Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 11 (186)/2008

Этюды об управлении непрерывностью бизнеса

(часть 2)

КОРПОРАТИВНЫЙ МЕНЕДЖМЕНТ

Этюды об управлении непрерывностью бизнеса (часть 2)

Константин Мусатов,
инженер-проектировщик в Группе консалтинга

СОДЕРЖАНИЕ

Введение

Внедрение управленческого процесса в организации можно условно разделить на два этапа. Первый — этап творческий, когда создается что-то новое, еще неизвестное. И второй — этап рутинный, когда активное созидание сменяется кропотливой работой по поддержанию в работоспособном состоянии всего того, что было создано на первом этапе. В журнале JetInfo, № 7(182), 2008, были даны комментарии к двум разделам британского стандарта BS 29999-2: «Планирование системы управления непрерывностью бизнеса» и «Внедрение и эксплуатация СУНБ». Эти разделы относятся к первому «творческому» этапу. Материал данного номера содержит комментарии к двум другим разделам того же стандарта «Мониторинг и анализ СУНБ» и «Сопровождение и совершенствование СУНБ», которые в большей степени посвящены регулярно повторяемым штатным действиям. Однако подобные характеристики нисколько не умаляют важности подобных действий для обеспечения непрерывности бизнеса организации.

Комментарии ко второй части стандарта «BS 25999: Управление непрерывностью бизнеса. Спецификации» (часть 2)

Мониторинг и анализ СУНБ

Главной задачей выполнения мониторинга и анализа СУНБ является обеспечение руководства компании объективной и полной информацией о работоспособности и эффективности СУНБ. На ее основе руководство организации может оценить адекватность политики непрерывности бизнеса, скорректировать цели и рамки обеспечения непрерывности бизнеса, а также определить, какие действия по корректировке и улучшению необходимо выполнить. Можно выделить три способа проверки эффективности СУНБ силами самой организации:

1) самооценка, т.е. попытка посмотреть на разработанные процедуры и документы самими разработчиками. Требования стандарта, относящиеся к данному способу, перечислены в разделе стандарта «Сопровождение и анализ мер по УНБ», комментарии к ним были даны в журнале JetInfo, № 7(182) 2008;
2) проведение внутреннего аудита, т.е. привлечение к аудиту представителей службы внутреннего аудита. Комментарии к требованиям стандарта, относящиеся к данному способу, даны ниже в разделе «Внутренний аудит»;
3) управленческий пересмотр, т.е. анализ проделанной работы руководителями организации. Комментарии к требованиям стандарта, относящиеся к данному способу, даны ниже в разделе «Анализ СУНБ со стороны руководства».

Раздел 5.1. Внутренний аудит
Раздел 5.2. Анализ СУНБ со стороны руководства
Раздел 5.2.1 Общие положения
Раздел 5.2.2. Входные данные для анализа
Раздел 5.2.3. Выходные данные анализа

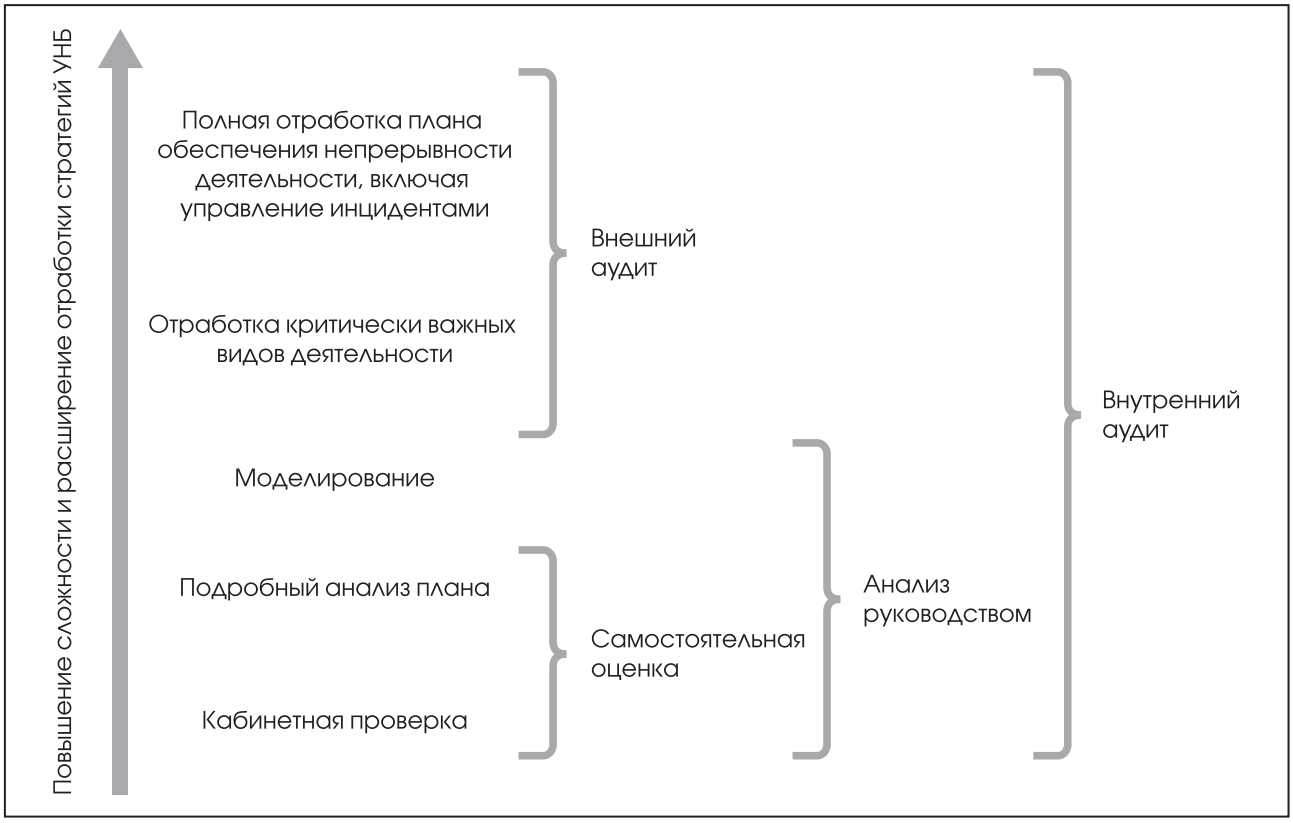

Рис. 1. Иерархия методов мониторинга и анализа СУНБ

Комментарии к разделу 5.1 стандарта BS 25999-2

Данный раздел посвящен проведению проверок СУНБ силами подразделения внутреннего аудита организации.

