MOEX GROUP

MOEX.COM

НЕПРЕРЫВНОСТЬ БИЗНЕСА И ОПЕРАЦИОННАЯ НАДЕЖНОСТЬ

MOEX GROUP

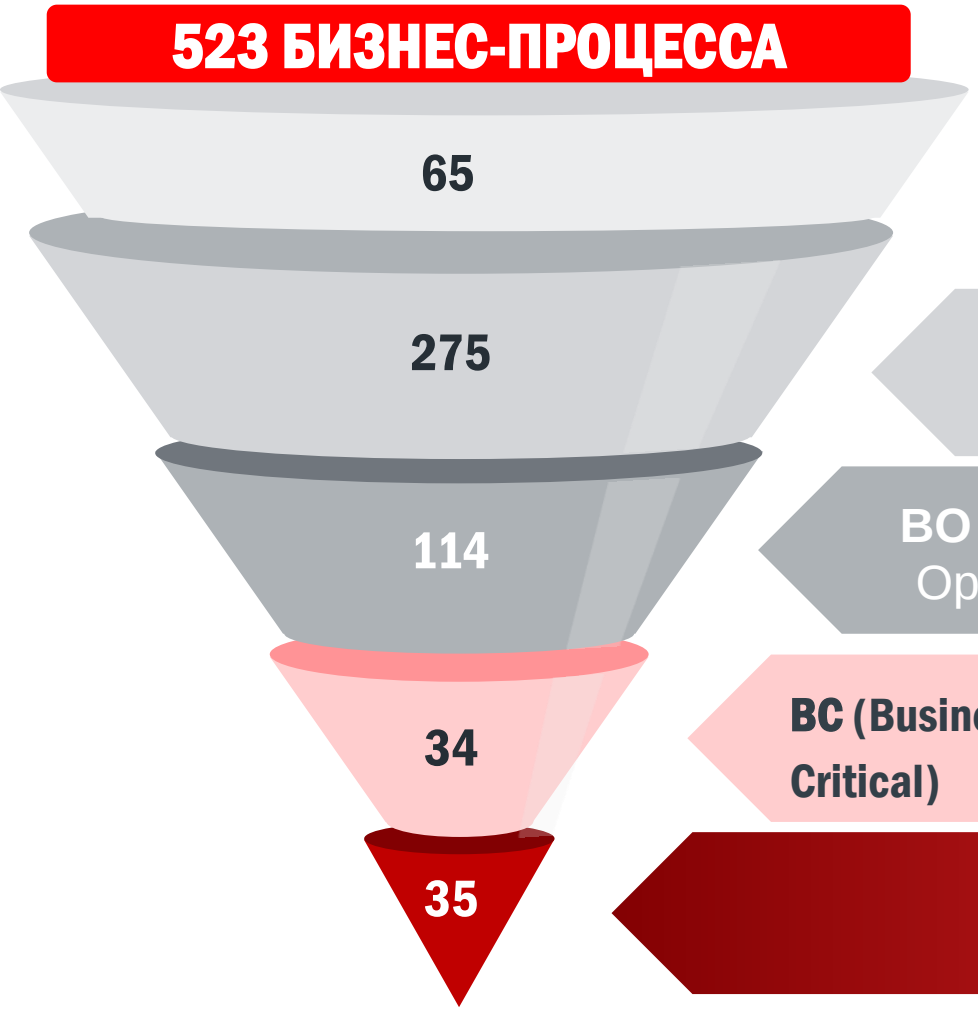
НЕПРЕРЫВНОСТЬ БИЗНЕСА

Общее определение

Обеспечение непрерывности бизнеса (далее ОНБ)- стратегическая и тактическая способность организации по планированию своих действий и реагированию на случай возникновения чрезвычайных ситуаций, влекущих за собой нарушение нормального хода деятельности, с целью продолжения выполнения операций/ взятых на себя обязательств на определенном приемлемом уровне.

