Приложение
к Приказу Генерального директора ООО «Атомайз»
от 01.02.2022 г. № АТМ/01.02.2022/1-п

Политика информационной безопасности платформы Атомайз

(в части взаимодействия с пользователями)

г. Москва, 2022 г.

1. Термины, определения и принятые сокращения

В настоящем документе используются следующие термины и определения:

Аутентификационные данные – совокупность логина, пароля и иных данных (кодового словосочетания или пары Публичного и Приватного ключа, предоставляемых Пользователю при его регистрации Оператором информационной системы или вводимых Пользователем самостоятельно), необходимых для доступа Пользователя на Платформу.

Аутентификация – процедура проверки подлинности Пользователя, осуществляемая с использованием Аутентификационных данных и Кода подтверждения.

Идентификация (KYC) – совокупность мероприятий по установлению определенных законом сведений о Пользователях, их представителях, выгодоприобретателях, бенефициарных владельцах и подтверждению достоверности этих сведений с использованием оригиналов документов и (или) надлежащим образом заверенных копий и (или) государственных и иных информационных систем.

Информационная система (ИС) – информационная система, являющаяся составной частью Платформы и организованная на основе распределенного реестра. Внесение записей в отношении ЦФА (в том числе при их выпуске) осуществляются исключительно в Информационной системе.

Информация ограниченного доступа (ИОД) – информация, доступ к которой ограничен в соответствии с международными правовыми нормами (применимыми для РФ), законодательством РФ и внутренними нормативными документами Оператора, раскрытие которой может привести к финансовым потерям, возникновению претензий к Оператору со стороны регулирующих органов и третьих лиц и ущербу деловой репутации Оператора.

ИТ – информационные технологии, совокупность аппаратных и программных средств, используемых в работе Оператора.

ИТ ресурсы – принадлежащие как Оператору, так и работникам персональные компьютеры, мобильные устройства, съемные носители информации, принадлежащие Оператору корпоративная сеть, базы данных, файловые каталоги, информационные системы и компьютерные программы.

Оператор информационной системы (Оператор) – общество с ограниченной ответственностью «Атомайз» (ОГРН 1207700427714), действующее в качестве оператора информационной системы в соответствии с ФЗ о ЦФА и включенное Банком России в реестр операторов информационных систем.

Код подтверждения - временный код, отправляемый на устройство или номер телефона Пользователя с помощью приложения, предназначенного для временных кодов, или СМС-сообщений.

Кошелек Пользователя – программное средство, являющееся частью Информационной системы и предназначенное для учета ЦФА. Кошельку Пользователя присваивается уникальный идентификационный номер и соответствует уникальная пара Публичного и Приватного ключей.

Личный кабинет – закрытый раздел Платформы и/или функциональный компонент

Мобильного приложения, использование которого требует прохождения Регистрации и в дальнейшем – Аутентификации, предназначенный для совершения Пользователем Сделок по приобретению ЦФА при их выпуске, внесения записей в Информационную систему, взаимодействия с Оператором информационной системы (в том числе путем получения уведомлений), а также получения Пользователем доступа к информации о балансе Пользователя.

Мобильное приложение – программное обеспечение, позволяющее, после его установки на мобильном устройстве Пользователя и при соблюдении условий Правил, осуществлять доступ к Платформе.

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователи – обладатель ЦФА, Эмитент, оператор обмена ЦФА, прошедшие Регистрацию на Платформе и присоединившиеся к Правилам.

Платформа – программное обеспечение, которое включает Информационную систему и иные сопутствующие программные модули, обеспечивающие возможность взаимодействия Пользователя с Информационной системой. Платформа доступна на сайте Оператора информационной системы или посредством Мобильного приложения.

Правила - правила информационной системы, утвержденные в соответствии с уставом ООО «Атомайз», согласованные с Банком России в порядке, предусмотренном ФЗ о ЦФА, и размещенные на сайте Оператора информационной системы.

Приватный ключ – кодовая строка, при помощи которой осуществляется доступ к Кошельку Пользователя и которая необходима для осуществления Пользователем Транзакций. Приватный ключ в сочетании с Публичным ключом представляет собой усиленную неквалифицированную электронную подпись по смыслу Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Публичный ключ - парная соответствующему приватному ключу кодовая строка, к которой имеется открытый доступ и которая используется наряду с Приватным ключом для осуществления Пользователем Транзакций. Публичный ключ соответствует Кошельку Пользователя.

