# Определение приоритетов аварийного восстановления

написано Александр Астахов | 10 июня, 2023

> *— Внимание, Земля! Говорит станция «Мир»! У нас отказал бортовой компьютер. Что делать?*
> *— Станция «Мир»! Станция «Мир»! Это диспетчер! Слышите меня? Играйте пока на резервном! Играйте на резервном!*
>
> *Анекдот*

В этом разделе устанавливается связь оценки рисков нарушения доступности приложений и информационных активов с процессом планирования непрерывности бизнеса.

Одной из основных задач информационной безопасности является обеспечение непрерывности бизнеса в той части, которая касается доступности для бизнеса его информационных активов. Поэтому процессы управления непрерывностью бизнеса и процессы управления информационной безопасностью и информационными рисками тесно взаимосвязаны и частично пересекаются. Вопросы управления инцидентами и рисками информационной безопасности, которые приводят к прерыванию критичных для организации бизнес-процессов, относятся к управлению непрерывностью бизнеса. Этот класс инцидентов обычно называют аварийными ситуациями. Многие подобные ситуации вынуждают организацию переходить на резервные площадки и в резервные центры обработки информации и там восстанавливать свои информационные системы.

Согласно определению британского стандарта BS 25999-1, *управление непрерывностью бизнеса (УНБ)* — это процесс, связанный с бизнесом и развивающийся в зависимости от него, в ходе которого в соответствии с поставленными целями формируется система, направленная на следующее:

- активное совершенствование способности организации к восстановлению при нарушении возможностей достижения ее основных целей;
- обеспечение отработанного метода восстановления способности организации производить основные продукты и услуги на заданном уровне в течение согласованного срока после нарушения нормального хода деятельности;
- обеспечение управления во время нарушения нормального хода бизнеса и защиты репутации и бренда организации.

УНБ дополняет систему управления рисками, направленную на основные продукты и услуги организации. Нормальный ход производства продуктов и предоставления услуг может быть нарушен в результате самых разнообразных инцидентов, многие из которых сложно предсказать и проанализировать.

Благодаря сосредоточению внимания на последствиях нарушения нормального хода деятельности, УНБ позволяет определить те продукты и услуги, от которых зависит выживание организации, а также предусмотреть меры, необходимые для непрерывного выполнения ее обязательств. В ходе УНБ организация получает представление о том, что нужно сделать до наступления инцидента, чтобы защитить людей, помещения, технологию, информацию, цепочку поставок, заинтересованные стороны и репутацию.

Имея подобное понимание, организация может реалистично оценить ответные меры, которые необходимо принять при нарушении нормального хода деятельности, чтобы справиться с любыми последствиями без недопустимого нарушения сроков производства продуктов или предоставления услуг.

Конкурентным преимуществом организации, принимающей надлежащие меры в области УНБ, является ее способность воспользоваться высокорискованными и одновременно наиболее перспективными и высокодоходными возможностями ведения бизнеса, которые не доступны другим организациям из-за высокого риска.

На этапе планирования УНБ организации следует определить и документально зафиксировать воздействие, которое способно оказать нарушение нормального хода различных видов деятельности, обеспечивающих производство основных продуктов и услуг. Данный процесс часто называют анализом воздействия на бизнес (business impact analysis). Анализ воздействия на бизнес – это процесс анализа функций, выполняемых бизнесом, и воздействия, которое может на них оказать нарушение нормального хода бизнеса.

Для каждого вида деятельности, обеспечивающего производство основных продуктов и услуг, в рамках программы УНБ организация должна:

- Оценить во времени воздействие, которое может оказать нарушение нормального хода деятельности.
- Установить максимально допустимую продолжительность нарушения нормального хода деятельности для каждого вида деятельности, определив:

- максимальный срок с начала нарушения нормального хода деятельности, в течение которого такую деятельность необходимо возобновить;
- минимальный уровень, на котором необходимо осуществлять такую деятельность после ее возобновления;
- продолжительность срока, в течение которого необходимо возобновить деятельность на нормальном уровне.

При нарушении нормального хода деятельности воздействие, как правило, возрастает со временем и по-разному влияет на различные виды деятельности. Кроме того, воздействие может быть различным в зависимости от дня, месяца или этапа жизненного цикла бизнеса.

- Определить любые взаимозависимые виды деятельности,

активы, элементы поддерживающей инфраструктуры или ресурсы, которые также необходимо непрерывно поддерживать на определенном уровне или восстановить через какое-то время.

При оценке воздействия организации следует учитывать его составляющие, относящиеся к целям и задачам бизнеса и заинтересованным сторонам. Сюда могут относиться:

- воздействие на персонал или общественное благополучие;
- последствия причинения ущерба помещениям, технологии или информации либо утраты таковых;

- последствия нарушения законодательных или нормативных требований;
- ухудшение репутации;
- ухудшение финансовой жизнеспособности;
- снижение качества продуктов или услуг;
- причинение ущерба окружающей среде.

Организации следует документально зафиксировать свой подход к оценке воздействия нарушения нормального хода деятельности, а также результаты своего анализа и выводы.

Приоритеты аварийного восстановления – результат анализа влияния на бизнес чрезвычайных ситуаций, производимого в ходе оценки рисков.

Ущерб, связанный с нарушением доступности активов, зависит от времени их восстановления. Для того чтобы этот ущерб минимизировать, важно правильно спланировать восстановление данных и систем. Такое планирование осуществляется в рамках процесса управления непрерывностью бизнеса. Основой такого планирования является анализ влияния чрезвычайных ситуаций на бизнес, который производится в ходе оценки рисков недоступности активов.