БИЗНЕС-ПРОЦЕССЫ, УЧАСТВУЮЩИЕ В BIA
(business impact analysis)

MOEX GROUP



	ИСПОЛНИТЕЛИ	ВЛИЯНИЕ	
NR (DO NOT RECOVERY)	Поддерживающие подразделения Биржи	нет влияния	НЕ КРИТИЧНЫЕ ПРОЦЕССЫ
BS (Business Supporting)	Все структурные подразделения Биржи	Регуляторное, правовое, репутационное, операционное	
BO (Business Operational)	Все структурные подразделения Биржи	Регуляторное, правовое, репутационное, операционное	
BC (Business Critical)	ОД, ДКП, ДЛ, Блок ИТ, ДОРИБиНБ, ОФП	регуляторное + правовое + репутационное	КРИТИЧНЫЕ ПРОЦЕССЫ

ОСНОВОПОЛАГАЮЩИЕ ПОДХОДЫ
К ОБЕСПЕЧЕНИЮ НЕПРЕРЫВНОСТИ БИЗНЕСА

ПОЛИТИКА ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ БИЗНЕСА

ТРЕБОВАНИЯ РЕГУЛИРУЮЩИХ ОРГАНОВ И СТАНДАРТОВ

ОЖИДАНИЯ ЗАИНТЕРЕСОВАННЫХ СТОРОН

СТРАТЕГИЯ ОНБ

РЕЗУЛЬТАТЫ АНАЛИЗА ВОЗДЕЙСТВИЯ НА БИЗНЕС

РЕЗУЛЬТАТЫ ОЦЕНКИ РИСКОВ И УГРОЗ НЕПРЕРЫВНОСТИ БИЗНЕСА

Анализ воздействия на бизнес (BIA) определяет и устанавливает:

- **Ключевую деятельность, зависимости и необходимые ресурсы**
- **Негативное влияние от простоя**
- **Приоритеты восстановления деятельности и необходимых ресурсов в случае сбоя/ЧС**

Анализ рисков идентифицирует и оценивает:

- **Угрозы и риски непрерывности**
- **Какие риски непрерывности требуют дополнительного управления**
- **Необходимые меры по митигации**

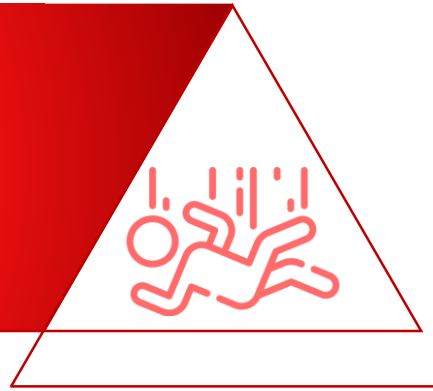
В отношении каждого типа ресурсов определяются стратегии восстановления и применяются меры по поддержанию их устойчивости к негативным воздействиям

ЦИКЛ УПРАВЛЕНИЯ
НЕШТАТНЫМИ СИТУАЦИЯМИ

MOEX GROUP

Источники информации о РЕАЛИЗОВАВШЕЙСЯ НС

- Инициативное информирование работниками
- Системы мониторинга
- Сообщения от участников торгов и контрагентов



РАБОТА В НС ОПИСАНА В ГРУППОВОМ ДОКУМЕНТЕ «РЕГЛАМЕНТ ДЕЙСТВИЙ ПОДРАЗДЕЛЕНИЙ ГРУППЫ МОСКОВСКАЯ БИРЖА В НЕШТАТНЫХ СИТУАЦИЯХ»

ПОРЯДОК РЕАГИРОВАНИЯ
НА НЕШТАТНУЮ СИТУАЦИЮ

MOEX GROUP

ДОД на основании доверенности **имеет полномочия принимать решения по приостановке торгов и урегулированию НС без созыва МКЦ и БКЦ**

(Применимо в случаях, когда ДОД имеет возможность корректно диагностировать ситуацию или не может организовать работу БКЦ в оперативное время)

Любой сотрудник, выявивший НС обязан сообщить об этом ДОДу (любому члену малого кризисного центра - МКЦ) **НЕЗАМЕДЛИТЕЛЬНО**

ДОД

Сбор МКЦ

Сбор БКЦ, если по итогам предыдущего шага МКЦ не может урегулировать НС

Оценка возможности решения НС в рамках текущих ресурсов/ полномочий

5 минут с момента диагностики **на принятие решения**

Приостановка торгов требуется?

