

**Предложение участника открытого конкурса в электронной форме о  
«качественных, функциональных и об экологических» характеристиках объекта  
закупки в соответствии с критериями оценки заявок на участие в открытом  
конкурсе в электронной форме**

**Настоящим подтверждаем согласие на выполнение работ в полном соответствии с конкурсной документацией, техническим заданием и проектом государственного контракта, в том числе в соответствии со следующими требованиями:**

## **1 Полное наименование работ**

Выполнение работ по созданию модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина.

## **2 Цели выполнения работ по Контракту**

Работы по созданию модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина (далее – Модуль) направлены на достижение Федеральной службой по финансовому мониторингу (далее – Служба) следующих целей:

1. Повышение эффективности деятельности финансовых институтов как субъектов первичного финансового мониторинга, повышение уровня их законопослушности с учетом выявленных рисков отмывания доходов, полученных преступным путем, финансирования терроризма и экстремизма, финансирования распространения оружия массового уничтожения. Снижение рисков финансирования незаконного оборота наркотиков с использованием криптовалют в качестве платежного инструмента.
2. Обеспечение сохранности и целевого использования бюджетных средств.
3. Участие в декриминализации и повышении прозрачности отраслей реального сектора экономики с учетом выявленных рисков ОД.
4. Снижение рисков финансирования терроризма и экстремизма, а также рисков финансирования распространения оружия массового уничтожения.

Создание Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина Единой информационной системы Росфинмониторинга предназначено для решения следующих задач:

- обеспечено прослеживание цепочки перемещения цифровых финансовых активов;
- обеспечено ведение базы данных криптовалютных кошельков, связанных с осуществлением противоправной деятельности и финансированием терроризма и экстремизма, а также финансированием распространения оружия массового уничтожения ;
- обеспечен мониторинг поведения участников криптовалютного рынка с целью их идентификации, составления профилей участников и оценки их роли в экономической деятельности, а также выявления вероятности их участия в противоправной деятельности.

### 3 Состав и содержание работ

Для достижения целей, указанных в разделе 4 и решению вышеуказанных задач будут выполнены следующие работы:

- Доработан технический проект ЕИС Росфинмониторинга;
- Разработана Пояснительная записка на создание Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина ЕИС Росфинмониторинга;
- Выполнены работы по созданию Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина ЕИС Росфинмониторинга;
- Проведение опытной эксплуатации, актуализирована эксплуатационная документация.

Заказчик в течение 3-х рабочих дней со дня заключения государственного контракта передает Подрядчику 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).

На основании вышеуказанной документации и информации, а также с учетом требований к Модулю мониторинга и анализа криптовалютных транзакций с использованием биткоина Единой информационной системы Росфинмониторинга будет актуализовано общее техническое задание на ЕИС Росфинмониторинга.

Технический проект будет актуализирован в соответствии с требованиями, указанными в техническом задании.

По результатам выполнения работ Подрядчик предоставит актуализированную техническую документацию на ЕИС Росфинмониторинга:

- Общее техническое задание на ЕИС Росфинмониторинга;
- Описание комплекса технических средств ЕИС Росфинмониторинга.

По результатам выполнения работ будет проведена опытная эксплуатация. В рамках опытной эксплуатации Модуля будут проведены следующие виды тестирования:

1. Тестирование программно-аппаратной части.
2. Тестирование интерфейса пользователя.
3. Нагрузочное тестирование системы (~100 запросов в секунду, чтение и запись в базу данных).
4. Пентестинг (тестирование на проникновение и безопасность).



### 3.1 Содержание работ по созданию программной составляющей и функций Модуля мониторинга и анализа криптовалютных транзакций с использованием биткойна Единой информационной системы Росфинмониторинга

Модуль мониторинга и анализа криптовалютных транзакций с использованием биткойна является неотъемлемой частью Единой информационной системы в сфере ПОД/ФТЭ/ФРОМУ Федеральной службы по финансовому мониторингу (далее – ЕИС Росфинмониторинга).

Целевая функциональная структура ЕИС Росфинмониторинга направлена на эффективную автоматизацию деятельности Службы при выполнении ею государственных функций и задач и обеспечивает применение рабочего процесса ПОД/ФТЭ/ФРОМУ (сбор – систематизация и хранение – анализ – взаимодействие – обратная связь) в направлениях деятельности, связанной с анализом данных.

Реализация функциональной структуры предполагает использование стандартизированных ИТ-инструментов, а также развитие интерфейсов гибкого использования системы аналитиками без помощи разработчиков.

ЕИС Росфинмониторинга в целевом состоянии разделена на отдельные информационные контуры, предназначенные для организации взаимодействия и обработки информации, исходя из класса информации. В рамках контуров выделены пересекающиеся сегменты коммуникации, исходя из требований к защищенности самой ЕИС Росфинмониторинга и ее контрагентов.

В настоящее время ЕИС Росфинмониторинга состоит из 6 прикладных систем, которые включают в себя более 15 компонентов. Разрабатываемый Модуль мониторинга и анализа криптовалютных транзакций с использованием биткойна ЕИС Росфинмониторинга входит в состав Компонента информационного взаимодействия Подсистемы внешнего взаимодействия.

Основу Системы составляет серверный комплекс (сервер ноды блокчейна Биткойна, сервер разметки, сервер аналитики, сервер архивации, сервер поддержки веб-интерфейса пользователя).

**В целях создания Модуля мониторинга и анализа криптовалютных транзакций с использованием биткойна ЕИС Росфинмониторинга будут выполнены работы, обеспечивающие решение перечисленных задач:**

№ п/п	Задача	Работы
1	Создание сервера ноды блокчейна биткойна	Должна быть реализована возможность проводить мониторинг транзакций и предоставлять доступ к данным. Должна быть обеспечена возможность доработки с целью добавления функционала мониторинга состояния нод других криптовалют и определения, какая из них является инициатором той или иной транзакции.



№ п/п	Задача	Работы
2	Создание сервера разметки	<p><b>Требования, в части связи с нодой биткойна</b>  Должно быть реализовано взаимодействие с независимым модулем ноды биткойна</p> <p><b>Требования, в части парсера</b>  Должны быть реализованы следующие возможности:</p> <ul style="list-style-type: none"> <li>- исторического функционала парсинга, т.е. конвертации всего содержимого ноды биткойна в таблицы базы данных системы.</li> <li>- конвертации онлайн-разметки, включая мониторинг всех транзакций, ожидающих подтверждения в сети Биткойн, с точки зрения того, какая нода инициировала транзакцию, и других данных о транзакциях.</li> <li>- работы в фоновом режиме и переноса транзакций по мере их появления в списке на подтверждение и упаковки в блок в ноде мониторинга.</li> <li>- пересчета и разметки в режиме онлайн входов и выходов по текущему курсу биткойна на доллар и по текущему курсу биткойна на рубль, а также историческую разметку по тем же курсам.</li> </ul> <p>Должно быть размечено по типам принадлежности к распространителям адресов не менее 100 млн. адресов.</p> <p><b>Требования, в части кластеризации</b>  Должна быть реализована возможность, по мере добавления блоков в разметку базы данных, производить разметку кластеров в соответствии с алгоритмом кластеризации по общей трате с использованием алгоритма маркирования вершин.</p> <p><b>Требования, в части разметки</b>  Должна быть реализована возможность подсчета промежуточных и общих значений по каждому субъекту разметки, включая адреса, кластеры и владельцев адресов и кластеров, для выдачи предварительной разметки и проведения дальнейшей оперативной аналитики.</p> <p><b>Требования, в части хранения упоминаний</b>  Должны быть реализованы следующие возможности:</p> <ul style="list-style-type: none"> <li>- сохранение поступающей от поисковых модулей информации;</li> <li>- разметку поступающих упоминаний по принадлежности к определенным адресам.</li> </ul> <p><b>Требования, в части расчета риска</b>  Должна быть реализована возможность:</p> <ul style="list-style-type: none"> <li>- расчета и хранения исторически накопленного риска каждого адреса, кластера и владельца;</li> <li>- выполнения разметки по риску для дальнейшей аналитики;</li> <li>- расчета риска транзакций по методике.</li> </ul>



№ п/п	Задача	Работы
3	Создание сервера аналитики	<p><b>Требования, в части работы с транзакциями</b>  Должны быть реализованы следующие возможности:</p> <ul style="list-style-type: none"> <li>- выдача совокупной информации о транзакциях.</li> </ul> <p><b>Требования, в части работы с адресами</b>  Должна быть реализована возможность обеспечения получения данных об адресе, в частности данных об обороте адреса с пересчетом сумм в долларах и рублях, получение риск-скоринга транзакций, графиков изменения остатка на адресе, графиков изменения приходящих на адрес средств.</p> <p><b>Требования, в части работы с кластерами</b>  Должны быть реализованы следующие возможности:</p> <ul style="list-style-type: none"> <li>- получение списка всех адресов кластера, с возможностью их сортировки по датам первых, входящих, и последних, исходящих, транзакций, по количеству транзакций, по объему полученных средств, по остатку средств, по риску адресов, остаточному риску адресов;</li> <li>- выдача совокупного риска всего кластера, истории по риску кластера;</li> <li>- получение данных об одном адресе в нескольких режимах, в биткоинах, долларах или рублях, а также с учетом или без учета внутреннего оборота, который происходит внутри кластера;</li> <li>- получения всех транзакций кластера с возможностью сортировки по размеру, риску, наличию контрагентов в транзакциях.</li> </ul> <p><b>Требования, в части работы с владельцами</b>  Должны быть реализованы следующие возможности:</p> <ul style="list-style-type: none"> <li>- получение списка владельцев;</li> <li>- получение данных о конкретном владельце с учетом расчета оборота по биткоинам/рублям/долларам, с возможностью фильтрации как по времени начала работы, так и по последним исходящим транзакциям;</li> <li>- поиск по риску, по типу, по категориям, по названию;</li> <li>- добавление, обновление и удаление данных о владельце.</li> </ul> <p><b>Требования, в части поиска и автозаполнения</b>  Должны быть реализованы следующие возможности:</p> <ul style="list-style-type: none"> <li>- поиск и автозаполнение по адресу;</li> <li>- поиск и автозаполнение по названию владельца;</li> <li>- проверка на существование адрес;</li> <li>- проверка на существование транзакции;</li> <li>- проверка на валидность адреса, которая определяет, создан ли адрес по правилам блокчейн биткоин;</li> <li>- проверка на существование кластера.</li> </ul>
4	Создание сервера архивации	<p>Должен обеспечивать резервирование БД Системы, ведение журнала запросов, а также истории изменений данных.</p>



№ п/п	Задача	Работы
5	Создание сервера поддержки веб интерфейса пользователя	<p><b>Требования, в части авторизации</b>  Должны быть реализованы следующие возможности:</p> <ul style="list-style-type: none"> <li>- авторизация, в том числе с использованием системы ЕСИА;</li> <li>- подтверждение и обновление пароля;</li> <li>- подтверждение регистрации с учетом субъекта, страны, и уровня доступа.</li> </ul> <p><b>Требования, в части веб-интерфейса</b>  Должна быть реализована возможность должен поддержки системы личных кабинетов. Система личных кабинетов предназначена для обеспечения и управления доступом пользователя к санкционированным данным, которые могут быть организованы в иерархию для хранения следующих видов информации:</p> <ul style="list-style-type: none"> <li>- Ссылки на объекты системы.</li> <li>- Ссылки на построенные графы.</li> <li>- Разметки, которая отражается только у него по запросу.</li> <li>- Рабочих групп.</li> <li>- Аггегированных объектов (например, адреса, кошелек и владельцы).</li> </ul> <p>Должна быть обеспечена настройка следующих параметров пользовательского интерфейса:</p> <ul style="list-style-type: none"> <li>- Даты и времени;</li> <li>- Типа отображения графа;</li> <li>- Языка интерфейса;</li> <li>- Выбор вида валюты.</li> </ul> <p>Система личных кабинетов должна обеспечивать следующую иерархию:</p> <ol style="list-style-type: none"> <li>1. Пользователь;</li> <li>2. Рабочая группа.</li> </ol> <p>Система личных кабинетов должна содержать систему уведомлений на почту или в мессенджер о преднастроенных событиях. Преднастроенными событиями могут быть изменения выше пороговых значений в одну и другую сторону по балансу объекта (адреса, кластера, сета, владельца), а также изменение пороговых значений по риску или появление транзакций, превышающих риск.</p>



## **3.2 Параметры основного аппаратно-программного модуля и интерфейса**

### **3.2.1 Параметры основного аппаратно-программного модуля**

При создании Системы должна использоваться операционная система семейства Linux;

Система будет развертываться на следующих серверах (ориентировочные характеристики):

1. Сервер 1 (сервер ноды блокчейна биткойна):
  - Аппаратные требования: Xeon 2.3 ГГц, 16 ядер, 64gb RAM, 400gb SSD;
2. Сервер 2 (сервер разметки):
  - Аппаратные требования: Xeon 2.3 ГГц, 32 ядра, 512gb RAM, 4TB SSD;
3. Сервер 3 (сервер аналитики и сервер поддержки веб-интерфейса):
  - Аппаратные требования: Xeon 2.3 ГГц, 32 ядра, 512gb RAM, 8TB SSD;
4. Сервер 4 (сервер архивации):
  - Аппаратные требования: Xeon 2.3 ГГц, 32 ядра, 512gb RAM, 192TB HDD.

