

Качество предлагаемых работ
на открытый конкурс в электронной форме
по определению подрядчика на выполнение работ по созданию модуля мониторинга и
анализа криптовалютных транзакций с использованием биткоина

Оглавление

Календарный план работ.....	2
Раскрытие и детализация, указанных в п.п.5.1 Технических требований конкурсной документации, задач разработки программной составляющей и функций Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина документации, планируемые к привлечению ресурсы	7
Инструменты	7
Задача №1: Создание сервера ноды биткоина.....	8
Задача №2: Создание сервера разметки	9
1.1. Компонент связи с нодой биткоина.....	10
1.2. Компонент Парсера	10
1.3. Компонент Кластеризации	10
1.4. Компонент разметки.....	11
1.5. Компонент хранения упоминаний	11
1.6. Компонент Оценка риска.....	12
Задача №3: Создание сервера аналитики.....	12
Задача №4: Создание сервера архивации.....	14
Задача №5: Создание сервера поддержки веб интерфейса пользователя.....	15
1.1. Авторизация	16
1.2. Личный кабинет.....	16
1.3. Визуализация	17
1.4. Компонент уведомлений.....	21

Календарный план работ

на выполнение работ по созданию модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина

№ этапа	Наименование	Отчетные материалы	
		Окончание	
Этап I	Доработка технического проекта третьей очереди ЕИС Росфинмониторинга	29.10.2021г.	
1	Заказчик передает Подрядчику комплект документов, исходные коды - необходимые для выполнения работ.	до 3-го дней со дня заключения государственного контракта	Комплект документов, содержащий информацию о текущем состоянии программной, технической составляющей и архитектуре ЕИС Росфинмониторинга, а также необходимые для выполнения работ документы (исходные коды, ранее разработанные частные технические задания и общее техническое задание).
2	Актуализация технического задания на ЕИС Росфинмониторинга	23.08.2021г.	<ul style="list-style-type: none"> - Общее техническое задание на ЕИС Росфинмониторинга; - Описание комплекса технических средств ЕИС Росфинмониторинга
3	Разработка технического проекта на основании технического задания	10.09.2021г.	Пояснительная записка на Модуль мониторинга и анализа криптовалютных транзакций с использованием биткоина
4	Оформление документации на новый модуль Мониторинга и анализа	29.09.2021г.	<ul style="list-style-type: none"> – Каталог базы данных; – Руководство пользователя; – Руководство администратора; – Руководство администратора по информационной безопасности;

№ этапа	Наименование	Отчетные материалы	
		Окончание	
5	Подрядчик передает Заказчику результаты выполненных работ по этапу № 1	29.10.2021г.	<p>Актуализированная техническая документация на ЕИС Росфинмониторинга:</p> <ul style="list-style-type: none"> – Общее техническое задание на ЕИС Росфинмониторинга; – Описание комплекса технических средств ЕИС Росфинмониторинга; – Пояснительная записка на Модуль мониторинга и анализа криптовалютных транзакций с использованием биткоина; – Компакт-диск с документацией на Модуль мониторинга и анализа криптовалютных транзакций с использованием биткоина; – Каталог базы данных; – Руководство пользователя; – Руководство администратора; – Руководство администратора по информационной безопасности. – Акт сдачи-приемки выполненных работ по этапу
Этап II	Работы по созданию Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина (раскрытие и детализация по каждой задаче разработки программной составляющей и функций Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина, планируемых к привлечению ресурсов указаны в приложении 1 к Календарному плану)	11.11.2021г.	<ol style="list-style-type: none"> 1. Программа и методика испытаний; 2. Компакт-диск с исходными кодами и дистрибутивом программного обеспечения; 3. Протокол проведения испытаний; 4. Программа опытной эксплуатации. 5. Акт сдачи-приемки выполненных работ по этапу
1	Задача № 1: Создание сервера ноды биткоина. Развертывание ноды	15.08.2021г.	
2	Задача № 2: Создание сервера разметки. Разработка	01.11.2021г.	
2.1	Компонент связи с нодой биткоина	01.09.2021г.	
2.2	Компонент парсера. Конвертация данных из ноды биткоина в БД. Конвертация онлайн разметки	01.09.2021г.	
	Работа в фоновом режиме. Очередь	01.10.2021г.	
	Пересчет и разметка адресов	01.10.2021г.	
2.3	Компонент кластеризации	01.10.2021г.	

