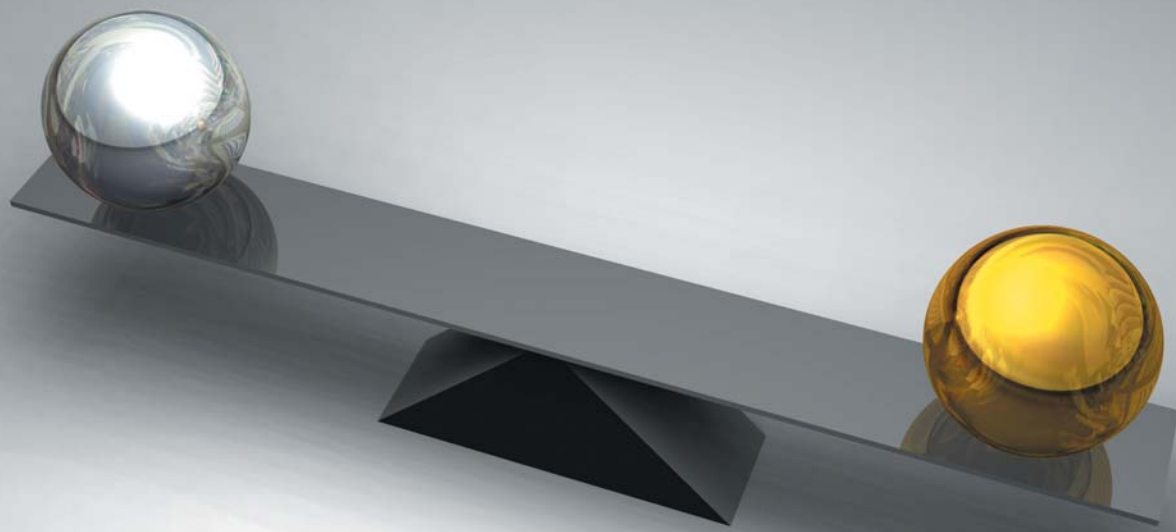
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 10 (197)/2009

Непрерывность бизнеса. Подходы к использованию нового Указания ЦБ РФ 2194-У: поиск «золотой середины»



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Непрерывность бизнеса. Подходы к использованию нового Указания ЦБ РФ 2194-У: поиск «золотой середины»

СОДЕРЖАНИЕ

Первое в России внедрение решения SAP CRM для банков

В Уральском федеральном округе УБРиР является крупнейшим кредитным учреждением, постоянно улучшает предоставляемые услуги и уделяет большое внимание повышению лояльности клиентов. Руководство банка приняло решение усовершенствовать бизнес-процессы управления взаимоотношениями с клиентами, создав единую систему розничных продаж на платформе SAP. Партнером по реализации проекта была выбрана компания «Инфосистемы Джет».

На момент начала проекта УБРиР использовал несколько автоматизированных банковских систем, в каждой из которых велась своя база клиентов. Кроме того, Банк уже имел разветвленную сеть филиалов с локальными клиентскими базами. На первом этапе проекта специалисты компании «Инфосистемы Джет» создали единую базу клиентов (ЕБК), где была консолидирована информация обо всех клиентах Банка. Для этого были определены и настроены структуры для хранения информации о клиентах и их взаимоотношениях между собой, а также правила контроля информации при вводе и редактировании карточки клиентов. Специалисты компании «Инфосистемы Джет» создали модуль очистки данных, загружаемых из внешних источников. Эта функциональность, помимо обеспечения корректности атрибутов клиента Банка и его адресной информации, позволяет производить выявление и обработку дублирования записей о клиенте. Модуль интеграции обеспечил синхронизацию информации о деловых партнерах Банка со всеми автоматизированными банковскими системами.

В ходе первого этапа проекта была решена задача интеграции общероссийского справочника адресов (классификатор адресов России – КЛАДР) в SAP CRM. Сотрудники компании «Инфосистемы Джет» разработали и реализовали уникальное для российского рынка решение, которое позволяет загружать и обновлять справочник адресов SAP CRM, используя КЛАДР.

Следующим этапом проекта стала организация решения «Единое место продаж» (ЕМП). Ранее сотрудник Банка при обработке запросов клиента в зависимости от выполняемой операции был вынужден работать с различными банковскими приложениями, что существенно увеличивало время обслуживания клиентов. Поэтому было принято решение создать единое рабочее место сотрудника фронт-зоны, позволяющее с помощью унифицированного интерфейса производить все необходимые для обслуживания клиентов операции.

ЕМП позволяет выполнять полный набор операций по обслуживанию физических лиц от открытия вклада до перевыпуска пластиковой карты. Оператор в рамках одной системы видит всю необходимую информацию о клиенте: его данные, историю обслуживания, счета, заявки, договоры. Под управлением интерактивных сценариев сотрудник Банка может правильно выстроить диалог с клиентом, выявить его потребности, предложить новые продукты и услуги, получить необходимую для выполнения операций информацию.

Кроме того, решение «Единое место продаж» позволяет Банку минимизировать затраты на проведение дорогостоящих тренингов для своих сотрудников: в случае ввода нового банковского продукта или маркетинговой программы ИТ-служба Банка по заказу бизнес-подразделений настраивает новый сценарий, и работа продолжается в привычном режиме.

С целью проведения анализа финансовых результатов и подготовки аналитической информации для принятия управленческих решений консультантами российского представительства SAP было внедрено хранилище данных на платформе SAP BW. Специалисты компании «Инфосистемы Джет» организовали поступление в него данных из SAP CRM, обеспечили их правильное хранение, помогли в создании ряда аналитических отчетов.

Завершающим этапом построения цикла взаимодействия с клиентом стало внедрение модуля «Маркетинг» и его настройка. В результате у маркетологов УБРиР появился инструмент для анализа и сегментации клиентской базы, планирования, настройки и проведения маркетинговых кампаний. Благодаря этому была оптимизирована система регистрации отклика клиента на маркетинговые сообщения, а также процедура предложения специалистами фронт-офиса других услуг Банка. Маркетинговые кампании стали более адресными, эффективными и менее затратными.

Первый в России проект по борьбе с нелегальной терминацией трафика в телефонных сетях фиксированной связи

В конце октября 2009 года в ОАО «Северо-Западный Телеком» были завершены работы по проверке корректности маршрутов терминации входящих международных и междугородных вызовов (МН/МГ-трафика) на сети связи Петербургского и Мурманского филиалов. Обследование телефонной сети ОАО «СЗТ» на предмет корректности терминации трафика осуществляла российская компания «Инфосистемы Джет».

В основе методики компании «Инфосистемы Джет» для обнаружения некорректной терминации[1] трафика лежит следующий способ тестирования: осуществление большого количества тестовых звонков из различных точек России, СНГ и дальнего зарубежья, совершаемых как с сетей фиксированной и мобильной телефонии, так и через VoIP-провайдеров. В рамках проекта в ОАО «СЗТ» в общей сложности было сделано более 20 000 звонков из более 300 сетей 56 стран.

По завершении тестирования экспертами компании «Инфосистемы Джет» были собраны и при помощи специализированного программного продукта Interconnect Bypass Detection проанализированы протоколы состоявшихся тестовых соединений. В результате был сформирован детальный отчет о маршруте каждого тестового звонка. Это позволило выявить более 20 точек некорректной терминации, через которые на сеть ОАО «СЗТ» направлялись существенные объемы входящих МН/МГ-вызовов под видом местных звонков, что является нарушением порядка пропуска трафика, регламентированного условиями действующих договоров о присоединении.

Проводимые работы позволят ОАО «СЗТ» обеспечивать контроль за легальностью терминации трафика на свою сеть, так как при этом достигается более высокое качество связи, более понятными и прозрачными становятся взаиморасчеты с присоединенными операторами. Корректное приземление МН/МГ-трафика на сеть ОАО «СЗТ» может дать компании дополнительный доход в сотни миллионов рублей в год.

Внимание: на экране Z-2!

Компания «Инфосистемы Джет» выпустила новую версию сертифицированного межсетевого экрана Z-2 — одной из немногих российских разработок, сертифицированной по самым высоким классам защиты, которая функционирует под самой современной операционной системой компании Sun Microsystems — Solaris 10.

Новая версия межсетевого экрана претерпела значительные изменения как в функциональности, так и во внутренней архитектуре продукта. В ней оптимизированы интерфейсы управления, средства кластеризации и обеспечения отказоустойчивости. Кроме того, включена поддержка многопроцессорных и многоядерных конфигураций, позволяющих работать на гигабитных скоростях.

Собственная разработка компании «Инфосистемы Джет» прошла сертификацию ФСТЭК России. Продукт сертифицировался по требованиям безопасности для межсетевых экранов и отсутствию недекларированных возможностей — программных закладок, позволяющих нарушить конфиденциальность, доступность или целостность обрабатываемой информации. Результаты испытаний подтвердили соответствие Z-2 очень высоким классам защиты: второму классу защиты для межсетевых экранов и второму уровню контроля недекларированных возможностей. Это одни из самых высоких показателей на российском рынке, большинство отечественных разработок сертифицированы по более низким классам защиты.

Выданный сертификат ФСТЭК России позволяет использовать межсетевой экран Z-2 в самых серьезных системах и решениях, в том числе для защиты информационных систем, в которых обрабатываются сведения, составляющие государственную тайну, для защиты персональных данных до класса К1 (наивысший класс защиты для персональных данных, под который подпадают информационные системы с количеством субъектов более 100 000, содержащие информацию о расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья).