Поддержка, колл-центр – подразделение Оператора, обеспечивающее решение проблем, возникающих у Пользователя в процессе работы на Платформе.

Транзакция – операция по переходу ЦФА, осуществляемая в Информационной системе.

ЦФА – цифровой финансовый актив (по смыслу ч. 2 ст. 1 ФЗ о ЦФА), за исключением цифровых финансовых активов, удостоверяющих права участия в капитале непубличного акционерного общества) и(или) цифровое право, включающее одновременно цифровые финансовые активы и иные цифровые права (по смыслу части 6 ст. 1 ФЗ о ЦФА), которые выпускаются и учитываются в Информационной системе в соответствии с ФЗ о ЦФА, иными требованиями законодательства и настоящими Правилами. Каждому ЦФА соответствует определенный Смарт-контракт.

ФЗ о ЦФА – Федеральный закон № 259-ФЗ от 31.07.2020 «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

Иные термины и определения имеют значение, указанное в Правилах оператора информационной системы, размещенных на сайте Оператора информационной системы.

В Политике используются следующие сокращения:

ИТ – информационные технологии;

ПО – программное обеспечение;

ИС – информационная система;

2. Общие положения

Политика информационной безопасности платформы Атомайз (в части взаимодействия с пользователями) (далее – Политика) является документом Оператора, регламентирующим процесс взаимодействия Пользователя с Оператором информационной системы.

Политика разработана в соответствии с ФЗ о ЦФА, Федеральными законами № 152-ФЗ от 27.07.2006 «О персональных данных», № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и защите информации», а также в соответствии с Правилами информационной системы ООО «Атомайз».

3. Цели

Цель настоящего документа – обеспечение информационной безопасности в процессе использования Пользователями Платформы и обрабатываемой в ней информации.

Информационное взаимодействие Оператора и Пользователей в рамках настоящей Политики осуществляется на Платформе.

Платформа Оператора используется для предоставления Пользователям услуг, связанных с выпуском и оборотом ЦФА.

На Платформе Оператора хранится и обрабатывается информация, связанная с бизнес-процессами выпуска и оборота ЦФА, регистрации Пользователей и ведения реестра Пользователей, другая информация, необходимая для функционирования Платформы.

Важными видами информации, подлежащей обязательной защите, в том числе, являются персональные данные, сведения о ЦФА, учитываемых Платформой, Аутентификационные и идентификационные данные.

Доступность, целостность, конфиденциальность информации являются обязательными условиями правомерной и эффективной работы Платформы Оператора, что накладывает требования на работу Пользователей с Платформой.

Пользователям следует руководствоваться настоящей Политикой при работе с Платформой.

Нарушение настоящей Политики может привести к компрометации данных Пользователя, утраты им контроля над своими активами и к утрате ЦФА.

4. Порядок подключения к Платформе и работы с ней

Для подключения и работы с Платформой используются два типа взаимодействия:

- Web интерфейс;
- Мобильное приложение.

4.1. Регистрация

Перед началом работы с Платформой Пользователь должен пройти процедуру регистрации, ознакомиться и предоставить согласие с условиями документов, изложенных в пункте 2.2.1.3 Правил информационной системы Оператора.

Оператор проводит проверки Пользователя в соответствии с порядком, принятым Оператором. После прохождения проверок Пользователь регистрируется на Платформе, и создает свои идентификационные и Аутентификационные данные, которые являются правами доступа Пользователя к его ЦФА, учитываемых на Платформе.

На Платформе будет создан Личный кабинет Пользователя, Кошелек, в котором Пользователь получает информацию об актуальном балансе Кошелька, доступ к витрине, где отображаются все доступные для покупки ЦФА. В Личном кабинете Пользователь создает пару приватного и публичного ключа, а также шифр безопасности (Шифр безопасности состоит из 12 слов), который в дальнейшем позволит Пользователю самостоятельно восстановить ключи, в случае их утери.

После прохождения процесса создания ключей, Платформа отображает сообщение Пользователю о необходимости сохранить в надежном месте предоставленные данные. Пользователь должен обеспечить меры по защите ключей и сохранности шифра безопасности.

4.2. Деактивация Личного кабинета

Для деактивации Личного кабинета Пользователь может подать заявку на деактивацию своего Личного кабинета на Платформе. Пользователь подписывает заявку Кодом подтверждения, полученным в СМС-уведомлении на мобильный телефон.

Оператор удовлетворяет заявку в случае отсутствия на Кошельке Пользователя непогашенных ЦФА и отсутствия неисполненных других обязательств перед другими Пользователями Платформы.

