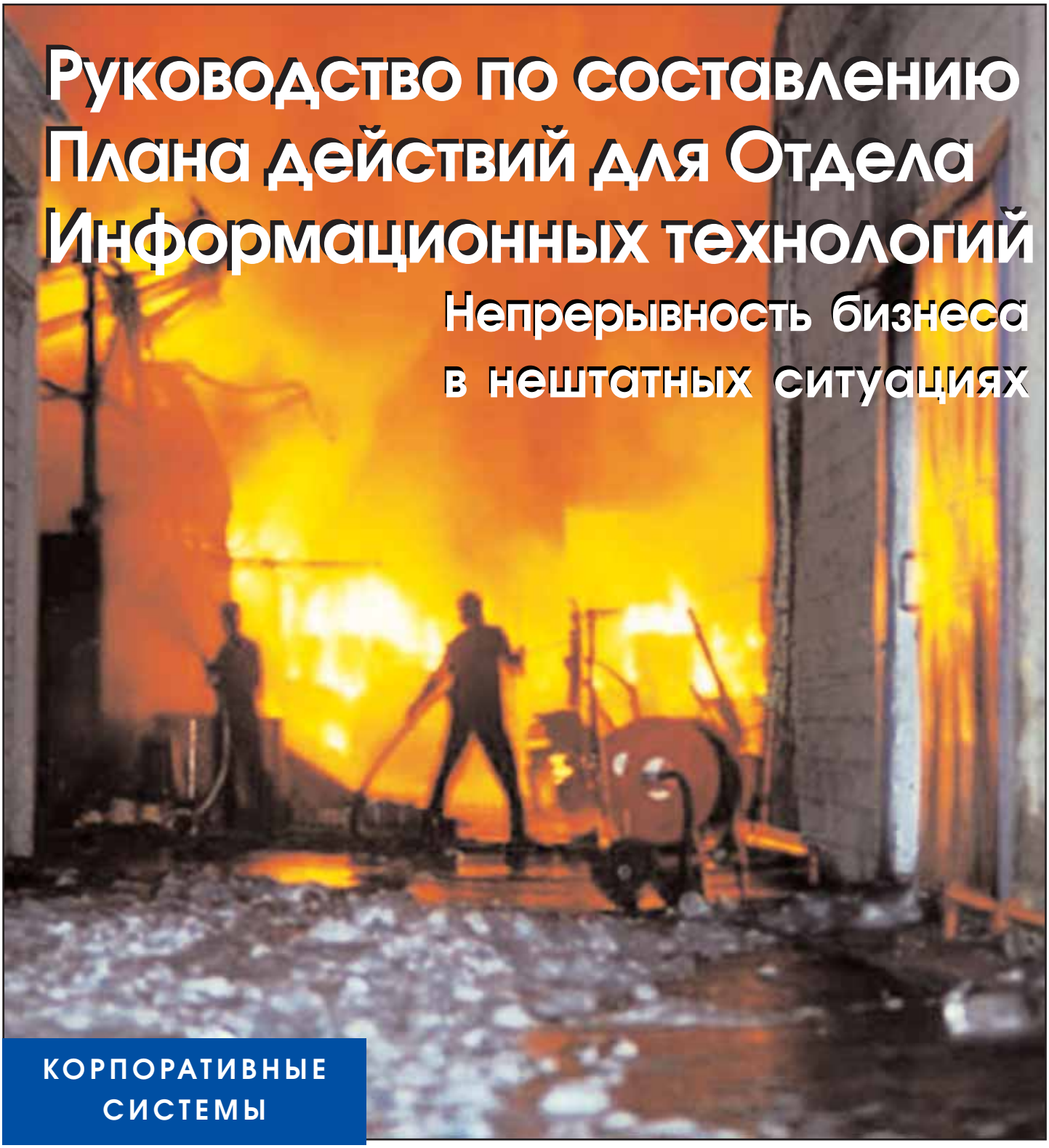
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 8 (123)/2003

Руководство по составлению Плана действий для Отдела Информационных технологий

Непрерывность бизнеса в нештатных ситуациях



КОРПОРАТИВНЫЕ СИСТЕМЫ

Руководство по составлению Плана действий для Отдела Информационных технологий

Непрерывность бизнеса в нештатных ситуациях

Б.Д. Альтерман
В.И. Дрожжинов
Г.Е. Моисеенко

Содержание

Введение

Цели чрезвычайного Плана Отдела Информационных технологий

Целями чрезвычайного Плана Отдела Информационных технологий являются:

- Обеспечение бесперебойной работы Отдела.
- Защита служащих и имущества Отдела от возможных угроз.
- Обеспечение сохранности критически важной для организации информации.

В Плане документируются согласованные решения, обеспечивающие бесперебойность работы Отдела, приводится набор процедур реагирования на бедствия и описывается способ их применения.

Под бедствием понимается возникновение любого события, которое вызывает значительное нарушение деятельности Отдела Информационных технологий.

Настоящий План рассчитан на масштабное бедствие (катастрофу), которое требует переезда в резервное помещение. При событиях менее серьезного характера осуществляются мероприятия в соответствии с определенной частью полного Плана.

В Плане изложены: подход, допущения и последовательность действий в нештатных ситуациях. В нем описываются подготовительные мероприятия, которые выполняются при штатном функционировании, и процедуры, выполняемые после наступления бедствия.

План рассылается всем указанным сотрудникам, которые должны периодически получать обновленные версии. Общий подход состоит в том, чтобы сделать план как можно более универсальным, независимым от типа бедствия.

Работы в рамках чрезвычайного плана ведутся заранее сформированными и обученными группами восстановления деятельности после бедствия (в дальнейшем «группы»). Руководителями каждой группы и их заместителями являются определенные сотрудники Отдела Информационных технологий. В плане указаны номера телефонов членов групп. Он представляет собой непрерывно обновляемый документ, который поддерживается в рабочем состоянии благодаря процессу обновлений, испытаний и экспертиз. План должен отражать актуальное состояние рабочей среды организации.

Допущения Плана Отдела Информационных технологий

Рассматриваемый План предполагает наступление катастрофического события, которое наносит существенный ущерб деятельности Отдела, вынуждая восстанавливать его работу в оборудованном резервном помещении. Хотя настоящий План разработан на основе предположения о возникновении катастрофического бедствия, связанного с полной передислокацией на резервную площадку, его можно быстро адаптировать и для менее серьезных событий.

В качестве резервных площадок рассматриваются два типа резервных помещений: «холодное» и «горячее». «Холодное» — это пустое помещение, оборудованное фальшполом, кондиционерами воздуха, электроснабжением, противопожарными средствами, т.е. помещение полностью готовое к установке вычислительного оборудования. Основные проблемы, которые возникают при ориентации на «холодное» резервное помещение, обычно связаны с приобретением и развертыванием новых аппаратных средств. Как правило, именно это занимает большую часть времени. «Горячее» резервное помещение, напротив, является полностью оборудованным и функционирующим вычислительным центром, готовым к использованию в чрезвычайных обстоятельствах. В целях проверки реализации Плана организация должна проводить тестирование работоспособности своих прикладных систем на резервном оборудовании.

В зарубежной практике организации, предоставляющие услуги по восстановлению деятельности после бедствия, предлагают широкий спектр «горячих» резервных помещений. Контрактом на предоставление услуг предусматривается проведение нескольких испытаний в течение года. Это позволяет гарантировать правильность работы всех прикладных систем в резервном помещении.

Среда обработки данных

В данном разделе приводится краткое описание вычислительного центра, включая описание прикладных систем и технической поддержки.

Указатель чрезвычайного Плана Отдела Информационных технологий

ПЛАН ДЕЙСТВИЙ ДЛЯ ОТДЕЛА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ КРУПНЫХ БЕДСТВИЯХ (КАТАСТРОФАХ)

Цикл от возникновения бедствия до полного восстановления нормальной работы имеет четыре этапа:

- Первоначальное реагирование
- Подготовка к временной работе в резервном помещении
- Полностью налаженная работа в резервном помещении
- Восстановление основного производственного помещения и возвращение в него

ОБНАРУЖЕНИЕ И РЕАГИРОВАНИЕ

Наименование шага	Исполнитель	Предпринимаемые меры
Идентификация проблемы	Персонал Службы эксплуатации	Уведомление руководства Службы эксплуатации
	Охранник	Вызов аварийных служб
Уменьшение последствий	Персонал Службы эксплуатации	Применение процедур действий в чрезвычайной ситуации
Эвакуация	Охранник	Электрическое питание, кондиционеры воздуха, ущерб от поступления воды
	Все находящиеся в здании	Эвакуация из здания
Уведомление Группы управления в чрезвычайной ситуации	Персонал Службы эксплуатации	См. приведенный ниже список
	Охранник	

Идентификация проблемы; уведомление руководства

Аварийные службы

Позвонить по следующим телефонам, чтобы информировать местные власти о чрезвычайных ситуациях типа пожара, взрыва, землетрясения, урагана и т.п.:

	Чрезвычайный вызов	Обычный номер
Пожарная служба	___	_____-_____
Отделение милиции	___	_____-_____
Скорая помощь	___	_____-_____

Среда эксплуатации

Если обнаруженная проблема касается среды эксплуатации компьютеров, например, электрического питания, проникновения воды, перегрева, переохлаждения или влажности, связаться со следующими руководителями:

	Служебный телефон	Домашний телефон
Руководитель службы эксплуатации	_____	_____-_____
Старший менеджер по эксплуатации	_____	_____-_____

Если не удается связаться ни с одним из вышеупомянутых лиц, информировать следующих руководителей:

	Служебный телефон	Домашний телефон
Руководитель Отдела Информационных технологий	_____	_____-_____

После контактов с одним из вышеупомянутых лиц решите к кому, в зависимости от возникшей проблемы, обращаться далее:

	Служебный телефон	Домашний телефон
Руководитель Отдела технического обслуживания	_____	_____-_____
Старший менеджер по техническому обслуживанию	_____	_____-_____

Снижение вероятности дополнительного ущерба

Описанные ниже оперативные меры касаются чрезвычайных ситуаций, связанных с нарушением кондиционирования воздуха, пожаром, нарушением электропитания или затоплением.

Отказ кондиционера воздуха

Температура помещения, в котором находятся компьютеры, не должна превышать 25 градусов, в противном случае принимаются следующие меры:

1. Уведомляется дежурный службы эксплуатации. Он ставит в известность специалиста Отдела технического обслуживания о необходимости вмешательства, а затем сообщает о происшествии руководителю службы эксплуатации.

2. Если температура поднимется выше 30 градусов, необходимо уведомить подрядчика на сервисное обслуживание технических средств. Руководитель службы эксплуатации должен решить, выполнение каких не критичных для бизнеса прикладных программ может быть приостановлено.

Если руководитель Службы эксплуатации решает выключить компьютеры или они отключаются сами из-за чрезмерного перегрева, их не следует включать до получения разрешения от подрядчика на сервисное обслуживание технических средств.

Процедуры в случае пожарной тревоги

При обнаружении пожара или дыма в помещении с компьютерами необходимо сделать следующее:

1. Немедленно выключить компьютеры.
2. Попытаться погасить пожар ручным огнетушителем.
   Примечание: огнетушитель должен быть установлен на стене рядом с дверью в помещение, в котором находятся компьютеры.
3. Если не удается погасить пожар:
   - Включите сигнал пожарной тревоги или вызовите пожарную охрану по телефону _____--_____(чрезвычайный вызов_____).
   - Позвоните охраннику по телефону _____.
   - Позвоните старшему менеджеру службы эксплуатации, который уведомит руководителя службы эксплуатации и других руководителей.
   - Убедитесь, что дверь хранилища закрыта и заперта.
   - Возьмите с собой экземпляр Плана действий в непредвиденных обстоятельствах для Отдела Информационных технологий (План ОИТ).
   - Выходя из помещения, в котором находятся компьютеры, выключите аварийный выключатель электрического питания, расположенный рядом с дверью этого помещения.
4. Если время позволяет:
   - Перенесите используемые носители информации из помещения, в котором находятся компьютеры, в безопасное место.
   - Закройте все оборудование большими пластиковыми пленками или листами.
5. Информируйте о происшествии Группу управления в чрезвычайной ситуации (ГУЧС).

Руководитель	_____	_____-_____
Старший менеджер	_____	_____-_____

Процедуры при отказе электропитания

На случай отказа электрического питания обслуживающий персонал должен быть обеспечен карманными фонариками. Небольшой карманный фонарик более удобное средство, чем открытое пламя зажигалки.

Если в компьютерном помещении появились проблемы с электрическим питанием, необходимо выполнить следующие шаги:

1. Немедленно уведомить старшего менеджера службы эксплуатации, который известит Отдел технического обслуживания и руководителя службы эксплуатации.
2. Выключить компьютеры, если это еще не было сделано.
3. Старший менеджер службы эксплуатации уведомит организацию, обеспечивающую сервисное обслуживание технических средств (Сервисный Центр) об отказе электрического питания. Он также уведомит Администраторов баз данных и программного обеспечения (Администраторов БД и ПО), с целью их привлечения к восстановлению работоспособности системы. Если в Компании имеется Справочная служба, которая отвечает на звонки пользователей, он уведомит ее об ожидаемом сроке восстановления системы.

Процедуры в случае затопления.

Ущерб от поступления воды может быть вызван срабатыванием или утечкой спринклерной системы, повреждением труб, поступлением воды из других помещений, например, при тушении пожара и т.п. При поступлении воды необходимо выполнить следующие шаги:

1. Выключите компьютеры.