Комментарии к разделу 5.1.1 стандарта BS 25999-2

1. В данном разделе перечисляются предъявляемые к внутренним аудиторским проверкам требования и цели, для достижения которых организации должны их проводить.
2. В стандарте отмечается, что данные проверки должны проводиться на регулярной основе.
3. В результате проведения внутренней аудиторской проверки должно быть определено, соответствует ли действующая система управления непрерывностью тем мерам, которые были запланированы, т.е. соответствует ли зафиксированное на бумаге суровой действительности.
4. Внутренняя аудиторская проверка должна оценить правильно ли СУНБ реализована и поддерживается в рабочем состоянии СУНБ.
5. По результатам внутренней аудиторской проверки должно быть сделано заключение о том, соответствует ли СУНБ целям, заявленным в политике УНБ организации.
6. Наконец, конечной целью всякого внутреннего аудита вообще и аудита СУНБ в частности является доведение результатов проверки до сведения высшего руководства организации.

Комментарии к разделу 5.1.2 стандарта BS 25999-2

1. Программа внутреннего аудита, как и любой другой процесс в организации имеет свой жизненный цикл, который описывается циклом Деминга: планирование — внедрение — реализация — поддержка[1]. Все этапы этого цикла должны основываться по крайней мере на следующей информации:
   - анализ воздействия на бизнес — нужен для определения того, действительно ли СУНБ обеспечивает непрерывность наиболее критичных бизнес-процессов;
   - анализ рисков — нужен для определения того, от каких рисков действительно обеспечивает защиту СУНБ;
   - меры контроля и превентивные меры — нужны для определения того, делается ли все возможное для предотвращения наступления ЧС и насколько эффективна система контроля СУНБ;
   - результаты предыдущих проверок — нужны для подтверждения того, что замеченные в ходе предыдущих аудиторских проверок, самостоятельных оценок и проверок СУНБ со стороны руководства недостатки были устранены.

Комментарии к разделу 5.1.3 стандарта BS 25999-2

1. В данном разделе перечислены вопросы, ответы на которые должно содержать описание процедуры проведения аудиторских проверок. Это описание используется на всех этапах, начиная с введения ее в действие и заканчивая поддержанием процедуры в актуальном состоянии.
2. В описании процедуры необходимо указать распределение зон ответственности при планировании, проведении проверок и составлении итоговых отчетов. Планирование и управление непрерывностью бизнеса включает в себя элементы многих дисциплин и один человек редко может в одиночку квалифицированно оценить все аспекты деятельности организации. Поэтому часто в аудиторской проверке СУНБ участвует группа специалистов и зоны ответственности каждого должна быть четко определена заранее.
3. В описании процедуры необходимо указать уровень квалификации персонала, осуществляющего проверку. Это особенно важно, если проведением подобных проверок будет заниматься сотрудник, незнакомый с процессом УНБ, например, внутренний финансовый аудитор.
4. В описании процедуры необходимо указать дополнительные требования, предъявляемые к планированию, проведению проверок и составлению итоговых отчетов.
5. В описании процедуры должны быть указаны критерии успешности прохождения проверки. Для этого необходимо четко сформулировать цели ее проведения. Ими могут быть, например:
   - соответствие законодательным или нормативным актам, требованиям стандартов или внутренним регламентам организации;
   - определение состояния дел перед началом или в ходе реализации проекта по внедрению СУНБ в организации;

1 Описание цикла Деминга приведено в журнале JetInfo, № 7(182) 2008.

- проверка осуществимости проекта по внедрению СУНБ в организации. Можно порекомендовать каждой организации осуществлять подобную проверку, когда она только собирается приступить к реализации широкомасштабного проекта в области УНБ;
- всестороннее исследование деятельности компании с целью определения целесообразности вступления в те или иные взаимоотношения с контрагентами (due diligence) или с целью достижения каких-либо других стратегических целей организации, составной частью которых является процесс УНБ;
- юридические действия, такие как предоставление вещественных доказательств, подтверждение соответствия планов реальным событиям и т.п.

6. В описании процедуры должны быть указаны рамки проверки. На практике подобное мероприятие часто воспринимается лишь как проверка состояния ИТ-инфраструктуры. Чтобы избежать подобного упрощенческого отношения, в описывающем рамки проверки документе необходимо в явном виде указать управленческие вопросы, которые будут рассмотрены. Такими вопросами могут быть определение бизнес-рисков или изучение уровня потенциальной ответственности организации в различных ситуациях.
7. В описании процедуры должна быть указана регулярность проведения проверки. В стандарте ничего не говорится о том, насколько часто следует проводить аудит, поэтому организация вправе сама выбирать их частоту, но, как правило, они проводятся не реже одного раза в год.
8. В описании процедуры должны быть указаны методы проведения проверки. Как видно на рис. 1 внутренняя аудиторская проверка может использовать самый широкий спектр этих методов, которые были подробно описаны в журнале JetInfo, № 7(182) 2008.

Комментарии к разделу 5.1.4 стандарта BS 25999-2

1. Данный раздел стандарта содержит требования, которые предъявляются к выбору аудиторов и порядку проведения аудиторских проверок. С одной стороны, внутренняя аудиторская проверка СУНБ является лишь частным случаем аудиторской проверки и поэтому должна отвечать тем же принципам, что и любая другая аудиторская проверка, а именно:

- во время проверки поведение аудиторов должно быть этичным;
- предоставление результатов должно быть справедливым;
- в течение всей проверки должно проявляться профессиональное внимание;
- процесс аудита должен быть независимым, что служит основой беспристрастности и объективности заключений;
- аудит должен базироваться исключительно на свидетельствах.

С другой стороны, в самом стандарте подчеркивается лишь обязательность объективности и беспристрастности при проведении проверки.

Комментарии к разделу 5.2 стандарта BS 25999-2

Данный раздел посвящен второму способу проведения проверок СУНБ, а именно анализу системы управления непрерывностью бизнеса руководством организации.

Комментарии к разделу 5.2.1 стандарта BS 25999-2

1. В стандарте подчеркивается, что руководство должно на регулярной основе проводить анализ СУНБ организации даже в том случае, если никаких значительных изменений не происходит. Однако в реальной жизни организации постоянно меняются. Появляются новые направления деятельности, происходят слияния и поглощения, применяются новые технологии. Каждое подобное изменение должно быть соответствующим образом отражено в СУНБ, как в индивидуальных планах непрерывности деятельности, так и в стратегических документах, таких, как политика непрерывности деятельности. Актуальность, адекватность и эффективность этих изменений должна быть проанализирована руководством.
2. Главной задачей участия руководства в этом анализе является, конечно, не просто одобрение или неодобрение внесенных изменений и выполненных работ, а поиск возможностей дальнейшего улучшения СУНБ. Именно руководство, а не исполнители или аудиторы, обладая всей полнотой информации об организации и зная ее стратегические цели, может предложить такие усовершенствования, которые не могут быть предложены рядовыми сотрудниками.