### **3.2.2 Интерфейс пользователя**

Интерфейс пользователя позволит аналитику выполнять работу по установке связей между субъектами криптовалютных транзакций, отслеживанию движения активов и представление результатов в графическом и табличном виде. Интерфейс будет выполнен в виде веб-интерфейса с поддержкой браузеров:

- Mozilla Firefox;
- Chrome;
- Yandex.

#### **5.2.2.1 Общие требования к интерфейсу:**

##### **а) Интерфейс авторизации**

Для входа в систему путем ввода логина и пароля, в том числе с использованием системы ЕСИА

##### **б) Интерфейс поиска**

Для поиска адресов, кошельков и владельцев в системе.

##### **в) Интерфейс информации**

Для формирования свода информации об адресе/кошельке:

1. Название;
2. Тип;
3. Количество адресов;
4. Количество транзакций;
5. Риск;
6. Первое и последнее упоминание;
7. Всего получено и потрачено BTC/USD;
8. Остаток BTC/USD;
9. Распределение транзакций;
10. Топ входящих/исходящих контрагентов:
  - а) Контрагент;
  - б) Сумма;



11. Топ входящих/исходящих транзакций:

- а) Дата;
- б) Хэш;
- с) Сумма;

12. Динамика входящих/исходящих транзакций;

13. Динамика баланса;

14. Динамика риска;

15. Упоминания:

- а) Заголовок;
- б) Текст упоминания;
- с) Ссылка.

К данным на странице можно применить фильтр по дате.

г) Интерфейс основных контрагентов

Для составления списков контрагентов кошелька или владельца, а также получения сводной информации о категориях, типах или конкретных владельцах-контрагентах.

Страница отображает полный список контрагентов кошелька/адреса, их название, тип и оборот в BTC, а также распределение входящих/исходящих контрагентов на круговой диаграмме. К данным на странице можно применить фильтр по дате, обороту и типу контрагентов.

Данные таблицы можно экспортировать в .CSV файл.

д) Интерфейс упоминания адресов

Для отображения списка упоминаний кошелька:

- 1. Адрес (название, тип);
- 2. Заголовок;
- 3. Текст упоминания;
- 4. Ссылка.

е) Интерфейс списков транзакций

Для отображения списка транзакций кошелька/адреса:

- 1. Дата и время;
- 2. Хэш;
- 3. Риск;
- 4. Сумма в BTC;
- 5. Список входов и выходов транзакции.

К данным на странице можно применить фильтр по дате, сумме и типу транзакций. Данные таблицы можно экспортировать в CSV файл.

ж) Интерфейс информации о транзакциях

Для отображения информации о транзакции:

- 1. Блок;
- 2. Дата и время;
- 3. Сумма;
- 4. Список входов и выходов транзакции с описанием названия и типа адреса/кошелька, если таковое имеется;



## 5. Риск.

### з) Интерфейс построения графов транзакций

Для отображения графа транзакции.

Каждый вход/выход транзакции представляет собой ноду, они соединены между собой линиями, на которых указана сумма и направление передачи средств в BTC.

Нажатие на ноду открывает меню:

- «Инфо» - открывает страницу с информацией об адресе.

Нажатие на связь открывает меню:

- «Инфо» - открывает страницу с информацией о транзакции;
- «Раскрыть» - добавляет на граф ноды и связи, входящие в транзакцию;
- «Раскрыть входы/выходы» - добавляет на граф ноды и связи, являющиеся входами/выходами транзакции;
- «Удалить» - удаляет связь и связанные с ними ноды.

Нажатие на «связь» открывает таблицу с описанием:

- Адреса отправителя;
- Адреса получателя;
- Суммы транзакции;
- Хэша транзакции.

В правом меню можно изменять тип графа. Данные графа можно экспортировать в .CSV файл или сохранять в виде статической ссылки.

### и) Интерфейс адреса

Для отображения списка адресов кошелька:

1. Адрес;
2. Тип;
3. Название;
4. Риск;
5. Баланс (BTC);
6. Оборот (BTC);
7. Количество транзакций;
8. Количество упоминаний.

К данным на странице можно применить фильтр по дате, балансу и обороту адресов. Данные таблицы можно экспортировать в CSV файл.

### к) Интерфейс построения графов контрагентов

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.

Нажатие на связь открывает таблицу с описанием:

- Адреса отправителя.
- Адреса получателя.
- Суммы транзакции.
- Хэша транзакции.

Данные можно отфильтровать по дате и сумме транзакций.

В правом меню можно изменять тип графа. Данные графа можно экспортировать в .CSV файл или сохранить в виде статической ссылки.

#### л) Интерфейс списка владельцев

Для отображения списка владельцев с указанием:

1. Названия;
2. Категории;
3. Типа;
4. Количества кошельков.

Данные можно отфильтровать категории, типу и названию владельцев. Данные графа можно экспортировать в CSV файл.

#### м) Интерфейс информации об отдельном владельце

Для отображения подробной информации об адресе/кошельке, с указанием:

1. Названия.
2. Типа.
3. Категории.
4. Количества адресов.
5. Количества кошельков.
6. Количества транзакций.
7. Уровня риска.
8. Первого и последнего упоминания.
9. Поступившей и выведенной суммы в BTC/USD.
10. Остаток в BTC/USD.
11. Распределения транзакций.
12. Списка юридических лиц:
  - а) Номер;
  - б) Названия;
  - в) Страна;
  - г) Домен;
  - д) Лицензия;
  - е) Адрес;
13. Списка сайтов:
  - а) Сайт;
  - б) IP;
  - в) Страна;
14. Страницы и профили в Интернете:



- a) Ссылка;
- b) Домен;
- 15. Кошельков:
  - a) Кошелек;
  - b) Баланс (BTC);
  - c) Оборот;
  - d) Адресов;
  - e) Транзакций;
  - f) Первое упоминание;
  - g) Последнее упоминание;
- 16. Адреса:
  - a) Адрес;
  - b) Баланс (BTC);
  - c) Оборот;
  - d) Транзакции;
  - e) Первое упоминание;
  - f) Последнее упоминание;
- 17. Упоминания:
  - a) Заголовок;
  - b) Текст упоминания;
  - c) Ссылка;
- 18. Динамика риска.

**н) Интерфейс интернет-поиска**

Позволяет осуществлять поиск BTC адресов по страницам в сети Интернет и Тор. Функционирует в двух режимах: поиск по ссылкам, поиск по запросу. Поиск по ссылкам осуществляет поиск BTC адресов на страницах, указанных в запросе (через запятую). Поиск по запросу осуществляет поиск адресов по поисковому запросу из поля Запрос в Яндексе (Первые 100 или 200 результатов).

Полученные данные выводятся в таблицу с указанием:

1. Адреса (название, тип);
2. Ссылки.

**3.2.3 Система образования и поддержки**

Система образования и поддержки будет представлять собой перечень обучающих мультимедийных материалов. Доступ к системе осуществляется через учетную запись пользователя.

**3.2.4 Система доступов**

Администратор будет иметь возможность управления базовыми настройками веб-интерфейса, просмотра статистики, иметь доступ к функциям разметки.

## **4 Срок, место и условия выполнения работ**

### **4.1 Сроки выполнения работ**

Сроки выполнения работ определены в Календарном плане выполнения работ (Приложение № 2 к Контракту)

### **4.2 Место и условия выполнения работ**

Работы по созданию Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина ЕИС Росфинмониторинга и актуализации документации выполняются на территории Подрядчика, за исключением работ, связанных с обработкой сведений ограниченного распространения. Перечень таких работ определяется Заказчиком.

Заказчик обеспечивает доступ специалистов Подрядчика на территорию выполнения работ в соответствии с установленным в Федеральной службе по финансовому мониторингу порядком на основании обоснованного письменного запроса Подрядчика.

Для допуска каждого специалиста Подрядчик предоставляет Заказчику следующие сведения: фамилия, имя, отчество, копия паспорта.

Специалисты Подрядчика в течение 3 (трех) рабочих дней с момента согласования Заказчиком их состава проходят ознакомление с нормативными правовыми актами, устанавливающими правила обращения со сведениями (информацией), и подписывают Обязательство.

Для выполнения работ по созданию Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина ЕИС Росфинмониторинга и актуализации документации на территории Заказчика, Заказчик предоставляет Подрядчику обоснованное количество рабочих мест и инфраструктуру (программные и технические средства разработки и документирования), исходный код и необходимую документацию.

## **5 Порядок приемки работ, требования к результатам работ и отчетным документам**

### **5.1 Общие требования к приемке работ**

**5.1.1** Приемка работ осуществляется по этапам Календарного плана выполнения работ (Приложение № 2 к Контракту).

**5.1.2** Приемка работ осуществляется Комиссией по согласованию технического задания и приемке результатов закупки товаров, работ, услуг, предметом которых являются создание, развитие, модернизация и эксплуатация подсистем и компонентов Единой информационной системы Росфинмониторинга, в порядке, оговоренном Контрактом.

**5.1.3** Все виды испытаний проводятся на территории Росфинмониторинга.

### **5.2 Требования к документации**

**5.2.1** Разрабатываемая техническая документация будет выполнена на русском языке.

**5.2.2** Структура и содержание технической документации будут соответствовать требованиям ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы» и удовлетворять требованиям Приложения № 1 к Регламенту внедрения и сопровождения программных систем Федеральной службы по финансовому мониторингу № 02-00-06/13505 от 29.06.2015 (предоставляется Заказчиком).



- 5.2.3 Документы оформлены на листах формата А4 без рамки, основной надписи и дополнительных граф к ней, без шифра (номера документа).
- 5.2.4 Правила оформления документов предварительно согласованы с Заказчиком.
- 5.2.5 Документы предоставляются Заказчику в бумажном (1 экземпляр), а также в электронном виде на оптическом носителе (1 экземпляр).

## **6 Требования к сроку гарантийных обязательств по Контракту**

- 6.1 Срок гарантийных обязательств на результаты выполненных работ составляет 12 (двенадцать) месяцев со дня подписания Акта сдачи-приемки выполненных работ по последнему этапу Контракта.

**Детализация предложения участника закупки по выполнению работ по каждой задаче разработки программной составляющей и функций Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина**

**1.1 Содержание работ по актуализации Технического проекта третьей очереди ЕИС Росфинмониторинга**

На данном этапе Заказчик в течение 3-х рабочих дней со дня заключения государственного контракта передает Подрядчику комплект документов, содержащий информацию о текущем состоянии программной, технической составляющей и архитектуре единой информационной системы (далее – ЕИС) Росфинмониторинга, а также необходимые для выполнения работ документы (исходные коды, ранее разработанные частные технические задания и общее техническое задание).

