Непрерывность бизнеса как основа функционирования промышленных компаний

В последнее время под термином "непрерывность бизнеса" все чаще подразумевают "непрерывность ИТ-услуг". На самом же деле, понятие непрерывности бизнеса охватывает куда большую часть предприятия, чем отделы информационных технологий. Чего будет стоить даже самая устойчивая система, если из-за эпидемии гриппа будет объявлен карантин или сотрудники не смогут войти в здание из-за уличных беспорядков? В чем будет ценность бесперебойной системы контроля отгрузки сырья, если произойдет физическое повреждение железнодорожного полотна и отгрузка будет просто невозможна? Очень часто предприятия сосредотачиваются лишь на повышении катастрофоустойчивости ИТ-систем, забывая о том, что это лишь часть инфраструктуры предприятия, хотя и значительная.

Данная статья ставит свое целью познакомить читателей с основами организации непрерывности бизнеса – с терминологией и последовательностью шагов по созданию соответствующей системы на современном промышленном предприятии.

Терминология

Для промышленных компаний основой жизнедеятельности является обеспечение непрерывности функционирования цепочки процессов подготовки и предоставления основного продукта, будь то нефть, газ, древесина или химические продукты. Прервать эту цепочку с вытекающими последствиями для бизнеса предприятия могут как реализованные внешние угрозы, так и внутренние инциденты в компании. Так, к примеру, в одной из крупных организаций долго готовились к обновлению ключевой системы. Подготовка длилась более месяца, сотрудники были предупреждены об обновлении системы и заранее обучены. Однако в тот день, когда система была введена в эксплуатацию, пользователи не смогли работать с ней по той простой причине, что подготовка нового релиза велась и тестировалась под правами администратора, которых нет у рядовых сотрудников. Из-за того, что организация не имела планов экстренного возобновления работы, основная деятельность предприятия была приостановлена на полдня, что привело к непредвиденным и крупным убыткам.

План непрерывности бизнеса описывает работы нескольких ключевых отделов, поддерживающих наиболее необходимые продукты или услуги компании силами минимального числа ключевых сотрудников.

Очевидно, что должны существовать разные планы работы в разных ситуациях. Например, на случай затопления нужно иметь план размещения сотрудников в другой части здания, при наступлении общего карантина требуется активировать планы удаленной работы сотрудников из дома. При выходе из строя собственных транспортных средств предприятия надо задействовать варианты срочного взаимодействия с внешними логистическими компаниями. При повреждении ИТ-систем в ряде случаев есть смысл начать предоставлять услуги из резервного центра, в других же ситуациях разумней постепенно восстановить ИТ-инфраструктуру в собственном здании. Все эти варианты весьма специфичны и определяются особенностями деятельности конкретного предприятия.

Сценарии активации соответствующих планов (или блоков единого плана) по обеспечению непрерывности бизнеса, а также краткое описание стратегических опций поведения в случае наступления чрезвычайной ситуации образуют основу стратегии непрерывности бизнеса.

При разработке стратегии должны быть также определены планы экстренного реагирования на инцидент (планы управления инцидентом), предусматривающие такие меры, как: эвакуация персонала, спасение имущества, вызов внешнего подкрепления для ликвидации последствий инцидента, либо самостоятельное сдерживание или ликвидацию инцидента. Под инцидентом подразумевается любое событие, влекущее прерывание деятельности предприятия и снижение уровня производства продуктов. В зависимости от масштабов инцидента он может быть классифицирован как минорный инцидент, авария или катастрофа.

Поддержание в актуальном состоянии планов по обеспечению непрерывности бизнеса и управления инцидентами – достаточно сложный процесс, который называется процессом управления непрерывностью бизнеса. Он включает в себя регулярное тестирование планов (в том числе тестирование схем взаимодействия со сторонними организациями в случае возникновения чрезвычайной ситуации), обучение новых сотрудников, строжайший контроль изменений в сопутствующей документации, непрерывное улучшение всего процесса на базе регулярного внутреннего аудита, вовлечение высшего руководства и т.д. Существующий

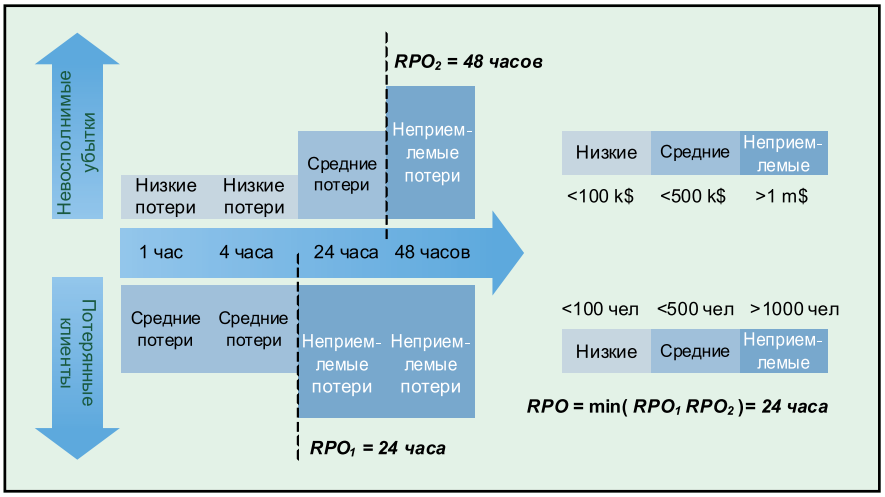

Рис. 1. Пример оценки влияния на бизнес и целевого времени восстановления

стандарт довольно подробно описывает, что должна иметь организация, чтобы быть способной незамедлительно привести планы в исполнение в случае реализации угрозы.

