (IABS)
- Мобильные приложения
- CRM
- Колл-центр
- и другие

В будущем должна быть возможность расширить этот список в случае необходимости.

Внешние системы, которые планируется интегрировать, могут иметь разные идентификации клиентов. Антифрод требует объединения данных клиентов из других систем с помощью уникального идентификатора.

Обмен данными в системе должен поддерживать все форматы.

Например:

- json
- xml
- yaml
- toml
- csv
- tsv

4.1.3. Требования к численности и квалификации пользователей системы и режиму их работы

№	Роль	Полномочие
1	Главный администратор	- предоставление администрирования; - изменение системных настроек; - настройка системных параметров; - установка минимальных совпадений; - налаживание обмена информацией с внешними источниками; - настройка внешних источников; - настройка сценариев.
2	Администратор	- изменение системных настроек; - настройка системных параметров; - установка минимальных совпадений; - налаживание обмена информацией с внешними источниками; - настройка внешних источников; - настройка сценариев.
3	Пользователь	- Onboarding решение; - Pre-screening клиента/контрагента; -screening клиента/контрагента; - матрица рисков, склонность к риску, факторы риска, а также просмотр сценариев запуска, сравнение клиента с факторами риска; - ручной ввод данных в профили клиентов; - приостановка/остановка операций клиента; - предоставление отчетов о клиентах другим подсистемам об их профиле.
4	Наблюдатель (только для чтения)	отслеживает выполняемые задачи и функции пользователя, формирует необходимые отчеты и информацию.

4.1.4. Показатели назначения

Система должна обеспечивать производительность не менее 10 сотрудников одновременно в течение рабочего процесса. Система не должна влиять на скорость выполнения транзакций других систем, которые планируется интегрировать.

Ниже приведены "временные" показатели системы:

1. Переход с одной страницы на другую не должен превышать 0,2-1 секунды.

2. Системе должно потребоваться не более 5-10 секунд для формирования больших объемов данных.

4.1.5. Требования к надёжности

Программно-аппаратный комплекс системы должен работать круглосуточно, в непрерывном режиме, за исключением следующих случаев:

- профилактические работы;
- восстановление данных;
- другие случие, требующие обновления версий программного обеспечения и вынужденные отключение технических средств;

Отказ одной из групп не должен приводить к прекращению деятельности остальных частей группы, то есть должна быть возможность выполнять функции всех оставшихся групп одновременно.

Все прикладные системы должны работать в режиме высокой надежности.

Запланированное отключение или сбой информационного ресурса системы не должны приводить к сбою программного обеспечения.

Неправильные действия, выполняемые пользователями, не должны приводить систему к аварийной ситуации.

Необходимо свести к минимуму ошибки технического персонала путем четкого установления прав доступа к системе, а также записывать выполняемые в системе действия в журнал (в log файлах).

Проектом не предусмотрена закупка или техническое обслуживание серверного оборудования. Выделение ресурсов для реализации проекта, а также поддержка серверного оборудования осуществляется департаментом Информационных технологий банка.

Предъявляются требования к надежности электроснабжения:

- система должна иметь функцию информирования администратора о том, что она перешла на автономное питание;
- система должна быть оснащена средствами автоматического отключения операционной системы в случае, если перерыв в подаче электроэнергии превышает 15 минут;
- активное сетевое оборудование должно быть снабжено постоянным источником питания.
- резервирование данных должно быть полностью завершено вовремя.

Надежность программного обеспечения под-систем обеспечивается за счет следующих факторов:

- общее программное обеспечение, предоставляемое поставщиком, и надежность программного обеспечения, предоставляемого в рамках технической миссии;
- осуществление мер по временному обходу (отладка), поиску и устранению системных ошибок.
- запись данных и ошибок в под-системах для будущих изменений настроек.

Надежность системы обеспечивается за счет:

- внедрения программного обеспечения, позволяющего сохранять информацию в системе в случаях, когда происходит нарушение стабильности работы системы или другие сбои в работе;
- выбор отказоустойчивого оборудования и его конструктивного резерва;
- улучшенное резервное копирование наиболее важных узлов системы, к которым относятся серверы баз данных, серверы приложений, сетевые компоненты, оборудование, обеспечивающее соединения в подсистемах, а также подключение каждого пользователя подсистемы к серверам база данных;
- использование источников бесперебойного питания;
- подбор топологии телекоммуникационных и локальных компьютерных сетей, обеспечивающих возможность маршрутизации информационных потоков;

- высококвалифицированный персонал, а также правильная организация работы;
- организация технического обслуживания с использованием современных методов диагностики и инструментов;
- использование только лицензионного программного обеспечения различных модификаций;
- тестирование всех модулей под-систем;
- наличие полных комплектов технической документации, обеспечивающих надежную работу всех модулей под-систем;
- информация, хранящаяся субъектом в других информационных системах, работающих совместно с системой мониторинга антифрод, осуществляется посредством активности модулей под-системы, которые должны быть уничтожены, повреждены или утеряны в результате взаимодействия.
- программно-аппаратные комплексы системы должны обладать свойством восстановления системы при возникновении сбоев.

4.1.6. Требования к безопасности

Необходимый уровень безопасности должен быть обеспечен банком путем строгого соблюдения правил эксплуатации и технического обслуживания оборудования, рекомендованных вендором и программистами.

Для входа в систему пользователю всегда необходимо пройти авторизацию. Логин и пароль для пользователя создаются администратором, и в случае первой попытки входа в систему пользователю открывается окно для смены пароля, и пользователь вводит свой пароль. При входе в систему количество неправильных вводов пароля будет ограничено. Учетной записи присваивается блокировка, если пользователь неправильно вводит пароль более 3 раз.

Пользователь автоматически выйдет из системы, если в течение 30 минут после входа в систему не будет выполнено ни одной операций.

Обмен данными между сервером и пользователем осуществляется по локальной сети.

Каждое поле (input), в которое вводится информация в системе, будет иметь свой собственный тип данных, и поле не будет получать данные любого типа, отличного от этого типа. При вводе неверной информации о типе пользователю возвращается "flash-message ".

Установка и настройка системы, а также воздействие на нее обслуживающего персонала банка посредством опасных показателей электрического тока, электромагнитных полей, акустического шума, вибрации и т.д. не должны быть. В этом случае общая безопасность сотрудников обеспечивается банком.

Технические средства должны обеспечивать защиту обслуживающего персонала от поражения электрическим током в соответствии с требованиями государственного стандарта.

Все внешние элементы (кабели) энергоемких технических средств системы должны иметь защиту от случайного прикосновения, а сами технические средства должны быть установлены в соответствии с установленными стандартами;

Безопасность помещений, где расположены технические средства комплекса, должна обеспечиваться соответствующей рабочей группой, которая отвечает как за работу системы в целом, так и за выполнение данного технического задания, и эта

рабочая группа предоставляется банком.

Система должна быть защищена от получения информации от незарегистрированных пользователей. Она также должна быть надлежащим образом распределена среди пользователей системы и администраторам. Следует предусмотреть предоставление пользователю доступа к определенному разделу интерфейса, а также осуществлять управление системой в установленном порядке.

Требования безопасности

Система должна обеспечивать информационную безопасность во всех чрезвычайных ситуациях.

Как ситуацию, характеризующуюся аварийной ситуацией в системе, следует понимать следующее:

- Полное или частичное прекращение функциональных задач;
- Положение нормальной работы системы или ее основных частей;
- Неподтверждение полномочий, приведшее к нарушению полноты и точности передачи информации;
- Несвоевременное получение пользователями запрошенной информации и ее недостаточность;
- Полная или частичная потеря информации;
- Незаконный доступ к системе, умышленное нарушение или уничтожение информации;
- Необходимо убедиться, что система защищена в рамках криптографических требований версии PCI DSS^4.0 в связи с использованием данных о банковских пластиковых карт.

В случае потери данных из-за различных событий данные должны быть восстановлены из резервной копии, предоставленной клиентом.

Восстановление данных должно соответствовать следующим требованиям:

- В случае аварии или сбоя во время выполнения пользовательских назначений база данных должна быть восстановлена во время последней завершенной транзакции.

4.1.7. Требования к эргономике и технической эстетике

Интерфейс не должен быть рассчитан на использование манипулятора одного типа "мышь", то есть управление должно осуществляться с помощью набора экранных меню, кнопок, символов и аналогичных элементов, а также должна быть доступна возможность использования "горячие клавиши".

Интерфейс системы должен быть удобным для пользователя и понятным.

Компьютер должен обеспечивать удобный и точный интерфейс для работы со всеми функциями, разработанными в соответствии с современной эргономикой и современным дизайном:

- формы интерфейса и меню должны быть простыми и понятными, элементи меню должны быть сгруппированы в соответствии с функциональными задачами и типом данных, каждый элемент меню должен соответствовать только одной выполненной функции;
- дизайн экранных форм должен быть стандартным, и если невозможно решить проблему со стандартной формой, должна быть возможность изменить форму;

- если в действиях пользователя есть ошибки, должно быть выдано уведомление, содержащее достаточно информации, чтобы представить причины ошибки.
- эргономичные элементы должны быть одинаковыми для всех компонентов и модулей;
- пользовательский интерфейс должен помочь снизить вероятность совершения ими случайных неправильных действий;
- интерфейс должен быть оптимизирован для выполнения обычных и часто используемых программных операций.
- компьютерный интерфейс должен обеспечивать отображение на экране функций, соответствующих роли пользователя;
- Система должна требовать подтверждение для выполнения важных операций. Пользовательский интерфейс должен содержать информативное описание ошибок. Система должна обеспечивать удобные механизмы, которые устанавливаются для мониторинга, когда пользователь вводит значения полей.

4.1.8. Требование к патенту и лицензии

Система должна быть внедрена в соответствии с требованиями действующего законодательства о патентах и нормативных документов.

Вендор обязан предоставить доказательства лицензионного соглашения или подтверждающие патентные права внедряемой системы.

Лицензия должна быть бессрочной. Если лицензия ограничена, должна быть доступна возможность изменить ее на неограниченную, а стоимость неограниченной лицензии не должна превышать 130% от первоначальной цены лицензии.

4.1.9. Требования к стандартизации и унификации

При запуске системы необходимо придерживаться принципов унификации.

Данные, загружаемые и обрабатываемые в систему, должны основываться на принципе единообразия, непротиворечивости, единообразного включения, полноты и надежности.

Все процессы должны работать в инфраструктуре TCP/IP;

Взаимодействие клиентских устройств с серверной частью системы должно осуществляться в режиме мультиплексирования TCP/IP, определенном документами RFC, в соответствии со стандартными протоколами обмена.

Система должна соответствовать следующим показателям, определяющим необходимый уровень использования стандартных, унифицированных методов для реализации функций (задач), предоставляемых программным обеспечением:

- CSV, DOC, XLS, PDF должны поддерживать форматы электронных документов при передачи данных;
- Должна быть возможность преобразования данных в формат HTML без использования отдельной программы;

4.2. Требования к функциям и задачам, выполняемым ИС

4.2.1. Авторизация

4.2.1.1. Вход

Доступ к программе осуществляется через логин и пароль, созданные пользователем

(сотрудниками банка). При первом входе пользователя в программу нажимается кнопка регистрации и вводятся данные пользователя.

Учетная запись пользователя создается с помощью администратора. Для ввода нового пользователя заполняется следующая форма.(Рисунок 1)

риснок 1

Технические требования

1. В поле ввода имени пользователя (Пример входа: И.Алиев) можно ввести до 50 букв «латинского» алфавита. Цифры и другие специальные символы не допускаются.
2. Пароль должен содержать хотя бы одну заглавную букву. Пароль должен содержать цифры, буквы и символы (/,*,-,+). Должно быть не менее 8 символов. Если какое-либо из этих условий не выполнено, должен появиться текст с рекомендацией установить другой пароль. Пример пароля: Asd123*-
3. Пароли должны быть хешированы (SHA1, SHA256) в базе антифрод-системы;
4. Должна быть возможность выполнить глобальные настройки политики паролей;
5. Фамилия – должно содержать до 50 букв «латинского» алфавита. Вводить цифры должно быть невозможно.
6. Имя – можно ввести максимум 50 букв «латинского» алфавита. Не должно быть возможности вводить цифры и другие специальные символы.
7. Имя отца – до 50 букв «латинского» алфавита. Вводить цифры должно быть невозможно.
8. PINFL – необходимо ввести 14 цифр. Не должно быть возможности ввести более или менее 14 цифр. Не должно быть возможности вводить символы, кроме цифр (буквы, специальные символы, пробелы и т. д.).

9. Процесс биоверификации должен предусматривать возможность сравнения данных с системой IABS через систему ONEID, либо добавление ролей на основе полномочий сотрудников этой службы.

Номер телефона – вводятся номера, используемые только на территории Республики Узбекистан *(второстепеннная аутентификация предусмотрена в будущем)* . Не должно быть возможности ввести другие цифры.

Пользователь входит в программу, заполнив следующую форму (*рис. 2*)

Рисунок 2

Пользователь должен обновить пароль во время входа в программу, причем обновление пароля обязательно каждый месяц. Если пользователь забудет логин или пароль, он обратится к администратору и они сбросят пароль.

4.2.1.2. Изменить пароль

рисунок 3

Технические требования

1. В поле ввода имени пользователя (Логин) вводится до 50 букв «латинского» алфавита. Числа вводить невозможно.
2. Пароль должен содержать хотя бы одну заглавную букву. Пароль должен содержать цифры, буквы и символы (/,*,-,+). Должно быть не менее 8 символов. Если какое-либо из этих условий не выполнено, должен появиться текст с рекомендацией установить другой пароль.

Пример пароля: Asd123*-

3. Пароли должны быть хешированы (SHA1, SHA256) в базе антифрод-системы;
4. Должна быть возможность выполнить глобальные настройки политики паролей;

4.2.2. Сценарий и правила

4.2.2.1. Сценарии

При входе в окно откроется экран , как показано на **рисунке 13** .

В этом окне появится список доступных сценариев. Список сценариев будет состоять из следующей информации:

- Структура сценариев (последовательность, формула);
- К какому направлению относятся сценарии;
- Приоритет (уровень важности);
- Кейсы (созданные сценарии и ситуации, подпадающие под правила);
- Инциденты (случаи, когда дела были расследованы и выявлены реальные случаи мошенничества).

Выявленные случаи расследуются сотрудником до статуса **«Инцидент».** будет проведено. (См. раздел «Кейсы и Инциденты»).

Вверху находится окно «Фильтр», в котором можно получить сценарии по ID, направлению, периоду, кейсу, инцидентам и приоритету.

Вверху списка расположены окна «Добавить» для добавления новых сценариев, «Заменить» для внесения изменений и дополнений в существующие сценарии, «Удалить» для отмены регистрации существующих сценариев и «Выход» для возврата в главное меню.

При проверке транзакций необходимо учитывать IP-адрес клиента, идентификационный номер устройства, тип транзакции, время регистрации или перерегистрации клиента.

При создание черного списка IP- адресов надо учитивать тип списка (Анонимайзер, Ботнет и т.д.)

Создание возможности проверки между транзакциями на сегодняшний день (из истории) с помощью нового правила, созданного для выявления подозрительных транзакций в системе.

Технические требования

1. Данные необходимо ввести в поле «Период» в фильтре в формате (ДД.ММ.ГГГГ ЧЧ:ММ). Пример: 12.01.2023 22:15
2. В поле «Кейсы» данные вносятся только в виде цифр.
3. Вносить информацию в поле «ID» только в виде числа.
4. Данные вводятся в поле поля путем выбора одного из следующих полей:
   - Мобильное приложение для ФЛ;
   - Интернет-банкинг для ФЛ;
   - Мобильное приложение для ЮЛ;
   - Интернет-банкинг для ЮЛ;
   - программа для ЮЛ «Банк-Клиент»;

- Узкард;
- Хумо;
- Way4;
- ИАБС: депозит ФЛ;
- ИАБС: МДП для ФЛ ;
- ИАБС: ПОВ для ФЛ.

5. Информация в поле инцидента вводится только в виде цифр. Это число означает количество инцидентов, обнаруженных за определенный период времени.

6. Ввод поле приоритета только в виде цифр.

7. Для создания нового сценария при нажатии кнопки «Добавить» должен автоматически открыться подраздел «Сценарии» раздела **«Настройки системы» , как показано на рисунке 13.1 .**

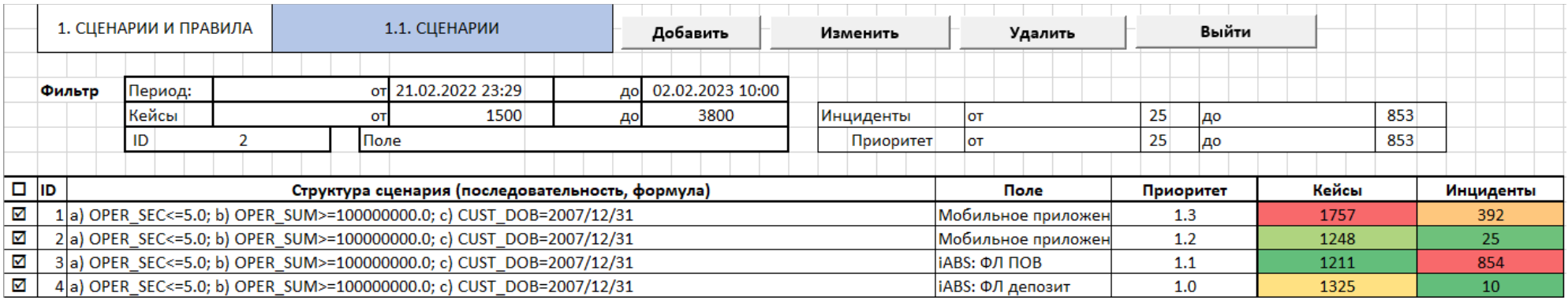
8. Сценарии, запущенные в реальной программе, удалять нельзя.