На основании вышеуказанной документации и информации будет актуализован Технический проект третьей очереди ЕИС Росфинмониторинга в соответствии с нижеперечисленным и стандартами:

- Межгосударственные стандарты ГОСТ 34.601–90, ГОСТ 34.201–89, ГОСТ 34.602–89, ГОСТ 34.603–92, ГОСТ 19.101–77, ГОСТ 19.503–79, ГОСТ 7.79–2000, ГОСТ 34.003–90, ГОСТ Р ИСО 15704–2008, ГОСТ Р ИСО/МЭК 15288–2005, ГОСТ 19.102–77, ГОСТ Р ИСО 21500, ГОСТ Р 54871–2011, ГОСТ Р 54869–2011, ГОСТ 12.1.030–81, ГОСТ 15150–69, ГОСТ 21958–76, ГОСТ Р 50922–2006, ГОСТ 27331–89, ГОСТ Р 51732–2001, ГОСТ Р ИСО 9001–2015, ГОСТ 10434–82, ГОСТ Р 51778–2001, ГОСТ Р ИСО 14001–2015, ГОСТ 12.2.003–91, ГОСТ Р 50571.22–2000;
- Санитарные (санитарно-эпидемиологические) правила (СП), нормы (СН), правила и нормы СанПин 2.2.2.542–96, СанПиН 2.2.2/2.4.1340–03, СНиП 23–01–99, СНиП 3.05.06–85, СНиП 23–05–95;
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР–К);
- Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Гостехкомиссии России от 30.03.1992);
- Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. Решением Гостехкомиссия России от 30.03.1992);
- Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Гостехкомиссии России от 25.07.1997);
- Нормативно–технический документ «Требования к системам обнаружения вторжений» (утв. приказом ФСТЭК России от 6.12.2011 № 638);
- Нормативно–технический документ «Требования к средствам антивирусной защиты» (утв. приказом ФСТЭК России от 20.03.2012 № 28);
- Нормативно–технический документ «Требования к средствам электронной подписи» (утв. приказом ФСБ России от 27.12. 2011 № 796);



- Нормы пожарной безопасности НПБ 88–2001 «Установки пожаротушения и сигнализации. Нормы и правила проектирования»;
- ТУ 3434–001–72059230–2005 «Щит распределительный».

Технический проект будет актуализирован в части создания нового Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина.

В техническом проекте будут описаны режимы функционирования.

Технический проект будет отражать распределение компонентов на аппаратных ресурсах ЕИС Росфинмониторинга.

По результатам выполнения работ Подрядчик представит актуализированный технический проект на создание ЕИС Росфинмониторинга.

## 1.2 Содержание работ по созданию программной составляющей и функций Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина Единой информационной системы Росфинмониторинга

Модуль мониторинга и анализа криптовалютных транзакций с использованием биткоина (далее – Система) является неотъемлемой частью Единой информационной системы в сфере ПОД/ФТЭ/ПРОМУ Федеральной службы по финансовому мониторингу (далее – ЕИС Росфинмониторинга).

Целевая функциональная структура ЕИС Росфинмониторинга направлена на эффективную автоматизацию деятельности Службы при выполнении ею государственных функций и задач и обеспечивает применение рабочего процесса ПОД/ФТЭ/ПРОМУ (сбор – систематизация и хранение – анализ – взаимодействие – обратная связь) в направлениях деятельности, связанной с анализом данных.

Реализация функциональной структуры предполагает использование стандартизированных ИТ-инструментов, а также развитие интерфейсов гибкого использования системы аналитиками без помощи разработчиков.

ЕИС Росфинмониторинга в целевом состоянии разделена на отдельные информационные контуры, предназначенные для организации взаимодействия и обработки информации, исходя из класса информации. В рамках контуров выделены непересекающиеся сегменты коммуникации, исходя из требований к защищенности самой ЕИС Росфинмониторинга и ее контрагентов.

В настоящее время ЕИС Росфинмониторинга состоит из 6 прикладных систем, которые включают в себя более 15 компонентов. Разрабатываемый Модуль мониторинга и анализа криптовалютных транзакций с использованием биткоина ЕИС Росфинмониторинга входит в состав Компонента информационного взаимодействия Подсистемы внешнего взаимодействия.

Основу Системы будет составлять серверный комплекс, состоящий из следующих компонент:

- Сервер ноды блокчейна биткоина;
- Сервер разметки;
- Сервер аналитики;
- Сервер архивации;
- Сервер поддержки веб интерфейса пользователя.

Предварительная архитектура Системы представлена на рисунке 1.



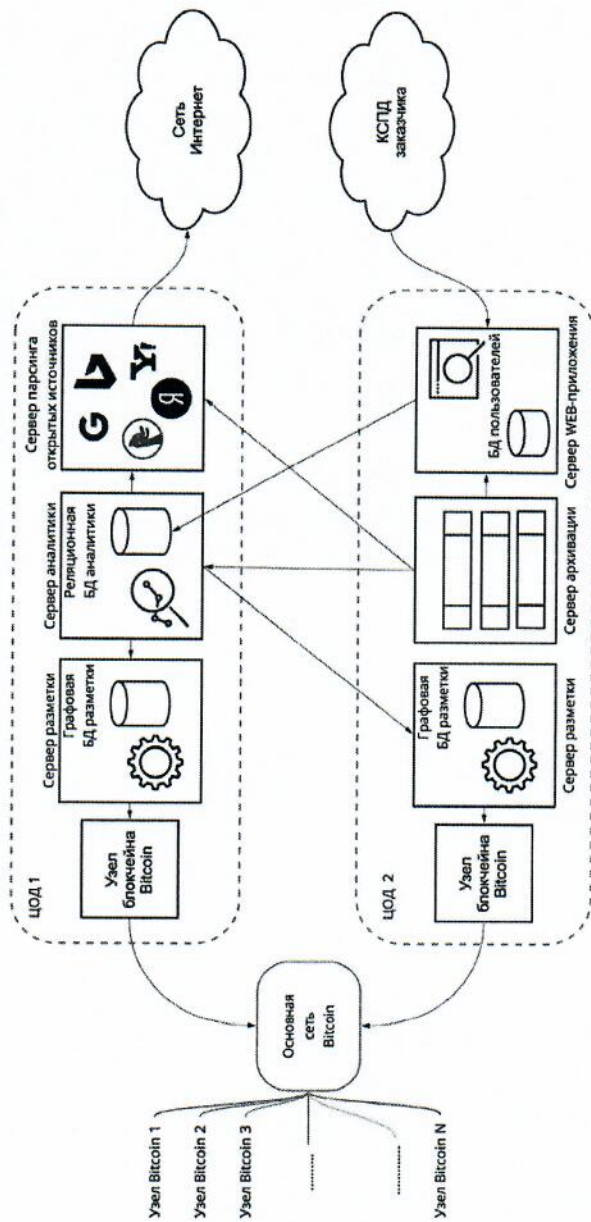


Рисунок 1. Предварительная архитектура Системы

В целях создания Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина ЕИС Росфинмониторинга будут выполнены следующие работы, обеспечивающие решение перечисленных задач:

Сервер	№ п/п	Задача	Очередь разработки ПО
Сервер ноды блокчейна биткоина	1	Обеспечение получения данных (мониторинга) блокчейна биткоина	1-я очередь
	1.1	<p>Получение данных о транзакциях сети Биткоина</p> <p>Будут реализованы следующие возможности:</p> <ul style="list-style-type: none"> <li>- Сбор данных.</li> <li>- Обработка данных.</li> <li>- Просмотр данных.</li> </ul>	

Сервер	№ п/п	Задача	Очередь разработки ПО
Создание сервера разметки	1.2	<b>Получение данных о блоках сети Биткойна</b> Будут реализованы следующие возможности: - Сбор данных. - Обработка данных. - Просмотр данных.	
	1.3	<b>Получение параметров сети Биткоин</b> Будут реализованы следующие возможности: - Сбор данных. - Обработка данных. - Просмотр данных.	
	2	<b>Обеспечение обработки данных</b>	
	2.1	<b>Информационное взаимодействие с независимым модулем ноды биткойна</b> Будут реализованы следующие возможности: - Сбор данных. - Просмотр данных.	1-я очередь
	2.2	<b>Парсинг данных</b> Будут реализованы следующие возможности: - Конвертация всех данных содержимого ноды биткойна в таблицы базы данных системы. - Конвертация онлайн-разметки. - Работа в фоновом режиме и перенос транзакций. - Пересчет и разметка в режиме онлайн входов и выходов по текущему курсу биткойна на доллар и по текущему курсу биткойна на рубль.	
	2.3	<b>Кластеризация данных</b> Будет реализована возможность разметки кластеров в соответствии с алгоритмом кластеризации по общей траге.	



Сервер	№ п/п	Задача	Очередь разработки ПО
Создание сервера аналитики	2.4	<b>Хранение данных</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Сохранение поступающей от поисковых модулей информации.</li> <li>- Разметка поступающих упоминаний по принадлежности к определенным адресам.</li> </ul>	
	2.5	<b>Расчет рисков</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Расчет и хранение исторически накопленного риска каждого адреса, кластера и владельца.</li> <li>- Выполнения разметки по риску для дальнейшей аналитики.</li> <li>- Расчет и хранение риска транзакций.</li> </ul>	
	3	<b>Обеспечение детального анализа данных и формирование выводов</b>	1-я очередь
	3.1	<b>Работа с транзакциями</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Выдача совокупной информации о транзакциях.</li> <li>- Хранение совокупной информации о транзакциях.</li> <li>- Просмотр совокупной информации о транзакциях.</li> </ul>	
	3.2	<b>Работа с адресами</b> Будет реализована возможность обеспечения получения данных об адресе.	
	3.3	<b>Работа с кластерами</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Получение списка всех адресов кластера.</li> <li>- Выдача совокупного риска всего кластера, истории по риску кластера.</li> <li>- Получение данных об одном адресе в нескольких режимах.</li> <li>- Получения всех транзакций кластера с возможностью сортировки по размеру, риску, наличию контрагентов в транзакциях.</li> </ul>	

Сервер	№ п/п	Задача	Очередь разработки ПО
	3.4	<b>Работа с владельцами</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Получение списка владельцев.</li> <li>- Получение данных о конкретном владельце с учетом расчета оборота по биткоинам/рублям/долларам.</li> <li>- Добавление, обновление и удаление данных о владельце.</li> </ul>	
	3.5	<b>Поиск и автозаполнение</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Поиск и автозаполнение по адресу.</li> <li>- Поиск и автозаполнение по названию владельца.</li> <li>- Проверка на существование адрес.</li> <li>- Проверка на существование транзакции.</li> <li>- Проверка на валидность адреса, которая определяет, создан ли адрес по правилам блокчейн биткоин.</li> <li>- Проверка на существование кластера.</li> </ul>	
	4	<b>Обеспечение архивации данных</b>	1-я очередь
Создание сервера архивации	4.1	<b>Резервирование базы данных</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Сохранение данных.</li> <li>- Хранение данных.</li> <li>- Просмотр данных.</li> </ul>	
	4.2	<b>Ведение журнала запросов</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Создание запроса.</li> <li>- Обработка запроса.</li> <li>- Сохранение информации о запросе.</li> <li>- Хранение информации о запросе.</li> <li>- Просмотр информации о запросе.</li> </ul>	



Сервер	№ п/п	Задача	Очередь разработки ПО
	4.3	<b>Ведение истории изменений данных</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Сохранение информации о изменениях.</li> <li>- Хранение информации о изменениях.</li> <li>- Просмотр информации о изменениях.</li> </ul>	
Создание сервера поддержки веб интерфейса пользователя	5	<b>Обеспечение обмена данными с пользователем</b> Будут реализованы следующие веб интерфейсы для пользователей Системы: <ul style="list-style-type: none"> <li>- Интерфейс авторизации.</li> <li>- Интерфейс поиска.</li> <li>- Интерфейс информации.</li> <li>- Интерфейс основных контрагентов.</li> <li>- Интерфейс упоминания адресов.</li> <li>- Интерфейс списков транзакций.</li> <li>- Интерфейс информации о транзакциях.</li> <li>- Интерфейс построения графов транзакций.</li> <li>- Интерфейс адреса.</li> <li>- Интерфейс построения графов контрагентов.</li> <li>- Интерфейс списка владельцев.</li> <li>- Интерфейс информации об отдельном владельце.</li> <li>- Интерфейс интернет-поиска.</li> </ul>	1-я очередь

### 1.2.1 Сервер ноды блокчейна биткоина

На рисунке 1 схематично представлено назначение и задачи Сервера ноды блокчейна биткоина.



Рисунок 2. Назначение и задачи сервера ноды блокчейна биткоина

Сервер ноды блокчейна биткоина предназначен для осуществления информационного взаимодействия (обмена данными) Системы с блокчейном биткоина. Сервер позволит проводить мониторинг транзакций и получать данные из блокчейна биткоина.

Сервер будет получать и обрабатывать следующие данные:

- Данные по транзакциям блокчейна биткоина;
- Данные по блокам блокчейна биткоина;
- Данные по адресам/кошелькам блокчейна биткоина;
- Общие параметры сети блокчейна биткоина.

Сервер будет обеспечивать возможность получения следующего состава данных по транзакциям:

- Блок транзакции;
- Дата проведения транзакции;
- Время проведения;
- Сумма транзакции в BTC;
- Сумма транзакции в долларах (по курсу Coinbase и/или Binance);
- Сумма транзакции в рублях (по курсу Coinbase и/или Binance);
- Список входов и выходов транзакции с описанием названия и типа адреса/кошелька;
- Размер комиссии транзакции;
- Хэш транзакции.

