Гонки по вертикали информационной безопасности

Ведущая темы
Галина БОЛЬШОВА

В Новый год принято говорить о приятном: о елке, о Деде Морозе... Мы традицию не нарушим. Только наша елка – это вертикаль (нет, не власти, упаси Бог!) рынка, на которой разместились отрасли экономики. А Дед Мороз – безусловно, Банк России, который преподнес (правда, лишь для «своих») новый стандарт по информационной безопасности (ИБ). Надеемся, что и подарок «ИКС» (как бы от Снегурочки) в виде небольшого исследования рынка вас не огорчит.

Энергетика, кредитно-финансовый сектор, транспорт, нефтегаз, телеком, торговля... Оказалось, что пользователям ИБ «всегда чего-то не хватает» для полного счастья. Нет, не «зимою – лета», а внимания руководства, денег на системы информбезопасности (СИБ), стандартов, норм и регламентов, совместимых продуктов, квалифицированных кадров. Однако передовиков все же удалось найти. Поэтому мы стали строить рейтинг правильных защитников не по отраслям, а по отдельным показателям и попытались дать общую картину внедрения СИБ на примерах лучших практик. И не беда, что таких пока немного, главное – они есть.

Известно, что построить СИБ, интегрированную с информсистемой компании, непросто, а цена вопроса может достигать заоблачных высот. Но можно и за разумные деньги. Не у всех получается? Посмотрите, как действуют те, чей девиз «Мы рождены, чтоб сказку сделать былью».

И наконец, нам удалось определить критерии, которым должен соответствовать системный интегратор.

Надеемся, что наше повествование окажется для читателя не менее поучительным, чем пушкинские «Повести Белкина», тем более что один из экспертов предпочел скрыть свое лицо за этим псевдонимом (как будто и мы «с Пушкиным на дружеской ноге»).

Невидимые миру слезы,
или Оценка по минимуму

Сознаюсь, представить хоть в какой-то мере реальную картину внедрения СИБ по «отраслям народного хозяйства» оказалось чрезвычайно сложно. Безопасность, и информационная в том числе, во все века отличалась конфиденциальностью. Не знаю, как в других странах, но в России «безопасники» особенно ревностно хранят свою тайну, пусть даже это и секрет Полишинеля.

Что мы оценивали

В первую очередь мы попытались выяснить, какие из отраслей наиболее ревностно относятся к подготовке кадров. Для этого мы запросили относительные данные по количеству прослушавших курсы ИБ у одного из наиболее популярных на российском рынке «просветителей» – Учебного центра «Информзащита». Данные относятся к 2006 г., но, по словам руководителя центра З. Поповой, статистика практически не менялась за все восемь лет существования УЦ.

Количество прослушавших курсы ИБ

Источник: Данные УЦ "Информзащита", 2006 г.

Для оценки состояния дел по отраслям мы выбрали на первый взгляд самые благополучные из них в части ИБ: банки, энергетику, связь, транспорт, а также нефтегазовый сектор и предприятия тяжелой промышленности. С помощью вопросов, сформулированных на основании созданного Банком России первого отраслевого стандарта по ИБ «Обеспечение ИБ организаций банковской системы РФ», конкретно – предложенной там модели зрелости процессов менеджмента ИБ организации, мы хотели выяснить, какому уровню зрелости соответствует СИБ «усредненной по отрасли» компании. Из более чем 20 запланированных респондентов – пользователей ИБ и системных интеграторов – на вопросы ответили немногим более половины (часть – анонимно).

Странно выглядит нежелание отраслевых компаний ответить на исключительно методические вопросы, никак не раскрывающие ни архитектуры, ни схемы, ни деталей построения СИБ: есть ли концепция и политика ИБ? как оценивается защищенность? регулярно ли проводится аудит ИБ? Неужели с этим все так плохо, что и сказать страшно? Утешает лишь одно – даже таких исследований не проводилось.

Как считали

По основным показателям зрелости в области ИБ доля каждой отрасли усреднялась по количеству респондентов. Степень доверия к полученным данным, независимо от вида деятельности компании и открытости респондента, была принята за единицу. Анализ критериев выбора СЗИ проводился для каждой выбранной отрасли. При этом все предпочтения (бренд, рекомендация интегратора и т.д.) нормировались. Аналогично оценивался и показатель ответственности за управление СИБ.

Оказалось, что практически во всех отраслях существуют внутренние административные документы по ИБ (инструкции, регламенты, разделы в трудовых соглашениях), а вот к сертификации ведомства относятся неоднозначно, предпочитая использовать сертифицированные продукты только при наличии обязательных для конкретного случая регламента или нормы закона. К сожалению, мало кто признавался, как производится оценка защищенности ИС и есть ли на это регламенты. А уж об аудите системы управления средствами информбезопасности (СУИБ) не удалось узнать ничего, будто и нет такового. Исключение составили лишь наши «лучшие практики».

Из стандарта «Обеспечение ИБ организаций банковской системы РФ»

Модель зрелости процессов менеджмента ИБ организации стандарта ЦБ основывается на определенной стандартом CobiT универсальной модели, которая устанавливает шесть уровней:

Нулевой – полное отсутствие процессов менеджмента ИБ в рамках деятельности организации. Организация не осознает существования проблем ИБ.

Первый («начальный») – наличие документально зафиксированных свидетельств осознания организацией существования проблем обеспечения ИБ. Однако используемые процессы менеджмента ИБ не стандартизованы, применяются эпизодически и бессистемно. Общий подход к менеджменту ИБ не выработан.

Второй («повторяемый») – проработаны процессы менеджмента ИБ до уровня, когда их выполнение обеспечивается различными людьми, решающими одну и ту же задачу. Однако отсутствуют регулярное обучение и тренировки по стандартным процедурам, а ответственность возложена на исполнителя. Руководство организации в значительной степени полагается на знания исполнителей, что влечет за собой высокую вероятность ошибок.

Третий («определенный») – процессы стандартизованы, документированы и доведены до персонала посредством обучения. Однако порядок использования данных процессов оставлен на усмотрение самого персонала. Это определяет вероятность отклонений от стандартных процедур, которые могут быть не выявлены. Применяемые процедуры неоптимальны и недостаточно современны, но являются отражением практики, используемой в организации.

Четвертый («управляемый») – обеспечиваются мониторинг и оценка соответствия используемых в организации процессов. При выявлении низкой эффективности реализуемых процессов менеджмента ИБ обеспечивается их оптимизация. Процессы менеджмента ИБ находятся в стадии непрерывного совершенствования и основываются на хорошей практике. Средства автоматизации менеджмента ИБ используются частично и в ограниченном объеме.

Пятый («оптимизированный») – процессы менеджмента ИБ проработаны до уровня лучшей практики, основанной на результатах непрерывного совершенствования и сравнения уровня зрелости относительно других организаций. Защитные меры в организации используются комплексно, обеспечивая основу совершенствования процессов менеджмента ИБ. Организация способна к быстрой адаптации при изменениях в окружении и бизнесе.

Увы, выборка оказалась не самой представительной, но определенные выводы сделать позволяет. Тем более что результаты эти не идут вразрез с мнением большинства экспертов (за исключением, пожалуй, позиции Ивана Белкина), которые согласились проанализировать состояние дел с ИБ на вертикальных рынках. ИКС

Повести о «вертикальной» безопасности

Иван Петрович БЕЛКИН

Темные предания гласят, что некогда Горюхино было село богатое и обширное…
В то время все покупали дешево и продавали дорого…
А.С. Пушкин «История села Горюхина»

Ведомственная ментальность, некогда помогавшая отечественным отраслевым структурам побеждать в соцсоревнованиях и двигать советскую науку, в годы перестройки вдруг повернулась ко многим из них неприглядной стороной. В условиях свободного экономического плавания самодостаточность министерств и их региональных «княжеств» оказалась мнимой. Особенно в области ИТ и служб информационной безопасности, для которых тема разбитого корыта и латания дыр остается актуальной уже много лет. И тут есть над чем задуматься…

Абсолютно защищенных систем не бывает, можно говорить только об относительных показателях СИБ, причем по причине конфиденциальности этих сведений в открытой печати приличествует обсуждать лишь уровень зрелости предприятия. В качестве оценочного используем отечественный критерий – модель зрелости СИБ компании, описанную в стандарте Банка России (см. выше).

Признаки или призраки?

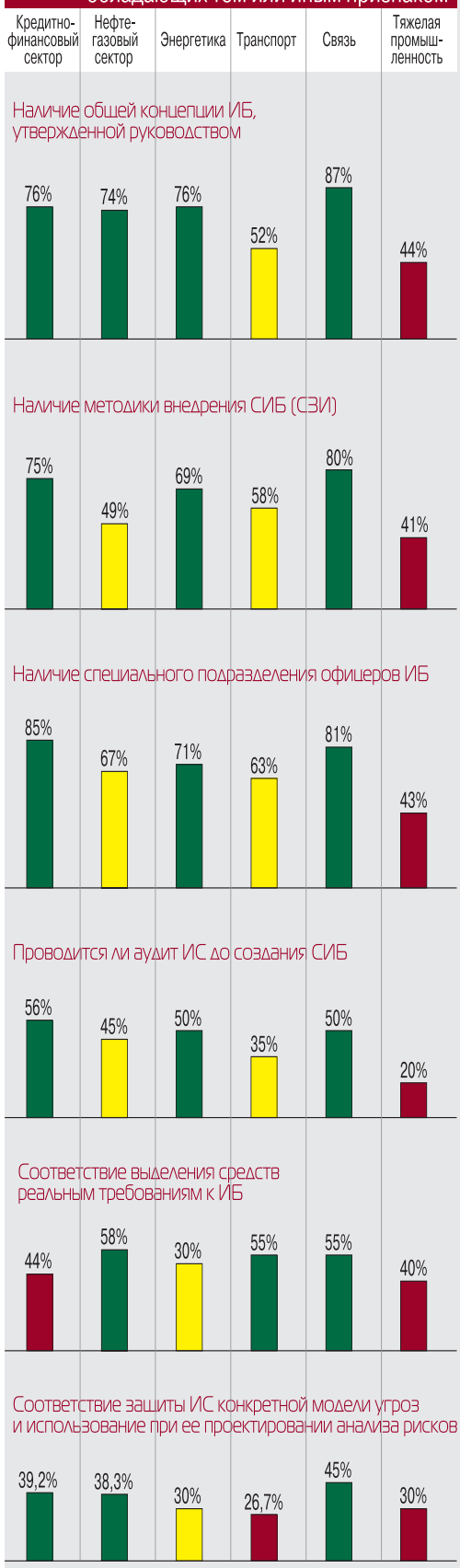
Принято считать, что о выходе организации на «взрослый» уровень по ИБ свидетельствует по меньшей мере наличие концепции и политик безопасности. Вообще же таких признаков гораздо больше.

Концепция как необходимый признак ИБ слабо сказывается на динамике создания законченных вертикальных решений (защищенных «как надо» ведомств, похоже, пока не

Вертикаль информационной безопасности

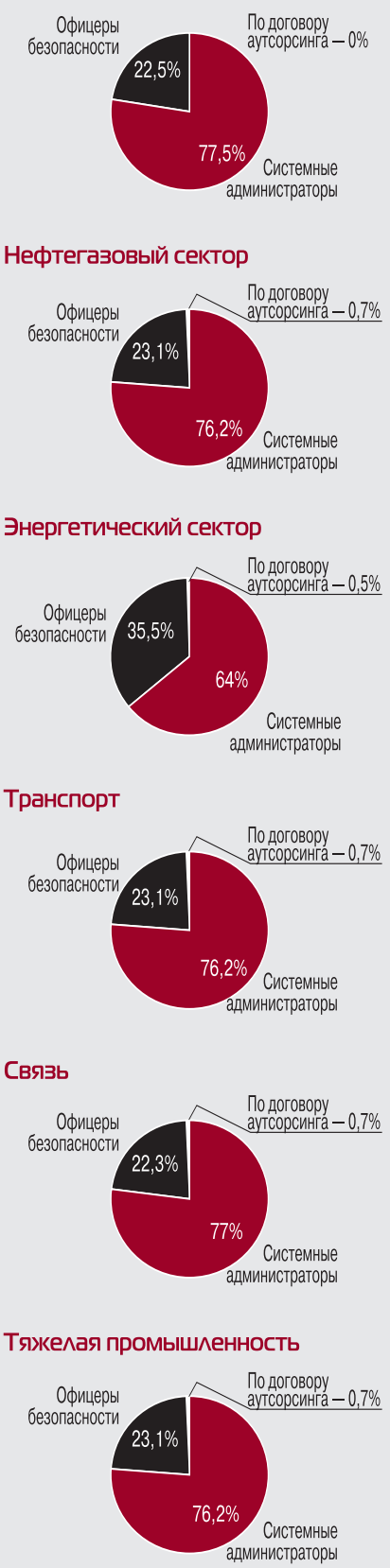
Оценка по минимуму

Доли компаний отрасли, обладающих тем или иным признаком



Что бралось за основу при подборе технических средств

Кто осуществляет управление СИБ



Источник: опрос "ИКС"

существует). Достаточным условием успеха может стать четкая реализация политик.

Увертюра «Связьинвеста». Когда у исторических операторов не было единой структуры, каждый из них при выборе ИТ-решений и СЗИ ориентировался на свой бюджет и свои представления о моделях угроз и нарушителей. Соответственно, и ориентиры (где, почем и что купить) существенно разнились. В итоге к моменту отраслевого объединения хозяйства ИБ региональных «княжеств» зачастую не поддавались интеграции.

Тем не менее в 2001–2002 гг., после опубликования «Доктрины информационной безопасности», именно «Связьинвест» разработал, возможно, первую в России концепцию ИБ – внятную и лаконичную. Начав реализацию программы, холдинг надолго закрепил за собой репутацию прогрессивной ведомственной структуры. Неизвестно, правда, доведено ли это начинание до логического конца. Реструктуризация создала препятствия для воплощения планов: команда меняется, и наследование созданного пока неочевидно.

Частично концепцию ИБ реализовали «Северо-Западный Телеком», «Уралсвязьинформ» и «Дальсвязь», и то в разной степени приближенности к СИБ, а целостной системы защиты информации так и не создано. Что уж говорить о тех предприятиях и ведомствах, которые озаботились проблемой недавно.

Будь то объединение СЗИ или «достройка» СИБ плюс внедрение новых СЗИ и их интеграция с действующими – задачи далеко не тривиальные. Да и каждое СЗИ не столь эффективно, как это утверждают производители и «независимые» интеграторы. Если первые вполне логично (с точки зрения конкуренции) нахваливают себя и сулят тотальную защищенность с помощью именно своего продукта, то вторые вынуждены идти на поводу у поставщиков, не имея времени и квалифицированных кадров, чтобы подобрать нужные конкретному заказчику СЗИ и интегрировать их в информационную систему. Многие российские интеграторы еще и «грешат» собственным производством СЗИ, которые редко сопрягаются с компонентами мультивендорных ИС. Еще одной опасной тенденцией становится использование только тех продуктов защиты информации, которые приносят прибыль не менее некоторого порогового значения.

Если на предприятии изначально СЗИ внедрялись разными специалистами и только потом интегратор написал концепцию, то ее реализация будет, мягко говоря, далеко не однозначной. Конечно, при построении системы безопасности сети можно ставить некие «реперные» точки с помощью аудита. Сегодня в России активно рекламируют фактически одну методику аудита (BS7799) две компании – KPMG и BSI, причем последняя появилась на нашем рынке всего год назад. Как провести аудит одной компании – понятно, но кто возьмется полностью отработать ведомство? Невозможно описать всю информационную систему таких колоссов, как «Газпром», Пенсионный фонд или РЖД. Только на инвентаризацию может уйти не меньше 3–5 лет. А уж если глубоко исследовать ее на степень защищенности... Вот и приходится гигантам включать на максимум проверенные годами механизмы оргмер.

Правда, есть и «правильные» ведомства, например РАО ЕЭС и Федеральная таможенная служба, где информационно-технологический порядок на каком-то базовом уровне наведен. А вот в банковской сфере (вопреки расхожему мнению, что там все хорошо) только началось движение по выполнению требований стандарта ЦБ, которые не обязательны, однако рекомендованы к исполнению.

Приходится с сожалением констатировать, что в глобальном масштабе картина с отраслевыми концепциями ИБ аналогична состоянию дел в «Связьинвесте». Наличия концепции и регламентов ИБ явно недостаточно для того, чтобы считать конкретное ведомство зрелым в области ИБ. Настоящая работа по созданию защищенных систем начинается с законодательной, нормативно-правовой, регламентирующей информации, организационных мер, технических средств защиты и применяемых технологий, построения комплексных систем. Задача чрезвычайно сложная, и каждое ведомство решает ее с разными продуктами, людьми, подходами, СЗИ и СКЗИ. И разными темпами: где-то все упирается в нехватку денег, где-то – в недостаток политической воли.

Движители прогресса

С нормативно-правовой точки зрения дела в нашей стране не слишком радужные, хотя некоторый прогресс наблюдается. Технический стандарт создается. Гигантская работа ФСТЭК дала свои плоды: с 2004 г. действуют «Специальные технические требования к защите», ГОСТ Р 15408. Технических регламентов, правда, нет (и неизвестно, когда появятся). У нас модно поручить разработку документа сначала одному ведомству, а затем передать другому, которое все пересматривает. Теперь вот Мининформсвязи разрабатывает концепцию по техническим регламентам...

Лирическое отступление в банковскую сферу

Если завелся миллион рублей, то куда бы вы его ни понесли – нет гарантии, что информация не появится на CD в Митино. И хотя СИБ, например, ЦБ или Сбербанка вполне удовлетворительны, 100%-ной гарантии конфиденциальности никто не даст.

Большинство организаций выходит из положения благодаря оргмерам, да еще у многих имеются собственные сети передачи данных, операторы и выделенные каналы. Предприятие не допускает никого извне. Тем не менее инциденты весьма вероятны, некоторые даже выплескиваются на страницы СМИ, хотя кредитно-финансовый сектор более других склонен их замалчивать.

