УТВЕРЖДАЮ
Директор ООО «Файнекс»

_____А.А. Сташевский
20.06.2023

ПЛАН
мероприятий по обеспечению непрерывной работы и восстановлению работоспособности информационной системы ООО «Файнекс»

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий План мероприятий по обеспечению непрерывной работы и восстановлению работоспособности информационной системы ООО «Файнекс» (далее – ПОНРВ) определяет перечень организационных и технологических мероприятий, которые должны выполняться до, во время и после возникновения кризисной (сбойной) ситуации в информационной системе ООО «Файнекс» (далее – Организация).

1.2. Настоящий ПОНРВ разработан в соответствии с Положением о требованиях, которым должны соответствовать отдельные заявители для регистрации их в качестве резидентов Парка высоких технологий (далее – ПВТ), утвержденным решением Наблюдательного совета ПВТ, Политикой информационной безопасности (кибербезопасности) ООО «Файнекс», Положением по обеспечению непрерывной работы и восстановления работоспособности информационной системы ООО «Файнекс».

1.3. Задачами настоящего ПОНРВ являются:

определение основных источников угроз и рисков возникновения кризисных (сбойных) ситуаций;

определение основных мер, предпринимаемых в подготовительном периоде, по снижению рисков возникновения кризисных (сбойных) ситуаций;

организация действий должностных лиц Организации при возникновении кризисных (сбойных) ситуаций;

определение мер, предпринимаемых после возникновения и устранения кризисной (сбойной) ситуации;

определение порядка тестирования и пересмотра ПОНРВ.

1.4. Для целей настоящего Положения нижеприведенные термины используются в следующих значениях.

архивирование – запись информации в электронном виде для долговременного хранения;

информационная система Организации – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств, используемая Организацией для осуществления своей деятельности;

кризисная (сбойная) ситуация – чрезвычайное происшествие, приводящее к нарушению процесса функционирования информационной системы Организации в целом, одной или нескольких отдельных ее частей;

оператор дата-центра – организация, которая осуществляет выполнение работ в рамках настоящего ПОНРВ на основании договора между ней и Организацией, а также на основании Соглашения об уровне услуг (SLA);

ПК – персональный компьютер;

ПО – программное обеспечение;

резервное копирование — процесс создания копии данных на носителе (жёстком диске и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения;

СВР – показатель, определяющий степень вероятности реализации угрозы информационной безопасности;

СТП – показатель, определяющий степень тяжести последствий от реализации угрозы информационной безопасности;

1.5. Структурно информационная система Организации состоит из следующих основных компонентов:

криптоплатформа – основной компонент информационной системы Организации, автоматизированная система, включающая в себя функции Онлайн-площадки, администрирования, настройки и управления Онлайн-площадкой и учета операций с цифровыми знаками (токенами), сервер базы данных;

внешние системы: системы взаимодействия с финансовыми / банковскими учреждениями по получению-отправке платежей, система для проведения операций с использованием реквизитов банковских платежных карточек по приобретению и выводу на фиатные денежные средства цифровых знаков (токенов); ПО «Система открытого взаимодействия»; система рассылки SMS- и Email-сообщений; система хранения отчетов, иные системы, подключаемые по мере развития и расширения функционала криптоплатформы;

ПК работников Организации.

1.6. Программно-технические комплексы криптоплатформы и внешних систем работают в виртуальной среде стороннего дата-центра. ПК работников Организации расположены в локальной вычислительной сети Организации.

1.7. На компоненты информационной системы Организации воздействуют угрозы внешнего и внутреннего происхождения, которые обуславливают вероятность возникновения кризисных (сбойных) ситуаций.

Перечень основных угроз и рисков возникновения кризисных (сбойных) ситуаций приведен в Приложении 1 настоящего ПОНРВ.

1.8. В отношении угроз, риски реализации которых являются недопустимыми, в подготовительном периоде (в режиме штатного функционирования) Организацией реализуется комплекс организационных и технологических мер, приведенных в Главе 2 настоящего ПОНРВ.

По объективным причинам предпринятых мер может оказаться недостаточным для минимизации риска до уровня «допустимый». В этом случае

остаточный риск обрабатывается в соответствии с Методикой управления риском нарушения информационной безопасности ООО «Файнекс».