№ этапа	Наименование	Отчетные материалы	
		Окончание	
2.4	Компонент разметки Блок разметки. Разбор конфликтов. Блок установки приоритетов. Блок логирования. Блок фильтрации доступа	15.10.2021г.	
2.5	Компонент хранения упоминаний	15.09.2021г.	
2.6	Компонент Оценка риска	01.11.2021г.	
3	Задача № 3: Создание сервера аналитики. Разработка	01.11.2021г.	
4	Задача № 4: Создание сервера архивации. Разработка и настройка Резервирование системы и БД. Журнал запросов.	01.10.2021г.	
5	Задача № 5: Создание сервера поддержки веб интерфейса пользователя.	01.11.2021г.	
	Дизайн интерфейсов	15.09.2021г.	
5.1	Авторизация	01.10.2021г.	
5.2	Личный кабинет	01.11.2021г.	
5.3	Визуализация аналитики	01.11.2021г.	
5.4	Компонент уведомлений	15.10.2021г.	
6	Подготовка документов для проведения приемо-сдаточных испытаний	15.10.2021г.	- Программа и методика испытаний; - Компакт-диск с исходными кодами и дистрибутивом программного обеспечения; - Протокол проведения испытаний
7	Приемо-сдаточные испытания (ПСИ)	11.11.2021г.	Протокол проведения испытаний
8	Подготовка к опытной эксплуатации	11.11.2021г.	Программа опытной эксплуатации
9	Подрядчик передает Заказчику результаты выполненных работ по этапу № 2	11.11.2021г.	– Программа и методика испытаний; – Компакт-диск с исходными кодами и дистрибутивом программного обеспечения; – Протокол проведения испытаний; – Программа опытной эксплуатации. – Акт сдачи-приемки выполненных работ по этапу

№ этапа	Наименование	Отчетные материалы	
		Окончание	
Этап III	Опытная эксплуатация Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина	10.12.2021г.	
1	Подготовка стенда для опытной эксплуатации. Установка и настройка сервера ноды биткоин. Подготовка и настройка сервера базы данных системы установка и настройка разработанного программного обеспечения.	15.11.2021г.	
2	Проведение опытной эксплуатации Тестирование – тестирование программно-аппаратной части, – тестирование интерфейса пользователя, – нагрузочное тестирование системы, – пентестинг (тестирование на проникновение и безопасность)	08.12.2021г.	Журнал проведения опытной эксплуатации Протокол проведения испытаний
3	Доработка документации, доработка исходного кода по замечаниям заказчика.	08.12.2021г.	– Программа и методика испытаний; – Каталог базы данных; – Руководство пользователя; – Руководство администратора; – Руководство администратора информационной безопасности
4	Подрядчик передает Заказчику результаты выполненных работ по этапу № 3	10.12.2021г.	– Акт сдачи-приёмки выполненных работ (итоговый, который подписывает после выполнения работ по всем этапам); – Счет; – Счет-фактура; – Журнал проведения опытной эксплуатации; – Доработанная по результатам опытной эксплуатации документация на Модуль мониторинга и анализа криптовалютных транзакций с использованием биткоина: – Программа и методика испытаний; – Каталог базы данных; – Руководство пользователя; – Руководство администратора; – Руководство администратора информационной безопасности

№ этапа	Наименование	Отчетные материалы	
		Окончание	
			<ul style="list-style-type: none"> – Компакт-диск с исходными кодами и дистрибутивом программного обеспечения; – Протокол проведения испытаний.

Раскрытие и детализация, указанных в п.п.5.1 Технических требований конкурсной документации, задач разработки программной составляющей и функций Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина документации, планируемые к привлечению ресурсы

Инструменты

Программное обеспечение будет функционировать под управлением операционной системы семейства Linux (предпочитаемые платформы RedHat Linux/CentOS/Ubuntu).

Серверный комплекс представляет собой набор модулей и компонентов, организованных по принципу микросервисной архитектуры. Такой подход позволит повысить масштабируемость, гибкость и расширяемость решения. Взаимодействие между микросервисами выполняется по протоколу http с использованием JSON в качестве формата обмена данными.

В качестве системы управления базами данных используется Postgres Pro. Postgres Pro - мощная объектно-реляционная система управления базами данных уровня предприятия с открытым исходным кодом, включенная в единый реестр российских программ для электронных вычислительных машин и баз данных (регистрационный номер 104). Postgres Pro имеет полноценную поддержку подмножеств SQL92/SQL99, ключей, объединений, представлений, триггеров, а также предоставляет поддержку хранимых процедур. Postgres Pro имеет мощный зрелый API для большинства современных языков программирования. В качестве СУБД уровня предприятия Postgres Pro обладает поддержкой кластеризации, мультиверсионности, механизмов репликации данных, резервирования и журналирования. В качестве формата обмена данными используются:

- JSON для обмена по протоколу JSON RPC между сервером разметки и нодой bitcoin
- JSON при обмене данными между сервером аналитики и сервером поддержки веб-интерфейса пользователя
- бинарный формат блока и транзакции для получения данных из очередей сообщений ноды bitcoin

В качестве инструментов разработки предполагается использование: - языков программирования Java, Python, Golang

Java - строго типизированный объектно-ориентированный язык программирования общего назначения с открытым исходным кодом. Язык обладает поддержкой базовых типов данных и стандартных коллекций (массивы, словари, списки), базовых средств создания сетевых и

пользовательских приложений, встроенных возможностей функционального программирования. Язык располагает широкой поддержкой сообщества и богатым набором мощных фреймворков и библиотек для решения широкого класса задач уровня предприятия.