Теперь рассмотрим, какие шаги и в какой последовательности следует предпринять, чтобы создать план управления непрерывностью бизнеса.

Шаг первый: анализ влияния на бизнес

Прежде всего, следует определить, от каких функций можно отказаться, чтобы предприятие могло продолжать предоставлять свои ключевые продукты. Собственно, на этой стадии необходимо понять, что будет происходить с предприятием при прерывании тех или иных активностей (рис. 1): сколько предприятие потеряет в первый день, сколько во второй; как будут нарастать финансовые потери, потери клиентов; через какое время простоя ключевые партнеры поставят вопрос о прекращении сотрудничества?

Такой анализ необходимо провести для каждого функционального подразделения компании. Часто бывает так, что определенные области бизнеса потребляют услуги извне. В этом случае надо понять, во что обойдется предприятию недоступность внешних поставщиков, как будут нарастать кумулятивные потери? Анализ кумулятивных потерь –первый шаг к определению требуемого времени восстановления. Затем следует определить максимально допустимый порог потерь. Обычно он устанавливается высшим руководством компании. Определив уровни потерь и увидев, что простой той или иной части предприятия приводит через какое-то время к превышению допустимых потерь, можно легко оценить то время, в течение которого функция должна быть восстановлена во что бы то ни стало. Зная это время, далее можно оценить, какое минимальное количество сотрудников и в течение какого периода смогут обеспечивать выполнение ключевых функций каждого из подразделений предприятия. В результате такого анализа окажется, что часть функций должна быть восстановлена в первые часы, другими же можно пренебречь без существенных потерь, какие-то провайдеры окажутся критичными, а от каких-то можно будет отказаться на все время восстановительных работ.

Шаг второй: анализ рисков

После того как определено, какие функции предприятия должны быть защищены, необходимо предусмотреть возможные угрозы, от которых следует защищаться. Можно воспользоваться перечнем существующих угроз и общим голосованием определить, какие из них реалистичные, а какие нет. Можно обратиться в пресс-центр МЧС и узнать статистику происшествий в вашем регионе. Инциденты, происходящие с частотой более 5 % в год, можно классифицировать (согласно рекомендациям BCI) как наиболее вероятные по пятибалльной шкале вероятностей. Также полезно учесть специфику внутренней инфраструктуры здания, возможные места хранения взрывчатых веществ, возможность прорыва труб, утечки газа, массовых беспорядков, отравления в корпоративной столовой и т.д. После составления списка реалистичных угроз, ранжированных по степени вероятности, следует оценить возможные последствия реализации этих угроз: степень ущерба, который может быть причинен персоналу, имуществу или иным активам, партнерам по бизнесу и т.д. (таблица 1). В каких разрезах оценивать ущерб – зависит от специфики предприятия. После того, как оценена суммарная степень ущерба каждой угрозы, умножьте степень реалистичности на степень ущерба – и вы получите оценочную величину риска. Из ранжированного списка рисков выберите топ-10 или топ-5 рисков, которые предприятие готово взять на себя. Остальные можно застраховать или просто не рассматривать, иначе величина учитываемых рисков может превысить ваши финансовые возможности по управлению ими.

Таблица 1. Пример простого анализа рисков

Список угроз	Вероятность (1↔5)	Степень повреждения персонала (1↔5)	Степень повреждения здания (1↔5)	Степень повреждения провайдера-услуги (1↔5)	Величина риска
		Вес. коэфф. = 2	Вес. коэфф. = 2	Вес. коэфф. = 1	
Пожар в здании	2	5	5	1	Высокая
Беспорядки в районе	3	2	1	3	Средняя
Отравление в столовой	1	5	1	1	Низкая

