Администрирование информационных систем

Смирнов Михаил
СПбГУ
2009

- 11.09
- Руст - 28 мая 1987 года

Эффективность и бесперебойность функционирования

- Задачи двух видов:
  - А. Задачи, связанные с выполнением компанией своих функций в соответствии с поставленными целями (задачи обеспечения эффективности);
  - Б. Задачи, связанные с функционированием компании в целом (задачи обеспечения бесперебойности).
- Задачи обеспечения безопасности :
  - 1. Задачи, решение которых допускает полное управление со стороны компании процессами для их достижения;
  - 2. Задачи, процессы решения которых не допускают или частично допускают управление со стороны компании

Безопасность и бесперебойность

	А. Задачи, связанные с выполнением компанией своих функций в соотвествии с поставленными целями	Б. Задачи, связанные с функционированием компании в целом.
1. Задачи, решение котрых допускает полное управление со стороны компании процессами для их достижения	**А.1.** Обеспечение неразглашения состояния клиентских счетов третьим лицам.	**Б.1.** Обеспечение бесперебойного снабжения электроэнергией помещений банка.
2. Задачи, процессы решения которых не допускают или частично допускают управление со стороны компании	**А.2.** Обеспечение сохранности вкладов клиентов (дефолт за счет политических изменений)	**Б.2.** Обеспечение функционирования банка после землетрясения.

Примеры классификации задач обеспечения безопасности банка.

	А. Задачи, связанные с выполнением компанией своих функций в соотвествии с поставленными целями	Б. Задачи, связанные с функционированием компании в целом.
1. Задачи, решение котрых допускает полное управление со стороны компании процессами для их достижения	**А.1.** Предупреждение ситуаций (собственная служба безопасности)	**Б.1.** Парирование ситуации (создание резервного источника питания)
2. Задачи, процессы решения которых не допускают или частично допускают управление со стороны компании	**А.2.** Минимизация потерь от ситуации (создание резервных фондов компенсации потерь клиентов)	**Б.2.** Минимизация потерь от ситуации (создание плана функционирования в условиях стихийного бедствия)

Примеры методов достижения задач обеспечения безопасности банка.

Приоритеты задач

- На первом месте – «Б. Задачи, связанные с функционированием хозяйствующего субъекта в целом.»
- Отсюда – требование бесперебойности работы компании
- В России – не востребовано

Риски	Действия	
	В преддверии 2000 г.	После 11 сентября 2001 г.
Киберугрозы организационным системам	ИТиндустрия создала инструменты для обнаружения и устранения проблемы 2000 (Y2K) в аппаратных и программных средствах. Компании понесли значительные затраты на тестирование, модификацию и замену своих систем	Имеется огромное число технических решений для обеспечения безопасности, но для конкретных применений требуется тщательный отбор. Очень важно отметить, что безопасность людей не менее важна, чем безопасность материальных активов
Коммерческие зависимости и взаимозависимости компаний	Различные объединения промышленных предприятий проводили оценку угроз нарушения логистических цепочек и их последствий. Компании требовали от своих поставщиков подтверждения приведения своих информационных систем в соответствие проблеме 2000	Углубилось осознание компаниями проблем устойчивости логистических цепочек. После 11 сентября компании стали меньше полагаться на пустые склады и поставки «толькововремя» (justintime) и больше на складские запасы «навсякийслучай» (justincase)

Y2K & 11.09 – 1

Киберугрозы критическим инфраструктурам	Владельцы и операторы инфраструктур (телекоммуникационных, трубопроводных и др.) обеспечили решение проблемы 2000 в своих системах, разработали и проверили планы восстановления после бедствия и создали сети сотрудничества для обмена информацией и координации действий в чрезвычайных ситуациях	Между компаниями имеет место очень вялый обмен информацией за исключением отрасли финансовых услуг, где существуют долговременные доверительные отношения, поддерживающие координацию действий в чрезвычайных ситуациях
Нежелание делиться информацией	Конгресс США издал закон, по которому обмен информацией между компаниями по проблеме 2000 не является нарушением антимонопольного законодательства	Сейчас в конгрессе США рассматривается закон об обмене между компаниями антитеррористической информацией, подобный закону по проблеме 2000