3. Естественным является требование стандарта документировать ход проведения анализа и полученные результаты.
4. Все, записанное во время проведения анализа, получает статус записи, поэтому подпадает под действие законодательства о хранении записей организации, включая сроки хранения, условия хранения и уничтожения, требования к неизменности.

Комментарии к разделу 5.2.2 стандарта BS 25999-2

1. Для того, чтобы сделанные выводы были максимально полезны при проведении пересмотра высшее руководство организации должно рассматривать не только саму систему УНБ, но и привлечь как можно больше дополнительных материалов. Данный раздел целиком посвящен перечислению тех данных, которые руководству организации следует использовать при проведении анализа.
2. Руководство организации должно учитывать результаты предыдущих аудиторских проверок. Если это предусмотрено в договорах или если это позволяет уровень доверительности взаимоотношений, руководители должны учитывать результаты аналогичных проверок у поставщиков и партнеров, предоставляющих услуги аутсорсинга.
3. С системой УНБ помимо сотрудников организации тем или иным образом взаимодействует множество людей, среди которых клиенты, контролирующие органы, аудиторы и другие заинтересованные стороны. Их замечания могут оказать неоценимую помощь, поскольку отражают взгляд на систему со стороны. Руководству организации следует предпринять усилия по сбору подобных отзывов о работе СУНБ и использовать эти отзывы при проведении анализа.
4. Вместе с совершенствованием законодательной базы и технологий развивается и управление непрерывностью бизнеса. Появляются новые программные продукты и интернет-услуги, облегчающие поддержание СУНБ в актуальном состоянии, методические рекомендации и стандарты, повышающие эффективность СУНБ. Сотрудники, ответственные за работу СУНБ, обязаны собирать информацию обо всех подобных изменениях и предоставлять собранную информацию руководству при проведении анализа.
5. Для обеспечения непрерывности деятельности используются действия двух типов — корректирующие и превентивные. Реализация и тех, и других, как правило, занимает длительное время, поэтому при проведении анализа высшему руководству следует принять во внимание их текущий статус. В следующем разделе эти действия будут рассмотрены более подробно.
6. Даже самая совершенная СУНБ не может свести к нулю вероятность реализации угроз. Кроме того, некоторые угрозы (например, разрушительное землетрясение в Москве) могут считаться настолько маловероятными, что риски их реализации расцениваются как приемлемые. Эти уровни остаточного и приемлемого риска должны быть приняты во внимание при проведении анализа. В организациях с достаточно высоким уровнем зрелости процессов управления обычно существует документ Политика или Положение по управлению рисками, который содержит перечень таких рисков. В случае его существования этот документ обязательно должен учитываться при проведении анализа высшим руководством.
7. Помимо изменений во внешнем мире в самой организации также регулярно происходят значительные перемены, например, обнаруживаются новые уязвимости, расширяется список угроз, в случае реализации которых может потребоваться обеспечивать непрерывность бизнеса. Возможна и такая ситуация, когда ряд угроз был ранее сознательно оставлен вне рамок проекта по построению СУНБ компании и только руководители организации могут принять решение о том, что наступило время расширить рамки проекта и включить в них эти угрозы.
8. Трудно представить ситуацию, в которой по результатам анализа не было бы выявлено никаких недостатков. Для их устранения замеченных недостатков разрабатывается соответствующий план действий. Чтобы этот план не остался лишь на бумаге, при проведении последующего анализа руководители организации должны не забыть проверить ход реализации ранее намеченных шагов.
9. Для проведения анализа руководителям организации должна быть предоставлена исчерпывающая информация обо всех рекомендациях по улучшению, полученных с момента проведения предыдущего анализа. Эти рекомендации могут поступать из множества источников, таких, как: клиенты, внешние аудиторы, новые нормативные документы, отраслевые, государственные,

международные стандарты, договорные обязательства и др.

10. В настоящее время в свободном доступе есть большое количество информации, посвященной методам обеспечения непрерывности деятельности. Среди англоязычных ресурсов можно указать сайт Британского института непрерывности бизнеса (Business Continuity Institute) http://www.thebci.org/ и портал Continuity Central http://www.continuitycentral.com/. Из русскоязычных ресурсов стоит назвать сайт «Управление Непрерывностью Бизнеса в России» http://www.bcp.ru/. Представленные на этих ресурсах материалы позволят всегда быть в курсе последних новостей в области УНБ и помогут применить лучшие практики для обеспечения непрерывности деятельности любой организации. При проведении анализа СУНБ руководителям организации полезно ознакомиться с представленными там материалами.
11. В первой части стандарта BS 25999 неоднократно подчеркивалась необходимость достаточного уровня квалификации персонала, ответственного за внедрение и поддержание СУНБ. Для достижения требуемого уровня квалификации соответствующие сотрудники проходят обучение и участвуют в тренингах. При проведении анализа СУНБ руководители организации должны проверить результаты прошедшего обучения и дать ответы на такие вопросы, как:
    - достаточен ли теперь уровень компетентности обучавшихся сотрудников?
    - нужно ли направить в программу обучения дополнительных сотрудников?
    - соответствует ли программа обучения стоящим перед сотрудниками задачам?
12. В первой части стандарта BS 25999 неоднократно подчеркивалась важность проведения тестирования всех элементов СУНБ, в т.ч. путем проведения учений различного масштаба. Уроки, извлеченные из применения мер УНБ на практике, всегда более ценны, чем теоретические знания. При проведении анализа СУНБ руководителям организации должна быть предоставлена исчерпывающая информация о проводившихся учениях и мерах по совершенствованию СУНБ, которые были предприняты по результатам этих учений.
13. Еще более ценную информацию о состоянии СУНБ, чем проведение учений, дает устранение последствий реальных инцидентов. Поэтому аналогично ситуации с учениями при проведении анализа СУНБ руководителям организации должна быть предоставлена исчерпывающая информация об имевших место инцидентах, предпринятых мерах реагирования и извлеченных уроках.
14. Наконец, стоит отметить, что ни в каком самом подробном документе не может быть предусмотрено все многообразие событий, которые способны оказать влияние на СУНБ. Для проведения анализа руководители вправе запрашивать любую другую информацию, которая, по их мнению, имеет отношение к совершенствованию СУНБ.