Судить о степени защищенности должны эксперты высокого уровня, с практикой аудита конкретного ведомства. Сообщений о подобных исследованиях в открытой печати пока нет.

Но все же главное – выделение бюджетов на цели ИБ, в первую очередь для госорганизаций. Если не будет централизованного и регламентированного финансирования с прозрачными механизмами проверок исполнения бюджета, не будет и реальной работы. Увы, в масштабе страны все зависит от оперативной ситуации, а чаще действуют по известному принципу – пока гром не грянет, мужик не перекрестится. Средства выделяются для Федеральной таможенной службы и Пенсионного фонда, для проектов СИБ в РАО ЕЭС и Минфине (но никто не застрахован от того, что выделенные ему средства не перебросят другому ведомству). Относительно благополучно с финансированием в нефтегазовой отрасли, поскольку там структуры коммер-

ческие или полукоммерческие, им есть что защищать. Многие предприятия имеют действующие внутренние стандарты ИС (как, например, «Лукойл»).

Практически во всех телекомах (как и на предприятиях тяжелой промышленности) состояние дел очень сильно зависит от «доброй воли» руководства и осознания им важности системы безопасности сети: зрелость СИБ определяется склонностью руководства к ИТ. Достаточно сказать, что операторов, внедривших, например, Fraud Control или средства защиты SS7, – единицы. А ведь от воровства трафика страдают практически все крупные операторы.

Отрасли, которые стремятся на мировой рынок, вынуждены готовиться к вступлению в ВТО. Именно этот факт часто определяет «правильную» стратегию в области ИБ. Но и там есть ведомства, принципиально не готовые, например, к внешним аудитам.

Авангард защитников

Если рассматривать средства защиты с точки зрения их интегрированности между собой и с информсистемой компании, управляемости системы ИБ в целом, то однозначно проранжировать ведомства не представляется возможным. Причина – в закрытости информации и разного рода реорганизациях, которые «накатывают» на ведомства с завидной для регламента СИБ регулярностью.

Среди передовиков в сфере информационных технологий и их безопасности, а также их интеграции – РАО ЕЭС. В кредитно-финансовом секторе с интеграцией откровенно плохо: типичная для отрасли ИС никак не связана с системами защиты и безопасности информации, управляется непонятно как и автономно от общей СУИБ. Зато со стандартизацией все в порядке. Стандарт ЦБ – надежда «безопасников» отрасли. Когда (и если) он будет достроен и начнет работать, появятся интегрированные решения. Главное – отраслевой стандарт позволил осознать, что помимо внутреннего аудита каждое кредитно-финансовое учреждение обязано проходить внешний аудит на информбезопасность.

В телекомах о внешнем аудите ИБ вообще не помышляют. Но передовики по защите сетевой информации имеются, среди них – «ВымпелКом» (в первую очередь с точки зрения кадров и менеджеров, принимающих решение). Руководитель службы ИБ этого оператора – один из положительных примеров обеспечения средств, наличия доброй воли и понимания важности ИБ. Как следствие проводится взвешенная политика создания СИБ, закупки ведутся с позиции необходимости средств защиты информации и ответственности перед акционерами.

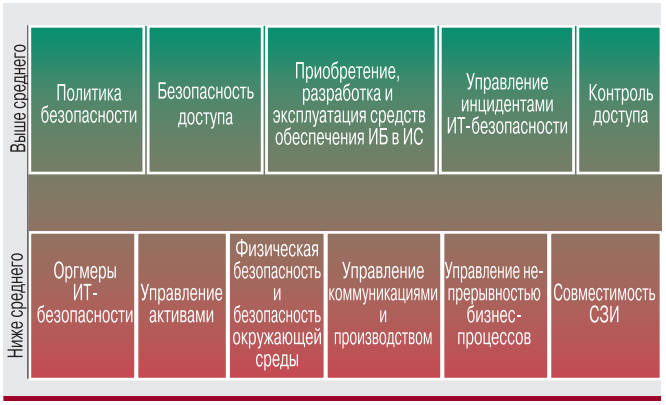
В «империи» МТС тоже отличные кадры «айтишников» и «безопасников», но их гораздо меньше – для последовательной политики в области ИБ просто не хватает ресурсов.

Из иных операторов, кроме уже упомянутых МРК, выделить некого. В отстающих – большинство: не хватает средств, а возможно, и воли. Повторю: в данном вопросе руководящие кадры решают всё. Хотя бывают ситуации, когда отдел ИБ возглавляет умный и квалифицированный специалист, но бюджетом-то распоряжается не он.

Взвешенная политика у руководства РЖД: СИБ там создается уже года два. И хотя выделяемые средства явно не поспевают за темпами строительства, ведомство далеко не в арьергарде. Благодаря неуклонному повышению компетентности специалистов (главное – руководства!) почти не осталось организаций, которые предпочитают выделять на безопасность сетей крохи (лишь на отдельные средства защиты типа антивирусов или межсетевых экранов).

Итак, подведем скромные итоги, не претендуя на их неоспоримость, поскольку и точных данных о ведомственных СИБ невозможно получить, и четких критериев оценки реальной защищенности или развитости СИБ нет. На текущий момент вырисовывается двойка лидеров: Федеральная таможенная служба и РАО ЕЭС. За ними следуют середнячки: ФНС, Пенсионный фонд, телекоммуникации,

Уровень соответствия СИБ международным стандартам



РАО «РЖД», нефтегазовая отрасль. И уж совсем в хвосте плетутся МВД, Федеральная служба земельного кадастра и все те, кто задачи по защите информации решает с помощью оргмер.

О вреде и пользе стандартизации и сертификации

Стандартами по информбезопасности мы не избалованы: ГОСТ 28147-89/Р 34.10-94/Р 34.11-94/Р 34.10-2001. Еще есть требования ФАПСИ к стойкости СКЗИ, ГОСТ Р 15408 «Общие критерии» и РД Гостехкомиссии. Негусто. Разговоры о том, чтобы разработать стандарт для СУИБ, ведутся годами – такое состояние дел и с сертификацией.

Дальше всех продвинулся процесс сертификации «на соответствие», а самая освоенная область – сертификация СЗИ по линии ФСТЭК. С одной стороны, это, безусловно, поможет заказчику определиться, приобретать сертифицированное решение или отказаться от него. С другой – степень доверия к сертификации по ТУ (в отсутствие соответствующего стандарта) падает с каждым днем, хотя сертификационные лаборатории честно проводят испытания на все заявленные производителем условия работы, и база сертифицированных решений дает заказчикам реальную возможность выбора.

Ясно, что насущная необходимость в сертификации СИБ есть, а развитой системы сертификации нет. Не доросли мы. Системы управления ИБ, которые создаются в ведомствах, делаются с чистого листа, а по сути – по зарубежным стандартам (например, ISO 17799). Государственных регламентирующих документов в этой области нет ни по отдельным ведомствам, ни по стране. Видимо, лишь стандарт ЦБ введет сертификацию на СУИБ.

Сила закона

Россия катастрофически отстает от развитых стран по многим направлениям законодательства. Например, в области электронной коммерции нет закона об электронной сделке, да и само понятие введено лишь в последней редакции «трехглавого» закона (ФЗ № 24 от 20.02.95 «Об информации, информационных технологиях и защите информации»). И такое бедственное положение во всем, поскольку существующие правовые акты не охватывают всех аспектов ИБ.

Нормативно-правовая база по информационной безопасности

- Доктрина информационной безопасности РФ
- ФЗ «О безопасности»
- ФЗ «О государственной тайне»
- ФЗ «О связи»
- ФЗ «Об информации, информационных технологиях и защите информации»
- ФЗ «О техническом регулировании»
- ФЗ «О лицензировании отдельных видов деятельности»
- ФЗ «Об участии в международном информационном обмене»
- ФЗ «О коммерческой тайне»
- ФЗ «О персональных данных»

Законодатели, видимо, и в будущем будут вынуждены принимать федеральные законы в сжатые сроки, когда этого потребует подписание различных международных соглашений. Но важные правовые акты, принятые в спешке, нуждаются в серьезной доработке, которая потом, как правило, тянется годами (вспомним закон об ЭЦП).

Ситуация не из легких, но светлое будущее проглядывается. Например, в этом году все же вышло два закона по ИБ («О персональных данных» и «трехглавый»), тогда как в прошлом – один («О коммерческой тайне»), а в позапрошлом – вообще ни одного.

Вместо заключения, или Извечное «что делать?»

Нельзя объять необъятное, нельзя сразу выстроить всеобъемлющий стандарт – задача непосильная даже для коллектива «яйцеголовых» из разных отраслей. Видимо, в наших условиях одно из возможных решений – принятие системы отраслевых стандартов. Ведь гораздо проще создать стандарт для предприятий одной отрасли, у которых много общих функций, а зачастую и параметров информационных потоков. Положительный опыт в России есть – «Газпром», который ведет работу в этом направлении.

Аттестацию на соответствие стандарту могли бы проводить лицензиаты ФСТЭК, которые так успешно проявили себя на ниве сертификации по ТУ. Тем более что для многих отраслей путем естественного отбора сузился круг и потребителей, и поставщиков средств ИБ.

Вспомним сказку Льва Толстого, где отец велел сыну сломать веник. Трудно? А по веточке – совсем просто. Может, и нам будет легче «по веточкам», по вертикалям? ИКС

Повесть о свете без конца

Когда в нашей стране наступит «конец света», знает только РАО ЕЭС. Так вот, ответственные специалисты этого ведомства утверждают, что он не наступит никогда.

А. КАЗАЧКОВ,
главный специалист отдела ИБ департамента экономической безопасности и режима КЦ РАО «ЕЭС России»

Собственно информбезопасность – важнейший бизнес-процесс отрасли под названием «Энергетика и электрификация», у которого своя, весьма отличная от других отраслей специфика. Здесь существуют

Четыре уровня защиты информационных систем

- **Первый защищает информацию, используемую высшим менеджментом для управления холдингом.**
- **Второй – в системах управления технологическими процессами**, где риски особенно велики и получение несанкционированного управления теми или иными процессами или системами может создать критически опасную ситуацию. Именно поэтому в концепции ИБ, принятой в РАО ЕЭС, существует очень важный раздел «анализ рисков», в том числе и технологических.
- **Третий – защита ИС, используемых исполнительным аппаратом РАО ЕЭС.**
- **Четвертый – взаимодействие с ИС отраслевых предприятий.**

Поэтому и концепций ИБ в холдинге РАО ЕЭС несколько: общеотраслевая и по технологическим направлениям деятельности, специфичным для того или иного вида сервиса компании. Другими словами, одна концепция – для защиты инфокоммуникационных систем, другая – для систем диспетчеризации, третья – для систем управления связью и т.д.

В этом контексте в РАО ЕЭС различают информационно-телекоммуникационные системы (ИТКС), автоматизированные системы управления технологическими процессами (АСУТП), автоматизированные системы диспетчерского технологического управления (АСДТУ)... Информбезопасность в них строится по единым принципам, но с разной степенью защиты. Обрабатываемая информация подразделяется на открытую и отнесенную к коммерческой тайне РАО (к защите последней предъявляются самые высокие требования).

По каждой системе внедрены регламентирующие документы, а также регламенты взаимодействия подразделений и организаций при обеспечении работоспособности систем. Они сопровождают все ИС и ИТКС РАО ЕЭС, определяя технологические требования к ИС компаний холдинга и к тем, кто оказывает аутсорсинговые ИТ-услуги.

А вот информбезопасность на аутсорсинг не отдана. Это ключевой бизнес-процесс, поэтому система управления

всеми СЗИ должна находиться у владельца информации. Кроме того, в компании существует собственный удостоверяющий центр ЭЦП, издающий ключевую документацию и сертификаты, на основе которых осуществляется доступ ко всем информационным ресурсам холдинга. Управляют средствами и системами ИБ офицеры информбезопасности. Вместе с тем мы понимаем, что безопасность – прикладной бизнес-процесс, а потому стараемся помогать «айтишникам» в решении проблем, но... с учетом требований по безопасности. Такие взаимоотношения устраивают всех.

Сила – в единстве

Один из краеугольных камней реально работающей СИБ – тесное взаимодействие и взаимопонимание с ИТ-специалистами. В компании принято при любых внедрениях или модернизациях ИТКС не делить их на «твои» и «мои», а организовывать общий процесс разработки и внедрения при непосредственном участии специалистов по ИБ. Такая «мода» введена не приказным порядком – такова корпоративная культура, и во многом это заслуга руководителя ИТ-подразделения. Кроме того, в компании разработан очень важный документ «Политика информационной безопасности при создании, модернизации и внедрении информационно-телекоммуникационных систем».

«Политика...» не только сильно облегчает жизнь нам и «айтишникам», главное – она помогает потенциальным контрагентам, которые участвуют в конкурсах (тендерах) на создание систем, так как в ней подробно расписаны требования по ИБ ко всем видам применяемых в РАО решений. Очень удобно: прежде чем «взяться за гуж», внимательно изучи документ и тогда уж, если сможешь выполнить – берись, если нет – отойди в сторону.

Уровень системного интегрирования в области ИБ в среднем по рынку не очень высок. Здесь все намного сложнее, чем кажется на первый неискушенный взгляд, поэтому и требования к компании-интегратору высоки. Заказчики и интеграторы должны работать как единый механизм, отсюда и может черпаться сила.

Достойный интегратор не «толкает» свое решение. Он знает рынок и продает не только свое, но и чужое, по необходимости вступая в альянсы с нужными поставщиками. Задача интегратора – оценить предложения рынка, проанализировать результаты, а затем предлагать заказчику самые лучшие решения, причем зная, у кого и что лучше покупать (независимо от того, совместимы данные продукты с собственным творением интегратора или только между собой). Увы, сегодня почти каждый интегратор стремится продать (даже скорее продавить) свое решение.

Особый аспект – системная интеграция в области ИБ. Сейчас даже гранды, которым под силу поставлять технические решения и продавать технологии как таковые, отдают вопросы интеграции средств и решений по ИБ на подряд специализированным компаниям. Такой подход нас как потребителей устраивает полностью. Одно условие: компания-субподрядчик должна быть согласована с заказчиком – это очень важно!!! Практически все крупные системы создавались в РАО ЕЭС именно по такой схеме и по сию пору надежно работают.

Открытая или закрытая?

РАО «ЕЭС России» как юридическое лицо является акционерным обществом, а потому на нас (1) впрямую не распространяются жесткие требования по применению сертифицированных продуктов, (2) в сети не циркулирует информация, относящаяся к гостайне, наконец (3), все пользователи корпоративной сети имеют практически неограниченный доступ в Интернет, не лишены портов флоппи-дисков, модемов или флэшек.

Однако с учетом того, что РАО ЕЭС относится к стратегически важным отраслям страны, одним из главных условий использования СЗИ (и это записано в концепции ИБ) является наличие сертификата по требованиям безопасности. Кроме того, мы участвуем в подготовке ряда законопроектов, где будут определены требования по ИБ к критически важным отраслевым объектам.

Что же касается свободы доступа, то здесь все ограничения определяются политикой ИБ, а также пунктами трудового договора, где говорится о сохранности коммерческой тайны РАО. Средства и методы – в методиках и инструкциях. Причем далеко не каждому сотруднику «грозит» работа с конфиденциальной информацией, а если уж случилось, то никаких паролей – только токен и сертификат с установленными правами доступа. Доступ в Интернет – для всех без исключения, с каждого рабочего места (не надо стоять на пути прогресса!).

Однако такой подход не означает, что мы не знаем «кто, куда, зачем». Отдел ИБ следит за выполнением требований по безопасности с помощью мощной СУИБ, не заклеивая порты и не вынимая флоппи-дисководы. Для нарушителей есть административные меры воздействия. Кстати, судя по статистике, злоупотреблений немного. Вместе с тем техническая оснащенность и автоматизация СИБ и СУИБ такова, что действия администраторов безопасности незаметны для пользователей.

Единая СИБ не входит в состав ИТ-систем, а существует обособленно, не теряя при этом тесной связи с интегрированными подсистемами безопасности. Эти подсистемы, охватывая все приложения и ресурсы, невидимыми для пользователей нитями связаны с единой СУИБ. В последней предусмотрена возможность активного воздействия на ИС, но не наоборот!

Из истории безопасной энергетики

Системное внедрение средств информбезопасности началось примерно в 1998–1999 гг. Сегодня отдел ИБ структурно входит в департамент экономической безопасности и режима корпоративного центра и административно не связан с подразделением ИТ. У «безопасности» свой бюджет, однако отдел участвует в планировании денежных средств и для ИТ, т.е. финансируется ИБ не по остаточному принципу, а исходя из потребностей.

Правда, после окончания реструктуризации схема взаимодействия подразделений безопасности предприятий отрасли изменится – появились и еще будут появляться управляющие компании, но основные принципы создания, управления и организации СИБ сохранятся.

Это модное слово «стандарт»

Сегодня зарегистрирован единственный отраслевой стандарт по информбезопасности – Банка России. В энергетике такового вообще нет, есть отраслевой стандарт по ИТ, точнее, по информационному обмену, разработанный ИТ-департаментом с привлечением специалистов нашего отдела. Отрасль практически полностью реструктуризована, и теперь приходится общаться с множеством акционерных обществ. Поэтому, скорее всего, разработка такого стандарта, внедрение и исполнение его требований, на постреструктуризационном этапе будет полезна!

Существующего комплекта документов «для всей страны» вполне достаточно для того, чтобы грамотно организовать ИБ на предприятии. Конечно, у каждого крупного отраслевого предприятия – своя специфика. Но государство – не Бог, который дарует однозначные требования ко всем системам, базовые уже определены ФСТЭК, а в части криптографии – ФСБ.