Сервер будет обеспечивать возможность получения следующего состава данных по блокам сети:

- Номер блока;
- Время регистрации блока в сети;
- Информация о майнере, который добыл блок включая:
  - o IP адрес;
  - o версия ПО;
  - o тип узла.



- Размер блока.

Сервер будет обеспечивать возможность получения следующего состава параметров сети биткоин:

- Скорость хэширования;
- Количество транзакций (за последние 24 часа);
- Объем транзакций (за последние 24 часа);
- Общий размер блокчейна.

Алгоритм взаимодействия с сервером ноды блокчейна биткоина будет поддерживать возможность доработки с целью добавления функционала мониторинга состояния нод других криптовалют и определения, какая из них является инициатором той или иной транзакции.

Будет обеспечена возможность доработки сервера с целью получения следующего состава данных по транзакциям других криптовалют:

- Блок транзакции;
- Дата проведения транзакции;
- Время проведения транзакции;
- Сумма транзакции в криптовалюте;
- Сумма транзакции в долларах (по курсу Coinbase и/или Binance);
- Сумма транзакции в рублях (по курсу Coinbase и/или Binance);
- Список входов и выходов транзакции с описанием названия и типа адреса/кошелька;
- Размер комиссии транзакции;
- Хэш транзакции.

Будет возможность доработки сервера с целью получения следующего состава данных по блокам:

- Номер блока;
- Время регистрации блока в сети;
- Информация о майнере, который добыл блок включая:
  - o IP адрес;
  - o версия ПО;
  - o тип узла.
- Размер блока.

Развертывание сервера ноды блокчейна биткоина будет осуществляться на сервере со следующими аппаратными требованиями:

- Xeon 2.3 ГГц, 16 ядер, 64gb RAM, 400gb SSD.

Представленный в настоящем разделе состав данных может быть изменен на этапе «Доработки технического проекта ЕИС Росфинмониторинга» по требованию Заказчика.

### **1.2.2 Сервер разметки**

На рисунке 2 схематично представлено назначение и задачи Сервера разметки.

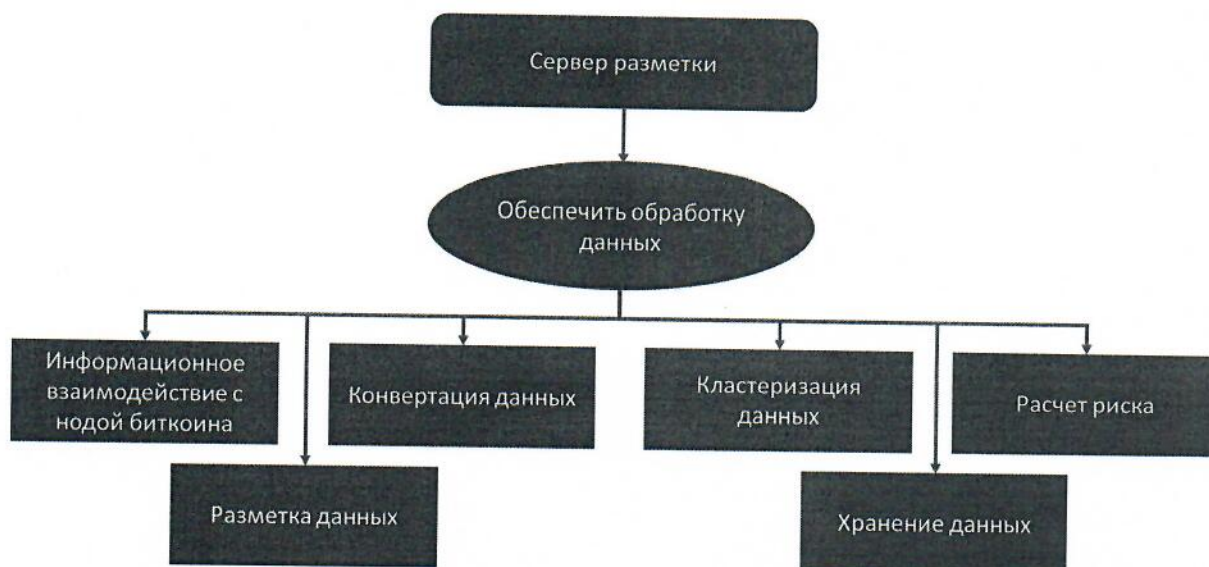


Рисунок 3. Назначение и задачи сервера разметки

Сервер разметки предназначен для детальной обработки и адаптации данных блокчейна биткоина для Системы (в частности для базы данных Системы).

Сервер разметки будет обеспечивать следующие возможности:

- Информационное взаимодействие (связь, обмен данными) с независимым модулем ноды биткоина;
- Парсинг данных;
- Кластеризация данных;
- Разметка данных;
- Хранение данных;
- Расчет основных параметров потенциальных рисков.

#### **Информационное взаимодействие (связь, обмен данными) с независимым модулем ноды биткоина**

Функция обмена данными с независимым модулем ноды биткоина будет обеспечивать возможность получения данных ноды биткоина с целью использования данной информации для дальнейшей разметки и аналитики. Сервер разметки будет принимать информацию по:

- Транзакциям блокчейна;
- Блокам блокчейна;
- Основным параметрам сети блокчейна.

Детальный состав данных по блокчейну биткоина, которые будут приниматься данной функцией представлен в разделе 1.2.1 настоящего документа.

Окончательный состав данных может быть изменен на этапе «Доработки технического проекта ЕИС Росфинмониторинга» по требованию Заказчика.

#### **Парсинг данных**

Функция парсинга данных будет обеспечивать следующие возможности:

- конвертацию всех данных содержимого ноды биткоина в таблицы базы данных системы (исторический функционал парсинга). Таким образом будет обеспечена возможность преобразования данных в части:
  - формата данных;
  - объединения схожих по типу/виду данных.



- конвертации онлайн-разметки, включая мониторинг всех транзакций, ожидающих подтверждения в сети Биткоин, с точки зрения того, какая нода инициировала транзакцию, и других данных о транзакциях.
- работы в фоновом режиме и переноса транзакций по мере:
  - o их появления в списке на подтверждение;
  - o упаковки в блок в ноде мониторинга.
- пересчета и разметки в режиме онлайн входов и выходов:
  - o по текущему курсу биткоина на доллар (по курсу Coinbase и/или Binance);
  - o по текущему курсу биткоина на рубль (по курсу Coinbase и/или Binance);
  - o историческую разметку по тем же курсам (доллара и рубля, по курсу Coinbase и/или Binance).

### **Кластеризация данных**

Функция кластеризации будет обеспечивать возможность производить автоматическую разметку кластеров, при этом:

- для реализации данной функции будет, в том числе, использоваться алгоритм кластеризации по общей трате с использованием алгоритма маркирования вершин;
- кластеризация будет осуществляться по мере добавления блоков в разметку базы данных.

Одна из основных задач функции кластеризации - возможность объединения в один кластер транзакций, в отношении которых была осуществлена попытка сокрытия истинного объема транзакции путем применения технологии “миксеров”, состоящей в том, что вместо одной транзакции от А к В осуществляются одна или несколько транзакций от А к миксеру М, который разделяет их по объему и времени на множество более мелких транзакций от М к В; все эти транзакции должны быть автоматически занесены в один кластер.

### **Разметка данных**

Функция будет обеспечивать возможность производить разметку данных для обеспечения эффективной работы других алгоритмов Системы, включая:

- алгоритм расчета риска;
- анализа данных.

При этом для реализации данной функции в т.ч. выдачи предварительной разметки и проведения дальнейшей оперативной аналитики будет реализованы следующие возможности:

- подсчета промежуточных значений по каждому субъекту разметки, включая:
  - o адреса;
  - o кластеры;
  - o владельцев адресов;
  - o владельцев кластеров.
- подсчета общих значений по каждому субъекту разметки, включая:
  - o адреса;
  - o кластеры;
  - o владельцев адресов;
  - o владельцев кластеров.

### **Хранение данных**

Функция хранения упоминаний будет обеспечивать следующие возможности:

- сохранения поступающей от поисковых модулей информации с возможностью бессрочного хранения данной информации;
- разметку поступающих упоминаний по принадлежности к определенным адресам.

## Расчет потенциальных рисков

Функция расчета риска будет обеспечивать следующие возможности:

- расчет риска с учетом:
  - потенциально неправоверных операций/ активностей;
  - связей с адресами/кошельками/владельцами, которые имеют высокий уровень риска (потенциальные злоумышленники);
  - расчет риска будет производиться для следующих групп:
    - адреса;
    - кластера;
    - владельца.
  - специализированных подходов и алгоритмов расчета и оценки риска, которые будут разработаны и зафиксированы в «Методики расчета потенциальных рисков в сфере криптовалютных операций».
- хранения исторически накопленного риска включая:
  - хранение изменения уровня риска;
  - хранение наиболее значимых операций/ действий, которые повлияли на уровень риска;
  - хранение исторической информации для следующих групп:
    - адреса;
    - кластера;
    - владельца.
- выполнения разметки по риску для дальнейшей аналитики;
- расчета риска транзакций с учетом:
  - потенциально неправоверных операций/ активностей;
  - связей с адресами/кошельками/владельцами, которые имеют высокий уровень риска (потенциальные злоумышленники);
  - специализированных подходов и алгоритмов расчета и оценки риска, которые будут разработаны и зафиксированы в «Методики расчета потенциальных рисков в сфере криптовалютных операций».

Развертывание сервера разметки будет осуществляться на сервере со следующими аппаратными требованиями:

- Xeon 2.3 ГГц, 32 ядра, 512gb RAM, 4TB SSD.

### 1.2.3 Сервер аналитики

На рисунке 3 схематично представлено назначение и задачи Сервера аналитики.





Рисунок 4. Назначение и задачи сервера аналитики

Сервер аналитики предназначен для проведения анализа данных блокчейна и формирования выводов по движению денежных средств, действиях отдельных кошельков/адресов и т.п.

Сервер аналитики будет обеспечивать следующие возможности:

- Выдача совокупной информации о транзакциях;
- Обработка и анализ данных адресов;
- Обработка и анализ данных кластеров;
- Работа с данными о владельцах;
- Поиск, проверка и автозаполнение данных.

#### **Выдача совокупной информации о транзакциях**

Основная цель данной функции - получение интегральной информации о совокупности транзакций, характеризующейся заданными общими признаками, включая интервал времени, суммарный объем, средний размер транзакции в денежных единицах (BTC, USD, RUB), средний размер транзакций в единицу времени, а также гистограмму распределения транзакций по указанным признакам.

Функция выдачи совокупной информации о транзакциях будет обеспечивать возможность аналитику работать со следующими данными:

- общая статистика по количеству узлов;
- общая статистика по количеству транзакций;
- общая статистика по высоте блока;
- общая статистика по производительности сети;
- общая статистика по географической распределённости сети за:
  - o выбранный период времени;
  - o итоговые данные на текущий момент времени.

Для каждой транзакции пользователю будет доступна следующая информация:

- Блок транзакции;
- Дата проведения транзакции;

- Время проведения;
- Сумма транзакции в BTC;
- Сумма транзакции в долларах (по курсу Coinbase и/или Binance);
- Сумма транзакции в рублях (по курсу Coinbase и/или Binance);
- Список входов и выходов транзакции с описанием названия и типа адреса/кошелька;
- Размер комиссии транзакции;
- Хэш транзакции.

Ниже представлены примеры возможных интерфейсов работы данной функции.

**GLOBAL BITCOIN NODES DISTRIBUTION**  
 Reachable nodes as of Mon Jul 19 2021 12:53:18  
 GMT+0300 (Москва, стандартное время).