Y2K & 11.09 – 2

Атмосфера страха и неопределенности	Предприятия и организации, их объединения организовали в прессе компании убеждения акционеров и публики в том, что последствия проблемы 2000 будут минимальными	Сразу после 11 сентября все компании публично выразили соболезнования родственникам погибших в зданиях ВТЦ
Горизонт планирования	Точная дата проявления проблемы 2000 и определение ее содержания сделали планирование работ по ее решению весьма простым. Инструментарий сократил время решения	Для атак террористов отсутствует определение времени и орудий. Необходимо тщательное исследование рисков, чтобы определить места установки и инструменты защиты от атак террористов

Y2K & 11.09 – 3

Тип прерывателя бизнеса	Английское название прерывателя	Русское название прерывателя
Предпринимательский	Business relocation	Переезд предприятия или организации в другое помещение или офис
	Espionage	Промышленный шпионаж
	Loss of records	Утрата архива
	Mergers & acquisitions	Слияние/приобретение предприятий/организаций
	Negative publicity	Негативная информация о компании в прессе
	IS swop	Переход с ручной на автоматизированную информационную систему или с одной автоматизированной системы на другую
	Mask show	«Маскишоу» — «наезд» криминальных и других структур

Классификация рисков бизнеса -1

Человеческий	Labor disputes	Трудовой конфликт (забастовка, локаут и др.)
	Loss of workforce	Организованный уход сотрудников или их потеря в результате, например, несчастного случая
	Staffing issues	Невозможность набрать сотрудников
	Succession planning	Отсутствие планирования замещения должностей
	The human factor	Человеческий фактор, терроризм в любой форме и любым оружием
	Unauthorized access	Несанкционированный доступ
	White collar crime	Преступления «белых воротничков»
	Workplace violence	Силовые конфликты на рабочих местах

Классификация рисков бизнеса -2

Техногенный	Blackouts	Веерное отключение электроэнергии
	Computer failure	Отказы компьютеров
	Computer hacking	Атаки хакеров
	Computer viruses	Компьютерные вирусы
	Environmental hazards	Аварии систем жизнеобеспечения (прорыв канализации, трубопроводов горячей и холодной воды, отказ воздуховодов и др.)
	Multitenant sites	Бизнесцентр, «населенный» несколькими компаниями
	Power outages	Отключение электроэнергии
	Sick building syndrome	Синдром здания, построенного из материалов с примесью опасных для здоровья компонентов
	Transportation disruptions	Нарушения работы общественного транспорта

Классификация рисков бизнеса -3

Природный	Blizzards	Снежная буря
	Earthquakes	Землетрясение
	Electrical storms	Электромагнитные бури
	Hurricanes	Ураганы
	Tornadoes	Торнадо
	Winter weather	Зимняя погода
Природно-техногенный	Biological hazards	Эпидемии
	Fire	Огонь
	Flooding	Наводнение
	Artificial and natural objects landing	Падение искусственных (например, самолетов) и природных (например, метеоритов) объектов с неба