2. Выключите аварийный выключатель электрического питания.
3. Закройте оборудование полиэтиленовой пленкой, которая должна иметься в хозяйственном отделе на этот случай.
4. Сообщите охраннику об инциденте с тем, чтобы он вызвал нужных специалистов по эксплуатации.
5. Уведомьте старшего менеджера службы эксплуатации, с тем, чтобы он вызвал сервисного инженера, обслуживающего подвергшиеся затоплению технические средства.

Примечание: Специалист Сервисного Центра должен осмотреть оборудование для определения ущерба от поступления воды прежде, чем оно будет включено снова.

Эвакуация помещения

Предприятия, как правило, имеют процедуры для организованной эвакуации здания. Эти процедуры включают в себя проверку оправданности эвакуации и указывают, кто уполномочен отдать распоряжение об эвакуации. Распоряжение об эвакуации из-за угрозы человеческой жизни, из-за пожара, землетрясений, наводнений, взрывов либо опасности взрыва может быть отдано любым лицом, но при других, менее очевидных угрозах, эвакуацию разрешает ответственное должностное лицо.

Служащие должны быть обучены необходимым действиям при чрезвычайных ситуациях и знать маршруты эвакуации из здания. Для поддержания соответствующих навыков должны периодически проводиться плановые учения. Во время учений сотрудники проигрывают чрезвычайные ситуации и знакомятся с людьми, руководящими эвакуацией.

Уведомление Группы управления в чрезвычайной ситуации (ГУЧС)

За своевременное информирование ГУЧС отвечает старший менеджер или руководитель службы эксплуатации. Если человек, находящийся на месте происшествия, не может установить контакт с руководством службы эксплуатации, он пытается сам связаться с ГУЧС. Все члены группы должны быть своевременно оповещены о происшествии:

Имя	Служебный телефон	Домашний телефон
_____	_____	____--_____
_____	_____	____--_____
_____	_____	____--_____
_____	_____	____--_____

Уполномоченные члены ГУЧС после осмотра места происшествия делают первоначальную оценку ущерба, в соответствии с которой принимается решение о целесообразности приведения Плана ОИТ в действие (полностью или частично). Группа принимает следующие решения:

1. Может ли быть продолжена работа компьютеров на месте происшествия в полном или ограниченном объеме и начато выполнение планов ремонта или замены непригодного оборудования.
2. Определяет степень пригодности помещения для дальнейшей эксплуатации и принимает решение о необходимости использования резервного помещения и запуске Плана ОИТ.
3. Намечает план дальнейших действий и информирует о нем высшее руководство.

Оценка ущерба

Незначительный ущерб — обработка данных может быть возобновлена в короткое время без вызова специального персонала. Ожидаемое время простоя — менее одного дня. Ущерб может быть нанесен аппаратным средствам, программному обеспечению, механическому оборудованию, электрооборудованию или зданию.

Серьезный ущерб — назначенные группы вызываются для восстановления нормальной работы в существующем помещении. Предполагаемое время простоя — от двух до шести дней. Нанесен серьезный ущерб аппаратным средствам или зданию.

Катастрофа — обширный ущерб. Восстановление потребует более одной недели. Помещение, в котором находятся компьютеры, или здание может быть полностью разрушено. Вызываются все руководители групп, чтобы начать полное выполнение Чрезвычайного Плана, в том числе:

- Определение степени развертывания Плана (полномасштабно или частично).

- Уведомление высшего руководства.
- Уведомление пользователей.
- Подготовка регулярных отчетов о процессе восстановления для высшего руководства.
- Уведомление пользователей о предполагаемом времени возобновления работ.

НАЧАЛО РАЗВЕРТЫВАНИЯ РЕЗЕРВНОГО ЦЕНТРА

Уведомление ГУЧС других групп

При возникновении чрезвычайной ситуации находящийся на месте происшествия персонал Службы эксплуатации, после принятия первоначальных мер, должен связаться с членами ГУЧС, начиная с первого имени в списке (форма А). Это лицо сразу же известит остальных членов ГУЧС. Группа собирается на месте бедствия, чтобы непосредственно оценить ущерб. Она определяет необходимые действия и уведомляет о них высшее руководство. Если принимается решение известить остальные группы, ГУЧС связывается с ними в соответствии с иерархической структурой оповещения. По телефону диктуется краткое сообщение, которое записывается получателем. По окончании чтения сообщения получатель повторяет его, чтобы исключить искажение информации.

Та же процедура используется при передаче сообщений остальным лицам. Таким образом, гарантируется, что все оповещенные сотрудники обладают одной и той же информацией. В форме А указаны имена всех членов групп и номера их телефонов.

Создание Центра управления

Первая задача ГУЧС состоит в том, чтобы создать Центр управления. Он должен располагаться вблизи места происшествия, например, в соседнем офисе или здании. Если ничего подходящего нет, можно воспользоваться близлежащей гостиницей. Центр управления должен обеспечить максимальную оперативность в течение этого периода.

Помимо основного здания в Плане ОИТ должна быть предусмотрена альтернативная площадка размещения Центра управления: _____.

Альтернативным вариантом является _____.

Начало деятельности Группы восстановления после бедствия (ГВПБ).

Руководитель ГВПБ должен документировать работу группы, фиксируя ее в Журнале регистрации действий по восстановлению после бедствия. На основе этих записей ГУЧС готовит для руководства отчеты о процессе восстановления и направляет их в архив организации. Кроме того, ГУЧС использует журнал для координации действий различных групп.

	Наименование	Служебный тел.	Домашний тел.
	Координатор планирования на случай бедствий		
	Группа управления в чрезвычайной ситуации		
	Группа эксплуатации вычислительных систем		
	Группа ввода и контроля ввода-вывода данных		
	Группа специальных проектов		
	Группа технической поддержки		
	Группа базы данных		
	Группа систем и программного обеспечения		
	Высшее руководство Отдела Информационных технологий		
	Группа Отдела страхования		
	Группа Отдела внутреннего аудита		

ВОССТАНОВЛЕНИЕ ДЕЯТЕЛЬНОСТИ В РЕЗЕРВНОМ ПОМЕЩЕНИИ

Обеспечение функционирования сети связи и другого оборудования

Договоритесь с поставщиками услуг связи относительно поставки и установки временного оборудования, при этом, например, бывшее в употреблении оборудование может быть поставлено в очень короткое время. Проведите предварительное тестирование оборудования, чтобы гарантировать полное восстановление функций сети связи. Обеспечьте полное восстановление связи в исходном или новом помещении.

Контрольные перечни Группы восстановления после бедствия

Приведенные ниже контрольные перечни (Форма Б) должны использоваться каждым руководителем группы, чтобы отслеживать большую часть работ, выполняемых его группой. ГУЧС собирает эти контрольные перечни и готовит детальный отчет о ежедневном выполнении работ. Перечни будут также использоваться для координации всех работ Центром управления.

Организация_____ Форма Б

Контрольный перечень для восстановления после бедствия

ГРУППА: Управления в чрезвычайной ситуации **Дата:** _____._____._____

Руководитель группы:_____

Заместитель:_____

Действия	Ответственный	Дата и время начала	Дата и время окончания
Координация первоначального реагирования на бедствие с использованием установленных для офиса процедур с целью защиты жизни сотрудников и минимизации ущерба имуществу			
Оценка ущерба			
Уведомление высшего руководства			
Принятие решения о выполнении Плана восстановления после бедствия			
Уведомление руководителей групп и начало процесса выполнения Плана			
Подача официального запроса на использование резервных помещений			
Обеспечение чрезвычайного финансирования для покрытия дополнительных расходов			
Создание Центра управления в основном производственном помещении или вблизи него и координация действий по восстановлению			
Начало ведения Регистрационных журналов для восстановления после бедствий			
Регулярное информирование высшего руководства об изменении состояния процесса восстановления			
Анализ политики организации, бюджета отдела и рекомендаций по ограничению затрат с другими группами			
Регулярное информирование пользователей об изменении состояния процесса восстановления			
Составление отчета об убытках			
Сбор Журналов регистрации для восстановления после бедствия от всех групп. Составление ежедневных отчетов о состоянии процесса восстановления			
Принятие мер для получения дополнительной профессиональной помощи			
Координация бесед с кандидатами на прием на работу, чтобы обеспечить заполнение всех вакансий			
Ведение графиков состояния процесса восстановления			

Организация_____ Форма Б

Контрольный перечень для восстановления после бедствия

ГРУППА: Эксплуатации вычислительных систем **Дата:** _____._____._____

Руководитель группы:_____

Заместитель:_____

Действия	Ответственный	Дата и время начала	Дата и время окончания
Оценка ущерба и определение оборудования, необходимого для замены			
Получение необходимого компьютерного оборудования и оборудования для обработки данных от поставщиков, указанных в списке Поставщиков для чрезвычайной ситуации			
Уведомление руководства, выездных специалистов, поставщика с целью анализа плана ремонта оборудования и установки поставленных устройств			
Встреча с членами Группы эксплуатации вычислительных систем и планирование обязанностей по подготовке резервных помещений для установки дополнительного оборудования			
Анализ «холодного» резервного помещения и проверка наличия требуемого электрического питания, громкоговорящей связи, телефонных линий и кондиционеров. Работа с обслуживающим персоналом.			
Получение необходимых носителей с резервными копиями для восстановления и документации, которые будут использоваться в резервном помещении			
Оценка состояния обработки данных и определение сроков восстановления всей системы и (или) отдельных элементов. Разработка плана возобновления выполнения работ в соответствии с графиком			
Создание Центра управления в основном производственном помещении или вблизи него и координация действий по восстановлению			
Составление планов возобновления функционирования высокоприоритетных систем и информирование о них всех пользователей			
Анализ списка требуемых поставок материалов			
Организация перевозки и (или) приобретения запасных частей для замены			
Уведомление поставщиков о бедствии и информирование их об адресе резервного помещения			
Начало приведения в порядок и восстановления основного производственного помещения после того, как резервное помещение будет готово			
Проверка выполнения требований к кабелям и соединителям и других требований, необходимых для возобновления работы в основном производственном помещении			
Составление графика тестирования совместно с обслуживающим персоналом			
Определение ущерба персональным компьютерам, офисному оборудованию, устройствам ввода данных и другому оборудованию и составление графика их замены			

Организация_____ Форма Б

Контрольный перечень для восстановления после бедствия

ГРУППА: Ввода-вывода и контроля данных **Дата:** _____._____._____

Руководитель группы:_____

Заместитель:_____

Действия	Ответственный	Дата и время начала	Дата и время окончания
Определение состояния данных, с которого должно быть начато восстановление			
Сопоставление данных пользователей и последних файлов резервных копий, которые Группа эксплуатации вычислительных систем планирует использовать для восстановления данных			
Получение оригиналов документов для повторного ввода, чтобы привести файлы в соответствие с текущим состоянием данных			
Определение сроков готовности оборудования для ввода данных			
Организация временных помещений для работы			
Уведомление пользователей о бедствии и информирование их о деталях плана возобновления функционирования и способах обработки входных данных			
Получение резервных копий документов и пересмотр календарных планов совместно с пользователями и Группой эксплуатации вычислительных систем			

Организация_____ Форма Б

Контрольный перечень для восстановления после бедствия

ГРУППА: Специальных проектов **Дата:** _____._____._____

Руководитель группы:_____

Заместитель:_____

Действия	Ответственный	Дата и время начала	Дата и время окончания
Организация перевозок в резервные помещения и из них, организация челночных перевозок по расписанию			
Организация перевозок материалов, запасов и оборудования			
Обучение служащих, которым, возможно, придется выполнять работы вне сферы их обязанностей			
Административные услуги: выполнение функций информационного центра с целью ускорения платежей, облегчения работы всех руководителей групп			
Организация доставки внутренней почты между производственными помещениями, расположенными в разных местах			
Доставка необходимой мебели в резервное помещение			
Доставка необходимого офисного оборудования в резервное помещение			
Установка телефонов в резервном помещении			

Организация_____ Форма Б

Контрольный перечень для восстановления после бедствия

ГРУППА: Технической поддержки **Дата:** _____._____._____

Руководитель группы:_____

Заместитель:_____

Действия	Ответственный	Дата и время начала	Дата и время окончания
Обеспечение наличия операционных систем, а также программного обеспечения других управляющих систем			
Последовательное восстановление системы с резервных копий в соответствии с приоритетами и проверка сохранения согласованности результатов обработки данных			
Работа с техническим персоналом поставщика (при необходимости)			
Определение ущерба, нанесенного сети связи, и требований к ее восстановлению			
Работа с телефонной компанией с целью полного восстановления услуг и подача необходимых заказов для замены телекоммуникационного оборудования			
Уведомление пользователей о нарушении предоставления услуг			

Организация_____ Форма Б

Контрольный перечень для восстановления после бедствия

ГРУППА: Базы данных **Дата:** _____._____._____

Руководитель группы:_____

Заместитель:_____

Действия	Ответственный	Дата и время начала	Дата и время окончания
Восстановление базы данных с резервных копий в соответствии с документацией для восстановления			
Восстановление промежуточных данных, чтобы можно было обновить файлы, приведя их в состояние, соответствующее текущей информации			
Выполнение тестов и сверка их результатов с распечатками пользователей			
Обеспечение непрерывности работы с пользователями			

