ПОЛОЖЕНИЕ

о порядке действий в случае нештатного функционирования или прекращения функционирования программно-аппаратных средств инвестиционной платформы

г. Москва
2022

1. Общие положения

1.1. Положение «О порядке действий в случае нештатного функционирования или прекращения функционирования программно-аппаратного средства инвестиционной платформы» (далее – Положение) определяет основные понятия и требования Оператора платформенного сервиса (далее – Оператор) для обеспечения бесперебойного функционирования инвестиционной платформы (далее – Платформа), а также при возникновении нештатных ситуаций в Платформе, связанные с:

- надежностью и бесперебойностью функционирования Платформы;

- доступностью сервисов Платформы;

- несанкционированным доступом к Платформе.

1.2. Настоящее Положение предусматривает порядок действий для восстановления штатного функционирования Платформы и меры, направленные на минимизацию отрицательного влияния на процессы платформенного сервиса, работоспособность которых оказалась нарушенной при возникновении нештатной ситуации.

1.3. Для поддержания бесперебойного функционирования Платформы должен обеспечиваться:

- доступ участников к Платформе в течение всего срока действия договора оказания услуг по привлечению инвестиций и договора оказания услуг по содействию в инвестировании;

- сохранность данных в системе Платформы, в течение сроков, установленных Правилами Платформы и законодательством Российской Федерации;

- своевременное переключение/восстановление/разворачивание функционирования Платформы на резервном программном обеспечении/резервном сайте при возникновении нештатной ситуации.

2. Определения

Для целей настоящего Положения используются следующие термины и определения:

Инцидент – это любое событие, которое не является частью штатного функционирования Платформы и вызывает или может негативно отразиться на бесперебойности или качестве функционирования Платформы.

Нештатная ситуация – ситуация, которая выходит за рамки правил и технологии работы Платформы и требует для ее разрешения специально организованной деятельности персонала оператора Платформы и/или провайдера критичных услуг.

Несанкционированные операции в Платформе – это противоправные преднамеренные деяния (действия, бездействия, злоупотребление доверием) персонала оператора Платформы/пользователя Платформы/провайдера критичных услуг или третьей стороны, направленные на несанкционированный доступ и использование информации Платформы.

К несанкционированным операциям относятся:

- распространение внутренней конфиденциальной информации;

- нарушение прав доступа к информации, оборудованию, допущение утечки информации;

- умышленное удаление/изменение информации, которое может привести к невыполнению обязательств оператора Платформы перед пользователями Платформы и третьими лицами;

- несанкционированное использование/передача реквизитов/ключей электронной подписи с целью получения инвестиций, а также перевода/хищения денежных средств.

3. Критически важные процессы Платформы

3.1. Под критически важными процессами с точки зрения обеспечения режима штатного функционирования Платформы понимаются такие процессы, которые в случае нарушения должны быть восстановлены в течение не более 24 часов.

3.2. В перечень критически важных процессов Платформы с учетом характера и масштаба деятельности Оператора включены:

3.2.1 Доступ пользователей к сервисам Платформы. Ключевые процессы: регистрация, авторизация, создание профиля, пополнение лицевого счета.

3.2.2. Инвестиционное предложение. Ключевые процессы: заявка на размещение инвестиционного предложения, его формирование, подписание электронной подписью.

3.2.3. Инвестирование в проект. Ключевые процессы: акцепт инвестиционного предложения, отзыв акцепта, перевод инвестиций получателю.

3.2.4. Учет операций по номинальному счету. Ключевые процессы: учет поступления/перевода/вывода средств по каждому бенефициару номинального счета; синхронизация операций по номинальному счету с персональным счетом каждого инвестора;

3.2.5. Сопровождение исполнения договоров инвестирования. Ключевые процессы: распределение средств, поступивших на номинальный счет от лица, привлекающего инвестиции, по счетам бенефициаров – инвесторов пропорционально размерам их требований, автоматическое уведомление о сроке платежа и просрочке.