Python - высокоуровневый объектно-ориентированный язык программирования общего назначения с динамической строгой типизацией, автоматическим управлением памятью и поддержкой возможностей функционального программирования.

Golang - компилируемый язык программирования общего назначения с открытым исходным кодом. Язык предоставляет возможность создания высокоэффективных многопоточных распределенных систем. Язык обладает простой грамматикой, обеспечивая простоту и читаемость кода, лаконичным синтаксисом, строгой явной типизацией без неявных преобразований и поддержкой таких общеупотребимых структур данных как строки, ассоциативные массивы и каналы для межпроцессного взаимодействия, а также эффективной системой пакетов с явным указанием зависимостей.

В целях создания Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина ЕИС Росфинмониторинга будут выполнены следующие работы:

Задача №1: Создание сервера ноды биткоина

Планируемые к привлечению ресурсы:

- Тестировщик
- Системный архитектор
- Системный администратор (DevOps)

Развертывание ноды биткоина

В качестве ноды биткоин предполагается использование открытого программного обеспечения Bitcoin Core, в частности сервер биткоин-сети bitcoind.

Bitcoind предоставляет:

- полную совместимость с оригинальным ПО биткоин
- полную реализацию API JSON-RPC
- поддержку ZeroMQ
- функционал full node
- функционал индексации транзакций

Также, разработка bitcoind активно ведется и поддерживается сообществом, что гарантирует его актуальность и функционирование в сети bitcoin.

Нода устанавливается и настраивается в режиме full со включенной индексацией транзакций и поддержкой ZeroMQ.

Режим full позволяет ноде хранить все блоки блокчейна, начиная с генезис-блока, загружать и валидировать каждый блок с транзакциями, руководствуясь исключительно алгоритмом консенсуса и отвергая блоки и транзакции, которые противоречат консенсусу.

Режим индексации транзакций позволяет ноде хранить полную информацию о всех транзакциях, когда-либо происходивших в сети и не противоречащих консенсусу.

Будет предоставляться возможность мониторинга нод других криптовалют. Сервер разметки предоставляет возможность взаимодействия с узлами различных криптовалют через механизм подключаемых модулей (плагинов) компонента связи с нодой криптовалюты. На данном этапе будет реализован плагин взаимодействия с нодой биткоин (далее -компонент связи с нодой биткоин). При добавлении узлов других криптовалют будет разработан соответствующий плагин. Веб-интерфейс будет разрабатываться с учетом возможности подключения других нод и наличия у контрагентов не только адресов биткоин, но и других криптовалют.

Чтобы иметь возможность проводить мониторинг транзакций и предоставлять доступ к данным будет сделана конвертация всего содержимого ноды биткоина в таблицы отдельной базы данных, предназначенной для работы серверов аналитики и разметки. Выбор сервера баз данных для хранения будет проведен на этапе технического проектирования.

Будет вестись журналирование событий ноды (старт, стоп, добавление блока). Журнальная информация о событиях будет реплицироваться на сервер архивации

Задача №2: Создание сервера разметки

Планируемые к привлечению ресурсы:

- Руководитель проекта
- Системный аналитик
- Аналитик данных
- Аналитик по информационной безопасности
- Бизнес-аналитик
- UX/UI дизайнер
- Старший разработчик BE (Java)
- Тестировщик
- Инженер по нагрузочному тестированию
- Пентестер
- Системный архитектор
- Системный администратор (DevOps)
- Технический писатель
- Разработчики BE (Java)

Все компоненты сервера разметки ведут внутренние журналы выполнения операций и изменений данных. Эти журналы на постоянной основе будут реплицироваться на сервер архивации.

1.1. Компонент связи с нодой биткоина

Компонент связи с нодой биткоин реализует два варианта взаимодействия:

- посредством API JSON-RPC, который предоставляет сервер ноды биткоин
- через очереди сообщений ноды bitcoin