1 Некорректная терминация — завершение звонков на сеть оператора связи, выполненное с нарушением действующих нормативно-правовых актов, договорных отношений между операторами связи и/или экономических интересов оператора.

ТЕМА НОМЕРА

Непрерывность бизнеса. Подходы к использованию нового Указания ЦБ РФ 2194-У: поиск «золотой середины»

Мария Акатьева,
старший консультант в группе систем менеджмента ИБ и НБ
Центра информационной безопасности, компания «Инфосистемы Джет»

«Избежать катастрофы может только тот, кто считает ее возможной».

Швебель Вильгельм,
немецкий ученый и публицист

В марте 2009 года Центральный Банк России выпустил указание № 2194 «О внесении изменений в Положение Банка России от 16 декабря 2003 года № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах». Выход нового указания послужил причиной появления множества вопросов относительно необходимости и глубины внесения изменений в уже имеющуюся документацию в части внутреннего контроля и управления непрерывностью бизнеса (НБ) кредитных организаций, которая требовались ранее в Положении 242-П.

Изменения и рекомендации, которые отражены в 2194-У, преследуют цель обеспечения большей устойчивости финансовой структуры России, призывают к пониманию финансовых функций, которые лежат на каждой конкретной кредитной организации как составной части единой финансовой системы. Центральный Банк сделал шаг на пути развития идеи о защите финансовой системы страны от воздействия чрезвычайных ситуаций крупномасштабного характера, которые наименее предсказуемы, но могут повлечь за собой невосполнимый ущерб.

Выход любого положения вызывает резонанс среди компаний по поводу достижения соответствия новым требованиям. Можно соответствовать формально, а можно построить действительно полезную и рабочую систему обеспечения непрерывности бизнеса в случае ЧС.

Еще недавно в подобных ситуациях большинство организаций интересовало формальное соответствие требованиям, чтобы иметь «правильно составленные бумаги» для регулирующего органа. Однако сейчас наступает то время, когда многие банки и другие кредитные организации сами, помимо обязательных требований ЦБ, приходят к осознанию реальной пользы от систем обеспечения непрерывности деятельности, когда точно спланированные действия в случае ЧС действительно снижают потери и убытки, когда правильно проведенный анализ рисков позволяет наиболее оптимально распорядиться вложениями в системы жизнеобеспечения организаций.

Сам факт выхода новых рекомендаций, изложенных в 2194-У, является отражением естественной «эволюции» понимания высокой значимости обеспечения непрерывности бизнеса в корпоративной культуре нашей страны.

Пример последствий ЧС

Май 2005 г, Москва — Отключение ЭЭ в Москве и ближайших регионах на несколько часов оставило более 2 млн. человек без ЭЭ.
12 января 2009 г, С-П — энергетический коллапс на подстанции «Южная», более 30 тыс. человек остались без света и горячей воды.

Однако до сих пор нет единого понимая относительно рекомендации Приложения 2194-У по структуре и содержанию Плана действий, направленных на обеспечение непрерывности деятельности кредитных организаций.

Данная статья посвящена наиболее распространенным вопросам, которые нередко возникают в связи с введенным указанием, а также поиску «золотой середины»: как достичь формального соответствия рекомендациям ЦБ РФ и фактически обеспечить непрерывность ключевых бизнес-процессов кредитных организаций, как экономно распорядиться ресурсами для достижения соответствия рекомендациям 2194-У и получить реальную пользу для бизнеса от проведенного проекта.

Статья подробно рассказывает об изменениях, которые были внесены в требования Указания № 2194 относительно Положения № 242-П, раскрывает само понятие непрерывности бизнеса с точки зрения документации ЦБ РФ, задачи, поставленные перед кредитной организацией, в свете введенных изменений, возможные сложности, которые эти изменения вызвали, а также самые распространенные несоответствия Указанию 2194-У, выделенные специалистами компании «Инфосистемы Джет», исходя из опыта работы с организациями.

Способы решения сложившейся ситуации описаны в контексте подходов, выработанных компанией «Инфосистемы Джет», к разработке и внедрению Планов ОНиВД.

В рамках каждого подхода будут раскрыты вопросы управления НД, учитывая специфику ведения бизнеса крупных компаний и более мелких организаций, а также особенности, на которые следует обращать внимание при проведении подобного рода проектов.

Зачастую компании, в случае необходимости соответствовать требованиям и рекомендациям, преследуют две цели: формально подготовить документацию для возможных проверок и вынести максимально возможную пользу из проделанной работы именно с точки зрения бизнеса организации.

Исследование в области непрерывности бизнеса, проведенное Техасским университетом, представило следующую статистику:

- 85% организаций **сильно или полностью** зависят от вычислительных систем.
- В среднем **на 6-й день перерыва в работе** компания теряет 25% ежедневного дохода, а **на 25-й день** — 40%.
- Спустя две недели после прекращения работы вычислительных систем у 75% компаний **потеря функционирования** становится **критической или полной**.
- 43% компаний, испытавших бедствие и не имевших плана обеспечения бесперебойного функционирования, **не возобновляют свою деятельность**, а спустя два года продолжает функционировать лишь 10% компаний.
- По оценке, **потери доходов** группы организаций, у которых есть План НБ, были бы **в 2,5 раза выше**, если бы при возникновении чрезвычайной ситуации они не привели в исполнение соответствующие планы.

Изменения, которые вносит в требования Указание № 2194 относительно Положения № 242-П

Первоначально, для понимания области, с которой предстоит работать, раскроем суть изменений, внесенных Указанием № 2194-У.

В соответствии с Положением № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» кредитная организация должна осуществлять внутренний контроль для того, чтобы обеспечить надлежащий уровень надежности в соответствии с характером и масштабом проводимых операций. Данное По-

Пример последствий ЧС

10 мая 2009 г — взрыв газопровода в г. Москва на Озерной улице (средний возраст трубопровода около 40 лет).

С начала 2009 года — в г. Москва было уже 7 крупномасштабных пожаров.

ложение предъявляет требования ЦБ РФ в целом к системе внутреннего контроля, к органам внутреннего контроля и непосредственно к службе внутреннего контроля.

Положение включает в себя документы отчетности, которые должны быть в обязательном порядке включены в состав годового отчета ЦБ РФ. В состав отчетных документов должен также входить План действий кредитной организации в случае возникновения непредвиденных ситуаций (п. 9 Форма N 0409639).

По прогнозам МЧС на 2009-2010 годы

На начало пожароопасного периода прогнозируется превышение среднемноголетних параметров пожарной обстановки (количество очагов, площадь ландшафтных пожаров) на территории Дальневосточного (Приморский, Хабаровский края, Амурская область, Еврейская АО), Сибирского (Алтайский, Забайкальский, Красноярский края, Иркутская, Кемеровская, Новосибирская, Омская, Томская области, Республика Алтай, Бурятия, Тыва, Хакасия), Уральского округов.

Какие положения должен содержать данный План действий, было приведено в 2194-У. Указание 2194-У содержит в себе не только изменения относительно требований Положения № 242-П, но и рекомендации по разработке Планов обеспечения непрерывности и восстановления деятельности в случаях чрезвычайных ситуаций.

Изменения, отраженные в 2194-У, можно разделить на две группы:

1. Технические изменения формулировок, в которых упоминается ответственный сотрудник (структурное подразделение) по ПОД/ФТ (ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»).
2. Изменения-дополнения к требованиям по обеспечению непрерывности деятельности и (или) восстановления деятельности, нарушенной в результате непредвиденных обстоятельств.

Пример последствий ЧС

12 марта 2007 — из-за просадки грунта был прорван трубопровод, произошел разлив дизельного топлива в Нижнем Новгороде.

Основные изменения технического характера коснулись следующих пунктов Положения Банка России № 242-П:

- п. 2.2.2 — относительно ответственного лица кредитной организации, которое осуществляет внутренний контроль;
- Приложение 1: абзац 4 — изменения в рекомендациях по осуществлению контроля со стороны органов управления за организацией деятельности Компании;
- п. 3.7 — изменение формулировок Планов действий на случай ЧС;
- п. 4.4.3 — изменение формулировок Планов действий на случай ЧС;
- Приложения 2 — дополнено содержание п. 15.

Технические изменения не требуют пересмотра порядка проведения внутреннего контроля. А вот изменения, которые изложены в Приложении 5 2194-У, носят существенный характер и по сути отражают концепцию обеспечения непрерывности деятельности бизнес-процессов кредитных организаций.

Задачи, поставленные перед кредитной организацией, в свете изменений, изложенных в 2194-У

Изменения, изложенные в 2194-У, ложатся в основу постановки задач внутри кредитной организации. Для того, чтобы учесть в работе своей организации новые рекомендации ЦБ, нужно предпринять следующие действия. Если в организации уже есть планы ОНиВД, соответствующие требованиям 242-П, то их необходимо пересмотреть и улучшить с учетом новых рекомендаций. Если в компании Планов ОНиВД нет, то Планы придется разработать с учетом допустимых затрат на минимизацию операционного риска. Уже на этапе постановки подобных задач в организациях возникают различные сложности с планированием и реализацией работ по обеспечению непрерывности бизнеса.