9. Внесите изменения в существующий сценарий , выбрав сценарий для задания и нажав кнопку «Заменить». Старый сценарий должен стать «серым» и автоматически стать «неактивным». Измененный сценарий должен появиться как новый сценарий.

10. Система должно спросить, запускать ли вновь добавленный сценарий в тестовом режиме или напрямую в режиме реального времени. После выбора одной из этих анкет необходимо еще раз запросить подтверждение выбранного режима. После нажатия кнопки «ОК» сценарий должен запуститься.

11. Значок окончательного удаления сценария реального времени не должен быть доступен. При выборе сценария и нажатии кнопки «Удалить» сценарий должен стать серым и автоматически переключиться на «неактивный».

Рисунок 13



☐	ID	Структура сценария (последовательность, формула)	Поле	Приоритет	Кейсы	Инциденты
☑	1	a) OPER_SEC<=5.0; b) OPER_SUM>=100000000.0; c) CUST_DOB=2007/12/31	Мобильное приложен	1.3	1757	392
☑	2	a) OPER_SEC<=5.0; b) OPER_SUM>=100000000.0; c) CUST_DOB=2007/12/31	Мобильное приложен	1.2	1248	25
☑	3	a) OPER_SEC<=5.0; b) OPER_SUM>=100000000.0; c) CUST_DOB=2007/12/31	iABS: ФЛ ПОВ	1.1	1211	854
☑	4	a) OPER_SEC<=5.0; b) OPER_SUM>=100000000.0; c) CUST_DOB=2007/12/31	iABS: ФЛ депозит	1.0	1325	10

Рисунок 13.1

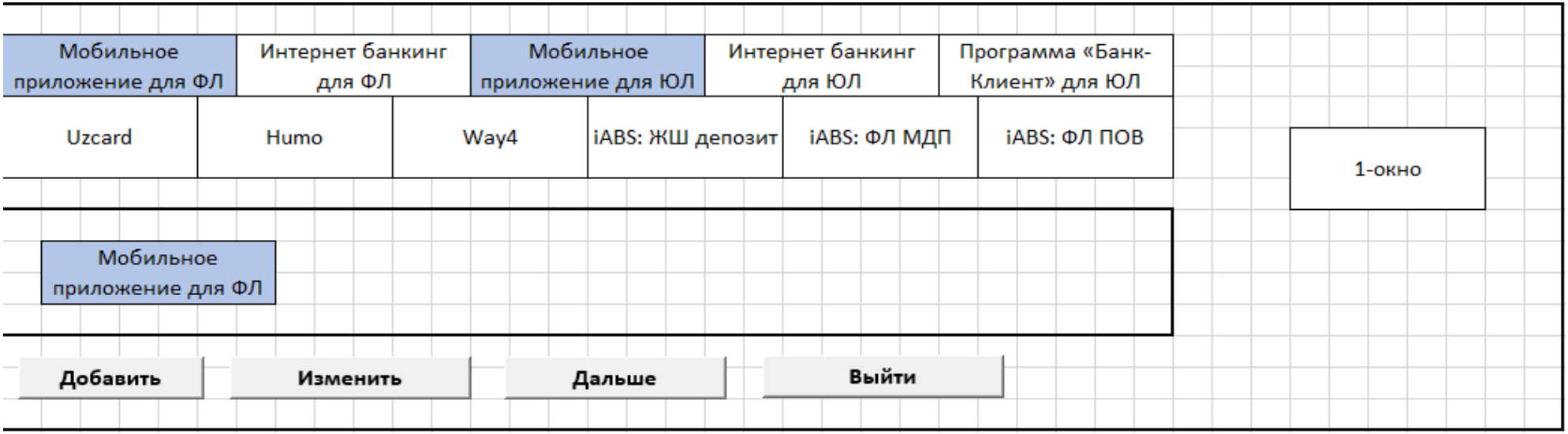


Рисунок 14

1. СЦЕНАРИИ И ПРАВИЛА	1.2. ПРАВИЛА

Фильтр | Период | от 21.02.2022 23:29 | до 02.02.2023 10:00

Тип точки | Чегара | 30% дан | 4000 гача

Огроничен | от 30% | дл 4000 | Количество пункта | от 250 | до 500

Добавить **Изменить** **Добавить**

Тип точки / Point Type	Огроничение	Количество пункта	Предел сходства	введеные дата и время
Динамик	30%		>130	02.02.2023 9:36
Статик	4000	250		02.02.2023 9:36

Фильтр | Тип точки | | Предел сходства | от 30% | до 4000

Адрес перенаправления | 30% | 30% | до 4000

Добавить **Добавить** **Добавить**

Тип	Предел сходства	Адрес перенаправления
от хоста	100%	172.1.10.25
от телефон номера	50%	+998901234567
от хоста	70%	172.2.15.15
от телефон номера	80%	+74951234567

от хоста	172.1.10.25
от телефон номера	+998901234567
от хоста	172.2.15.15
от телефон номера	+74951234567

4.2.2.2. Правила

При входе в окно откроется экран как показано на **рисунке 14** . В этом разделе изложены общие правила для Redirect и Ratelimit.

Ratelimit — это ограничение, налагаемое на поток трафика. Типы транспортных потоков делятся на 2 типа: статические и динамические. Динамический предел указывается в процентах, а предел статических волн — в виде конкретного числа.

В верхней части этого раздела находится «Фильтр», который позволяет фильтровать правила по типу баллов, определенному периоду, лимиту и сумме баллов.

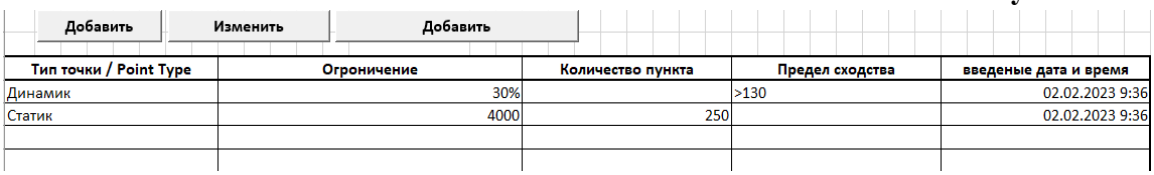
Также внизу окна формируются общие правила для подозрительных IP-адресов и номеров телефонов относительно Redirect. В этой таблице показана информация о типе операции, степени перекрытия, а также IP-адресе или номере телефона.

Тип транзакции состоит из 4 частей: от хоста к хосту, от номера телефона к номеру телефона.

Технические требования

1. В «Фильтре» по Ratelimit:
   - «Период» необходимо вводить в формате (ДД.ММ.ГГГГ ЧЧ:ММ). Образец: 01.12.2023 22:15;
   - «Тип точки» — выбирается один из Динамического и Статического;
   - «Лимит» - если для типа потока выбран Динамический лимит его необходимо ввести в %;
   - «Лимит» - следует вводить цифрами если лимит выбран для типа потока «Статический»;
   - «Количество баллов» — указывается цифрами;
2. В нижней части фильтра формируются следующие правила по Ratelimit. (*Рисунок 15*)

Рисунок 15



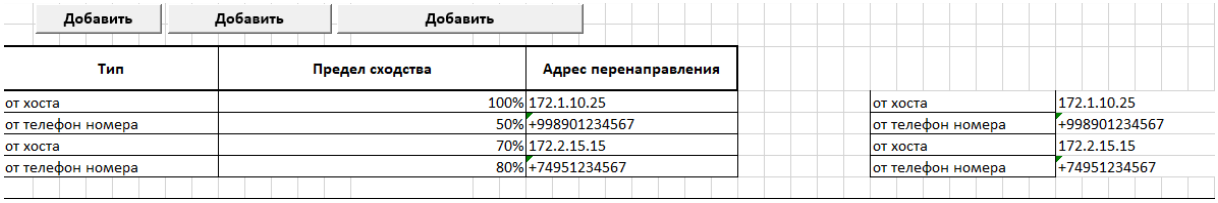
Тип точки / Point Type	Огроничение	Количество пункта	Предел сходства	введеные дата и время
Динамик	30%		>130	02.02.2023 9:36
Статик	4000	250		02.02.2023 9:36

   - Когда необходимо ввести новое правило, нажимается кнопка «Добавить» и заполняются Тип точки, Ограничение, Количество пункта, Предел сходства.
   - «Тип точки» — выбирается один из Динамического и Статического;
   - « Ограничение » - если для типа потока Динамический выбран лимит, его необходимо ввести в %;
   - «Лимит» - следует вводить цифрами, если лимит выбран для типа потока «Статический»;
   - вводится числа со знаками больше (>), меньше (<) и равно (=). Пример: >120, <200, =555.
   - Введенные дата и время должны генерироваться автоматически при запуске правила;

- При введении нового Правила старое должно автоматически стать «неактивным» по тем же правилам;
- При нажатии кнопки «Заменить» данные, введенные по существующим правилам, будут сохранены, а изменения будут внесены по необходимым критериям;
- Старое правило не следует удалять после активации изменения. Старое правило должно автоматически стать «неактивным», и должно начаться новое правило.
- При нажатии кнопки «Отключить» правило должно перейти в состояние «неактивно», но не должно быть удалено.
- Должна быть создана история любых изменений и обновлений.

3. В «Фильтре» Redirect :
   - Выбирается «Тип точки» — от хоста, номер телефона— от, к хосту, номер телефона — к;
   - «Передел сходства» – поле заполняется в %;
   - «Адрес перенаправления» — необходимо ввести номера телефонов, IP-адреса;
4. В нижней части фильтра правила введенные на Redirect, формируются как показано ниже. (*Рисунок 16*)

Рисунок 16



- Когда необходимо ввести новое правило, нажимается кнопку «Добавить» и заполните Тип точки, Сумма сходства и Адрес перенаправления;
- При нажатии кнопки «Заменить» данные, введенные по существующим правилам, будут сохранены, а изменения будут внесены по необходимым критериям;
- Старое правило не следует удалять после активации изменения. Старое правило должно автоматически стать «неактивным», и должно начаться новое правило.
- При нажатии кнопки «Отключить» правило должно перейти в состояние «неактивно», но не должно быть удалено.
- Должна быть создана история любых изменений и обновлений.

4.2.3. Уведомления и текущее состояние

«Уведомления и текущая состояние» будет состоять из списка подозрительные случаи, выявленных по созданным сценариям, и их анализа.

В верхней части этого окна анализ мониторинга подозрительных случаев за последний час отображается в следующей форме. (*Рисунок 17*)

Рисунок 17

Список подозрительных случаев, выявленных по созданным сценариям, формируется в виде **рисунка 18** .

1. ID – состоит из латинских букв и цифр, присвоенных уведомлениям программой;
2. Отметку времени необходимо вводить в формате (ДД.ММ.ГГГГ ЧЧ:ММ:СС). Пример: 12.01.2023 22:15:20;
3. Оценка – серьезность практик оценивается по 1-10 баллам;
4. Уровень – баллы от 1 до 10 оцениваются по следующим критериям:
    1. Мошенничество не выявлено
    2. Небольшое событие
    3. Среднее событие
    4. Большое событие
    5. Маленький серьезный кейс
    6. Серьезный случай
    7. Очень серьезный случай
    8. Небольшая критическая проблема
    9. Средняя критическая проблема
    10. Очень критическая проблема
5. В этом столбце (Мобильный?) указано «Да» или «Нет».
6. Процесс – в этом столбце выбирается один из следующих вариантов:
    - Мобильное приложение для ФЛ;
    - Интернет-банкинг для ФЛ;
    - Мобильное приложение для ЮЛ;
    - Интернет-банкинг для ЮЛ;
    - программа для ЮЛ «Банк-Клиент»;
    - Узкард;
    - Хумо;
    - Way4;

- ИАБС: депозит ФЛ;
- ИАБС: МДП для ФЛ ;
- ИАБС: ПОВ для ФЛ.

7. Имя клиента - Ф.И.О клиента;
8. Уникальный – 8 цифр, начиная с 10-й цифры номера банковского счета клиента;
9. Телефон – последовательность цифр, начинающаяся со знака +;
10. Тип события – введите одно из следующих:
    - Черный список;
    - Ratelimit;
    - Redirect;
    - Необычный вход;
    - Не авторизованный доступ;
    - Аномальний оборот;
    - Дропы;
    - Превышение лимита;
    - Неожидая активность спящего счета

Этот список не является исчерпывающим. Администратор может добавить дополнительные типы событий.

11. Остановлен? – Состоит из Да или Нет.
12. Решение. Типы решений, которые могут быть приняты в отношении операций:
    - Останавливаться
    - Остановитесь и сообщите
    - Уведомление
    - Остановитесь и поищите похожее.
    - Глобальная остановка
    - Глобальная остановка и отчет
    - Перевод к кейсам
    - Черный список
    - Перевод к инцидентам

Но типы принимаемых решений этим списком не ограничиваются. Администратор должен иметь возможность менять решения или принимать новые решения.

Внизу этого окна должна быть кнопка для перехода к следующим разделам: «Случаи» и «Инциденты».

рисунок 18

2. УВЕДОМЛЕНИЯ И ТЕКУЩИЙ СТАТУС

Выйти

Мониторинг в последний час

Просмотрен: 120 Сигналы: 120 Инциденты: 5

Количество подозрительных звонков за сегодня: 12

Оценка	
1	Мошенничество не выявлено
2	Небольшое мероприятие
3	Среднее событие
4	Большое событие
5	Маленький серьезный случай
6	Серьезный случай
7	Очень серьезный случай
8	Небольшая критическая проблема
9	Средняя критическая проблема
10	Очень критическая проблема

Решение
Останавливать
Останавливать и сообщить
Сообщить
Остановить и искать подобные
Глобалное остмановktybt
Глобально остановить и сообщить
Передача в кейсах
Передача в черный список
Передача в инцидентах

ПОСМОТРЕТЬ

РЕШЕНИЕ ПО ВЫБРАННЫМ

Последние уведомления

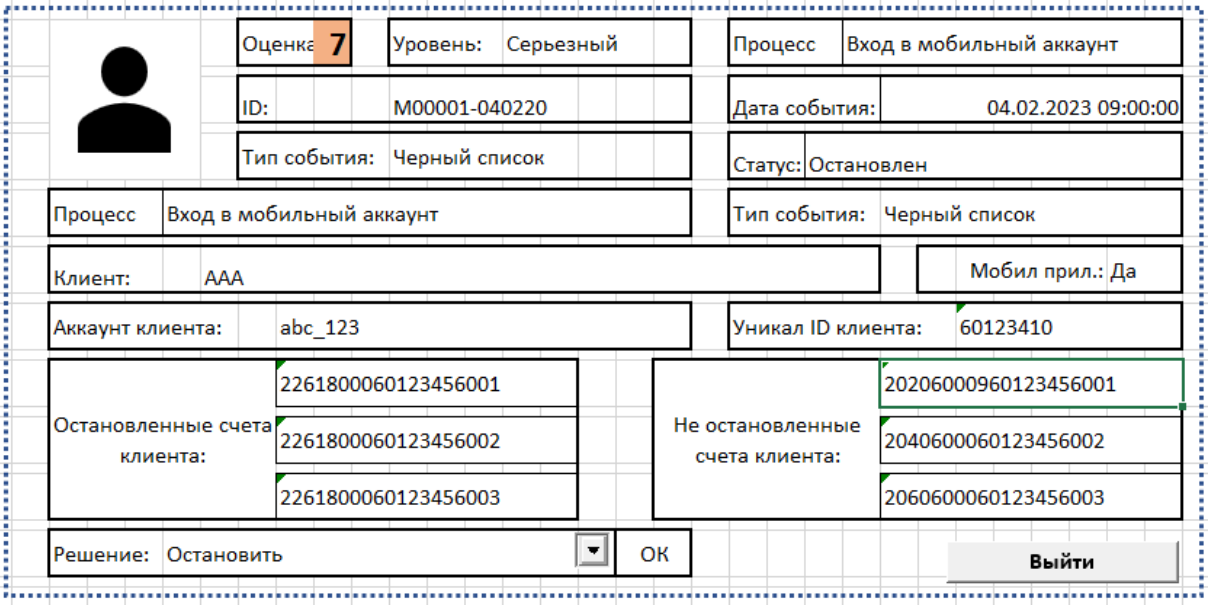
☐	ID	Дата	Оценка	Уровень	Мобильность	Процесс	Имя клиента	Уникал	Телефон	Тип события	Остановлен	Решение	☐
☑	M00001-040220	04.02.2023 09:00:00	7	Серьезный слу	да	Вход в мобильное устрой	AAA	60123410	+749501234567	Черный список	Да	Остановить	☐
☑	M00001-040221	04.02.2023 09:00:01	8	Небольшая кр	нет	Денежный перевод	ББВ	60123421	+998941234567	Ratelimit	Нет	Остановить и сообщить	☑
☑	M00001-040222	04.02.2023 09:00:02	9	Средняя крити	да	МДП	ВВВ	60123432	+749501234567	Redirect	Да	Остановить	☐
☑	M00001-040223	04.02.2023 09:00:03	10	Очень критиче	да	Мобильное передача	ГГГ	60123443	+998941234567	Черный список	Да	Сообщить	☐
☑	M00001-040224	04.02.2023 09:00:04	1	Мошенничест	нет	депозит	ДДД	60123454	+749501234567	Необычный вход	Нет	Остановить	☑
☑	M00001-040225	04.02.2023 09:00:05	2	Небольшое ме	нет	Банковская карта	ЖЖЖ	60123465	+998941234567	Не разрешенный вход	Нет	Остановить и сообщить	☑
☑	M00001-040226	04.02.2023 09:00:06	3	Среднее собы	нет	Внутренный фрод	333	60123476	+749501234567	Необычный оборот	Да	Остановить	☐
☑	M00001-040227	04.02.2023 09:00:07	4	Большое собы	нет	Внутренный фрод	ЕЕЕ	60123487	+998941234567	Распределенный оборот	Нет	Сообщить	☐
☑	M00001-040228	04.02.2023 09:00:08	5	Маленький се	нет	Внутренный фрод	ЁЁЁ	60123498	+749501234567	Превышение лимита	Нет	Остановить	☑
☑	M00001-040229	04.02.2023 09:00:09	6	Серьезный слу	нет	Внутренный фрод	ИИИ	60123409	+998941234567	Необычный вход	Да	Остановить и сообщить	☐