**12935 NODES**

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	5592 (43.23%)
2	United States	1831 (14.16%)
3	Germany	1648 (12.74%)
4	France	554 (4.28%)
5	Netherlands	422 (3.26%)
6	Canada	309 (2.39%)
7	United Kingdom	244 (1.89%)
8	Russian Federation	209 (1.62%)
9	Finland	173 (1.34%)
10	Switzerland	158 (1.22%)

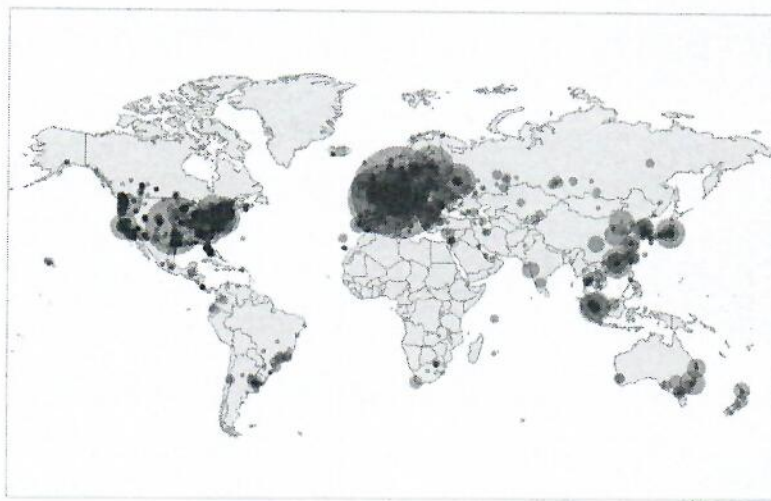


Рисунок 5. Пример №1 возможного интерфейса работы данной функции

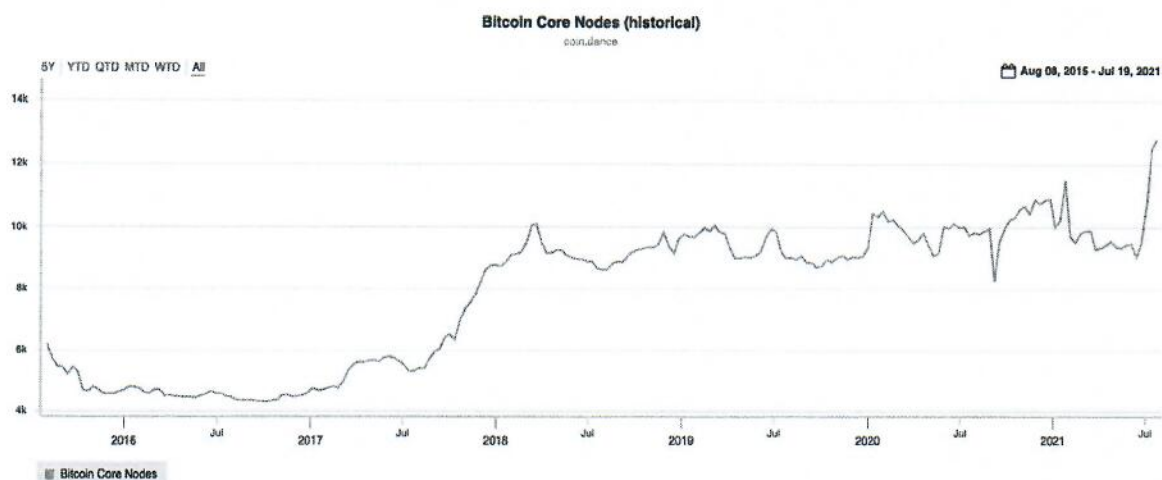


Рисунок 6. Пример №2 возможного интерфейса работы данной функции



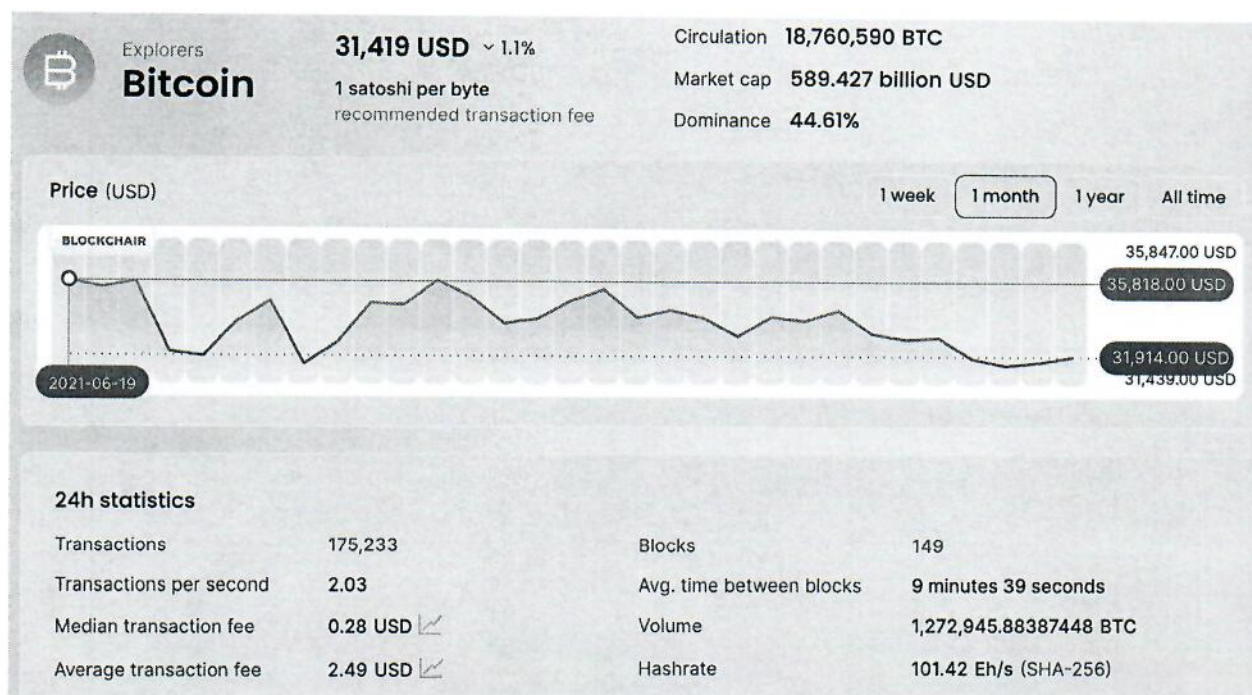


Рисунок 7. Пример №3 возможного интерфейса работы данной функции

Представленные в настоящем разделе интерфейсы не являются итоговыми, а носят информативный характер. Итоговые интерфейсы Системы будут разработаны и согласованы с Заказчиком на этапе «Доработки технического проекта ЕИС Росфинмониторинга».

Представленный в настоящем разделе состав данных может быть изменен на этапе «Доработки технического проекта ЕИС Росфинмониторинга» по требованию Заказчика.

### Обработка и анализ данных адресов (лицевых счетов)

Основная цель данной функции - получение интегральной информации о балансе и движении криптовалютных средств для указанного адреса (который может быть ассоциирован с владельцем - физическим или юридическим лицом).

Данная функция предоставляет пользователю возможность получения сводной информации по отдельному адресу (лицевому счёту) сети Bitcoin и/или о связях нескольких адресов (лицевых счетов) через выполненные прямые или косвенные транзакции за выбранный период времени или итоговых данных на текущий момент времени, а также сделать отметки в записной книжке личного кабинета по каждому выбранному адресу.

Будут реализованы следующие возможности:

- обеспечение получения данных об адресе включая:
  - адрес;
  - тип;
  - название;
  - риск;
  - баланс (BTC);
  - оборот (BTC);
  - количество транзакций;
  - количество упоминаний;
- получение риск-скоринга транзакций. риск-скоринг рассчитывается на основе данных, позволяющих ассоциировать владельца адреса с физическим или юридическим лицом, а также виртуальным пользователем сети Интернет, в



отношении которого имеется какая-либо дополнительная информация, влияющая на риск-скоринг;

- графиков изменения остатка на адресе;
- визуализация информации (построение графиков) в отношении приходящих на адрес средств, исходящих с адреса средств, изменения баланса на адресе;
- графиков изменения приходящих на адрес средств.
- автоматическое обнаружение статистически-значимых событий, связанных с адресом, таких как изменение режима прихода или расхода средств, аномальные по размеру транзакции, аномальные по частоте возникновения последовательности транзакций.

Ниже представлен пример возможного интерфейса работы данной функции:

The screenshot displays a Bitcoin address analysis interface. On the left, a sidebar shows the address type as 'pubkeyhash' and provides balance change history: 'First balance change Received 8 years ago' and 'Last balance change Received 5 minutes ago'. It also shows 'Transaction count 72,120', 'Output count 72,355', and 'Unspent output count 19'. At the bottom of the sidebar are buttons for 'Show script' (Op, Bin, Hex) and an 'Additional info' section. The main area shows the address '1KFHE7w8BhaENAswwryaocccDb6qcT6DbYY' with a QR code. Below the address, a 'Balance' section shows '610.49612733 BTC · 19,483,373.41 USD'. A table lists 'Total received' as '5,173,465.53235681 BTC · 12,917,929,772.41 USD' and 'Total spent' as '5,172,855.03622948 BTC · 12,920,286,534.47 USD'. The 'Transaction history' section shows two transactions: a 'Sent' transaction of 4.00000539 BTC (127,656.10 USD) and a 'Received' transaction of 6.51673640 BTC (207,975.00 USD), both confirmed on Jul 19, 2021.

Рисунок 8. Пример №4 возможного интерфейса работы данной функции

Представленный в настоящем разделе интерфейс не является итоговым, а носит информативный характер. Итоговые интерфейсы Системы будут разработаны и согласованы с Заказчиком на этапе «Доработки технического проекта ЕИС Росфинмониторинга».

Представленный в настоящем разделе состав данных может быть изменен на этапе «Доработки технического проекта ЕИС Росфинмониторинга» по требованию Заказчика.

### Обработка и анализ данных кластеров

Данная функция позволяет аналитику получить сводную информацию по связанным потокам средств с сети Bitcoin, а также назначить кластеру (связанному списку адресов) категорию в записной книжке личного кабинета.

Ниже представлены примеры возможных интерфейсов работы данной функции:



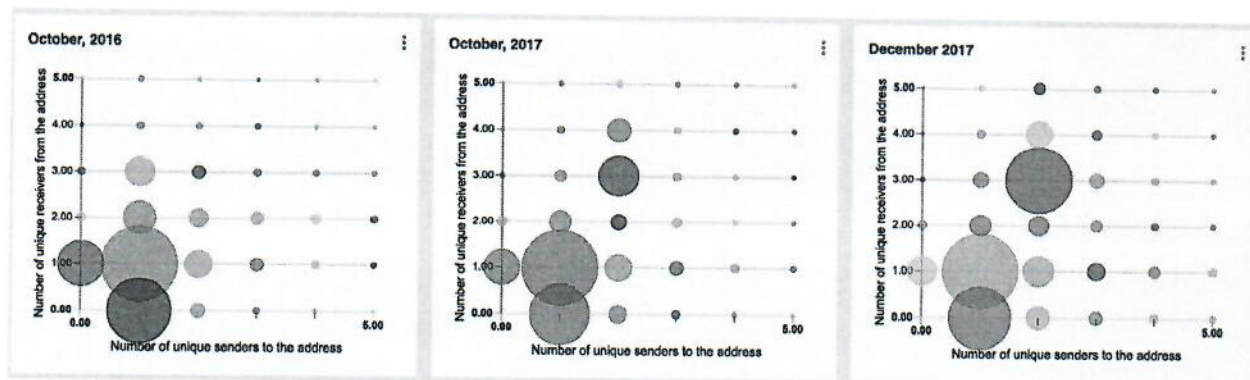


Рисунок 9. Пример №5 возможного интерфейса работы данной функции

Total blocks

691,700

Blocks 24h

148

Latest block

6 минут назад

Next readjustment

через 1 неделю

Next estimated difficulty

14,655,090,568,239

Table fields

10 / 36

Номер

Хеш

Время

Майнер

Данные coinbase

Bin

Hex

Количество транзакций

Количество транзакций со свидетелем

Количество входов

Количество выходов

Уничтоженные монетодни

Входы

BTC

USD

Выходы

BTC

USD

Комиссия

BTC

USD

Комиссия за Кбайт

BTC

USD

Номер	Хеш	Время (UTC)	Майнер	Количество транзакций	Выходы (BTC)
691,699	00000...45dbf	2021-07-19 10:09:53	Unknown	2304	3,612.13
691,698	00000...edc99	2021-07-19 10:03:11	F2Pool	2578	7,766.71
691,697	00000...f235e	2021-07-19 09:37:02	Unknown	491	15,252.55
691,696	00000...4bf21	2021-07-19 09:36:00	Unknown	2656	20,795.01
691,695	00000...30e82	2021-07-19 09:17:00	SlushPool	405	786.67
691,694	00000...72182	2021-07-19 09:14:12	F2Pool	1265	3,648.69
691,693	00000...fc698	2021-07-19 09:05:42	Binance	1078	2,001.60
691,692	00000...9547b	2021-07-19 08:59:26	F2Pool	1529	2,551.34
691,691	00000...6b467	2021-07-19 08:58:47	SlushPool	259	563.85
691,690	00000...6c7cf	2021-07-19 08:55:53	AntPool	530	1,945.22
691,689	00000...0051d	2021-07-19 08:44:27	F2Pool	1478	3,459.59
691,688	00000...2e9b2	2021-07-19 08:35:08	F2Pool	876	1,082.34

Рисунок 10. Пример №6 возможного интерфейса работы данной функции

Будут реализованы следующие возможности:

- получение списка всех адресов и/или транзакций кластера, с возможностью их сортировки:
  - по дате первых, входящих транзакций;
  - по дате последних, исходящих транзакций;
  - по количеству транзакций;
  - по частоте транзакций;
  - по объему полученных средств;
  - по остатку средств;
  - по риску адресов;
  - по остаточному риску адресов;
- выдача совокупного риска всего кластера;
- выдача истории по риску кластера. Распределение адресов и/или транзакций кластера по риск-параметрам;
- получение данных об одном адресе в нескольких режимах:
  - в биткоинах;
  - в долларах;
  - в рублях;



- с учетом внутреннего оборота, который происходит внутри кластера;
- без учета внутреннего оборота, который происходит внутри кластера;
- получения всех транзакций кластера с возможностью сортировки:
  - по размеру;
  - по риску;
  - по наличию контрагентов в транзакциях.