> Государство – не Бог, который дарует однозначные требования ко всем системам

В основе любой системы защиты лежит анализ рисков и, как следствие, определение требований к средствам и методам защиты, системам аудита. А вот как их выполнить – зависит от профессионализма специалистов по ИБ. Особые требования предъявляются к реализации систем аудита и мероприятий по аудиту. Профессионал понимает, что нужен и внутренний, и внешний аудит ИС, только тогда можно говорить о достоверной защищенности системы.

Кстати, после изучения ISO 17799 и ISO 27001:2005 я пришел к выводу, что для нашей организации они, увы, практически неприменимы, столь специфичны наши требования. В бизнесе или банковской сфере – возможно, но в крупной компании, у которой огромное количество специализированных технологических систем, – вряд ли.

Решение нерешаемых задач

Проблемы глобального масштаба перед нашим подразделением не стоят. Кадры высококвалифицированные, технологии высокие, бюджет достаточный. А вот серьезные производственные задачи есть. Одна из них – внедрение системы защиты и разграничения доступа к информации корпоративного хранилища данных.

Дело в том, что в результате реструктуризации появилось большое количество компаний-акционерных обществ. Каждая из них использует информацию из корпоративного хранилища, вкладывает и извлекает ее. Работой хранилища занимается другая компания на условиях аутсорсинга. В такой ситуации важно, чтобы каждый мог сохранять собственную информацию, получать доступ к той, которая необходима, а что-то отдавать «в общий котел».

В такой непростой структуре мы должны обеспечить каждой компании защищенную работу с хранилищем, исключив возможность несанкционированного доступа к данным даже его администратора. Насколько мне известно, практической реализации такого решения пока не существует. В течение 2006 г. мы (вместе с компанией-интегратором) трудились над этой задачей, и небезуспешно. Надеюсь, что в 2007 г. решение будет реализовано на практике.

Вообще я убежден в прочности информзащиты систем РАО ЕЭС. По вине СИБ «конца света» точно не произойдет. ИКС

Повесть об отличном банке

ОТЛИЧНЫЙ. **1.** *от чего-кого.* Отличающийся, иной.
С.И. Ожегов, Н.Ю. Шведова. Толковый словарь русского языка.

Наш рассказ – не о каком-то мифическом или идеальном банке, а о вполне реальном кредитно-финансовом учреждении, которое, правда, по скромности избегает публичности, согласившись на изложение своей позиции без упоминания названия. А значение слова «отличный» оставим на суд читателей.

Итак, есть в городе N банк NNN, по делам своим немногим отличающийся от иных, но с особой информационно-безопасной судьбой. И первое отличие – руководство, которое, как известно, решает все. Поскольку начальство твердо знает, что циркулирующая по сетям и компьютерам NNN информация – главный капитал банка, специальное подразделение ИБ (в количестве более 20 профессионалов) не обделено ни заботой, ни вниманием и подчиняется напрямую первому лицу организации.

Второе, тоже существенное, отличие в том, что служба информбезопасности не входит в состав ИТ-отдела.

А еще у подразделения ИБ собственный бюджет, а отнюдь не финансирование по остаточному принципу (конечно, расходы на ИТ и ИБ взаимоувязаны, но пропорция соблюдается).

Заметим, что все эти «привилегии» находятся в полном соответствии с законами и нормативными актами нашей страны и отраслевым стандартом Банка России.

Первичное, вторичное и вечное

Как у всякого крупного банка, информсистема банка NNN как живой организм развивается, прирастает модулями и подсистемами. Одни модернизируются, другие отмирают. Но поскольку в NNN утверждены концепция ИБ и политика ИБ, любая разработка любой подсистемы или модуля ИС банка, начиная с ТЗ, согласовывается с подразделением информбезопасности. При любом внедрении (изменении) требования ИБ становятся в некотором смысле

> Информация, циркулирующая по сетям и компьютерам банка, – главный его капитал

столь же первичными, сколь собственно функционал модуля или подсистемы, а потому выполняются автоматически. На этом основании специалисты банка по ИБ считают, что интегрировать надо сам процесс внедрения, тогда и СИБ будет интегрированной.

Политика безопасности (концепция существует в виде отдельного документа) представляет собой совокупность внутренних нормативных актов (требования, инструкции, положения, регламенты, пункты в трудовых соглашениях), которые регламентируют все аспекты защиты информации, определяемые ЦБ и законами России. Отдел защиты информации полностью отслеживает эти направления – от обеспечения специальных условий для выделенных и защищаемых помещений до организации закрытых каналов связи, аттестации оборудования для обработки информации разных уровней секретности, вплоть до гостайны. В каждом филиале банка есть специалисты по ИБ, а в каждом бизнес-подразделении – администраторы ИБ (из работников, хорошо разбирающихся в ИТ и прослушавших курс по ИБ), которые занимаются защитой информации в своем подразделении с позиции собственников информации.

В NNN внедрена единая инфраструктура открытых ключей, действует распределенный удостоверяющий центр: центр сертификации в Москве и центры регистрации более чем в 70 городах страны. В полной мере представлено традиционное направление – защита информации при ее обработке (защита от НСД, межсетевые экраны, защита периметра, IDS и IPS, анализ ПО на уязвимости и недекларируемые возможности и т.п.). Аналитические исследования выполняются как сотрудниками отдела ИБ, так и сторонними организациями, уполномоченными проводить аттестацию продуктов. В 2007 г., в связи с принятием стандарта ЦБ, банк NNN начнет подготовку к сертификации СУИБ на соответствие требованиям ISO 27001.

Контроль ИС и СИБ (это уже из разряда вечного) также выполняется и собственными силами, и внешними аудиторами. Для периодических проверок есть внутренний регламент (не реже одного раза в год), предусмотрен аудит при изменении бизнес-процесса. Первый выполняется по наиболее «опасным» направлениям, второй более обширен, поскольку изменения могут повлиять на все информресурсы банка.

Контроль защищенности ИС – многоуровневый. Первый уровень обеспечивает служба внутреннего контроля (в банке существует управление внутреннего контроля с отделом аудита ИС). Второй – периодические проверки внешних аудиторов (в том числе международный аудит, проводимый компаниями KPMG, Ernst & Young и др.). Третий – периодические законодательно закрепленные проверки ЦБ. Четвертый – аудит «для имиджа», проверка нанятыми сторонними специализированными организациями.

При внедрении той или иной банковской технологии специальные риск-аналитики из отдела ИБ оценивают риски, возникающие в смежных бизнес-процессах, и рекомендуют способы их снижения. Эту работу вполне можно отнести к вечной, поскольку изменения в информсистемах происходят постоянно, в полном соответствии с громким словом «прогресс».

Почти по Дарвину, или О соответствии требований и возможностей

Безопасность – штука комплексная. Стоит упустить один момент, и вся деятельность станет бессмысленной. Поэтому в NNN при выборе средств и минимизации рисков, помимо неких стандартных требований нормативных документов, как правило, пользуются экспертными оценками собственных риск-аналитиков и специалистов по ИБ. Следовательно, и технические средства для СИБ подбираются на основании анализа технологии-кандидата на соответствие требованиям ИБ. Другой аспект выбора – системный подход. Выбираются те СЗИ, которые либо уже используются банком в других системах, либо известна практика их применения у коллег.

Внедрение технологий или подсистем почти всегда возлагается на системного интегратора, выбранного по результатам конкурса. Такая многоуровневая «селекция» позволяет добиться выполнения всех требований к устанавливаемым в ИС продуктам, модулям, подсистемам. А поскольку при проведении тендеров требования ИБ – одни из основных, то продукты без встроенных СЗИ просто не рассматриваются.

Правда, существуют интеграторы, которые пытаются сделать ИБ «фоновой темой». Здесь действует естественный отбор: банк остается с партнерами, которые внимательны к вопросам ИБ.

Проблемы глобальные, рабочие и мелочи

Специалисты по ИБ банка NNN насчитали у себя всего четыре глобальные и типичные проблемы, все остальные для них – уже мелочи.

Первая (правда, она уже решена в 2002 г.): пробивание у руководства решения о создании подразделения информбезопасности.

Вторая: подбор квалифицированных кадров. Учебные заведения, которые готовили специалистов до «эры капитализма», в значительной мере утратили свои позиции, а те, кто пытается занять эту нишу сейчас, увы, не способны обеспечить должное качество обучения.

Третья: выстраивание деловых взаимоотношений со службой ИТ. Без этого внедрение любой политики ИБ обречено на мучительный «прусский путь» – склоки, скандалы, разбирательства, подставы и т.д.

Наконец, **самая сложная и трудоемкая проблема**: внедрение политик ИБ в среде персонала собственной организации таким образом, чтобы они стали частью корпоративной культуры. Необходимо, чтобы нормативы соблюдались на деле, а для этого все должны понимать их нужность. Поэтому каждый приходящий на работу направляется на адаптационные курсы, где есть тематика ИБ и где сотруднику поясняют, что можно, чего нельзя. Обучают не только собственных сотрудников по отдельным углубленным целевым программам, но и сотрудников ИБ всех филиалов, администраторов ИБ подразделений. Проводят регулярные инструктажи на местах.

Все течет, все изменяется, или Нормы и требования в жизни банка

Хоть кредитно-финансовая отрасль и единственная, которая может похвастать своим отраслевым стандартом ИБ, общая нормативная база страны, по мнению специалистов NNN,

безусловно, нуждается в совершенствовании: «Если бы она полностью соответствовала требованиям к информбезопасности всех и вся, то не менялась бы. Но она постоянно корректируется». Отредактирован «трехглавый закон», внесены поправки в закон об ЭЦП, постоянно дорабатывается статья 26 ФЗ «О банках и банковской деятельности». Более того, не первый год перераспределяются функции между госорганами. Не стало ФАПСИ, часть функций ФСБ перешла к ФСО, Гостехкомиссия при Президенте преобразовалась во ФСТЭК...

Другой аспект – недостаточные знания чиновниками высоких технологий. Из-за непонимания нашими законодателями многих технических аспектов периодически возникают ляпсусы. Например, в области криптографии в свое время был выпущен нормативный акт, запрещающий ввоз на территорию страны шифровальных средств иностранного производства. А о том, что вся банковская система остановится, поскольку нельзя будет использовать S.W.I.F.T., никто не подумал.

Наносят урон и непросчитанные экономические эффекты. Так, до сих пор в России действуют ограничения на вывоз сертифицированных отечественных средств криптографии (даже в страны СНГ!). Это создает огромные трудности для любой организации, которая пытается расширить свою деятельность за пределы нашей отчизны.

Словом, не дай тебе Бог жить в эпоху перемен. Но, как сказал мудрец, и это проходит. А информационная безопасность остается. ИКС

Следует говорить не о совершенстве или несовершенстве законов, а о том, что разные госорганы никак не могут договориться друг с другом. Живой пример – технология открытых ключей. Когда стали развертывать такие инфраструктуры и удостоверяющие центры, был принят ФЗ № 128 от 08.08.01 «О лицензировании отдельных видов деятельности», где регламентировалась процедура выдачи сертификатов открытых ключей ЦБ. Но положение о порядке лицензирования за прошедшие годы так и не появилось. А все потому, что ведомства не смогли между собой договориться: никто не захотел взять на себя финансовую ответственность за деятельность удостоверяющих центров.

Сегодня выдача сертификатов открытых ключей не подлежит лицензированию.

Почти святочная история

История создания этой интегрированной СИБ вместила в себя и нелегкий выбор, и сложное сопряжение программ и устройств, и трудности организации единого управления. Но, как и положено святочному рассказу, у него счастливый конец.

А. ГРИЦИЕНКО,
начальник службы ИБ банка «Возрождение», к.т.н.

Банковское сообщество должно быть достаточно открытым – таково мнение руководства нашего банка, такова и моя позиция. Это дает возможность вкладчикам и инвесторам оценивать риски работы с каждым кредитным учреждением. Чем выше степень открытости, тем больше доверия.

Дорогу осилит идущий

В больших банковских мультисервисных сетях проблем с ИБ немало, одна из основных – организация защищенного доступа. Дело в том, что банки пользуются многими программными продуктами для решения задач разных направлений деятельности, а производители ПО, как это ни прискорбно, свои издержки производства принципиально снижают за счет ухудшения функционала механизмов защиты.

При внедрении, когда заказчик выдвигает требования по безопасности, встречное условие поставщика решения – доработка продукта за дополнительную цену. Кажется, все по Марксу: труд = стоимость. Однако наш печальный опыт показывает, что цена доработки практически у всех поставщиков ПО соизмерима со стоимостью самого продукта. А поскольку серьезных интеграторов в области ИБ единицы (мы имели дело с тремя), то их позиция вполне объяснима. Увы, таков механизм прибавочной стоимости в условиях недостаточно развитого рынка сервисов ИБ.

По нашим оценкам, издержки при внедрении СИБ в случае работы с системным интегратором чрезвычайно высоки. Главная проблема интеграции в области ИБ – индивидуальный подход для каждого продукта. Известный «пул» интеграторов имеет готовые решения, в которых с большим трудом удалось заставить работать совместно лишь несколько СЗИ. Это порождает скудость выбора средств ИБ. Вместо исследований рынка по требованиям заказчика и предложения зрелых продуктов или решений, совместимых с СЗИ, интеграторы предпочитают протолкнуть одну-две наработанные схемы, не задумываясь, насколько они отвечают требованиям заказчика.

Из исследованного нами списка поставщиков никто не смог предложить удовлетворительного решения ни по стоимости, ни по срокам исполнения (не менее 2 лет!), ни по функционалу. Они оказались не готовы построить систему

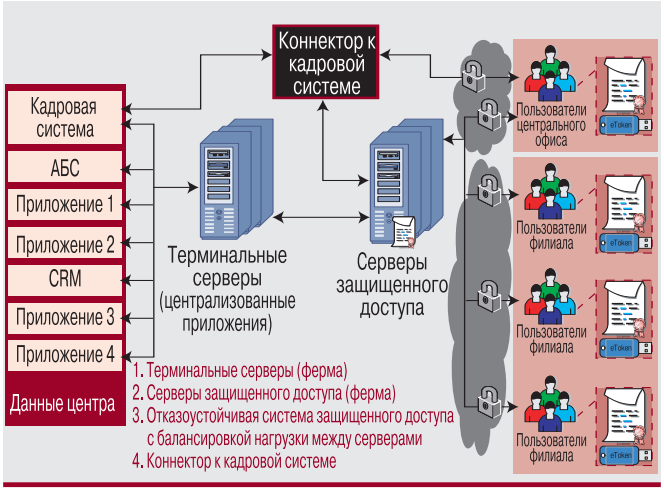
О масштабе системы

- ✓ У банка «Возрождение» – **60 филиалов**, в некоторых из них работают более 300 человек.
- ✓ Один только волгоградский филиал банка выпустил **100 тыс. банковских карт** (всего же в области действует 500 тыс. карт от 28 московских банков).
- ✓ Удостоверяющий центр банка выпустил в 2006 г. **20 тыс. сертификатов**.

управления 5 тысячами eToken, ключами и доступом в системы разных производителей, в том числе иностранных.

Интеграторы сейчас занимаются не системной интеграцией, а делают деньги, причем с возможно меньшими издержками (не в обиду будь сказано – «Дженерал Моторс» тоже делает не автомобили, а деньги). Бизнес есть бизнес – извлечь максимальную прибыль при минимальных накладных расходах. Если продукт, решение, услуга не удовлетворяют по цене – ищите дешевле. Вот мы ходили, ходили... В итоге решили самостоятельно строить систему защищенного доступа к централизованным ресурсам согласно требованиям безопасности.

Система защищенного доступа



Задача и требования нетривиальны. Чтобы интегрировать выбранные нами продукты с ИС банка и заставить всю цепочку работать прозрачно, пришлось самостоятельно дописывать большие блоки кодов – коннекторы к бизнес-приложениям. Разработали единую архитектуру, в которую встроили СЗИ и СКЗИ, серверы защищенного доступа с балансировкой нагрузки, написали практически свою систему управления и т.д. Реализация в какой-то мере типового масштабируемого решения для банка с разветвленной сетью филиалов заняла у нас ровно год. По сравнению с запросами интеграторов (цифра с семью знаками в американской валюте) цена реализации СИБ уменьшилась на один-два порядка.

Обеспечиваем защищенный доступ

Готового решения по управлению PKI для предприятия с разветвленной и территориально разнесенной структурой на рынке просто нет. Мы сами разработали систему защищенного доступа на основе оригинального алгоритма, обеспечивающего полный цикл управления аутентифицированным доступом к централизованным ресурсам.

Необходимость защиты передаваемых по открытым сетям данных и немалая клиентская база обусловили требование управления ключевыми контейнерами и носителями, а множество приложений и сред – управления паролями сотрудников. Изменение статуса и полномочий сотрудников надо было отслеживать в реальном масштабе времени. Основные требования: использование сертифицированных средств, централизованный контроль выпуска, приостановки и отзыва сертификатов (система полностью ориентирована на PKI), выработка и смена паролей, контроль из единого центра.

Предусмотрены сложные иерархические структуры правил доступа, а надежность и отказоустойчивость достигнуты путем многократного дублирования основных рабочих узлов системы. Функциональность системы наращивается за счет подключения новых модулей. Соединение с кадровой подсистемой с помощью коннектора автоматизирует процесс управления PKI инфраструктурой, паролями и ключевыми носителями.

Как только принимается новый сотрудник, администратору безопасности передается сообщение с требованием подключить новый eToken для автоматического оформления всех назначенных работнику пользовательских прав: генерируются пароли доступа к разрешенным приложениям, выполняются запросы на сертификаты, которые затем устанавливаются в ключевые контейнеры.

При переводе в другое подразделение в систему защищенного доступа через коннектор автоматически передаются данные обо всех изменениях пользовательских прав работника. Система автоматически отзывает ненужные права и сертификаты, создает новые. При увольнении она отзывает все сертификаты и права сотрудника, а на время его отпуска приостанавливает их действие. Во время командировок тоже полезно отслеживать места использования ключевых носителей.