1.2. Компонент Парсера

- конвертации всего содержимого ноды биткоина в таблицы базы данных системы. При первоначальном запуске ноды криптовалюты (биткоин) выполняется конвертация содержимого ноды (информация о блоках и транзакциях) в таблицы offchain базы данных для дальнейшей обработки (разметки, кластеризации, обогащения). Процесс переноса данных реализуется с помощью последовательных запросов к серверу ноды биткоин через API JSON-RPC о блоках и транзакциях, парсинга полученных данных и помещения полученной информации в соответствующие таблицы базы данных системы.
- Мониторинг транзакций, ожидающих подтверждения, осуществляется путем подключения к соответствующей очереди сообщений ноды биткоин. После получения транзакции производится ее конвертация в структуру данных, с которой удобно производить операции по разметке. Из этой структуры выделяются такие данные как вход и выход транзакции, адреса отправителя и получателя, электронные подписи, баланс. Информация о том, от какой ноды криптовалюты мы получили транзакцию, известна из параметров подключения к очереди сообщений (в случае с биткоин). Таким образом собранная информация помещается в базу данных системы и становится доступна для дальнейшей обработки.
- работы в фоновом режиме.. Перенос новых транзакций и блоков из ноды биткоина в базу данных системы выполняется в фоновом режиме при появлении таковых в соответствующих очередях сообщений ноды биткоин. После добавления новых транзакций или блоков в базу данных системы выполняется обработка новых данных. В фоновом режиме согласно установленному расписанию выполняется переразметка входов и выходов транзакций по текущим курсам биткоина к рублю и доллару.

1.3. Компонент Кластеризации

Чтобы определить, имеет ли кошелек отношение к подозрительной деятельности, адреса будут сгруппированы по признакам принадлежности к одному владельцу, или по полученным платежам. Разметка кластеров будет происходить в соответствии с алгоритмом кластеризации по общей трате с использованием алгоритма маркирования вершин. В кластер группируются адреса

- которые являются входами одной или нескольких транзакций и имеют одного или нескольких общих получателей

- которые являются выходами одной или нескольких транзакций и имеют одного или нескольких общих отправителей

1.4. Компонент разметки

Для того, чтобы учитывать последние изменения и дополнения в базе данных системы, разметка выполняется на регулярной основе в фоновом режиме согласно установленному расписанию. Компонент разметки состоит из следующих функциональных блоков:

- Скрипт актуализации
- Блок обеспечения разметки кластеров
- Блок разбора конфликтов с разметкой
- Блок установления приоритетов
- Блок журналирования действий в области разметки
- Блок фильтрации доступа

Для выдачи первичной разметки и проведения аналитической работы компонент разметки обеспечивает возможность подсчета промежуточных и общих значений по следующим субъектам разметки:

- адреса
- владельцы адресов
- кластеры
- владельцы кластеров

Первичная разметка производится на основе открытых источников. Методика определения параметров причисления субъектов разметки к противоправной деятельности будет определена совместно с заказчиком.

1.5. Компонент хранения упоминаний

Компонент используется для разметки и хранения упоминаний адресов в глобальной сети. Компонент обладает следующим функционалом:

- сохранение поступающей от поисковых модулей информации, включая признак «где встретилось упоминание» (WEB и TOR, имя поискового ресурса с помощью которого было найдено упоминание, имя и адрес ресурса на котором имеется упоминание)
- сохранение истории изменений упоминаний адреса
- разметку поступающих упоминаний
- сохранение истории изменений разметки упоминаний.

Упоминания используются для оценки рисков. Регулярно будут анализироваться данные из различных общедоступных источников, оценивая упоминания о принадлежности адресов различным собственникам, которые можно найти в Интернете, а также переводы средств через онлайн-платформы для оценки процедур соответствия.

1.6. Компонент Оценка риска

Компонент используется для:

- выполнения разметки по показателю риска для таких субъектов разметки как адреса, кластеры и их владельцы
- расчета риска для каждого субъекта разметки риска с учетом исторически накопленного значения риска
- хранения последнего рассчитанного показателя риска для каждого из субъектов разметки риска
- хранения исторических показателей риска для каждого из субъектов разметки риска

При работе размечаются объекты, которые осуществляют незаконную деятельность, в соответствии с критериями оценки рисков. Таким объектам присваивается высокий уровень риска. Объекты с высоким уровнем надежности – отмечаются низким уровнем риска. Каждая оценка риска влияет на другие объекты, которые взаимодействуют с известными объектами. Риски могут рассчитываться по алгоритму, на основе классификации рисков, а также могут быть проставлены на основе ручного экспертного анализа.

Для методики оценки и присвоения контрагенту степени риска нужно предусмотреть:

1. Классификацию рисков. Для оценки вероятности связи субъекта разметки риска с подозрительной деятельностью могут быть применены такие критерии оценки рисков, как:
 - сбор средств с получением небольших сумм с многочисленных разных счетов,
 - необычно большое количество операций по счету,
 - значительные по объему трансграничные переводы денежных средств,
 - финансовые операции, совершаемые с участием объектов, подозреваемых в подозрительной деятельности,
 - транзакции с участием биткоин-миксеров (сервисы анонимизации),
 - обмен на биржах без строгих требований проверки КУС (требования к идентификации пользователей),
 - транзакции с участием адресов, зарегистрированных в даркнет,
 - риски, связанные со странами и отдельными географическими территориями (страновые риски).

Окончательные критерии оценки будут определены на этапе разработке после согласования с Заказчиком.