Представленные в настоящем разделе интерфейсы не являются итоговыми, а носят информативный характер. Итоговые интерфейсы Системы будут разработаны и согласованы с Заказчиком на этапе «Доработки технического проекта ЕИС Росфинмониторинга».

Представленный в настоящем разделе состав данных может быть изменен на этапе «Доработки технического проекта ЕИС Росфинмониторинга» по требованию Заказчика.

### **Работа с данными о владельцах**

Целью данной функции является возможность внесения в систему информации о физических лицах, юридических лицах и виртуальных пользователях сети Интернет, которые могут быть ассоциированы с владением криптовалютными средствами и осуществлением транзакций в блокчейне биткоина.

Данная функция предоставляет аналитику следующие возможности:

- Получать данные о владельце адреса (лицевого счёта) сети Bitcoin;
- Вносить данные о владельце адреса (лицевого счёта) сети Bitcoin;
- Корректировать данные о владельце адреса (лицевого счёта) сети Bitcoin.

Информация о транзакциях в сети Bitcoin является публично доступной, что позволяет беспрепятственно её анализировать. Однако, одной из важнейших особенностей данной реализации распределённого реестра данных является анонимность каждого адреса, участвующего в транзакциях. Открытые источники данных о соответствии адреса и его владельца практически отсутствуют или тщательно защищены от публичного доступа. В связи с этим для обеспечения необходимой функциональности в Системе предусмотрен сервер парсинга открытых источников (см. п. 1.2 «Предварительная архитектура системы» настоящего документа), результат работы которого позволяет выдвигать гипотезы о соответствии и предлагать их пользователю в соответствующем интерфейсе (см. п. 1.2.5 настоящего документа), где он может подтвердить или отвергнуть гипотезу, опираясь на данные личного опыта. На основе таких решений может быть построена база данных владельцев, которая будет постоянно пополняться и совершенствоваться не только за счёт улучшения алгоритмов поиска и увеличения количества источников данных, но также за счёт ручного внесения корректировок аналитиками.

Будут реализованы следующие возможности:

- внесение в список информации о владельцах (физических лицах, юридических лицах, виртуальных пользователях), в том числе с возможностью внесения неструктурированных и специальных данных;
- получение списка владельцев;
- осуществление поиска по стандартным (структурированным) данным о пользователях;
- осуществление поиска по нестандартным (неструктурированным) данным о пользователях;
- получение данных о конкретном владельце с учетом расчета оборота:
  - по биткоинам;
  - по рублям;
  - по долларам;



с возможностью фильтрации как по времени начала работы, так и по последним исходящим транзакциям;

- поиск:
    - по риску;
    - по типу;
    - по категориям;
    - по названию;
- поиск может осуществляться:
- на основе регулярных выражений;
  - на основе нечеткой логики;
- добавление данных о владельце;
  - обновление данных о владельце;
  - удаление данных о владельце.

### **Поиск, проверка и автозаполнение данных**

Целью данной функции является предоставление пользовательского интерфейса, позволяющего осуществлять поиск данных в удобном для пользователя формате. За предоставление функции отвечает сервер поддержки веб-интерфейса (см. п. 1.2.5 настоящего документа), который индексирует и агрегирует данные, полученные с сервера аналитики, что позволяет быстро, без выполнения длительных комплексных запросов к блокчейну биткоина или к базе данных аналитики, дополнить данные в полях ввода наиболее подходящим значением, найденным в индексе, или предоставить пользователю выбор из нескольких подходящих значений (если они есть), когда он только начинает набор текста или адреса.

Будут реализованы следующие возможности:

- поиск и автозаполнение по адресу:
  - отправителя транзакции;
  - получателя транзакции;
- поиск и автозаполнение по названию владельца:
  - по данным физического лица, если имеется информация об ассоциации физического лица с транзакциями в блокчейне биткоина;
  - по данным юридического лица, если имеется информация об ассоциации юридического лица с транзакциями в блокчейне биткоина;
  - по данным виртуального пользователя сети Интернет, если имеется информация об ассоциации такого пользователя с транзакциями в блокчейне биткоина;
- проверка на существование адреса определенных сущностей, для которых указаны значения ключей или возможные диапазоны значений, включая:
  - адреса (в том числе включая проверку валидности адреса, которая определяет, создан ли адрес по правилам блокчейн биткоин);
  - транзакции;
  - объемы транзакций, выраженный в биткоинах, USD или рублях.
- проверка на существование транзакции;
- проверка на валидность адреса, которая определяет, создан ли адрес по правилам блокчейн биткоин;
- проверка на существование кластера:
  - на основании диапазона предполагаемых размеров кластера;
  - на основании принадлежности указанных входящих адресов к кластеру;
  - на основании принадлежности указанных исходящих адресов к кластеру;
  - на основании принадлежности указанных транзакций к кластеру.



- также возможность формирования произвольных логических запросов данных с использованием SQL-подобного языка.

Развертывание сервера аналитики будет осуществляться на сервере со следующими аппаратными требованиями:

- Xeon 2.3 ГГц, 32 ядра, 512gb RAM, 8TB SSD.

### **Механизмы реализации сервера аналитики**

Предполагается, что вышеуказанные функции сервера аналитики будут интегрированы с функциями сервера архивации (см. раздел 1.2.4) и реализованы на основе современных технологий колоночно-ориентированных систем баз данных (СУБД) временных рядов с открытым кодом.

Указанные технологии является в настоящее время де-факто стандартом, принятым в российской финансовой индустрии, и предназначены для хранения и высокопроизводительной и высоконадежной обработки больших и сверхбольших объемов финансовой и аналогичной информации.

Важной особенностью и технологическим преимуществом указанных СУБД является интеграция высокопроизводительной системы управления базами данных, специально оптимизированной для хранения и представления временных рядов финансовой и аналогичной информации, с высокоэффективным встроенным языком программирования бизнес-логики и запросов, а также поддержка, в целях совместимости, стандартного языка запросов SQL.

Применение специального встроенного языка запросов позволяет эффективно реализовать бизнес-логику любой степени сложности внутри базы данных, что исключает необходимость обмена большими объемами данных с внешними приложениями и значительно повышает эффективность решения в целом.

#### **1.2.4 Сервер архивации**

На рисунке 4 схематично представлено назначение и задачи Сервера архивации.



Рисунок 11. Назначение и задачи сервера аналитики

Сервер архивации предназначен для реализации обмена информацией с пользователями Системы.

Сервер архивации будет обеспечивать следующие возможности:

- Резервирование базы данных (далее – БД) Системы;
- Ведение журнала запросов;



- Ведение истории изменений данных.

#### **Резервирование базы данных**

Будет реализована возможность резервирования базы данных Системы с возможностью бессрочного хранения данных. Также будет реализована возможность изменения параметра периодичности резервирования при необходимости. Для обеспечения высокого уровня надежности данных и эффективности работы с данными будет реализована стратегия резервного копирования, которая сочетает два взаимодополняющих метода:

- периодическое полное резервное копирование базы данных;
- ведение двоичных журналов, в которых регистрируются все изменения данных в промежутках между резервными копированиями.

#### **Ведение журнала запросов**

Журнал запросов будет содержать (сохранять) следующую информацию:

- Запрос;
- Конечная точка;
- Дата создания запроса;
- Время создания запроса;
- Дата окончания обработки запроса;
- Время окончания обработки запроса;
- Общее время обработки запроса;
- Статус запроса;
- Пользователь, который инициировал запрос.

В Журнале запроса будет возможность фильтрации запросов по датам.

#### **Ведение истории изменений данных**

История изменений данных будет содержать следующую информацию:

- Пользователь, который внес изменения;
- Данные до изменения (старые данные);
- Данные после изменения (новые данные);
- Дата внесения изменений.

В Истории изменений данных будет реализована возможность фильтрации изменений по датам.

Развертывание сервера архивации будет осуществляться на сервере со следующими аппаратными требованиями:

- Xeon 2.3 ГГц, 32 ядра, 512gb RAM, 192TB HDD.

#### **1.2.5 Сервер поддержки веб интерфейса пользователя**

На рисунке 5 схематично представлено назначение и задачи Сервера поддержки веб интерфейса пользователя.

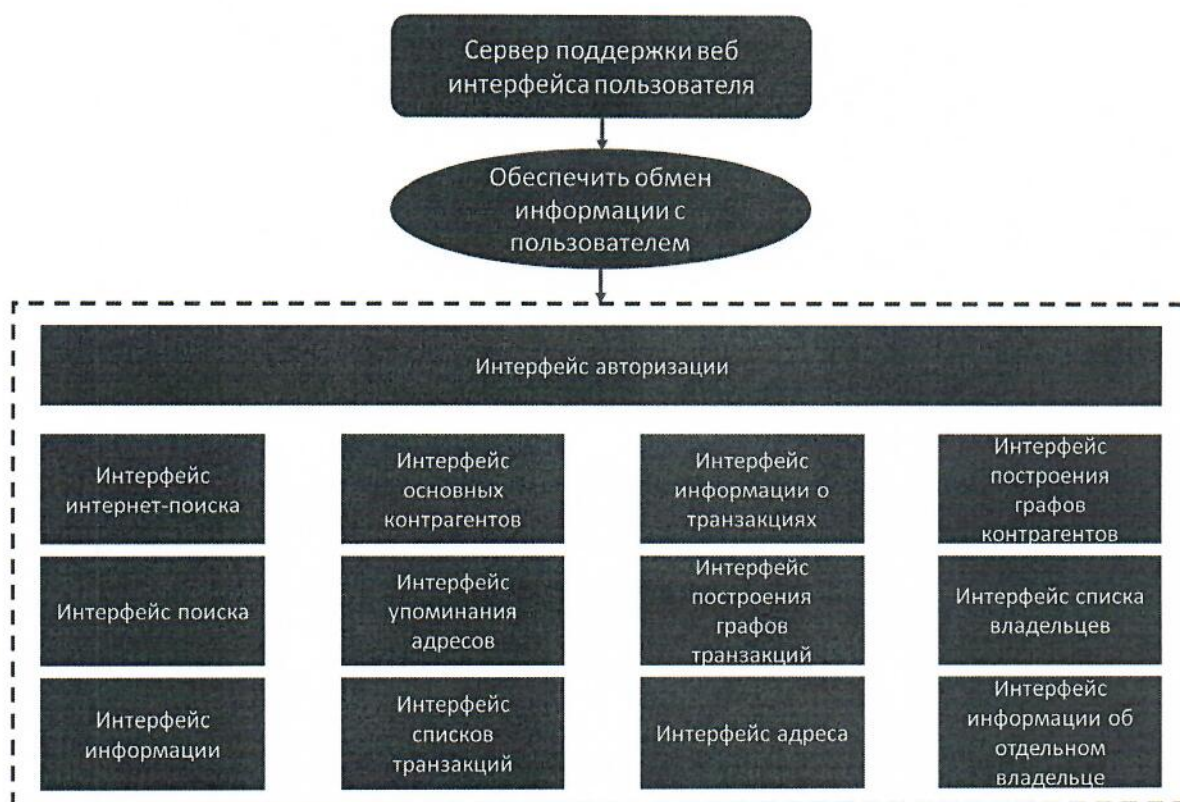


Рисунок 12. Назначение и задачи сервера поддержки веб интерфейса пользователя

Сервер поддержки веб интерфейса пользователя предназначен для реализации обмена информацией с пользователями Системы.