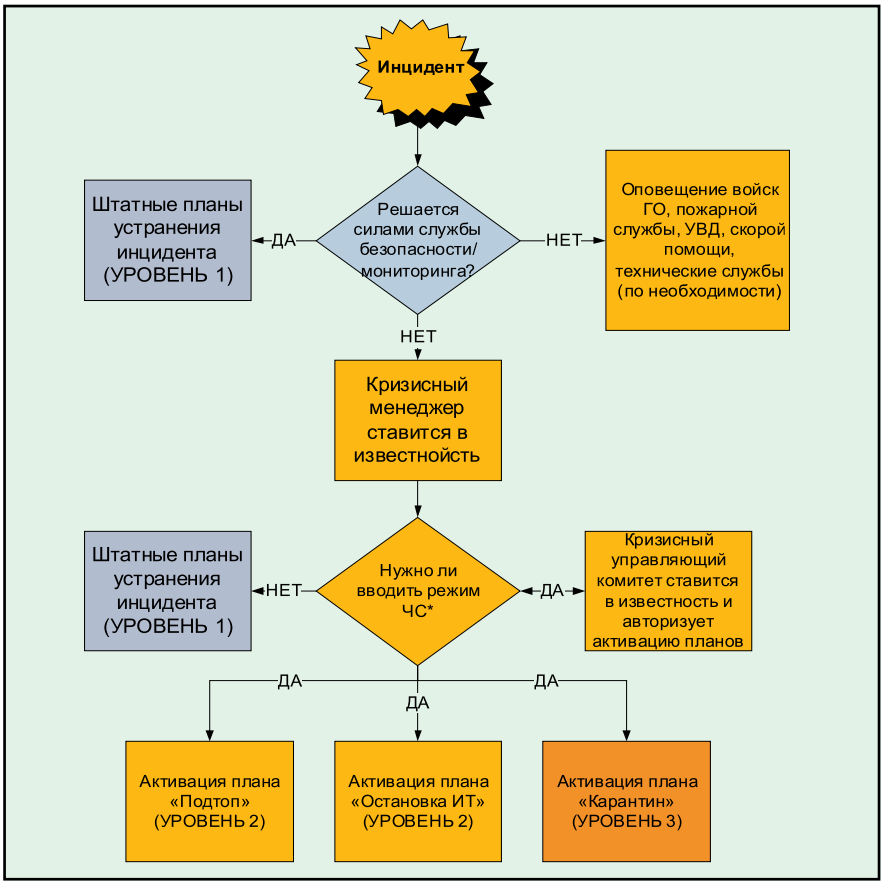

Рис. 2. Пример структуры реагирования на инцидент

Шаг третий: создание стратегии

Теперь, когда известны возможные угрозы и те отделы, которые могут подвергнуться "удару", учитывая информацию о том, в какие сроки эти отделы должны быть восстановлены, а также какое минимальное количество сотрудников должно поддерживать их функционирование на время полного восстановления бизнеса до прежнего состояния, можно приступить к определению стратегических опций поведения отделов предприятия в разных чрезвычайных ситуациях. Где вы создадите командные посты и как будете мобилизировать команду экстренного реагирования? Построите ли вы собственный резервный центр для ИТ или закупите услугу "резервный центр ИТ" у внешнего поставщика? Какие ИТ-системы будут "синхронизированы" и должны быть восстановлены в считанные минуты, какие будут восстанавливаться постепенно, с завозом оборудования со склада? Где будет храниться дополнительное оборудование на случай выхода из строя основного? Как вы будете его доставлять в случае блокировки основных маршрутов? Есть ли необходимость в распределении работников по разным зданиям предприятия? Будет ли предусмотрена возможность работы из дома для части сотрудников? Ответы на эти вопросы получают исходя из оценки возможных угроз, стоимости решения и стоимости простоев. После того, как намечены опции поведения компании в различных чрезвычайных ситуациях, определяют, как именно, в какой последовательности будут приниматься решения об активации тех или иных опций. Для наглядности можно оформить эту последовательность в виде небольшой диаграммы, которая называется структурой реагирования на инцидент (рис. 2).

Шаг четвертый: разработка планов

После того, как определена стратегия, разрабатываются подробные планы экстренного реагирования и обеспечения непрерывности бизнеса. Данный этап включает не только написание четких инструкций, подготовку маршрутных схем, но и выбор конкретных зданий, внешних поставщиков, заключение особых контрактов на случай активации планов. Это наиболее длинная и трудоемкая часть проекта.

Шаг пятый: подготовка к тестированию и тестирование

План по обеспечению непрерывности бизнеса, как и любой план хорош только тогда, когда он работоспособен. Для этого целесообразно регулярно проводить тестирование разработанных планов. Подобное тестирование проводят "на столе", без прерывания основной деятельности. В рамках операции проверяются списки экстренных телефонов, телефоны ближайших родственников сотрудников, доступ к зданиям, системы оповещения, актуальность маршрутных карт, контракты с поставщиками и т.д. Выбранные сотрудники имитируют свои действия в чрезвычайной ситуации, не покидая границ здания.

Шаг шестой: поддержание системы

После проведения первых тестов планируются периодические пересмотры рисков и анализа влияния, регулярно осуществляются внешние и внутренние аудиты, проводятся тренинги для сотрудников, в том числе с привлечением высшего руководства. Очень важно на этой стадии, чтобы все изменения, вносимые в документацию, происходили в соответствии с требованиями процесса управления изменениями.

В заключение отметим, что проекты по обеспечению непрерывности бизнеса не относятся к разряду тех, которые ориентированы на сокращение издержек, оптимизацию работы или сокращение численности персонала. Их назначение – обеспечить защиту основных бизнес-процессов предприятия от прерывания, и с этой точки зрения подобные проекты являются не просто модным течением на российском рынке, а объективной необходимостью, продиктованной реальными условиями существования современных предприятий.

Алексей Авакян, старший консультант отдела консалтинга, компания "Информзащита"