ПЕРЕХОД К КЕЙСАМ

ПЕРЕХОД К ИНЦИДЕНТАМ

Вверху этого списка находится кнопка «Просмотреть клиента». Если выбрать пункт и нажать эту кнопку, информация о клиенте появится в следующем *виде (рис. 19)* :

Рисунок 19



отображаются «Приостановленные учетные записи клиентов» и «Неприостановленные учетные записи клиентов» .

Решение по каждой операции принимается нажатием кнопки «Решение по выбранному».

Также внизу этого раздела находятся кнопки «Перейти к обращениям» и «Перейти к инцидентам».

Случаи — это все действия, определенные в сценариях.

Инциденты – это действия, которые были определены как случаи реального мошенничества.

4.2.4. Кейсы

«Кейсы» имеет вид рисунка 20 и состоит из общей информации по кейсам, недавним кейсам и кейсов в мониторингу.

При выборе кейсов в этом разделе также отображается информация о клиенте.

1. ID – состоит из латинских букв и цифр, присвоенных уведомлениям программой;
2. Отметку времени необходимо вводить в формате (ДД.ММ.ГГГГ ЧЧ:ММ:СС). Пример: 12.01.2023 22:15:20;
3. Мобильный? – в этом столбце будет либо Да, либо Нет.
4. Процесс – этот столбец будет включать:
   - Мобильное приложение для ФЛ;
   - Интернет-банкинг для ФЛ;
   - Мобильное приложение для ЮЛ;
   - Интернет-банкинг для ЮЛ;
   - программа для ЮЛ «Банк-Клиент»;
   - Узкард;
   - Хумо;

- Way4;
- ИАБС: депозит ФЛ;
- ИАБС: МДП для ФЛ ;
- ИАБС: ПОВ для ФЛ.

5. Имя клиента - Ф.И.О клиента;
6. Уникальный – 8 цифр, начиная с 10-й цифры номера банковского счета клиента;
7. Телефон – последовательность цифр, начинающаяся со знака +;
8. Тип события – введите одно из следующих:
   - Черный список;
   - Ratelimit ;
   - Redirect;
   - Необычный вход;
   - Не авторизованный доступ;
   - Аномальний оборот;
   - Дропы;
   - Превышение лимита;
   - Неожидая активность спящего счета

Этот список не является исчерпывающим. Администратор может добавить дополнительные типы событий.

9. Остановлено? – Выбрано одно из Да или Нет.
10. Решение. Типы решений, которые могут быть приняты в отношении операций:
    - Останавливать
    - Остановить и сообщить
    - Уведомление
    - Остановить и поискатт похожее.
    - Глобальная остановка
    - Глобальная остановка и отчет
    - Передача в кейсы
    - Черный список
    - Переход к инцидентам

рисунок 20

3. КЕЙСЫ

Последные кейсы

ПЕРЕХОД В ИНЦИДЕНТЫ | **ПОСМОТРЕТЬ КЛИЕНТА** | **РЕШЕНИЕ ПО ВЫБРАННЫМ**

☐	ID	Дата	Мобильность	Процесс	Имя клиента	Уникал	Телефон	Тип события	Остановлен?	Решение	☐
☑	M00001-040220	04.02.2023 09:00:00	да	Вход в мобильное устрой(	ААА	60123410	+749501234567	Черный список	да	Остановить	☐
☑	M00001-040221	04.02.2023 09:00:01	нет	Денежный перевод	ББВ	60123421	+998941234567	Ratelimit	нет	Остановить и сообщить	☑
☑	M00001-040222	04.02.2023 09:00:02	да	МДП	ВВВ	60123432	+749501234567	Redirect	да	Остановить	☐
☑	M00001-040223	04.02.2023 09:00:03	да	Мобильное передача	ГГГ	60123443	+998941234567	Черный список	да	Сообщить	☐
☑	M00001-040224	04.02.2023 09:00:04	нет	депозит	ДДД	60123454	+749501234567	Необычный вход	нет	Остановить	☑
☑	M00001-040225	04.02.2023 09:00:05	нет	Банковская карта	ЖЖЖ	60123465	+998941234567	Не разрешенный вход	нет	Остановить и сообщить	☑
☑	M00001-040226	04.02.2023 09:00:06	нет	Внутренный фрод	333	60123476	+749501234567	Необычный оборот	нет	Остановить	☐
☑	M00001-040227	04.02.2023 09:00:07	нет	Внутренный фрод	ЕЕЕ	60123487	+998941234567	Распределенный оборот	нет	Сообщить	☐
☑	M00001-040228	04.02.2023 09:00:08	нет	Внутренный фрод	ЁЁЁ	60123498	+749501234567	Превышение лимита	нет	Остановить	☑
☑	M00001-040229	04.02.2023 09:00:09	нет	Внутренный фрод	ИИИ	60123409	+998941234567	Необычный вход	нет	Остановить и сообщить	☐

Все кейсы

Просмотрен: 120

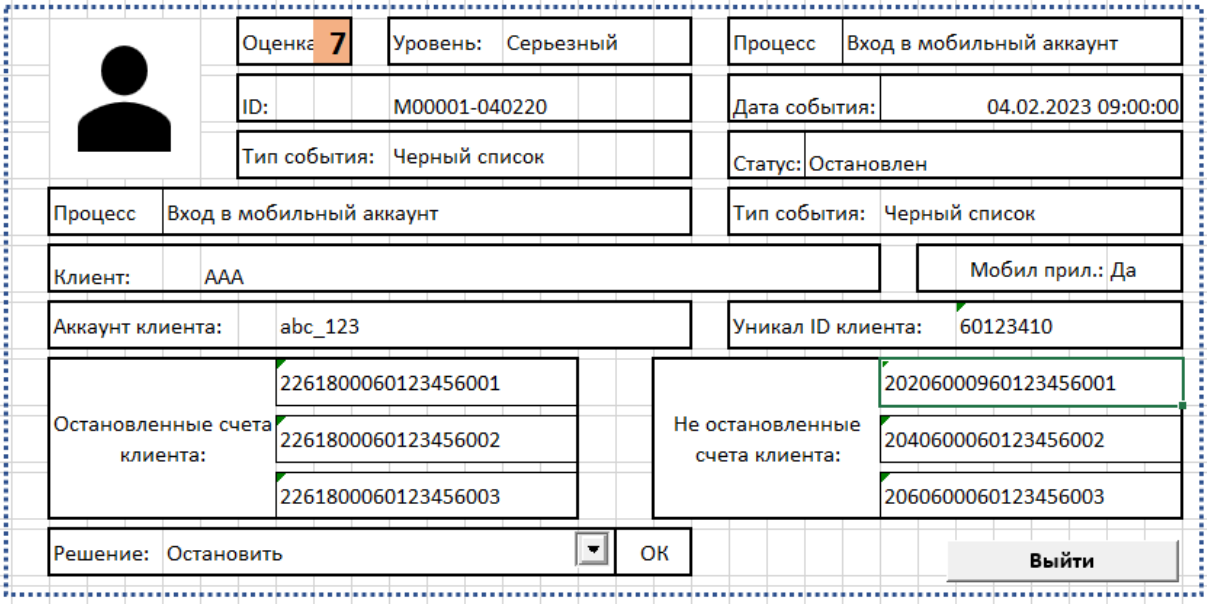
Инциденты: 5

Количество подозрительных звонков за сегодня: 12

Но типы принимаемых решений этим списком не ограничиваются. Администратор должен иметь возможность менять решения или принимать новые решения.

Вверху этого списка находится кнопка «Просмотреть клиента». Если выбрать практику и нажать эту кнопку, информация о клиенте появится, как показано на *рисунке 21 :*

Рисунок 21



Помимо информации в таблице, в этом окне отображаются «Приостановленные учетные записи клиентов» и «Неприостановленные учетные записи клиентов».

4.2.5. Инцидент

«Инциденты» аналогичен разделу «Кейсы», формируется только информация об Инцидентах. (**Рисунок 22)**

Рисунок 22

4. ИНЦИДЕНТЫ

Последние кейсы

ПРОСМОТР ИНЦИДЕНТОВ КЛИЕНТОВ

РЕШЕНИЕ ПО ИЗБИРАТЕЛЬАМ

☐	ID	Дата	Мобильность	Процесс	Имя клиента	Уникал	Телефон	Тип события	Остановлен?	Решение	☐
☑	M00001-040220	04.02.2023 09:00:00	да	Вход в мобильное устрой	ААА	60123410	+749501234567	Черный список	да	Остановить	☐
☑	M00001-040221	04.02.2023 09:00:01	нет	Денежный перевод	ББББ	60123421	+998941234567	Ratelimit	нет	Остановить и сообщить	☑
☑	M00001-040222	04.02.2023 09:00:02	да	МДП	ВВВ	60123432	+749501234567	Redirect	да	Остановить	☐
☑	M00001-040223	04.02.2023 09:00:03	да	Мобильное передача	ГГГ	60123443	+998941234567	Черный список	да	Сообщить	☐
☑	M00001-040224	04.02.2023 09:00:04	нет	депозит	ДДД	60123454	+749501234567	Необычный вход	нет	Остановить	☑
☑	M00001-040225	04.02.2023 09:00:05	нет	Банковская карта	ЖЖЖ	60123465	+998941234567	Не разрешенный вход	нет	Остановить и сообщить	☑
☑	M00001-040226	04.02.2023 09:00:06	нет	Внутренный фрод	333	60123476	+749501234567	Необычный оборот	нет	Остановить	☐
☑	M00001-040227	04.02.2023 09:00:07	нет	Внутренный фрод	ЕЕЕ	60123487	+998941234567	Распределенный оборот	нет	Сообщить	☐
☑	M00001-040228	04.02.2023 09:00:08	нет	Внутренный фрод	ЁЁЁ	60123498	+749501234567	Превышение лимита	нет	Остановить	☑
☑	M00001-040229	04.02.2023 09:00:09	нет	Внутренный фрод	ИИИ	60123409	+998941234567	Необычный вход	нет	Остановить и сообщить	☐

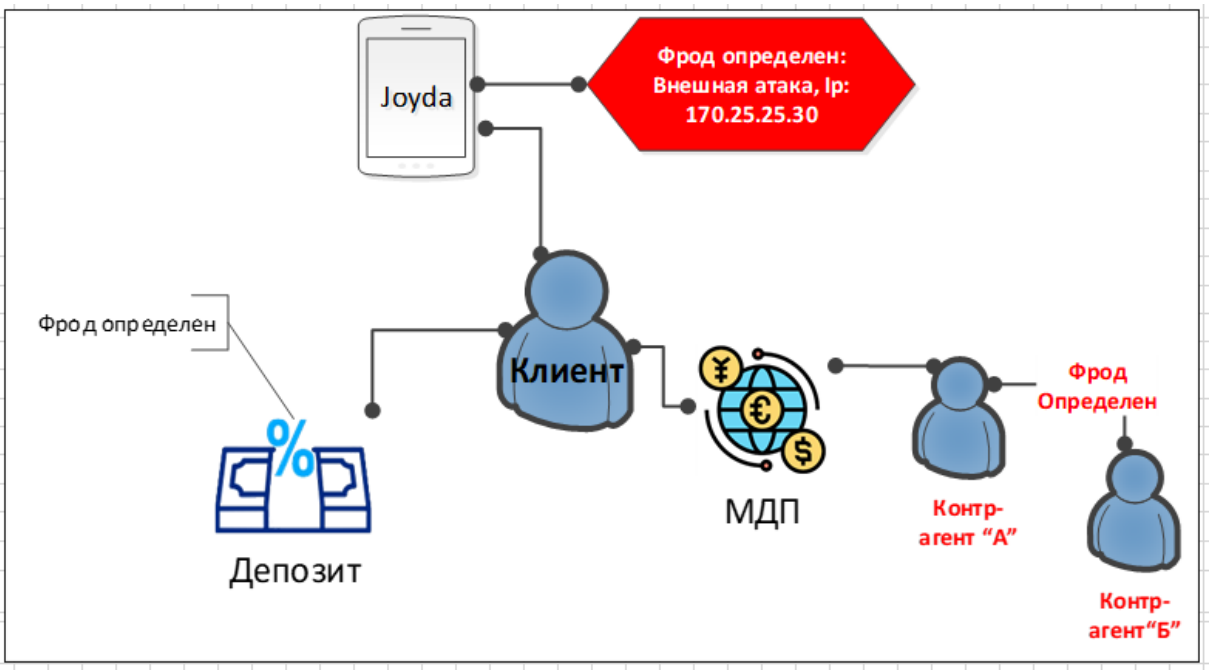
Все кейсы

Просмотрен: 120

Инциденты: 5

Количество подозрительных звонков за сегодня: 12

Рисунок 23



Если в этом разделе выбраны инциденты и нажата кнопка «Просмотреть инциденты, связанные с клиентом», то схемы будут сформированы на основе выбранного инцидента *(Рисунок 23)* . Данную функцию можно активировать после формирования базы данных обнаруженных инцидентов после эксплуатации программы не менее одного года.

4.2.6. Лимиты и настройки

«Настройки лимитов» - раздел позволяет устанавливать ограничения на операции. Превышение лимита может привести к уведомлению или приостановке деятельности клиента и другим мерам. Этот раздел откроется, как показано на **рисунке 24** .

Столбцы этой таблицы означают:

1. ID – уникальный символ, состоящий из цифр и букв, автоматически генерируемый программой при создании каждого лимита;
2. Тип клиента, например: нерезидент и резидент;
3. Тип операций – Приход и расход;
4. Валюта – тип валюты (840, 000 итд);
5. Сумма – устанавливаемая лимитная сумма. (лимиты задаются знаками > ; < ; = и их сочетаниями);
6. Период – к какому периоду времени относится установленная сумма;
7. Решение – тип решения по данному лимиту.
8. Время активации – дата и время установки данного лимита;
9. Время деактивации – дата приостановки действия установленного лимита;
10. Пользователь – это пользователь, изменивший состояние лимита на Активный или Деактивированный.

Новые лимиты устанавливаются с помощью кнопки «Добавить».

кнопку «Заменить» на существующем установленном лимите и внесите необходимые изменения. После внесения изменения существующий лимит будет автоматически приостановлен, и появится новый лимит с новым идентификатором. Старый лимит станет серым и его статус изменится на неактивный.

Вновь созданные или замененные лимиты активируются непосредственно нажатием кнопки «Сохранить».

С помощью кнопки «Тест» вновь созданные или измененные лимиты переводятся в тестовый режим.

С помощью кнопки «Удалить» можно удалить только лимиты, работающие в тестовом режиме, или лимиты, которые еще не активированы. Любое активированное ограничение не должно быть удалено, а только включить или отключить.

С помощью кнопки «Протокол» можно просмотреть историю изменений. (*Рисунок 24.1)*

Лимиты можно включить или отключить с помощью кнопки «Активация/Деактивация».

«Excel» Перенести список лимитов в таблицу Excel.