Под сенью норм и стандартов

Сегодня система ИБ банка должна удовлетворять требованиям целого комплекса документов – международных, национальных, отраслевых. В кредитно-финансовой сфере по большей части есть все необходимое и по лицензированию видов деятельности, и по техзащите, и по средствам криптографии, и по защите вычислительной техники. Нормативная база России, в частности стандарт ЦБ (четвертая часть которого посвящена аудиту СИБ), гармонизирована с международными стандартами и соответствует требованиям к ИБ банков. Нет, к сожалению, единого подхода к информбезопасности в государственном масштабе.

Постановка задачи

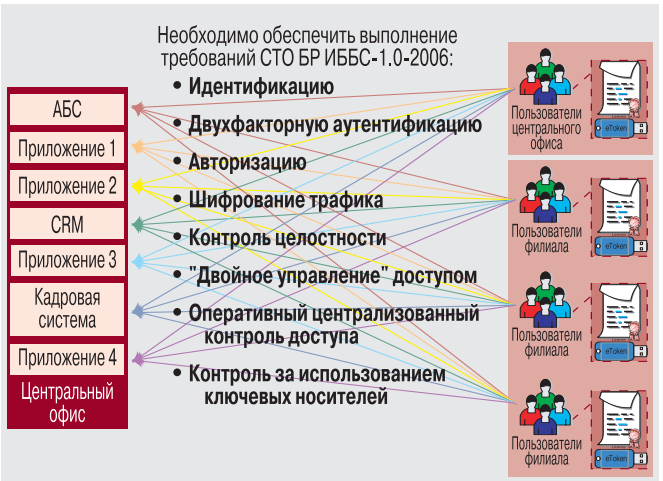
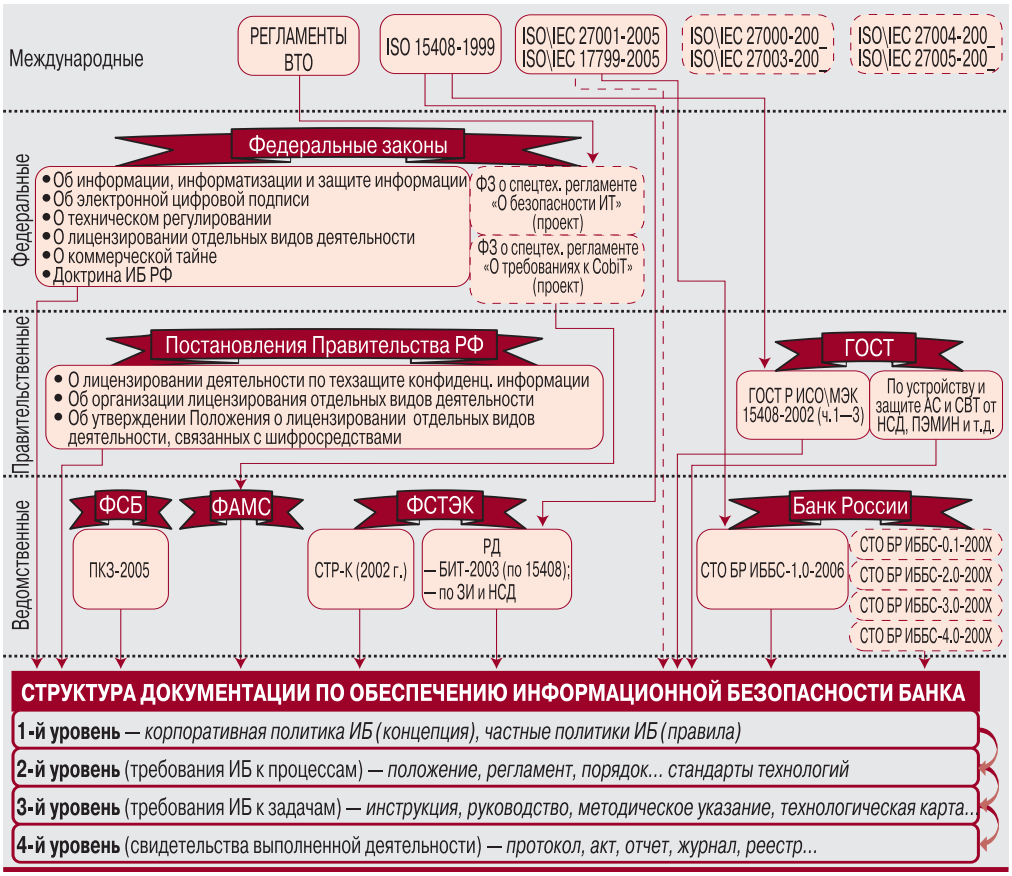


Рис. 3. Базовый набор требований к СИБ



Сколько у нас в стране ведомств занимается вопросами защиты информации? Тьма. А составить по их документам концепцию ИБ непросто, у каждого ведомства своя терминология. Наши собственные документы соответствуют действующим нормам и требованиям. Утверждены общая корпоративная политика информбезопасности и политики по отдельным направлениям, которые определяют руководство банком в области ИБ и деятельность подразделений. Требования для каждой частной политики прописаны в Положении о защите и безопасности информации в банке.

Подразделение ИБ в центральном офисе управляет системой ИБ, администраторы безопасности или главные специалисты по ИБ всех филиалов напрямую подчиняются своему управляющему. Таким образом, информбезопасность в нашем банке – часть производственного процесса, обеспечивающая необходимый функционал для различных бизнес-процессов. Наша СИБ живет в полном согласии с другими подсистемами ИС предприятия. В скором времени начнем ее сертификацию на соответствие требованиям ФСТЭК РФ, СУИБ тоже не забудем.

Вот такая история. ИКС

Интегральные оценки

Особенности национальной СИБ

Л. ФИСЕНКО,
ведущий специалист компании «Информзащита»

Без сомнения, защищать информацию и ИС необходимо, но... У кого-то ограничен бюджет или требуют обосновать эффективность потраченных денег. Кто-то выходит на международный рынок, что требует организации управления безопасностью (а это дополнительные траты). Над кем-то довлеют требования нормативов контролирующих органов. Поэтому все заметнее отрадная тенденция: защищать не любой ценой ради самой информации, а защищать бизнес в целом по принципу разумной достаточности.

Причины и стимулы

Несмотря на информационную шумиху вокруг проблемы защиты сетей, далеко не все компании созревают до внедрения СИБ, а уже существующие системы, за редким исключением, построены по лоскутному принципу: СЗИ внедряются бессистемно, в основном с учетом компетенции конкретных специалистов либо наличия на рынке продуктов. Доводы о важности анализа рисков лишь недавно начали завоевывать место под солнцем. Основными же аргументами в пользу внедрения тех или иных СЗИ, как правило, являются требования руководящих документов, международных или отраслевых требований и стандартов.

Увы, анализ рисков ИБ как поиск бизнес-процессов, уязвимых с точки зрения связанности с ИТ-инфраструктурой, в российских компаниях пока не прижился. Сыграло свою роль отсутствие в большинстве компаний культуры управления рисками, а кроме того, специализированные организации изначально оказывали эту услугу непрофессионально. Анализ опрометчиво сводился лишь к определению степени защищенности/уязвимости серверов без учета остальной инфраструктуры. Негативно сказалась и неопределенность критериев оценки рисков. В итоге анализ рисков стал инструментом обоснования внедрения СИБ, выгодного компании-подрядчику.

Таким образом, если отбросить такие побудительные причины, как популярный принцип «пока гром не грянет, мужик не перекрестится», а также не ставший естественным анализ рисков, то главным аргументом в пользу выбора средств для строительства СИБ оказываются некоторые требования норм, регламентов или законы РФ.

Нормы и рекомендации

На смену «морально устаревшим» руководящим документам для обеспечения ИБ приходят новые законы и стандарты, которые вызывают растерянность у игроков рынка либо своей неочевидной применимостью, либо отсутствием проработанной нормативной базы, чья цель пояснять и детализировать требования закона (пример тому – закон об ЭЦП).

Один из наиболее сбалансированных и жизнеспособных документов – внутриотраслевой стандарт Банка России по ИБ. Его последняя редакция (2006 г.) свидетельствует о явном намерении Центробанка сменить рекомендательный характер документа на обязательный статус. В других отраслях создание технических регламентов и отраслевых стандартов по ИБ – на стадии «прожектов». Будем надеяться, что национальные нормы по информбезопасности все же появятся, хотя гораздо больше надежд на ратификацию мировых стандартов.

Базовым ориентиром совершенствования СИБ для основной массы компаний до недавнего времени оставался ISO 17799. Документ аккумулировал опыт построения комплексных систем ИБ и их фрагментов, но не отвечал на вопрос: насколько это целесообразно для конкретной организации? Возможно, именно поэтому с энтузиазмом был встречен ISO 27001:2005, где приведены методики выбора защитных мер, адекватных рискам, за счет создания СУИБ. Впервые было определено, что в процесс управления системой ИБ должны быть вовлечены все сотрудники – от исполнителей до руководства компании. Если же организация стремится выйти на международный рынок, то она должна присматриваться еще и к международным нормативам.

Некоторые требования мирового рынка

- Акт Сарбейниса–Оксли (SOX) приводит методики внедрения механизмов внутреннего финансового контроля компании, необходимого для выхода на фондовый рынок США.
- Соглашение Basel II (планируется его применение в России в 2008–2009 гг.) регламентирует требования к признанным на мировом рынке кредитно-финансовым учреждениям и национальным банковским системам в целом.

Отраслевой срез

На наш взгляд, наиболее активные пользователи решений в области ИБ – кредитно-финансовая и телекоммуникационная отрасли, топливно-энергетический комплекс.

В **кредитно-финансовом секторе** активность обусловлена родом деятельности компаний: работа с деньгами и необходимость хранить финансовые секреты. Банковские структуры ставят во главу угла борьбу с инсайдерами, которые инициируют около 80% всех инцидентов в ИБ. Однако не забывают и про внешние угрозы – вирусы, спам, попытки несанкционированного доступа и т.д. Другая тенденция этого вертикального рынка – рост потребности в автоматизированных системах для ведения специального архива электронной корреспонденции, а также для расследования инцидентов.

Однако даже в этой отрасли (где денег на СИБ, как правило, не жалеют) есть определенные проблемы реализации эффективной СИБ, основная – дороговизна решения, особенно для небольших банков (менее 200 рабочих станций).

Принято также считать, что защита сетевой информации не приносит прибыли, а лишь обеспечивает непрерывность бизнес-процессов (вот оно – отсутствие анализа рисков и возможных потерь!). Кроме того, в отрасли редко встречаются СИБ, интегрированные в ИС компании, хотя чаще используются многофункциональные СЗИ или их комплексы, что обусловлено территориальной распределенностью и отсутствием на местах специалистов по ИБ.

Однако стандарт ЦБ сделал свое дело, и в преддверии его обязательности все больше кредитно-финансовых структур начинают создавать или модифицировать уже существующие СИБ согласно его требованиям.

Телекоммуникационный сектор намного менее развит в части стандартизации. Компании пока сами себе регуляторы. Сегодня типовой угрозой сети оператора считаются атаки типа DoS (отказ в обслуживании), многие задумываются о спаме, несанкционированном доступе и прочих внешних угрозах сети. И хотя компании рассматривают СИБ как один из бизнес-процессов, в ближайшем будущем им придется переосмыслить свой подход к ИБ. После вступления в силу ФЗ «О персональных данных» к компаниям будут предъявляться особенно жесткие требования по сбору и обработке приватных записей. Тем более что основной угрозой здесь считаются инсайдеры.

Телекоммуникационные же компании, планирующие выход во внешний мир, должны придерживаться международных требований к ИБ. В частности, в соответствии с Директивой о сохранении данных, принятой Евросоюзом в конце 2005 г., все данные, передаваемые по электронным каналам связи, должны храниться в течение года.

Топливно-энергетический комплекс, получая баснословные сверхприбыли, может позволить себе СИБ любого масштаба и сложности. При наличии целого ряда непрерывных технологических процессов их нарушение (как и работы ИС) может нанести серьезный экономический, физический и экологический ущерб и предприятию, и окружающей среде. Поэтому вопросы защиты инфраструктур предприятий рассматриваются на государственном уровне.

Особое значение придается безопасности инфраструктуры в контексте террористической угрозы и возможных крупномасштабных аварий. И хотя фактически от компа-

ний не требуют соблюдения стандартов ИБ (разве что регламенты работы с информацией государственной важности) даже на международном уровне, ИС этих предприятий наиболее защищены, особенно от внешних атак. Традиционно они закрыты для доступа извне.

Общая картина обеспечения информбезопасности в российских компаниях рассмотренных отраслей не выглядит удручающей, хотя и далека от идеальной. Однако, как правило, процесс напоминает латание дыр. Лишь немногие компании имеют СИБ, функционирующую как бизнес-процесс. Далеко не все могут позволить себе эффективную систему, которая требует значительных финансовых и человеческих ресурсов.

Есть два варианта разрешения проблемы. Первый: компаниям-подрядчикам, оказывающим услуги в области ИБ, следовало бы предлагать наряду с дорогими и доступные решения, адаптированные к конкретным требованиям. Второй: использовать услуги по аутсорсингу ИБ. ИКС

«Интегральная» вертикаль

Взгляд на «вертикаль ИБ» любого специалиста в этой области достаточно субъективен. Он зависит не только от сферы его профессиональных интересов или конкретных рынков, с которыми его компания ведет бизнес, но и от «горизонтальной» составляющей – масштаба компании-заказчика, стоимости проекта. Может сложиться впечатление, что у богатых клиентов дела обстоят хорошо. Однако далеко не всегда объем инвестиций свидетельствует о благополучии в области ИБ.

И. КАМОЛОВ, замдиректора департамента системной интеграции Корпорации ЮНИ

С. РЯБКО, гендиректор «С-Терра СиЭсПи».

М. ЛЕВАШОВ, куратор вопросов защиты информации в службе автоматизированных систем МГТС

«ИКС»: Ваш рейтинг зрелости по отраслям?

И. КАМОЛОВ: Наша приоритетная «зона обслуживания» – кредитно-финансовые компании и телекомы, энергетики, нефте- и газодобывающие предприятия. В силу своей специфики и значимости для государства, наверное, дальше всех ушли в вопросах ИБ энергетики. В РАО ЕЭС есть собственные отраслевые инструкции и регламенты по ИБ, адаптированные под конкретные нужды, концепция построения СИБ, налицо и прочие признаки зрелости организации в области ИБ.

Все уважающие себя банки имеют концепцию СИБ, чтобы удовлетворять условиям системы страхования. И по объемам финансирования крупные банки, безусловно, впереди. Например, из порядка 500 столичных банков способны выделять значительные средства не более 20–30. У остальных же весь годовой бюджет ИТ вместе с безопасностью – $150–200 тыс., смешные деньги по меркам мощной СИБ. Да и 90% наших банкиров не готовы выделять на безопасность столько же, сколько, скажем, на средства производства. Потому методику построения или план-проект внедрения СИБ имеют лишь единицы банков, остальные решают проблемы ИБ «кусочно».

С. РЯБКО: Моего 12-летнего опыта работы и статистики контрактов фирмы маловато для такого ответственного дела, как рейтинг. Рейтинг – результат специального исследования, которое на отечественном рынке никем не проводилось. Подчеркну: мое мнение относится к рынку защиты конфиденциальной информации.

Впереди, безусловно, кредитно-финансовый сектор. За ним – добывающие отрасли (деньги – двигатель прогресса и в ИТ, и в ИБ). В других отраслях ситуацию определяют скорее личные и субъективные факторы. Например, в числе лидеров – электроэнергетика. Я склонен приписать это достижение личной позиции одного из наиболее жадных до информатизации бизнеса руководителей России – А.Б. Чубайса. В металлургии и тяжелой промышленности «плотность» внедрений ИБ существенно ниже.

Еще ярче роль субъективного фактора на транспорте. Например, в РАО «Российские железные дороги» в годы работы там С.Е. Ададурова задачам ИБ всегда уделялось повышенное внимание. За вехами создания СИБ РЖД просматривается целостная управленческая стратегия. А вот о серьезных проектах ИБ в авто- и авиатранспорте слышать не приходилось. Судя по доступной информации, безопасность на авиатранспорте сейчас сконцентрирована на защите от человека с оружием и взрывчаткой. Не стоит ли задуматься о противостоянии и другим атакам?

Поэтому, в силу определяющей роли личности, мне кажется более показательным рейтинг не отраслей, а культуры пользования средствами информатизации и менталитета руководителей.

М. ЛЕВАШОВ: Зрелость отрасли в значительной степени зависит от ИТ-инфраструктуры в целом, осознания акционерами важности проблемы, финансовых возможностей. Средняя зрелость в области ИБ – где-то между II и III уровнями (в терминах CobiT): проработанность процессов управления ИБ, наличие элементов обучения сотрудников, применение дисциплинарных мер к нарушителям, стандартизация отдельных процессов управления ИБ.

Наиболее высокий уровень – у кредитно-финансовых организаций, в том числе по причине наличия серьезного регулятора в лице ЦБ. Выросла роль ИБ и в телекомах – как мобильных, так и фиксированных. Принятые законы («трехглавый» и «О персональных данных») формулируют требования к ИБ и делают легитимными некоторые методы защиты. Сегодня почти у всех операторов есть специалисты или даже подразделения по информбезопасности. Судя по данным различных форумов, рейтинг зрелости по ИБ столь же высок в добывающих отраслях нефтегазового комплекса.

С. РОМАНОВСКИЙ: С 2005 г. российские компании проявляют явный интерес к защите информации, хотя это происходит скорее из желания «сделать не хуже других», а не от осознания проблем ИБ. Передовые позиции по защищенности бизнеса уверенно держат финансово-кредитная сфера, частные коммерческие предприятия и телеком. Хуже обстоят дела у госструктур.