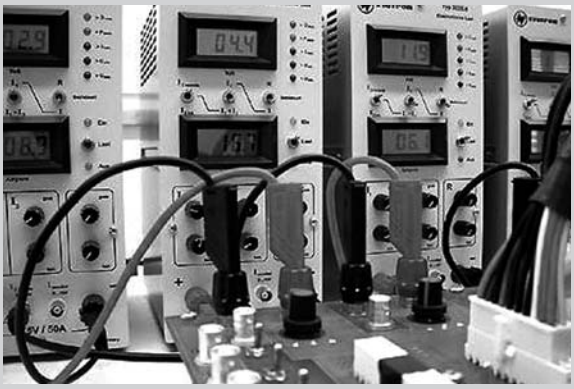
Сложности для Кредитной Организации на пути реализации задач по НБ

Одной из наиболее распространенных сложностей является общее непонимание, что в себя включает само понятие «**обеспечение непрерывности и восстановления деятельности».** Эта сложность является корнем других нерешенных вопросов, таких как:

- Какие несоответствия рекомендациям 2194-У есть в уже имеющейся документации?
- Какие шаги нужно сделать, чтобы разработать Планы ОНиВД, удовлетворяющие требованиям ЦБ (иначе говоря, какова методика разработки подобного рода Планов)? Что из себя представляют сами Планы ОНиВД? Кто в Организации должен быть ответственным за поддержание и развитие Планов ОНиВД?
- Какие дополнительные нормативные документы следует учитывать при разработке и модернизации Планов ОНиВД?
- Каким образом внедрять эти Планы в своей организации?

Наши специалисты по опыту работы с кредитными организациями нашли пути решения этих сложностей в зависимости от размера организации и готовности средств для обеспечения непрерывности своего бизнеса, поскольку подход, применимый для крупных компаний, может быть неудобен и даже невозможен в реализации для среднего и мелкого бизнеса.

Далее я постараюсь внести ясность в понятие непрерывности бизнеса с точки зрения 2194-У и дать ответ на эти сложные вопросы.



Пример последствий ЧС

8 мая 2006, Сбой в Citibank — 275 тыс. ошибочных операций.

Крупный сбой произошел в компьютерной системе японских филиалов Citibank.

30 марта 2008, пятый терминал лондонского аэропорта Хитроу — сотни рейсов отменены, 15 тыс. чемоданов потеряны, десятки тысяч человек ожидают возврата багажа.

«Обеспечение непрерывности и восстановления деятельности» с точки зрения 2194-У

Чтобы выполнить поставленные задачи по обеспечению непрерывности бизнеса и разработки Планов ОНиВД, необходимо разобраться, что же стоит за определением «обеспечения непрерывности и восстановления деятельности» с точки зрения 2194-У.

Указание 2194-У написано в довольно общих терминах и вносит больше вопросов, чем ясности в понятие обеспечения непрерывности бизнеса.

Из множества материалов, представленных на семинарах, которые проводят представители Центрального Банка, становится понятно, что ЦБ не рекомендует рассматривать 2194-У и 242-П в отрыве от практики расчета операционных рисков (в соответствии с лучшими мировыми стандартами и рекомендациями в этой области), в том числе от Basel. ЦБ РФ трактует обеспечение непрерывности бизнеса как меру снижения операционных рисков. Речь идет именно об операционных рисках, потому что, исходя из определения операционного риска, под это понятие попадают как риски ИТ, ИБ, так и риски прерывания бизнес-процессов в случае возникновения ЧС, это так называемые крупные операционные нарушения. В связи с этим ЦБ РФ рекомендует рассматривать Планы ОНиВД как меру снижения операционных рисков кредитных организаций, как механизм снижения нагрузки на капитал. При разработке Планов ОНиВД желательно руководствоваться тем уровнем затрат, которые кредитная организация способна выделить из резерва на случай реализации операционных рисков, чтобы в последствии за счет наличия и использования Планов ОНиВД сократить объем данного резерва.

Эти сведения не прописаны в явном виде в самом Указании и были получены нашими специалистами на специализированных семинарах ЦБ, которые проходили в течение нескольких месяцев сразу после выхода Указания.

Нормативные документы РФ и ЦБ, которые необходимо учитывать при разработке Плана ОНиВД

Опираясь на рекомендации ЦБ, организация, которая собирается модернизировать или разрабатывать Планы ОНиВД, должна учитывать не только принципы Объединенного форума, но и лучшие мировые практики разработки систем управления непрерывностью бизнеса и операционными рисками. Начать можно с таких известных стандартов, как: PAS 77:2006, PAS 56:2003, BS 25999 (part 1/part 2), а также рекомендаций международного института BCI — Business Continuity Institute. На внешнем Интернет-ресурсе BCI — http://www.thebci.org/ в свободном доступе можно найти разнообразные стандарты и лучшие мировые практики в области обеспечения непрерывности бизнеса. При разработке Планов ОНиВД необходимо также обратить внимание на нормативные документы российского законодательства (см. Приложение 1, стр. 18).

Из дополнительной информации семинаров также становится понятно, что в основу выданных рекомендаций Приложения 2194-У были положены принципы, выпущенные Объединенным форумом. Эти принципы были изложены в документе «Руководящие принципы обеспечения непрерывности бизнеса», август 2006 года («The Join Forum, High-level principles for business continuity», august 2006). Всего было выделено 7 принципов или 7 фокусов внимания, отраженных в 2194-У:

В Объединенный форум вошли:
- Базельский комитет по банковскому надзору
- Международная организация комиссий по ценным бумагам
- Международная ассоциация органов надзора за деятельностью страховых компаний (для Банка международных расчетов)

Принцип 1: Ответственность совета директоров и высшего руководства кредитной организации
Данный принцип возвращает фокус ответственности за управление всеми рисками организации на совет директоров и исполнительные органы управления организацией.

Принцип 2: Крупные операционные нарушения
Из всех возможных аварий, угроз Планы ОНиВД фокусируются на случаях крупного операционного нарушения. Такие нарушения могут привести к затруднению проведения банковских операций участниками деятельности финансового сектора или финансовой системы страны в целом.

Принцип 3: Цели восстановления деятельности
Принцип гласит, что все участники деятельности финансового сектора должны сами сформулировать для себя цели восстановления своей деятельности, отражающие уровень риска для финансовой системы, который может возникнуть со стороны участников в случае ЧС. Для формирования таких целей необходимо отчетливо понимать, какой урон от прекращения деятельности организации может понести финансовая система в целом. Если организация не может самостоятельно сформировать такие цели, то финансовые органы РФ (МинФин, ЦБ РФ и т.п.) обязаны принять необходимое участие в определении подобных целей восстановления.

Принцип 4: Обмен информацией с заинтересованными сторонами
Данный принцип фокусирует внимание на важности своевременного и правильного внутреннего и внешнего обмена информацией в случае крупного операционного нарушения. Должны быть заранее продуманы, спланированы и отработаны процедуры оповещения в случае ЧС, что позволит в момент «Х» минимизировать последствия кризисной ситуации и сохранить доверие населения к организации и финансовой системе.

Пример последствий ЧС

Красноярск, 17 августа — крупная авария произошла в понедельник утром на Саяно-Шушенской ГЭС в Республике Хакасия. Благодаря заранее проведенному анализу рисков, было проведено страхование реализовавшихся рисков. РОСНО выплатит «РусГидро» 200 миллионов долларов на ремонт Саяно-Шушенской ГЭС после расследований причин аварии.

Принцип 5: Трансграничный обмен информацией
В случае крупного операционного нарушения, которое может проходить в пределах нескольких различных юрисдикций, также необходимо спланировать и разработать процедуры оповещения и обмена информацией о подобном нарушении.

Принцип 6: Аудиты или проверки
Для того, чтобы разработанные Планы ОНиВД могли действительно предупредить и минимизировать последствия ЧС и обеспечить восстановление в требуемое бизнесом время, нужно производить регулярную проверку Планов ОНиВД на актуальность, а также оценивать эффективность и результативность их работы.

Принцип 7: Контроль за управлением непрерывностью бизнеса со стороны финансовых органов
Заключительный принцип гласит о том, что финансовые органы (в нашей стране это ЦБ) обязаны проводить внешнюю независимую оценку участников деятельности финансового сектора.

Вероятно, по оценкам ЦБ, реализация данных принципов поможет обеспечить в кредитных организациях управление непрерывностью деятельности с точки зрения успешного функционирования финансовой системы страны в целом.

Несоответствия рекомендациям 2194-У в уже имеющейся документации организации

Разобравшись в сути определения обеспечения непрерывности деятельности с точки зрения 2194-У, можно рассмотреть картину общих недостатков, которые были выявлены специалистами компании «Инфосистемы Джет», исходя из практики работы в области непрерывности бизнеса. Был установлен ряд наиболее распространенных слабых мест систем обеспечения непрерывности деятельности, которые можно расценивать как несоответствия рекомендациям 2194-У. Среди основных недостатков можно выделить следующие:

- В качестве объектов восстановления рассматриваются ИТ-системы и другие ресурсы, а не услуги, предоставляемые клиентам, и бизнес-процессы.
- Неполная структура планов ОНиВД:
  - наличие высокоуровневого документа, но отсутствие детальных планов по восстановлению конкретных бизнес-процессов и соответствующих ресурсов;
  - наличие низкоуровневых документов по восстановлению ресурсов, но отсутствие единого документа для всех критичных бизнес-процессов.
- Низкоуровневые планы ОНиВД в рамках одного подразделения часто не содержат требования ко времени восстановления со стороны бизнеса.
- Отсутствие описания критичных бизнес-процессов до уровня средств обеспечения НД, ресурсов, ответственных (владельцев бизнес-процессов), временных рамок выполнения процессов, альтернативных способов выполнения процессов.
- Отсутствие планирования регулярного тестирования и проведения обучения персонала в части НД. У сотрудников нет понимания, как им действовать в случае наступления ЧС.
- Отсутствие четкого разделение ответственности и обязанностей по реализации планов восстановления бизнес-процессов и бизнес-операций.
- Планы реагирования не синхронизированы с планами восстановления.
- Не предусмотрен орган чрезвычайного управления в случае ЧС.
- Планы не пересматриваются и устаревают, изменения, которые происходят в организации, в планы не попадают, поэтому они очень быстро становятся неработоспособными.