В течение основного периода после аварийного восстановления придется смириться с определенным сокращением работоспособности. Для целей планирования необходимо определить два ключевых положения:

- для каких приложений жизненно необходимо функционирование после аварии;
- какие из наиболее важных приложений потребуют неотложного внимания сразу после начала действий по ликвидации последствий аварии.

Таблица приоритетов аварийного восстановления обеспечивает связь между процессом оценки рисков информационной безопасности и процессом планирования непрерывности бизнеса. Параметр «Время восстановления» приложения определяется на основе оценки рисков нарушения доступности приложений и связанных с ними информационных активов. Остальные параметры, такие как «Потребность в особых ресурсах» или «Устойчивость к потерям», характеризуют возможности и сложность восстановления конкретного приложения. Приоритет аварийного восстановления определяется в результате комбинирования требований по доступности приложений и возможностей их восстановления.

| Название информационного актива | Название прикладной системы | Время восстановления | Потребность в особых ресурсах | Устойчивость к потерям | Рабочие неисправности | Уровень защищенности | Приоритет восстановления |
|---|---|---|---|---|---|---|---|
| **Информационные ресурсы центра обработки данных:**<br>Корпоративный веб сайт<br>Веб сайт проекта<br>Персональные данные клиентов<br>Транзакционные данные<br>База данных логистики<br>Аналитические данные и отчеты | **Приложения центра обработки данных:** | | | | | | |
| **Информационные ресурсы офисной сети:**<br>Сообщения электронной почты<br>Протоколы совещаний и внутренняя документация<br>Проектная документация<br>Клиентские и партнерские договоры<br>Бухгалтерская база данных<br>Первичные бухгалтерские документы<br>Финансовая и налоговая отчетность<br>Платежная информация<br>Маркетинговые отчеты<br>Маркетинговые материалы<br>Персональные данные сотрудников<br>Зарплатные данные<br>Трудовые книжки | **Приложения офисной сети:** | | | | | | |

Для оценки критичности прикладных систем используются семь

показателей, позволяющих установить степень уязвимости приложения к падению производительности ИТ инфраструктуры после аварии, а также ограничения, которые могут возникнуть при восстановлении приложения:

1. Допустимое время, которое может пройти перед тем, как приложение заработает после аварии.
2. Особые ресурсы, которые необходимы в случае, если приложение будет восстанавливаться.
3. Способность приложения переносить смену компьютера в процессе восстановления.
4. Опыт сотрудников в тестировании процесса восстановления.
5. Предельные значения потерь, на которые можно пойти, если восстановление приложения задерживается или невозможно.
6. Структурные или функциональные ошибки, которые могут присутствовать в приложении.
7. Требования к структуре или функционированию.

Все эти факторы вместе определяют относительную важность после аварийного восстановления данного приложения. Оценки отдельных факторов располагаются в следующем порядке:

- *Время восстановления:*

5 – требуется достичь среднего уровня производительности за время от 4 до 6 часов после аварии;

4 – требуется достичь среднего уровня производительности за время от 7 до 12 часов после аварии;

3 – требуется достичь среднего уровня производительности за время от 13 до 24 часов после аварии;

2 – требуется достичь среднего уровня производительности за время от 25 до 48 часов после аварии;

0 – никаких ограничений по времени восстановления.

- *Потребность в особых ресурсах:*

5 – восстановление в достаточном объеме возможно только при восстановлении специальной базы данных и/или программной/аппаратной части заказчика и/или средств связи по некоммутируемым линиям;

4 – возможно функционирование в достаточной мере при использовании связи по коммутируемым линиям, если есть все необходимые ресурсы;

3 – достаточная степень производительности может быть обеспечена при частичном восстановлении ключевых ресурсов (например, при использовании текущей/резервной версии базы данных);

2 – для восстановления не нужно никаких уникальных ресурсов;

0 – может функционировать в течение периода после аварийного восстановления даже при отсутствии отдельных блоков и подсистем.

- *Переносимость:*

5 – приложение не может быть восстановлено нигде, кроме основного рабочего компьютера;

3 – приложение может быть успешно перемещено, но с задержкой, превосходящей фактор времени данного приложения;

0 – при перемещении приложения не предвидится никаких трудностей.

- *Необходимая квалификация:*

5 – сотрудники не смогли успешно протестировать процесс восстановления приложения;

3 – тестирование восстановления приложения было успешным, но достигнуто это было с большой задержкой;

0 – тестирование восстановления прошло успешно. Не было встречено никаких проблем.

- *Устойчивость к потерям:*

5 – задержка с восстановлением, скорее всего, приведет к финансовым потерям, превышающим пределы, установленные руководством;

4 – задержка с восстановлением вызовет проблемы с главными заказчиками/поставщиками, которые превысят эксплуатационные или установленные руководством пределы;

2 – приложение должно быть успешно восстановлено, но проблемы потерь, связанные с неполным или задержанным восстановлением, не выходят за установленные пределы;

0 – при задержанном или неполном восстановлении никаких проблем или потерь не предвидится.

- *Рабочие неисправности:*

5 – успешное восстановление и «нормальная» эксплуатация требуют непосредственного участия основного программиста и оператора;

4 – приложение нуждается документировании;

3 – Приложение имеет значительную чувствительность к изменениям в объемах входных данных, их качеству и/или имеет склонность к отказам;

0 – никаких известных дефектов.

- *Необходимый уровень защищенности:*

5 – приложение содержит важные для компании сведения;

4 – приложение содержит систему управления финансовыми активами;

0 – не нужны никакие дополнительные меры безопасности сверх организации обслуживания на время процесса восстановления.