Организация_____ Форма Б

Контрольный перечень для восстановления после бедствия

ГРУППА: Систем и программного обеспечения **Дата:** _____._____._____

Руководитель группы:_____

Заместитель:_____

Действия	Ответственный	Дата и время начала	Дата и время окончания
Координация действий с группами эксплуатации вычислительных систем и контроля ввода-вывода данных, чтобы правильно установить момент восстановления работы. Проверка прикладных систем и библиотек			
Восстановление файлов и обеспечение непрерывности данных путем проведения тестов и сравнения результатов с распечатками пользователей			
Обеспечение работы критически важных прикладных систем			
Задание полного графика обработки данных			

Организация_____ Форма Б

Контрольный перечень для восстановления после бедствия

ГРУППА: Отдела страхования **Дата:** _____._____._____

Руководитель группы:_____

Заместитель:_____

Действия	Ответственный	Дата и время начала	Дата и время окончания
Обследование места бедствия и определение степени ущерба			
Фотографирование места бедствия, если это возможно			
Подготовка подробного отчета об ущербе и расположении оборудования			
Обращение в страховые компании и работа с диспашерами			
Подготовка требований к страховой компании о возмещении ущерба			
Уведомление других групп об условиях замены оборудования согласно имеющемуся страховому полису и о скидке для аренды необходимого оборудования			

Организация_____ Форма Б

Контрольный перечень для восстановления после бедствия

ГРУППА: Отдела внутреннего аудита **Дата:** _____._____._____

Руководитель группы:_____

Заместитель:_____

Действия	Ответственный	Дата и время начала	Дата и время окончания
Проверка правильности процесса восстановления данных, с целью обеспечения их целостности и сохранения согласованности результатов обработки данных			
Анализ финансовой информации, чтобы убедиться в окончании процесса восстановления			
Контроль восстановления файлов, средств контроля данных и средств обеспечения безопасности в течение процесса восстановления			

ВОССТАНОВЛЕНИЕ ПРОИЗВОДСТВЕННЫХ ПОМЕЩЕНИЙ И ФУНКЦИОНИРОВАНИЯ В ПЕРВОНАЧАЛЬНОМ И (ИЛИ) РЕЗЕРВНОМ ПРОИЗВОДСТВЕННОМ ПОМЕЩЕНИИ

Когда в качестве вычислительного центра на период восстановления деятельности используется резервное помещение, необходимо вовремя сфокусироваться на восстановлении основного вычислительного центра. Обычно полное восстановление — двухэтапный процесс. Первый этап заключается в заказе и запуске замещающих аппаратных средств, которые, в конечном счете, будут использоваться как стационарные средства. После того, как постоянное помещение будет готово к использованию, аппаратные средства будут перемещены в постоянное помещение.

ГРУППЫ ВОССТАНОВЛЕНИЯ ПОСЛЕ БЕДСТВИЙ

ОРГАНИЗАЦИОННАЯ СТРУКТУРА ОИТ

За исключением групп Отдела страхования и Отдела внутреннего аудита все члены групп являются сотрудниками Отдела информационных технологий. Очень важно определить круг их обязанностей и полномочий. Структура подчинения определяется схемой организационной структуры.

Разместите здесь организационную структуру вашего Отдела Информационных технологий

СОСТАВ, ФУНКЦИИ И ОБЯЗАННОСТИ ГРУПП

Координатор планирования на случай бедствий

Ф.И.О._____
назначен Координатором планирования на случай бедствий. Он координирует выполнение работ, предусмотренных настоящим Планом.

При составлении Плана Координатор отвечает за накопление всей информации, которая должна быть включена в план. Большая часть данных уже имеется в организации, но не всегда в удобной для использования форме. По мере назначения сотрудников их обязанности, имена, адреса и номера телефонов должны быть введены в различные части Плана. По мере изменения адресов и телефонов вносятся исправления в эталонный экземпляр Плана. Каждое полугодие или год осуществляется рассылка обновлений.

После составления первоначального варианта Плана делаются его копии, которые рассылаются руководителям групп и их заместителям. Копии также должны иметься во всех офисах, указанных в этом документе. Копии должны храниться сотрудниками дома, а не в ящиках столов в офисе, поскольку в случае крупномасштабного бедствия офисы могут быть разрушены.

План должен быть полностью испытан. Это не только подтвердит выполнимость всех процедур, но и обеспечит обучение различных групп. Координатор планирует испытания и документирует их успех или неудачу. Он готовит отчеты для руководства и Отдела внутреннего аудита. В случае неудачных испытаний, он взаимодействует с руководителями групп, чтобы разрешить проблемы и составить план повторных испытаний.

Координатор планирования на случай бедствий представляет свою организацию на семинарах и совещаниях, касающихся восстановления после бедствий. Он должен обладать новейшей информацией и сведениями о процедурах и информирует о них всю организацию. При обновлении аппаратных средств, программного обеспечения и телекоммуникационного оборудования Координатор связывается с сотрудником, ответственным за «горячее» резервное помещение, чтобы убедиться в пригодности резервного центра для функционирования всех критически важных систем.

Группа управления в чрезвычайной ситуации

Руководитель группы систем и программного обеспечения:
Ф.И.О._____
Заместитель:
Ф.И.О._____

Обязанности:

- Координация первоначального реагирования на бедствие, защита жизни сотрудников и имущества.
- Оценка ущерба.
- Определение полноты выполнения Плана ОИТ (полномасштабно, либо частично).
- Уведомление высшего руководства.
- Уведомление руководителей групп и начало выполнения Плана ОИТ.

Члены группы:

- Руководитель Группы эксплуатации вычислительных систем:
  Ф.И.О._____
- Администратор баз данных
  Ф.И.О._____
- Руководитель Группы технической поддержки
  Ф.И.О._____
- Руководитель Группы специальных проектов
  Ф.И.О._____
- Координатор планирования на случай бедствий
  Ф.И.О._____

Функции по восстановлению после бедствия:

- Создание Центра управления в соответствии с положениями Плана ОИТ для обеспечения централизованного управления всеми действиями.
- Информирование всех групп о номере телефона с указанием, что его следует использовать только для передачи и получения необходимой информации.

- Подача официального запроса на использование резервных помещений.
- Начало ведения Журналов регистрации для восстановления после бедствий, в которых регистрируются все действия.
- Регулярное информирование высшего руководства об изменении состояния процесса восстановления.
- Регулярное информирование пользователей об изменении состояния процесса восстановления.
- Принятие мер для получения профессиональной дополнительной помощи.
- Координация бесед с кандидатами на прием на работу, чтобы обеспечить заполнение всех вакансий.

Группа эксплуатации вычислительных систем

Руководитель Группы эксплуатации вычислительных систем:

Ф.И.О._____

Заместитель:

Ф.И.О._____

Обязанности:

- Восстановление файлов, запуск систем в «горячем» резервном помещении.
- Составление графика выполнения работ в «горячем» резервном помещении.
- Координация работ, необходимых для восстановления функционирования систем в прежнем или новом постоянном помещении.
- Заказ и установка вычислительного оборудования, необходимого для нормальной работы в постоянном помещении.

Члены группы:

- Руководитель Службы эксплуатации
  Ф.И.О._____
- Операторы компьютеров — согласно назначениям.
- Ответственный за библиотеку резервных копий.

Функции по восстановлению после бедствия:

Эксплуатация компьютеров:

- Управление работой вычислительных систем или оказание помощи оператору в «горячем» резервном помещении.
- Получение носителей с резервными копиями и восстановление файлов в «горячем» резервном помещении.
- Определение момента возобновления работы критически важных систем.
- Тестирование критически важных систем для решения производственных задач.
- Составление графика обработки данных в «горячем» резервном помещении.
- Уведомление пользователей о графике обработки данных в «горячем» резервном помещении.
- Организация перевозки запасных частей для замены в «горячее» резервное помещение.
- Организация перевозки носителей с резервными копиями из внешнего хранилища в «горячее» резервное помещение.

Подготовка помещения:

- Координация работ по ремонту или строительству нового постоянного помещения в первоначальном или новом месте.

Замена оборудования:

- Определение ремонтопригодности имеющихся аппаратных средств. При необходимости замены надо обратиться к поставщику для получения информации о предлагаемых сроках поставки. Если сроки поставки неудовлетворительны, получить предложения от поставщиков бывших в употреблении технических средств.
- Проверка выполнения требований к кабелям и соединителям, необходимых для возобновления работы.
- Организация поставок другого оборудования для обработки данных.
- Составление графика тестирования совместно со специалистами по техническому обслуживанию.

Подготовка «холодного» резервного помещения:

- Предварительное обследование «холодного» резервного помещения, необходимо убедиться в том, что оно обеспечит временное функционирование размещенного в нем оборудования;
- Подводка необходимого электрического питания, кабелей и соединителей.
- Обеспечение выполнения требований к системе связи.
- Организация охраны и ограниченного доступа в помещение, в котором находятся компьютеры.

- Организация хранения вне основного помещения.

Оборудование, обеспечивающее функционирование компьютеров:
Определение потребности и заказ обеспечивающего оборудования:
- ПК.
- Офисное оборудование для ввода данных;.
- Оборудование для обработки бумажных документов.

Материалы:
- Анализ списка потребностей.
- Обращение к поставщикам, указанным в списке поставщиков на случай чрезвычайной ситуации.
- Организация перевозки имеющихся материалов или закупка материалов для замены.
- Уведомление поставщиков о бедствии и информирование их об адресе резервного помещения.

Группа ввода-вывода и контроля данных

Руководитель Группы ввода и контроля данных:
Ф.И.О._____
Заместитель:
Ф.И.О._____

Обязанности:
- Возобновление работы Группы ввода-вывода и контроля данных в резервном помещении или в дополнительном месте.

Члены группы:
- Руководитель Группы ввода-вывода данных **Ф.И.О.**_____
- Руководитель Группы контроля данных **Ф.И.О.**_____
- Персонал, ответственный за ввод-вывод данных — согласно назначениям.
- Персонал, ответственный за контроль данных — согласно назначениям.

Ввод-вывод данных:
- Определение совместно с Группой эксплуатации вычислительных систем точки, с которой должно быть начато восстановление данных. Сопоставление последних файлов резервных копий, которые Группа эксплуатации вычислительных систем планирует использовать для восстановления данных, с данными пользователя. Получение оригиналов документов, необходимых для повторного ввода данных, чтобы привести файлы в соответствие с текущим состоянием данных;
- Определение сроков готовности оборудования для ввода данных. При необходимости организация ввода данных внешними исполнителями.

Контроль данных:
- Уведомление пользователей о бедствии и информирование их о временных процедурах ввода-вывода данных.
- Обеспечение временных производственных помещений либо в резервном помещении, либо вблизи основного производственного помещения.
- Получение резервных копий документов и пересмотр календарных планов совместно с пользователями и Группой эксплуатации вычислительных систем.

Группа специальных проектов

Руководитель Группы специальных проектов:
Ф.И.О._____
Заместитель:
Ф.И.О._____

Обязанности:
- Организация перевозок людей, материалов и оборудования;
- Административное обеспечение работ по восстановлению.

Члены группы:
- Персонал, ответственный за специальные проекты.

Функции по восстановлению после бедствия:
- Организация перевозок в резервные помещения и из них, организация челночных перевозок по расписанию.
- Организация перевозок людей, запасов материалов и оборудования.

Обучение:
- Обучение служащих, которым, возможно, придется выполнять работы вне сферы их обязанностей.

Административные услуги:
- Организация доставки внутренней почты между производственными помещениями, расположенными в разных местах.
- Обеспечение предоставления всех необходимых административных услуг, например, оплата счетов, расчет заработной платы, обработка

требований о выплате пособий по страхованию служащих, выписка критически важных счетов.
- Организация размещения персонала, работающего в резервном помещении.
- Обеспечение дополнительных офисных помещений мебелью, телефонами и другим офисным оборудованием.

Группа технической поддержки

Руководитель Группы технической поддержки:
Ф.И.О._____
Заместитель:
Ф.И.О._____

Обязанности:
- Инсталляция в резервном помещении программного обеспечения и средств связи, необходимых для возобновления основной деятельности организации.

Члены группы:
- Системные программисты.

Функции по восстановлению после бедствия

Системное программное обеспечение
- Установка операционных систем, а также программного обеспечения других управляющих систем.
- Последовательное восстановление системы с резервных копий в соответствии с приоритетами и проверка консистентности данных.
- Работа в резервном помещении и с техническим персоналом поставщика (по мере необходимости).

Сеть связи:
- Определение ущерба, нанесенного сети связи, и установка оборудования для замены.
- Работа с телефонной компанией с целью полного восстановления услуг и, при необходимости, замена телекоммуникационного оборудования.
- Уведомление пользователей о нарушении предоставляемых услуг.

Группа базы данных

Руководитель группы-администратор базы данных :
Ф.И.О._____
Заместитель:
Ф.И.О._____

Обязанности:
- Полное восстановление базы данных и проверка актуальности данных.

Члены группы:
- Персонал, ответственный за администрирование базы данных.

Функции по восстановлению после бедствия

Восстановление базы данных и обеспечение ее целостности:
- Управление восстановлением базы данных с резервных копий;
- Восстановление промежуточных данных, чтобы можно было обновить файлы, приведя их в состояние, соответствующее текущей информации;
- Прогон тестов и сверка их результатов с распечатками пользователей;
- Работа с пользователями для обеспечения точности обработки данных в будущем.

Группа систем и программного обеспечения

Руководитель Группы систем и программного обеспечения:
Ф.И.О._____
Заместитель:
Ф.И.О._____

Обязанности:
- Обеспечение восстановления производственных систем и проверка непрерывности выполняемой обработки данных.