В соответствии с Приложением к письму Банка России от 27 февраля 2006 года № 30-Т «О проведении анкетного опроса кредитных организаций о состоянии управления операционным риском» было выявлено, что более 75% всех кредитных организаций России имеют планы обеспечения непрерывности деятельности, однако насколько они в рабочем состоянии и реально могут быть использованы в случае ЧС, определено не было.

Данное исследование было проведено специалистами нашей компании самостоятельно, при этом за критерии соответствия были взяты положения самого указания 2194-У. Что, как и с какой тщательностью будет проверено в ходе аудитов ЦБ остается большим вопросом, и тут можно только догадываться о серьезности и глубине проверки.

Приведенная выше информация поможет сотрудникам кредитных организаций сформировать для себя общее представление о сути направления, занимающегося обеспечением непрерывности бизнеса и выполнением положений новов-

веденного Указания, а также сделать вывод о «масштабе бедствия» с точки зрения обеспечения непрерывности бизнеса в своей компании.

На основании такой общей картины происходящего, потребностей и ресурсных возможностей организация может выбрать подход по разработке и внедрению Планов ОНиВД.

Решение задач, стоящих перед организациями в области НБ. Подход компании «Инфосистемы Джет»

Когда руководство организации определило стратегию по снижению операционных рисков посредством разработки ОНиВД, встает вопрос — кому поручить работы проекта по обеспечению непрерывности бизнеса в компании, чтобы решить задачи по НБ наиболее эффективным способом и преодолеть вышеперечисленные сложности.

Можно разрабатывать Планы ОНиВД, а также систему поддержки и управления непрерывностью бизнеса самостоятельно — силами специалистов компании, а можно приглашать внешних консультантов.

Если организация идет первым путем, необходимо грамотно распределить работу между многими подразделениями кредитной организации: операционных рисков, внутреннего контроля, описания бизнес-процессов, управления документацией, департаментами ИТ и ИБ, а также привлечь ответственных специалистов по каждому бизнес-процессу внутри организации. Необходимо изначально определить внутреннюю проектную команду, которая будет включать представителей вышеперечисленных подразделений и в обязательном порядке специалиста по системам управления НБ, который в последствие будет наделен ролью менеджера по НБ в организации. Рынок специалистов по обеспечению непрерывности бизнеса в России до сих пор остается очень узким, поскольку культура данного направления еще не прижилась в большинстве отечественных организаций, как это уже давно практикуется на Западе. Однако тот небольшой процент организаций, который уже дорос до осознания значимости защиты своей компании от ЧС, развивает свои собственные компетенции по обеспечению непрерывности бизнеса. В помощь таким специалистам можно порекомендовать перечень информационных ресурсов и курсов в соответствии с лучшими мировыми практиками и стандартами (см. Приложение 1, стр. 18).

Риски разработки системы управления и обеспечения НБ собственными силами заключаются в отсутствии практики реализации подобных проектов и системного подхода у внутренних специалистов, что может изначально заложить большое количество ошибок уже на этапе проектирования системы НБ и планов ОНиВД.

Можно пойти по пути приглашения внешних консультантов для проведения подобного рода работ. В зависимости от финансовых возможностей и потребностей организации специалистами компании «Инфосистемы Джет» по проведению консалтинговых проектов, с точки зрения практических навыков работы, были выделены 3 варианта решений по разработке и внедрению Планов ОНиВД с учетом текущей кризисной ситуации:

- **Активный консалтинг.** Данный вариант позволяет провести все работы силами внешних консультантов. Работы включают весь цикл разработки Планов и Системы управления Планами НБ (см. выше). Данный вариант работ подходит для организаций, серьезно прорабатывающих вопросы обеспечения непрерывности бизнеса.
- **Пассивный консалтинг.** Данный вариант позволяет выполнить работы по разработке Планов и Системы управления Планами ОНиВД путем разделения работ между специалистами кредитной организации и внешними консультантами. При этом процент распределения нагрузки между проектными группами Исполнителя и Заказчика сказывается на стоимости проекта. Данный вариант в наибольшей степени приближает нас к той самой «золотой середине» и подходит для организаций, которые нацелены извлечь пользу из работ по достижению соответствия рекомендациям 2194-У.
- **Модернизация/разработка Планов ОНиВД и процессов поддержания Планов.** Данный вариант позволяет обеспечить экспресс-анализ и разработку необходимой документации Планов ОНиВД и Системы управления Планами ОНиВД в соответствии с лучшими мировыми практиками. Данный вариант применим для организаций, в которых Планы уже существуют, однако необходима их модернизация с учетом 2194-У. Этот метод может быть применим, если сама организация сочтет такой вариант достаточным, исходя из уровня операционных рисков, и идеально подходит для быстрого достижения соответствия 2194-У.

По опыту консалтинговых проектов компании «Инфосистемы Джет» выработка данных ва-

риантов решений позволила уйти от общепринятого представления, что внешние консультанты — это «очень дорого, долго и мучительно», а также сохранить очень высокий уровень качества работ при относительно невысокой их стоимости за счет передачи уникальных знаний специалистам заказчика и использованию внутренних ресурсов. При реализации подобного рода проектов нужно всегда руководствоваться следующими принципами:

- адаптация лучших мировых практик к российской реальности;
- работа единой командой: от технического проектировщика до аналитика бизнес-процессов, использование «мозгового штурма» для решения сложных задач;
- индивидуальный подход с учетом специфики компании, при котором во главу угла ставится удобство работы с решением по НБ.

Рис. 1. Цикл реализации, внедрения и совершенствования непрерывности бизнеса

Как разработать систему обеспечения непрерывности бизнеса качественно и с пользой для бизнеса. Шаги по разработке Планов ОНиВД (схемы работ активного и пассивного консалтинга)

Следуя рекомендациям Приложения 2194-У, организация приходит к пониманию принципов реализации Системы управления непрерывностью бизнеса, а также осознанию того, что обеспечение непрерывности бизнеса — это не проект, это процесс, который необходимо не только выстроить единожды, но поддерживать, улучшать, контролировать и оценивать, как любой другой процесс организации.

Для того, чтобы в организации разработать, внедрить и поддерживать Планы ОНиВД, необходимо следовать основному циклу разработки и внедрения процессов НБ (см. рис. 1).

Исходя из цикла внедрения процессов НБ, можно выделить следующие этапы работ по реализации проекта:

1. Обследование организации и анализ ее работы с точки зрения НБ, проведение анализа возможного ущерба от воздействия ЧС на бизнес, анализ рисков, определение требований по НБ.
2. Выделение и описание критичных бизнес-процессов.
3. Разработка Стратегии НБ с выбором способа восстановления.
4. Разработка Политики НБ, определение ролевой структуры, разработка процессов обеспечения и управления НБ.
5. Разработка решений по НБ (технических и организационных), разработка Планов ОНиВД.
6. Внедрение мер по обеспечению НБ в организации (технических и организационных), проведение обучения, тестирования Пла-

На этапе изучения организации специалисты компании «Инфосистемы Джет» применяют наиболее распространенный и зарекомендовавший себя подход описания бизнес-процессов с использованием инструментария и методологии ARIS, что позволяет легко и быстро обеспечивать проектирование, моделирование и внедрение процессов обеспечения непрерывности бизнеса на практике.

В ходе проекта применяются наиболее подходящие для каждой конкретной задачи средства и способы представления результатов:

- ARIS Business Architect — моделирование и анализ архитектуры предприятия;
- ARIS Business Designer — упрощенный инструмент для моделирования архитектуры предприятия;
- ARIS Business Publisher — публикация моделей архитектуры предприятия и их динамическое представление;
- ARIS IT Architect — проектирование ИТ-архитектуры предприятия;
- ARIS IT Inventory — децентрализованное web-ориентированное управление ИТ-ресурсами;
- ARIS Defense Solution — для организационных архитектур по DoDAF/C4ISR;
- ARIS Business Simulator — динамическое моделирование бизнес-процессов (платформа Java).

Когда процессы обеспечения бизнеса уже смоделированы, а планы разработаны, встает вопрос их поддержания в актуальном состоянии, ведь именно наличие в организации актуальных Планов ОНиВД является залогом успеха в случае наступления ЧС.