«Выход», чтобы вернуться в основной интерфейс.

Рисунок 24

5. УПРАВЛЕНИЕ ЛИМИТАМИ | Добавить | Изменить | Сохранить | Тест | Удалить | Протокол | Активация / Деактивация | Excel | Выйти

☐	ID	Тип	Направление	Валюта	Сумма	Период	Решение	Дата активации	Дата деактивации	Пользователь
☑	NE0001-040220	ФЛ не резидент	Выход	840	1000>X	1 раз	Разрешать	06.02.2023 09:00:00	06.02.2023 09:00:00	Алиев
☑	RE0001-040221	ФЛ резидент	Вход	840	3000>X>1000	1 день	Остановить	06.02.2023 09:00:00	06.02.2023 09:00:00	Валиев
☑	NE0001-040220	ФЛ не резидент	Выход	840	X>15000	1 месяц	Разрешать	06.02.2023 09:00:00	06.02.2023 09:00:00	Санаев
☑	RE0001-040221	ФЛ резидент	Вход	840	X>300000	1 квартал	Остановить	06.02.2023 09:00:00	06.02.2023 09:00:00	Ғаниев
☑	NE0001-040220	ФЛ не резидент	Выход	840	45000>X>30000	6 месяц	Разрешать	06.02.2023 09:00:00	06.02.2023 09:00:00	Алиев
☑	RE0001-040221	ФЛ резидент	Вход	840	X>1200000	1 год	Остановить	06.02.2023 09:00:00	06.02.2023 09:00:00	Валиев
☑	NE0001-040220	ФЛ не резидент	Выход	840	X>12000	1 раз	Разрешать	06.02.2023 09:00:00	06.02.2023 09:00:00	Санаев
☑	RE0001-040221	ФЛ резидент	Вход	840	X>30000	1 день	Остановить	06.02.2023 09:00:00	06.02.2023 09:00:00	Ғаниев
☑	NE0001-040220	ФЛ не резидент	Выход	840	X>90000	1 месяц	Разрешать	06.02.2023 09:00:00	06.02.2023 09:00:00	Санаев
☑	RE0001-040221	ФЛ резидент	Вход	840	X>120000	1 квартал	Остановить	06.02.2023 09:00:00	06.02.2023 09:00:00	Ғаниев

Рисунок 24.1

5. УПРАВЛЕНИЕ ЛИМИТАМИ | Протокол | Excel | Выйти

☐	ID	Тип	Направление	Валюта	Сумма	Замененный ID	Фойдаланувчи	Активация вақти	Фойдаланувчи	Деактивация вақти	Пользователь
☑	NE0001-040220	ФЛ не резидент	Выход	840	1000>X	NE0001-040220	Алиев	06.02.2023 09:00:00	Алиев	06.02.2023 09:00:00	Алиев
☑	RE0001-040221	ФЛ резидент	Вход	840	3000>X>1000	RE0001-040221	Валиев	06.02.2023 09:00:00	Валиев	06.02.2023 09:00:00	Валиев
☑	NE0001-040220	ФЛ не резидент	Выход	840	X>15000	RE0001-040221	Санаев	06.02.2023 09:00:00	Санаев	06.02.2023 09:00:00	Санаев
☑	RE0001-040221	ФЛ резидент	Вход	840	X>300000	NE0001-040220	Ғаниев	06.02.2023 09:00:00	Ғаниев	06.02.2023 09:00:00	Ғаниев
☑	NE0001-040220	ФЛ не резидент	Выход	840	45000>X>30000	RE0001-040221	Санаев	06.02.2023 09:00:00	Санаев	06.02.2023 09:00:00	Алиев
☑	RE0001-040221	ФЛ резидент	Вход	840	X>1200000	NE0001-040220	Валиев	06.02.2023 09:00:00	Ғаниев	06.02.2023 09:00:00	Валиев

4.2.7. Чёрный список

«**Черный список**» информация о черном списке формируется в виде, **показанном на рисунке 25** .

рисунок 25

7. Черный список

Добавить | Изменить | Удалить | Выйти

Фильтр										
	Период	от	21.02.22 23:29	до	02.02.23 10:00					
	Кейсы	от	1500	до	3800	Инцидентлар	от	25	до	854
	ID	2	Поле			Приоритет	от	25	до	854

☐	ID	Черный список	Направление	Приоритет	Связанные кейсы	Связанные инциденты
☑	1	+99989712345%	phone number	1.3	1757	392
☑	2	172.25.25*	Host	1.2	1248	25
☑	3	110.25.10.90	Host	1.1	1211	854
☑	4	abc_123_illegal	username	1.0	1325	10

Черный список может содержать номера телефонов, IP-адреса, имена хостов и другую информацию, проверенную в результате мошенничества. Кроме того, в этом окне формируется направление объекта, занесенного в черный список, приоритет, количество связанных случаев и количество связанных инцидентов.

С помощью кнопки «Фильтр» вы можете скачать список по нужной графе.

Технические требования

1. «Период» необходимо вводить в формате (ДД.ММ.ГГГГ ЧЧ:ММ). Образец: 01.12.2023 22:15;
2. В поле «Кейсы» данные вносятся только в виде цифр.
3. Информацию в поле «ID» только в виде числа.
4. Данные вводятся в поле поля путем выбора одного из следующих полей:
   - Мобильное приложение для ФЛ;
   - Интернет-банкинг для ФЛ;
   - Мобильное приложение для ЮЛ;
   - Интернет-банкинг для ЮЛ;
   - программа для ЮЛ «Банк-Клиент»;
   - Узкард;
   - Хумо;
   - Way4;
   - ИАБС: депозит ФЛ;
   - ИАБС: МДП для ФЛ ;
   - ИАБС: ПОВ для ФЛ.
5. Информация в поле инцидента вводится только в виде цифр. Это число означает количество инцидентов, обнаруженных за определенный период времени.
6. Ввод в поле приоритета только в виде цифр.
7. Ввести новую информацию с помощью нажатием кнопку «Добавить»,.
8. При нажатии кнопки «Редактировать» выбирается старая информация и нажимается кнопка «Редактировать». При внесении необходимых изменений и нажатии кнопки сохранения старая информация не должна удаляться (старая информация должна быть «неактивной» и отображаться как новая на измененной информации.)

Должна храниться история всех изменений, причем история изменений должна включать информацию о том, когда каким пользователем она была создана и когда каким пользователем она была изменена.

10. При нажатии кнопки «Отключить» информация переводится в «неактивное» состояние. История всех «удаленных» изменений должна быть сохранена.

4.2.8. Белый список

Раздел **«Белый список»** отображается в виде **рисунка 26 .** Номера телефонов, IP-адреса, имена хостов из белого списка не учитываются при запуске сценариев. Эта фильтрация выполняется перед любой обработкой по любому правилу.

рисунок 26

8. БЕЛЫЙ СПИСОК

Добавить | Изменить | Удалить | Выйти

Фильтр										
	Период:	от	21.02.22 23:29	до	02.02.23 10:00					
	Период:	от	1500	до	3800	Уведомления	от	25	до	854
	Пер	2		Соха		Связанные кейсы	от	25	до	854

☐	ID	Белый список	Направление	Приоритет	Связанные кейсы	Связанные инциденты
☑	1	+99989712345%	phone number	1.3	1757	392
☑	2	172.25.25*	Host	1.2	1248	25
☑	3	110.25.10.90	Host	1.1	1211	854
☑	3	Anvar Aliev / 60123456	client	1.1	1211	854
☑	4	abc_123_illegal	username	1.0	1325	10

С помощью кнопки «Фильтр» можно скачать список по нужной графе.

Технические требования

1. «Период» необходимо вводить в формате КК.ОО.ГГГГ СС:ММ (ДД.ММ.ГГГГ ЧЧ:ММ). Образец: 01.12.2023 22:15;
2. В поле «Кейсы» данные вносятся только в виде цифр.
3. Вносится информация в поле «ID» только в виде числа.
4. Данные вводятся в поле поля путем выбора одного из следующих полей:
   - Мобильное приложение для ФЛ;
   - Интернет-банкинг для ФЛ;
   - Мобильное приложение для ЮЛ;
   - Интернет-банкинг для ЮЛ;
   - программа для ЮЛ «Банк-Клиент»;
   - Узкард;
   - Хумо;
   - Way4;
   - ИАБС: депозит ФЛ;
   - ИАБС: МДП для ФЛ ;
   - ИАБС: ПОВ для ФЛ.
5. Информация в поле инцидента вводится только в виде цифр. Это число означает количество инцидентов, обнаруженных за определенный период времени.
6. Ввод вполе приоритета только в виде цифр.
7. Нажимается кнопка «Добавить», чтобы ввести новую информацию.
8. При нажатии кнопки «Редактировать» выбирается старая информация и нажимается кнопка «Редактировать». При внесении необходимых изменений и нажатии кнопки сохранения старая информация не должна удаляться (старая информация должна быть «неактивной» и отображаться как новая на измененной информации.)

Должна храниться история всех изменений, причем история изменений должна включать информацию о том, когда каким пользователем она была создана и когда каким пользователем она была изменена.

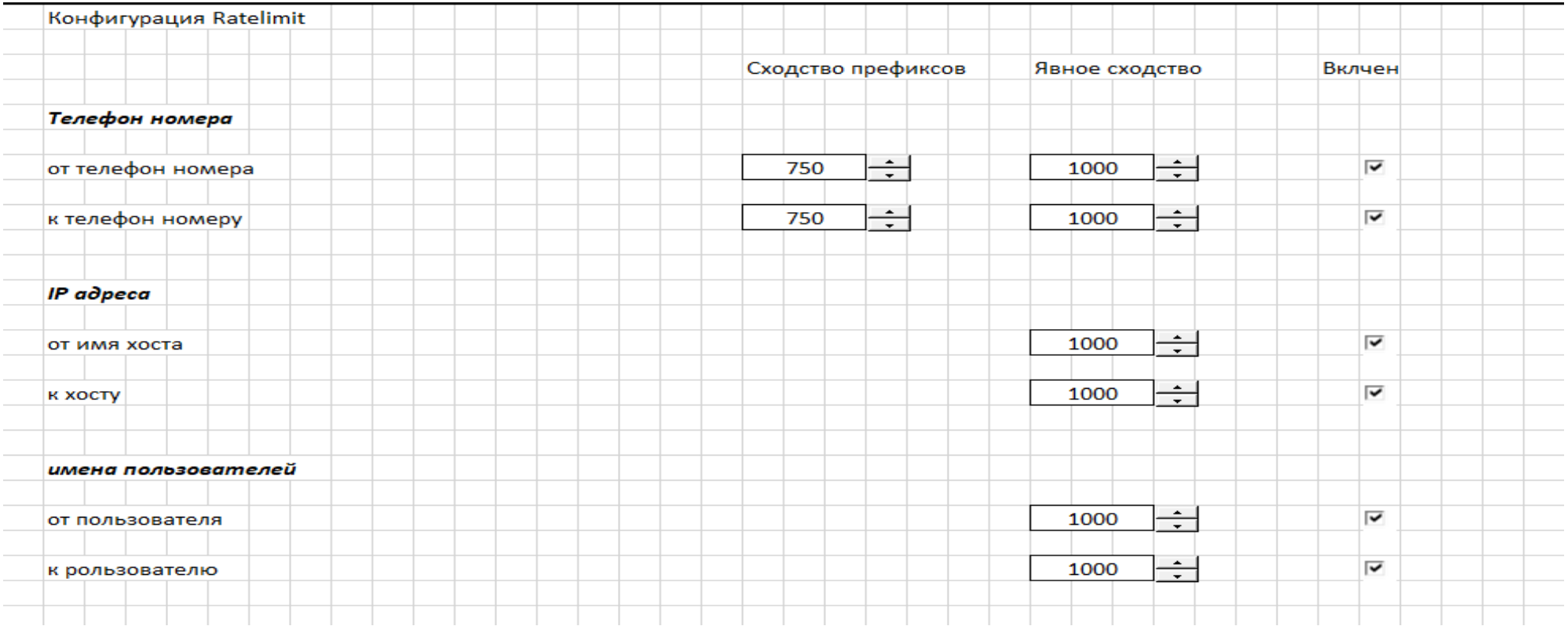
При помощи кнопки «Отключить» данные переводится в «неактивное» состояние. История всех изменений пункта «Удалить» должна сохраняться.

4.2.9. Специальные правила по списку

«Особые правила для списков» состоит из 2 подразделов: 8.1 «Управление белым списком» и 8.2 «Управление черным списком». Эти подразделы аналогичны разделам 6 и 7, за исключением того, что в этом разделе также можно установить параметры «Ratelimit» и «Redirect» для белых и черных списков.

«Особые правила для объявлений» **Откроется** окно раздела в виде **рисунка 27** .

рисунок 27



4.2.10. Тестинг

Тестирование. В этом разделе все вновь добавленные настройки сценариев, ограничений, черного и белого списков изначально запускаются в тестовом режиме. При этом формируется информация об операциях, соответствующих введенному сценарию. Но клиенты фактически не блокируются и сообщение не отправляется.

После опробования сценария в тестовом режиме его можно реализовать или отменить.

Имеется подраздел «Сценарии, правила и уровни серьезности», доступные сценарии, правила и уровни показаны на рисунке 28.

В этом разделе **9.1.** Имеется **подраздел «Сценарии, правила и уровни серьезности»**, доступные сценарии, правила и уровни показаны на рисунке 28.

В этом разделе появляются созданный сценарий и правила . Новые сценарии и правила выбираются и управляются следующими кнопками:

- Режим тестирования запускается кнопкой «Начать тест с выбранным»;
- Тесты, запущенные кнопкой «Завершить тест с выбранным», завершается;
- Тесты удаляются с помощью кнопки «Удалить». Но данные о запущенных тестах должны сохраняться;
- Удалить все тесты можно с помощью кнопки «Удалить полученные по всем тестам». Но данные о запущ енных тестах должны сохраняться;

Также при выборе новых сценариев и правил формируется мониторинг Общих ситуаций, Уведомлений и Критических ситуаций в период до и **после теста .** *(Рисунок 29)*

Рисунок 29

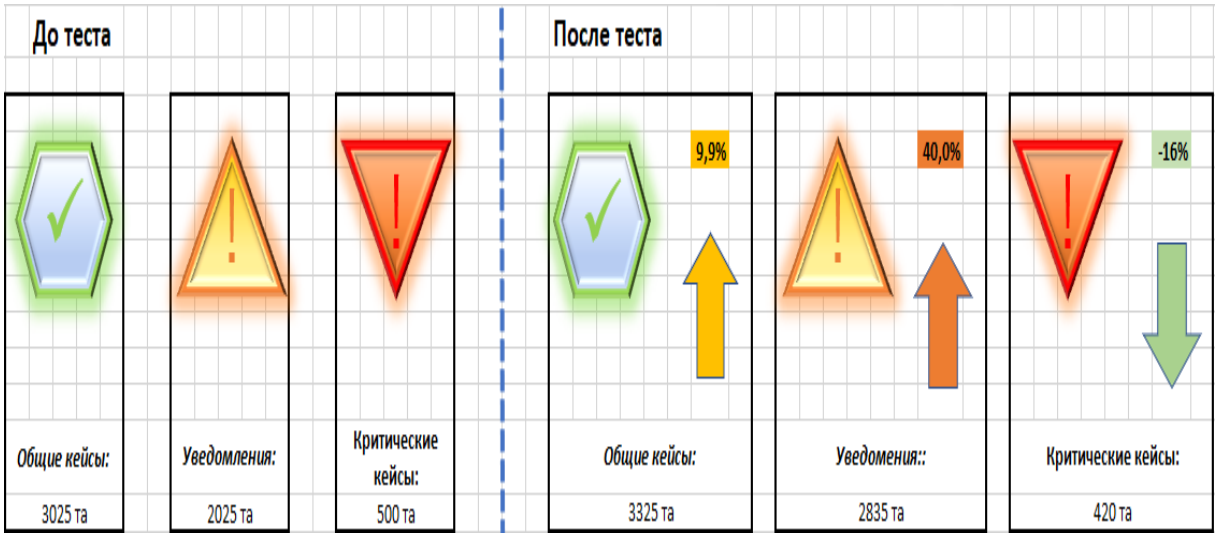


рисунок 28

9. ТЕСТИНГ | **9.1. СЦЕНАРИИ, ПРАВИЛА И УРОВЕНЬ СЕРЬЕЗНОСТИ**

☐	ID	Структура сценария (последовательность, формула)	Поле	Приоритет	Прот.	Point Type	Ограничение	Количество пункта	Предел сходства	Введеные дата и время
☑	1	a) OPER_SEC<=5.0; b) OPER_SUM>=100000000.0; c) CUST_DOB=2007/12/31	мобильнре приложение	1.3	...	Динамик	30%		>130	02.02.2023 9:36
☑	5		мобильнре приложение	1.3	...	Статик	4000	250		02.02.2023 9:36
☑	2	a) OPER_SEC<=5.0; b) OPER_SUM>=100000000.0; c) CUST_DOB=2007/12/31	мобильнре приложение	1.2	...					02.02.2023 9:36
☑	4	a) OPER_SEC<=5.0; b) OPER_SUM>=100000000.0; c) CUST_DOB=2007/12/31	iABS: ФЛ депозит	1.0	...	Статик	4000	250		02.02.2023 9:36