Члены группы:
- Персонал, ответственный за системы и программное обеспечение.

Функции по восстановлению после бедствия

Восстановление прикладных систем и возобновление их работы:
- Координация действий с Группами эксплуатации вычислительных систем и контроля ввода-вывода данных, чтобы правильно установить точку, с которой должно быть начато восстановление.
- Проверка прикладных систем и библиотек.
- Управление восстановлением файлов и проверка результатов путем тестирования и сравнения результатов с распечатками пользователей.

Прикладные программы:
- Контроль за работой критически важных прикладных систем в резервном помещении или внешних вычислительных центрах.

Группа Отдела страхования

Руководитель Группы отдела страхования:
Ф.И.О._____
Заместитель:
Ф.И.О._____

Обязанности:

- Анализ ущерба и направление в страховую компанию запроса на проведение оценки;
- Предоставление высшему руководству подробного отчета об ущербе.
- Обработка всех заявлений об ущербе.

Члены группы:

- Согласно назначениям.

Функции по выживанию после бедствия
Страхование и компенсация за спасение имущества:

- Обращение в страховые компании и работа с диспашерами.
- Анализ ущерба и определение ремонтопригодности технических средств.
- Подготовка подробного отчета об ущербе и расположении оборудования.
- Подготовка требований к страховой компании о возмещении ущерба.
- Уведомление других групп об условиях замены оборудования согласно имеющемуся страховому полису и о скидке для аренды необходимого оборудования.

Группа Отдела внутреннего аудита

Руководитель Группы внутреннего аудита:
Ф.И.О._____
Заместитель:
Ф.И.О._____

Обязанности:

- Проверка правильности процесса восстановления данных и последующей их обработки.

Члены группы:

- Согласно назначениям.

Функции по восстановлению после бедствия
Проверка полноты процесса восстановления:

- Проверка правильности процесса восстановления данных, с целью обеспечения их целостности и непрерывности обработки.
- Анализ финансовой информации, чтобы убедиться в окончании процесса восстановления.
- Обеспечение контроля и безопасности во время восстановления.
- Контроль восстановления файлов, средств контроля данных и средств обеспечения безопасности в течение процесса восстановления.

ЗАБЛАГОВРЕМЕННОЕ ПЛАНИРОВАНИЕ И ТЕКУЩИЕ ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ ГРУПП

Координатор планирования на случай бедствий:

1) Обновляет документацию Плана, исправляя имена, адреса и номера телефонов.
2) Обеспечивает должную рассылку Плана членам групп.
3) Разрабатывает график проведения испытаний всех этапов Плана.
4) Сотрудничает с Отделом внутреннего аудита, чтобы проверять правильность процедур.
5) Распространяет литературу по безопасности и восстановлению после бедствия.
6) Периодически проверяет резервные помещения.
7) Официально обновляет План каждые шесть месяцев на основе информации, поступающей от групп.

Группа управления в чрезвычайной ситуации

1) Руководитель группы планирует ежеквартальные встречи, обсуждает текущее состояние.

Группа эксплуатации вычислительных систем

1) Обеспечивает обновление поэтажных планов основного и резервного помещений.
2) Обеспечивает обновление схем организационной структуры.
3) Хранит копию всех конфигураций аппаратных средств компании.
4) Обеспечивает обновление списков поставщиков аппаратных средств, программного обеспечения, средств связи, материалов и бланков.
5) Обеспечивает обновление процедур на случай чрезвычайных ситуаций (пожар, затопление и другие потенциальные опасности).
6) Обеспечивает обновление резервных копий, хранящихся вне основного производственного помещения.
7) Обеспечивает обновление резервных копий критически важных отчетов.
8) Обеспечивает хранение данных Журнала регистрации вне основного производственного помещения.
9) Обеспечивает возможность практического использования Планов действий в непредвиденных обстоятельствах.

Группа ввода-вывода и контроля данных

1) Непрерывно обновляет список используемых систем и документов.
2) Хранит копию инструкций по вводу данных вне основного производственного помещения.
3) Заключает соглашения на случай непредвиденных обстоятельств с местными пользователями и (или) поставщиками, предусматривающие возможность использования оборудования другой стороны в случае чрезвычайной ситуации.

Группа специальных проектов

1) Обновляет список транспортных компаний, к которым нужно будет обращаться в случае чрезвычайной ситуации.
2) Устанавливает планы действий в непредвиденных обстоятельствах, касающиеся использования резервов в чрезвычайных ситуациях.

Группа технической поддержки

1) Обеспечивает хранение резервных копий операционных систем и телекоммуникационного программного обеспечения вне основного производственного помещения.
2) Обеспечивает обновление списка файлов и мест их размещения.
3) Обеспечивает обновление информации о сети связи.
4) Обеспечивает возможности восстановления с использованием резервных копий, хранящихся вне основного производственного помещения.

Группа базы данных

1) Обеспечивает полноту мер по хранению резервной копии базы данных вне основного производственного помещения.

Группа систем и программного обеспечения

1) Анализирует все системы с целью принятия должных мер для хранения резервных копий программ, файлов и документов вне основного производственного помещения.
2) Проверяет правильность хранения в соответствии с принятой в компании политикой.
3) Составляет списки всех систем, пользователей, приоритетов обработки данных и ответственных лиц.
4) Выявляет критически важные системы и подготавливает детальные планы восстановления.

Группа Отдела страхования

1) Анализирует охват страхованием и проверяет достаточность Плана.
2) Проверяет отвечает ли страхование требованиям Чрезвычайного Плана и учитывают ли страховые премии затраты на создание резервов.

Группа Отдела внутреннего аудита

Анализирует Чрезвычайный План с целью формирования представления о его адекватности поставленным задачам, проверяет наличие контрольных точек и полноту плана.

ПОСТАВЩИКИ

В настоящем разделе должны быть перечислены не все поставщики, с которыми организация активно сотрудничает в обычной ситуации, а только те конкретные поставщики, к которым необходимо обращаться для ремонта или замены оборудования, либо для получения материалов, критически важных для восстановления работы информационных систем.

Информация о поставщиках должна содержать имена и адреса торговых представителей и технических специалистов, а также списки всех местных и центральных номеров телефонов для чрезвычайного вызова (форма Г).

Кроме того, укажите для каждого из поставщиков степень готовности к реагированию (время реагирования на чрезвычайные ситуации).

ПОСТАВЩИКИ НОВОГО И БЫВШЕГО В УПОТРЕБЛЕНИИ ОБОРУДОВАНИЯ

Для восстановления функционирования после бедствия важно иметь полный список всего оборудования и его спецификации. В этом разделе плана должен быть приведен список поставщиков нового и бывшего в употреблении (б/у) оборудования с краткими характеристиками каждого из поставщиков (список оборудования, которое является основным для этого поставщика, с учетом списка установленного в организации оборудования).

ПОСТАВЩИКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Необходимо иметь полный список всего специального программного обеспечения (как операционных систем, так и прикладных систем). В плане должны быть предусмотрены специальные меры по созданию резервных копий этих пакетов.

ПОСТАВЩИКИ СРЕДСТВ СВЯЗИ

Выполнение заказов на средства связи обычно требует длительного времени, которое, даже в чрезвычайной ситуации, может быть сокращено лишь незначительно. При составлении списка поставщиков следует учитывать время выполнения поставщиками заказов. Если время выполнения заказа превышает требуемое время восстановления функционирования, необходимо предусмотреть закупку менее быстродействующего или более дорогого оборудования, которое может быть поставлено в нужные сроки. Например, можно использовать коммутируемые линии вместо арендованных каналов и т.п.

ПОСТАВЩИКИ СПЕЦИАЛЬНОГО ОБОРУДОВАНИЯ

В основном вычислительное оборудование выполнено в виде унифицированных модулей. Время выполнения заказов такого оборудования относительно невелико. Однако при наличии старого, уникального оборудования либо аппаратно-зависимого прикладного программного обеспечения в плане должны быть приведены специальные стратегии на этот случай. Если обновление или изменение конфигурации уже запланированы, было бы разумно ускорить их осуществление.

ПОСТАВЩИКИ ВСПОМОГАТЕЛЬНОГО ОФИСНОГО ОБОРУДОВАНИЯ

Необходимо перечислить вспомогательное офисное оборудование с указанием альтернатив и возможностей получения услуг от внешних организаций.

ПОСТАВЩИКИ СПЕЦИАЛЬНЫХ БЛАНКОВ

В плане должен быть указан полный список поставщиков специальных бланков. Для того, чтобы описать требования к поставщику, полезно иметь образцы бланков и спецификаций. Время выполнения заказа на бланки часто может быть длительным, особенно если необходимо выполнить весь цикл от эскиза до конечного продукта. Полезно иметь несколько поставщиков одного и того же бланка, поскольку один сильно загруженный поставщик не всегда может достаточно быстро отреагировать на ваши потребности в случае чрезвычайной ситуации. Чтобы ускорить весь процесс, можно обеспечить поставщиков оригинал-макетами бланков.

Форма Г Обновлена _____

Наименование поставщика _____
Адрес локального офиса _____
Номер телефона _____
Контакты:
А.Торговый представитель:_____
Б. Технические представители:_____
1. Аппаратные средства_____
2. Программное обеспечение _____
В. Номер телефона для чрезвычайной ситуации _____
Время реагирования поставщика_____
Оборудование_____
Альтернативное резервное помещение_____

УПОРЯДОЧЕНИЕ ВСЕХ ПРИКЛАДНЫХ СИСТЕМ ПО ПРИОРИТЕТАМ

РАНЖИРОВАНИЕ ВСЕХ СИСТЕМ ПО ПРИОРИТЕТАМ

Основной задачей Отдела Информационных технологий должно быть обеспечение быстрого и гарантированного восстановления функционирования критически важных прикладных систем в случае серьезного прекращения или нарушения нормальной работы из-за пожара, стихийного бедствия, сбоев питания или других чрезвычайных обстоятельств. Выявление критически важных систем проводится для того, чтобы разработать план восстановления функционирования информационной системы предприятия после бедствия. План включает действия, которые должны выполняться как до, так и после бедствия с целью обеспечения полного восстановления работы вычислительных систем. Планирование должно быть достаточно детальным, чтобы главные решения были уже приняты до момента возникновения чрезвычайной ситуации. В этом случае при возникновении бедствия не придется в экстремальной ситуации решать, кто, что и как должен делать.

Полномасштабное функционирование Отдела Информационных технологий в резервном помещении сразу после бедствия как по техническим, так и по финансовым причинам вряд ли будет возможно. Как правило, это не имеет существенного значения, так как степень влияния выполняемых

задач на основной бизнес различна. Следует проанализировать относительную важность выполняемых функций. Ниже приведены процедуры для задания приоритетов функций.

Следует принять во внимание, что в течение начального периода восстановления после бедствия функции вычислительных систем будут выполняться в уменьшенном объеме. При составлении плана необходимо определить, каким критически важным прикладным системам нужно срочно уделить внимание после начала процесса восстановления.

Методика выявления критически важных для организации прикладных систем использует семь факторов, которые позволяют определить возможность ухудшения работы прикладной системы в случае бедствия, а также ограничения, которые могут возникнуть при восстановлении работы прикладной системы.

Этими факторами являются:

1. Допустимое время восстановления прикладной системы после бедствия.
2. Потребность в использовании уникальных ресурсов для восстановления работы прикладной системы.
3. Возможность переноса прикладной системы при ее восстановлении.
4. Опыт обслуживающего персонала Отдела Информационных технологий по успешному проведению испытаний процесса восстановления.
5. Предельно допустимые потери из-за задержки или невозможности восстановления прикладной системы.
6. Наличие недостатков в структуре или функционировании прикладной системы.
7. Аспекты защиты информации, касающиеся структуры или функционирования системы.

Все эти факторы в совокупности определяют относительную важность восстановления конкретных прикладных систем после бедствия. Конкретные баллы устанавливаются следующим образом:

Оценки: Допустимое время восстановления

5 — Требуется обеспечить средний уровень функционирования в течение 4-6 часов после бедствия.
4 — Требуется обеспечить средний уровень функционирования в течение от 7 до 12 часов после бедствия.
3 — Требуется обеспечить средний уровень функционирования в течение от 13 до 24 часов после бедствия.
2 — Требуется обеспечить средний уровень функционирования в течение от 25 до 48 часов после бедствия.
0 — Требования к времени восстановления отсутствуют.

Оценки: Потребность в использовании уникальных ресурсов

5 — Для адекватного восстановления функционирования системы требуется полностью восстановить уникальную базу данных и (или) заказное программное или аппаратное обеспечение и (или) средства связи по некоммутируемым каналам.
4 — Система может адекватно функционировать с использованием коммутируемых каналов при условии наличия всех других уникальных ресурсов.
3 — Адекватное рабочее состояние системы может быть восстановлено лишь при частичном восстановлении ключевых ресурсов, то есть с использованием текущей / резервной версии базы данных.
2 — Для восстановления не требуется никаких уникальных ресурсов.
0 — Система может функционировать в течение периода восстановления после бедствия с отключением некоторых функций / подсистем.

Оценки: Переносимость системы

5 — Прикладная система не может быть успешно восстановлена в помещении, отличном от основного производственного помещения.
3 — Прикладная система может быть успешно перенесена, но с существенной задержкой.
0 — Не ожидается никаких трудностей при перемещении прикладной системы.

Оценки: Опыт восстановления

5 — Обслуживающий персонал Отдела Информационных технологий не имеет успешного опыта проведения испытаний восстановления прикладной системы.
3 — При проведении испытаний прикладная система была успешно восстановлена после значительной задержки.
0 — При успешном проведении испытаний восстановления прикладной системы не возникло никаких задержек или других проблем.