Е. АКИМОВ: Вспоминается шутка Марка Твена о трех видах лжи: есть ложь, хитрая ложь и статистика. На мой взгляд, рейтинговать отрасли по уровню ИБ неправильно. Можно ли однозначно утверждать, кто находится в большей безопасности: рабочий в каске или без нее? Если они оба на стройплощадке – тот, что в каске. А если человек с непокрытой головой загорает на пляже? Так и с безопасностью: если банки и телекомы прилагают массу усилий для защиты информации, это совсем не значит, что на каком-нибудь кирпичном заводике, где даже бухгалтерия ведется на бумаге, уровень ИБ будет ниже. Картина зрелости отрасли в плане безопасности просто отражает зависимость бизнеса от информационных технологий.

М. БАШЛЫКОВ: Явно выделяется кредитно-финансовый сектор, ведь Центробанк обязывает банки при построении СИБ следовать стандартам. Защищенность предприятий других отраслей скорее недостаточная. Лидеров среди отраслей выделить невозможно, есть лишь отдельные передовые компании и предприятия, которые больше инвестируют в защиту сетей. Подход везде субъективный, закономерности не наблюдается.

А. РАЗУМОВ: Впереди, конечно же, кредитно-финансовые учреждения. Несколько отстают от них телекомы. Всеобщая тенденция – рост интереса к решениям по защите веб-приложений и удаленному доступу к корпоративным ресурсам.

С. РОМАНОВСКИЙ,
руководитель направления по ИБ «АМТ-Груп»

Е. АКИМОВ,
менеджер направления ИБ компании «Открытые Технологии»

М. БАШЛЫКОВ,
руководитель направления ИБ компании «КРОК»

«ИКС»: Какова отраслевая специфика ИБ и механизмы ее реализации?

И. КАМОЛОВ: Первым и наиболее сформированным сейчас вертикальным рынком ИБ стали государственные организации: органы власти и управления, структуры, специфика ИБ которых прописана в законах и постановлениях и контролируется специальными органами. Государство как владелец бизнеса непосредственно указывает, что и каким образом строить, за какие деньги, кому и когда отчитываться.

Второй вертикальный рынок, который жестко регулируется государством, – кредитно-финансовые учреждения. За ним следуют сегменты, связанные с предоставлением услуг населению, в которых могут таиться угрозы для жизни или экономики страны: транспортные предприятия, а также предприятия и опасные производства. Для всех перечисленных отраслей существуют госнормы в области ИБ.

Коммерческие предприятия при разработке СИБ руководствуются внутренними мотивами – главным образом эффективностью производства и угрозами бизнесу. Так, конкурентные угрозы заставляют создавать СИБ те компании, которые владеют информацией о большом количестве субъектов и их отношений. Специфика их систем ИБ: с одной стороны, не позволить эту информацию использовать во вред владельцу, с другой – обеспечить ее доступность. Для предприятий, скажем, промышленных или торговых типового набора требований нет: система строится в основном согласно пожеланиями владельцев бизнеса. Исключение – требования, связанные с криптографией.

Есть немало ситуаций, когда госорганизации обязаны применять российскую криптографию. Но она не всегда работает,

А. РАЗУМОВ,
специалист по ИБ Check Point

И. АСТАХОВ,
начальник управления широкополосных и телематических услуг «Комкор»

т.е. конкретные устройства функционируют автономно, не поддаваясь интеграции с себе подобными, да еще и с СЗИ. Я не видел ни одной VPN на базе российской криптографии объемом даже в 200 точек.

Причина в том, что политика государства привела к полному отсутствию на этом рынке конкурентного окружения: существует 5–7 «уполномоченных» разработчиков СКЗИ, давно поделивших сферы деятельности. «Коммерсантов», правда, выручает «трехглавый закон», где сказано, что собственник информации определяет, как, какую и каким способом информацию ему защищать.

В части сертификации СЗИ состояние дел иное. В свое время Гостехкомиссия (сейчас ФСТЭК) создала условия для здоровой конкуренции. И родился достаточно конкурентный и представительный рынок сертифицированных средств ИБ. Конкуренция же обусловила и корректную работоспособность продуктов в любых сетях.

С. РЯБКО: Аспекты ИБ, связанные с деятельностью организации, могут быть специфичны. Во-первых, есть строго «вертикальные» приложения (скажем, система управления активами предприятия горнодобывающего предприятия), встроенные в них механизмы ИБ специфичны. Во-вторых, предприятия вертикальных рынков работают с информацией разных классов конфиденциальности. В этом случае законом предписано применение различных средств защиты. Следовательно, формально вертикальная специфика существует, однако она нефундаментальна. Фундаментальные механизмы ИБ, обеспечивающие конфиденциальность, целостность, аутентификацию, подотчетность, лишены какой-либо специфики. Продукты ИБ, реализующие эти механизмы, могут применяться везде, где их стойкость соответствует требованиям заказчика.

Е. АКИМОВ: Специфика – в обеспечении и управлении ИБ. Она отражает критичность бизнес-процессов. Например, в банковской сфере это бизнес-процессы, связанные с переводом денежных средств, обработкой информации клиентов, поскольку требуют конфиденциальности данных. При создании СУИБ финансовые организации, как правило, применяют рисковую методологию. Схожие подходы используются и в телекомах. Новая тенденция в этих отраслях – внедрение ISO 27001. В топливно-энергетическом комплексе критично нарушение конфиденциальности информации. Поэтому упор делается как на средства криптографии, так и на борьбу с инсайдерами, где организационные меры сочетаются со средствами защиты от утечек. На промышленных предприятиях усиление внимания к ИБ связано с появлением критичных бизнес-приложений (в частности ERP-систем) и усложнением АСУТП.

М. БАШЛЫКОВ: Отраслевые особенности незначительны. Заметна лишь разница в подходе к ИБ государственных и коммерческих организаций: для первых законодательство требует использовать лишь сертифицированные СЗИ, у вторых больше возможностей для маневра – подход к ИБ зависит лишь от воли руководства.

«ИКС»: В каких отношениях ИБ и деньги?

И. КАМОЛОВ: Самое печальное в создании СИБ – разговаривать с потенциальным заказчиком о затратах. Даже его высший менеджмент порой представляет себе информзащиту как некую расходную статью. А ведь именно типичный – «кусочный» и бессистемный – подход увеличивает траты и лишает смысла само понятие информационной безопасности. На самом деле информационная безопасность, которая сберегает ресурсы, – не пассив, а актив компании.

М. ЛЕВАШОВ: СИБ должна строиться на основе анализа рисков, а оценивать их необходимо в деньгах. Определив риск как среднестатистическую величину потери (сумма потери, помноженная на вероятность события, которое к ней привело), можно доходчиво показать руководителю предприятия возможный ущерб, чтобы решение о выделении финансирования на ИБ было обоснованным. Если же специалисты по ИБ не сумеют это показать, денег на ИБ никто не даст.

«ИКС»: Как оцениваете интеграцию ИС и СИБ в отраслях?

И. КАМОЛОВ: Когда средства ИБ не интегрированы в общую ИТ-структуру, «совместная жизнь» невозможна. Другой вопрос – интеграция системы управления ИБ с общим управлением информсистемы или создание общей адаптивной системы управления, которая автоматически подстраивается либо настраивает параметры остальных ИТ-систем. Но, как правило, СИБ рождается позже системы автоматизации предприятия. Еще одно «но»: на практике не более 20% компаний внедряют действительно системы, а не набор отдельных средств ИБ. Чаще всего запросы не идут дальше firewall и антивируса (плюс бесплатные утилиты). И возникает локальная проблема, например с веб-сервером, когда скачивается ПО и «пристраивается сбоку», в результате снижается защищенность информсистемы.

С. РЯБКО: Думаю, что СИБ интегрирована с ИС у 100% компаний: вообразите себе систему защиты информации, работающую в полном отрыве от системы обработки информации. Это нонсенс. Вопрос в степени и качестве интеграции. Отмечу, что требования и критерии здесь совсем неочевидны. Предполагаю, что в ряде случаев система ИБ по показателям применения должна быть выделенной и изолированной, т.е. минимальная степень интеграции со смежными системами будет благом, а не бедой. Поэтому целесообразно говорить не о фактической степени интеграции, а об интеграционном потенциале заданной СИБ. А он пропорционален числу стандартов, которые поддерживаются используемыми в компании продуктами.

Оценивая ситуацию с позиции интеграционного потенциала, стоит посетовать на тяжкую участь России. Национальное законодательство требует сертификации СЗИ, что само по себе позитивно. Однако оно дало производителям свободу проталкивать кустарное изделие под лозунгом «Стандарт – не указ, главное – сертификат». Опасность отказа от стандартизации определяется для меня тремя доводами:

- Интеллектуальные ресурсы, привлекаемые к созданию кустарного изделия, существенно уступают разработчикам индустриального стандарта, а значит, архитектура безопасности у первого, вероятнее всего, будет проработана хуже.
- Стандарт документирован, но я не видел ни одного удовлетворительно документированного кустарного решения. Стандарт открыт, а кустарь предъявляет органам сертификации (и никому на рынке!) в лучшем случае только часть проектной документации. Безопасность решения подкреплена лишь уверенностью самого производителя в совершенстве своего изделия.
- Стандартный продукт допускает кросс-отладку с продуктами третьих производителей, а с кем «отлаживается» кустарь?

К счастью, рост уровня стандартизации продуктов ИБ – объективная тенденция российского рынка. И в этом смысле интегрируемость решений также растет.

С. РОМАНОВСКИЙ: На самом деле компаний, где ИС и СИБ интегрированы, совсем немного. Однако развитию данного направления способствует внедрение систем Service Management и мода на использование стандартов серии BS ISO/IEC 20000-1(2).

Е. АКИМОВ: В последние годы процесс интеграции технических средств обеспечения безопасности, обычного ПО и оборудования ИС набирает силу. А развитие методологии обеспечения ИБ помогло понять, что многие аспекты, ранее рассматривавшиеся отдельно от информбезопасности, правильней воспринимать как составные части этой системы, например непрерывность и нормальное функционирование бизнеса. Даже регулярное обновление ПО для бизнеса повышает защищенность системы в целом.

И. АСТАХОВ: Бессмысленно говорить об ИБ вне системного подхода. Для надежной защиты ИС нужен комплекс технических и оргмер. Эффективная СИБ – плод совместных усилий людей из разных подразделений. Мы рассматриваем защиту информации как часть системы непрерывности и общей безопасности бизнеса. Решение этой задачи требует тесного взаимодействия департаментов ИТ и ИБ, служб развития и эксплуатации сети. Будь то создание системы разграничения и управления доступом или системы централизованного управления сети, для достижения эффекта требуется интеграция программных и аппаратных средств.

«ИКС»: Насколько нормативная база отвечает требованиям отраслей?

И. КАМОЛОВ: Есть обязательные и рекомендательные юридические документы. И если рекомендаций вполне хватает, то обязательная база явно недостаточна. По ее части в авангарде – кредитно-финансовый сектор, а вот для телекома это понятие весьма относительное (кроме криптографии и СОРМ). Стандарт Банка России имеет рекомендательный характер. Кстати, рекомендательные документы гораздо действеннее, пример – международные стандарты Basel-II и ISO 17799. Но российские заказчики ждут прямых инструкций, поскольку классические банкиры, окончившие экономические вузы, мало что понимают в ИБ, а стандарт не дает на этот счет прямых указаний. На мой взгляд, развитием стандарта должны стать положения для конкретной ситуации, причем понятные банкирам. И здесь зарыта главная проблема – неосведомленность руководства в области ИТ, в том числе ИБ.

С. РЯБКО: Думаю, что с российскими нормативами ИБ фатальных проблем нет. Бизнес динамично развивается в направлении создания продуктов и услуг ИБ, а это верный признак того, что регулирование не перешло в зарегулированность. Полагаю, что для корпоративного бизнеса недоработки законов, стандартов и нормативов ИБ не являются сдерживающим фактором. Неполноту федерального регулирования здесь компенсирует внутренний норматив и корпоративный стандарт. Проблема – в осмыслении «областей правовой недостаточности», в наличии сил и компетенций для разработки локальных правовых актов уровня предприятия. Также необходима известная политическая воля руководства для проведения этих нормативов в жизнь. Если же всего этого нет, то и идеальное законодательство не поможет – его требования просто не будут исполняться...

М. ЛЕВАШОВ: Если в кредитно-финансовой отрасли есть Центробанк, регулирующий вопросы ИБ, то в других отраслях такового не наблюдается. Телекому нужны свои стандарты по безопасности. И такие работы ведутся как минимум в двух направлениях. В рамках МСЭ разрабатываются рекомендации к базовому уровню безопасности сетей связи (www.rans.ru/arrangements), которые впоследствии вполне могут стать рекомендательными (или обязательными) для российских операторов. Суть второго направления – согласование с Мининформсвязи постановки задачи «стандарт ИБ для телекоммуникаций» и определение финансирования данного проекта.

Е. АКИМОВ: Нормативная база только формируется. Тем не менее законодательно четко определено, что режим защиты информации определяется ее владельцем, а проблемы начинаются, когда она передается в другую компанию. К сожалению, сложно назвать сферу деятельности, где вопросы стандартизации были бы решены. Даже в наиболее зарегулированных госорганах многие документы устарели и, с одной стороны, не обеспечивают должного уровня ИБ, с другой – трудновыполнимы. В передовиках – лишь кредитно-финансовая сфера благодаря Банку России. Главная ценность стандарта ЦБ в том, что «процесс пошел».

И. АСТАХОВ: Вся нормативная база в области ИБ несколько устарела. Достаточно инерционное законодательство не успевает за развитием информационных технологий. И проблема эта не только российская. ИКС

ФОКУС

Традиционный оператор в борьбе за существование, или Бизнес-уроки Старого Света

Краски на историческом поле операторов сгущаются, воздух уплотняется. Звучит тревожная музыка. В вихре танца кружатся крупные поставщики контента, MVNO, поставщики услуг Wi-Fi- и SIP-телефонии. Ворвавшиеся на телекоммуникационную сцену новые игроки в авангардных костюмах пытаются вытеснить с нее классических участников рынка.

«Мы наблюдаем операторов, которые пытаются работать в условиях рынка XXI века, используя бизнес-процессы XX века, и видим, что это весьма негативно отражается на их финансовых результатах», – констатирует Кит Уиллетс, председатель совета директоров TeleManagement Forum.

Революционные перемены в структуре рынка, новые области конкуренции, отток абонентов от традиционных операторов, мобильная каннибализация... Знакомая ситуация? Причем если в России межрегиональные компании только начинают ее осознавать и о ней задумываться, их коллеги за рубежом активно ищут противоядие.

Не дают базовые услуги доход – и не надо! Дело дошло до того, что мобильная телефония становится бесплатной – придется лишь несколько секунд прослушать рекламу.

«Компании, которые сосредоточатся на формировании доходов от услуг нового поколения, а не на поддержании уменьшающихся доходов от «старых» услуг, и компании, способные к гибкому сотрудничеству с поставщиками контента и технологий, могут оказаться победителями», – убежден Винсент де Ла Башелери, руководитель глобальной практики Ernst & Young.

Итак, средства борьбы: удешевление базовых услуг или полный отказ от платы за них; пакетирование услуг; превращение телефонной связи не в источник дохода, а в стратегическое средство привлечения абонентов и в среду для размещения рекламы...

У традиционных операторов Европы есть и другие инструменты борьбы за рынок, которые могут быть полезны в России, – читайте ФОКУС «ИКС».

Вертикально интегрированные холдинги

Большинство традиционных европейских операторов в последние годы были преобразованы в вертикально интегрированные холдинги, т.е. в рамках одного холдинга были объединены операторские компании, занимающиеся оказанием различных услуг связи, продажей услуг разным целевым группам и т.д.

Основной причиной, вынудившей операторов к столь масштабным преобразованиям, стало набирающее силу перераспределение финансовых потоков между разными услугами (табл. 1). В таких условиях вертикальная интеграция позволяет оператору сохранить свои доходы, поскольку вне зависимости от их распределения по разным сегментам рынка все они остаются в пределах холдинга. Кроме того, в интегрированной компании можно снизить издержки за счет унификации бизнес-процессов внутри ее подразделений.

В интегрированной компании снижаются издержки за счет унификации бизнес-процессов

Другим побудительным мотивом вертикальной интеграции является стрем-

Табл. 1. Перераспределение финансовых потоков между рынками разных услуг

Наименование услуги	Рынок, теряющий доходы	Рынок, в пользу которого перераспределяются финансовые потоки
SIP-телефония	Фиксированная связь	Интернет
Конвергентные услуги	Подвижная связь	Фиксированная связь
Wi-Fi-телефония	Подвижная связь Фиксированная связь	Интернет
Доступ Wi-Fi	Подвижная связь	Интернет Фиксированная связь
IPTV	Кабельное телевидение	Фиксированная связь

Источник: аналитический отчет ЦНИИС

ление традиционных операторов к внедрению конвергентных услуг связи, которое, в свою очередь, обусловлено необходимостью создания различных механизмов перераспределения затрат и доходов внутри холдинга.

Поскольку доходы от услуг фиксированной связи постоянно снижаются, акционеры (которые в Европе следят только за котировками акций, не обращая внимания на особенности деятельности операторских компаний) заинтересованы в ликвидации соответствующих неприбыльных подразделений. Вертикальная интеграция дает руководству холдинга механизм перераспределения доходов от мобильной связи в пользу операторских компаний фиксированной связи.

Причины вертикальной интеграции:

- перераспределение финансовых потоков между рынками разных услуг;
- стремление выйти на рынок конвергентных услуг связи;
- необходимость сохранения и усиления рыночных позиций;
- желание создать входные барьеры для новых участников;
- стремление выйти на новые рынки.

Кроме того, вертикальная интеграция для оператора – это способ диверсификации деятельности благодаря выходу на новые рынки, увеличения рыночной власти за счет пакетирования и конвергенции услуг, усиления эффекта масштаба и создания барьеров для выхода новых игроков.