Требуется

5 минут на приостановку торгов
15 минут на раскрытие на сайте ПАО МБ и информирование БР

Не требуется

15 минут на раскрытие на сайте МБ
1 т. д. информирование БР о характере, причинах НС, мерах

Выработка коллегиального решения

Принятие решения о раскрытии на сайте ПАО МБ, Группа «MOEX Incidents»

Сбор IT Incident Management (техническая конференция)

ИТ обеспечивает регулярный обмен информацией

УРЕГУЛИРОВАНИЕ НС

ПРОВЕРКА КРИТЕРИЕВ НС:
- Влияние на ГК и клиентов - множественные обращения >10;
- Влияние на продукт – частичная/полная недоступность
- Влияние на торги и клиринг – частичная/полная недоступность
- Нарушение регуляции
- Существенные убытки

Если НС требует приостановки торгов, но отсутствует возможность оперативно собрать БКЦ (либо при отсутствии кворума БКЦ), ДОД уполномочен принимать решения по урегулированию НС

ИНФОРМИРОВАНИЕ:
- Информация уровня **HIGH** – СОИ, сайт, торговая система
- Информация уровня **MEDIUM/INFO** – СОИ

Кого информируем: клиентов, контрагентов, регулятора, работников

ОПЕРАЦИОННАЯ НАДЕЖНОСТЬ

Общее определение

Способность организации обеспечить непрерывность функционирования критически важных процессов с учетом соблюдения целевых показателей операционной надежности.

ПОКАЗАТЕЛИ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

MOEX GROUP

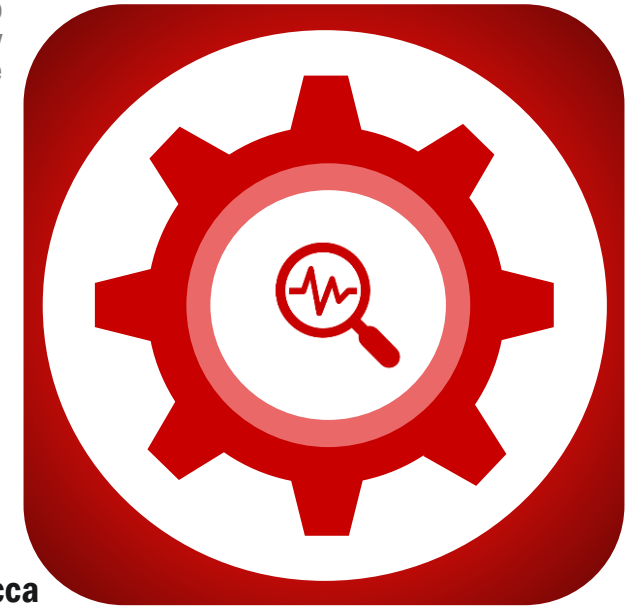
ДОПУСТИМАЯ ДОЛЯ ДЕГРАДАЦИИ технологических процессов

отношение общего количества финансовых сделок, заключенных во время деградации технологических процессов к ожидаемому количеству финансовых сделок за тот же период в случае бесперебойного функционирования.