Оценки: Допустимые потери

5 — Невозможность восстановить систему с выполнением требований к срокам и выполняемым функциям может привести к денежным потерям, размер которых превышает установленный руководством предел.

4 — Невозможность восстановить систему с выполнением требований к срокам и функциям создаст проблемы в отношениях с главными заказчиками / поставщиками / профсоюзными объединениями / регулирующими органами, недопустимые с точки зрения руководства и работы.

2 — Система должна быть восстановлена успешно. Потери, связанные с неполным или задержанным восстановлением, являются допустимыми.

0 — Не ожидается никаких потерь, связанных с неполным или задержанным восстановлением.

Оценки: Эксплуатационные недостатки

5 — Для успешного восстановления и нормальной работы требуется непосредственное участие ключевых специалистов и обслуживающего персонала.

4 — Отсутствует обновленная документация прикладной системы и (или) планируется замена прикладной системы.

3 — Прикладная система продемонстрировала чувствительность к изменениям объема, состава и (или) качества вводимых данных и (или) интенсивность отказов была значительной.

0 — Никаких известных недостатков не выявлено.

Оценки: Защита информации

5 — Прикладная система содержит конфиденциальные данные.

4 — Прикладная система управляет распределением денежных средств или иным образом влияет на сохранность собственности.

0 — Не требуется никаких особых мер по защите информации в процессе восстановления, за исключением обычной осторожности.

Использование этой методики оценки позволяет ранжировать прикладные системы по их относительной важности. Максимальный балл 35, соответствует наиболее критически важным системам. Ранжирование послужит основой для соответствующего распределения ограниченных ресурсов в течение периода восстановления.

ЗАЩИТА НОСИТЕЛЕЙ ИНФОРМАЦИИ

ЗАЩИТА И СОХРАНЕНИЕ ЖИЗНЕННО ВАЖНЫХ ДОКУМЕНТОВ

Защита и сохранение жизненно важных документов является частью повседневной работы. Кроме того, компания также несет юридическую обязанность хранить ряд документов определенное количество лет.

Важные документы должны храниться в нескольких экземплярах, необходимо ввести в действие процедуры, обеспечивающие хранение одного из экземпляров в удаленном безопасном месте.

В целях гарантированного сохранения информации, имеющейся в компьютерах, ее копируют на носители, которые помещают в хранилище вне основного производственного помещения.

Независимо от метода, используемого для сохранения документов вне основного производственного помещения, необходимо иметь письменную процедуру, график вывоза и доставки и ответственного за выполнение процедуры.

ЗАЩИТА БАЗЫ ДАННЫХ

Резервные копии базы данных

Полные резервные копии создаются в то время, когда база данных не открыта. Если возможно, скопируйте базу данных на два отдельных носителя и направьте один из них в удаленное хранилище. Другой носитель хранится в основном производственном помещении до создания следующей полной копии.

Обновления

Создаются Журналы регистрации, в которых фиксируются образы всех измененных записей до и после изменения. Эти журналы хранятся в течение семи дней.

Описание базы данных

Если описание базы данных остается практически неизменным, его резервная копия должна создаваться только после его изменения. Если описание изменяется часто, его копии могут создаваться еженедельно наряду с копированием данных изменений. Эти копии должны храниться в удаленном хранилище.

Исходные тексты программного обеспечения

Резервные копии файлов исходных текстов программного обеспечения создаются еженедельно.

СТАНДАРТНЫЕ ПРОЦЕДУРЫ СОЗДАНИЯ РЕЗЕРВНЫХ КОПИЙ

Большинство вычислительных центров создают резервные копии своих файлов и направляют их в удаленное хранилище. Если копия является просто новой версией файла, необходимой для дальнейшей обработки данных, следует создать вторую копию, чтобы ее можно было поместить в удаленное хранилище. Копии, направляемые в удаленное хранилище, должны представлять текущее состояние файлов после обработки данных. Периодичность обработки данных может быть одной из следующих:

- **Ежедневная обработка данных;**
- **Еженедельная обработка данных;**
- **Ежемесячная обработка данных;**
- **Ежегодная обработка данных;**
- **Циклы прикладных систем;**
- **Создание резервных копий дисков.**

ХРАНЕНИЕ ВНЕ ПРОИЗВОДСТВЕННОГО ПОМЕЩЕНИЯ

Удаленное хранение является одним из способов защиты носителей, гарантирующих восстановление файлов после бедствия. Вместе с резервными копиями в удаленном хранилище должен храниться и их реестр. Вторая группа копий должна оставаться в основном производственном помещении. В реестре указываются: сотрудник, ответственный за ведение библиотеки, наименование и описание файлов, время и дата создания файлов.

ДОКУМЕНТАЦИЯ ДЛЯ СИСТЕМ И ПРОГРАММ

Системная документация должна храниться в электронном виде. Если документация существует только в виде оригиналов, нужно сделать копии и поместить их в удаленное хранилище. В качестве программной документации часто используются исходные тексты программ. Резервные копии исходных текстов программ должны создаваться еженедельно, в интервалах создаются копии всех вносимых изменений.

РЕЗЕРВНЫЕ КОПИИ ДОКУМЕНТАЦИИ ДЛЯ ВВОДА ДАННЫХ

Если форматы ввода данных изменяются редко, копия файла форматов ввода данных должна создаваться при каждом изменении формата. Резервная копия должна храниться как в основном производственном помещении, так и в удаленном хранилище. При частых изменениях предпочтительно еженедельное создание резервных копий. При этом до момента создания полной резервной копии регистрируются все изменения. Все изменения сохраняются, пока не создан файл с полной резервной копией. Форматы могут быть внутренние, разработанные для ввода данных с помощью имеющегося специализированного оборудования. Кроме того, должны существовать форматы, которыми смогут воспользоваться внешние организации при необходимости восстановления данных. Остальная документация, касающаяся ввода данных, копируется в виде файла и помещается в удаленное хранилище. Эта документация может содержать такие сведения: представители для контактов среди пользователей, графики, объемы и т.д.

СОЗДАНИЕ РЕЗЕРВНЫХ КОПИЙ ФАЙЛОВ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ

Пользователи, работающие на персональных компьютерах, сами отвечают за защиту файлов. Следует помнить, что хранение единственной копии конфиденциальной информации на рабочем месте не гарантирует ее сохранности в случае бедствия в офисе.

СПЕЦИАЛЬНЫЕ БЛАНКИ

Восстановление запаса специальных бланков в случае бедствия путем заказа их у поставщиков, достаточно длительная процедура. Ситуация может стать критической, если эти бланки нужны для важных прикладных систем, например, для расчета заработной платы, счетов заказчиков и календарного планирования производства. Образцы бланков должны храниться в безопасном месте.

ПРОЦЕДУРЫ ЭКСПЛУАТАЦИИ СЕРВЕРНЫХ ПОМЕЩЕНИЙ

- **СПИСОК ОТВЕТСТВЕННЫХ ЗА ПРИКЛАДНЫЕ СИСТЕМЫ**

Приведите здесь список всех систем, находящихся в эксплуатации, и имена лиц, ответственных за них, указав номера их телефонов и почтовые адреса.

- **ПРОЦЕДУРЫ ВКЛЮЧЕНИЯ ПИТАНИЯ**

Приведите здесь текст установленных процедур или укажите, где их можно найти.

- **ПРОЦЕДУРЫ НАЧАЛЬНОЙ ЗАГРУЗКИ**

Приведите здесь текст установленных процедур или укажите, где их можно найти.

- **ПРОЦЕДУРЫ ВЫКЛЮЧЕНИЯ ПИТАНИЯ**

Приведите здесь текст установленных процедур или укажите, где их можно найти.

- **ГРАФИКИ**

Приведите здесь текст установленных процедур или укажите, где их можно найти.

- **РЕГИСТРАЦИЯ ВЫЧИСЛИТЕЛЬНЫХ РАБОТ**

Приведите здесь текст установленных процедур или укажите, где их можно найти.

ОПЕРАЦИОННАЯ СИСТЕМА

ОПЕРАЦИОННАЯ СРЕДА

Оптимальным является использование в резервном помещении тех же операционных систем, что и в основном вычислительном центре.

СПИСОК СИСТЕМНЫХ ПРОГРАММНЫХ ПАКЕТОВ

Приведите здесь список используемого программного обеспечения или дайте на него ссылку.

НАКОПИТЕЛИ НА ДИСКАХ И РАЗМЕЩЕНИЕ ФАЙЛОВ

Если тип и (или) количество накопителей на дисках, имеющихся в резервном помещении, отличаются от используемых в основном вычислительном центре, составьте заранее схему размещения на них постоянных файлов.

ФИЗИЧЕСКОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И УПРАВЛЕНИЕ ДОСТУПОМ

Физическое обеспечение безопасности начинается с ограничения доступа к имуществу организации. Защищенные компании содержат охрану, которая контролирует все пути доступа к офису. Дополнительная безопасность при этом обеспечивается персоналом, находящимся в приемной каждого здания, каждого этажа или отдела. Дальнейший доступ к различным зонам здания обычно контролируется системой управления доступом. Система управления доступом предотвращает доступ неуполномоченных на это лиц в защищенные зоны.

Системы управления доступом бывают:

- механические (блокировки);
- электронные (обычно электронный блок управления с ключом);
- электромеханические (типа кнопочных устройств, которые работают с электронными устройствами считывания пропусков);
- цифровые (устройства, которые дают возможность пользователям устанавливать любую комбинацию);
- компьютерные (также системы, которые могут включать сигнал тревоги, регистрировать посещаемость сотрудников, контролировать местонахождение сотрудников и формировать отчеты об оперативном контроле).

Права доступа должны быть разграничены для следующих категорий персонала:

- Персонал, обслуживающий компьютеры.
- Персонал отдела информационных технологий.
- Специалисты по техническому обслуживанию и сопровождению.
- Персонал других компаний.

Список защищенных зон:

- Аппаратные средства.
- Средства связи.
- Прочее.

ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ПАРОЛИ ДОСТУПА К СИСТЕМАМ

Как правило, покупное программное обеспечение, равно как и хост-компьютер, защищены паролями. При входе в систему проводится внутренняя проверка паролей по таблицам. Если пароль верен, на экран выводится меню. Когда оператор выбирает элемент меню, система проверяет по таблице паролей имеет ли оператор право доступа к выбранному элементу. Права доступа могут ограничиваться возможностью совершать любые действия с информацией или только считывать ее. Можно маскировать данные на экране так, чтобы была видна только информация, которую оператор имеет право видеть. Если оператор выбирает в главном меню другой покупной пакет программ, ему, вероятно, придется вводить новый пароль, чтобы получить доступ к вновь выбранному пакету.

СОПРОВОЖДЕНИЕ ПРИКЛАДНЫХ СИСТЕМ

Если исходными текстами прикладных систем заведует система ведения библиотеки, некоторые прикладные программы могут быть защищены паролем, ограничивающим доступ к исходному тексту. Во многих организациях, которые не изготавливают продукцию для конфиденциального использования, единственными программами, которые защищены паролем, являются программы для распределения денежных средств, например, расчета заработной платы и дебиторской задолженности. Защита с использованием пароля поможет предотвратить несанкционированное внесение изменений в программное обеспечение.

ВЕДЕНИЕ ПАРОЛЕЙ

Каждая организация должна иметь формальную процедуру ведения паролей. В начале процедуры устанавливается порядок задания паролей для новых сотрудников. Перед выдачей паролей документы должны быть утверждены руководством. При этом должны быть указаны все полномочия на доступ, которые предоставляются сотруднику. Ввод паролей обычно является обязанностью лица, ответственного за безопасность, или сотрудника Отдела технического обслуживания. Независимо от того, кто отвечает за ввод данных, за проверку паролей отвечает другой, наделенный только правами просмотра сотрудник, который осуществляет контроль паролей, по крайней мере, один раз в месяц. Процедура ведения паролей должна также предусматривать обязательный ввод нового пароля всеми операторами терминалов по крайней мере один раз в квартал.

Формальная процедура также предусматривает обязательную ликвидацию пароля, когда сотрудник покидает организацию.

РЕЗЕРВНЫЕ ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ (ЦОД)

Наличие «горячего» резервного центра обработки данных (ЦОД) с установленным оборудованием, протестированной операционной средой и критически важными приложениями минимизирует отрицательные последствия для организации при возникновении бедствия.

«Холодный» резервный ЦОД — пустое помещение, оборудованное, как минимум, фальшполом, кондиционерами, гарантированным электроснабжением, противопожарными средствами и освещением, которое готово к установке вычислительного оборудования.

При возникновении чрезвычайной ситуации поставщики технических средств будут максимально помогать вам, но, тем не менее, поставка оборудования займет от 6 до 10 дней. Поставленное оборудование должно быть установлено и протестировано. Эти задержки необходимо учитывать при оценке последствий чрезвычайных ситуаций для бизнеса.

Наличие полностью оборудованного основного ЦОД и «холодного» резервного помещения, вкупе с разработанными в «Плане восстановления после бедствия (DRP)» процедурами его перевода в «горячий» режим, как правило, экономически наиболее целесообразное решение. Основным недостатком при этом является неизбежная задержка, связанная с переводом «холодного» резервного помещения в «горячий» режим.