Комментарии к разделу 5.2.3 стандарта BS 25999-2

1. Анализ СУНБ высшим руководством имеет очень большое значение. Не случайно в первом международном стандарте ISO 22399:2007, посвященном управлению непрерывностью операционной деятельности, этот анализ выделен в отдельный этап процесса УНБ (см. рис. 2, стр. 8).
   Такое большое значение придается участию руководителей по вполне понятной причине. Выводы, которые они сделают, и решения, которые они примут, имеют огромное значение для дальнейшей судьбы СУНБ и могут радикально изменить ход ее развития. Данный раздел стандарта целиком посвящен перечислению тех решений, которые руководство организации может принять по результатам проведения анализа.
2. По результатам проведенного пересмотра руководством организации может быть принято решение о расширении рамок СУНБ, т.е. рассмотрении тех бизнес-процессов, которые ранее оставались за рамками СУНБ. Это закономерный процесс, так как наиболее безопасный подход к построению СУНБ заключается в построении системы для какого-нибудь одного бизнес-процесса и последующем постепенном включении в нее все новых и новых бизнес-процессов организации. Случаи сужения рамок на практике встречаются чрезвычайно редко.
3. Проведенный руководством организации анализ должен приводить к повышению эффективности СУНБ. В качестве примера принятых решений и намеченных действий, связанных с ее повышением, можно указать такие, которые позволят:
    - уменьшить количество нарушений в работе, причины которых не установлены или не устранены;

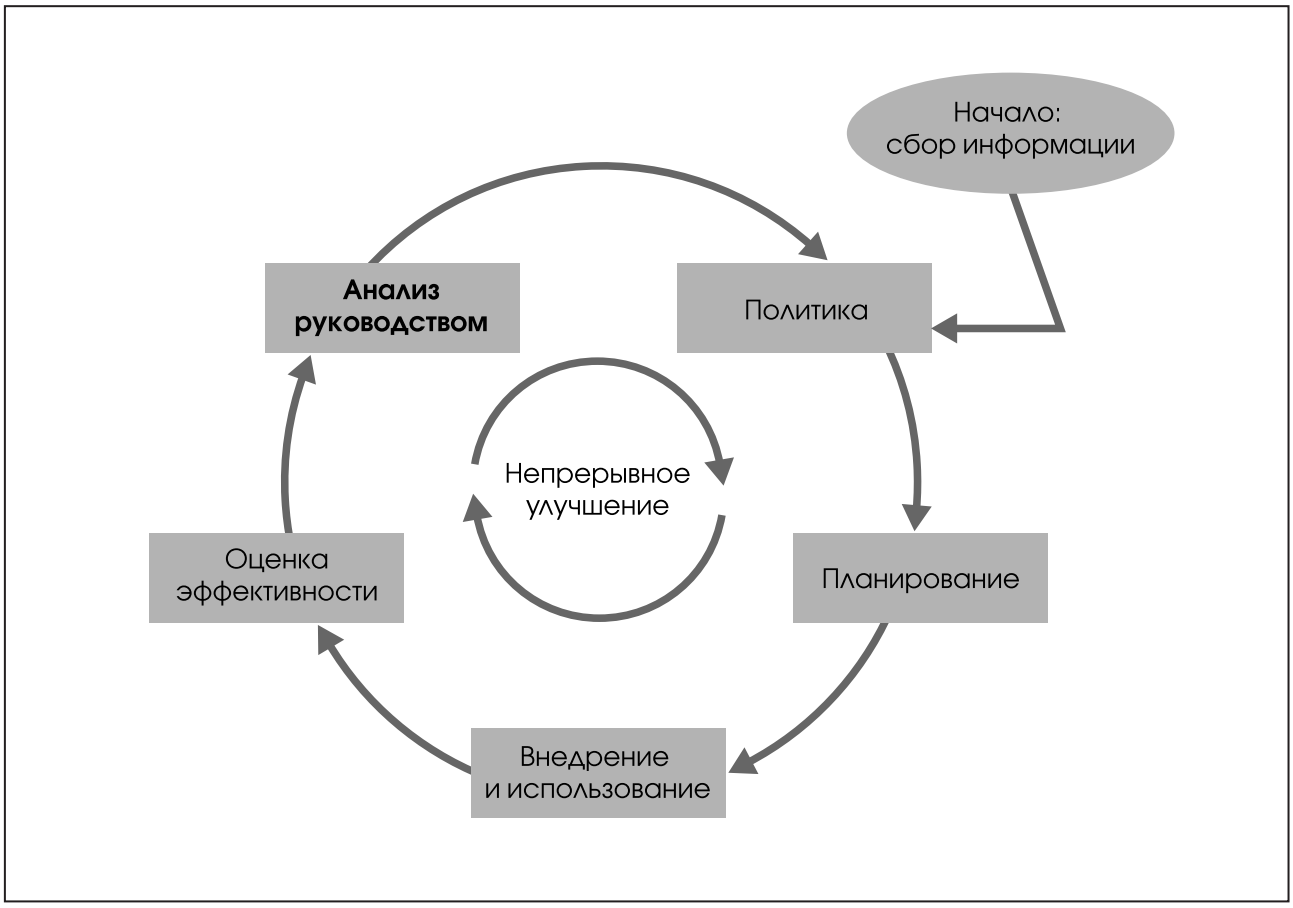

Рис. 2. Важная роль анализа СУНБ высшим руководством организации в соответствии со стандартом ISO 22399:2007

- уменьшить продолжительность прерываний бизнес-процессов;
- уменьшить размер ущерба от прерывания бизнес-сервисов;
- сократить время, которое проходит с момента изменений в организации до момента отражения этих изменений в планах;
- сократить время обнаружения инцидента и принятия решения об активации плана обеспечения непрерывности деятельности;
- сократить время, требующееся для возвращения в штатный режим работы после выполнения плана обеспечения непрерывности деятельности;
- расширить список реализованных превентивных мер;
- ускорить внедрение новых элементов СУНБ, упущенных из внимания;
- повысить качество обучения сотрудников процессу УНБ;
- увеличить частоту проведения тестирования СУНБ.

