УТВЕРЖДАЮ
Директор ООО «Файнекс»

_____А.А. Сташевский
20.06.2023

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

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по обеспечению непрерывной работы и восстановлению работоспособности информационной системы ООО «Файнекс» (далее – Положение) устанавливает общие требования к организационно-методическим и программно-техническим мерам для обеспечения непрерывной работы и восстановлению работоспособности информационной системы ООО «Файнекс» (далее – Организация).

1.2. Настоящее Положение разработано 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 и Политикой информационной безопасности (кибербезопасности) ООО «Файнекс».

1.3. Для целей настоящего Положения нижеприведенные термины используются в следующих значениях:

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;

План мероприятий по обеспечению непрерывной работы и восстановлению работоспособности информационной системы Организации (далее – ПОНРВ) – документально оформленный комплекс организационных и практических мероприятий, которые должны выполняться до, во время и после возникновения кризисной (сбойной) ситуации в информационной системе Организации;

ПО – программное обеспечение;

эксплуатационная документация – документация, предназначенная для использования при эксплуатации, обслуживании и сопровождении информационной системы Организации.

1.4. Иные термины, используемые в настоящем Положении, и не указанные в подпункте 1.3, имеют значения, определенные нормативными

правовыми (техническими нормативными правовыми) актами Республики Беларусь, актами Наблюдательного совета Парка высоких технологий, Политикой информационной безопасности (кибербезопасности) ООО «Файнекс», иными локальными правовыми актами Организации (далее – ЛПА).

1.5. Обеспечение непрерывной работы и работоспособности информационной системы Организации содержит меры:

реализуемые Организацией – при организации технологических процессов в информационной системе Организации на вычислительных мощностях Организации;

реализуемые организацией-контрагентом – при организации технологических процессов в информационной системе Организации на вычислительных мощностях сторонней организации-контрагента.

1.6. При организации технологических процессов в информационной системе Организации на вычислительных мощностях сторонних организаций-контрагентов, Организация, помимо прочего, обеспечивает включение в договоры с организацией-контрагентом:

меры по обеспечению отказоустойчивости и информационной безопасности предоставляемых организацией-контрагентом сервисов;

показатели уровня доступности услуг;

порядок и условия предоставления технической поддержки в отношении предоставляемых услуг;

процедуры, связанные с устранением сбойных ситуаций, проведением плановых и неотложных работ;

правила и сроки оповещения должностных лиц Организации о возникших кризисных (сбойных) ситуациях;

иные согласованные с организацией-контрагентом меры для обеспечения целостности, конфиденциальности и доступности сервисов и информационных активов информационной системы Организации.

ГЛАВА 2
ОБЩИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ НЕПРЕРЫВНОЙ РАБОТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ

2.1. Непрерывность работы и минимизация времени восстановления работоспособности информационной системы Организации обеспечивается:

разработкой и применением организационно-методических документов;

разработкой и выполнением требований Организации в области обеспечения информационной безопасности;

качественной разработкой и сопровождением ПО информационной системы Организации;

созданием условий по обеспечению надежности функционирования информационной системы Организации;

управлением безопасностью и надежностью доступа к используемым информационным ресурсам;

эффективным управлением информационными ресурсами;

качеством управления системами жизнеобеспечения;

созданием условий для успешной работы персонала.

2.2. Организация обеспечивает достаточное количество персонала с соответствующим уровнем квалификации, а также выделяет достаточное количество финансовых и материальных ресурсов для обеспечения надежного, безопасного функционирования информационной системы Организации.

2.3. В целях обеспечения надежного функционирования информационной системы Организации, а также минимизации на ее работу негативного воздействия кризисной (сбойной) ситуации, Организация разрабатывает ПОНРВ.

2.4. Разработка и сопровождение ПОНРВ осуществляется должностным лицом, ответственным за системное администрирование и информационную безопасность Организации.

2.5. ПОНРВ утверждается директором Организации.

2.6. При разработке ПОНРВ кризисные (сбойные) ситуации должны быть категорированы. Присвоение категорий кризисной (сбойной) ситуации осуществляется по одному или нескольким признакам:

масштаб кризисной (сбойной) ситуации;

размер наносимого ущерба при реализации выхода из кризисной (сбойной) ситуации;

причины возникновения кризисной (сбойной) ситуации;

время реакции и восстановления работоспособности;

уровень оповещения руководства и (или) принятия им решений.

2.7. Основными причинами возникновения кризисной (сбойной) ситуации в функционировании Организации являются:

стихийные бедствия (землетрясение, наводнение, ураган и т.д.);

чрезвычайные ситуации (пожар, затопление, отравления ядовитыми веществами и т.д., включая террористический акт или его угрозу, возникновение, распространение и объявление в Республике Беларусь эпидемии смертельно опасного заболевания);

технологические ошибки;

отказ систем жизнеобеспечения;

отказ программно-технических средств;

ошибки персонала, вызванные неправильными действиями случайного или умышленного характера;

атаки со стороны хакеров вредоносными программными кодами;

нарушение требований к информационной безопасности.