☐	ID	Тип	Направление	Валюта	Сумма	Период	Решение	Дата активации	Дата деактивации	Пользователь
☑	NE0001-040220	ФЛ Не резидент	Выход	840	1000>X	1 раз	Разрешить	06.02.2023 09:00:00	06.02.2023 09:00:00	Алиев
☑	RE0001-040221	ФЛ резидент	Вход	840	3000>X>1000	1 день	Не разрешить	06.02.2023 09:00:00	06.02.2023 09:00:00	Валиев
☑	RE0001-040221	ФЛ резидент	Вход	840	X>120000	1 квартал	Не разрешить	06.02.2023 09:00:00	06.02.2023 09:00:00	Ганиев

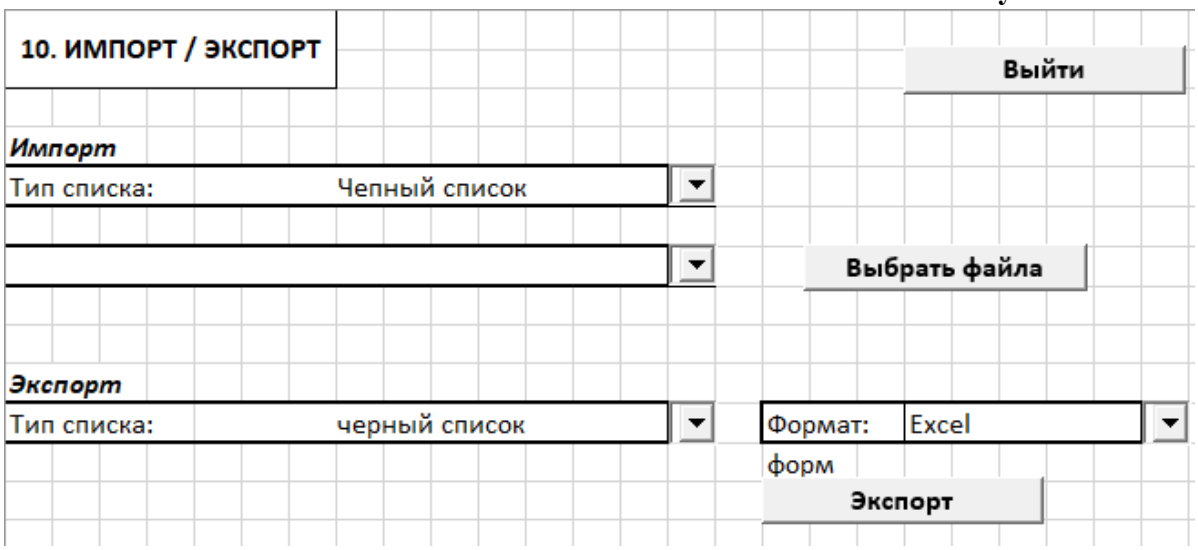
☐	ID	Черный список	Направление	Приоритет	Связанные кейсы	Связанные инциденты	Приоритет	Прот.	Точка	аничен	Пункт	Предел	Введеные дата и
☑	1	+99989712345%	phone number	1.3	1757	392	1.3	...	Динам	30%		>130	02.02.2023 9:36
☑	2	172.25.25*	Host	1.2	1248	25	1.3	...	Статик	4000	250		02.02.2023 9:36
☑	3	110.25.10.90	Host	1.1	1211	854	1.2	...					02.02.2023 9:36
☑	4	abc_123_illegal	username	1.0	1325	10	1.0	...	Статик	4000	250		02.02.2023 9:36

Начинать тест с | Завершение теста с | Удалить | Удалить всех тестируемых

4.2.11. Импорт / Экспорт

«Импорт/Экспорт» выполняет задачу загрузки существующих данных в программу или выгрузки данных из программы. *(Рисунок 30)*

Рисунок 30



Для импорта данных выбирается один из следующих типов списков и существующие данные вводятся в программу.

- Сценарии;
- Правила;
- Уведомления;
- Кейсы;
- Инциденты;
- лимиты;
- Черный список;
- Белый список;
- Особые правила по спискам;
- Тесты;
- Пользователи;
- Роли и функции;
- Внутреннее мошенничество.

При экспорте данных определяются тип списка и формат данных. После этого нажимается кнопка **«Экспорт»** и данные загружаются.

4.2.12. Отчеты / Аудит

«Отчеты/Аудит» состоит из подразделов «Уведомления», «Кейсы и инциденты» и «Визуализация».

В разделе Уведомления, кейсы и инциденты представлен список выявленных случаев, статистика и анализ сценариев, правил и инцидентов. (*Рис. 31*)

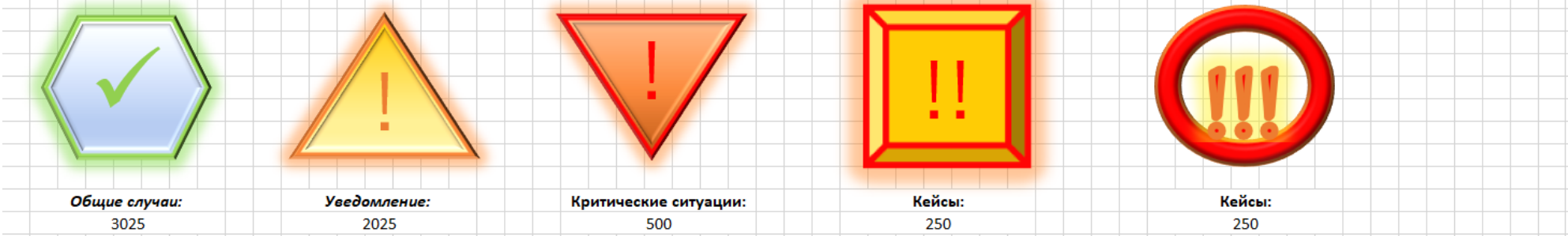
рисунок 31

11. ОТЧЕТЫ/АУДИТ	11.1 ОТЧЕТЫ	11.1.1 СООБЩЕНИЯ, КЕЙСЫ И ИНЦИДЕНТЫ	Фильтр	Изменить	Удалить	Выйти

	ID	Дата	Оцен	Уровень	Мобильность	Процесс	Имя клиент	Уника	Телефон	Тип события	Остановлен	Решение	Дата и врем	Дата и врем	
☑	M00001-040220	04.02.2023 09:00:00	7	Серьезный слу	да	Вход в мобильное устрой	AAA	60123410	+749501234567	Черный список	Да	Остановить	05.02.2023	06.02.2023	☐
☑	M00001-040221	04.02.2023 09:00:01	8	Небольшая кр	нет	Денежный перевод	ББВ	60123421	+998941234567	Ratelimit	Нет	Остановить и сообщить	-	-	☑
☑	M00001-040222	04.02.2023 09:00:02	9	Средняя крити	да	МДП	ВВВ	60123432	+749501234567	Redirect	Да	Остановить	05.02.2023	06.02.2023	☐
☑	M00001-040223	04.02.2023 09:00:03	10	Очень критиче	да	Мобильное передача	ГГГ	60123443	+998941234567	Черный список	Да	Сообщить	05.02.2023	06.02.2023	☐
☑	M00001-040224	04.02.2023 09:00:04	1	Мошенничеств	нет	депозит	ДДД	60123454	+749501234567	Необычный вход	Нет	Остановить	-	-	☑
☑	M00001-040225	04.02.2023 09:00:05	2	Небольшое ме	нет	Банковская карта	ЖЖЖ	60123465	+998941234567	Не разрешенный вход	Нет	Остановить и сообщить	05.02.2023	06.02.2023	☑
☑	M00001-040226	04.02.2023 09:00:06	3	Среднее собы	нет	Внутренный фрод	333	60123476	+749501234567	Необычный оборот	Да	Остановить	-	-	☐
☑	M00001-040227	04.02.2023 09:00:07	4	Большое собы	нет	Внутренный фрод	ЕЕЕ	60123487	+998941234567	Распределенный оборот	Нет	Сообщить	-	-	☐
☑	M00001-040228	04.02.2023 09:00:08	5	Маленький се	нет	Внутренный фрод	ЁЁЁ	60123498	+749501234567	Превышение лимита	Нет	Остановить	-	-	☑
☑	M00001-040229	04.02.2023 09:00:09	6	Серьезный слу	нет	Внутренный фрод	ИИИ	60123409	+998941234567	Необычный вход	Да	Остановить и сообщить	05.02.2023	06.02.2023	☐

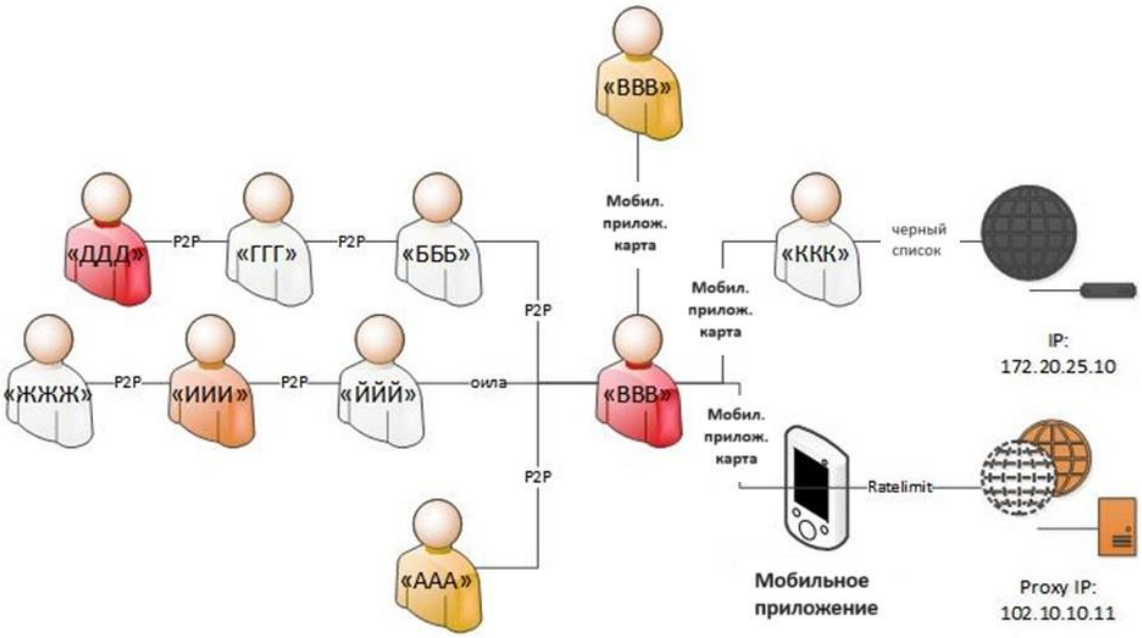
В разделе визуализации представлен анализ выявленных случаев. **Рисунок 32**

11. ОТЧЕТЫ/АУДИТ	11.1 ОТЧЕТЫ	11.1.2 ВИЗУАЛИЗАЦИЯ	11.1.2.1 ОБЩИЕ	Фильтр	Изменить	Удалить	Выйти



Общие случаи:	*Уведомление:*	Критические ситуации:	Кейсы:	Кейсы:
3025	2025	500	250	250

Также будет графический отчет, показывающий отношения одного клиента с другими клиентами.



4.2.13. Пользователь

Когда пользователи используют систему, все процессы должны логироваться (вход в систему, переключиться на новые окна, изменить настройки (информация о старых настройках и новых настройках)). Журналы должны иметь возможность отправляться ***онлайн на другие серверы через протокол системного журнала .***

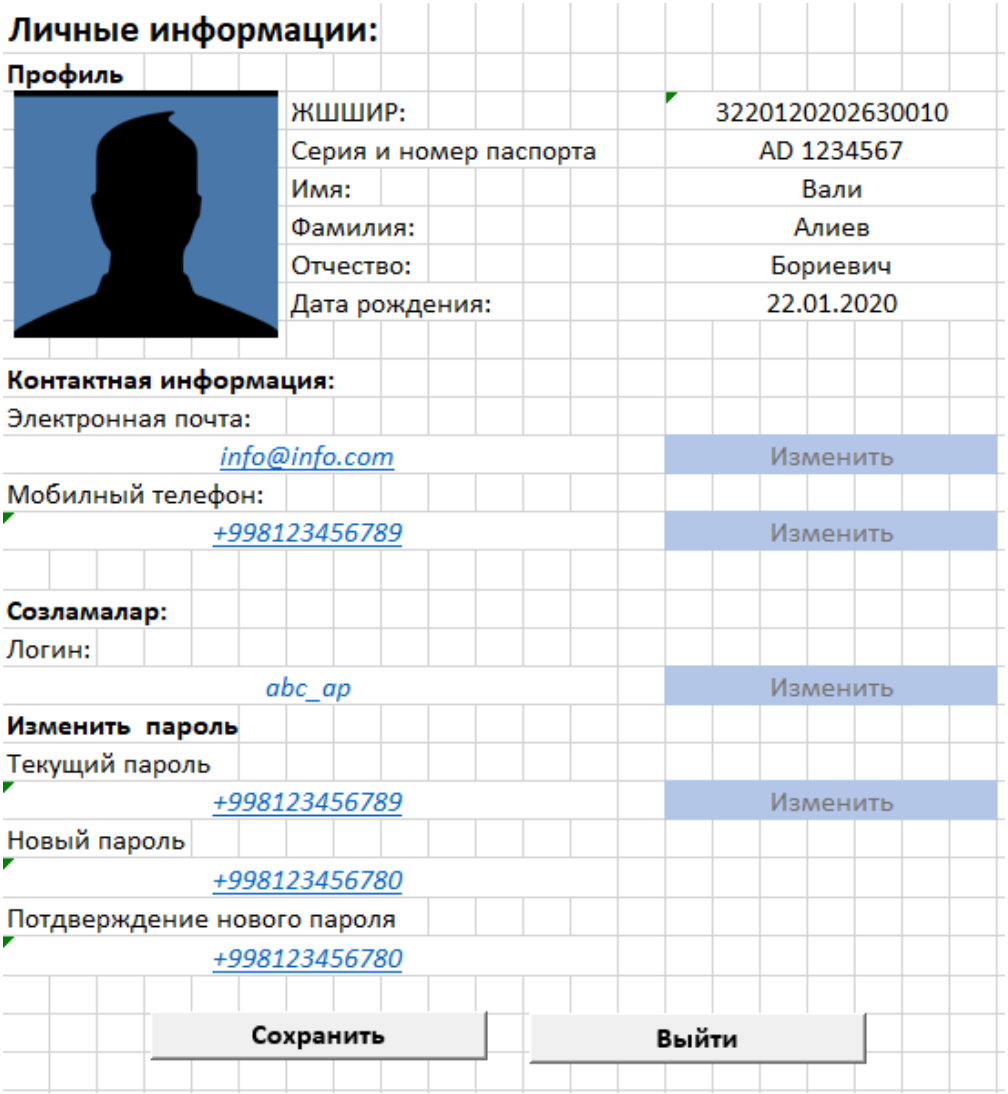
«Пользователь» по вертикали будут появляться подразделы, относящиеся к этому разделу. Подразделы включают «Мой профиль», «Версия программного обеспечения», «Роли и функции», «Настройки обмена сообщениями» и «Выход». (*Рисунок 4*)