2. Структура степеней риска (высокий, средний, низкий). Степень риска будет отображена на графе соответствующим цветом.

Задача №3: Создание сервера аналитики

Планируемые к привлечению ресурсы:

- Руководитель проекта
- Системный аналитик
- Аналитик по информационной безопасности
- Бизнес-аналитик
- UX/UI дизайнер
- Старший разработчик BE (Java)
- Тестировщик
- Инженер по нагрузочному тестированию
- Пентестер
- Системный архитектор
- Системный администратор (DevOps)
- Технический писатель
- Разработчик FE
- Разработчики BE (Java)

Сервер аналитики состоит из двух функциональных частей:

- препроцессинг данных
- REST-интерфейс для доступа к результатам препроцессинга

В части препроцессинга сервер аналитики выполняет следующие задачи:

- обновление данных о валидности адресов
- актуализация данных об оборотах адресов с учетом перерасчета сумм в долларах и рублях
- обогащение данных об оборотах адресов информацией о внутрикластерных оборотах
- актуализация данных о показателях риск-скоринга для транзакций
- актуализация списков адресов, входящих в состав кластеров
- обогащение данных о кластерах данными о транзакциях, в которых участвуют адреса кластера
- обогащение данных о кластерах данными об оборотах адресов кластера
- обогащение данных о кластерах данными о показателях риска адресов кластера
- актуализация данных о показателях риска кластеров
- актуализация списков владельцев адресов/кластеров
- обогащение данных о владельцах данными об оборотах, суммах в рублях/долларах
- обогащение данных о владельцах данными о рисках, актуализация этой информации
- обогащение данных о владельцах данными о временных интервалах работы
- обогащение данных о владельцах данными о транзакциях

Сервер аналитики предоставляет REST интерфейс для доступа к предварительно подготовленной аналитической информации, сгруппированный по следующим признакам:

- информация о блоках
 - совокупная информация о блоках
 - информация о конкретном блоке
- информация о транзакциях
 - совокупная информация о транзакциях
 - детальная информация по транзакции с указанным идентификатором
 - информация о риск-скоринге транзакции
- информация об адресах
 - данные о принадлежности адресами

- данные об обороте адреса, включая пересчет сумм в долларах и рублях
- информация об историческом изменении риска
- информация о кластерах
 - совокупная информация о кластерах
 - список всех адресов кластера
 - информация о совокупном риске кластера
 - информация об историческом изменении риска кластера
 - информация о транзакциях кластера
 - информация об обороте кластера в биткоин/рубли/доллар с учетом и без учета оборота внутри кластера
- информация о владельцах

Все компоненты сервера аналитики ведут внутренние журналы выполнения операций и изменений данных. Журналы на постоянной основе будут реплицироваться на сервер архивации.

Задача №4: Создание сервера архивации

Планируемые к привлечению ресурсы:

- Системный аналитик
- Тестировщик
- Системный архитектор
- Системный администратор (DevOps)
- Разработчики BE (Java)
- Разработчик FE

Функционал:

- резервирование БД системы,
- резервная копия основной базы данных,
- ведение журнала запросов к сайту,
- история изменений данных

Резервирование базы данных системы выполняется при помощи механизма кластеризации сервера базы данных и репликации данных между узлами кластера. Для этого на сервере архивации разворачивается резервный узел сервера баз данных системы, который предполагается использовать в качестве «теплой» реплики с асинхронной репликацией данных/трансляцией журналов. Такое решение позволит обеспечить быстрое (1-3 с) переключение на резервный узел сервера баз данных в случае каких-то неполадок на основном узле БД.

Резервная копия базы данных создается при помощи встроенных инструментов резервного копирования программного обеспечения сервера баз данных. Резервная копия базы данных будет создаваться по расписанию на регулярной основе. Запуск резервного копирования по расписанию реализуется при помощи механизма cron. Резервная копия базы данных создается для основного и резервного узлов БД.

Сервер архивации предоставляет такие возможности работы с записями журналов функционирования всех блоков системы, как:

- получение журналов событий от других блоков системы, в том числе поиск по истории изменений данных и запросам к данным системы, в том числе поиск по истории изменений данных и запросам к данным системы

- архивация журналов событий от других блоков системы, в том числе поиск по истории изменений данных и запросам к данным системы

- поиск по записям журналов событий от других блоков системы, в том числе поиск по истории изменений данных и запросам к данным системы

- агрегация записей журналов событий от других блоков системы, в том числе поиск по истории изменений данных и запросам к данным системы

- просмотр записей журналов событий от других блоков системы, в том числе поиск по истории изменений данных и запросам к данным системы

Сервер архивации будет обеспечивать возможность хранения данных (резервные копии баз данных, журналы событий) в течении некоторого разумного периода времени и обеспечивать периодическую своевременную ротацию данных.