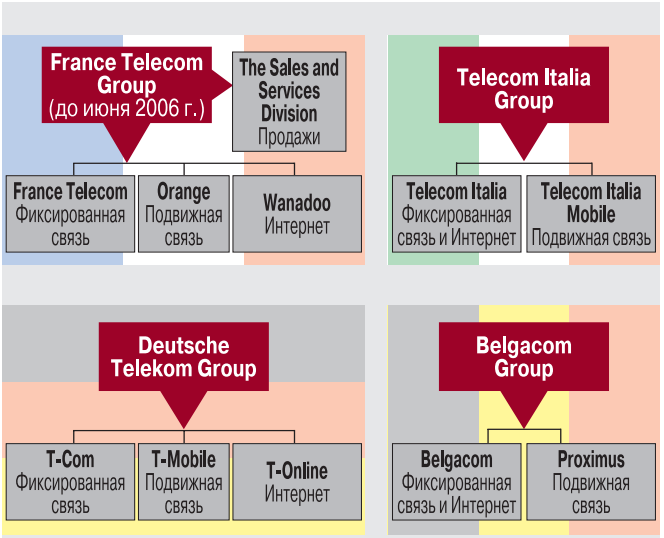
Последнее обстоятельство беспокоит регулирующие органы, отвечающие за создание конкуренции на рынке связи. В этом отношении показательна неудавшаяся попытка оператора Telecom Italia запустить конвергентные услуги. Итальянский регулирующий орган AGCOM в июне 2006 г. запретил компании внедрение новых услуг, мотивируя это отсутствием конкуренции на национальном рынке.

В 2005–2006 гг. целый ряд европейских операторов запустил и анонсировал конвергентные услуги (табл. 2).

«Холдингостроение» может происходить несколькими способами. Первый – это слияние и поглощение компаний, занимающихся оказанием иных видов услуг или действующих на других рынках, например в других странах. Так, оператор France Telecom в 2004 г. объединился с поставщиком услуг высокоскоростного доступа Wanadoo, а мобильный оператор Vodafone планирует купить английского оператора фиксированной связи Tiscali. Толчком к образованию холдинга вторым способом служит решение традиционного оператора самому начать оказывать новые услуги связи. Например, British Telecom в 2002 г. стал оператором MVNO на базе сети Vodafone.

На европейском рынке существует два основных типа телекоммуникационных холдингов. Наиболее распространенный тип – холдинг, в который входят операторские компании, автономно работающие в разных сегментах рынка (фиксированной, мобильной связи и услуг Интернета) (рис. 1).

Рис. 1. Организационные структуры европейских операторов



Источник: аналитический отчет ЦНИИС

В холдингах второго типа компании специализируются на организации продаж услуг разным целевым группам потребителей. Функции эксплуатации и развития сетей связи могут быть переданы отдельной компании.

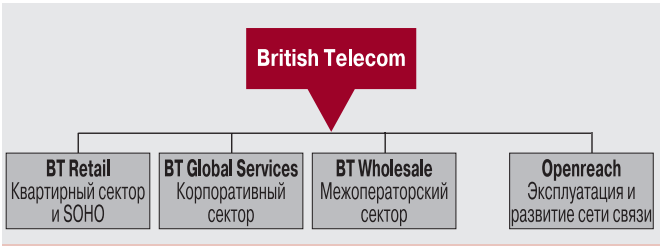
Табл. 2. Проекты по внедрению конвергентных услуг

Страна	Оператор фиксированной связи	Оператор подвижной связи	Дата вывода услуг
Великобритания	British Telecom	British Telecom	Q3'2005 (коммерческая эксплуатация)
Германия	T-Com	T-Mobile	Q3'2006 (коммерческая эксплуатация)
Италия	Telecom Italia	Telecom Italia Mobile	Q3'2006* (приостановлен)
США	Sprint	Nextel	Q3'2006 (опытная эксплуатация)
Франция	Orange	Orange	Q3'2006 (коммерческая эксплуатация)

* Вывод услуг приостановлен решением AGCOM из-за отсутствия конкуренции

Источник: аналитический отчет ЦНИИС

Рис. 2. Организационная структура холдинга British Telecom



Источник: аналитический отчет ЦНИИС

Табл. 3. Примеры вертикальной интеграции операторских компаний

Страна	Оператор фиксированной связи и услуг Интернета	Оператор подвижной связи	Формы объединения
Бельгия	Telenet	Mobistar	Telenet — MVNO на базе сети связи Mobistar. Mobistar — VNO на базе сети Wi-Fi, принадлежащей компании Telenet
Великобритания	British Telecom	Vodafone	British Telecom — MVNO на базе сети связи Vodafone
Германия	T-Com/ T-Online	T-Mobile	Холдинг
Италия	Telecom Italia	Telecom Italia Mobile	Холдинг
Италия	FastWeb	Vodafone	Соглашение о совместной деятельности
США	Sprint	Nextel	Соглашение о совместной деятельности
Франция	France Telecom	Orange	Холдинг

Источник: аналитический отчет ЦНИИС

Такова, например, структура холдинга BT (рис. 2); оператор перешел к ней, готовясь к строительству сети NGN 21CN (подробно см. «ИКС» № 5'2006 с. 98–99).

Впрочем, не всегда союз операторских компаний столь тесен, как в холдинге (табл. 3).

Объединение служб продаж операторских компаний

Как правило, один из первых масштабных шагов, которые делает руководство вертикально интегрированных холдингов, – это объединение отделов продаж отдельных операторских компаний в единое подразделение, подчиненное руководству холдинга.

Подобные объединения были проведены Telecom Italia и France Telecom в конце 2005 г. В июне 2006 г. об объединении подразделений продаж фиксированной и подвижной связи объявил австрийский традиционный оператор Telekom Austria.

Такой шаг обусловлен несколькими причинами. Во-первых, вертикально интегрированные холдинги заинтересованы в комплексном продвижении своих услуг на рынок. Однако исторически сложилось так, что подходы к организации продаж услуг у операторов мобильной и фиксированной связи сильно разнятся. Мобильные операторы имеют гораздо больший опыт в продвижении услуг на рынок, их дифференциации и работе с абонентами, поскольку всегда работали на высококонкурентном рынке. Операторы фиксированной связи, наоборот, до сих пор существовали в благоприятных условиях, на регулируемом в их пользу монопольном или олигопольном рынке.

Вертикальная интеграция – механизм перераспределения доходов от разных услуг связи

Различия в подходах к организации продаж приводят к существенным различиям в темпах роста доходов от оказания услуг на разных сегментах рынка. От этого страдают данные финансовой отчетности отдельных подразделений, предоставляемые акционерам, а они обычно склоняются к ликвидации неприбыльных активов. Поэтому руководство холдингов крайне заинтересовано в улучшении финансовых показателей фиксированных операторов. Это особенно актуально для холдингов, акции которых обращаются на открытых биржах: их акционеры чаще всего определяют момент сброса акций на основе технического анализа без учета рыночной обстановки.

Во-вторых, при внедрении конвергентных услуг с использованием двухрежимных терминалов доходы перетекают от мобильных операторов к фиксированным. Это неизбежно приводит к противоречиям между руководством соответствующих операторских компаний и скрытому противодействию решениям холдинга. Объединение служб продаж позволяет консолидировать все доходы на уровне холдинга, снять с руководителей операторских компаний ответственность за рост доходов и стоимость акций, ограничив их задачи эксплуатацией и развитием сетей.

В-третьих, для комплексного продвижения своих услуг операторы стремятся вывести их под единый бренд, для чего как раз необходимо объединение служб продаж и создание единой розничной сети.

Причины объединения служб продаж:

- необходимость комплексного и сбалансированного продвижения услуг связи на рынок;
- негативное отношение руководства операторских компаний к внедрению конвергентных услуг;
- создание единого бренда.

Ряд крупных зарубежных операторов провел сквозной ребрендинг своих услуг, объединив их под единой торговой маркой. Например, в июне 2006 г. France Telecom отказался от широко известных брендов и объединил услуги Интернета, мобильной связи, телевидения и телефонии под сквозным брендом Orange (о ребрендинге на российском рынке связи см. «ИКС» № 12'2006 с. 58–66).

Единый бренд усиливает интеграцию компаний холдинга как в глазах руководства и работников компаний, так и в глазах потребителей, которые благодаря «зонтичной» рекламе начинают воспринимать различные услуги одного оператора как единое целое.

Собственные розничные сети

В июне 2006 г. английский мобильный оператор O2 приобрел сеть розничных магазинов по продаже мобильных телефонов The Link, что позволило ему значительно расширить собственную сеть магазинов и провести масштабную рекламную акцию по продвижению запущенных недавно конвергентных услуг.

В марте 2006 г. подразделение Deutsche Telekom – T-Punkt Vertriebsgeseeschaft, отвечающее за рынок сбыта, в дополнение к 450 действующим магазинам открыло 60 универсальных магазинов совместно с

The Phone House, крупной сетью по продаже мобильных телефонов и услуг связи. Новые магазины под брендом The Phone House создаются в небольших городах с населением не более 90 тыс. человек, в то время как магазины T-Punkt в основном ориентированы на крупные города. Однако дизайн и организация продаж в универсальных магазинах обоих типов одинаковы.

Наиболее последовательного подхода придерживается France Telecom, который активно развивает точки продаж как в крупных торговых центрах, так и в собственных магазинах. На конец 2005 г. у оператора во Франции было более 600 точек продаж.

Объединение служб продаж позволяет создать единый бренд

Единая точка продаж France Telecom – это крупный магазин, в котором представлен весь комплекс услуг оператора. Такой подход позволяет привлекать больше клиентов, рекламировать и демонстрировать им различные новые услуги и осуществлять персональное обслуживание.

Стоит отметить, что универсальные магазины France Telecom Store построены по типовому проекту и различаются лишь размером площади (45, 80 или 150 м^2). При этом внутри каждая торговая точка разделена на отделы продаж услуг фиксированной, подвижной связи и Интернета. Однотипное устройство магазинов упрощает абонентам выбор и покупку услуг связи.

Конвергентные услуги

Ведущие традиционные операторы уже начали внедрение конвергентных услуг с использованием двухрежимных терминалов GSM/Wi-Fi или GSM/Bluetooth. Одним из первых был BT, запустивший в коммерческую эксплуатацию услуги FMC под брендом BT Fusion в июне 2005 г. К концу III квартала 2006 г. количество абонентов этих услуг, по разным оценкам, достигло 70–100 тыс. человек.

Основная причина формирования рынка конвергентных услуг – стремление фиксированных операторов в условиях снижения доходности их услуг перераспределить в свою пользу доходы мобильных операторов. Также многие фиксированные операторы рассматривают конвергентные услуги как средство защиты от замещения услуг фиксированной связи услугами мобильной связи (FMS, Fixed-to-Mobile Substitution) и как способ экспансии на рынок мобильной связи.

Услуги FMC перераспределяют доходы мобильных операторов в пользу фиксированных, поэтому, как правило, их внедрение происходит в вертикально интегрированных компаниях (France Telecom, Telecom Italia). BT для оказания конвергент-ных услуг BT Fusion стала оператором MVNO, воспользовавшись либеральным законодательством в этой области.

Однако иногда для совместного оказания услуг FMC объединяются компании, не входящие в один холдинг. Примером могут служить планы операторов FastWeb и Vodafone и союз американских компаний Time Warner Cable и Sprint Nextel, которые вынуждены объединяться, чтобы не допустить доминирования холдингов на рынках новых услуг.

Мобильные операторы, в свою очередь, тоже пытаются защититься от действий фиксированных операторов. Для этого они выводят на рынок услуги, которые аналогичны по потребительским свойствам конвергентным, но не требуют от абонентов приобретения двухрежимных терминалов. Сценарий этих услуг таков: когда пользователь находится дома или в офисе (что определяется с помощью локализации местоположения его мобильного телефона), он может совершать или принимать вызовы по тарифам фиксированной сети. При этом пользователю не нужно менять терминал, а оператору – создавать инфраструктуру для оказания конвергентных услуг. Пока подобные услуги более популярны у потребителей, чем конвергентные.

Бесплатные базовые услуги

В последнее время на рынке услуг связи появились новые участники, которые рассматривают базовые услуги как средство привлечения и удержания большого количества абонентов и как канал для размещения рекламы. Основные доходы они получают от размещения рекламы и продажи контента, товаров и услуг с добавленной стоимостью. Поэтому базовые услуги связи они оказывают бесплатно или почти бесплатно.

Новые участники готовы предоставлять базовые услуги бесплатно, видя в них средство привлечения абонентов

Низкие или бесплатные тарифы на услуги телефонной связи позволяют новым участникам рынка создавать большую клиентскую базу за относительно короткие сроки. Выбор телефонии в качестве стратегического средства привлечения абонентов обусловлен ее технологической простотой и доступностью для большинства населения, а самое главное, ее необходимостью в повседневной жизни. Таким образом, оказание услуг телефонии позволяет охватывать не узкие целевые группы, а широкие слои потребителей, невзирая на пол, возраст, интересы, квалификацию и пр.

Причины формирования рынка услуг FMC:

- стремление фиксированных операторов перераспределить в свою пользу доходы мобильных операторов;
- защита от мобильной каннибализации и попытка экспансии на рынок мобильной связи.

Новые участники телеком-рынка – конкуренты традиционных операторов:

- поставщики услуг SIP-телефонии. Это молодые, динамично развивающиеся компании (их доля мирового рынка по количеству обслуживаемых абонентов выросла с 9,1% в 2003 г. до 33,2% в 2005 г.). Самая известная из них – Skype;
- поставщики услуг Интернета, например Google, Yahoo!, AOL, которые купили в 2005–2006 гг. небольших поставщиков услуг SIP-телефонии, что говорит о росте их интереса к рынку услуг телефонной связи;
- операторы сетей кабельного телевидения, которые выступают на рынке со сформированным предложением triple play и активно используют возможности SIP-телефонии;
- операторы MVNO. Ориентируясь на узкие целевые группы потребителей, они рассматривают базовую услугу связи в качестве канала сбыта иных услуг или товаров;
- производители бытовой электроники, например Apple и Kodak. Чтобы добиться наибольшей лояльности потребителей, они активно продвигают фирменные пользовательские приложения и технологии и создают единые порталы продаж для стимулирования сбыта техники. Так, основой стратегии Apple заявлена «конвергенция прогрессивных технологий и тенденций рынка для достижения наибольшей лояльности потребителей». В конце 2006 г. Apple объявила о планах по выходу на рынки услуг GSM-, Wi-Fi-телефонии и обмена мгновенными сообщениями – Instant Messaging.

После создания большой клиентской базы новые игроки получают возможность транслировать рекламу абонентам, которые готовы принимать ее в обмен на снижение своих затрат на услуги связи.

Такую бизнес-модель планирует использовать, например, оператор MVNO Xero Mobile, который будет бесплатно оказывать услуги мобильной связи в обмен на прослушивание рекламы перед установлением соединения.

В качестве канала размещения рекламы новые участники рынка также используют коммуникаторы с функциями телефонии. Реклама передается пользователю одновременно с поступлением входящего вызова, а не в другое время, когда она может вызвать у него раздражение.

Производители электронной техники, например Apple, при помощи фирменных устройств привязывают к себе потребителей и могут проводить косвенную рекламу услуг и продавать контент через интернет-порталы.

Наибольшие доходы от размещения рекламы получают поставщики услуг Интернета, SIP-телефонии и операторы MVNO, оказывающие часть своих услуг бесплатно. Примером такой бизнес-модели являются проекты компаний Google и Microsoft, которые в США принимают участие в построении так называемых муниципальных сетей Wi-Fi. По замыслу компаний и городских властей, услуги беспроводного доступа будут оказываться бесплатно (в социальных целях), а доходы должны поступать от размещения рекламных объявлений. При этом Google планирует с помощью информации о местонахождении абонента сделать рекламу персонализированной.

Словом, круг конкурентов традиционных операторов непрерывно расширяется (табл. 4), и оставаться далекими от народа они не собираются.

Табл. 4. Новые участники рынка и стратегические направления их деятельности

Компания (страна)	Категория	Основной источник дохода	Действия
Google (США)	Поставщик услуг	Показ рекламы	Строительство сетей Wi-Fi с бесплатным доступом в ряде городов США
AOL (США)	Поставщик услуг	Показ рекламы	Оказание бесплатных услуг высокоскоростного доступа DSL
Skype—eBay (США)	Интернет-аукцион	Продажа аукционных лотов	Бесплатные вызовы "компьютер—телефон" в США, Канаде и Англии
BSkyB (Англия)	Оператор вещания	Показ рекламы	Оказание бесплатных услуг высокоскоростного доступа
Xero Mobile (США)	Оператор MVNO	Воспроизведение рекламы	Оказание бесплатных услуг мобильной связи

Источник: аналитический отчет ЦНИИС

Тенденция оказания дешевых или бесплатных базовых услуг связи – это серьезная угроза для традиционных операторов связи, поскольку платные услуги конкурировать с бесплатными не могут. Вследствие ценовой политики новичков, ARPU в сетях фиксированной и мобильной связи постоянно снижается, абоненты крупных операторов перетекают к конкурентам, доходы уменьшаются.

Поэтому, чтобы удержать абонентов и сохранить свои рыночные позиции, крупные операторы вынуждены следовать примеру новых игроков или создавать новые бизнес-модели поведения на рынке.

Попытки прямой конкуренции приводят к значительному снижению тарифов и падению доходности. Например, под давлением конкурентов традиционный бельгийский оператор Belgacom в середине 2005 г. ввел низкодоходный тарифный план на базовые услуги связи, по которому местные и междугородные телефонные вызовы для абонентов в выходные и рабочие дни с 18.00 до 9.00 бесплатны. В рабочие дни с 9.00 до 18.00 оплачивается только количество исходящих соединений без учета продолжительности и дальности связи. Но эти шаги не привели к росту доходов или абонентской базы, и Belgacom стал искать другие источники дохода и, в частности, создал фирменный портал Skynet, который, по его замыслу, должен стать крупнейшей рекламной площадкой в бельгийском Интернете.

Однотипное устройство точек продаж услуг связи упрощает абонентам их выбор и покупку

Пакетирование услуг

Еще одна защитная мера – пакетирование услуг, т.е. формирование оператором стандартного или индивидуального набора услуг для оказания их абоненту.