4. В процессе проведения анализа на руководство организации ложится важная роль по донесению до ответственных за создание и поддержание стратегии и процедур УНБ сотрудников требований бизнеса, которые вытекают из новых стратегических целей, стоящих перед организацией. В ряде случаев представителям бизнес- и поддерживающих подразделений бывает непросто найти общий язык. В таких случаях именно руководство организации должно принять окончательное решение о том, каким именно образом следует модифицировать СУНБ.
5. При проведении анализа руководители организации должны принять во внимание изменения в требованиях, предъявляемых к устойчивости деятельности организации. Это может быть особенно важно для тех организаций, от своевременного предоставления услуг которых может зависеть человеческая жизнь, например, услуг телекоммуникационной связи.
6. Наступление определенных событий как внутри, так и вовне организации может приводить к необходимости изменить корпоративные бизнес-процессы. А поскольку изменение бизнес-процессов обычно ведет к ужесточению бизнес-требований к обеспе-

чению их непрерывности, эти изменения также должны быть отражены в результатах анализа СУНБ.

7. Руководство организации при проведении анализа должно обратить внимание на соответствие существующей СУНБ требованиям новых законодательных и нормативных актов и контрактных обязательств. В качестве примера можно привести Указание от 5 марта 2009 г. N 2194-У «О внесении изменений в положение Банка России от 16 декабря 2003 года 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах». Если до принятия этого Указания многие кредитные организации ограничивались созданием плана обеспечения непрерывности своей ИТ-инфраструктуры, то после его принятия все эти документы предстоит модифицировать для достижения гораздо более широкого круга целей, таких, как:
   - поддержание способности кредитной организации выполнять принятые на себя обязательства перед вкладчиками и кредиторами, в том числе перед Банком России (по кредитам Банка России, уплате процентов по ним и другим денежным обязательствам перед Банком России);
   - предупреждение и предотвращение возможного нарушения режима повседневного функционирования кредитной организации;
   - снижение тяжести последствий нарушения режима повседневного функционирования кредитной организации (в том числе размера материальных потерь, потерь информации, потери деловой репутации);
   - сохранение уровня управления кредитной организацией, позволяющего обеспечить условия для принятия обоснованных и оптимальных управленческих решений, их своевременную и полную реализацию;
   - обеспечение способности кредитной организации осуществлять расчеты в соответствии с принятыми на себя обязательствами, в том числе по кредитам Банка России, процентам по ним и другим денежным обязательствам перед Банком России;
   - обеспечение информационной безопасности кредитной организации, в том числе ее расчетной системы;
   - обеспечение благоприятных условий труда и безопасности служащих кредитной организации, безопасности лиц, находящихся в помещениях (посетителей) кредитной организации.
8. Одним из решений, которые может принять лишь высшее руководство организации, является определение уровня остаточных рисков, которые сохраняются даже после реализации СУНБ. Принятие решения о снижении уровня остаточных рисков автоматически будет означать дополнительные расходы на более надежные и, как правило, более дорогостоящие превентивные меры и меры реагирования. Еще один параметр — уровень приемлемого риска — также может быть указан лишь руководителями организации, поскольку он описывает так называемый риск-аппетит, т.е тот уровень риска, при котором они все еще чувствуют себя комфортно. Снижение этого уровня обычно означает расширение рамок СУНБ, т.е. рассмотрение ряда рисков, которые ранее не рассматривались либо из-за незначительности ущерба, либо из-за очень малой вероятности реализации.
9. Существует целый класс решений, которые могут быть приняты только руководителями организации по результатам проведения анализа СУНБ. Эти решения касаются выделения дополнительных материальных и людских ресурсов.
10. Наконец, последним в списке, но не по значению, в стандарте упоминаются принятые по результатам анализа решения, касающиеся финансового и бюджетного обеспечения СУНБ.

Сопровождение и совершенствование СУНБ

Данный раздел посвящен вопросам функционирования и развития СУНБ. В процессе функционирования системы может возникнуть ситуация, в которой возникает угроза или происходит нарушение каких-либо нормативных, законодательных или других требований. Для предотвращения этой угрозы или устранения последствий ее реализации в организации выполняются соответствующие меры — превентивные или корректирующие. Требования стандарта, относящиеся к этим мерам, представлены в разделе 6.2. Внедрение в СУНБ этих мер для предотвращения случаев повторного нарушения служит одним из побудительных мотивов совершенствования СУНБ. Другие побудительные мотивы описаны в разделе 6.3.

Раздел 6.1. Превентивные и корректирующие меры
Раздел 6.1.1. Общие положения
Раздел 6.1.2. Превентивные меры

Раздел 6.1.3. Корректирующие меры
Раздел 6.2 Непрерывное совершенствование

Комментарии к разделу 6.1 стандарта BS 25999-2

Данный раздел посвящен мерам, которые организация должна предпринять, чтобы предотвратить нарушение нормативных, законодательных или других требований или устранить последствия такого нарушения, если оно все-таки произошло.

Комментарии к разделу 6.1.1 стандарта BS 25999-2

1. Практические шаги по совершенствованию СУНБ имеют вид превентивных или корректирующих действий. В данном подразделе описываются требования общего характера, предъявляемые к подобным шагам.
2. Соответствие реализуемых превентивных или корректирующих действий масштабу решаемых проблем всегда является непростой задачей. Например, для устранения выявленного в ходе внутреннего аудита недостаточного уровня компетенции сотрудников, который будет недостаточным для выполнения своих функций в условиях ЧС, можно предпринять широкий круг превентивных мер, начиная с покупки дополнительной литературы (чего, как правило, не достаточно), заканчивая приемом на постоянную работу профессиональных консультантов в этой области (что может быть чрезмерной мерой).
3. Превентивные и корректирующие действия должны не только эффективно устранять возникшую проблему, но и соответствовать таким документам, как политика непрерывности бизнеса.
4. Реализация превентивных и корректирующих действий не должна происходить спонтанно, т.к. вместе с устранением одной проблемы это может привести к развалу всей СУНБ, когда процедуры, записанные в планах, не могут быть выполнены в результате выполненных мер. По этой причине в стандарте выдвигается требование обязательного документирования всех изменений и соответствующей модификации планов обеспечения непрерывности деятельности.