Рисунок 4

12. ПОЛЬЗОВАТЕЛЬ	12.1. ПРОФИЛЬ	12.2. ВЕРСИЯ ПРОГРАММЫ	12.3. РОЛЫ И ФУНКЦИИ	12.4. УВЕДОМЛЕНИЯ И НАСТРОЙКИ	12.4. ВЫЙТИ

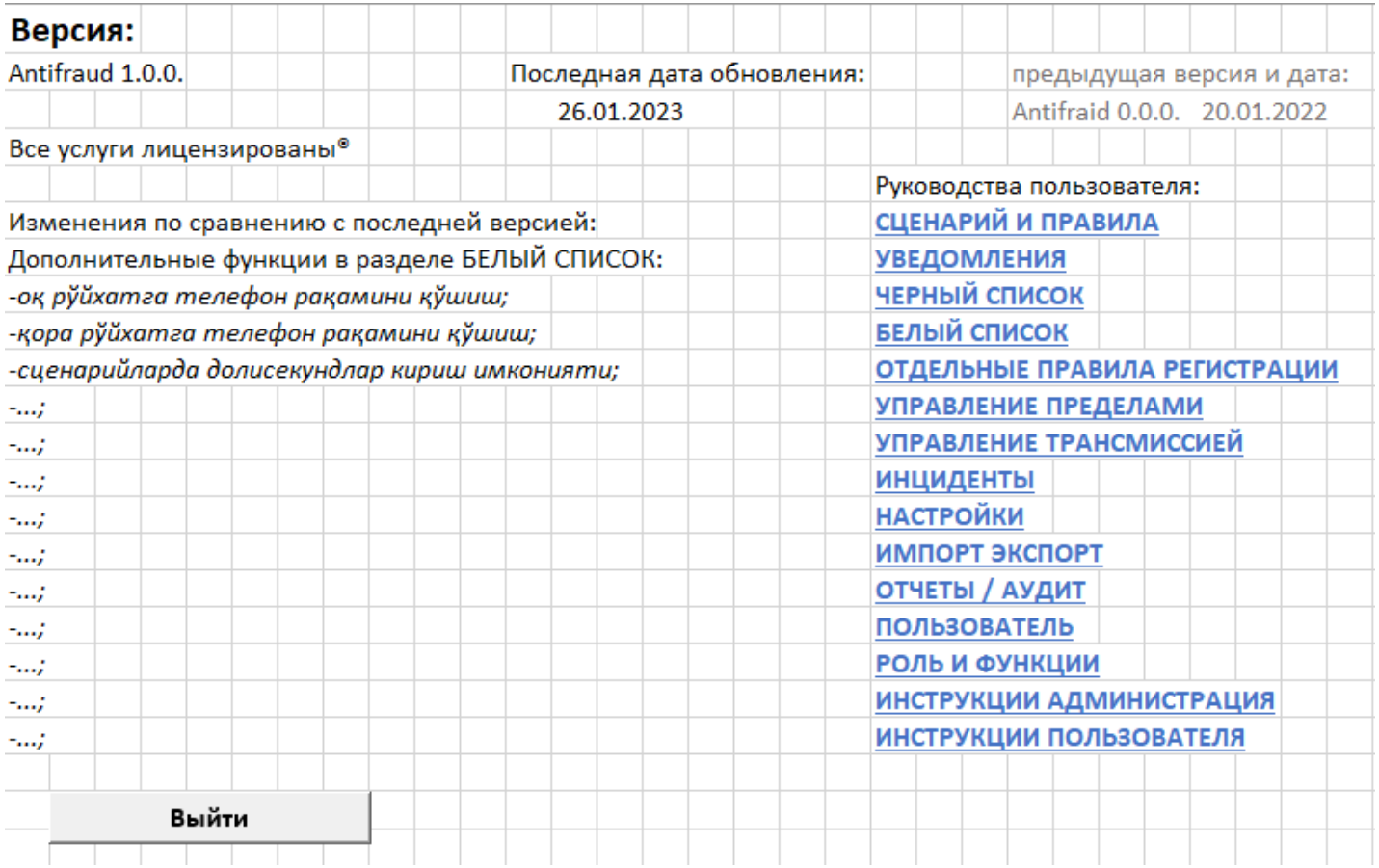
Подраздел **«Мой профиль».** Данный подраздел будет состоять из **информации о владельце профиля в следующем виде.** *(рис. 5)*

рисунок 5



Раздел **«Версия программы»**. В этом подразделе формируется **список информации о версиях программного обеспечения и руководств пользователя,** как показано на **рисунке 6** .

Рисунок 6


Версия:
Antifraud 1.0.0.
Последная дата обновления:
26.01.2023
предыдущая версия и дата:
Antifraid 0.0.0. 20.01.2022
Все услуги лицензированы®
Руководства пользователя:
Изменения по сравнению с последней версией:
Дополнительные функции в разделе БЕЛЫЙ СПИСОК:
-оқ рўйхатга телефон рақамини қўшиш;
-қора рўйхатга телефон рақамини қўшиш;
-сценарийларда долисекундлар кириш имконияти;
-...;
-...;
-...;
-...;
-...;
-...;
-...;
-...;
-...;
-...;
СЦЕНАРИЙ И ПРАВИЛА
УВЕДОМЛЕНИЯ
ЧЕРНЫЙ СПИСОК
БЕЛЫЙ СПИСОК
ОТДЕЛЬНЫЕ ПРАВИЛА РЕГИСТРАЦИИ
УПРАВЛЕНИЕ ПРЕДЕЛАМИ
УПРАВЛЕНИЕ ТРАНСМИССИЕЙ
ИНЦИДЕНТЫ
НАСТРОЙКИ
ИМПОРТ ЭКСПОРТ
ОТЧЕТЫ / АУДИТ
ПОЛЬЗОВАТЕЛЬ
РОЛЬ И ФУНКЦИИ
ИНСТРУКЦИИ АДМИНИСТРАЦИЯ
ИНСТРУКЦИИ ПОЛЬЗОВАТЕЛЯ
Выйти

Подраздел **«Роли и функции»**. Данный подраздел формирует **типы настроек для пользователей** в виде, показанном на **рисунке 7 . Типы настроек** будут состоять из разделов «Пользователи», «Роли», «Формы» и «Выход».

В разделе «Пользователи» окна «Роли и функции» формируется список всех пользователей, которым разрешено использование программы. Список будет содержать следующую информацию о пользователях:

- ID (специально привязанный к пользователю код)
- Территориальная подразделения (код рабочего подразделения работника)
- Фамилия, имя сотрудника
- Группа (прикрепленная роль)
- Положение дел

Предназначенном только **для администратора**, вверху списка находится параметр **«Добавить** » для **добавления новых пользователей , параметр «Изменить»** для **изменения** ранее добавленных параметров, параметр « **Присоединить роли»** для назначения ролей пользователей и журнал для отображения истории всех настроек , которые были изменены. У других пользователей не должно быть этих опций.

В разделе «Роли» (**рис. 8)** формируется список всех пользователей, которым разрешено использовать программу. Список будет содержать следующую информацию о пользователях:

- ID (специально привязанный к пользователю код)
- Имена ролей (Администратор)
- Статус (активный, пассивный)
- Время активации (дд.мм.гггг чч:мм)
- Время деактивации (дд.мм.гггг чч:мм)

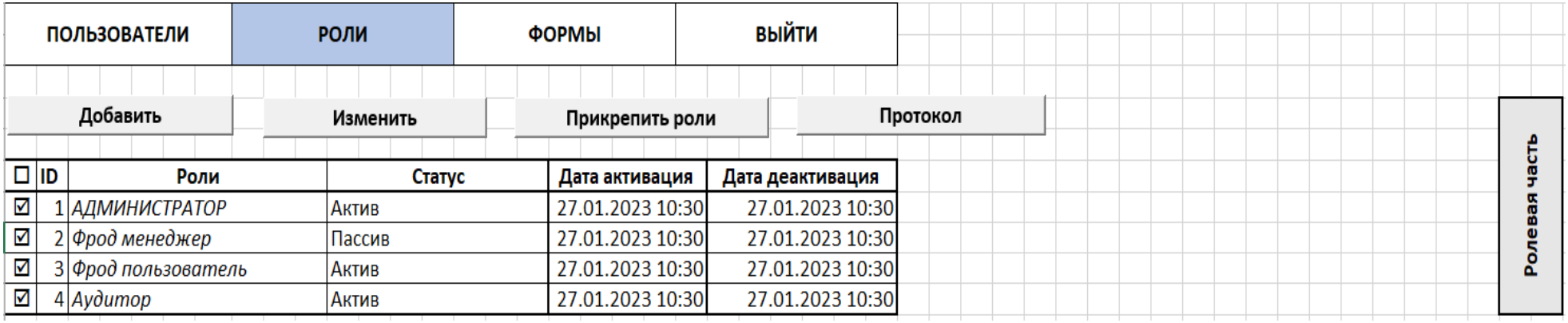
Верхняя часть списка состоит из параметра **«Добавить»** для **добавления новых ролей, параметра «Изменить»** для внесения изменений в ранее добавленные роли, параметра **«Прикрепить фигуры» ,** позволяющего пользователям определять форму ролей, и окна журнала , в котором отображается история всех ролев**.**

Список пользователей появится в окне «Протокол». В этом списке должна формироваться информация о том, какие операции каким админом были «разрешены» и когда для каждого пользователя. Любые внесенные изменения необходимо сохранить.

Рисунок 7

☐	ID	Подразделение	Имя подразделения	ФИО	Группа	Должность	Статус
☑	1	09003	*Главный офис*	Буронов Феруз	Администратор	Администратор	Актив
☑	2	26D00	*Шахристонский филиал*	Халилова Наиля	Пользователь	Пользователь	Уволнение
☑	3	22S00	*Сариосиё филиал*	Мамадалиев Илхом	Пользователь	Пользователь	Отпуск
☑	4	12R00	*Навоийский филиал*	Ўрозов Ҳасан	Пользователь	Пользователь	Актив

Рисунок 8



☐	ID	Роли	Статус	Дата активация	Дата деактивация
☑	1	*АДМИНИСТРАТОР*	Актив	27.01.2023 10:30	27.01.2023 10:30
☑	2	*Фрод менеджер*	Пассив	27.01.2023 10:30	27.01.2023 10:30
☑	3	*Фрод пользователь*	Актив	27.01.2023 10:30	27.01.2023 10:30
☑	4	*Аудитор*	Актив	27.01.2023 10:30	27.01.2023 10:30

В разделе «Формы» **(Рис. 9)** формируется список всех пользователей, имеющих право на использование программы. Список будет содержать следующую информацию о пользователях:

- ID (специально привязанный к пользователю код)
- Имена ролей (формы ролей)
- Статус (активный, пассивный)
- Время активации (дд.мм.гггг чч:мм)
- Время деактивации (дд.мм.гггг чч:мм)
- Окно «Выход» для возврата в основной интерфейс.

курсора на окно **«Настройки сообщения»** и двойном щелчке мыши. В этом подразделе представлена информация о **типах сообщений, отправляемых клиентам и сотрудникам** в форме, представленной на **рисунке 10.** сформирован.

Данный раздел состоит из окон **«Сообщения клиенту»** и **«Сообщения сотрудникам».**

«Сообщения клиенту». Сообщения можно отправлять на 3-х языках (узбекском, английском и русском).

Например:

- (o‘zb) Hurmatli SQB mijozi! Mobil ilova akkauntingi firibgarlikka shubha tufayli to'xtatildi, bankka murojaat qilishingiz so'raladi!
- (рус) Уважаемый клиент SQB! Ваш аккаунт мобильного приложения приостановлен в связи с подозрением на мошенничество, просим обратиться в банк!
- (eng) Dear customer! Your mobile app account is suspended with suspection on fraud, please, visit the bank!

Этот список состоит из столбца «Функционально», в котором указано, когда отправлять сообщения, содержание сообщения и средства доставки сообщений.

Вы можете создавать новые сообщения, нажав кнопку «+», или удалять существующие сообщения, нажав кнопку «-».

Как отправлять сообщения Требуются следующие типы сообщений:

- мобильный;
- Push
- SMS;
- Электронная почта.

«Сообщения сотрудникам» формируется список сообщений, которые будут отправлены сотрудникам. **Рисунок 11**

Сообщения можно отправлять на 3-х языках (узбекском, английском и русском):
Например:

- (o‘zb) Hurmatli xodim! Jiddiy salbiy holat mavjud, tizimni tekshirish lozim!
- (рус) Уважаемый сотрудник! Возник серьёзный инцидент, необходимо проверить систему!
- (eng) Dear collegue! We have serious incident, please, check the system!

Этот список состоит из столбца «Функционально», в котором указано, когда отправлять сообщения, содержание сообщения и средства доставки сообщений.

Вы можете создавать новые сообщения, нажав кнопку «+», или удалять существующие сообщения, нажав кнопку «-». Как отправлять сообщения Справа выберите нужные типы сообщений.

Рисунок 9

ПОЛЬЗОВАТЕЛИ	РОЛИ	ФОРМЫ	ВЫЙТИ

Ролевая часть

☐	ID	Роли	Статус	Дата активация	Дата деактивация
☑	1	*Импорт / Экспорт*	Актив	27.01.2023 10:30	27.01.2023 10:30
☑	2	*Инцеденты*	Пассив	27.01.2023 10:30	27.01.2023 10:30
☑	3	*Черный список*	Актив	27.01.2023 10:30	27.01.2023 10:30
☑	4	*Аудитор*	Актив	27.01.2023 10:30	27.01.2023 10:30

Рисунок 10

Типы сообщений, отправляемых клиентам:

☐	ID	Функционал	Хабар мазмуни	Mob.	Push	SMS	e-mail		
☑	1	Сообщение, которое появляется при закрытии клиентского мобильного приложения	(o'zb) Hurmatli SQB mijozi! Mobil ilova akkauntingi firibgarlikka shubha tufayli to'xtatildi, bankk (рус) Уважаемый клиент SQB! Ваш аккаунт мобильного приложения приостановлен в свя (eng) Dear customer! Your mobile app account is suspended with suspection on fraud, please, v	☑	☑	☑	☑		
☑	2	Сообщение, которое появляется при блокировке карты клиента Soobshcheniye, kotoroye	(o'zb) Hurmatli SQB mijozi! Mobil ilova akkauntingi firibgarlikka shubha tufayli to'xtatildi, bankk (рус) Уважаемый клиент SQB! Ваш аккаунт мобильного приложения приостановлен в свя (eng) Dear customer! Your mobile app account is suspended with suspection on fraud, please, v	☑	☑	☑	☑	+	-

Часть сообщений клиенту

Рисунок 11

Виды сообщений сотрудникам:

☐	ID	Функционал	Содержание сообщения												
☑	1	Очень серьезные нежелательные явления	(o'zb) Hurmatli xodim! Jiddiy salbiy holat mavjud, tizimni tekshirish (рус) Уважаемый сотрудник! Возник серьёзный инцидент, необ (eng) Dear collegue! We have serious incident, please, check the sy								☑	☑	☑	☑	
☑	2	Значительные нежелательные явления	(o'zb) Hurmatli xodim! sezilarli salbiy holat mavjud, tizimni tekshiris (рус) Уважаемый сотрудник! Возник значимый инцидент, необ (eng) Dear collegue! We have significant incident, please, check the								☑	☑	☑	☑	+ -

Часть сообщений клиенту

4.2.14. Системные настройки

4.2.14.1. Системные настройки

Системных настроек Антифрода позволяет настраивать сценарии, настраивать уведомления, черный список, белый список, ограничение скорости, перенаправление, списки импорта/экспорта, а также создавать автоматические списки, необходимые для успешной работы “Fraud Monitoring”.

«Системные настройки» подразделы, относящиеся к этому разделу, будут отображаться вертикально. Подразделы:

13.1 Особенности сценариев;
13.2.Особенности правил;
13.3.Особенности черного списка;
13.4. Возможности белого списка;
13.5. Особенности Ratelimit;
13.6. Особенности Redirect;
13.6 Механизм посредничества.

13. СИСТЕМНЫЕ НАСТРОЙКИ	13.1. ОСОБЕННОСТИ СЦЕНАРИЙ	13.2. ОСОБЕННОСТИ ПРАВИЛ	13.3. ОСОБЕННОСТИ ЧЕРНОГО СПИСКА

13.4. ОСОБЕННОСТИ БЕЛОГО СПИСКА	13.5. ОСОБЕННОСТИ RATELIMIT	13.6. ОСОБЕННОСТИ REDIRECT

4.2.14.2. Особенности сценариев

Особенности сценариев. При входе в раздел формируется список доступных сценариев, представленный на рисунке 33. Список состоит из следующей информации:

- идентификатор (пользовательский код, прикрепленный к скрипту)
- Структура сценария (последовательность, формула)
- Поле (какому отделу или направлению принадлежит сценарий)
- Приоритет
- Прот.

Рисунок 33

13.1. ОСОБЕННОСТИ СЦЕНАРИЙ | 13.1.1. СПИСОК ДОСТУПНЫХ СЦЕНАРИЙ | Посмотреть | Изменить | Удалить | Выйти | Фильтр

☐	ID	Структура сценария (последовательность, формула)	Поле	Приоритет	Прот.
☑	1	a) OPER_SEC<=5.0; b) OPER_SUM>=100000000.0; c) CUST_DOB=2007/12/31	Мобил приложение д	1.3	...
☑	5	a) OPER_SEC<=5.0; b) OPER_SUM>=100000000.0; c) CUST_DOB=2007/12/30	Мобил приложение д	1.3	...
☑	2	a) OPER_SEC<=5.0; b) OPER_SUM>=100000000.0; c) CUST_DOB=2007/12/31	Мобил приложение д	1.2	...
☑	3	a) OPER_SEC<=5.0; b) OPER_SUM>=100000000.0; c) CUST_DOB=2007/12/31	iABS: ФЛ ПОВ	1.1	...
☑	4	a) OPER_SEC<=5.0; b) OPER_SUM>=100000000.0; c) CUST_DOB=2007/12/31	iABS: ФЛ депозит	1.0	...

Вверху списка расположена окна «Добавить» для добавления новых сценариев, «Заменить» для внесения изменений и дополнений в существующие сценарии, «Удалить» для отмены регистрации существующих сценариев и «Выход» для возврата в главное меню.

При входе в окно «Добавить» список полей формируется в виде **рисунка 34** .