Задача №5: Создание сервера поддержки веб интерфейса пользователя

Планируемые к привлечению ресурсы:

- Руководитель проекта
- Системный аналитик
- Аналитик по информационной безопасности
- Бизнес-аналитик
- UX/UI дизайнер
- Старший разработчик BE (Java)
- Тестировщик
- Инженер по нагрузочному тестированию
- Пентестер
- Системный архитектор
- Системный администратор (DevOps)
- Технический писатель
- Разработчик FE
- Тестировщик

Веб-сервер будет располагаться на сервере аналитики.

Все компоненты веб интерфейса GUI ведут внутренние журналы выполнения операций и изменений данных. Эти журналы на постоянной основе будут реплицироваться на сервер архивации.

1.1. Авторизация

Компонент будет обеспечивать аутентификацию и авторизацию зарегистрированных пользователей и обеспечивать разграничение доступа к функциям компонента Веб-интерфейс в соответствии с ролью пользователя. Доступ к Веб-интерфейсу будет предоставляться пользователям, имеющим учетную запись ЕСИА или по логину/паролю. Предоставление функциональных возможностей будет осуществляться в соответствии с ролевой моделью. Будет реализована возможность:

- регистрация новых пользователей
- подтверждение регистрации новых пользователей с учетом информации о пользователе, стране нахождения пользователя и предполагаемого уровня доступа пользователя
- смены пароля пользователем
- подтверждение смены пароля пользователем
- группировки пользователей в рабочую группу

1.2. Личный кабинет

Модуль будет предоставлять автоматизированное рабочее место пользователя - веб интерфейс для обеспечения необходимых функций в соответствии с ролевой моделью. Предусмотрен интерфейс – Личный кабинет Администратора и Личный кабинет Пользователя, с соответствующим функционалом.

Личный кабинет Администратора

- возможность управления базовыми настройками интерфейса
- просмотр статистики работы модуля
- доступ к функциям разметки
- доступ к функциям сервера архивации
- возможность добавления/ограничения доступа к модулю
- размещение обучающих материалов

Личный кабинет Пользователя

- возможность управления базовыми настройками интерфейса
- отслеживание движения активов
- доступ к интерфейсам с информацией об адресе/владельце/транзакциям
- настройка уведомлений
- отслеживание подозрительных платежей
- доступ к функциям построения графов транзакций/контрагентов
- доступ к спискам владельцев/транзакций/адресов
- доступ к образовательной системе

1.3. Визуализация

Веб-интерфейс будет позволять доступ к следующим возможностям.

Поиск

Поиск адресов, поиск кошельков, владельцев кошельков. Поиск по транзакциям. Поиск BTC адресов по страницам в сети Интернет и TOR.

Для поиска в сети Интернет планируется использовать технологии, предоставляемые Яндекс.

Поиск в TOR выполняется на поисковых ресурсах, размещенных как в сети Интернет и имеющих шлюз в TOR (например, поисковый сервис DuckDuckGo), так и на ресурсах, размещенных в сети TOR (Ahmia, Candle, TorSearch, Caronte). Список поисковых ресурсов, размещенных в сети TOR будет формироваться автоматически с возможностью ручной корректировки.

Информация о кошельке

Информация о транзакциях, количество адресов. Информация о движениях на счету, сколько было потрачено/получено в BTC/USD. Динамика транзакций, баланса, риска.

Фильтр по дате.

Информация об Адресах

- получение **списка всех адресов кластера**, с возможностью их сортировки по:
 - свойствам (даты первых, входящих, последних, исходящих) транзакций,
 - количеству транзакций
 - объему полученных средств
 - остатку средств
 - риску адресов
 - остаточному риску адресов;
- получения всех транзакций кластера с возможностью сортировки по:
 - размеру
 - риску
 - наличию контрагентов в транзакциях
- обеспечения получения данных об адресе, в частности:
 - данные об обороте адреса с пересчетом сумм в долларах и рублях
 - получение риск-скоринга транзакций
 - отображение графиков изменения остатка на адресе
 - отображение графиков изменения приходящих на адрес средств.

Упоминание адресов

Упоминание кошелька в WEB и TOR

Список контрагентов

Список контрагентов с указанием названия, типа, оборота BTC/RUR/USD.

Круговая диаграмма с распределением входящих/исходящих контрагентов.

Фильтр по дате, обороту и типу контрагентов.

Список владельцев

Название, категория, тип владельца. Информация о кошельках.

Фильтр по категории, типу и названию владельцев.

Возможность экспортировать полученные данные в CSV файл.

Информация по владельцу

Возможность просматривать подробную информацию по каждому владельцу с учетом расчета оборота по BTC/RUR/USD.

Возможность фильтрации по времени начала работы, по последним исходящим транзакциям;

Возможность добавления, обновления и удаления данных о владельце.