Интерфейс пользователя позволит аналитику выполнять работу по:

- установке связей между субъектами криптовалютных транзакций;
- отслеживанию движения активов;
- представлению результатов в графическом и табличном виде.

Интерфейс будет выполнен в виде веб-интерфейса с поддержкой следующих браузеров:

- Mozilla Firefox;
- Chrome;
- Yandex;
- Microsoft Edge;
- Opera.

В Системе будет реализована возможность поддержки системы личных кабинетов. Таким образом каждый зарегистрированный пользователь будет иметь собственный личный кабинет в Системе. Система личных кабинетов предназначена для обеспечения и управления доступом пользователя к санкционированным данным, которые будут организованы в иерархию для хранения следующих видов информации:

- Ссылок на объекты системы.
- Ссылок на построенные графы.
- Разметки, которая отражается только у конкретного пользователя по запросу.
- Рабочих групп.
- Агрегированных объектов (например, адреса, кошельки и владельцы).

Также в Системе будет обеспечена настройка следующих параметров пользовательского интерфейса:



- Даты;
- Времени;
- Типа отображения графа;
- Языка интерфейса, включая:
  - Русский язык;
  - Английский язык;
- Выбор вида валюты.

Система личных кабинетов будет обеспечивать следующую иерархию:

- Пользователь;
- Рабочая группа.

Система личных кабинетов будет содержать систему уведомлений. Уведомления о преднастроенных событиях будут направляться пользователям (в зависимости от настроек):

- На почту;
- В мессенджер.

Для настройки (преднастроенных) событий будут реализованы следующие возможности:

- Отслеживание изменения выше пороговых значений в одну и другую сторону по балансу объекта, а именно:
  - Адреса;
  - Кластера;
  - Сета;
  - Владельца.
- Отслеживание изменения пороговых значений по риску.
- Отслеживание появления транзакций, превышающих риск.

В рамках реализации функции по обмену информации с пользователями будут реализованы следующие интерфейсы:

- Интерфейс авторизации;
- Интерфейс поиска;
- Интерфейс информации;
- Интерфейс основных контрагентов;
- Интерфейс упоминания адресов;
- Интерфейс списков транзакций;
- Интерфейс информации о транзакциях;
- Интерфейс построения графов транзакций;
- Интерфейс адреса;
- Интерфейс построения графов контрагентов;
- Интерфейс списка владельцев;
- Интерфейс информации об отдельном владельце;
- Интерфейс интернет-поиска.

## **1. Интерфейс авторизации**

Интерфейс будет поддерживать возможность входа пользователя в систему. Для входа пользователя в систему будут реализованы следующие варианты:

- вход с использованием ввода логина и пароля

- вход с использованием системы ЕСИА<sup>1</sup>.

Для входа в систему с использованием логина и пароля пользователю будет предоставлена возможность заполнения следующих полей:

- Логин (тип данных: строка);
- Пароль (тип данных: строка).

По итогам заполнения данных полей у пользователя будет возможность нажатия на кнопку входа в систему. При нажатии данной кнопки будет осуществляться авторизация и аутентификация пользователя в системе. В случае успешного проведения авторизации и аутентификации пользователь будет получать доступ к функциям системы в соответствии с его ролью и правами в системе. В случае если введенные данные не могут быть идентифицированы в системе (введен не верный логин или пароль), пользователь будет уведомляться о необходимости внесения корректных данных.

Для входа в систему с использованием ЕСИА пользователю будет доступна возможность нажатия на кнопку входа с использованием ЕСИА. При нажатии на данную кнопку будет осуществляться авторизация и аутентификация пользователя в системе с использованием данных ЕСИА. В случае успешной авторизации и аутентификации пользователь будет получать доступ к функциям системы в соответствии с его ролью и правами в системе. В случае если система не может идентифицировать пользователя через данные ЕСИА, пользователь будет уведомляться об инструкциях для настройки корректного входа.

Также для пользователя будут доступны следующие функции:

- Подтверждение и обновление пароля. Для смены пароля пользователю будет необходимо:
  - Ввести старый пароль и далее новый пароль, который он планирует установить (новый пароль вводится дважды для исключения ошибки ввода);
  - Подтвердить права на учетную запись через электронную почту далее новый пароль, который он планирует установить (новый пароль вводится дважды для исключения ошибки ввода);
- Подтверждение регистрации с учетом:
  - Субъекта;
  - Страны;
  - Уровня доступа.

## **2. Интерфейс поиска**

Интерфейс будет поддерживать возможность поиска информации по следующим объектам:

- Адреса;
- Кошелька;
- Владельца.

## **3. Интерфейс информации**

Интерфейс будет поддерживать возможность отображения сводной информации об адресе/кошельке. Сводная информация будет содержать следующие данные :

16. Название;
17. Тип;
18. Количество адресов;

---

<sup>1</sup> Единая система идентификации и аутентификации — информационная система в Российской Федерации, обеспечивающая санкционированный доступ участников информационного взаимодействия к информации, содержащейся в государственных информационных системах и иных информационных системах.



19. Количество транзакций;
20. Риск;
21. Первое и последнее упоминание;
22. Всего получено и потрачено BTC/USD;
23. Остаток BTC/USD;
24. Распределение транзакций;
25. Топ входящих/исходящих контрагентов:
  - с) Контрагент;
  - д) Сумма;
26. Топ входящих/исходящих транзакций:
  - д) Дата;
  - е) Хэш;
  - ф) Сумма;
27. Динамика входящих/исходящих транзакций;
28. Динамика баланса;
29. Динамика риска;
30. Упоминания:
  - д) Заголовок;
  - е) Текст упоминания;
  - ф) Ссылка.

Для удобства пользователя к данным на странице можно будет применить фильтр для сортировки информации по дате.

#### **4. Интерфейс основных контрагентов**

Данный интерфейс предназначен для составления списков контрагентов кошелька или владельца, а также получения сводной информации о:

- категориях;
- типах;
- конкретных владельцах-контрагентах.

Страница будет отображать:

- полный список контрагентов кошелька/адреса;
- их название;
- тип;
- оборот в BTC;
- распределение входящих/исходящих контрагентов на круговой диаграмме.

Для удобства пользователя к данным на странице можно будет применить фильтр для сортировки информации по:

- дате;
- обороту;
- типу контрагентов.

Также для обеспечения удобства работы с информацией в интерфейсе будет реализована возможность экспортировать данные таблицы в .CSV файл.

#### **5. Интерфейс упоминания адресов**

Данный интерфейс предназначен для отображения списка упоминаний кошелька:

5. Адрес (название, тип);

6. Заголовок;
7. Текст упоминания;
8. Ссылка.

#### **6. Интерфейс списков транзакций**

Данный интерфейс предназначен для отображения списка транзакций кошелька/адреса:

6. Дата и время;
7. Хэш;
8. Риск;
9. Сумма в BTC;
10. Список входов и выходов транзакции.

Для удобства пользователя к данным на странице можно будет применить фильтр для сортировки информации по:

- дате;
- сумме;
- типу транзакций.

Также для обеспечения удобства работы с информацией в интерфейсе будет реализована возможность экспортировать данные таблицы в .CSV файл.

#### **7. Интерфейс информации о транзакциях**

Данный интерфейс предназначен для отображения информации о транзакции:

6. Блок;
7. Дата и время;
8. Сумма;
9. Список входов и выходов транзакции с описанием названия и типа адреса/кошелька, если таковое имеется;
10. Риск.

#### **8. Интерфейс построения графов транзакций**

Данный интерфейс предназначен для отображения графа транзакции.

Каждый вход/выход транзакции представляет собой ноду, они соединены между собой линиями, на которых указана сумма и направление передачи средств в BTC.

Нажатие на ноду открывает меню:

- «Инфо» - открывает страницу с информацией об адресе.

Нажатие на связь открывает меню:

- «Инфо» - открывает страницу с информацией о транзакции;
- «Раскрыть» - добавляет на граф ноды и связи, входящие в транзакцию;
- «Раскрыть входы/выходы» - добавляет на граф ноды и связи, являющиеся входами/выходами транзакции;
- «Удалить» - удаляет связь и связанные с ними ноды.

Нажатие на «связь» открывает таблицу с описанием:

- Адреса отправителя;
- Адреса получателя;
- Суммы транзакции;
- Хэша транзакции.



В правом меню можно изменять тип графа. Данные графа можно экспортировать в .CSV файл или сохранять в виде статической ссылки.

## **9. Интерфейс адреса**

Данный интерфейс предназначен для отображения списка адресов кошелька:

9. Адрес;
10. Тип;
11. Название;
12. Риск;
13. Баланс (BTC);
14. Оборот (BTC);
15. Количество транзакций;
16. Количество упоминаний.

Для удобства пользователя к данным на странице можно будет применить фильтр для сортировки информации по:

- дате;
- балансу;
- обороту адресов.

Также для обеспечения удобства работы с информацией в интерфейсе будет реализована возможность экспортировать данные таблицы в .CSV файл.

## **10. Интерфейс построения графов контрагентов**

Данный интерфейс позволяет получить пользователю информацию о контрагентах путем нажатия на ноду, которое 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.

Нажатие на связь открывает таблицу с описанием:

- Адреса отправителя.
- Адреса получателя.
- Суммы транзакции.
- Хэша транзакции.

Для удобства пользователя к данным на странице можно будет применить фильтр для сортировки информации по:

- дате;
- сумме транзакций.

Будет реализована возможность изменять тип графа в правом меню.

Также для обеспечения удобства работы с информацией в интерфейсе будет реализована возможность экспортировать данные таблицы в .CSV файл или сохранить в виде статической ссылки.

#### **11. Интерфейс списка владельцев**

Данный интерфейс позволяет отобразить список владельцев с указанием:

5. Названия;
6. Категории;
7. Типа;
8. Количества кошельков.

Для удобства пользователя к данным на странице можно будет применить фильтр для сортировки информации по:

- категории;
- типу;
- названию владельцев.

Также для обеспечения удобства работы с информацией (данными графа) в интерфейсе будет реализована возможность экспортировать данные таблицы в .CSV файл.

#### **12. Интерфейс информации об отдельном владельце**

Данный интерфейс предназначен для отображения подробной информации об адресе/кошельке, с указанием:

19. Названия.
20. Типа.
21. Категории.
22. Количества адресов.
23. Количества кошельков.
24. Количества транзакций.
25. Уровня риска.
26. Первого и последнего упоминания.
27. Поступившей и выведенной суммы в BTC/USD.
28. Остаток в BTC/USD.
29. Распределения транзакций.
30. Списка юридических лиц:
  - g) Номер;
  - h) Названия;
  - i) Страна;
  - j) Домен;
  - k) Лицензия;
  - l) Адрес;
31. Списка сайтов:
  - d) Сайт;
  - e) IP;
  - f) Страна;
32. Страницы и профили в Интернете:
  - c) Ссылка;



- d) Домен;
- 33. Кошельков:
  - h) Кошелек;
  - i) Баланс (BTC);
  - j) Оборот;
  - k) Адресов;
  - l) Транзакций;
  - m) Первое упоминание;
  - n) Последнее упоминание;
- 34. Адреса:
  - g) Адрес;
  - h) Баланс (BTC);
  - i) Оборот;
  - j) Транзакции;
  - k) Первое упоминание;
  - l) Последнее упоминание;
- 35. Упоминания:
  - d) Заголовок;
  - e) Текст упоминания;
  - f) Ссылка;
- 36. Динамика риска.

### **13. Интерфейс интернет-поиска**

Данный интерфейс предназначен для поиска BTC адресов по страницам в сети Интернет и Тог. Для обеспечения эффективности работы пользователя будут разработаны два режима:

- Поиск по ссылкам. Данный вид поиска будет осуществлять поиск BTC адресов на страницах, указанных в запросе. Ввод страниц будет осуществляться через запятую.
- Поиск по запросу. Данный вид поиска будет осуществляться по поисковому запросу из поля Запрос в интернет-поисковике компании Яндекс. Для пользователя будут выводиться порядка 200 первых результатов.

Полученные, в результате поиска, данные будут выводиться в таблицу с указанием следующих параметров:

- 3. Адреса (название, тип);
- 4. Ссылки.

Развертывание сервера поддержки веб интерфейса пользователя будет осуществляться на сервере со следующими аппаратными требованиями:

- Xeon 2.3 ГГц, 32 ядра, 512gb RAM, 8TB SSD.