ГЛАВА 2
ОСНОВНЫЕ МЕРЫ, ПРЕДПРИНИМАЕМЫЕ В ПОДГОТОВИТЕЛЬНОМ ПЕРИОДЕ, ПО СНИЖЕНИЮ РИСКОВ ВОЗНИКНОВЕНИЯ КРИЗИСНЫХ (СБОЙНЫХ) СИТУАЦИЙ

2.1. С целью снижения рисков возникновения кризисных (сбойных) ситуаций в подготовительный период силами Организации, а также силами стороннего дата-центра, реализуются организационные и технологические меры.

2.2. Силами Организации в подготовительный период реализуются следующие мероприятия:

организация резервирования основных процессов информационной системы Организации;

организация резервного копирования баз данных и образов ПО;

контроль работоспособности резервных компонентов информационной системы Организации;

реализация мероприятий по обеспечению информационной безопасности Организации;

организация мониторинга состояния компонентов криптоплатформы;

проведение периодического технического обслуживания средств телекоммуникации;

ограничение доступа к компонентам информационной системы Организации;

использование лицензионного ПО;

резервное копирование данных;

архивирование данных;

контроль соблюдения разработчиками установленных действующими техническими нормативными правовыми актами правил разработки ПО;

обеспечение наличия актуальных версий проектной и эксплуатационной технической документации на компоненты информационной системы Организации;

разработка ПОНРВ и проведение его тестирования;

организация взаимодействия участников ПОНРВ, заключение договоров, составление и актуализация контактных сведений участников ликвидации кризисных (сбойных) ситуаций.

Организацию мероприятий, указанных в настоящем пункте, осуществляет должностное лицо, ответственное за системное администрирование и информационную безопасность в Организации.

2.3. Оператор дата-центра в рамках договора с Организацией обеспечивает:

резервирование вычислительных процессов информационной системы Организации и мест обработки информации в соответствии с технологическими процессами, реализованными оператором дата-центра;

резервирование мест хранения резервных копий и архивов данных информационной системы Организации.

2.4. Перечень данных, подлежащих резервному копированию и архивированию, сроки копирования, а также обязанности должностного лица Организации, ответственного за реализацию указанного процесса, определяются Регламентом резервного копирования и архивирования данных информационной системы ООО «Файнекс».

ГЛАВА 3
ДЕЙСТВИЯ РАБОТНИКОВ ПРИ ВОЗНИКНОВЕНИИ КРИЗИСНЫХ (СБОЙНЫХ) СИТУАЦИЙ

3.1. После реализации мер по обработке рисков в подготовительный период, имеют место остаточные риски, которые обуславливают возникновение кризисных (сбойных) ситуаций информационной системы Организации.

3.2. Для оперативного реагирования на кризисные (сбойные) ситуации информационной системы в Организации реализуются мероприятия по оповещению должностных лиц Организации о кризисных (сбойных) ситуациях, в том числе в нерабочее время.

3.3. Источниками информации о возникновении кризисной (сбойной) ситуации являются:

программно-аппаратные средства мониторинга событий системного и прикладного ПО;

программно-аппаратные средства безопасности;

работники Организации;

контрагенты Организации и взаимодействующие с ней сервисы;

пользователи информационной системы.

3.4. Участниками ликвидации кризисных (аварийных) ситуаций являются:

директор Организации;

системный администратор Организации;

работник оператора дата-центра.

3.5. Перечень мероприятий, реализуемый системным администратором Организации и сроки их выполнения при возникновении кризисных (сбойных) ситуаций, а также контактные данные участников ликвидации кризисных (аварийных) ситуаций представлены в Приложении 2 настоящего ПОНРВ.

ГЛАВА 4
МЕРЫ, ПРЕДПРИНИМАЕМЫЕ ПОСЛЕ ВОЗНИКНОВЕНИЯ И УСТРАНЕНИЯ КРИЗИСНОЙ (СБОЙНОЙ) СИТУАЦИИ

4.1. Для проведения расследования причин возникновения кризисной (сбойной) ситуации и действий персонала Организации и сторонних организаций в указанной ситуации может проводится служебное разбирательство.

4.2. Для проведения служебного разбирательства распоряжением директора Организации создается комиссия, в которую включаются заинтересованные лица Организации.