АБОНИРОВАНИЕ РЕЗЕРВНОГО ЦОД

На западном рынке существует широкий выбор полностью оборудованных резервных ЦОД. Помещения могут отличаться по предлагаемой площади, типу и размерам установленного оборудования, средствам обеспечения физической защиты помещения или географическому положению, но во

всех случаях предлагается основное — работающие компьютеры, готовые к использованию клиентами.
Контракт на услуги должен содержать следующие сведения: условия и дату вступления в силу, определение терминологии контракта, условия использования помещения, суммы и график платежа, условия, касающиеся нескольких одновременных бедствий, ответственность, изменения аппаратных средств, конфиденциальность и условия расторжение контракта.

ПЛАН ПОМЕЩЕНИЯ

Компания, с которой заключен контракт, должна предоставить план помещений, включая компьютерный зал, приемную, зал заседаний и т.п.

ИСПЫТАНИЯ

Для уверенности в действенности Плана в случае бедствия он должен регулярно испытываться. Основной и резервный ЦОДы как правило непрерывно обновляются. Добавляется новое программное обеспечение, модернизируется оборудование и возможно появление проблем с прикладными системами, которые ранее успешно прошли испытания. Испытания — единственный способ обеспечить гарантированный и относительно безболезненный перенос деятельности в резервный ЦОД.
Испытания должны регулярно документироваться. Нельзя полагаться на знания ключевого специалиста, который отвечает за восстановление операционной системы, необходимых библиотек и файлов. В момент бедствия ключевой специалист наверняка будет отсутствовать.

Первоначальное испытание

Первоначальное испытание должно касаться восстановления операционной системы, тестирования языка управления заданиями (JCL), восстановления файлов на специфических дисковых системах, проверки системы связи и проверки простого пакетного задания, запускающего приобретенное программное обеспечение. Потребуются испытания критических прикладных систем. Первоначальные испытания порой оказываются неудачными. Ключ к успеху — регистрация успехов и неудач с последующей корректировкой Плана, учитывающей результаты предыдущих испытаний.

Восстановление файлов и библиотек
Удачное восстановление части библиотек и файлов на диске при первой попытке испытаний — уже успех. При последующих испытаниях проверяется восстановление файлов по резервным копиям, заархивированным в удаленном хранилище. Если дисковые массивы в резервном помещении отличаются от основных, заранее запланируйте, как на них переписывать файлы, сколько места отвести под рабочие области и т.д.

Испытание критически важных прикладных систем
Все критически важные прикладные системы должны тестироваться. Это единственный способ убедиться, что они будут работать в резервном помещении. Подготовьте график проведения испытаний всех критически важных прикладных систем и зафиксируйте все успехи и неудачи.

Испытание систем связи
При испытании некоторых прикладных систем может потребоваться система связи. Испытание системы связи должно быть проведено как можно скорее, чтобы заранее определить потребности в каналах связи.

Имитация бедствий
Несмотря на наличие плана испытаний в резервном помещении, руководство должно спланировать проведение неожиданных внеплановых испытаний с использованием имитации бедствий. При имитации бедствия, когда персонал заранее не знает, когда и какой вид испытаний должен быть проведен, можно лучше оценить эффективность своего Плана.

Испытания компиляции программ
Обеспечение возможности работы программистов в резервном помещении — существенная часть Плана восстановления после бедствия. Программисты должны иметь доступ к исходным текстам программ, перетранслировать их, редактировать связи. Они также нуждаются в доступе к средствам программирования и отладки. Необходимо проверить возможность трансляции для всех используемых языков.

ОБЪЕМ СТРАХОВОЙ ОТВЕТСТВЕННОСТИ

Информация — это собственность организации, которая требует такой же защиты, как и другие формы собственности. Руководство несет ответственность перед акционерами по защите всей собственности. Компьютеры так же важны для организации, как электроэнергия. Компания не сможет выжить, если из-за бедствия нельзя будет использовать компьютеры.

Страхование может покрывать стоимость замены/восстановления оборудования и помещений, которым нанесен ущерб в результате бедствия. Страхование от прерывания деятельности служит защитой от дополнительных издержек в течение периода восстановления.

Некоторые большие организации имеют «зонтичное» страхование, которое охватывает несколько компаний, расположенных в различных местах. Любой тип страхования организации должен быть согласован с положениями Плана. Наличие хорошо документированного и регулярно испытываемого Плана снижает размеры страховых взносов.

- **СТРАХОВАНИЕ ОБРАБОТКИ ДАННЫХ**

Укажите, что покрывается страхованием (или приведите ссылку на источник этой информации).

- **СТРАХОВАНИЕ АППАРАТНОГО ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРОВ**

Укажите, что покрывается страхованием (или приведите ссылку на источник этой информации).

- **СТРАХОВАНИЕ ОБРАБОТКИ ДАННЫХ ИНЫМИ СРЕДСТВАМИ И ОФИСНОГО ОБОРУДОВАНИЯ**

Укажите, что покрывается страхованием (или приведите ссылку на источник этой информации).

- **СТРАХОВАНИЕ ОТ ПРЕРЫВАНИЯ ДЕЯТЕЛЬНОСТИ**

Укажите, что покрывается страхованием (или приведите ссылку на источник этой информации).

ВЕДЕНИЕ И ВЫПОЛНЕНИЕ ПЛАНА

После разработки Плана запускается процесс его регулярного обновления и совершенствования, что гарантирует его актуальность и эффективность. Ответственность за ведение Плана несет Координатор планирования на случай бедствий. Выполнение Плана — обязанность каждого сотрудника. Руководитель Отдела информационных систем несет ответственность за выполнение Плана в целом, но весь персонал должен знать содержание Плана и уведомлять руководителя о выполнении или невыполнении любого действия, предусмотренного в Плане.

Одним из «церберов» организации является Отдел внутреннего аудита. Отдел отвечает за проверку того, что все отделы следуют стратегии, которую установило руководство. Во многих случаях именно Отдел внутреннего аудита "подталкивает" руководство Отдела Информационных технологий к формализации Плана и доведению его до каждого сотрудника.

ВЕДЕНИЕ ПЛАНА ДЕЙСТВИЙ В НЕПРЕДВИДЕННЫХ ОБСТОЯТЕЛЬСТВАХ

ОБЯЗАННОСТИ КООРДИНАТОРА ПЛАНИРОВАНИЯ НА СЛУЧАЙ БЕДСТВИЙ

Для того, чтобы предотвратить устаревание Плана, устанавливается график его официального обновления (см. форму ниже). Наряду с плановыми обновлениями проводятся и промежуточные обновления для учета возникших изменений (например, изменения адресов, обновления аппаратных средств, закупки программного обеспечения и т.д.). Плановые обновления проводятся с интервалом в шесть месяцев.

Плановая дата		Дата выполнения

ОБЯЗАННОСТИ РУКОВОДИТЕЛЯ ГРУППЫ

Каждый Руководитель группы обязан также просматривать и обновлять свой раздел Плана по крайней мере каждые шесть месяцев (см. форму ниже).

Руководители групп	Дата	ФИО
Группа эксплуатации вычислительных систем	_____	_____
Группа ввода и контроля ввода-вывода данных	_____	_____
Группа специальных проектов	_____	_____
Группа технической поддержки	_____	_____
Группа систем и программного обеспечения	_____	_____
Группа Отдела страхования	_____	_____
Группа Отдела внутреннего аудита	_____	_____

КОНТРОЛЬНЫЙ ПЕРЕЧЕНЬ ДЛЯ ПЛАНИРОВАНИЯ НА СЛУЧАЙ БЕДСТВИЙ

После того, как организация выполнила анализ рисков, необходимо провести инвентаризацию существующей среды и запланированных улучшений. Элементы контрольного перечня отражают передовой опыт ведения деятельности, который может быть внедрен в вашу практику.

Подготовка к составлению Плана требует участие специалистов во многих областях деятельности. Это не только дает точное представление о состоянии организации, но и создает чувство ответственности у всего персонала. Любой план, хороший или плохой, будет иметь больший успех, если к нему будут стремиться все участники.

Контрольный перечень разделен на следующие основные категории:

- Общие сведения.
- Вычислительный центр.
- Ввод данных.
- Контроль данных.
- Помещение, в котором находятся компьютеры.
- Библиотека резервных копий.
- Передача данных.
- Системы и программирование.
- Техническая поддержка.
- Администрирование базы данных.
- Внутренний аудит.
- Страхование.
- Резервное помещение.
- Взаимные соглашения.

Многие из категорий непосредственно соответствуют разделам Плана действий в непредвиденных обстоятельствах для Отдела информационных технологий. После каждого вопроса имеется место для ответа: «Да», «Нет» и «Выполняется». Обязательно должен быть ответственный за выполнение действия. Контрольный перечень представляет собой рабочий документ, который может модифицироваться с течением времени.

ОБЩИЕ СВЕДЕНИЯ

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Если бы сегодня в вашем вычислительном центре произошло крупное бедствие, смогла бы ваша организация выжить?				
2. Проводился ли в последнее время анализ риска и последствий бедствия?				
3. Известна ли общая стоимость возможных потерь в связи с вашей незащищенностью от внешнего воздействия?				

4. Установлены ли приоритеты всех ваших программ?				
5. Определено ли максимально допустимое время бездействия для всех ваших систем?				
6. Установлены ли цели плана на случай бедствий и допущения, на которых он основан?				
7. Имеется ли план на случай бедствий и регулярно ли он в обновляется?				
8. Указаны ли в плане резервные помещения: • «Горячее» резервное помещение, • «Холодное» резервное помещение, • Предусмотрены ли взаимные соглашения?				
9. Поступают ли из резервного помещения уведомления об изменениях в аппаратных средствах или программном обеспечении?				
10. Определена ли стоимость планирования на случай бедствий, включая: • Первоначальные затраты, • Стоимость разработки плана, • Стоимость ведения плана?				
11. Утвержден ли План высшим руководством?				
12. Назначен ли Координатор планирования на случай бедствий?				
13. Назначен ли ответственный за корректировку плана?				
14. Используется ли в плане концепция групп?				
15. Назначен ли руководитель каждой группы?				
16. Руководит ли одно и то же лицо несколькими группами?				
17. Обновляются ли регулярно имена и номера телефонов?				
18. Был ли План рассмотрен отделами внутреннего аудита, защиты информации и страхования?				
19. Обеспечивает ли План восстановление деятельности после крупного бедствия и может ли быть скорректирован на случай менее серьезного события?				
20. Прошел ли план испытания с использованием только материалов, хранящихся вне основного производственного помещения?				
21. Проверяется ли план по крайней мере каждые 6 месяцев?				
22. Был ли скорректирован План по результатам испытания?				
23. Проводилось ли когда-либо внезапное испытание плана?				
24. Имеются ли в плане инструкции, касающиеся: • Процедур действий в чрезвычайной ситуации, • Организационной структуры, которая начинает функционировать после бедствия, • Хранения всех материалов, используемых для восстановления деятельности после бедствия, вне основного производственного помещения?				
25. Обеспечены ли для хранилища вне основного производственного помещения: 24-часовый доступ, физический контроль доступа, наличие сейфов, защита от пожара, курьерская служба, время перемещения по замкнутому маршруту менее 1 часа, доступ в него только уполномоченных лиц?				
26. Хранятся ли резервные копии в отдельно контролируемом помещении внутри контролируемой зоны?				
27. Вся ли системная документация, за исключением распечаток программ, хранится в несгораемом шкафу, когда она не используется?				
28. Имеются ли письменные инструкции, которые определяют обязанности пользователей персональных компьютеров (ПК) по резервному копированию и защите своих файлов?				
29. Доведены ли эти инструкции до сведения всех пользователей ПК?				
30. Проинформирован ли весь персонал вычислительного центра относительно конфиденциальности всей информации, с которой он работает?				

ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Имеет ли вычислительный центр освещенные наружные указатели?				
2. Защищено ли здание охранниками, оградой, системами сигнализации и (или) системой внутреннего наблюдения?				
3. Помещена ли проводка всех систем контроля и сигнализации в трубопроводы?				
4. Совершают ли охранники регулярный обход здания?				
5. Если охранники не используются, имеются ли лица, ответственные за безопасность, обученные профессионалами?				
6. Назначен ли ответственный за безопасность вычислительного центра, компании или здания?				
7. Находятся ли охранники или персонал помещения, в котором расположены компьютеры, всегда на рабочем месте?				
8. Организован ли доступ в помещение и различным его зонам по карточкам?				
9. Все ли служащие носят идентификационные значки?				
10. Осуществляется ли регистрация входящих и выходящих посетителей?				
11. Имеется ли охрана в приемной?				
12. Опубликована ли информация на случай чрезвычайной ситуации в офисе или здании, которая содержит описание процедур на случай: • Оказания медицинской помощи, • Пожара, • Эвакуации, • Угрозы наличия бомбы, • Проникновения посторонних, • Отказа электрического питания?				
13. Назначен ли ответственный за обеспечение информацией, обучение и контроль за положениями, указанными в пункте 12?				
14. Имеются ли во всех коридорах схемы эвакуации?				
15. Все ли служащие получили инструктаж и обучение по процедурам действий в чрезвычайных ситуациях?				
16. Проводятся ли регулярные пожарные учения под контролем начальника местной пожарной команды?				
17. Имеется ли письменная процедура увольнения, которая включает контрольный перечень предметов, которые должны быть возвращены компании (например, ключей, идентификационных значков, карточек для доступа и т.д.) в случае увольнения сотрудника?				
18. Выполняют ли обязанности всех служащих, находящихся в отпуске, другие лица?				
19. Все ли помещения всех зданий имеют систему пожарной сигнализации?				
20. Проводились ли испытания оборудования для обнаружения и тушения пожара в последние 6 месяцев?				
21. Проводит ли страховая компания или отдел пожарной охраны ежегодные противопожарные инспекции?				
22. Защищено ли хранилище для форм и запасов материалов спринклерными системами?				
23. Имеются ли в хранилище датчики дыма?				