Поддержание планов в актуальном состоянии довольно трудоемкий непрерывный процесс. Для того, чтобы сделать этот процесс наиболее удобным на практике и менее ресурсоемким, существуют современные средства автоматизации этих процессов, такие как, например, продукты от компании Strohl Systems. Для работы с планами и автоматизации процессов обеспечения непрерывности бизнеса могут быть использованы различные решения этого производителя:

- LDRPS 10 (Living Disaster Recovery Planning System) – система для создания и поддержания в актуальном состояния планов обеспечения непрерывности бизнеса/аварийного восстановления. LDRPS 10 позволяет создавать планы, базирующиеся на информации об инфраструктуре компании, бизнес-процессах и приложениях, данных о сотрудниках, контрагентах и т.п. Благодаря своим функциональным возможностям, LDRPS 10 позволяет удовлетворить значительному числу требований основного стандарта по непрерывности бизнеса – BS 25999, касающихся вопросов создания и поддержания планов.
- BIA Professional (Business Impact Analysis Professional) – инструмент для проведения анализа воздействия на бизнес. BIA Professional предоставляет удобный механизм для разработки опросных листов, их распространения, сбора и последующего анализа информации. За счет хранения всей собранной информации BIA Professional существенно ускоряет процесс проведения повторного анализа воздействия на бизнес, который проводится через определенный интервал времени – анкетируемые сотрудники получают возможность просмотреть свои предыдущие ответы и, в случае необходимости, внести изменения. Для компаний с многоуровневой структурой управления BIA Professional предусматривает возможность для руководителей подразделений просмотреть анкеты, заполненные их подчиненными, и либо утвердить, либо направить на доработку (или самостоятельно внести исправления).
- NotiFind – услуга предоставления кризисной коммуникации, обеспечивающая гарантированную доставку сообщений (в том числе, массовую) в случае наступления ЧС. Сообщения могут доставляться в виде записанных заранее голосовых сообщений, текстовых (SMS, e-mail) и графических (факс, e-mail). NotiFind поддерживает все доступные средства связи – телефон, факс, SMS, e-mail, пейджер, blackberry и т.п., обеспечивает гибкую систему эскалации в случае недоступности пользователей. Система обладает достаточной производительностью, чтобы осуществить рассылку в течение часа до 160 тысяч голосовых и 500 тысяч текстовых сообщений. Хостинг NotiFind осуществляется в двух катастрофоустойчивых центрах обработки данных, расположенных в США (Массачусетс и Иллинойс). За счет интеграции с LDRPS 10 NotiFind позволяет автоматически загружать ту часть планов, которая содержит «деревья вызовов» и контактную информацию сотрудников и контрагентов, за счет чего задача поддержания всей информации в актуальном состоянии решается автоматически.

нов ОНиВД, внедрение процедур обеспечения и управления НБ, автоматизация работы с Планами ОНиВД.

7. Поддержка Планов ОНиВД – актуализация, постоянное совершенствование.

Обеспечение непрерывности бизнеса – свойство любой организации независимо от ее масштабов по своевременному возобновлению критичных бизнес-процессов в случае наступления чрезвычайных ситуаций для предотвращения непредвиденных убытков и наступления кризиса. Критичными бизнес-процессами является набор внутренних последовательных работ подразделений организации, в результате которых производится ключевой продукт или оказывается ключевая услуга, потребляемые клиентами и приносящие основную прибыль бизнесу. Чтобы обеспечить непрерывность бизнеса, необходимо гармонично встроить систему управления обеспечением непрерывности деятельности в общую структуру менеджемента организации (см. рис. 2.) Система разрабатывается в зависимости от потребностей, возможностей организации, ее размеров, количества видов деятельности и работающего персонала.

Основной задачей при планировании непрерывности деятельности становится изучение и спецификация своей организации. Для этого необходимо учесть: продукты и услуги организации, доходность, обеспечиваемая каждой услугой

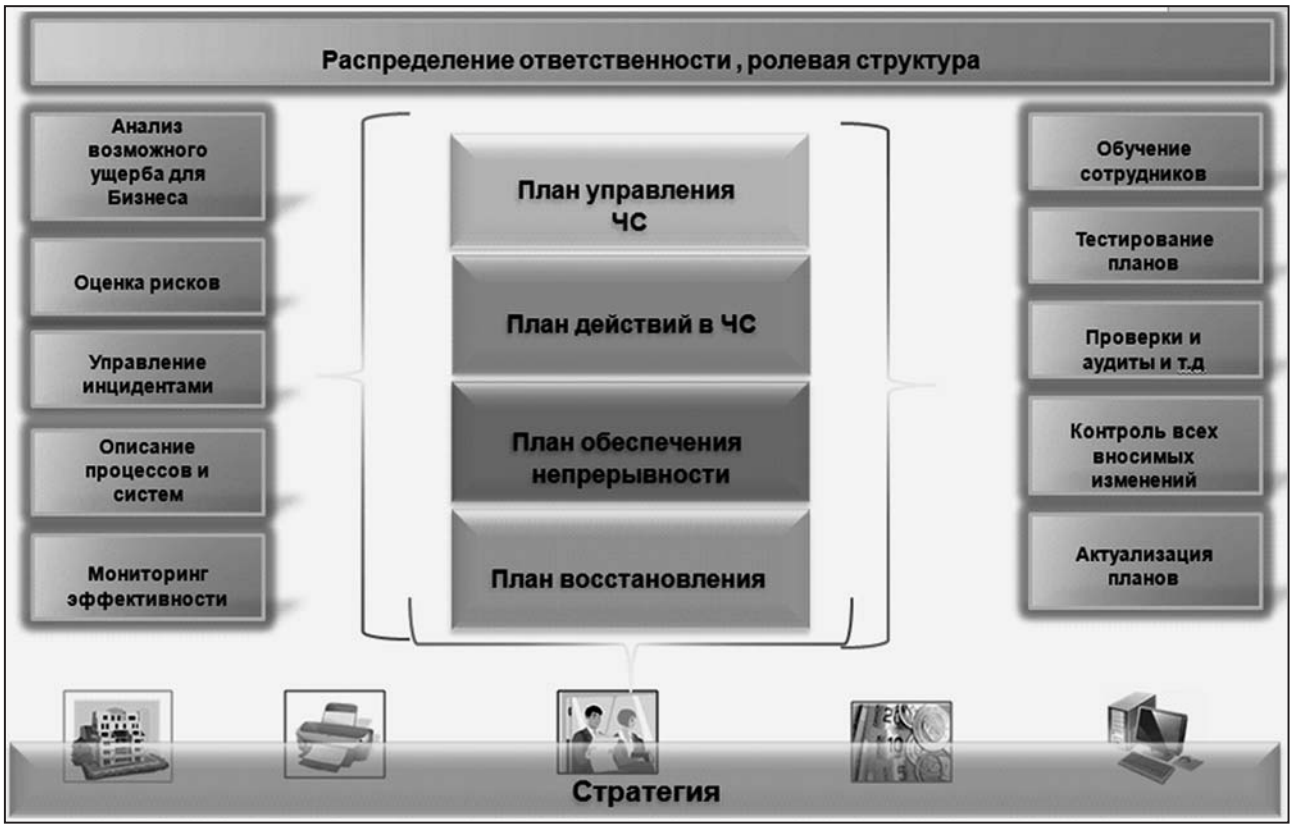


Рис. 2. Элементы системы управления и обеспечения НБ

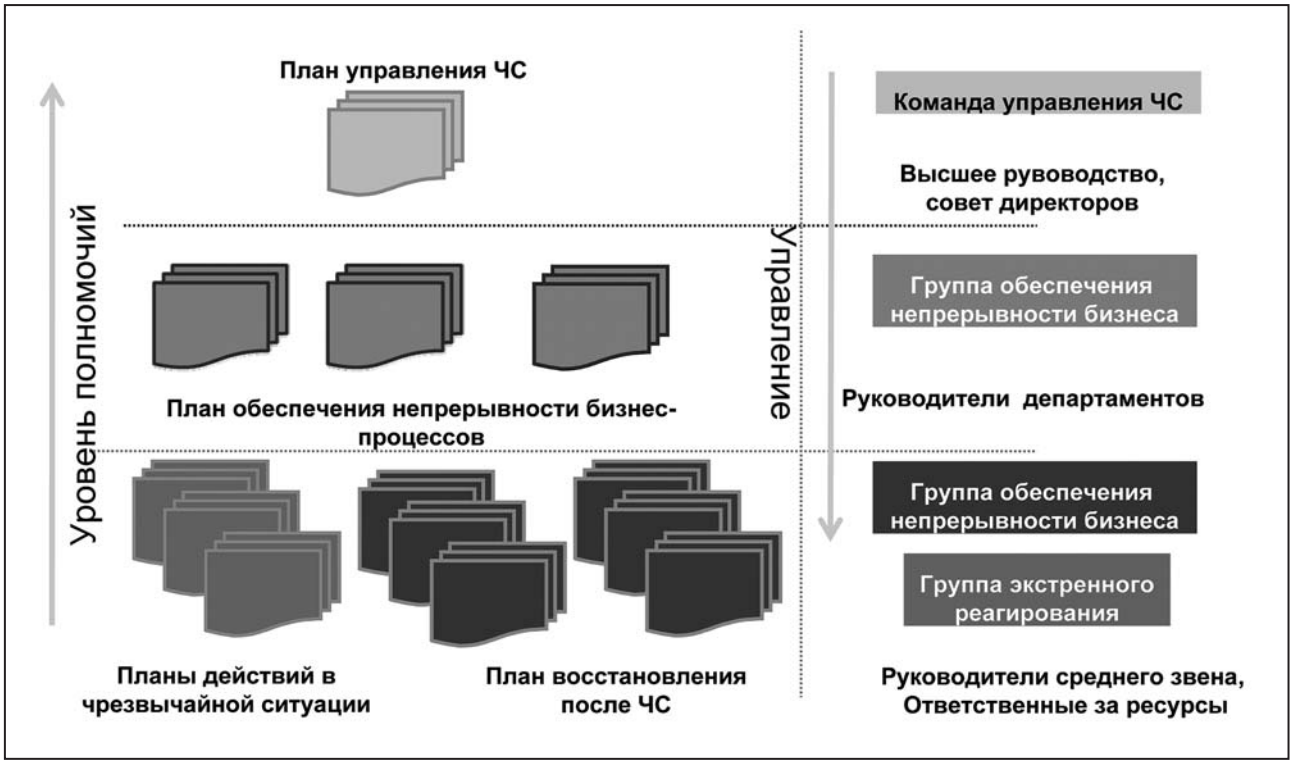


Рис. 3. Структура планов и уровни полномочий

или выпуском продукта, ключевых клиентов, критичные договора и обязательства, нарушение которых может повлечь штрафные санкции, специфику внутренних бизнес-процессов, обеспечивающих выполнение обязательств, их взаимосвязи между собой, а также необходимые ресурсы (в том числе ИТ-системы).