Поиск по риску, по типу, по категориям, по названию;

Владелец
000 X

Тип
Exchange

Количество адресов
3

Количество транзакций
1 000

Баланс
19 199 BTC /
633 567 000 USD /
121 170 291 000 RUR

Информация

Всего транзакций

Всего получено: 1 040 344 BTC

Всего отправлено: 990 045 BTC

Время последней транзакции: 25.04.2021

Оценка рисков

15%

связь с игорным сервисом

Упоминания в сети

Тип упоминания

post

Адрес в сети

www.reddit.com

Баланс



■ bc1qpy9n7qm3fdpdrw70mpghl8lyn6wrwk565uyvrs
■ bc1qyhnmw6z06r9sp47sq7qzwrud5z0jwam5m29sz2
■ c1qpy9n7qm3fdpdrw70mpghl8rud5z0jwam5m29sz2

Адреса

Адрес	Баланс	Количество транзакций	Последняя активность
1qpy9n7qm3fdpdrw70mpghl8lyn6wrwk565uyvrs	15 500	900	25.04.2021 18:
1qyhnmw6z06r9sp47sq7qzwrud5z0jwam5m29sz2	3 499	90	25.04.2020 18:
qpy9n7qm3fdpdrw70mpghl8rud5z0jwam5m29sz2	200	10	25.04.2018 18:

Транзакции

Хэш	Дата/время	Адрес отправителя	Адрес получателя	Сумма
dde585b4a55f7d01ad42e7...	14.07.2021 15:30	c1qpy9n7qm3fdpdrw70mpghl8...	bc1qpy9n7qm3fdpdrw70mpgh...	0.00001000 BTC
GaxNCC2qzwpPfrq1Pre...	14.07.2021 15:30	c1qpy9n7qm3fdpdrw70mpghl8...	bc1qpy9n7qm3fdpdrw70mpgh...	0.00001000 BTC
dde585b4a55f7d01ad42e7...	14.07.2021 15:30	GaxNCC2qzwpPfrq1Pejlygi...	bc1qpy9n7qm3fdpdrw70mpgh...	0.00001000 BTC
GaxNCC2qzwpPfrq1Per...	14.07.2021 15:30	c1qpy9n7qm3fdpdrw70mpghl8...	bc1qpy9n7qm3fdpdrw70mpgh...	0.00001000 BTC
dde585b4a55f7d01ad42e7...	14.07.2021 15:30	c1qpy9n7qm3fdpdrw70mpghl8...	bc1qpy9n7qm3fdpdrw70mpgh...	0.00001000 BTC
dde585b4a55f7d01ad42e7...	14.07.2021 15:30	c1qpy9n7qm3fdpdrw70mpghl8...	bc1qpy9n7qm3fdpdrw70mpgh...	0.00001000 BTC

Возможный вариант интерфейса для страницы с информацией о контрагенте

Список транзакций

Фильтр по дате, сумме и типу транзакций.

Возможность экспортировать полученные данные в CSV файл.

Информация о транзакции

Возможность просмотреть информацию по каждой транзакции.

Графы

Модуль загружает требуемые данные, содержащие узлы и связи. Анализируемые данные преобразуются в граф, к которому предоставляется пользовательский интерфейс, позволяющий отображать узлы графа и передвигаться по связям между узлами.

Графы транзакций

Будет реализована возможность построить схему движения всех известных транзакций в виде графа, используя силовые алгоритмы визуализации графов. Каждый вход/выход транзакции представляет собой ноду, они соединены между собой линиями, на которых указана сумма и направление передачи средств в BTC.

Данные графа можно экспортировать в .CSV файл

Графы контрагентов

Представление контрагентов в виде графа со следующим функционалом:

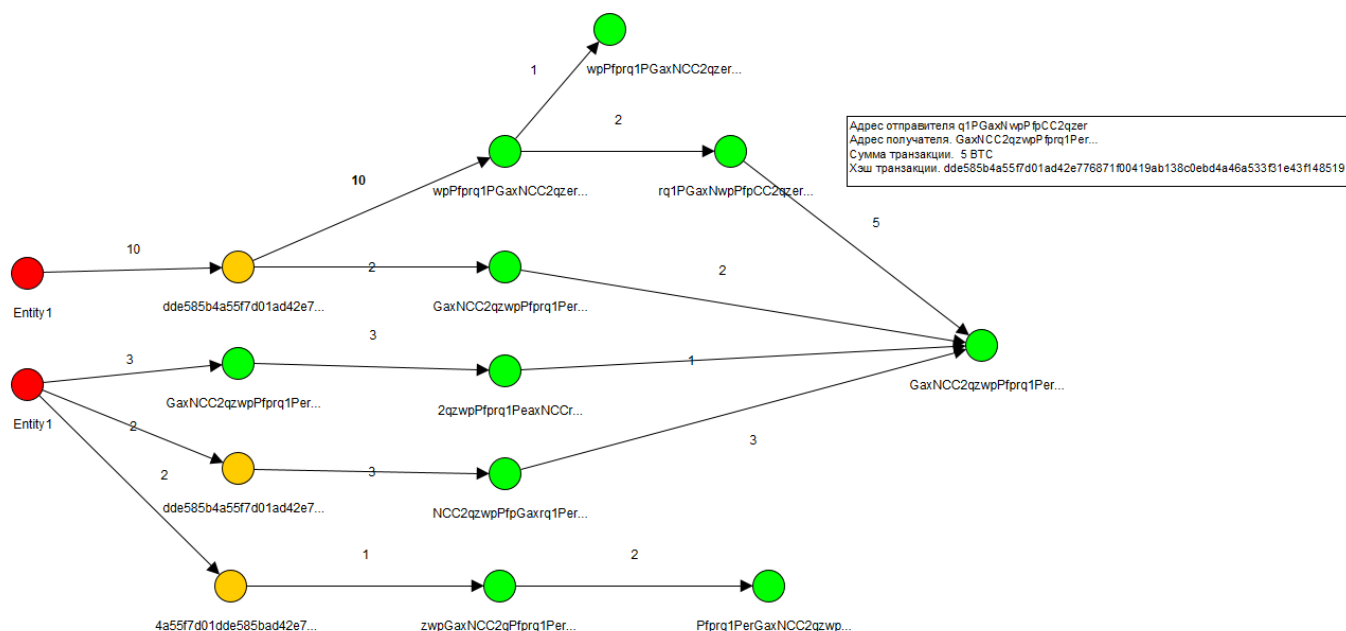
- отображение контрагентов (входящих и/или исходящих) выбранного адреса,
- отображение связей между контрагентами (входящими и/или исходящими) выбранного адреса,
- скрывание/отображение неизвестных контрагентов адреса,
- трейсинг входящих/исходящих транзакций с целью поиска известного адреса в ветви графа путем поиска кратчайшего, среднего и наибольшего путей между вершинами графа,
- отображение справочной информации по адресу/контрагенту при нажатии на узел графа и/или ребро графа.

Представление контрагентов в виде графа со следующим функционалом:

Нажатие на ноду открывает меню:

- Инфо - открывает страницу с информацией об адресе/кошельке.
- Раскрыть - добавляет на граф контрагентов выбранного адреса/кошелька и связи между ними.
- Раскрыть входы/выходы - добавляет на граф входящих/исходящих контрагентов выбранного адреса/кошелька и связи между ними.
- Трейсинг входов/выходов - по очереди раскрывает связи с наибольшим входящим/исходящим контрагентом, а также всем известным, которые встретились в процессе, до тех пор, пока не наткнется на известный адрес/кошелек.
- Свернуть неизвестные - скрывает неизвестных контрагентов адреса/кошелька.
- Удалить - удаляет ноду.

Данные графа можно экспортировать в .CSV файл или сохранить в виде статической ссылки.



Пример возможного отображения Графа для контрагентов

Система поддержки

На странице будут размещены обучающие материалы.

Поиск, автозаполнение

- Поиск адресов/кошельков в WEB и TOR
- поиск и автозаполнение по адресу;
- поиск и автозаполнение по названию владельца;
- проверка на существование адреса;
- проверка на существование транзакции;
- проверка на валидность адреса, которая определяет, создан ли адрес по правилам блокчейн биткоин;
- проверка на существование кластера.

1.4. Компонент уведомлений

Система личных кабинетов будет содержать систему отправки уведомлений на электронную почту или в мессенджер. Система будет отправлять сообщения при наступлении определенных событий. Преднастроенными событиями могут быть изменения выше пороговых значений по балансу объекта (адреса, кластера, сета, владельца), а также изменение пороговых значений по риску или появление транзакций, превышающих риск.

Пользователь в личном кабинете может настроить параметры автоматической отправки оповещений. Каждая группа обладает своим набором событий, которые служат поводом для отправки сообщения.

Система отправки уведомлений состоит из трёх подсистем: регистрации событий, отправки сообщений и конфигурации.

Подсистема регистрации событий следит за происходящими событиями и регистрирует их наступление. Для этого подсистема хранит список триггеров (представляющих собой набор параметров событий) и сравнивает все происходящие события с заданными шаблонами триггеров.

Подсистема отправки уведомлений предоставляет собой унифицированный высокоуровневый программный интерфейс между компонентами уведомлений и внешними системами, такими, как почтовые сервера, сервера мессенджеров и шлюзы SMS.

Подсистема конфигурации хранит конфигурацию и предоставляет программные интерфейсы для редактирования параметров хранимой конфигурации.

Кроме этого, будет организована возможность редактирования конфигурации пользователем и отправки уведомлений о наступлении событий из других подсистем модуля в компонент уведомлений.