Комментарии к разделу 6.1.2 стандарта BS 25999-2

1. Превентивными мерами являются действия, которые заблаговременно предпринимаются с целью недопущения нарушения требований законодательных и нормативных актов, контролирующих органов, договорных обязательств и т.п. В организации должен существовать документ, содержащий описание процедуры выполнения превентивных мер. В данном подразделе перечислены требования, которые должны содержаться в этой процедуре.
2. Процедура реализации превентивных мер должна содержать требования к выявлению потенциальных несоответствий и их последствий, т.е. описывать критерии, по которым может быть выявлено потенциальное нарушение законодательства.
3. Процедура реализации превентивных мер должна описывать то, каким образом определяется нужное превентивное действие. Кроме того, в процедуре могут быть указаны отдельные требования, относящиеся к порядку выполнения превентивной меры.
4. Как и при выполнении любых других действий в рамках СУНБ, к выполнению превентивных действий относится требование протоколировать результаты выполненного действия. Данные протоколы являются записями, которые подтверждают выполнение работ по совершенствованию СУНБ, а также служат источником информации для проведения последующего анализа.
5. Протоколирование результатов является очень важным шагом, который служит для решения нескольких задач. Одной из этих задач является проведение анализа выполненной превентивной меры. Выполнение анализа необходимо для совершенствования СУНБ организации.
6. Помимо нарушений законодательных требований процедура выполнения превентивных действий должна содержать критерии выявления изменившихся рисков. Эти критерии должны отвечать на вопрос, не упущены ли из внимания какие-либо важные риски.
7. Само по себе выполнение превентивных мер порой бывает необходимым, но недостаточным для обеспечения непрерывной деятельности. Информация о выявленном потенциальном нарушении законодательных требований и реализованных превентивных мерах должна быть доведена до всех заинтересованных сторон, возможно, даже за пределами организации. По этой причине в процедуре выполнения превентивных мер должно быть указано, каким образом можно убедиться в том, что информация доведена до всех, кто в ней нуждается.

8. Наконец, превентивных мер может быть несколько. В этом случае может потребоваться вводить приоритеты их выполнения. Эти приоритеты должны быть обоснованы с точки зрения анализа рисков, анализа влияния на бизнес и других факторов, например, доступности ресурсов. В процедуре выполнения превентивных мер должны быть указаны требования, в соответствии с которыми выстраивается эта система приоритетов.

Комментарии к разделу 6.1.3 стандарта BS 25999-2

1. Корректирующими мерами являются действия, которые выполняются с целью уменьшения последствий разнообразных нарушений, связанных с реализацией и функционированием СУНБ, и предотвращения повторения подобных нарушений в будущем. Аналогично ситуации с превентивными мерами в организации должен существовать документ, содержащий описание процедуры выполнения корректирующих мер. В данном подразделе перечислены требования, которые должны содержаться в этой процедуре.
2. Процедура выполнения корректирующих действий должна содержать критерии, отслеживание которых позволит выявить случаи нарушений.
3. Помимо задачи обнаружения нарушений процедура выполнения корректирующих действий должна содержать критерии, которые позволят выявить причины произошедших нарушений.
4. После выяснения причин процедура выполнения корректирующих действий должна содержать критерии, позволяющие сделать заключение о необходимости выполнения дополнительных действий, которые обеспечат невозможность повторного нарушения в будущем.
5. В описании процедуры выполнения корректирующих действий должно быть подробно описано, каким образом определяется корректирующее действие, требуемое в данной ситуации. Здесь же, в случае необходимости, излагаются требования, предъявляемые к ходу выполнения выбранного действия.
6. Так же как и в случае превентивных мер, процедура выполнения корректирующих действий должна содержать требования к протоколированию результатов выполненного. Данные протоколы являются в глазах проверяющих свидетельством выполнения работ по совершенствованию СУНБ, а также источником информации для проведения последующего анализа.
7. Наконец, процедура реализация корректирующих мер должна содержать требования к проведению анализа выполненного корректирующего действия. На основе этого совершенствуются как корректирующие действия, так и вся СУНБ в целом.

Комментарии к разделу 6.2 стандарта BS 25999-2

1. Данный раздел стандарта подчеркивает важность постоянного повышения эффективности СУНБ организации. Для этой цели следует использовать все инструменты, перечисленные в стандарте:
   - пересмотр политики и целей непрерывности деятельности;
   - аудиторские проверки;
   - анализ превентивных и корректирующих действий;
   - анализ СУНБ со стороны руководства.
2. К этому надо добавить, совершенствование СУНБ включает в себя не только написание документов и тренировку команд, но и изменение атмосферы в организации, когда сотрудники организации чувствуют свою вовлеченность в процесс УНБ, не сопротивляются изменениям, а принимают участие в их реализации. Этого можно достигнуть с помощью таких мер, как:
   - награждение лучших в области УНБ (здесь ценна не столько награда, сколько возникновение духа соревновательности);
   - введение в организации специальной символики;
   - учреждение специальных корпоративных ритуалов;
   - активный пример со стороны высшего руководства;
   - популяризация достижений, выпуск специального информационного листка, распространение историй успеха.
3. Следует заметить, что процесс управления непрерывностью деятельности организации не ограничивается СУНБ и тесно связан со множеством других управленческих процессов и процедур внутри организации. Ниже перечислены те из них, интеграция которых с процессом УНБ является абсолютно необходимой:
   - политика безопасности, включая физическую и информационную;

- управление проектами;
- процедуры репликации данных;
- кризис-менеджемент;
- инцидент-менеджмент;
- политики удаленного доступа к ресурсам организации;
- программа обучения персонала;
- процедуры эскалации и оповещения;
- взаимодействие со страховыми компаниями;
- взаимодействие с государственными, муниципальными и проверяющими органами;
- политика управления изменениями. На этом пункте хочется остановиться подробнее. Для поддержания актуальности планов обеспечения непрерывности в организации должна существовать политика управления изменениями, которая охватывает все происходящие и планируемые изменения операционной деятельности. В организации должна быть разработана и внедрена методология, которая позволит при изменении любого приложения, вычислительного оборудования или любого другого ресурса, участвующего в производственной деятельности, гарантировать, что все резервные копии данных, вычислительные или другие ресурсы обновлены соответствующим образом. Кроме того, если в промышленную эксплуатацию вводится новая система, в результате чего появляется новое оборудование, новые требования к производительности и т.д., руководители должны убедиться, что и планы обеспечения непрерывности деятельности изменены соответствующим образом. Политика управления изменениями не должна вносить значительных задержек в процесс их внедрения, однако, это не отменяет необходимости ведения их мониторинга и документирования.

Заключение

На этом комментирование содержательной части британского стандарта BS 25999-2:2007 можно считать завершенным. В двух номерах журнала JetInfo, № 7(182), 2008, и №11(186), 2008 описаны все этапы планирования, реализации и совершенствования процесса управления непрерывностью бизнеса. Важность и сложность этого процесса заслуживает большого внимания, а его реализация требует много сил, времени, настойчивости и дает немалый простор для творчества. Ранее я сетовал на то, что в России вопросу обеспечения непрерывности деятельности не уделяется должного внимания. Но ситуация меняется очень быстро. За время, прошедшее между выпусками этих двух номеров, банковская отрасль обрела если не полноценный стандарт, то весьма емкий и конкретный документ Указание ЦБ РФ от 5 марта 2009 г. N 2194-У «О внесении изменений в положение Банка России от 16 декабря 2003 года 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах». Кроме того, очень активно идет работа и в тех странах, которые считаются лидерами в области УНБ. Новые документы регулярно появляются в США, Великобритании. Вскоре после BS 25999 свет увидел первый международный стандарт ISO 22399. Думаю, что вскоре и российская законодательная база, относящаяся к УНБ, значительно расширится, что значительно облегчит работу по обеспечению непрерывности деятельности организации.