Получив все необходимые сведения об организации, можно оценить потенциальный ущерб от прерывания деятельности в результате наступления ЧС (финансовые потери, потери деловой репутации), проработать конкретные сценарии выявленных угроз и проанализировать вероятность их наступления, оценив риски.

Оценка потенциального ущерба позволяет определить наиболее оптимальный способ обеспечения непрерывности деятельности. Данный способ отражается, как правило, в стратегии обеспечения непрерывности деятельности и позволяет сбалансировать необходимый для выбранного способа бюджет. Стратегия определяет, каким именно образом будет обеспечена непрерывность и порядок восстановления, она отвечает на вопрос «ЧТО?». Если в результате анализа будет установлена необходимость изменять текущую инфраструктуру, разрабатываются эскизные проекты и на основании них проводится внедрение катастрофоустойчивых решений.

На основании выбранной стратегии и учитывая наиболее значимые сценарии наступления ЧС, разрабатываются Планы антикризисного управления ЧС, планы действий в случае ЧС, планы обеспечения непрерывности и восстановления деятельности. Такая структура планов позволяет эффективно использовать их в организации на всех уровнях управления (см. рис. 3, стр. 14).

Планы непосредственно предназначены для реализации выбранного способа восстановления и обеспечения непрерывности на практике, они описывают точные последовательные действия, должны быть четко синхронизированы друг с другом и отвечать на вопрос «КАК?». Именно Планы являются «сердцем» системы обеспечения НБ, от того насколько они правильно составлены, актуальны и доведены до персонала, зависит успех реагирования и восстановления бизнеса. Поскольку около 85% организацией используют информационные технологии в своих бизнес-процессах, то особое внимание нужно уделять планам восстановления ИТ-систем и ИТ-инфраструктуры. Планы также должны содержать порядок обращения с конфиденциальной информацией и способы ее защиты от раскрытия, утраты или искажения в случае ЧС.

Для малого и среднего бизнеса разработка системы управления и обеспечения НБ может носить облегченный характер для того, чтобы быть удобной в использовании и отражать потребности бизнеса. Не нужно разрабатывать множество отдельных документов и создавать искусственную ролевую структуру НБ, достаточно продумать подробный план действий в случае ЧС и четко определить расписание актуализации и тестирования для плана. Так, к примеру, группа экстренного реагирования может включать одного ответственного сотрудника, наделенного соответствующей ролью, вместо строгой структуры планов могут быть разработаны инструкции по действию в каждой конкретной ситуации и приведен порядок информирования о ЧС. Однако при организации непрерывности бизнеса очень важно руководствоваться именно системным подходом при разработке мер НБ.

При этом все работы по разработке и внедрению Планов ОНиВД могут проводиться по схеме «активного или пассивного» консалтинга в зависимости от возможностей самой организации.

Проекты по обеспечению непрерывности бизнеса всегда непросты и очень индивидуальны для каждой компании. Так, например, отличительной особенностью проекта компании «Инфосистемы Джет» «Отправка платежных поручений в рублях в МЦИ» по обеспечению непрерывности бизнес-процесса крупного российского банка явился упор на обеспечение непрерывности выполнения операций процесса с точки зрения доступности всех ресурсов, а не только ИТ-сервисов, как это часто делалось на других проектах по НБ.

Целью проекта было обеспечение непрерывного выполнения процесса отправки платежных поручений в рублях в МЦИ. Работы по проекту специалистами компании «Инфосистемы Джет» были разбиты на 5 этапов: анализ и описание бизнес-процесса; определение требований непрерывности (временные рамки, применяемые технологии, уровень производительности процесса); оценка рисков; выбор способа обеспечения непрерывности бизнес-процесса (задача — обеспечить НБ за счет имеющихся средств в Банке); разработка Плана обеспечения непрерывности бизнес-процесса (Инструкции для персонала); разработка рекомендаций по обеспечению непрерывности деятельности Банка. Все работы были выполнены в течение 2.5 месяцев.

Наиболее трудоемким, но одновременно и наиболее полезным для Банка оказался этап анализа и описания бизнес-процесса. Специалиста-

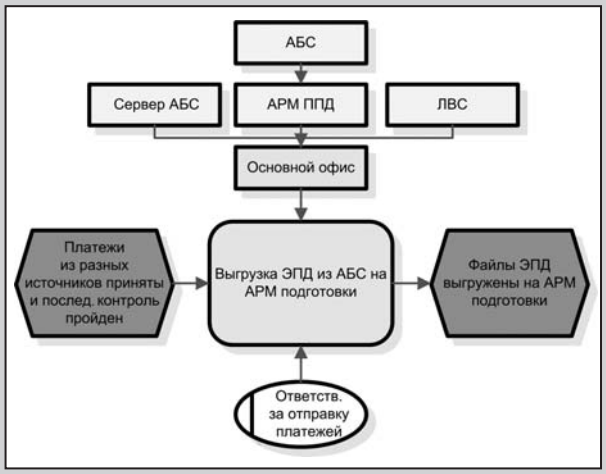


Рис. 4. Формат описания бизнес-процесса

ми компании «Инфосистемы Джет» в нотации ARIS были описаны операции выполнения бизнес- процесса, этапы выполнения, события, роли исполнителей, все ресурсы (автоматизированные системы, программные, аппаратные компоненты, помещения и т.д.), временные рамки его выполнения, виды платежей, существующие меры обеспечения бесперебойной работы процесса, а также совместно с сотрудниками банка определены возможные альтернативные способы выполнения процесса в случае ЧС. Для каждой операции были определены ресурсы, роли и результат.

Результатом описания стал отчет, в котором в удобной графической, табличной и текстовой форме были описаны все операции выполнения бизнес-процесса (см. рис.4).

После описания бизнес-процесса был проведен анализ влияния на бизнес недоступности бизнес-процесса. В ходе выполнения работ были установлены:

- штрафные санкции от простоя бизнес-процесса в соответствии с договорными обязательствами;
- требуемое время восстановления бизнес-процесса (без потерь составляет 30 минут);
- требуемый объем операций;
- определены требования к применяемым технологиям с точки зрения обеспечения непрерывности деятельности относительно следующих ресурсов:
  - персонал;
  - офис, помещение;
  - серверные компоненты;
  - аппаратно-программные компоненты АРМ;
  - сетевые компоненты/каналы связи;
  - носители информации.

Исходя из полученных показателей, были определены границы возможных потерь, которые может понести банк в случае простоя бизнес-процесса, возможное время простоя бизнес-процесса и стратегии восстановления. Параллельно шла работа по проведению анализа рисков прерывания бизнес-процесса. В ходе выполнения данного этапа специалистами компании «Инфосистемы Джет» были выделены риски невыполнения заданных требований непрерывности бизнес-процесса, основанные на анализе сценариев реализации чрезвычайных ситуаций и действий, которые принимаются в текущих условиях.

Результатом этапа стала матрица критичных и некритичных рисков (см. таб. 1), в соответствии с которой была выбрана стратегия обеспечения непрерывности бизнес-процесса. Страте-

Таб. 1. Матрица оценки рисков

№ п.п.	Возможные сценарии	Действия исполнителей процесса (реагирование на инцидент)	Время восстановления/ уровень риска
01	Первый ответственный не вышел на работу, задержался, с ним невозможно связаться по телефону	Первый ответственный информирует Второго ответственного и Директора Операционного департамента. Процесс выполняет Второй ответственный за отправку/прием платежных поручений МЦИ. Второй ответственный информирует Директора Операционного департамента и выполняет процесс.	Время восстановления процесса < Т минут
02	Первый ответственный не вышел на работу, задержался, с ним невозможно связаться по телефону	Оба ответственных расположены в одном кабинете. Меры по территориальному распределению персонала не предусмотрены. Инструкция по выполнению процесса существует, но сотрудникам У КО, ответственным за выполнение процесса, неизвестно где она находится.	Время восстановления процесса > Т минут

гия, выбранная руководством, не потребовала дополнительных изменений инфраструктуры, а вносила коррективы в штатную структуру и порядок бизнес-процесса. На основании утвержденной стратегии были разработаны План действий в случае ЧС, который позволяет обеспечить восстановление бизнес-процесса не более чем за 30 минут в случае возникновения сбоев ПО, оборудования основного АП или проблем с ЛВС.

По желанию Заказчика они включили в себя низкоуровневые инструкции: План действий Ответственного за отправку-прием платежей в МЦИ в случае нештатных ситуаций и План действий Администратора АП в случае нештатных ситуаций. Так же был описан порядок оповещения, реагирования и восстановления ресурсов и бизнес-процессов в случае наступления ЧС (см. рис. 5).

После проведение проекта банку были выданы рекомендации, которые необходимо выполнить для обеспечения работоспособности подготовленных планов, рекомендации по повышению эффективности разработанных планов и снижению риска возникновения нештатных ситуаций; рекомендации по обеспечению непрерывности бизнес-процессов для Банка в целом. На текущий момент ведутся работы по продолжению проекта в связи с успешным положительным опытом работы над одним бизнес-процессом.