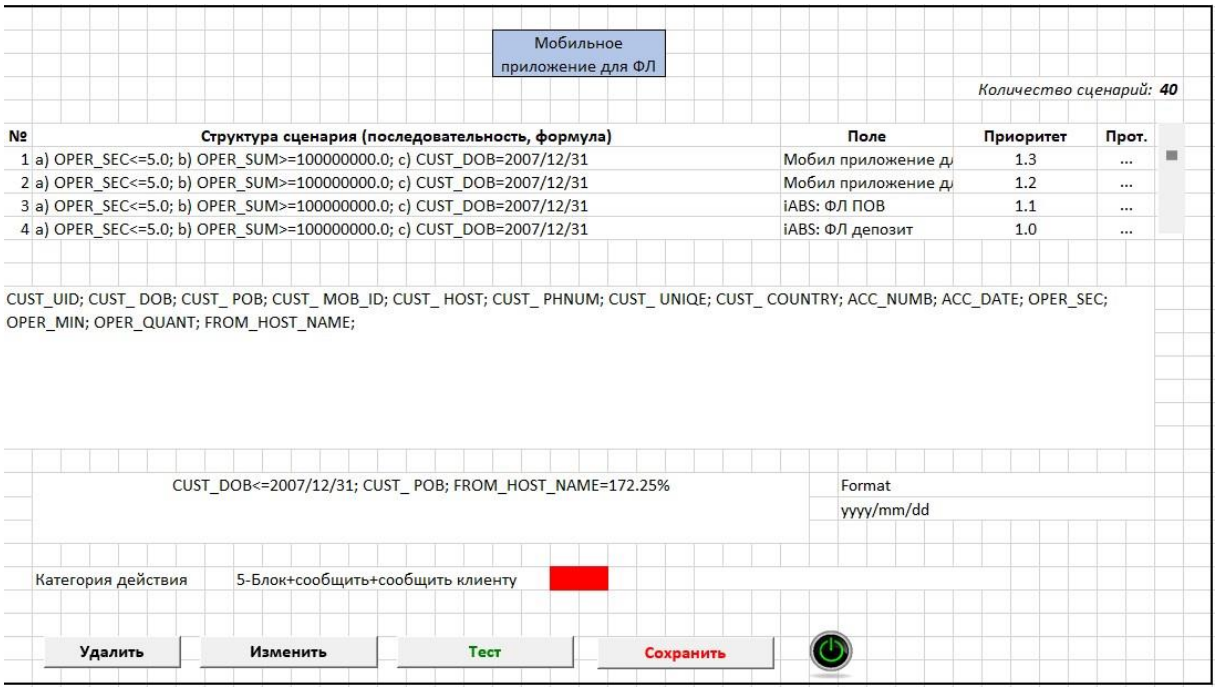
Рисунок 34

При наведении курсора на каждое поле оно загорится синим цветом, а настройки этого поля появятся внизу списка. *(Рисунок 35)*

Рисунок 35

При выборе нужной области и двойном нажатии курсора создается следующая область создания сценария. *(Рисунок 36)*

Рисунок 36

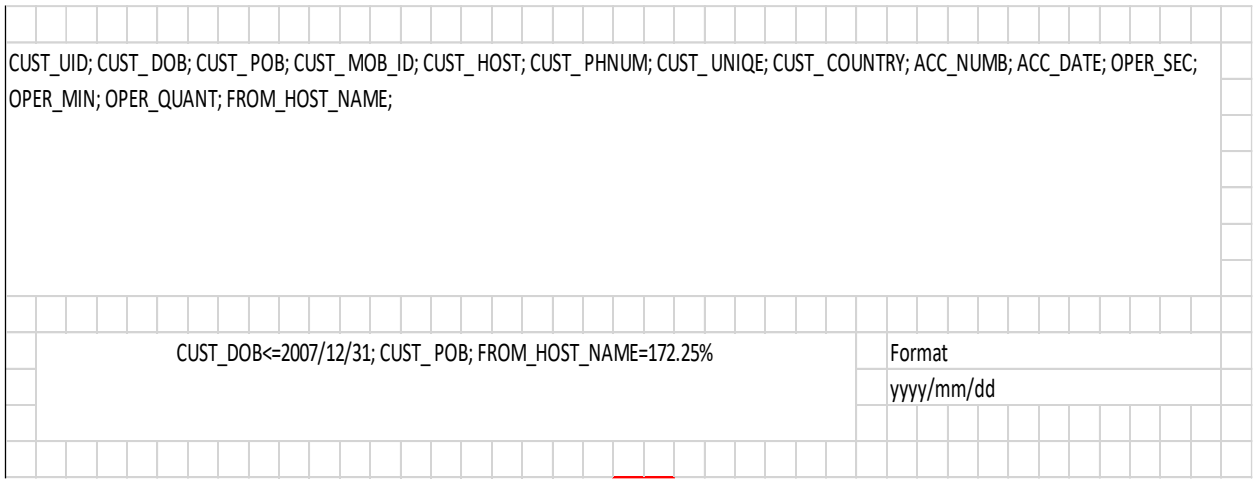


В верхней части этого окна появится **список доступных сценариев .** *(Рисунок 37)*

Рисунок 37

В середине поля будет список показателей, которые необходимо ввести. *(Рисунок 38)*

Рисунок 38



Из этого списка один за другим выбираются и перекидываются в нижнее окно нужные показатели, и для каждого показателя вводится значение. Значение вводится в поле «Формат» справа. Значение вводится для каждого индикатора в зависимости от его формата. Например: дата, процент, текст и т. д.

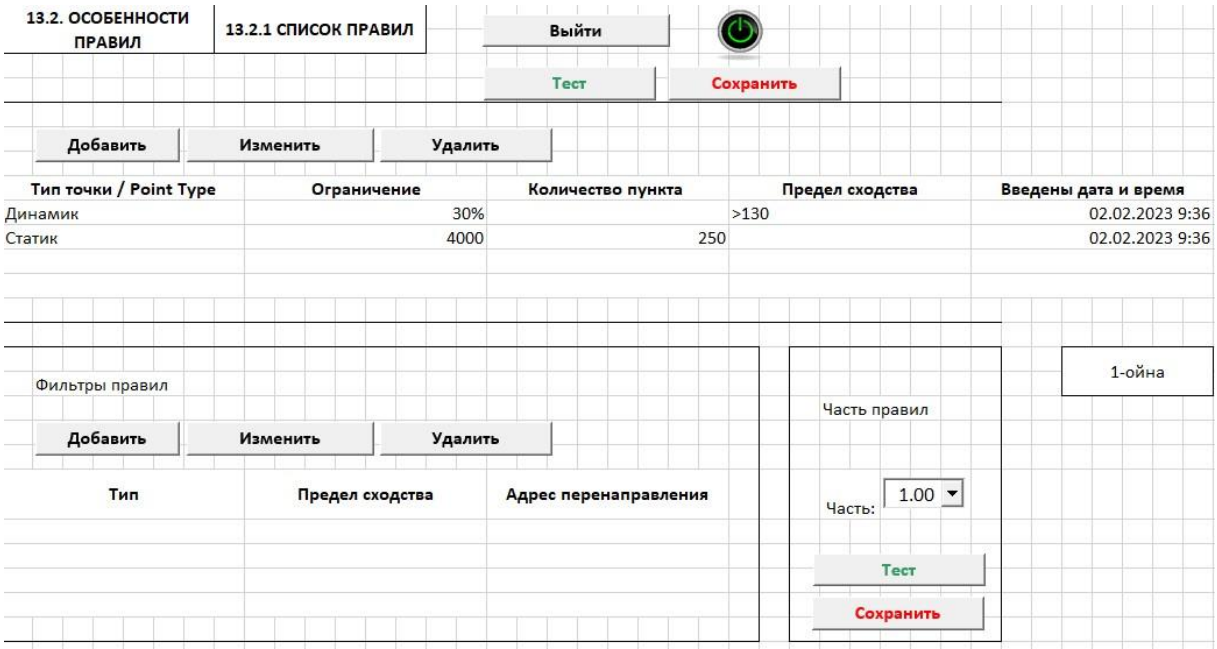
Каждый из включенных сценариев имеет свою категорию действий, которая определяет, как отправлять сообщения клиентам и сотрудникам при обнаружении действия, соответствующего сценарию. Категория действий состоит из 5 частей, они следующие:

1. Сообщение
2. Сообщение + аккаунт
3. Сообщение + превышение лимита
4. Блокировать + сообщение
5. Блокировать + сообщение + сообщение клиенту

4.2.14.3. Особенности правил

Особенности правил при входе в окно откроется следующее окно *(рис. 39) :*

Рисунок 39



На изображении выше показаны настройки Traffic Waves. В настройках волны трафика задаются порог, количество баллов и порог сходства по типам трафика. На каждой панели параметров есть кнопки **«Добавить** », **«Изменить** » и **«Удалить» , которые можно использовать для настройки правил.**

Каждому правилу назначается доля. По умолчанию — 1,00. Доля правил может использоваться для обозначения некоторых правил как более важных, чем другие.

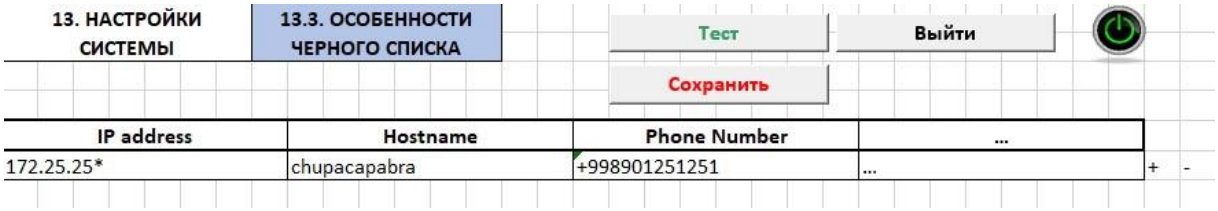
Каждый сценарий имеет возможность опробовать его в тестовом режиме после ввода индикаторов, а после периода тестирования сценарий можно сохранить, изменить или отменить.

Когда возникает необходимость запуска сценария напрямую, кнопка **«Сохранить»** нажимается после установки параметров. На экране появится **текстовое предупреждение** о том, что сценарий **запущен напрямую, и кнопка подтверждения.** После нажатия кнопки подтверждения сценарий запустится.

4.2.14.4. Особенности черного списка

Возможности черного списка. Черный список содержит номера телефонов, IP-адреса и имена хостов, которые были признаны мошенническими. Можно включить и отключить функцию «Черный список» для существующих данных в меню настроек. Окно **свойств черного списка** выглядит следующим образом. *(Рисунок 40)*

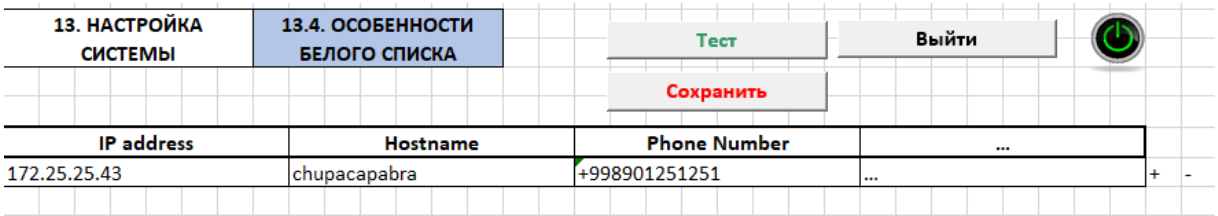
Рисунок 40



4.2.14.5. Особеснности белого спика

При входе в окно особенности **белого списка** формируется список клиентов по номерам телефонов, IP-адресам и именам хостов. В этот список можно добавлять, изменять и удалять дополнительную информацию. (Рисунок 41)

41-расм



В процессе, в котором работают сценарии, номера телефонов, IP-адреса, имена хостов, которые включены в белый список, не учитываются. Эта фильтрация выполняется перед любой обработкой в соответствии с любым правилом.

4.2.14.6. Настройки Ratelimit и Redirect

4.2.14.6.1. Особенности Ratelimit

Ratelimit (ограничение тарифа) - это стратегия ограничения сетевого трафика. Она ограничивает частоту повторения кем-либо действия в течение определенного периода времени - например, попытки войти в учетную запись. Ограничение тарифа поможет остановить вредоносные действия ботов определенного типа. Ограничение скорости часто используется для предотвращения негативного воздействия вредоносных ботов на веб-сайт или приложение.

Как правило, тарифное ограничение основано на отслеживании IP-адресов, с которых поступают запросы, и отслеживании того, сколько времени проходит между каждым запросом. IP-адрес-это основной способ определить, кому или чему приложение

отправляет запрос.

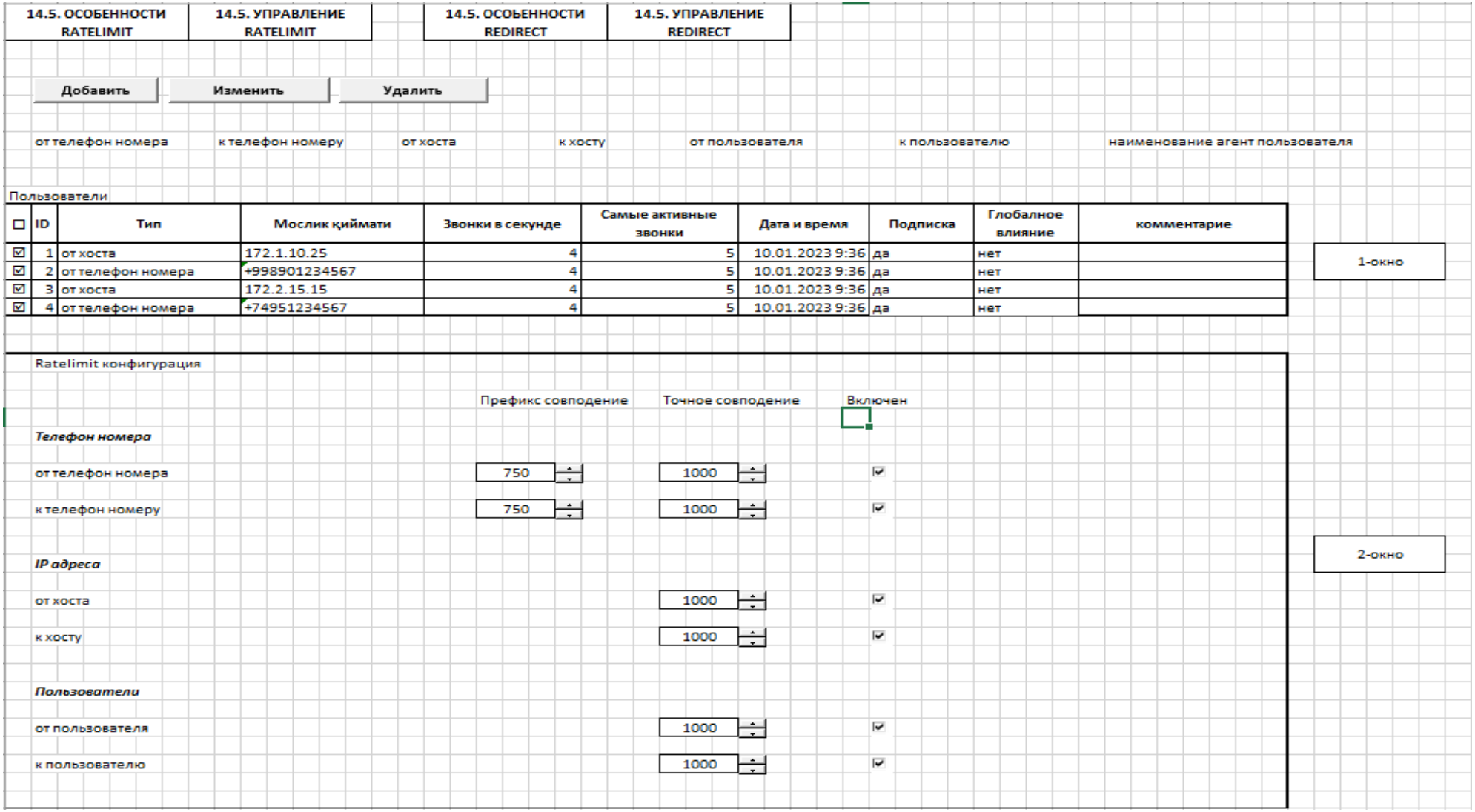
Решение с ограничением тарифов измеряет промежуток времени между каждым запросом с каждого IP-адреса, а также количество запросов за определенный промежуток времени. Когда поступает слишком много запросов с одного IP-адреса за заданный промежуток времени, решение с ограничением скорости не выполняет запросы IP-адресов в течение заданного периода времени.

Если пользователи попытаются войти в систему слишком много раз за короткое время, их учетная запись может быть заблокирована.

Эта мера предосторожности используется не для пользователей, которые забыли свои пароли, а для предотвращения атак со стороны сил, которые проверяют тысячи различных паролей с помощью бота чтоб найти правильный и взломать учетную запись.

Ratelimit позволяет добавлять специальные примечания. Вы можете добавлять номера телефонов, IP-адреса, имя пользователя и sip-агенты пользователей.