Классификация рисков бизнеса -4

В России

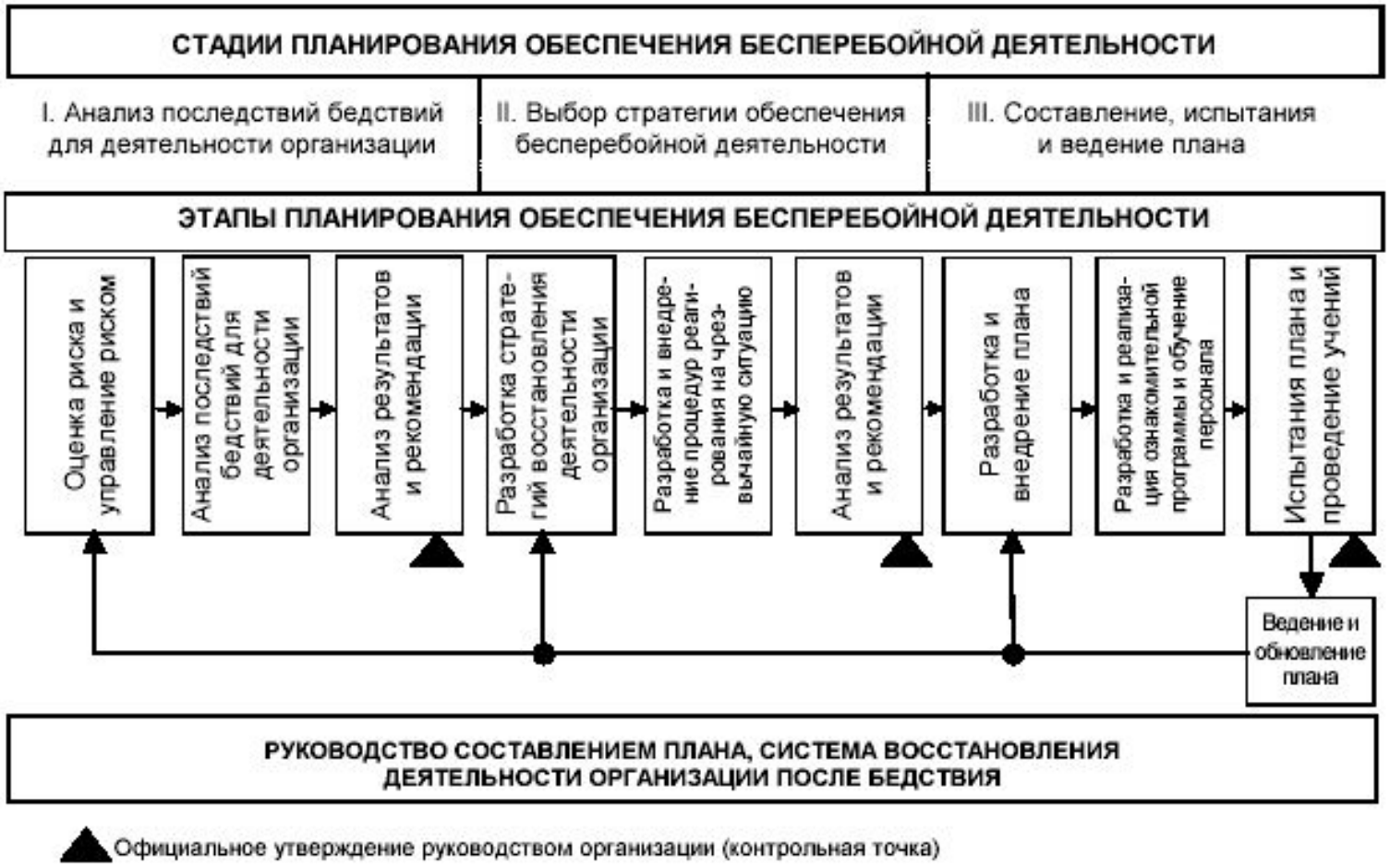
- 67% опрошенных ею российских компаний имеют планы обеспечения непрерывности бизнеса (Business Continuity Plans)
  - У 61,2% этих компаний планы протестированы,
  - у 38,8% — нет.
- Речь про информационную безопасность

Тип ЧС	Параметры ЧС				Силы и средства, осуществляющие ликвидацию ЧС
	Число пострадавших, чел. (L	Число лиц, условия жизнедеятельности которых нарушены, чел. (M)	Материальный ущерб, тыс. мин. размеров оплаты труда на день ЧС (N)	Зона ЧС	
Локальная	L<=10	M<=100	N<=1	Не выходит за пределы территории объекта производственного или социального назначения	Организации
Местная	10<L<=50	100<M<=300	1<N<=5	Не выходит за пределы населенного пункта, города, района	Органы местного самоуправления

Классификация чрезвычайных ситуаций (ЧС) природного и техногенного характера 1

Территориальная	50<L<500	300<M<500	5<N<500K	Не выходит за пределы субъекта РФ	Органы исполнительной власти субъекта РФ
Региональная	50<L<=500	500<M<=1000	500K<N<=5000K	Не выходит за пределы территории двух субъектов РФ	Органы исполнительной власти двух субъектов РФ
Федеральная	L>500	M>1000	N>5000K	Выходит за пределы территории двух субъектов РФ	Органы исполнительной власти субъектов РФ, оказавшихся в зоне ЧС
Трансграничная	не определено	не определено	не определено	Выходит за пределы РФ, либо ЧС произошли за рубежом и затрагивает территорию РФ	По решению Правительства РФ в соответствии с нормами международного права и международными договорами РФ
Примечание: K = 1000.					

Классификация чрезвычайных ситуаций (ЧС) природного и техногенного характера 2



Методология планирования бесперебойной деятельности организации в случае бедствий

- выбор хорошо структурированной и всеобъемлющей методологии оценки бизнес-процессов и разработки плана;
- разработка прагматичного, экономичного и работоспособного плана, который обеспечит бесперебойность критически важных процессов в случае серьезного нарушения деятельности организации;
- минимизация последствий любого бедствия для организации.

Цели проекта по составлению плана, обеспечивающего бесперебойность и восстановление деятельности организации в случае бедствий