ВВОД ДАННЫХ

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Существуют ли иные варианты ввода данных, которые обычно вводятся в оперативном режиме?				
2. Обеспечены ли возможности для ввода данных во внешнем помещении при чрезвычайных ситуациях?				
3. Хранится ли копия инструкций по вводу данных в удаленном хранилище?				
4. Если для ввода данных используется пакет программ, доступен ли он для внешних служб?				
5. Приняты ли меры для того, чтобы ввод данных могли осуществлять дочерние предприятия или филиалы?				
6. Задокументированы ли все ручные процедуры, выполняемые при вводе данных, и хранятся ли копии этих документов в удаленном хранилище?				
7. Собраны ли исходные документы в пакеты и контролируются ли они другим отделом?				
8. Регистрируется ли на исходных документах после ввода дата и время ввода и оператор?				
9. Хранятся ли в течение непродолжительного времени исходные документы в их первоначальных пакетах, чтобы в случае необходимости их можно было ввести заново?				
10. Возвращаются ли исходные документы после ввода данных в Отдел контроля данных?				
11. Можно ли в случае необходимости восстановить деятельность Отдела ввода данных в другом помещении в приемлемо короткое время?				

КОНТРОЛЬ ДАННЫХ

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Ограничен ли доступ в Отдел контроля данных?				
2. Проходят ли все исходные документы и компьютерные отчеты через этот отдел для контроля и устранения несоответствий?				
3. Имеется ли альтернативный способ передачи отчетов пользователям при отказе системы связи?				
4. Отвечает ли этот отдел за контроль бланков чеков? 5. Имеется ли письменная процедура для выдачи запаса незаполненных чеков вне помещения, в котором находятся компьютеры?				
6. Разные ли люди подписывают чеки, балансируют и распределяют их?				
7. Можно ли заменить подписанта чеков в течение ночи?				
8. Имеется ли какое-либо специальное офисное оборудование, которое имеет критически важное значение для работы вычислительного центра и меры по резервированию которого не были приняты?				
9. Хранятся ли в организации резервные факсимиле подписей в удаленном хранилище?				
10. Имеется ли формальная система для заказных форм, в которой хранятся идентификаторы всех форм, даты их повторного заказа, данные об их поставщиках и альтернативных поставщиках?				
11. Хранится ли небольшое число всех критически важных заказных форм в удаленном хранилище?				
12. Хранятся ли экземпляры всех спецификаций форм и экземпляры окончательно утвержденных форм в удаленном хранилище?				
13. Хранится ли адресный список для всех поставщиков офисного оборудования и форм?				
14. Запланирован ли альтернативный способ вывоза и доставки на тот случай, если нельзя будет использовать основной способ?				
15. Имеется ли для каждого напечатанного отчета список рассылки, в котором указывается: количество экземпляров, сортировка, разбивка на части, способ доставки, наименования получателя и номер телефона получателя?				

ПОМЕЩЕНИЕ, В КОТОРОМ НАХОДЯТСЯ КОМПЬЮТЕРЫ

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Ограничен ли доступ в помещение, в котором находятся компьютеры?				
2. Разрешено ли пользоваться компьютерами только операторам?				
3.Защищена ли комната галогенным, углекислым газом или спринклерными системами?				
4. Размещаются ли датчики дыма: • На потолке, • Под фальшполом, • В трубопроводах кондиционеров воздуха?				
5. Будут датчики дыма функционировать даже в случае отключения электрического питания?				
6. Размещены ли огнетушители у всех выходов?				
7. Размещены ли под полом датчики воды?				
8. Хранятся ли в помещении, в котором находятся компьютеры, водонепроницаемые покрывала на случай чрезвычайных ситуаций?				
9. Установлена ли система бесперебойного электрического питания на случай кратковременных отключений питания?				
10. Имеется ли генератор на случай длительного отключения питания?				
11. Имеется ли аварийное освещение в помещении, где находятся компьютеры?				
12. Установлен ли у выходов аварийный выключатель электрического питания?				
13. Имеется ли более одной системы охлаждения, чтобы обеспечить работоспособность компьютеров, если одна из систем откажет?				
14. Будет ли подан сигнал тревоги при отключении системы кондиционирования воздуха?				
15. Осуществляется ли контроль температуры и влажности?				
16. Сработает ли какая-либо визуальная или звуковая аварийная сигнализация, если будут превышены предельно допустимые значения?				
17. Установлены ли противопожарные двери на всех входах в помещение, в котором находятся компьютеры?				
18. Хранятся ли бланки чеков в защищенном месте?				
19. Имеются ли письменные инструкции для включения и выключения питания системы?				
20. Имеются ли письменные инструкции для действий в чрезвычайной ситуации?				
21. Имеется ли копия Плана действий в непредвиденных обстоятельствах для Отдела Информационных технологий в помещении, в котором находятся компьютеры?				
22. Используется ли библиотека процедур, которая содержит все управление заданиями, необходимое для выполнения потоков заданий?				
23. Имеется ли формализованная система составления графика выполнения заданий либо с помощью компьютера, либо вручную?				
24. Назначен ли ответственный за анализ графика и ввод всей информации контрольной записи?				
25. Защищен ли ввод информации контрольной записи и подобных функций управления заданиями от вмешательства оператора?				

26. Управляются ли лентопротяжные устройства системой ведения библиотеки?				
27. Анализирует ли руководитель причины, по которым оператор действует в обход системы ведения библиотеки?				
28. Просматривает ли руководство службы эксплуатации протокол регистрации на системной консоли и список ошибок, чтобы убедиться в том, что выявленные ошибки исправлены, а повторяющиеся ошибки предотвращены?				
29. Имеются ли письменные процедуры перезапуска для всех эксплуатируемых систем?				
30. Указано ли в процедурах перезапуска, что выполнение заданий другими системами, вероятно придется повторить, даже если оно было выполнено успешно?				
31. Задокументированы ли детальные процедуры восстановления для всех высокоприоритетных систем?				
32. Регистрируются ли все проблемы в помещении, в котором находятся компьютеры?				
33. Осуществляется ли сопоставление измеренного времени с истекшим?				
34. Имеется ли формализованная Система управления разрешением проблем для помещения, в котором находятся компьютеры, в соответствии с которой проблемы рассматриваются специалистами службы эксплуатации и программистами и определяются меры для их устранения?				
35. Анализирует ли руководство службы эксплуатации все простои?				
36. Анализирует ли Отдел эксплуатации все управление заданиями, после того как испытания завершены и прежде чем программы будут введены в эксплуатацию?				
37. Имеются ли Руководства по выполнению заданий для всех производственных прикладных систем?				
38. Имеют ли операторы легкий доступ к Руководствам по выполнению заданий?				
39. Хранятся ли копии Руководств по выполнению заданий в удаленном хранилище?				
40. Задокументирована ли вся специальная обработка данных в конце каждого квартала и года?				
41. Планируется ли выполнение пакетных заданий для каждой смены?				
42. Имеется ли автоматизированная система учета заданий?				
43. Анализируются ли отчеты о выполнении заданий, чтобы обнаружить необычный ход их выполнения?				
44. Проводится ли анализ всех новых систем, чтобы проверить, что копии файлов должным образом направляются в удаленное хранилище?				
45. Имеется ли список всех аппаратных средств компьютеров с указанием серийных номеров, средств и линий связи, требований к электрическому питанию, требований к охлаждению, требований к площади и список допустимого оборудования для замены всего перечисленного выше и хранится ли копия этого списка в удаленном хранилище?				
46. Имеется ли схема размещения кабелей и описание разъемов для имеющегося оборудования и хранятся ли их копии в удаленном хранилище?				
47. Ведется ли список данных о всех поставщиках компьютерного оборудования и материалов?				
48. Запросили ли вы у поставщика технических средств, бывших в употреблении, список имеющегося оборудования, чтобы подготовиться к чрезвычайной ситуации?				
49. Осуществляется ли ежедневное создание резервных копий и их передача в удаленное хранилище для следующего: • библиотека процедур; • система ведения библиотеки резервных копий; • график выполнения заданий?				
50. Имеется ли формальная процедура вывода программ из употребления?				
51. Задокументированы ли процедуры для работы с микрофишами и хранятся ли их копии в удаленном хранилище?				
52. Имеются ли водопроводные трубы вблизи или над помещением, в котором находятся компьютеры?				
53. Имеется ли угроза утечки воды из близлежащих помещений: кухни, комнат для отдыха и т.п.?				

БИБЛИОТЕКА РЕЗЕРВНЫХ КОПИЙ

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Защищена ли библиотека галогенным, углекислым газом или спринклерными системами?				
2. Имеются ли в библиотеке датчики дыма?				
3. Имеется ли на входе в библиотеку противопожарная дверь?				
4. Имеется ли в библиотеке аварийное освещение?				
5. Ограничен ли доступ к библиотеке благодаря использованию карточек или других средств ограничения доступа?				
6. Установлен ли снаружи входа в библиотеку огнетушитель?				
7. Хранятся ли в библиотеке другие материалы, кроме резервных носителей?				
8. Имеет ли удаленное хранилище резервных носителей средства обеспечения безопасности, защиту от пожара, 24-часовый доступ, систему вывоза и доставки?				

СИСТЕМЫ И ПРОГРАММИРОВАНИЕ

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Создаются ли резервные копии всего прикладного программного обеспечения, которые направляются в удаленное хранилище?				
2. Требуется ли утверждение всех изменений в программах?				
3. Имеются ли контрольные следы, идентифицирующие любую программу, которая была скопирована для изменения, или новую разрабатываемую программу?				
4. Защищено ли паролями все прикладное программное обеспечение, ответственное за распределение денежных средств, например, подготовку расчетной ведомости и счетов к оплате?				
5. Имеют ли вышеупомянутые системы адекватные средства контроля, например, подсчет итоговых величин для пакета, подсчет контрольных сумм и др.?				
6. Делаются ли в отчете отметки о контрольном следе контрольные величины, значения которых выходят за пределы нормального диапазона?				
7. Указаны ли в контрольном следе счетов к оплате список получателей платежа для всех проверок?				
8. Для всех ли финансовых прикладных программ составляются полные отчеты о контрольных следах?				
9. Хранится ли вся документация для систем, функционирующих в основном производственном помещении, в несгораемых шкафах?				
10. Просят ли пользователей помочь в подготовке данных для испытаний?				
11. Имеется ли формальная методика для проектирования и программирования?				
12. Завершается ли этап проектирования до начала этапа программирования?				
13. Имеются ли письменные стандарты проектирования и программирования?				
14. Классифицированы ли постоянные файлы как критически важные, важные, полезные и несущественные?				
15. Требуется ли в соответствии со стандартами создание резервных копий всех критически важных файлов?				
16. Хранятся ли 3 самых последних версии всех важных и критически важных файлов?				
17. Требуют ли стандарты, чтобы все программы имели должные средства контроля и контрольные суммы для аудита, обнаружения и исправления ошибок?				
18. Сохраняются ли данные для испытаний с требуемыми результатами испытаний и используются ли они для усиленно сопровождаемых систем типа систем для подготовки расчетной ведомости?				

19. Вносятся ли изменения всегда в исходный текст программ?				
20. Хранится ли исходный текст программ в библиотеке, резервная копия которой создается и направляется в удаленное хранилище?				
21. Анализируются ли отчеты о редактировании связей программ на наличие ошибок и сохраняются ли они с распечаткой исходного текста?				
22. Всегда ли тестируются программы даже тогда, когда в них вносятся незначительные изменения?				
23. Анализирует ли руководство время от времени изменения в программах и результаты испытаний?				
24. Утверждают ли отделы пользователей изменения программ и анализируют ли они результаты испытаний?				
25. Имеется ли формальная процедура для ввода разрабатываемой программы в эксплуатацию?				
26. Необходимо ли наличие Руководства по эксплуатации для ввода программы в эксплуатацию?				
27. Задокументированы и запрограммированы ли все изменения приобретенного программного обеспечения таким образом, что это не нарушает поставленного текста программ?				
28. Имеется ли список всех имеющихся систем с указанием ответственных лиц?				
29. Имеется ли список всех программ системы?				
30. Имеется ли для каждой системы лицо, ответственное за резервное копирование?				
31. Обновляется ли документация?				
32. Ведется ли документация в компьютере, создается ли ее резервная копия и направляется ли она в удаленное хранилище?				
33. Имеется ли список всех технических руководств, чтобы они могли быть заменены в случае необходимости?				
34. Устанавливает ли политика вашей компании период хранения файлов информации о фондах компании, об акционерах, данных о налогообложении, информации о персонале и других жизненно важных данных?				
35. Хранится ли информация о размещении данных в течение периода хранения вместе с носителями файлов?				
36. Была ли идентифицирована исходная информация, на основе которой созданы сохраняемые данные?				