Основные причины пакетирования услуг:

- снижение доходов от базовых услуг связи, вызванное их бесплатным или почти бесплатным оказанием новыми участниками рынка;
- необходимость взаимной косвенной рекламы новых услуг;
- необходимость укрепления лояльности абонентов.

Пакетирование услуг позволяет традиционным операторам внедрять бизнес-модели, аналогичные тем, что используют их новые конкуренты. Например, в пакет услуг triple play входит бесплатное предоставление доступа.

Кроме того, операторы вынуждены увеличивать ассортимент услуг при постоянном снижении доходности каждой из них, что происходит вследствие высокой конкуренции.

Пакетирование помогает и удерживать абонентов, поскольку стоимость пакета ниже суммарной стоимости услуг связи, входящих в пакет. При этом пользователь, как правило, не может отказаться от услуг, не нужных ему, но входящих в пакет.

Телефония – стратегическое средство привлечения абонентов благодаря технологической простоте, доступности и необходимости в повседневной жизни

Например, пакет услуг triple play может помочь оператору связи защититься от поставщиков услуг SIP-телефонии, если он сделает стоимость своего пакета услуг ниже, чем суммарная стоимость его услуг IPTV, высокоскоростного доступа и услуг SIP-телефонии другого поставщика услуг.

Таким образом, для оператора пакетирование услуг – способ увеличения или, во всяком случае, поддержания на прежнем уровне дохода от их оказания, а также путь укрепления лояльности абонентов.

Новая концепция triple play

Сложившаяся ситуация вынуждает операторов не рассматривать базовые услуги связи как источник доходов в среднесрочной и долгосрочной перспективе. Это, в свою очередь, меняет их понимание концепции triple play.

Так, если ранее под triple play понималось оказание в пакете услуг телефонии, доступа в Интернет и IPTV, то сейчас эти услуги являются всего лишь одним элементом так называемой новой концепции triple play.

Эта новая концепция была сформулирована оператором Telecom Italia в 2005 г.

Первый уровень предложенной концепции triple play – базовые услуги: телефония, SIP-телефония, высокоскоростной доступ в Интернет, IPTV, которые могут обеспечить технологическое лидерство оператора связи, но не способны стать самодостаточными источниками дохода в долгосрочной перспективе. Этот уровень является аналогом прежней концепции triple play.

Второй уровень – пользовательские и сетевые приложения, конвергированные терминалы и прочие средства, обеспечивающие удобный доступ к информации, возможность персонализации услуг связи, порталы, коллективное взаимодействие пользователей. Этот уровень должен обеспечить лояльность абонентов, одновременно являясь универсальной точкой доступа ко множеству услуг оператора.

Третий уровень – контент, доход от продажи которого в долгосрочной перспективе, по расчетам Telecom Italia, должен составить наибольшую долю в структуре дохода оператора фиксированной связи.

Эта концепция в целом аналогична бизнес-моделям таких участников рынка, как Skype, Google, AOL, Yahoo!, Apple, Microsoft.

Несколько позже свое видение услуг triple play представили два других ведущих европейских операторов – BT и France Telecom. Их подходы несколько отличаются от мнения Telecom Italia (табл. 5).

BT и France Telecom также выделяют базовые услуги в первую группу, которая необходима, но недостаточна для получения значительного дохода. Остальные услуги делятся на развлекательные и необходимые в повседневной жизни.

Вторую группу составляют услуги, предоставлять которые приходится в условиях жесткой ценовой конкуренции и продвижение которых требует значительных маркетинговых и рекламных затрат.

Третью группу образуют услуги, которыми пользуются для обеспечения безопасности, поддержания социального и общественного статуса. Поскольку потребитель вынужден пользоваться такими услугами, оператор может установить на них выгодные

Табл. 5. Три подхода к концепции triple play

Telecom Italia	British Telecom	France Telecom
Communications	**Communications**	**Communications**
Телефония, подвижная связь, IPTV, доступ в Интернет, SIP-телефония	Телефония, подвижная связь, доступ в Интернет, SIP-телефония, Wi-Fi-телефония	Телефония, подвижная связь, универсальная почта, SIP-телефония, доступ в Интернет
Collaboration & Messaging	**Infotainment**	**Entertainment**
Доступ в Интернет, чаты, Instant Messaging	Игры, обмен фотографиями, музыка, видео	IPTV, музыка, видео, игры
Media	**Everyday Life Services**	**Life management**
Игры, музыка, видео, гороскопы, логотипы, рингтоны	Видеонаблюдение, охранная система, IPTV	Защита персональных данных, видеонаблюдение, охранная система, резервное хранение контента

Источник: аналитический отчет ЦНИИС

для себя тарифы и, привязав абонентов к своим услугам, продавать различное дополнительное оборудование и получать доход от его продажи.

Выход на рынок продаж пользовательского оборудования

В поисках новых источников дохода ведущие европейские операторы на протяжении последних двух лет все активнее занимаются продажей пользовательского оборудования – домашних шлюзов и устройств, подключаемых к ним (SIP- и Wi-Fi-телефоны, видеотелефоны, приставки IP-STB, камеры наблюдения, охранные системы и т.д.). Более того, операторы сами заказывают производителям терминалы, которые выполняются в корпоративном стиле и адаптируются под фирменные услуги.

Причина выхода операторов на рынок продаж пользовательского оборудования –

высокая доходность этого вида деятельности и желание привязать к своим услугам абонента, которому должно быть жалко выбрасывать купленное устройство.

У Telecom Italia и BT продажи пользовательского оборудования обеспечивают значительную долю доходов. Так, у Telecom Italia продажи оборудования для видеотелефонии и Wi-Fi-телефонии достигают почти 40% общего дохода от деятельности, связанной с оказанием услуг Wi-Fi-телефонии, что в 2005 г. составило 277,9 млн евро.

Фирменные домашние шлюзы

Основой технической политики многих ведущих европейских операторов является внедрение домашних шлюзов – устройств, которые предназначены для доставки большого количества услуг через единую точку входа и взаимодействия со множеством бытовых устройств. Домашние шлюзы рассматриваются как центральный элемент концепции «цифрового дома».

Так, шлюз BT Home Hub по интерфейсам и протоколам Ethernet, USB, Wi-Fi, Bluetooth и SIP обеспечивает подключение различного пользовательского оборудования: домашних компьютеров, ноутбуков, плееров, IP-STB, систем видеонаблюдения, Wi-Fi- и SIP-телефонов, двухрежимных терминалов Fusion, а также до пяти телефонных трубок DECT. Сам он подключается к сети по интерфейсу DSL. С помощью терминалов Fusion шлюз BT Home Hub может устанавливать до пяти одновременных вызовов.

Пакет услуг triple play поможет оператору связи защититься от поставщиков услуг SIP-телефонии

В отличие от модема DSL, к которому можно подключить в лучшем случае несколько компьютеров, но услуги будут предоставляться с профилем только одного пользователя, домашний шлюз позволяет оператору оказывать различные персонифицированные услуги сразу нескольким абонентам в одной семье.

Причина внедрения домашних шлюзов –

необходимость создать новые источники доходов и удержать абонентов.

Возможность подключения множества различных устройств к одному домашнему шлюзу позволяет оказывать целый спектр услуг для всей семьи. Тем самым решается задача увеличения количества предоставляемых услуг при сокращении доходности каждой из них.

Чтобы обеспечить совместимость домашних шлюзов с управляемыми ими бытовыми устройствами, было создано несколько рабочих групп, в частности группы форума DSL Forum, Home Gateway Initiative и NGN@home института ETSI. Задача рабочих групп – сформировать технические и функциональные требования к домашним шлюзам. В числе изучаемых ими вопросов – реализация SIP-телефонии, передача видео, управление классами QoS, удаленное управление и конфигурирование, дистанционное управление с инфракрасных пультов, взаимодействие с системами охранной сигнализации и пр.

Необходимость внедрять как можно больше недорогих услуг и привязывать их к фирменному оборудованию заставляет операторов искать нетривиальные пути разработки услуг. Например, France Telecom в июле 2006 г. создал открытый центр разработки услуг Livebox Lab, где любой желающий может придумать услугу для домашнего шлюза Livebox и где ему окажут содействие по созданию макета услуги. Если оператор признает услугу интересной для рынка, то она будет передана на разработку коммерческой версии, а авторы идеи получат часть доходов от ее продаж.

Внедрение домашних шлюзов, помимо возможности оказывать большое количество услуг, важно для продвижения инновационных услуг. Например, конвергентные услуги BT предоставляются только на базе домашнего шлюза BT Home Hub, реализующего функциональность UMA. А у France Telecom в шлюзе Livebox поддерживается управление QoS на беспроводных интерфейсах, что позволяет оказывать услуги SIP- и Wi-Fi-телефонии с высоким качеством.

Домашние шлюзы очень популярны. Например, всего за восемь месяцев во Франции пользователями шлюзов Livebox стали более 2 млн человек. Причем покупали их не только новые клиенты, подключающиеся к услугам DSL, но и абоненты со стажем.

Фирменные технологии для удержания абонентов

Отход от практики использования открытых стандартов и создание фирменных технологий – одна из важнейших стратегий, направленных на повышение лояльности клиентской базы (табл. 6). В основе ее лежит принцип: продукт, продаваемый потребителю,

Табл. 6. Фирменные технологии крупнейших компаний

Компания	Технологии
Apple	Кодирование контента
Real Networks	Кодирование контента
Skype	Телефонная сигнализация
ICQ	Обмен мгновенными сообщениями (IM)
MSN	Обмен мгновенными сообщениями (IM)
Yahoo!	Обмен мгновенными сообщениями (IM)
Telecom Italia	Телефонная сигнализация для Wi-Fi-телефонии
British Telecom	Технология передачи голосовой информации Hi-dS
France Telecom	Технология передачи голосовой информации (2007 г.)

Источник: аналитический отчет ЦНИИС

технологически не должен позволять ему перейти к конкуренту. Достигается это двумя путями:

- привязкой к контенту;
- привязкой к пользовательскому оборудованию.

Первый способ подразумевает, что пользователь приобретает контент, воспроизведение которого возможно только на оборудовании, продаваемом производителем контента. В этом случае чем больше будет аудио- или видеобиблиотека пользователя, тем меньше вероятность его ухода к конкуренту. Этот подход используют Apple, Kodak, Google. По такому же пути пошла компания Microsoft в своем новом плеере Zune.

Второй способ – привязка абонента посредством продажи ему пользовательского оборудования, которое работает только в сети конкретного оператора. Смена оператора будет означать, что деньги на пользовательское оборудование потрачены зря (выброшены на ветер), что вызывает психологический дискомфорт. Этот способ более распространен среди традиционных операторов.

Так, Telecom Italia в 2003 г. создал фирменную технологию загрузки контента на Wi-Fi-телефоны для оказания услуг с добавленной стоимостью.

BT в июне 2006 г. объявил о внедрении новой фирменной технологии передачи голоса с высоким качеством – Hi-dS. Эта технология реализуется при помощи фирменных аппаратных средств BT, например домашнего шлюза BT Home Hub, и использование ее возможно только в сети BT.

Та же тенденция прослеживается и на примере Skype, который использует фирменную сигнализацию и голосовые кодеки. Это сделано для ограничения возможности появления альтернативного ПО, функциональность которого не соответствует долгосрочным целям Skype.

А что же в России?

Первые шаги по пути, проложенному европейскими операторами, на российских просторах уже сделаны. МРК «Связьинвеста» диверсифицируют свой бизнес и оказывают услуги не только фиксированной телефонии, но и мобильной связи, доступа в Интернет и КТВ. Сквозного бренда для всех услуг пока нет ни у кого, а вот нишевые бренды уже появились. Для массовых услуг на основе широкополосного доступа в Интернет ими обзавелись «ЦентрТелеком» (Domolink, см. «ИКС» № 10'2006, с. 51), «Северо-Западный Телеком» («Авангард»), «ВолгаТелеком» (J), ЮТК (Disel, см. «ИКС» № 12'2006 с. 63–64) и «Сибирьтелеком» (WebStream), а для мобильных услуг – «Уралсвязьинформ» (Utel). Он же внедрил и пакетирование услуг. Абонентам предлагается несколько пакетов (домашний Интернет, фиксированная и мобильная связь в разных комбинациях, а в некоторых регионах и КТВ) и прямо указывается, какова будет экономия при покупке пакета по сравнению с приобретением тех же услуг по отдельности.

Телефония, доступ в Интернет и IPTV – сегодня лишь один элемент новой концепции triple play

Конечно, реальность, в которой действуют российские традиционные операторы (читай – МРК), пока выглядит не столь угрожающе, как в Европе. О бесплатном предоставлении базовых услуг связи речь пока не идет. С одной стороны, тарифы МРК регулируются государством и пока продолжают плавно расти, с другой стороны, в тысячах населенных пунктов тарифы на связь и не могут снизиться, поскольку связи там просто нет, а с третьей – многие из них уже зарабатывают на нерегулируемом поле.

Переход от открытых стандартов к фирменным технологиям – стратегия повышения лояльности клиентской базы

Но бдительности терять нельзя. Слово и дело Skype становится все популярнее и в России. Альтернативные операторы новой генерации все больше озабочиваются завоеванием аудитории, чем тарифами на голосовую связь, и число абонентов в их сетях (например, в Externet, где внутрисетевая связь бесплатна) неуклонно растет...

По материалам аналитического отчета ЦНИИС

РАКУРС

ВКСС: здравствуй, племя младое, незнакомое!

Им работать в технопарке

ВКСС всегда стояла особняком в ряду международных отраслевых выставок. Телеком-сообщество привыкло воспринимать ее как кастовое, корпоративное мероприятие, в границах одного «города» со своими проспектами и площадями, героями и главными действующими лицами, многие из которых представляют собой «государство в государстве». Девятая Международная выставка ведомственных и корпоративных информационных систем, сетей и средств связи – ВКСС-2006 (Москва, Гостиный Двор, 21–24 ноября) начала понемногу разрушать складывавшийся годами стереотип: эту некогда закрытую корпоративную территорию осваивают – и не без успеха – новые игроки, и в первую очередь молодежь.

В этом году организаторы выставки решили отказаться от «градостроительной» терминологии: размещение экспонентов в соответствии с их специализацией было во многом условным и довольно часто имела место «непрофильная застройка». Тем не менее посетители по привычке ориентировались на поквартальное размещение экспонентов, которых к тому же оказалось почти на четверть меньше по сравнению с пиковым, 2003-м, годом (150 компаний против 193). Места стало побольше (возможно, сказалась конкуренция с NAT EXPO, проходившей в те же дни в «Крокус Экспо»), и на освободившиеся площади организаторы пригласили профильные вузы. Но нет худа без добра – выставка неожиданно помолодела.

Вузовское племя

Что ни говори, а традиции берут свое. Хотя организаторы ВКСС-2006 и сменили названия тематических разделов, по-прежнему велико искушение продолжить «градостроительство». Тем более что в этом году в «городке» ВКСС выросли новые современные «кварталы»: к проспекту (назовем его так!) Прессы, о котором «ИКС» мечтал год назад (см. № 1'2006, с. 20), пристроился Вузовский переулок. Самый представительный дом здесь у СПбГУТ им. проф. М.А. Бонч-Бруевича. Его обитатели – студенты второго–пятого курсов. Молодые люди пока затрудняются сказать, кем они видят себя в ИТ-парке, на фоне которого была развернута их экспозиция, зато уже знают, куда идут деньги, выделенные на его строительство, и какими темпами оно продвигается. Студенты МИФИ, они же сотрудники созданного всего пару месяцев назад при институте Microsoft Innovation Center, продвигали свои первые разработки, например IP-видеокамеру. Экспозиции других университетов были поскромнее. А на стенде МТУСИ вообще обосновалась некая фирма, предлагающая продукцию, явно не относящуюся к образовательным технологиям.

В рамках ВКСС впервые прошла студенческая конференция «Инфокоммуникации

XXI века – будущее за тобой!». За круглым столом собрались студенты и недавние выпускники нескольких профильных вузов, принявших участие в ВКСС-2006. Обсуждали актуальные для сегодняшних студентов проблемы: качество образования и трудоустройство молодых специалистов. Об учебных центрах, созданных в своих вузах, рассказали представители Сибирского госуниверситета телекоммуникаций и информатики (СибГУТИ), СПбГУТ им. проф. М.А. Бонч-Бруевича и МИФИ. Оказалось, что зарубежные компании (Alcatel, Cisco, Huawei, Microsoft, IBM, Intel) гораздо больше озабочены подготовкой молодых специалистов в нашей стране, чем их российские коллеги. Ну а государство и вовсе устранилось не только от решения этих проблем, но даже от формулирования своих интересов и постановки задач государственным же вузам.

По замыслу организаторов, приоритетами ВКСС-2006 должны были стать информационная и энергобезопасность, повышение надежности телекоммуникационных систем, но многие экспоненты, похоже, узнали об этом только на открытии форума, и, видимо, поэтому их экспозиции по традиции больше напоминали выставку собственных достижений. Хотя были, конечно, и профильные экспозиции по этой тематике.

Какие же ВКСС без военного оркестра?

Защита техническая и бюрократическая

«Информзащита» занимала на ВКСС два стенда, расположенных в разных местах. На одном из них демонстрировало свои разработки инженерное подразделение компании. Здесь были представлены решения для обеспечения безопасности современных информационных систем различного назначения. В этом году «Информзащита» выпустила третью версию аппаратно-программного комплекса шифрования «Континент», получившую название Evolution. В отличие от своей предшественницы она обеспечивает более высокую пропускную способность, в ней упрощены процедуры управления и диагностики комплекса и усовершенствованы технологии обработки различных видов сетевого трафика.

Аппаратно-программный комплекс шифрования CryptoAir предназначен для защиты данных, передаваемых как по кабельным, так и по беспроводным сетям Wi-Fi. Кроме того, он защищает кабельную сеть от несанкционированного доступа со стороны пользователей беспроводной сети и обеспечивает последним безопасный доступ к ресурсам кабельной сети.