4.3. В процессе работы комиссией устанавливаются следующие основные обстоятельства:

своевременность получения работниками Организации информации о возникновении (признаках возникновения) кризисной (сбойной) ситуации;

действия работников Организации и сторонних организаций по устранению (локализации) кризисной (сбойной) ситуации;

причины возникновения кризисной ситуации;

прямой и косвенный ущерб, понесенный Организации от кризисной (сбойной) ситуации;

учитывалась ли возможность ее возникновения в ПОНРВ;

наличие подобных кризисных (сбойных) ситуаций;

иные обстоятельства, существенные для оценки причин возникновения кризисной (сбойной) ситуации и действий персонала Организации и сторонних организаций в указанной ситуации.

4.4. По результатам работы комиссия вырабатывает предложения по внедрению дополнительных организационных и практических мер по повышению надежности и восстановлению работоспособности информационной системы Организации.

ГЛАВА 5
ТЕСТИРОВАНИЕ И ПЕРЕСМОТР ПОНРВ

5.1. Для успешного планирования действий в кризисных (сбойных) ситуациях регулярно, но не реже одного раза в год Организацией проводится тестирование (контроль) действий, предусмотренных ПОНРВ. Данное тестирование предполагает воспроизведение отдельного сценария возникновения и развития кризисной (сбойной) ситуации в функционировании информационной системы Организации. Информация по результатам тестирования ПОНРВ отражается в актах испытаний ПОНРВ, протоколах установленных несоответствий, планах корректирующих мероприятий.

5.2. ПОНРВ подлежит регулярному профилактическому, частичному или полному пересмотру.

5.2.1. Профилактический пересмотр ПОНРВ проводится ежегодно для поддержания ПОНРВ в актуальном состоянии или для оценки эффективности ПОНРВ в случае необходимости.

5.2.2. Частичный пересмотр ПОНРВ проводится при изменении:

конфигурации информационной системы Организации, не изменяющей технологии обработки информации;

численности и состава персонала, а также его обязанностей и полномочий.

5.2.3. Полный пересмотр ПОНРВ проводится в следующих случаях:

при изменении перечня решаемых задач или конфигурации информационной системы Организации, приводящей к изменению технологии обработки данных;

при получении неудовлетворительных (отрицательных) результатов тестирования (контроля);

после урегулирования кризисных (сбойных) ситуаций.

5.3. Организация осуществляет периодический контроль качества предоставляемых сторонней организацией (сторонними организациями) услуг методом анализа качества и своевременности проводимых работ, сведений об используемых средствах защиты и безопасности, оценки имеющих место рисков нарушения непрерывности работ и безопасности информации.

Приложение 1

к Плану мероприятий по обеспечению непрерывной работы и восстановлению работоспособности информационной системы ООО «Файнекс»

ПЕРЕЧЕНЬ
основных угроз и рисков возникновения кризисных (сбойных) ситуаций[1]

№	Угроза	СВР угрозы	СТП при реализации угрозы	Риск реализации угрозы
1	Стихийные бедствия в виде наводнения, землетрясения и т.д.	нереализуемая	критическая	допустимый
2	Пожар в здании дата-центра	минимальная	критическая	недопустимый
3	Сбои в подаче электропитания дата-центра	высокая	средняя	недопустимый
4	Сбои в работе коммуникационного оборудования	высокая	средняя	недопустимый
5	Сбои в работе серверного оборудования	высокая	средняя	недопустимый
6	Сбои при отключении кондиционирования и вентилирования	средняя	высокая	недопустимый
7	Сбои в результате атак внешних злоумышленников, направленных на отказ в обслуживании	высокая	средняя	недопустимый
8	Сбои в результате несанкционированного проникновения внешних и	средняя	высокая	недопустимый

[1] сопоставление СВР и СТП для оценки рисков нарушения непрерывной работы информационной системы Организации представлены в приложении 2 к Методике управления риском нарушения информационной безопасности ООО «Файнекс»

	внутренних злоумышленников			
9	Сбои в результате замены, ввода в эксплуатацию нового системного и прикладного ПО	средняя	высокая	недопустимый
10	Сбои в результате замены, ввода в эксплуатацию нового оборудования	средняя	высокая	недопустимый
11	Ошибки персонала	средняя	высокая	недопустимый

Приложение 2

к Плану мероприятий по обеспечению непрерывной работы и восстановлению работоспособности информационной системы ООО «Файнекс»