рисунок 42


14.5. ОСОБЕННОСТИ RATELIMIT
14.5. УПРАВЛЕНИЕ RATELIMIT
14.5. ОСОЬЕННОСТИ REDIRECT
14.5. УПРАВЛЕНИЕ REDIRECT
Добавить
Изменить
Удалить
от телефон номера
к телефон номеру
от хоста
к хосту
от пользователя
к пользователю
наименование агент пользователя
Пользователи
☐ ID Тип Мослик қиймати Звонки в секунде Самые активные звонки Дата и время Подписка Глобалное влияние комментарие
☑ 1 от хоста 172.1.10.25 4 5 10.01.2023 9:36 да нет
☑ 2 от телефон номера +998901234567 4 5 10.01.2023 9:36 да нет
☑ 3 от хоста 172.2.15.15 4 5 10.01.2023 9:36 да нет
☑ 4 от телефон номера +74951234567 4 5 10.01.2023 9:36 да нет
1-окно
Ratelimit конфигурация
Префикс совподение
Точное совподение
Включен
Телефон номера
от телефон номера
750
1000
к телефон номеру
750
1000
IP адреса
от хоста
1000
к хосту
1000
Пользователи
от пользователя
1000
к пользователю
1000
2-окно

4.2.14.6.2. Особенности Redirect

Свойства **Redirect** формируются правилами, размещенными для подозрительных IP-адресов и телефонных номеров в разделе Перенаправление. В этой таблице отображается информация о типе операции, степени сходства и IP-адресах или телефонных номерах.

Тип операции состоит из 6 частей: от хоста к хосту, от номера телефона к номеру телефона, от имени пользователя к имени пользователя.

4.2.15. Внутреннее мошенничество

Внутреннее мошенничество подразумевается под подозрительными действиями сотрудников банка.

В процессе обслуживания клиентов:

При подтверждении операции по обслуживанию клиентов (физических и юридических лиц) без их биометрических (отпечаток пальца, face-id) данных сотруднику системы мониторинга Antifrod должно поступить автоматическое сообщение.

В процессе работы сотрудников:

Каждому сотруднику банка выдается логин-пароль и электронный ключ для работы в системе iABS, и у каждого сотрудника есть IP-адреса устройства. Сотруднику системы мониторинга Antifrod должно быть получено сообщение, если сотрудник вошел в систему со своего IP-адреса с помощью чужого ключа, или если он вошел в систему со своим ключом с другого компьютера.

Для того чтобы искусственно увеличить показатели KPI, сотрудники банка пытаются совершить несколько видов операции. Система должна уведомлять администраторов, когда происходит такие операции.

4.3. Требования к видам обеспечения

4.3.1. Требования к математическому обеспечению

Требования к математическому обеспечению не приводятся. Но должна быть возможность установить ограничения на методы, выполняемые с помощью интегрированных систем. Необходимо, чтобы была возможность останавливать действия, которые в сумме превышают установленный лимит или которые соответствуют установленным сценариям (если предполагается остановка во время установки лимита), или подавать сигнал в соответствии с этими действиями.

Например:

1) Подача сигналов, если за 1 день на счет 1 клиента будет переведено более 10 000 долларов США.

2) Заблокировать IP-адрес, если в течение 1 часа будет предпринята попытка доступа к нескольким учетным записям мобильного приложения с использованием 1 IP-адреса.

3) Временная блокировка этой учетной записи, если в течение 1 часа будут предприняты попытки доступа к 1 учетной записи в мобильном приложении с IP-адресов разных государств.

4) Блокировать IP-адрес и подать сигнал, если количество обращений с 1 IP-адреса к мобильным приложениям резко увеличивается.

Программа Антифрод должна иметь возможность создавать правил показанным

выше. Этими указанными ограничениями должен управлять администратор (возможность создания нескольких правил и их клонирования). Предполагается, что анализ клиентов будет проводиться с использованием правил и сценариев с внедрением искусственного интеллекта в процессы идентификации/оценки рисков.

4.3.2. 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.

4.3.3. Требования к лингвистическому обеспечению

В этой системе должен был использоваться инструмент многоязычия, который обеспечивает возможность использования нескольких языков в одном интерфейсе. Исходя из этого, названия полей в экранных формах должны быть на английском или русском языках.

Инструмент многоязычия не подразумевает перевода документов на государственный язык;

Инструмент многоязычия используется как часть его стандартных возможностей для отображения этой системной информации на разных языках.

4.3.4. Требования к программному обеспечению

Все программное обеспечение, входящее в состав системы, должно иметь сертификаты, а также контракты (лицензии), подтверждающие законность их использования.

Программное обеспечение должно поставляться с набором лицензий в соответствии с количеством пользователей. Каждый пользователь должен использовать лицензию на свое имя, а также эта лицензия должна быть последней версии поставщика.

Лицензии на программное обеспечение должны быть указаны следующим образом:

Категории системных лицензий:

- Лицензии на ядро системы;
- Лицензия на систему управления базами данных;
- Серверные лицензии операционной системы;
- Лицензии на отказоустойчивые программные компоненты (кластерное программное обеспечение;
- Программное обеспечение, интегрированное со всеми системами;
- Виртуальное программное обеспечение для резервного копирования.

Программное обеспечение должно обладать следующими функциями:

- выполнять полный список математических алгоритмов обеспечения;
- обеспечивать устойчивость в ситуациях, когда возникает дезинформация и ошибки;
- перебои в работе программы, отказ части вычислительных функций, выдача сообщений для диагностики ошибок сотрудников, а также отсутствие перебоев в работе системы;
- при неожиданном отключении и восстановлении питания система должна автоматически перезапускаться, без ошибок;
- все комбинации информации, введенные в процессе выполнения задач должен дат правильные результаты;
- -система должна иметь возможность настраивать работу в процессе эксплуатации.

Для внесения изменений в программное обеспечение необходимо иметь возможность ввести пароль и установить определенные ограничения.

Технический документ на программное обеспечение (документация) должен быть представлен в печатном виде (на бумаге) и в электронном виде на русском и узбекском языках. Если разработчик программного обеспечения не располагает технической документацией на государственном (узбекском) языке, перевод технической документации на государственный язык осуществляется заказчиком.

4.3.5. Требования к техническому обеспечению

Техническая поддержка проекта включает в себя обеспечение доставки, установку, настройку и составление руководства по системе, внедрение компьютерной системы, обучение, обеспечение поставки в соответствии со всеми требованиями, тестирование работоспособности поставляемого оборудования и программного обеспечения (приемо-сдаточные испытания), запуск всего комплекса и начало полноценного использования.

Архитектура аппаратного и программного обеспечения должна соответствовать следующим требованиям. Программное обеспечение должно представлять собой открытую систему, построенную в соответствии с модульной сервис-ориентированной многоступенчатой архитектурой со следующими уровнями:

- централизованный сбор, хранение и обработка данных;

- расширяемый сервер приложений, на котором сосредоточена вся логика бизнес-процессов и основная вычислительная нагрузка;

- пользовательский веб-интерфейс.

Пользовательский интерфейс должен формироваться в сети и обеспечивать его

использование через веб-браузер.

4.3.6. 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.

4.3.7. Требования к организационному обеспечению

Исполнитель должен предоставить полный комплект документации, к каждой единице поставляемой Продукции должен быть приложен полный комплект-оригинал технической документации.

Исполнитель в течение действия гарантийных обязательств должен обеспечить необходимую информационно-консультационную помощь специалистам Заказчика.

Исполнителем должна быть представлена эксплуатационная документация и руководства пользователя в бумажном и электронном виде.

Гарантийное сервисное обслуживания всего программного обеспечения (ИС) должно осуществляться по месту эксплуатации, специалистами Исполнителя.

Производитель оборудования, приобретаемая в процессе реализации ИС и его модулей, должны иметь сервисные гарантии для обеспечения ремонта поставляемого оборудования в Узбекистане (преимущественно поставщик и сервисный центр должны быть регистрированы на территории республики Узбекистан).

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 72 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.

Исполнитель обеспечивает гарантийное обслуживание самой ИС и его модулей, путём дистанционного обслуживания, или путём явки на место специалистов Исполнителя, если это необходимо.

4.3.8. 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:

- Уз. Госст 1986:2018 Государственный стандарт Узбекистана Информационная технология. Информационные системы. Стадии создания
- Уз. Госст 1987:2018 Государственный стандарт Узбекистана «Информационная технология. Техническое задание на создание информационной системы».
- Уз. Госст 1985:2018 Виды, комплектность и обозначение документов при создании информационной системы (ИС),
- Уз. Госст 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.

4.3.9. Обучение пользователей

Поставщик проводит обучение системе не более чем для 20 пользователей (как базовых, так и новых пользователей системы). Обучение проводится в городе Ташкенте в месте, указанном заказчиком.

Заказчик предоставляет пользователям:

- формирование спроса на обучение соответствующего количества пользователей;
- наличие компьютерной техники в учебном кабинете в необходимом количестве и соответствие требованиям для работы в системе;
- Презентационное оборудование.

Документация по информационной системе должна быть предоставлена поставщиком заказчику.

4.3.10. Требования к страхованию товаров

Товары, поставляемые в рамках проекта, должны быть полностью застрахованы с момента погрузки производителем оборудования до их приемки заказчиком в соответствии с условиями поставки товара.

Товар должен быть застрахован поставщиком от риска любой потери или повреждения, связанного с производством или покупкой, транспортировкой, хранением

до момента доставки заказчику.

4.3.11. Требования к размеру и/или сроку действия гарантий

Предложение требует, чтобы рассматриваемая техника и программное обеспечение были новыми (неиспользуемыми, не ремонтировавшимися, не рекламируемыми), произведенными после 2022 года и соответствовали международным стандартам.

На все оборудование должна быть гарантия не менее 3 лет. На все программное обеспечение должна быть гарантия не менее 1 года.

Чтобы всесторонне оценить общую стоимость владения системой (TCO), поставщик должен предоставить информацию о будущих затратах, необходимых для надежной и бесперебойной работы в течение следующих 3 лет после ввода системы в эксплуатацию (техническая поддержка, продление, официальная гарантия производителя и т.д.).

Поставщик должен учитывать стоимость послегарантийного обслуживания (после истечения официального гарантийного срока поставщика) и технической поддержки в течение 1 года по заявленной цене.

V. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

RACI-матрица (лойиҳа иштирокчилари ўртасида вазифаларни тақсимлаш)

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.
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.

Состав и содержание проекта по этапам с точки зрения ответственности сторон.

№	Название этапа	Срок	Ответственный	
			Исполнитель	Покупатель
Этап 1. Подготовка к реализации проекта				
1	Организация внутренних процессов для запуска проекта: принятие Приказа/решения Совета, координация ресурсов, подготовка рабочих мест и другие организационные и подготовительные работы.	1-2 м.	C, I	R, A
2	Предоставлие необходимую техническую		C, I	R, A

	документацию по внутренним и внешним системам, а также предоставлие консультации по некоторым вопросам в процессе работы.			
3	Подготовка документов по реализации проекта.		R, A	C, I
4	Утверждение и подписание документов, связанных с подготовительным этапом к реализации проекта.		C, I	R, A
Этап 2. Проектирование				
1	Своевременное предоставление информации, технологических инструкций и документов, необходимых для проектирования, по запросу.	3 м.	C, I	R, A
2	Выделять рабочую группу для ответа на вопросы в рамках проектирования, разработки и тестирования.		C, I	R, A
3	Провести работу по сбору требований, необходимых для проектирования.		R, A	C, I
4	Анализировать данных, полученных в процессе сбора требований.		R, A	C, I
5	Подготовка документов этапа проекта, необходимых для дальнейшей реализации		R, A	C, I
6	Утверждение и подписание полученных документов этапа проекта.		C, I	R, A
Этап 3. Реализация и тестирование.				
1	Оптимизация алгоритмов для функциональных разработок, полученных в этапе проектирование	2 м.	R, A	C, I
2	Тестирование разработанного проекта перед интеграцией.		R, A	C, I
3	Внедрение разработанных функций существующих систем банка и интеграция с партнерами.		R, A	C, I
4	Устранение недоработок и ошибок, выявленных в результате интеграции с банковскими системами и партнерами.		R, A	C, I
5	После устранения недостатков, выявленных в процессе интеграции, выделить стендов для их комплексного тестирования.		C, I	R, A
6	Подготовка стендов для комплексного тестирования улучшения интеграции.		R, A	C, I
7	Проведение комплекс тестирование.		R, A	C, I
8	Устранение существенных дефектов, выявленных в результате комплексных приемо-сдаточных испытаний.		R, A	C, I
9	Своевременное тестирование и приемка работ, выполненных Вендором.		C, I	R, A
10	Оценивать и информировать об организационной, технической и ресурсной готовности к эффективному реализацию.		C, I	R, A
11	Подготовка итоговой документации этапа улучшения интеграции и тестирования.		R, A	C, I
12	Утверждение и подписание проектной,		C, I	R, A

	организационной, эксплуатационной и официальной документации этапа реализации проекта и тестирования.			
Этап 4. Окончательная эксплуатация				
1	Принятие решения о том, как эффективно запустить проект.	2 м.	C, I	R, A
2	Команда для начала улучшения проекта.		C, I	R, A
3	Отделение специалистов от заказчика для обучения сотрудников заказчика, не более 10 человек в городе Ташкенте.		C, I	R, A
4	Предоставление места для организации и преподавания в городе Ташкенте.		C, I	R, A
5	В Ташкенте обучить сотрудников заказчика численностью не более 10 человек работе в качестве пользователей системы.		R, A	C, I
6	Подготовка полученной документации завершающего этапа.		R, A	C, I
7	Подтверждение и подписание полученных документов завершающего этапа.		C, I	R, A

VI. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

Контроль и приемка Системы должны проводиться в соответствии с требованиями Уз. Гостст 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.

Возникшие в процессе предварительных испытаний и эксплуатации дополнительные требования Заказчика, не предусмотренные в техническом задании, не являются основанием для отрицательной оценки результатов эксплуатации и испытаний. Они могут быть удовлетворены по дополнительному соглашению в согласованные сроки.

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.

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 3 стадии.

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.

Во время эксплуатации Системы ведется рабочий журнал, в который заносятся сведения о продолжительности функционирования, отказах, сбоях, аварийных ситуациях, изменениях параметров объекта модернизации, проводимых корректировках документации и программных средств, наладке технических средств. Сведения фиксируют в журнале с указанием даты и ответственного лица. В журнал могут быть занесены замечания персонала по удобству эксплуатации Системы.

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.

VII. ТРЕБОВАНИЯ К 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 Заказчика, 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.

1	Предельная стоимость	Не предусмотрена
2	Источник финансирования	Собственные средства АКБ «Узпромстройбанк»
3	Условия оплаты	Условия оплаты приведены в конкурсной документации. Порядок финансирования проекта осуществляется согласно действующему законодательству.
4	Валюта платежа	Для иностранных поставщиков - доллар США Для отечественных производителей и поставщиков - сум Республики Узбекистан.
5	Условия поставки	Для всех участников местом поставки является IT инфраструктура (инсталляция ИС, интеграция, обучение/дистанционное обучение) Заказчика
6	Сроки поставки	- не более 24 месяца с даты получения авансового платежа согласно контракту на поставку (сроки могут быть уточнены согласно дорожной карте в сторону уменьшения)
7	Срок выполнения сопутствующих работ, услуг (обучение персонала)	- не более 24 месяца с начала даты получения авансового платежа согласно контракту на поставку (сроки могут быть уточнены согласно дорожной карте в сторону уменьшения)

8	Срок действия тендерного предложения	Три месяца после окончания срока подачи тендерных предложений

VIII. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Исполнитель информационной системы обязан предоставить согласованные с банком операционные документы в соответствии с требованиями стандартов, в том числе:

- руководство пользователя ИС;
- Руководство по управлению ИС.

Руководство пользователя должно содержать описание принципов и функций ИС, а также методов работы в ИС, связанных с созданием, обработкой и использованием электронных документов.

Управление ИС включает в себя следующие руководства:

- инструкции по установке ИС;
- описание принципов организации ИС (на уровне администратора);
- Описание методов работы ИС;
- описание методов управления ИС-каталогом;
- Рекомендации по обеспечению информационной безопасности ИС.

Все операционные документы в рамках данного проекта будут переданы банку в электронном виде на компакт-дисках.

Квалификационные требования к участникам

Участник должен иметь опыт успешной реализации аналогичных проектов в зарубежных странах, высококвалифицированный персонал, хорошую репутацию и достаточные ресурсы для реализации данного проекта.

Члены проектной команды должны иметь квалификацию и практический международный опыт работы в банковском секторе зарубежных стран.

Для реализации проекта поставщик должен иметь команду узбекских и русскоязычных специалистов.

Наличие технической поддержки со стороны продавца на узбекском или русском языках.

При прочих равных условиях компании-вендоры имеют преимущество при выборе поставщиков.

Председатель АКБ
“Узпромстройбанк" _____ **А.Акбаржонов**

Директор департамента
информационных
технологий _____ **А.Кенжаев**

Директор департамента
Комплаенс контроль _____ **А.Ёқубжонов**