4. Требования к функционированию Платформы

4.1. Оператор обеспечивает функционирование Платформы в режиме, обеспечивающем выполнение следующих технических требований:

- должно обеспечиваться функционирование Платформы в круглосуточном режиме 7 дней в неделю 365 дней в году;

- допустимое максимальное время нештатного функционирования или прекращения функционирования критически важных процессов не должно превышать 24 часов;

- должно обеспечивать оповещение пользователей об инциденте;

- использование средства обеспечения сохранности данных, обрабатываемых Платформой в случае возникновения аварийных ситуаций: отказы в системе электроснабжения, отказы аппаратных средств, отказы программных средств;

- обеспечение на регулярной основе (не реже одного раза в сутки) резервного копирования данных Платформы;

- обеспечение защиты информации Платформы от потери и несанкционированного доступа на этапах ее обработки.

5. Программно-аппаратные средства Оператора

1.3. Для обеспечения штатного функционирования Платформы Оператор использует следующие программно-аппаратные средства:

- программное обеспечение (далее – ПО);

- OpenJDK 17

- операционная система Ubuntu Linux 22.04 LTS;

- сервер приложений Apache Tomcat 10.1.5;

- СУБД PostgreSQL 14.7

- Брокер сообщений RabbitMQ 3.11.12

- Сервер авторизации Keycloak 20.0.3

- Средство контейнеризации Docker CE 23.0.3

- Оркестратор контейнеров Kubernetes

- СУБД для сбора метрик Prometheus

- Панель для мониторинга приложений Grafana
- Система управления контентом Strapi
- каналы связи и средства безопасной передачи данных.
- Облачная инфраструктура Selectel
- Регулярно обновляемые HTTPS-сертификаты Letsencrypt

6. Типы инцидентов

6.1. Все инциденты разделяются на категории, каждому из которых присваивается уровень критичности и приоретизация согласно, приведенным ниже таблицам.

Таблица 1 «Категории инцидентов».

Значение	Описание
Программно-технические (включая выход из строя технических средств, сбои в работе автоматизированных информационных систем)	Инциденты, связанные с работой программных и аппаратных средств, участвующих в критически важных процессах Оператора, а также связанные с работой средств защиты информации. **Отказ работы сервисов:** - Приостановка работы СУБД - Приостановка работы брокера сообщений - Приостановка работы сервера авторизации - Приостановка работы сервисов самой платформы **Дефекты, внесенные в процессе разработки ПО:** - Дефекты в коде сервисов - Дефекты в коде используемых библиотек и фреймворков **Сбои, связанные с безопасностью:** - DDoS-атаки на сервис - Попытки атак на сервис **Сбои, связанные с нехваткой ресурсов:** - Используемое ПО не успевает обрабатывать запросы клиентов - Заканчиваются ресурсы (диск, ОЗУ, прочее) на серверах **Сбои, связанные с финансовыми причинами:** - Отказ сервисов по причине пропущенной оплаты

Отказ провайдеров услуг	Приостановка критически важных процессов из-за отказа провайдера услуг (Интернет). Приостановка критически важных процессов из-за отказа провайдера услуг (Облачный провайдер).
Перебои в электроснабжении	Приостановка критически важных процессов из-за перебоев в электроснабжении.
Административные	События и инциденты, связанные с административными нарушениями (в том числе нарушениями трудового распорядка).

6.2. После определения категории инцидента определяется его критичность по шкале, приведенной в Таблице 2. Приоритет в обработке должен отдаваться событиям с большим уровнем критичности.

Таблица 2 «Критичность инцидентов».

Значение	**Приоритет (целевое время реагирования ответственных лиц)**	**Описание**
Высокий	8 часа	Инцидент, указывающий на событие, связанное с тем, что была успешно атакована, затронуты критически важные процессы Оператора. Это может привести к нарушению работы критических серверов, приводящих к недоступности сервисов Платформы и полному непредоставлению услуг. В
Умеренный	16 часов	Инцидент, который потенциально может привести к компрометации данных системы.
Низкий	24 часов	Инцидент, не представляющий угрозу безопасности Платформы. К таким относятся нарушение трудового распорядка и других корпоративных правил.

7. Реагирование на инциденты

7.1. Реагирование на инцидент включает следующие этапы:

7.1.1. Обнаружение и анализ;

7.1.2. Регистрация;

7.1.3. Восстановление.