Список литературы

1. Британский стандарт «BS 25999-2:2007: Управление непрерывностью бизнеса. Часть 2: Спецификация» (перевод на русский язык ООО «Глобалтраст солюшинс».
2. Publicity Available Specification ISO/PAS 22399 Societal security — Guidelines for incident preparedness and operational continuity management.
3. Указание ЦБ РФ от 5 марта 2009 г. N 2194-У «О внесении изменений в положение Банка России от 16 декабря 2003 года 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах».
4. Auditing Business Continuity. Global Best Practices by Rolf von Roessing, 2002.
5. Business Continuity Management. A crisis management approach by Dominic Elliott, Ethne Swartz and Brahim Herbane.
6. HB 292-2006 A Practitioners Guide to Business Continuity Management.
7. Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента (ISO 19011:2002).
8. Federal Financial Institutions Examination Council. Business Continuity Planning. IT Examination Handbook. March 2008

НАШИ ПРОЕКТЫ

Внедрение стратегии обеспечения непрерывности бизнеса в ОАО «ВымпелКом» значительно снизило объем возможных финансовых потерь

Темпы развития бизнеса ведущего российского оператора мобильной связи ОАО «ВымпелКом» определяли и развитие вычислительного центра компании, однако, со временем стало ясно, что одного ВЦ уже не достаточно. При увеличении числа абонентов за два года с 10 млн до 52 млн московский ВЦ оставался единой точкой отказа. В тесном сотрудничестве с компаниями Symantec Consulting и «Инфосистемы Джет» «ВымпелКом» реализовал масштабную стратегию обеспечения непрерывности бизнеса и послеаварийного восстановления с применением широкого спектра инструментов Symantec. Это один из крупнейших проектов подобного рода в мире, его реализация позволила ОАО «ВымпелКом» снизить уровень рисков для бизнеса, защитить активы и минимизировать последствия аварий.

В России, Украине, Казахстане, Таджикистане и Узбекистане «ВымпелКом» работает под торговой маркой «Билайн» (Beeline). Два года назад у компании было около 10 млн абонентов. Сегодня их число превысило 50 млн. После открытия филиалов в Украине, Таджикистане и Узбекистане операционная выручка компании за 12 месяцев увеличилась на 50%: с $590 млн до $890 млн.

Лицензии группы компаний «ВымпелКом» на предоставление услуг сотовой связи охватывают территорию, на которой проживает около 240 млн человек. Сюда входят — 78 регионов России с населением в 136,5 млн человек (что соответствует 94% населения России), а также вся территория Казахстана, Украины, Таджикистана, Узбекистана, Грузии и Армении.

Однако столь впечатляющие успехи сопровождались растущими технологическими трудностями. Пока «ВымпелКом» активно расширял зону покрытия сети, его технические службы были сосредоточены главным образом в московском вычислительном центре, который оставался единой точкой отказа. В случае аварии в ВЦ «ВымпелКом» мог мгновенно потерять контакт с 52 млн абонентов, что поставило бы под угрозу само существование компании.

Дмитрий Устюжанин, руководитель департамента информационной безопасности ОАО «ВымпелКом» комментирует: «*Мы реализовали очень эффективную, хорошо управляемую и централизованную ИТ-стратегию, направленную на развитие бизнеса компании. Она стала нашим конкурентным преимуществом, но в области обеспечения непрерывности бизнеса и послеаварийного восстановления оставалась довольно слабой. Основная проблема заключалась в том, что у нас был единственный вычислительный центр, и в случае аварии мы могли потерять контроль над бизнесом».*

Разработка эффективной и всеобъемлющей стратегии обеспечения непрерывности бизнеса не только устранила бы технологические проблемы в системе предоставления услуг клиентам, но и позволила бы сделать весь бизнес более надежным, доступным и качественным. «Зависимость бизнеса от доступности ИТ-инфраструктуры настолько велика, что без специальных и очень серьезных мер как технического, так и организационного характера возможности развития компании были бы под угрозой» — заявил директор по ИТ-инфраструктуре ОАО «ВымпелКом» Сергей Шилин.

Первые шаги проекта

Катализатором преобразований стала авария, произошедшая в офисе главного партнера «ВымпелКома» по системной интеграции — компании «Инфосистемы Джет». В ее вычислительном центре возник пожар, и хотя все данные удалось восстановить без потерь, это событие обнажило проблему уязвимости любой высокотехнологичной компании к нештатным ситуациям. Последствия пожара сняли на видео, и эту запись продемонстрировали руководству «ВымпелКома».

Рассказывает Владимир Филиппов, вице-президент по ИТ «ВымпелКома»: «*Этот фильм, наряду с оценками возможных потерь в случае, если подобное произойдет в нашем центре обработки данных, наглядно продемонстрировал, насколько критична физическая защита данных и отказоустойчивость ИТ-инфраструктуры. Ведь в такой компании, как «ВымпелКом», даже небольшой перерыв в работе может нанести бренду серьезный ущерб. В результате было принято решение приступить к* разработке мер по обеспечению *непрерывности бизнеса и строить резервный центр обработки и хранения данных».*

В «ВымпелКоме» задумались над проблемой сохранения работоспособности в случае чрезвычайной ситуации — началось рассмотрение предложений компаний, предоставляющих консалтинговые услуги по обеспечению непрерывности бизнеса. Виталий Задорожный, начальник отдела непрерывности бизнеса «ВымпелКома», объясняет, почему для разработки программы обеспечения непрерывности бизнеса были выбраны компании Symantec Consulting и «Инфосистемы Джет».

«Для проекта требовались наилучший опыт, реалистичный подход и высокая квалификация, — говорит он. — *Специалисты «Инфосистем Джет» глубоко знали ИТ-инфраструктуру наших вычислительных центров, а консультанты Symantec четко поняли наши задачи и, используя системный подход, предложили признанную на мировом уровне методологию. В результате с нами работала команда специалистов с богатым практическим опытом внедрения систем обеспечения непрерывности бизнеса как на техническом, так и на организационном уровне: специалисты Symantec разработали методики и планы, соответствующие международным стандартам, а специалисты компании «Инфосистемы Джет» разработали и внедрили технические решения, обеспечивающие их выполнение».*

Эффективный план обеспечения непрерывности бизнеса

Специалисты Symantec Consulting в тесном сотрудничестве с командой «Инфосистемы Джет» вели работы по двум направлениям. С одной стороны, велось проектирование, разработка и внедрение физической ИТ-инфраструктуры. С другой — создавался всеобъемлющий план обеспечения непрерывности бизнеса.