2.8. Для обеспечения непрерывного функционирования и восстановления работоспособности информационной системы Организации реализуется:

разработка и поддержание в актуальном состоянии описания технологических процессов, используемых в информационной системе Организации;

наличие учтенных рабочих и резервных копий ПО;

использование сертифицированного и лицензионного ПО;

установление порядка разработки, сопровождения (внесения изменений), хранения и эксплуатации ПО;

управление функционированием и восстановлением информационной системы Организации;

резервирование критически значимых ресурсов информационной системы Организации;

контроль работоспособности резервных компонентов информационной системы Организации;

техническое обслуживание информационной системы Организации;

организация дежурства специалистов по техническому сопровождению (при необходимости).

2.9. При работе с персоналом в Организации реализуются меры по:

подбору и подготовке персонала необходимой квалификации;

учету мотивации персонала к положительным результатам работы;

управлению переподготовкой и повышением квалификации персонала;

созданию резерва и организации замещения персонала;

обеспечению снижения текучести кадров.

ГЛАВА 3
ОБЩИЕ ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ БЕЗОТКАЗНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ

3.1. Безотказность работы информационной системы Организации достигается за счет проведения мероприятий, направленных на предупреждение нарушения их работоспособности и минимизацию времени их восстановления при возникновении кризисных (сбойных) ситуаций.

3.2. Защита от сбоев в работе электрической сети, воздействия окружающей среды обеспечиваются посредством размещения критически важных компонент информационной системы Организации в сертифицированном дата-центре,

3.3. Повышение уровня безотказной работы информационной системы Организации обеспечивается посредством осуществления ее периодического технического обслуживания и тестирования, которые проводятся не реже одного раза в год.

3.4. Проведение периодического технического обслуживания и тестирования информационной системы Организации фиксируется в специальном журнале (содержащем информацию о перечне работ, дате проведения технического обслуживания, подпись и расшифровку подписи ответственного лица), в котором отражаются все обнаруженные дефекты.

3.5. На основании результатов тестирования информационной системы Организации проводится анализ причин возникновения обнаруженных дефектов и принимаются меры по их устранению.

3.6. На информационную систему Организации разрабатывается паспорт, включающий следующую информацию:

наименование;

дата ввода в эксплуатацию;

ФИО лиц, ответственных за эксплуатацию;

ФИО лиц, ответственных за техническую поддержку;

состав средств телекоммуникаций и их размещение;

состав ПО;

перечень технической и эксплуатационной документации на информационную систему Организации;

перечень резервного оборудования с указанием места его размещения.

Форма типового паспорта на информационную систему Организации приведена в Приложении 1 к настоящему Положению.

3.7. Поступление ПО и включение его в состав информационной системы Организации (ввод в эксплуатацию) фиксируются в специальном журнале.

3.8. В комплект разрабатываемого (поставляемого) ПО включается эксплуатационная документация на данное ПО.

3.9. Безотказность работы средств телекоммуникаций и каналов связи достигается за счет проведения мероприятий, направленных на предупреждение нарушения их работоспособности и минимизацию времени ее восстановления при возникновении кризисных (сбойных) ситуаций.

3.10. В состав средств телекоммуникаций входят оборудование, коммуникационное ПО, кабельные сети и каналы связи, обеспечивающие обмен информацией и данными в информационной системе Организации.

3.11. Для обеспечения требуемого уровня доступности информационной системы Организация использует каналы связи, арендуемые у поставщиков услуг связи – провайдеров.

ГЛАВА 4
ОБЩИЕ ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ СОХРАННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

4.1. Меры по обеспечению информационной безопасности информационных активов регламентированы в ЛПА Организации по вопросам информационной безопасности.

4.2. Дополнительно при организации работы с информационными ресурсами обеспечивается выполнение требований по:

разделению информационных ресурсов по среде использования (среда разработки, среда тестирования и производственная среда);

распределению зон ответственности при эксплуатации, сопровождении и обслуживании информационных ресурсов;

управлению процедурами создания эталонных и рабочих копий информационных ресурсов, а также их резерва.

4.3. В состав информационных ресурсов, подлежащих хранению, включаются:

документированная информация, связанная с организацией работы информационной системы Организации;

копии баз данных;

события системного и прикладного ПО.

4.4. Информационные ресурсы, подлежащие хранению, размещаются в специальном архиве, для организации которого может привлекаться внешний поставщик услуг хранения информации.

Приложение 1

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

(примерная форма)

ПАСПОРТ
на информационную систему «_____»

Дата ввода в эксплуатацию:	
Фамилия, имя, отчество лиц, ответственных за эксплуатацию:	
Фамилия, имя, отчество лиц, ответственных за техническую поддержку:	
Состав средств телекоммуникаций и их размещение:	
Состав ПО:	
Перечень технической и эксплуатационной документации:	
Перечень резервного оборудования и его размещение:	