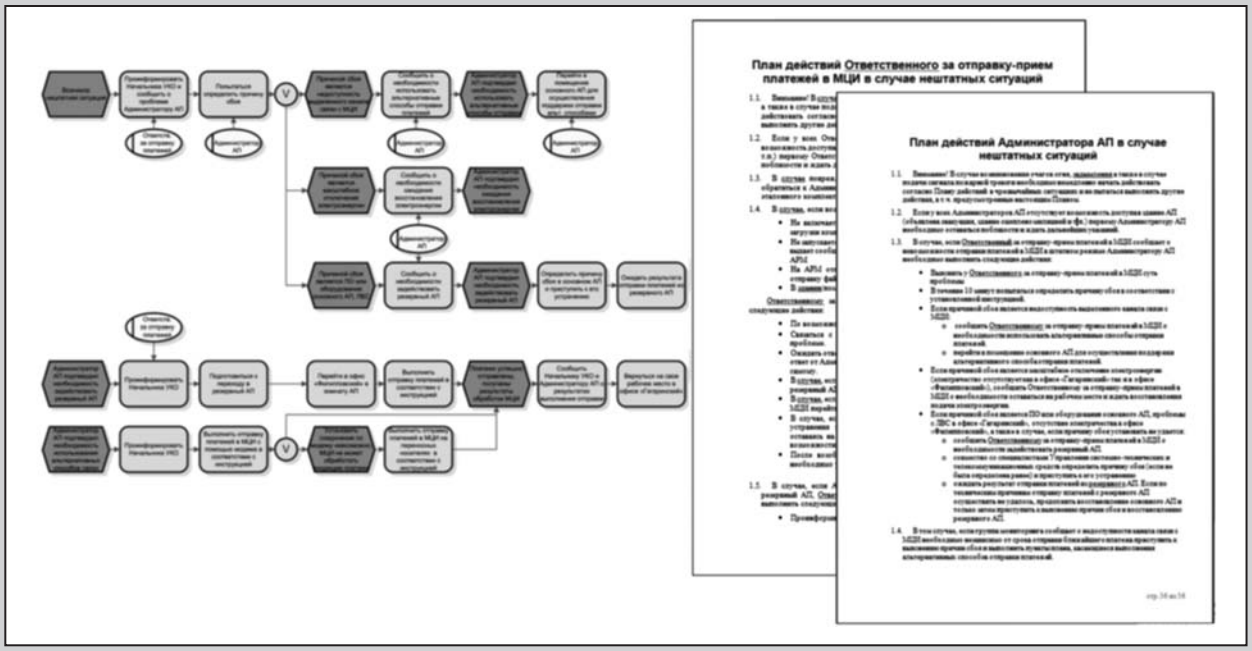


Рис. 5. Схема оповещения и реагирования в случае ЧС

Выполнять рекомендации ЦБ является нормальной практикой в любом государстве, где имеется центральный финансовый регулирующий орган. Но кризис вносит свои коррективы в планы и распределение финансовых вложений внутри организаций, поэтому сейчас очень часто перед компанией, в связи с недостатком бюджетирования, встает вопрос достижения формального соответствия рекомендациям ЦБ. Эта задача становится первостепенной, а мера краткосрочной, в то время, когда разработка и внедрение системы НБ откладывается на более поздний срок.

Если основная задача компании добиться формального соответствия требованиям и рекомендациям 2194-У, то специалистами нашей компании проводятся работы по приведению в соответствие имеющейся в компании документации и средств непрерывности бизнеса. Такие работы могут опираться на уже имеющиеся в кредитной организации материалы, разработанные ранее в соответствии с 242-П, тогда схема работ будет проводиться в соответствии с 3-м вариантом решений — «Модернизация/разработка Планов ОНиВД и процессов поддержания Планов».

Выводы

В заключение можно еще раз отметить, что «золотая середина» обеспечения непрерывности бизнеса проходит на стыке пользы от построенной системы и затратами, которые в принципе готова понести организация на ее разработку и внедрение. При этом разработка системы обеспечения непрерывности бизнеса может быть построена

с учетом рекомендаций 2194-У или иных требований, которые необходимо выполнить кредитной организации. Если организация заинтересована в работающей системе обеспечения непрерывности бизнеса и заранее заботится о сохранности своих финансовых средств, клиентов, активов и репутации в случае наступления ЧС, следует задуматься о разработке и внедрении полноценной системы обеспечения и управления непрерывностью бизнеса. Данные работы должны быть организованы и проведены с учетом специфики деятельности и ресурсных возможностей организации, используя при этом либо свои собственные силы, либо приглашая внешних специалистов. Если цель — работающая система, то разработка и внедрение, в обязательном случае, должны пройти по циклу, приведенному на рис.1 (см. стр. 12). Уровень зрелости системы при этом будет постепенно нарастать, а система становиться частью культуры организации. Для этого так же может быть выбрана какая-то конкретная область организации (например, ИТ — инфраструктура), с которой можно начать, постепенно распространяя практику на другие области. Такой подход позволит достичь соответствия различным стандартам, в том числе и рекомендациям 2194-У, поскольку они базируются на общемировой практике, добавляя лишь специфику законодательства РФ. Однако, если организация ставит перед собой цель добиться только формального соответствия, то, возможно, следует задуматься — ведь, скорее всего, достичь формального соответствия можно так же с пользой и выгодой для бизнеса.

Пусть Ваш бизнес будет непрерывным!

Приложение 1

Перечень документов российского законодательства в части, касающейся НБ

- Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Статья 7. Права и обязанности организаций, осуществляющих операции с денежными средствами или иным имуществом (в редакции от 30.10.2002 № 31-ФЗ);
- Приложение 5 к Положению Банка России от 16 декабря 2003 года № 242-П «ОБ организации внутреннего контроля в кредитных организациях и банковских группах»;
- Гражданский кодекс Российской Федерации, статья 401. Основания ответственности за нарушения обязательств;
- Унифицированные правила и обычаи для документарных аккредитивов (публикация Международной торговой палаты № 500, ред. 1993 г., вступила в силу с 1 января 1994 г.), Статья 14. Форс-мажор;
- Федеральный закон от 21 декабря 1994 года № 68-ФЗ «О защите населения и территории от чрезвычайных ситуаций природного и техногенного характера» (в частности, Статья 14);
- Постановление Правительства РФ от 21 мая 2007 года № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера»;
- «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2008);
- Письмо ЦБ РФ от 24.05.2005 N 76-Т «Об организации управления операционным риском в кредитных организациях» и т.д.

Перечень информационных ресурсов по НБ

- ASIS International Disaster Preparation Guide — www.asisonline.org/newsroom/crisisResponse/disaster.pdf;
- Disaster Recovery Institute International — https://www.drii.org/docs/profprac_details.pdf, http://www.drj.com/GAP/gap.pdf ;
- Business Continuity Institute, Professional Practices & Methodology — http://www.thebci.org/businesscontinuityguides.htm;
- Business Continuity Management Good Practice Guidelines (2008-2) — http://www.thebci.org/;
- Join Disaster Recovery Information Exchange (DRIE) — http://toronto.drie.org/;
- BS 25777 — Information and communication technology (ICT);
- Basel II Accord;
- Bank for International Settlements — High-level Principles for Business Continuity Planning — August 2006;
- European Commission — Markets and Financial Instruments Directive (MiFID);
- BS 25999 — Business Continuity Management — www.bsi-global.com , www.bsi-russia.ru;
- HB221-2004, HB292-2006, HB293-2006;
- NFPA 1600 Standard on Disaster/Emergency and Business Continuity Programs;
- SS 540 — Business Continuity Management;
- Курсы по направлению BS 25999 компании BSI MS.

СОБЕСЕДНИК

Рассказывая в этом номере о новом постановлении в области обеспечения непрерывности бизнеса, мы не могли не уделить внимание важному моменту, который связан с оценкой операционных рисков. Экспертным мнением в рубрике «Собеседник» по этому вопросу с нами поделился Вячеслав Железняков, руководитель группы экспертного аудита компании «Инфосистемы Джет».

J.I.: Какова в настоящий момент ситуация с оценкой операционных рисков в банках, с которыми вам приходилось работать?

В.Ж.: В настоящее время большинство банков старается придерживаться в этой области принципов, описанных в международном соглашении Basel II, а также рекомендаций, изложенных в письме ЦБ РФ № 76-т «Об организации управления операционным риском в кредитных организациях».

J.I: Не могли бы Вы рассказать немного о подходе по расчету операционных рисков в соответствии со стандартом Basel. Насколько я знаю, ЦБ РФ активно продвигает подход, изложенный в данном стандарте, среди российских кредитных организаций.

В.Ж.: Да, ЦБ РФ ведет планомерную работу по присоединению банковской системы РФ к соглашению BASEL II. В настоящее время банки обязаны резервировать капитал под кредитные и рыночные риски. Очередь за операционными.
Если говорить в двух словах, то соглашение BASEL II предусматривает три основных подхода:

- подход базовых показателей (Basic Indicator Approach) – необходимый резерв капитала определяется исходя из ежегодного дохода организации банковской системы и коэффициента, характеризующего уровень операционного риска для конкретного государства;
- стандартизованный подход (Standardised Approach) – необходимый резерв капитала определяется исходя из ежегодного дохода организации банковской системы по каждому из направлений бизнеса и коэффициентов, уникальных для каждого из направлений и конкретного государства;
- подход усовершенствованных измерений (Advanced Approach) – основан на внутренней методологии оценки рисков банка в соответствии с предписанными стандартами.