7.2. На этапе обнаружения и анализа осуществляется сбор информации об инциденте и его категоризация. Порядок действий на этапе обнаружения: **ЭТАП**	**Действия ответственного лица**
Обнаружение и анализ	1) Сбор информации об инциденте
	2) Выявление наступивших или потенциально возможных негативных последствий для Платформы
	3) Сопоставление с другими событиями Платформы
	4) Если событие имеет признаки инцидента – доклад руководителю платформы

7.3. Регистрация. На данном этапе принимается решение о регистрации инцидента в электронном журнале учета по форме приведенной в разделе 8 настоящего Положения. Для каждого инцидента устанавливается уровень критичности и соответствующие ему критерии реакции (высокий, умеренный, низкий). Порядок действий на этапе регистрации:

ЭТАП	**Действия**
Регистрация	1) Информирование руководства Платформы о выявленном инциденте.
	2) Принятие решения о присвоении инциденту категории и уровня критичности.
	3) Назначение ответственного лица (осуществляется из числа работников на основании приказа руководителя компании).
	4) Регистрация в журнале учета инцидентов.

7.4. Цель этапа восстановление – приведение Платформы в состояние, в котором находилась до возникновения инцидента. Порядок действий на этапе восстановления:

ЭТАП	**Действия**
Восстановление	1) Принятие решения о расследовании выявленного инцидента, время выполнения - не более 8 часов
	2) Закрытие инцидента – возвращение Платформы к функционированию в штатном режиме, время выполнения - не более 24 часов
	3) Реализация мер по снижению инцидентов и поддержания бесперебойного функционирования Платформы, указанных в разделе 9 Регламента.

7.5. Порядок реагирования оператора на произошедший функциональный сбой с учетом его категории:

Значение	**Описание**
Программно-технические (включая выход из строя технических средств, сбои в работе автоматизированных информационных систем)	1. Анализ журналов сервиса, просмотр сервисов мониторинга и алертов, классификация проблемы по таблице «Категории инцидентов». 2. Если восстановление сервиса затягивается, оповестить пользователей о временной недоступности сервиса Дальнейшие шаги зависят от типа сбоя **Сбои, связанные с отказом сервисов (кроме СУБД):** 3. Выбрать один из возможных методов решения проблем: - Перезагрузка сервиса - Пересоздание экземпляров сервиса - Анализ и устранение прочих причин падения **Сбои, связанные с отказом СУБД:**

	3. Выбрать один из возможных методов решения проблем: - Разворачивание БД из резервной копии. - Перезагрузка СУБД - Анализ и устранение прочих причин падения **Сбои, связанные с дефектами в разработанном ПО:** 3. Если применимо, попробовать развернуть более старую версию сервиса 4. Занести задачу в системе отслеживания задач с подробным описанием дефекта и логами 5. Устранить дефект **Сбои, связанные с нехваткой ресурсов:** 3. Попытаться освободить недостающие ресурсы: очистить диск, завершить ненужные процессы 4. Если освобождение ресурсов не дало результата, увеличить количество недостающего ресурса путем изменения конфигурации серверов 4.1 Если нехватка ресурса вызвана дефектом ПО, см. пункт «Сбои, связанные с дефектами в разработанном ПО» **Сбои, связанные с финансовыми причинами:** 3. Произвести оплату, включить отключенные сервисы **Сбои, связанные с безопасностью:** 3. Определить, на каком уровне ведется атака (сетевой, приложения, операционный) 4. Если применимо, попробовать задействовать инструменты для предотвращения атак (DDoS-экраны, Firewall-ы) 5. Если есть подозрения, что конфиденциальные данные утекли: 5.1 Изолировать атакуемые сервисы 5.2 Оповестить внешние стороны (клиентов, регуляторов) о возможной утечке данных. **ПОСЛЕ УКАЗАННЫХ ДЕЙСТВИЙ:** 1. Продолжить мониторинг и отслеживать, когда сервис полностью будет доступен 2. Завести инцидент в системе отслеживания задач с подробным описанием проблемы, логами,

	метриками из системы мониторинга, и, если применимо, решением
Отказ провайдеров услуг	Смена провайдера, предоставляющего услуги
Перебои в электроснабжении	Переход на резервное питание
Административные	Исправление причины инцидента, при необходимости консультируясь с юристами и государственными органами

8. Оповещение об инцидентах и отчетность

8.1. При возникновении инцидента, препятствующему штатному функционированию Платформы, Оператор оповещает пользователей о сбое через личный кабинет пользователя путем публикации соответствующего сообщения.