«Запускать процесс легко, когда бизнес созрел для этого. А момент осознания критичности обеспечения непрерывности бизнеса уже наступил для нашей компании. Проектная команда специалистов компаний Symantec и «Инфосистемы Джет» демонстрировала свое превосходное знание предмета на каждом этапе реализации проекта, — говорит В. Филиппов. — *Она провела тщательный анализ влияния чрезвычайных ситуаций на работу «ВымпелКома», изучила возникающие у нас риски, оценила используемые технологические решения и предложила варианты их модернизации. Все решения строились с учетом наших потребностей».*

Одним из главных выводов, сделанных на этапе определения стратегии, стало осознание необходимости построения в Москве резервного вычислительного центра. «*В основном вычислительном центре работают около 300 RISC-серверов Sun Microsystems, объединенных сетью хранения данных с дисковыми массивами. В этой среде емкостью более 300 ТБайт работает большинство основных приложений «ВымпелКома», включая такие критически важные, как системы самообслуживания клиентов, биллинга и управления взаимоотношениями с клиентами и партнерами»*, — комментирует директор ИТ-инфраструктуры ОАО «ВымпелКом» Сергей Шилин.

С помощью Veritas NetBackup™ Enterprise Edition создаются резервные копии данных на магнитных лентах, которые хранятся в резервном ВЦ. Система Veritas Storage Foundation™ for Oracle, в состав которой входит Veritas Cluster Server™, обслуживает кластер серверов «активный-активный» для обеспечения сверхвысокого уровня готовности.

«Прозрачное» восстановление после отказа

Недавно непрерывность предоставления услуг подверглась испытанию. Из-за отказа межсетевого экрана в одном из вычислительных центров возникла проблема с доступом в Интернет. При отсутствии резервного ВЦ это стало бы серьезной аварией. Под угрозу ставилась способность компании гарантировать на территории нескольких часовых поясов непрерывность предоставления таких услуг, как поддержка самообслуживания клиентов и кассовых терминалов партнеров по розничным продажам. В новой инфраструктуре проблема осталась незамеченной за пределами вычислительного центра: обслуживание было просто передано в резервный ВЦ. Частью стратегии обеспечения непрерывности бизнеса является проведение тщательного анализа влияния чрезвычайной ситуации на бизнес (Business Impact Analysis, BIA). В ходе его проведения все приложения «ВымпелКома» были разбиты по степени важности на четыре класса, каждый со своими требованиями к объемам восстановленных данных (Recovery Point Objective, RPO) и срокам восстановления (Recovery Time Objective, RTO). Способ репликации данных теперь зависит от того, чем измеряется время восстановления: минутами, часами или — в некоторых случаях — днями. Для обеспечения антикризисного управления в Symantec Consulting для персонала «ВымпелКома» разработаны практические процедуры, тренинги и подготовлена документация. Внедрение решения по обеспечению непрерывности бизнеса дало заметный экономический эффект. Углублен-

Краткий обзор решения

Потребности бизнеса
- Снижение финансовых потерь в случае чрезвычайной ситуации.
- Восстановление предоставления бизнес-услуг в согласованное время при наступлении чрезвычайной ситуации.

Технологические задачи
- Создание масштабируемой, высокопроизводительной и гибкой инфраструктуры.
- Защита от локальных и широкомасштабных проблем, способных вызвать длительный перерыв в работе компании.
- Разработка процессов и процедур, а также подготовка документации по преодолению критических ситуаций в ИТ-инфраструктуре.

Решение
- Разработка и внедрение стратегии обеспечения непрерывности предоставления ИТ-услуг.
- Разработка и внедрение стратегии обеспечения непрерывности бизнеса.

Продукты Symantec
- Veritas NetBackup™ Enterprise Edition;
- Veritas Storage Foundation™ for Oracle;
- Veritas Cluster Server™;
- Veritas CommandCentral™.

Технологическая среда
- Два вычислительных центра в Москве;
- До 300 RISC-серверов Sun Microsystems, подключенных через сеть хранения данных к дисковым массивам среднего и высшего уровня;
- Емкость производственной среды: более 300 Тбайт;
- Критически важные приложения: система самообслуживания клиентов, биллинг, управление взаимоотношениями с партнерами и клиентами;
- В рамках программы были также установлены системы пожаротушения, средства контроля физического доступа, источники бесперебойного питания (UPS), подсистема мониторинга климатических условий в серверных помещениях.

Услуги Symantec
- Услуги по разработке стратегии обеспечения непрерывности бизнеса и планов послеаварийного восстановления ВЦ.

Услуги «Инфосистемы Джет»
- Услуги по сбору и обработке информации;
- Разработка, проектирование, внедрение и тестирование технических решений.

Партнер Symantec
- «Инфосистемы Джет»

ный анализ рисков показал, что решение по обеспечению непрерывности бизнеса значительно снизило объем возможных финансовых потерь «ВымпелКома». Согласно независимому исследованию, серьезная авария или прекращение обслуживания может серьезно сказаться на оценке стоимости бренда «Билайн». Из этого можно заключить, что решение, реализованное специалистами Symantec и «Инфосистемы Джет», существенно снизило ущерб бренду «Билайн». «*Хочется отметить, что во время нашей совместной работы консультанты компаний Symantec и «Инфосистемы Джет» продемонстрировали высокий профессионализм и нацеленность на достижение конкретного результата,* — сказал г-н Устюжанин, — *На каждом этапе разработки программы обеспечения непрерывности бизнеса они объясняли, какие имеются риски, какова вероятная экономия и какими могут быть убытки, если этап не будет реализован. Можно сказать, что мы говорили на одном языке».*

Экономические выводы и технические преимущества

Снижение риска
- Значительное снижение объема возможных финансовых потерь. Снижение ущерба бренду «Билайн» в случае наступления чрезвычайных ситуаций.

Готовность
- Обеспечен постоянный, бесперебойный доступ к данным и услугам.
- Снижена частота и продолжительность простоев компонентов ИТ-инфрастуктуры.

Производительность
- Разработаны эффективные планы восстановления для процессов, приложений, данных и компонентов ИТ-инфраструктуры.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Редактор: Слободчикова Т.А. *(slobodchikova@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555