ДОПУСТИМОЕ ВРЕМЯ ПРОСТОЯ И (ИЛИ) ДЕГРАДАЦИИ технологических процессов

2 часа

отношение фактической продолжительности времени штатного функционирования к нормативной



СОБЛЮДЕНИЕ РЕЖИМА РАБОТЫ (функционирования) технологического процесса

отношение суммарного времени деградации сервисов к общему времени функционирования за вычетом суммарного времени технологических окон

ДОПУСТИМОЕ СУММАРНОЕ ВРЕМЯ ПРОСТОЯ И (ИЛИ) ДЕГРАДАЦИИ технологических процессов

суммарное время простоя и (или) деградации технологических процессов за отчетный календарный месяц

НАПРАВЛЕНИЯ РАЗВИТИЯ
ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

MOEX GROUP

Кибер безопасность

- организационные и технические меры, направленные на разработку сценарного анализа и проведение с использованием сценарного анализа тестирования готовности НФО противостоять реализации информационных угроз в отношении критичной архитектуры
- обеспечение осведомленности об актуальных информационных угрозах.

Контроль критичной архитектуры

- предотвращение возникновения уязвимостей в критичной архитектуре
- планирование и внедрение изменений в критичной архитектуре, направленных на обеспечение бесперебойного функционирования программно-аппаратных средств;
- управление конфигурациями программно-аппаратных средств;
- управление уязвимостями и обновлениями программно-аппаратных средств.

Инцидент менеджмент

- выявление и регистрация инцидентов ОН,
- восстановление функционирования технологических процессов и программно-аппаратных средств после реализации инцидентов операционной надежности;
- анализ причин и последствий реализации инцидентов ОН;
- организацию взаимодействия между подразделениями НФО, а также между НФО и Банком России, иными участниками.

Вендор менеджмент

- управление риском реализации информационных угроз при привлечении поставщиков услуг, в том числе защиту программно-аппаратных средств от возможной реализации информационных угроз, включая компьютерные атаки, со стороны поставщиков услуг;
- управление риском технологической зависимости функционирования программно-аппаратных средств НФО от поставщиков услуг.

Риски и непрерывность

- Анализ рисков и угроз непрерывности бизнеса
- Выделение потенциально возможных сценариев ЧС, меры по снижению вероятности ЧС
- Меры по восстановлению критичных процессов при ЧС
- Поддержание резервных площадок и мощностей;
- Регулярные тестирования.

АКТУАЛЬНАЯ ПРОБЛЕМАТИКА

МОДЕЛИРОВАНИЕ УГРОЗ – Отсутствие системности и четкой позиции регулятора по части моделирования. Какие сценарии должны тестировать организации. Отсутствие готовых базовых сценариев для проработки, отсутствие методологии в части моделирования угроз.

КОНЦЕНТРАЦИЯ И РИСКИ АУТСОРСИНГА – вся экономика страны сконцентрирована в том числе и территориально. В случае реализации угроз в отношении критической инфраструктуры возрастают общие риски прерывания бизнеса.
В отношении аутсорсинга регуляция подсвечивает риски аутсорсинга, но не рассказывает о механизмах управления ими

ДУБЛИРОВАНИЕ МЕХАНИЗМОВ РЕГУЛИРОВАНИЯ - дублирование механизма управления оперрисками, а не комплементарное его дополнение. Наличие конфликтующих пунктах в нормативных документах действующих и новых.
Так, в части возобновления торгов в случае технического сбоя: Организатор торгов следуя клиентоориентированному подходу в соответствии с 437-П ожидает, что для возобновления торгов необходимо подтверждения большинства участников даже при наличии технической возможности запуска торгов ранее. В случае изменений в 779-П Организатор торгов будет заинтересован возобновить торги при доступности системы, а не участников, что негативно скажется на проведении торгов по различным инструментам.

ИМПОРТОЗАМЕЩЕНИЕ и СУВЕРЕНИТИЗАЦИЯ – отсутствуют понятные подходы в части оценки рисков по импортозамещению и влияния импортозамещения на операционную надежность. Новые технологии могут снижать риск зависимости от иностранных вендоров и одновременно с этим повышать риска нарушения ОН в виду незрелости решений.
Кроме того, переход на российские альтернативы увеличивает и риски концентрации – малое количество зрелых решений вынуждает всю отрасль использовать одни и те же технологии. В случае выявления и эксплуатации критичной уязвимости под ударом откажутся все.