В случае невозможности входа в личный кабинет информация об инциденте публикуется на главной странице Платформы.

Для взаимодействия с клиентом в случае возникновения функционального сбоя также может быть использована электронная почта.

8.2. После возобновления функционирования Платформы Оператор не позднее 30 минут размещает на Платформе информацию в форме электронного сообщения с указанием даты и времени возобновления работы Платформы, о мерах принятых Оператором для устранения функционального сбоя.

8.3. Оператор учитывает информацию о каждом инциденте в электронном журнале учета инцидентов по форме, приведенной ниже, без фиксирования их на бумажном носителе. Если учет информации в электронной форме невозможен по объективным причинам, ответственный работник учитывает информацию об инцидентах Платформы на бумажном носителе с указанием причин, по которым регистрация в электронной форме невозможна (например, отсутствие электроснабжения, доступа к сетевому диску, на котором содержится файл электронного журнала). После устранения причин, послуживших основанием для учета инцидента на бумажном носителе, информация об инциденте вносится в электронный журнал. Резервное копирование электронного журнала осуществляется не реже одного раза в месяц на переносной электронный носитель. Содержащиеся в журнале учета записи выводятся на бумажный носитель не позднее одного месяца после окончания календарного года.

Журнала учета инцидентов в Платформе

№ п/п	Дата и время регистрации инцидента	Дата выявления инцидента	Дата и время устранения инцидента	Процесс, котором произошел инцидент	Категория и уровень инцидента	Краткое описание инцидента	Причины возникновения инцидента	Принятые решения по предотвращению инцидента	Контрольные меры/мероприятия	ФИО ответственного работника

9. Реализация мер по снижению инцидентов

9.1. В целях снижения вероятности возникновения функциональных сбоев Оператор осуществляет:

- тестирование программно-аппаратных средств с целью определения максимальной производительности; предупреждения отказов системы в промышленной эксплуатации, ухудшения производительности показателей программно-аппаратных средств; выявления зависимых, скрытых сбоев, ошибок (например, некорректных настроек);

- мониторинг показателей работоспособности программно-аппаратных средств, информации о функциональных сбоях, количества и частоты ошибок в результате использования программно-аппаратных средств Платформы. Мониторинг показателей может осуществляться с помощью программных средств **Prometheus, Grafana**.

9.2. Полученная в результате тестирования и мониторинга информация учитывается в базе данных о выявленных событиях функциональных сбоев.

9.3. На основании полученной информации осуществляется:

- анализ состояния программно-аппаратных средств и оборудования;

- оценка степени влияния произошедших (возможных) инцидентов на доступность и качество услуг Платформы;

- построение шаблонов характерного поведения различных компонентов программно-аппаратных средств и выявление ее отклонений;

- поиск проблем и прогнозирование возникновения функциональных сбоев.

9.3. В зависимости от результатов проведенного анализа для целей снижения вероятности возникновения функциональных сбоев могут быть приняты следующие меры:

- внесение изменений в процессы Платформы;

- обновление и модернизация программно-аппаратных средства;

- дополнительные способы контроля в зависимости от характера поведения различных компонентов программно-аппаратных средств;

- обучение участников процессов;

- автоматизация выявления событий, приводящих к функциональным сбоям.

9.4. Для обеспечения оперативного восстановления штатного функционирования Платформы на ежедневной основе осуществляется резервное копирование данных Платформы.

9.5. Для обеспечения защиты информации Платформы от потери и несанкционированного доступа на этапах ее обработки осуществляется:
- обмен данными по протоколу https в зашифрованном виде;
- аутентификация и идентификация всех пользователей при входе в систему;
- контроль допуска к информации для пользователей разных уровней;
- обнаружение и регистрация попыток несанкционированного доступа;
- контроль работоспособности программно-аппаратных средств.

9.6. Ответственным за штатное функционирование программно-аппаратных средств и устранение функциональных сбоев является технический директор ООО «ПФЛ Новые инвестиции».