Использование стандартизованного подхода или подхода усовершенствованных измерений позволяет резервировать меньше средств на покрытие операционных рисков, но при этом, чтобы использовать эти два подхода, в организации должна быть построена инфраструктура управления операционными рисками, которая включает процессы выявления, оценки, мониторинга и снижения операционных рисков.

J.I.: Как можно использовать подход по расчету операционных рисков, который уже сложился в организации, в качестве основы для расчета рисков прерывания бизнес-процессов в случае наступления ЧС?

В.Ж.: Управление рисками прерывания бизнес-процессов в случае наступления ЧС возможно осуществлять в рамках имеющейся инфраструктуры управления операционными рисками, поскольку негативные события и ущерб, возникающие вследствие ЧС, относятся к категориям операционного риска, определяемого соглашением BASEL II. Например, к таким категориям относят-

ся потери, связанные с утратой или повреждением ресурсов в связи со стихийными бедствиями или иными событиями, а также потери, связанные со сбоями в бизнесе или отказом систем.

J.I.: ЦБ РФ трактует обеспечение непрерывности бизнеса именно как меру снижения операционных рисков. Как Вы видете реализацию данной идеи на практике?

В.Ж.: Это, в первую очередь, отражается на организационной (ролевой) структуре организации. В большинстве случаев ответственность за управление непрерывностью бизнеса имеет смысл делегировать подразделению, отвечающему за управление операционными рисками.

J.I.: На ваш взгляд, как эксперта в области бизнес-аналитики, какие первые шаги должна предпринять кредитная организация, чтобы понять, сколько средств может быть затрачено на реализацию Плана обеспечения непрерывности бизнеса? Как провести расчет возврата инвестиций при реализации подобного рода проектов?

В.Ж.: В общем случае работу можно разделить на два основных этапа. На первом этапе организацией разрабатывается и внедряется методология управления операционными рисками, обеспечивается ее эффективность с точки зрения выявления операционных рисков в различных областях. На втором этапе, после того, как организация научится выявлять операционные риски, она может приступать ко второму этапу, на котором собственно и происходит их снижение.

Эффект от внедрения инфраструктуры управления операционными рисками может быть достаточно точно оценен после окончания первого этапа, который часто выполняется в виде пилотного проекта в ограниченной области.

НАШИ ПРОЕКТЫ

Приведение процессинговых систем ЗАО «Компания объединенных кредитных карточек» в соответствие с требованиями PCI DSS

О заказчике

ЗАО «Компания объединенных кредитных карточек» (UCS) — крупнейшая в России процессинговая компания, основные бизнес-направления которой включают эмиссию и эквайринг пластиковых карт таких международных платежных систем, как VISA International, MasterCard Worldwide, Diners Club International, JCB International. Широкая линейка решений, которые сегодня предлагает компания, тесно связана с процессингом кредитных карт. Компания является одним из лидеров рынка более 30 лет. Преимущества UCS, как специализированного процессора, позволяют оказывать наиболее качественный и полный сервис всем клиентам, для которых выпуск или прием карт в оплату является стратегически важным.

Задачи проекта

Стандарт PCI DSS разработан в целях повышения уровня обеспечения безопасности в индустрии платежных карт и сформулирован в 12 требованиях. Организации, которые производят обработку и хранение информации о держателях платежных карт и работают с международными платежными системами, должны каждый год подтверждать соответствие защищенности своих платежных систем требованиям стандарта PCI DSS.

Когда международные платежные системы обязали своих клиентов соответствовать требованиям стандарта PCI DSS, направленным на повышение уровня обеспечения безопасности клиентских данных, компания UCS одной из первых начала вести работу по усовершенствованию систем информационной безопасности. Руководство компании приняло решение о приведении процессинговой системы в соответствие с требованиями стандарта PCI DSS.

Несоответствие требованиям стандарта наблюдалось по следующим параметрам:

- отсутствие некоторых средств защиты информации, требуемых PCI DSS;
- отсутствие возможности реализации требований Стандарта техническими средствами;
- недостаточная документированность процессов управления информационной безопасностью.

Исполнителем проекта была выбрана компания «Инфосистемы Джет» — одна из немногих, обладающих необходимыми для проведения аудита на соответствие PCI DSS статусами Qualified Security Assessor (QSA, для аудита) и Approved Scanning Vendor (ASV, для сканирования сети), а также практическим опытом.

Кроме того, у компаний уже был опыт успешной совместной работы — крупный проект по построению дата-центра «под ключ».

Решение

Работа над проектом строилась в три этапа: первоначальный анализ соответствия требованиям стандарта, устранение несоответствий и внедрение необходимых организационно-технических мер защиты, сертификационный аудит.

Первый этап проекта включал в себя предварительную экспертизу процессинговых систем компании UCS. Были обследованы ИТ-система, технологические и бизнес-процессы компании, а также их взаимодействие.

Игорь Ляпунов, начальник Центра информационной безопасности компании «Инфосистемы Джет», подчеркнул: «Мы провели полномасштабное обследование, которое потребовало большого количества ресурсов, в том числе, человеческих. Мы собрали огромное количество данных, опросили не один десяток сотрудников, согласовали полученные данные — таким образом мы собрали всю необходимую информацию для второго этапа».

Обследование выявило несколько несоответствий требованиям стандарта PCI DSS, например, существовала проблема с внесением изменений в платежную систему — был высок риск нарушений в ее работе. Поэтому в рекомендациях по устранению несоответствий были учтены и эти моменты. По рекомендациям был разработан

план приведения в соответствие, содержащий конкретные действия по удовлетворению всех требований.

Второй этап начался с анализа рисков в работе ИТ-инфраструктуры, препятствующих выполнению некоторых требований стандарта PCI DSS. По результатам анализа консультанты компании «Инфосистемы Джет» предложили ряд компенсирующих мер. Эти меры позволили удовлетворить требования PCI DSS, а также сократить затраты заказчика, не уменьшив уровень безопасности.

В рамках второго этапа специалисты компании «Инфосистемы Джет» выполнили проектирование и внедрение комплекса организационных и технических решений для защиты данных о держателях платежных карт. Они разработали необходимую документацию, выполнили внедрение процессов управления информационной безопасности, требуемых стандартом: процессы управления рисками, инцидентами и уязвимостями. Был реализован ряд технических решений, требуемых PCI DSS, либо выступающих в качестве компенсирующих мер:

- внедрена система обнаружения вторжений;
- создана система сквозного мониторинга событий ИБ;
- создана система контроля целостности на всех этапах работы с данными;
- проведена сетевая сегментация;
- внедрен процесс управления инцидентами.

Особое внимание было уделено решениям по управлению доступом к информации и информационным ресурсам.

Многие действия приходилось выполнять «по-живому» — без остановки даже отдельных компонентов — ведь работу процессингового центра остановить нельзя.

Дмитрий Сидоров, директор Дирекции ИТ UCS, заметил: «Мы пользовались технологией параллельных решений, когда новый процесс внедрялся параллельно со старым, велась верификация результатов старого и нового процессов, и если результаты верификации совпадали, то новый процесс уже внедрялся на место старого. Ни одного серьезного сбоя не было».

При реализации проектов, затрагивающих изменение привычных для пользователей бизнес-процессов, очень важным аспектом является работа с коллективом, особенно участие руководства компании-заказчика в проекте, донесение и разъяснение сотрудникам важности и необходимости такой перестройки. Руководство UCS принимало активное участие в проекте, что во многом способствовало сплочению коллектива и скорейшему разрешению любых проблем.

Третий этап проекта — проведение независимого аудита на соответствие требованиям стандарта PCI DSS — был выполнен отдельной командой сертифицированных специалистов компании «Инфосистемы Джет». Аудиторы заполняли анкеты, проводили интервью, проверяли внутренние документы компании и настройки средств защиты информации. По итогам аудита было дано подтверждение соответствия процессингового центра компании UCS требованиям стандарта PCI DSS.

Результат

Отчет о проведенном аудите был отправлен экспертам компаний VISA и MasterCard, которые подтвердили статус соответствия компании UCS международному стандарту PCI DSS.

Компания «КОКК» (UCS) одной из первых в Российской Федерации получила сертификат соответствия, свидетельствующий о полном выполнении требований последней версии стандарта PCI DSS 1.2.

Теперь «КОКК» отвечает постоянно растущему уровню требований клиентов и партнеров, а также может свободно оперировать на западном рынке.

Более того, требования стандарта PCI DSS во многом пересекаются с требованиями СТО БР и «Закона о персональных данных», которому должны соответствовать все организации, обрабатывающие персональные данные. Поэтому некоторые внедренные организационные и технические меры также помогают выполнению требований ФЗ-152 и стандарта СТО БР, а главное, обеспечивают реальную защиту клиентских данных.

Дмитрий Сидоров, директор Дирекции ИТ ЗАО «Компания объединенных кредитных карточек»(UCS): «Сертификат на соответствие требованиям стандарта PCI DSS подтверждает высокий уровень защиты персональных данных в нашей компании. Он дает большие преимущества нам и, что еще более важно, — нашим клиентам. Среди них много крупных банков, каждый из которых может пойти по собственному пути развития бизнеса. И мы, в свою очередь, готовы сопровождать их на всех этапах. Например, теперь мы можем осуществлять полный аутсорсинг базы счетов банка, будучи уверенными в безопасности нашей процессинговой системы. Специалисты компании «Инфосистемы Джет» помогли нам достичь согласия с требованиями стандарта, и мы готовы рекомендовать их как экспертов высочайшего уровня».

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