Деактивация Личного Кабинета осуществляется через 30 календарных дней после даты подачи заявления об деактивации.

Пользователь вправе отозвать заявку на деактивацию Личного кабинета до даты предполагаемой деактивации, но не позднее рабочего дня, предшествующего дате деактивации.

Личный кабинет Пользователя, по которому проведена деактивация, не подлежит восстановлению на Платформе Оператора.

4.3. Восстановление доступа к Личному кабинету

Для восстановления доступа к Личному кабинету и приватного и публичного ключей Пользователю доступен раздел «Управление ключами», в котором Пользователь может по-новому создать пару публичного и приватного ключа по шифру безопасности, который Пользователь получает при регистрации на Платформе. Для восстановления ключей необходимо ввести «Шифр безопасности» в поле раздела «Управление ключами» и нажать на кнопку «Сгенерировать ключи».

В случае утери мобильного телефона и/или шифра безопасности, Пользователю необходимо обратиться в Колл-центр ООО «Атомайз» по телефону: 8-800-600-83-86, пройти процедуру подтверждения личности, сообщить сотруднику Колл-центра о потере мобильного устройства и/или потере шифра безопасности. Сотрудник Колл-центра зарегистрирует заявку и проконсультирует Пользователя о дальнейших действиях.

4.4. Процесс восстановления доступа к ЦФА

Данный функционал описывает возможность Платформы по восстановлению доступа к записям информационной системы по требованию обладателя ЦФА, если таковой был им утрачен.

Процесс восстановления доступа описан на схеме ниже (см. Рисунок 1)

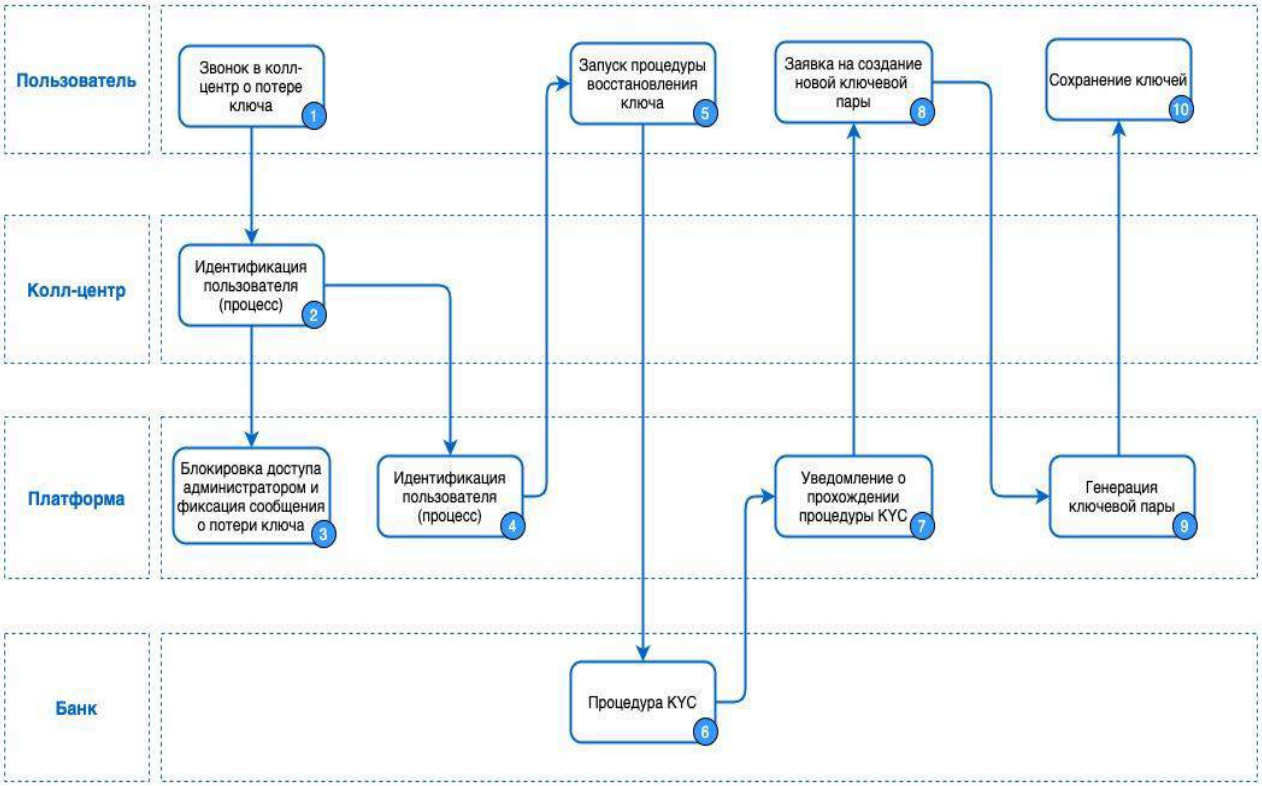

Рисунок 1

Описание шагов процесса представлено ниже (см. Таблица 1)