ПЕРЕЧЕНЬ МЕРОПРИЯТИЙ И СРОКИ ИХ ВЫПОЛНЕНИЯ ПРИ ВОЗНИКНОВЕНИИ КРИЗИСНЫХ (СБОЙНЫХ) СИТУАЦИЙ

№	Содержание мероприятий	Время М[2]
1.	В случае выхода из строя компонентов ПТК онлайн-площадки:	
1.1.	Получение сведений о наличии (признаках наличия) кризисной (сбойной) ситуации	М+0
1.2.	Определение степени серьезности и масштабов кризисной (сбойной) ситуации	М+20
1.3.	выявление причин возникновения кризисной (сбойной) ситуации	М+30
1.4.	выявление неработоспособных компонентов информационной системы Организации, локализация кризисной ситуации, определение причин нарушений, возможности устранения нарушения собственными силами	М+40
1.5.	информирование заинтересованных работников Организации о приостановке работы криптоплатформы	М+50
1.6.	информирование о возникновении кризисной (сбойной) ситуации должностного лица, ответственного за системное администрирование и информационную безопасность в Организации, и работника оператора дата-центра по каналам связи с использованием контактных сведений в соответствии с таблицей ниже	М+70
1.7.	информирование директора Организации о времени, источнике информации и обстоятельствах возникновения кризисной (сбойной) ситуации	М+80
1.8.	размещение на сайте Организации информации о временном приостановлении работы криптоплатформы	М+120
1.9.	при необходимости актуализация необходимых данных в производственной системе управления базами данных	М+240
1.10.	при восстановлении работоспособности компонентов информационной системы, проведение тестирования и включение в производственный режим	М+260

[2] Указывается в минутах с момента начала наступления события

№	Содержание мероприятий	Время $М^2$
2.	В случае обнаружения попытки несанкционированного изменения данных о фактически совершаемых действиях клиентов:	
2.1.	получение информации о совершении клиентом подозрительных действий	М+0
2.2.	с применением поисковой системы Elasticsearch проведение анализа подозрительных действий клиентов	М+20
2.3.	при выявлении попыток совершения клиентом незадекларированных действий, блокирование IP-адрес (адреса), с которого (которых) предпринималась попытка несанкционированных действий	М+30
2.4.	информирование директора Организации о данном инциденте	М+40
3.	В случае выявления подозрительных событий системного и прикладного программного обеспечения:	
3.1.	получение от средств мониторинга информации о подозрительных событиях системного (прикладного) ПО	М+0
3.2.	сбор и анализ событий, правил корреляции, которые могут быть существенными для определения причин и источников подозрительной активности	М+30
3.3.	при необходимости локализация источников подозрительной активности, или принятие иных мер по недопущению дальнейшего распространения вредоносной активности на иные компоненты информационной системы Организации	М+40
3.4.	выявление причин возникновения вредоносной активности	М+50
3.5.	при необходимости направление информации должностному лицу, ответственному за системное администрирование и информационную безопасность в Организации, и работнику оператора дата-центра	М+60
3.6.	информирование директора Организации о данном инциденте	М+65
3.7.	контроль ситуации	М+80
4.	В случае выявления признаков нарушения доступности онлайн-площадки в результате реализации злоумышленниками внешних атак, направленных на отказ в обслуживании (DOS, DDOS):	
4.1.	получение информации о снижении доступности криптоплатформы	М+0
4.2.	оценка количества обращений к криптоплатформе	М+10
4.3.	определение возможной (возможных) причин потери (снижения) доступности криптоплатформы	М+20

№	Содержание мероприятий	Время M^2
4.4	при необходимости направление информации должностному лицу, ответственному за системное администрирование и информационную безопасность в Организации, и работнику оператора дата-центра	M+40
4.5	информирование директора Организации об инциденте	M+50
4.6	при необходимости размещение на интернет-сайте Организации информации о временном приостановлении работы криптоплатформы	M+60
4.7	контроль выполненных работ	M+80

КОНТАКТНЫЕ ДАННЫЕ УЧАСТНИКОВ ЛИКВИДАЦИИ КРИЗИСНЫХ (АВАРИЙНЫХ) СИТУАЦИЙ

Должность (роль)	ФИО	Контактные данные
Директор		
Должностное лицо, ответственное за системное администрирование и информационную безопасность		
Системный администратор		
Работник оператора дата-центра		