### **1.3 Содержание работ по проведению опытной эксплуатации Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина**

На данном этапе Подрядчик осуществляет проведение опытной эксплуатации разработанного Модуля мониторинга и анализа криптовалютных транзакций с

использованием биткоина в соответствии с разработанной Программой опытной эксплуатации. По результатам проведения опытной эксплуатации осуществляется:

1. Программная доработка Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина, с учетом выявленных в ходе опытной эксплуатации недочетов.
2. Доработка документации 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.



## КАЛЕНДАРНЫЙ ПЛАН

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

№ этапа	Наименование	Отчетные материалы	
		Окончание	
1	Доработка технического проекта ЕИС Росфинмониторинга	29 октября 2021 г.	<ol style="list-style-type: none"> <li>1. Актуализированная техническая документация на ЕИС Росфинмониторинга:  a) Общее техническое задание на ЕИС Росфинмониторинга;  b) Описание комплекса технических средств ЕИС Росфинмониторинга;</li> <li>2. Пояснительная записка на Модуль мониторинга и анализа криптовалютных транзакций с использованием биткоина;</li> <li>3. Компакт-диск с документацией на Модуль мониторинга и анализа криптовалютных транзакций с использованием биткоина:  a) Каталог базы данных;  b) Руководство пользователя;  c) Руководство администратора;  d) Руководство администратора по информационной безопасности.</li> <li>4. Акт сдачи-приемки выполненных работ по этапу</li> </ol>

№ этапа	Наименование	Отчетные материалы	
		Окончание	
2	Работы по созданию Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина <i>(поэтапная детализация представлена в отдельной таблице)</i>	11 ноября 2021 г.	<ol style="list-style-type: none"> <li>1. Программа и методика испытаний;</li> <li>2. Компакт-диск с исходными кодами и дистрибутивом программного обеспечения;</li> <li>3. Протокол проведения испытаний;</li> <li>4. Программа опытной эксплуатации.</li> <li>5. Акт сдачи-приемки выполненных работ по этапу</li> </ol>
3	Опытная эксплуатация Модуля мониторинга и анализа криптовалютных транзакций с использованием биткоина	10 декабря 2021 г.	<ol style="list-style-type: none"> <li>1. Акт сдачи-приёмки выполненных работ (итоговый, который подписывает после выполнения работ по всем этапам);</li> <li>2. Счет;</li> <li>3. Счет-фактура;</li> <li>4. Журнал проведения опытной эксплуатации;</li> <li>5. Доработанная по результатам опытной эксплуатации документация на Модуль мониторинга и анализа криптовалютных транзакций с использованием биткоина: <ol style="list-style-type: none"> <li>а) Программа и методика испытаний;</li> <li>б) Каталог базы данных;</li> <li>в) Руководство пользователя;</li> <li>г) Руководство администратора;</li> <li>д) Руководство администратора информационной безопасности;</li> </ol> </li> <li>6. Компакт-диск с исходными кодами и дистрибутивом программного обеспечения;</li> <li>7. Протокол проведения испытаний.</li> </ol>
ИТОГО:			



**Поэтапная детализация календарного плана (2 этап)**

<b>Сервер</b>	<b>№ п/п</b>	<b>Задача</b>	<b>Описание выполняемых работ</b>	<b>Планируемые к привлечению ресурсы</b>	<b>Сроки выполнения работ</b>	<b>Очередь разработки ПО</b>
Сервер ноды блокчейна биткоина	<b>1</b>	<b>Обеспечение получения данных (мониторинга) блокчейна биткоина</b>			18 дней	1-я очередь
	<b>1.1</b>	<b>Получение данных о транзакциях сети Биткоина</b> Будут реализованы следующие возможности: - Сбор данных. - Обработка данных. - Просмотр данных.	- Анализ, проектирование и постановка задачи на развёртывание (реализацию) сервера ноды блокчейна биткоина	- Системный архитектор - Архитектор JAVA		
	<b>1.2</b>	<b>Получение данных о блоках сети Биткоина</b> Будут реализованы следующие возможности: - Сбор данных. - Обработка данных. - Просмотр данных.	- Развёртывание (реализация) сервера ноды блокчейна биткоина			
	<b>1.3</b>	<b>Получение параметров сети Биткоин</b> Будут реализованы следующие возможности: - Сбор данных. - Обработка данных. - Просмотр данных.				
	<b>2</b>	<b>Обеспечение обработки данных</b>				
					25 дней	1-я очередь

Сервер	№ п/п	Задача	Описание выполняемых работ	Планируемые к привлечению ресурсы	Сроки выполнения работ	Очередь разработки ПО
Создание сервера разметки	2.1	<b>Информационное взаимодействие с независимым модулем ноды биткойна</b> Будут реализованы следующие возможности: - Сбор данных. - Просмотр данных.	Развертывание	Системный администратор		
			Настройка шардирования базы данных	Разработчик		
			Разработка компонента связи с нодой блокчейна биткойна	Разработчик		
	2.2	<b>Парсинг данных</b> Будут реализованы следующие возможности: - Конвертация всех данных содержимого ноды биткойна в таблицы базы данных системы. - Конвертация онлайн-разметки. - Работа в фоновом режиме и перенос транзакций. - Пересчет и разметка в режиме онлайн входов и выходов по текущему курсу биткойна на доллар и по текущему курсу биткойна на рубль.	Реализация исторического парсинга (конвертация содержимого ноды блокчейна биткойна в таблицы базы данных)	Разработчик		
			Конвертация онлайн разметки и мониторинг транзакций	Разработчик		
			Перенос транзакций в блок ноды мониторинга	Разработчик		



Сервер	№ п/п	Задача	Описание выполняемых работ	Планируемые к привлечению ресурсы	Сроки выполнения работ	Очередь разработки ПО
			Пересчет и разметка входов и выходов	Разработчик		
	2.3	Кластеризация данных Будет реализована возможность разметки кластеров в соответствии с алгоритмом кластеризации по общей трапе.	Разработка основной логики компонента	Разработчик		
			Проверка сохранения разметки	Разработчик		
			Разработка скрипта актуализации	Разработчик		
			Разработка блока обеспечения разметки кластеров	Разработчик		
			Разработка блока разбора конфликтов с разметкой	Разработчик		
			Разработка блока установления приоритетов	Разработчик		
			Разработка блока логирования действий в области разметки	Разработчик		

Сервер	№ п/п	Задача	Описание выполняемых работ	Планируемые к привлечению ресурсы	Сроки выполнения работ	Очередь разработки ПО
			Разработка блока фильтрации доступа	Системный аналитик		
	2.4	<b>Хранение данных (упоминаний)</b> Будут реализованы следующие возможности: - Сохранение поступающей от поисковых модулей информации. - Разметка поступающих упоминаний по принадлежности к определенным адресам.	Сохранение поступающей от поисковых модулей информации  Разметка поступающих упоминаний по принадлежности к адресам	Разработчик   Разработчик		
	2.5	<b>Расчет рисков</b> Будут реализованы следующие возможности: - Расчет и хранение исторически накопленного риска каждого адреса, кластера и владельца. - Выполнения разметки по риску для дальнейшей аналитики. - Расчет и хранение риска транзакций.	Расчет и хранение накопленного риска адреса/ кластера/ владельца  Выполнение разметки по риску  Расчет риска транзакций	Разработчик   Разработчик  Разработчик		
	3	<b>Обеспечение детального анализа данных и формирование выводов</b>			18 дней	1-я очередь



Сервер	№ п/п	Задача	Описание выполняемых работ	Планируемые к привлечению ресурсы	Сроки выполнения работ	Очередь разработки ПО
Создание сервера аналитики	3.1	<b>Работа с транзакциями</b> Будут реализованы следующие возможности: - Выдача совокупной информации о транзакциях. - Хранение совокупной информации о транзакциях. - Просмотр совокупной информации о транзакциях.	Проектирование системы работы с транзакциями (включая граф транзакций) Реализация системы работы с транзакциями (включая граф транзакций)	Системный аналитик  Ведущий разработчик		
	3.2	<b>Работа с адресами</b> Будет реализована возможность обеспечения получения данных об адресе.	Проектирование системы работы с адресами Реализация системы работы с адресами	Системный аналитик Ведущий разработчик		
	3.3	<b>Работа с кластерами</b> Будут реализованы следующие возможности: - Получение списка всех адресов кластера.	Проектирование системы работы с кластерами	Системный аналитик		

Сервер	№ п/п	Задача	Описание выполняемых работ	Планируемые к привлечению ресурсы	Сроки выполнения работ	Очередь разработки ПО
		<ul style="list-style-type: none"> <li>- Выдача совокупного риска всего кластера, истории по риску кластера.</li> <li>- Получение данных об одном адресе в нескольких режимах.</li> <li>- Получения всех транзакций кластера с возможностью сортировки по размеру, риску, наличию контрагентов в транзакциях.</li> </ul>	Реализация системы работы с кластерами	Ведущий разработчик		
			Проектирование системы работы с владельцами	Системный аналитик		
			Реализация системы работы с владельцами	Ведущий разработчик		
	3.4	<b>Работа с владельцами</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Получение списка владельцев.</li> <li>- Получение данных о конкретном владельце с учетом расчета оборота по биткойнам/рублям/долларам.</li> <li>- Добавление, обновление и удаление данных о владельце.</li> </ul>	Проектирование системы поиска и автозаполнения	Системный аналитик		
	3.5	<b>Поиск и автозаполнение</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Поиск и автозаполнение по адресу.</li> </ul>				



Сервер	№ п/п	Задача	Описание выполняемых работ	Планируемые к привлечению ресурсы	Сроки выполнения работ	Очередь разработки ПО
		<ul style="list-style-type: none"> <li>- Поиск и автозаполнение по названию владельца.</li> <li>- Проверка на существование адрес.</li> <li>- Проверка на существование транзакции.</li> <li>- Проверка на валидность адреса, которая определяет, создан ли адрес по правилам блокчейн биткойн.</li> <li>- Проверка на существование кластера.</li> </ul>	Реализация системы поиска и автозаполнения	Ведущий разработчик		
Создание сервера архивации	4	<b>Обеспечение архивации данных</b>			14 дней	1-я очередь
	4.1	<b>Резервирование базы данных</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Сохранение данных.</li> <li>- Хранение данных.</li> <li>- Просмотр данных.</li> </ul>	Проектирование системы резервного копирования базы данных Реализация системы резервного копирования базы данных	Системный аналитик Разработчик		
	4.2	<b>Ведение журнала запросов</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"> <li>- Создание запроса.</li> <li>- Обработка запроса.</li> </ul>	Проектирование журнала запросов (логирования запросов, записи логов)	Системный аналитик		

Сервер	№ п/п	Задача	Описание выполняемых работ	Планируемые к привлечению ресурсы	Сроки выполнения работ	Очередь разработки ПО
		<ul style="list-style-type: none"><li>- Сохранение информации о запросе.</li><li>- Хранение информации о запросе.</li><li>- Просмотр информации о запросе.</li></ul>	Реализация журнала запросов (логирования запросов, записи логов)	Разработчик		
	4.3	<b>Ведение истории изменений данных</b> Будут реализованы следующие возможности: <ul style="list-style-type: none"><li>- Сохранение информации о изменениях.</li><li>- Хранение информации о изменениях.</li><li>- Просмотр информации о изменениях.</li></ul>	Проектирование системы ведения истории изменения данных (логирования изменений, записи логов)	Системный аналитик		
			Реализация системы ведения истории изменения данных (логирования изменений, записи логов)	Разработчик		



Сервер	№ п/п	Задача	Описание выполняемых работ	Планируемые к привлечению ресурсы	Сроки выполнения работ	Очередь разработки ПО
Создание сервера поддержки веб-интерфейса пользователя	5	<b>Обеспечение обмена данными с пользователем</b> Будут реализованы следующие веб-интерфейсы для пользователей Системы: <ul style="list-style-type: none"> <li>- Интерфейс авторизации.</li> <li>- Интерфейс поиска.</li> <li>- Интерфейс информации.</li> <li>- Интерфейс основных контрагентов.</li> <li>- Интерфейс упоминания адресов.</li> <li>- Интерфейс списков транзакций.</li> <li>- Интерфейс информации о транзакциях.</li> <li>- Интерфейс построения графов транзакций.</li> <li>- Интерфейс адреса.</li> <li>- Интерфейс построения графов контрагентов.</li> <li>- Интерфейс списка владельцев.</li> <li>- Интерфейс информации об отдельном владельце.</li> <li>- Интерфейс интернет-поиска.</li> </ul>	Проектирование, создание макетов необходимых интерфейсов	Архитектор JAVA. Дизайнер.	20 дней	1-я очередь
			Разработка необходимых интерфейсов	Архитектор JAVA. Ведущий разработчик.		