№ Шага	Описание шага
1	Пользователь обращается (телефонный звонок) в Колл-центр Платформы с сообщением о компрометации (потере) закрытого ключа.
2	Сотрудник Колл-центра инициирует процесс идентификации Пользователя и передает данные о поступившем обращении сотруднику Платформы.
3	Учетная запись и доступ в Личный кабинет блокируются сотрудником Платформы.
4	После завершения прохождения процесса идентификации Пользователя Платформа создает уведомление пользователю о разблокировке его учетной записи и получении доступа в Личный кабинет.
5	Для получения новой ключевой пары пользователь инициирует процедуру восстановления ключа.
6	Для восстановления ключей пользователь проходит повторную процедуру Идентификации. После успешного прохождения процедуры Идентификации у пользователя появляется возможность создания новой ключевой пары (кнопка “Восстановить ключи)”.
7	После успешного прохождения процедуры идентификации Платформа создает уведомление пользователю об успешном прохождении Идентификации.
8	Пользователь инициирует заявку на создание новой ключевой пары.
9	Платформа осуществляет создание закрытого и открытого ключа и шифра безопасности для Пользователя.
10	Пользователь получает закрытый и открытый ключ и сохраняет их (вне периметра Платформы) в соответствии с рекомендациями по безопасному хранению ключей.

Таблица 1

5. Требования к техническим и программным средствам работы с Платформой

Для работы с Платформой требуется:

- Для работы через web интерфейс необходимо любое устройство, подключенное к сети Интернет и имеющее установленный web браузер. Рекомендуемый браузер Google Chrome версии 89.0 и выше. Доступ к Платформе осуществляется через сайт https://atomyze.ru;
- Для работы через Мобильное приложение требуется смартфон под управлением iOS или Android с установленным приложением Atomyze. Приложение устанавливается средствами Apple AppStore или GooglePlay. В Apple AppStore или GoolgePlay находятся актуальные версии приложений, установка приложения на смартфон Пользователя регулируется правилами и политиками Apple AppStore или GooglePlay.

6. Требования к информационной безопасности.

Пользователь обязуется:

- не передавать Аутентификационные данные и Коды подтверждения третьим лицам, в том числе сотрудникам Оператора;
- принимать меры по защите Аутентификационных данных и Кодов подтверждения от разглашения третьим лицам, в том числе воздерживаться от использования для доступа к Личному кабинету мобильных устройств со снятыми программными ограничениями производителя на установку неразрешенного программного обеспечения;
- не использовать Платформу в целях совершения сделок, направленных на легализацию (отмывание) доходов, полученных преступным путем, финансирование терроризма и финансирование распространения оружия массового уничтожения.

Пользователю рекомендуется:

- использовать сложные пароли, длиной не меньше 8 символов, содержащие заглавные и прописные буквы латинского алфавита, цифры, специальные символы;
- хранить идентификационные и Аутентификационные данные в защищенном месте недоступном для посторонних лиц, в специализированном ПО;
- не открывать электронные письма от неизвестных отправителей;
- не посещать непроверенные сайты в сети Интернет;
- использовать только лицензионное ПО;
- устанавливать ПО только из официальных источников (Apple AppStore, Apple MacStore, Windows Store, Google Play);
- установить на устройство, используемое для работы с платформой, антивирус;
- не проводить на своём мобильном устройстве настроек типа root и jailbreak;
- при возникновении подозрений о компрометации идентификационных и Аутентификационных данных незамедлительно обратиться в Поддержку Оператора для блокировки;
- если вы обнаружили что sim-карта вашего телефона неожиданно заблокирована, незамедлительно обратитесь в Поддержку Оператора.

7. Контакты Поддержки Оператора в рамках взаимодействия

Наименование	Номер телефона, e-mail
Колл-центр	8-800-600-83-86 help@atomyze.ru