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Создаются ли резервные копии операционных систем, которые направляются в удаленное хранилище?				
2. Ведется ли список всего программного обеспечения операционной системы?				
3. Прошел ли персонал Отдела обучение смежным специальностям, чтобы каждый мог осуществлять резервное копирование?				
4. Задокументированы ли все ответственности, обязанности и процедуры и хранятся ли копии этих документов в удаленном хранилище?				
5. Ведется ли список данных о всех поставщиках программного обеспечения?				
6. Приняты ли меры для того, чтобы приобретенное программное обеспечение могло функционировать на другой системе в случае чрезвычайной ситуации?				
7. Хранится ли копия параметров SYSGEN в удаленном хранилище?				
8. Имеется ли полная версия документации, объясняющая как восстановить операционную систему в резервном помещении?				
9. Документируется ли использование всех дисковых устройств?				
10. Составлен ли план использования дополнительных дисковых устройств?				
11. Имеется ли документация, объясняющая как изменить язык управления заданиями для их выполнения в резервном помещении?				

АДМИНИСТРИРОВАНИЕ БАЗЫ ДАННЫХ

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Идентифицированы ли все базы данных?				
2. Идентифицированы ли все программы, которые обновляют данные в каждой базе?				
3. Проводится ли непрерывная регистрация всех действий, которые обновляют базы данных?				
2. Идентифицированы ли все программы, которые обращаются к каждой базе данных?				
5. Создаются ли резервные копии баз данных, которые направляются в удаленное хранилище?				
6. Имеются ли контрольные следы, идентифицирующие базы данных, которые архивируются, и формируются ли эти отчеты ежедневно?				
7. Имеются ли задокументированные процедуры проверки правильности информации в каждой базе данных после ее восстановления?				
8. Имеется ли документация, идентифицирующая несколько баз данных, которые должны быть синхронизированы друг с другом?				

ВНУТРЕННИЙ АУДИТ

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Проводили ли вы анализ Плана действий в непредвиденных обстоятельствах для Отдела Информационных технологий?				
2. Наблюдали ли вы за выполнением испытаний по восстановлению, при которых использовались только материалы, хранящиеся вне основного производственного помещения?				
3. Анализируете ли вы периодически работу вычислительного центра и делаете ли письменные рекомендации по совершенствованию процедур, обеспечения безопасности и контроля?				
4. Требуется ли отделам пользователей сверять выходные данные компьютеров с полученными вручную итогами в целях аудита и обеспечения безопасности?				
5. Сохраняете ли вы тестовые данные, которые обрабатываются системами выплаты денежных средств, чтобы убедиться, что эта обработка дает требуемые результаты?				

СТРАХОВАНИЕ

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Было ли проинформировано руководство вычислительного центра относительно того, что покрывается страхованием?				
2. Предусматривает ли страховой полис покрытие прерывания деятельности?				
3. Имеется ли в организации отдел, ответственный за страховую защиту?				
4. Есть ли у вас экземпляр страхового полиса?				
5. Проводили ли вы анализ страховой защиты в прошлом году?				
6. Проводите ли вы ежегодно анализ вашего страхования со страхователем?				
7. Охватывает ли страховое покрытие аппаратные средства обработки данных и программное обеспечение?				
8. Проводили ли Вы анализ риска или последствий для вычислительного центра?				

РЕЗЕРВНОЕ ПОМЕЩЕНИЕ

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Абонируете ли вы в настоящее время полностью оборудованное резервное помещение?				
2. Расположено ли резервное помещение на таком расстоянии, которое гарантирует, что это помещение не будет затронуто крупномасштабным бедствием?				
3. Обеспечена ли безопасность резервного помещения, по крайней мере настолько же хорошо, как вашего нынешнего помещения?				
4. Использовали ли вы когда-либо резервное помещение при имитации бедствия?				
5. Имеется ли возможность доступа в резервное помещение в течение времени, достаточного для проведения испытаний?				

ВЗАИМНЫЕ СОГЛАШЕНИЯ

	Да	Нет	Выполняется	Ответственный/ Мероприятие
1. Имеете ли вы официальное взаимное соглашение, действующее в настоящее время?				
2. Имеет ли компьютер другой организации достаточно временных ресурсов, чтобы вы могли использовать его совместно с этой организацией?				
3. Имеет ли ваш компьютер организации достаточно временных ресурсов, чтобы другая организация могла использовать его совместно с вашей?				
4. Являются ли обе совместимые компьютерные системы совместимыми?				
5. Имеют ли обе компьютерных системы пропускную способность, достаточную для одновременного функционирования критически важных прикладных систем обеих организаций?				
6. Является ли совместимыми операционные системы?				
7. Сможет ли ваша сеть связи быстро соединяться с компьютерами другой организации и имеется ли достаточно памяти?				
8. Имеет ли вычислительный центр специализированные аппаратные средства типа лазерных принтеров или накопителей на кассетах?				
9. Согласились ли обе организации уведомлять друг друга об изменениях в аппаратных средствах или программном обеспечении?				
10. Будет ваше приобретенное программное обеспечение работать в другом вычислительном центре?				
11. Протестировали ли вы критически важную прикладную систему в другом вычислительном центре?				
12. Имеется ли в другом вычислительном центре временное хранилище для печатных форм?				
13. Имеется ли в другом вычислительном центре временное хранилище вашей библиотеке резервных копий?				
14. Имеется ли в другом вычислительном центре временное офисное помещение для персонала, обеспечивающего эксплуатацию компьютеров?				

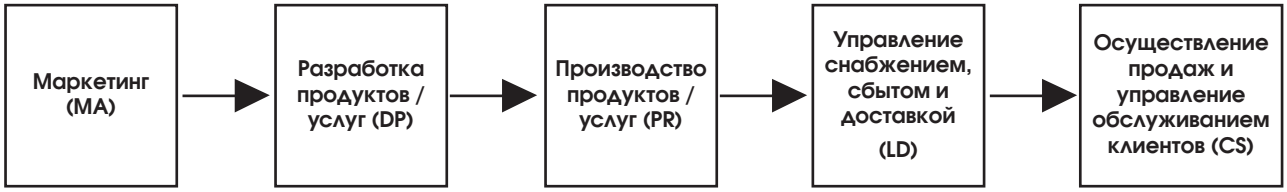
ПРИЛОЖЕНИЕ 1. МЕЖОТРАСЛЕВАЯ КЛАССИФИКАЦИЯ БИЗНЕС-ПРОЦЕССОВ НА ПРЕДПРИЯТИЯХ

Концепция цепочки продуктивных процессов предложена профессором Гарвардской школы бизнеса Майклом Портером и широко используется в области консультационных услуг по совершенствованию деятельности компаний для обеспечения их конкурентоспособности.

Компания Прайс Уотерхаус адаптировала данную концепцию для ее использования в системе KnowledgeViewSM в качестве модели для классификации и структуризации бизнес-процессов и разработала на основе этой концепции «Международный язык бизнеса», который позволяет анализировать и сопоставлять на единой основе процессы в различных сферах деятельности. Этот язык охватывает 9 областей цепочек для отдельных сфер деятельности. Продуктивные процессы непосредственно влияют на продукт или услугу, предоставляемую клиенту.

Данная классификация процессов используется в программе KnowledgeView для структуризации информации о лучших практических методах работы и помогает компаниям проводить мероприятия по повышению эффективности своей деятельности.

ОБЛАСТИ ЦЕПОЧКИ ПРОДУКТИВНЫХ ПРОЦЕССОВ



ОБЛАСТИ ОБЕСПЕЧИВАЮЩИХ ПРОЦЕССОВ

- (BI) Совершенствование деятельности организации
- (EM) Управление защитой окружающей среды
- (EX) Управление внешними связями
- (FA) Управление корпоративными службами/помещениями
- (FM) Управление финансами
- (HR) Управление персоналом
- (LG) Управление юридическими услугами
- (PM) Планирование и управление
- (PO) Снабжение
- (SY) Разработка и сопровождение систем/технологий

ОБЛАСТИ ЦЕПОЧКИ ПРОДУКТИВНЫХ ПРОЦЕССОВ

Маркетинг MA

MA — Изучение клиентов/рынков
MA — Разработка стратегии/планов маркетинга
MA — Управление продуктами/услугами
MA — Задание и регулирование цен
MA — Планирование и управление каналами продаж
MA — Рекламирование и продвижение продуктов/услуг

Разработка продуктов/услуг DP

DP — Исследование продуктов/услуг
DP — Проектирование и разработка продуктов/услуг
DP — Создание и испытание прототипов
DP — Разработка и реализация процессов изготовления
DP — Разработка и реализация процедур обслуживания

Производство продуктов/услуг PR

PR — Разработка и корректировка процедур
PR — Планирование и использование производственных мощностей
PR — Календарное планирование производства
PR — Производство и упаковка продуктов/услуг
PR — Управление техническими изменениями
PR — Управление качеством продуктов/услуг
PR — Выбор, получение, установка оборудования и его техническое обслуживание

Управление снабжением, сбытом и доставкой LD

LD — Управление запасами
LD — Получение материалов/припасов
LD — Поставка продуктов
LD — Установка продуктов, предоставление услуг

Осуществление продаж, управление обслуживанием клиентов CS

CS — Продажа продуктов/услуг
CS — Развитие и поддержание взаимоотношений с клиентами
CS — Ввод и обработка заказов, отслеживание их выполнения
CS — Выставление счетов клиентам
CS — Обработка запросов и предоставление сервисной поддержки клиентам
CS — Обработка жалоб/гарантийных обязательств/ претензий/возвратов
CS — Оценка степени удовлетворенности клиентов

ОБЛАСТИ ОБЕСПЕЧИВАЮЩИХ ПРОЦЕССОВ

Совершенствование деятельности организации BI

BI — Оценка существующей структуры/культуры организации
BI — Проектирование и внедрение новой организационной структуры
BI — Разработка и ведение процесса сопоставительного анализа
BI — Разработка и ведение процесса непрерывного совершенствования деятельности
BI — Разработка и ведение процесса управления знаниями

Управление защитой окружающей среды EM

EM — Обеспечение соблюдения требований постановлений и законов
EM — Формулировка стратегии управления защитой окружающей среды
EM — Реализация программы реагирования на чрезвычайные происшествия
EM — Реализация программы предотвращения загрязнения внешней среды
EM — Управление мероприятиями по восстановлению окружающей среды
EM — Контроль выполнения программы управления защитой окружающей среды
EM — Теоретическое и практическое обучение сотрудников в области защиты окружающей среды

Управление внешними связями EX

EX — Управление отношениями с местным населением и общественностью
EX — Управление отношениями с государственными и регулирующими органами
EX — Управление отношениями с инвесторами
EX — Управление взаимоотношениями с потенциальными финансирующими организациями
EX — Управление отношениями с профсоюзами

Управление корпоративными службами/помещениями FA

FA — Разработка и руководство программой ведения учетных документов
FA — Управление рабочими помещениями и уход за ними
FA — Организационная работа
FA — Планирование и приобретение помещений

Управление финансами FM

FM — Оценка финансовой эффективности и управление ею
FM — Управление наличностью
FM — Управление финансовыми политиками и процедурами
FM — Управление финансовым риском
FM — Управление внутренним аудитом
FM — Управление внутренним контролем
FM — Обработка сбора долгов и управление им
FM — Обеспечение финансирования
FM — Распределение капитала
FM — Закрытие
FM — Учет и контроль затрат
FM — Управление затратами
FM — Учет основных фондов и управление ими
FM — Ведение общего бухгалтерского учета
FM — Выставление внутренних счетов и управление внутриорганизационными расчетами
FM — Планирование, составление бюджета и прогнозирование
FM — Оценка прибыльности
FM — Обработка счетов к получению
FM — Обработка счетов к оплате
FM — Оценка кредитоспособности клиента
FM — Обработка возмещения служебных затрат сотрудникам
FM — Обработка заработной платы
FM — Обработка налогов
FM — Подготовка финансовых отчетов

Управление персоналом HR

HR — Руководство процессом разбора жалоб сотрудников
HR — Разработка программы вознаграждения
HR — Разработка и внедрение системы сбора предложений сотрудников
HR — Управление и руководство предоставлением льгот
HR — Управление обменом информацией среди сотрудников
HR — Планирование и проведение обучения сотрудников
HR — Оценка эффективности труда и вознаграждение за хорошую работу
HR — Набор сотрудников

Управление юридическими услугами LG

LG — Разработка и выполнение программы превентивной юридической грамотности
LG — Обеспечение соблюдения законодательства и инструкций
LG — Управление взаимоотношениями с внешними юрисконсультами
LG — Участие в переговорах и подготовка проектов соглашений/контрактов
LG — Защита интеллектуальной собственности
LG — Предоставление юридических рекомендаций/консультаций
LG — Разрешение конфликтов и участие в судебных процессах

Планирование и управление PM

PM — Разработка плана капиталовложений и инвестиций
PM — Разработка оперативного плана
PM — Разработка стратегического плана
PM — Разработка и ведение плана налогообложения
PM — Разработка и применение систем управления общей эффективностью деятельности организации
PM — Управление программами/проектами
PM — Контроль выполнения и корректировка планов

Снабжение PO

PO — Управление взаимоотношениями с поставщиками и субподрядчиками
PO — Приобретение материалов/припасов
PO — Оценка и выбор поставщиков/субподрядчиков

Разработка и сопровождение систем/технологий SY

SY — Разработка и сопровождение прикладных программ
SY — Разработка, сопровождение и управление системами защиты информации
SY — Оценка, выбор и приобретение технических средств/компьютерных платформ
SY — Оценка, выбор и приобретение пакетов программного обеспечения
SY — Управление ресурсами информационной системы
SY — Планирование развития систем и технологий
SY — Предоставление информационных отчетов

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Овчинникова Г.Ю. *(galya@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
Email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555

Полное или частичное воспроизведение материалов, содержащихся в настоящем издании, допускается только по согласованию с издателем