В **Учебном центре «Информзащита»** в один из выставочных дней прошел семинар «Защита информационных и телекоммуникационных сетей и систем критически важных объектов». Обсуждались не технические, а нормативно-правовые, методологические и организационные проблемы обеспечения энергетической и информационной безопасности.

ФСТЭК, ФСБ, Минин-формсвязи России, Росинформтехнологии – выступавшие говорили о необходимости разработки в России системы нормативных правовых актов, определяющих вопросы защиты информации. Подчеркивалось, что наши стандарты должны соответствовать международным нормам, так как в эпоху глобализации требования к ИБ должны быть едиными во всем мире. В Госдуме лежит проект ФЗ «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры». Если он будет принят в 2007 г., то все необходимые регламенты организации информационной защиты будут готовы к 2010 г., а пока начальник управления ФСТЭК России А. Кораблев рекомендовал пользоваться международными стандартами, выразив надежду, что будущие российские документы противоречить им не будут.

Стенд «Интеграл-Электро» посетили порядка 150 человек

Российские производители ИБП не упустили шанс

По разным причинам зарубежные поставщики систем защиты электропитания выставку игнорировали. И весь поток заинтересованных специалистов устремился на стенды российских участников. Акцент в экспозиции компании **«Интеграл-Электро»** был сделан на комплексные системы питания средней и малой мощности серии ВСП с универсальным диапазоном выходного напряжения 48 и 60 В. На выставке демонстрировались действующие модели такого оборудования, состоящие из 3 и 5 выпрямительных модулей по 200 или 350 Вт каждый, доукомплектованные конвертерами и инверторами, а также русифицированным цифровым контроллером сбора информации системы мониторинга. Программное обеспечение позволяет дистанционно отслеживать параметры работы любых элементов системы электроснабжения и извещает оператора о подходе их значений к границе опасной зоны, что помогает своевременно принять решение о ремонте или замене того или иного оборудования.

«Связь Инжиниринг» демонстрировала свои новинки. Первая – вертикальное исполнение известного источника бесперебойного питания ИБП7-48/111-3.3, где компактность обеспечивается за счет размещения автоматических выключателей, модуля управления и цифрового контроллера непосредственно над выпрямительными модулями. Вторая – стойка конвертеров СК24/48, рассчитанная на 3 конвертера по 1,7 кВт. Будучи подключенной сбоку к ИБП этого производителя, имеющему выходное напряжение 24 В, она обеспечивает объект связи и напряжением 48 В.

Операторы предпочитают семь раз отмерить

Повышенные требования к надежности оборудования, достоверности и конфиденциальности передаваемой информации заставляют крупные ведомства делать серьезные инвестиции в развитие сетей технологической связи. Хотя ведомственные операторы, сохранившие верность ВКСС, предпочитают проверенные решения и с осторожностью относятся к технологическим новшествам.

Центральное место в Экспозиции Операторов (в терминологии ВКСС-2006) ведомственных сетей связи занимала **«Газсвязь»**. Информация о корпоративной системе «Газпрома» одновременно транслировалась на двух мониторах. Так что любой посетитель, набравшись терпения, мог узнать, что сеть связи «Газпрома» включает в себя 85,7 тыс. км магистральных и зоновых кабельных линий, 21 тыс. км многоканальных радиорелейных линий, 750 узлов связи, 350 транкинговых радиостанций, спутники связи «Ямал», 66 наземных станций спутниковой связи.

Тут же можно было ознакомиться с планами оператора по обеспечению технологической связью новейших объектов строительства: газопроводов «Ямал–Европа», «Россия–Турция», Северо-Европейского газопровода и обустройству Штокмановского месторождения. Так, например, на сухопутном участке Северо-Европейского газопровода Грязовец–Выборг планируется построить две ВОЛС общей протяженностью около 1200 км. Их резервирование будут обеспечивать цифровые радиорелейные линии связи. А при управлении по ВОЛС на морском участке Штокмановского месторождения оператор намерен воспользоваться опытом Alcatel, проложившей для передачи больших объемов информации подводные кабели на глубине до 8 тыс. метров без усилителей на расстоянии от 300 до 450 км.

Задача **«Системного оператора ЦДУ ЕЭС»** – обеспечение диспетчерского управления энергосистемой страны, от Калининграда до Дальнего Востока. Требования к достоверности информации, к надежности каналов связи определены государственными нормативными документами, а потому с затратами на дублирование оборудования и каналов связи приходится мириться. Сегодня все 64 региональных филиала объединены цифровой сетью связи, построенной на арендованных у «Ростелекома» и «ТрансТелеКома» каналах и включающей объекты связи и информационные системы ЦДУ ЕЭС. В роли поставщиков коммутационного оборудования выступают Siemens и «Информтехника», гибких мультиплексоров – Alcatel, сетевого оборудования – Cisco. Ближайшая задача системного оператора – развитие инфраструктуры для внедрения и функционирования автоматизированной системы диспетчерского управления, проектирование которой ведется сегодня под эгидой РАО «ЕЭС России».

СО-ЦДУ ЕЭС пригласил партнеров – **«ЕЭС Телеком»**, **НТЦ НАТЕКС**, **NGTel** – представить на его стенде реализованные проекты. Решения видеоконференцсвязи, которые уже сегодня используются в 7 объединенных диспетчерских управлениях, в том числе и для дистанционного обучения, демонстрировал **КРОК**. А **Siemens Enterprise Communication**, которую с ЦДУ ЕЭС связывают 10-летние партнерские отношения, показала «сигнальный вариант» диспетчерской системы нового поколения. Ее отличительные особенности – сенсорное управление (технология touch screen), гибкость программирования и широкий набор функций. Система имеет дружественный интерфейс и заметно облегчает работу диспетчеров как на отдельных предприятиях, так и в компаниях с большим количеством филиалов.

Как и на большинстве сегодняшних телекоммуникационных выставок, не обошлось без автомобиля. Красивый и безумно одинокий, микроавтобус «Соболь» под названием «Мобильный узел связи Банка России» украшал совместную экспозицию компаний **«Радиокомсистема»** и **«Морсвязьспутник»**. Из-под поднятой вверх задней двери проглядывала высокотехнологичная начинка. Сухопутная подвижная радиосвязь, спутниковая и транкинговая компоненты, система диспетчеризации обеспечивают мобильных абонентов Банка России услугами связи на территории всей страны.

Мобильный узел связи Банка России

В отсутствие сети система электропитания гарантирует автономную работу автомобиля в течение суток. В систему также входит малошумный генератор, кондиционер и обогреватель. Особенность автомобиля – мачта с электроприводом, позволяющая за 5 минут развернуть транкинговую радиосвязь МРТ-1327. В чрезвычайной ситуации банковские служащие могут передавать данные со скоростью 500 кбит/с через систему Inmarsat BGAN, с помощью которой можно также войти в ТфОП.

Представлению единой системы подвижной радиосвязи (ЕСПР) **Банка России** в рамках выставки был посвящен от-

Паровозик из Ромашково

дельный семинар. Вопрос объединения существующих сетей подвижной радиосвязи центрального банка страны в единую систему, сопряженную с ведомственной телефонной сетью, встал еще в 2000 г. Требовалось обеспечить управление транспортными средствами и безопасность их передвижения, повышение надежности и оперативности, формирование единого информационного пространства подвижной связи, обмен информацией между абонентами (в том числе в чрезвычайных ситуациях и в особый период), мобилизационную готовность банка. Выбор пал на систему МРТ-1327 на базе оборудования Rohde & Schwartz, генподрядчиком стала «Радиокомсистема».

Сегодня ЕСПР состоит из 4 крупных подсистем: сухопутной подвижной радиосвязи, подвижной спутниковой радиосвязи, контроля подвижных объектов и диспетчеризации. Первая подсистема объединяет территориальные сети транкинговой связи на базе протокола МРТ-1327. В настоящее время ЕСПР насчитывает более 50 территориальных сетей, построенных по радиально-зоновому принципу. Транкинг позволил реализовать в подсистеме сухопутной подвижной радиосвязи возможность общения между различными группами абонентов, постановки их в очередь на организацию сеансов связи и др. В подсистеме используется также конвенциональная, сотовая и микросотовая связь, системы персонального радиовызова.

Подсистема подвижной спутниковой связи обеспечивает резервирование и позволяет организовать обмен информацией между абонентами. Возможности этих подсистем используются подсистемами контроля за подвижными объектами и диспетчеризации.

Для обеспечения связи в любой точке данного региона задействованы мобильные узлы связи, оснащенные современными спутниковыми системами, такими как Inmarsat BGAN EXPLORER 500 – компактный мобильный терминал широкополосной связи сети BGAN, обеспечивающий передачу данных со скоростью 400 кбит/с и выше, доступ в Интернет.

Экспозиция Network Systems Group в стиле ретро

Мобильность, мультисервисность, защищенность

Разработчики и производители составляли, пожалуй, самый многочисленный отряд на выставке. И здесь тон задавали отечественные компании.

Концерн **Goodwin** представлял свою систему «Гудвин Бородино-И1», разработанную для применения на шахтах и рудниках. Новое в ней – возможность создания в подземных выработках удаленных кластеров взрывозащищенных базовых станций (БС), обеспечивающих покрытие площадью 300–400 кв. км. В состав такого кластера входит устройство управления, состоящее из модема для подключения к сети по потоку E1 и мультиплексора БС с искробезопасным окончанием, и ИБП с аккумуляторной поддержкой, блоком защиты по току с искробезопасным питанием 12 В на выходе и барьерами линии питания для обеспечения линейного питания БС. «Гудвин Бородино-И1» позволяет безопасно подключать до 64 вынесенных кластеров и 800 БС.

Стенд **Государственного Рязанского приборного завода** на ВКСС предлагал ознакомиться с FSO-оборудованием нового поколения – многоцелевой оптической системой для телекоммуникаций artLink, предназначенной для построения корпоративных и распределенных кампусных сетей, а также городских мультисервисных высокоскоростных сетей и ТфОП.

Этому ноутбуку от TS Electronics не страшна буря в пустыне

С помощью новой системы можно оперативно организовать канал связи с пропускной способностью от 2 до 200 Мбит/с на дистанциях от 0,1 до 4 км и более, в зависимости от места установки и требований к доступности канала. Она является экономичной альтернативой проводным, радио- и оптоволоконным линиям, например, для решения проблемы «последней мили», оперативного резервирования линий связи или увеличения пропускной способности существующих соединений.

НПО «Телеоника» сфокусировало внимание посетителей на системах оперативно-диспетчерской связи. Представленное им цифровое коммутационное оборудование позволяет строить многоуровневые корпоративные и ведомственные сети организациям разного масштаба. Функции оперативно-диспетчерской связи заложены в основной блок управления и коммутации АТС и реализуются с помощью цифрового телефона-пульта на 21, 72, 120 и 168 кнопок.

«Ангстрем-Телеком» из подмосковного Зеленограда демонстрировал на выставке свою продукцию выпуска 2006 г. SHDSL-модемы M2048 предназначены для работы с симметричными медными кабелями. Они могут использоваться как на выделенных абонентских, так и на соединительных линиях. Максимальная скорость передачи данных – 4640 кбит/с (по двум парам). Благодаря многоуровневому линейному кодированию TC-PAM, в модемах M2048 удалось одновременно добиться большого рабочего расстояния и высокой скорости передачи данных. При скорости 2048 кбит/с максимальное

рабочее расстояние может достигать 27 км, а при скорости 256 кбит/с – почти 50 км. Это позволяет либо вообще отказаться от регенераторов, либо существенно сократить их количество.

SHDSL-системы абонентского доступа ИКМ-2/4/6/8/12/15ДМ – модификация систем семейства ИКМ-2/4/6/8/12М. Они предназначены для подключения по одной паре проводов от 2 до 15 абонентов ТфОП (причем с учетом специфики российских сетей). Системы ИКМ-хДМ обеспечивают уплотнение телефонных каналов и удаленный доступ к сети, в том числе к Интернету. В базовой комплектации все эти системы имеют интерфейсы Ethernet с функцией моста, поэтому с их помощью можно организовать высокоскоростное подключение к Интернету как отдельных абонентов, так и целых локальных сетей, соединяющих сотни компьютеров.

Старшие модели этого семейства (ИКМ-6/8/12/15ДМА) комплектуются программно-аппаратными средствами для динамического кодирования каналов, что позволяет увеличить скорость передачи данных и рабочее расстояние. Эти системы позволяют использовать регенераторы, и за счет этого их рабочее расстояние можно увеличивать почти неограниченно. Они также могут быть использованы для замены традиционных систем уплотнения каналов.

Буквально за пару недель до открытия ВКСС-2006 разработчик, производитель и поставщик телекоммуникационного оборудования для цифровых сетей передачи данных компания **«КБ Кроникс»** представила модем Cronyx FOM8/M-E1 в мини-корпусе (размеры – 180 x 156 x 36 мм, вес – 700 г). Модем, предназначенный для работы в ВОЛС типа E1 (2048 кбит/с), совместим по оптическому каналу с мультиплексорами семейства Cronyx FMUX и поддерживает совместную работу по кольцевой схеме (до 44 каналов E1 по двум волокнам) и в режиме «точка-точка» (по одному волокну). Максимальное рабочее расстояние – 150 км.

Выпущенная минувшим летом бюджетная модель мультиплексора Cronyx FMUX/M-4E1 для ВОЛС (тоже в корпусе типа мини) обеспечивает передачу по оптоволоконной линии четырех каналов E1, каждый из которых передается независимо. Она совместима с другими устройствами Cronyx (мультиплексорами семейства FMUX, оптоволоконными модемами FOM8, в том числе с FOM8/M-E1). По заявлению разработчиков, настройка модели очень проста и производится с помощью переключателей на передней панели.

В экспозиции **ГК «Информтехника»** выделялись две новые разработки, каждая из которых является портативным дополнением к системам, выпускаемым уже несколько лет. АТС «МиниКом DX-500-compact» предназначена для установки на объектах с относительно небольшим числом абонентов.

Но с особой гордостью сотрудники «Информтехники» демонстрировали посетителям новый портативный комплекс подвижной связи «МиниКом-TETRA-Compact», мобильный вариант системы «МиниКом-TETRA». Комплекс предназначен для быстрой организации подвижной радиосвязи на ограниченной территории и может обслуживать до 150 абонентов. Базовая станция упакована в чемодан размером 34 x 46 x 17 см и весит всего 15 кг. Правда, в комплект входит еще антенная опора весом до 70 кг, ретранслятор радиосигнала, АРМ оператора (ноутбук в полевом исполнении) и сервер управления (компьютер в ударопрочном корпусе), но для перевозки этого оборудования достаточно легкового автомобиля. «МиниКом-TETRA-Compact» может заинтересовать МЧС, Минобороны, учреждения здравоохранения, транспортные компании и другие организации.

Чемодан с «МиниКом-TETRA-Compact» весит всего 15 кг

МТА сделала акцент на мультисервисную составляющую NGN. Мультисервисный абонентский концентратор M-200 обеспечивает абонентский широкополосный ADSL-доступ и межстанционные связи (E1+Eth) со встроенных HDSL-модемов, мультисервисный концентратор доступа MP-128 поддерживает до 4096 точек доступа, а ИБП M-200 – 100%-ный мониторинг всей схемы электропитания оборудования. «Малышка» УПАТС M-200, как ласково называют это экономичное решение сотрудники компании, обладает неплохим для ее параметров функционалом – от передачи голоса до широкополосного доступа – и помогает оператору сохранить инвестиции при переводе своих сетей связи на NGN.

Ту же цель – интегрировать существующие решения в инфраструктуру нового поколения – преследуют продукты **Network Systems Group**. Компания представила только что выпущенные или уже готовые к запуску в начале 2007 г. продукты на базе технологии E1-over-IP.

НТЦ НАТЕКС, участвовавший в экспозиции СО-ЦДУ ЕЭС, организовал еще и собственный стенд и объединил их конференц-связью на базе оборудования беспроводной связи Nateks-Multilink 3. Во время выставки можно было увидеть, как работают датчики охранной сигнализации, встроенные в модемы FlexDSL Orion2, система наружного наблюдения, установленная на систему передачи данных Megatrans-3/4, мультисервисные технологические узлы на базе FlexDSL Orion/Orion2, SDH-мультиплексоров и т.д.

Разработчики **«АМ Телеком»** развернули мультисервисную коммутационную платформу оперативной проводной

связи «Регион-DXE». Ориентированная на применение в силовых ведомствах система, модули которой связаны универсальной внутристанционной шиной Ethernet, позволяет разнести все станции «хоть на Луну». «Регион-DXE» обеспечивает сопряжение как с локальными (городскими, районными), так и с удаленными (областными, ведомственными, общегосударственными) сетями и базами данных.

На стенде башкирского **«Полигона»** почетное место среди оптических мультиплексоров занимало шасси 3U-15-1. В конструктиве 3U, по функциональности равном 6U или 10U, размещается до 15 разных блоков. Уровень энергопотребления моноблока благодаря современной элементной базе минимальный.

«Супертел», отечественный разработчик и производитель современных цифровых средств связи (PDH, xDSL, SDH, CWDM), представил синхронные мультиплексоры серии СМ уровней STM-1/4/16, платформы сетевого доступа МКСС с функцией спектрального оптического управления, сетевую систему управления «Супертел-NMS» и др.

Самарская оптическая кабельная компания продвигала на ВКСС самонесущие диэлектрические оптические кабели типа ОКЛЖ для широкополосных мультисервисных сетей, оптические кабели 10/125 СОКК 2006 с максимальным количеством волокон в кабеле от 24 до 96 при длине пролета 20–60 м, обеспечивающие статическую растягивающую нагрузку 3,5 кН, и т.д.

Самарские кабели

Huawei Technologies – один из немногих мировых поставщиков, принявших участие в выставке, представлял оборудование передачи данных и NGN-оборудование, наиболее интересные для использования в корпоративных и ведомственных сетях связи. Посетители выставки могли получить у специалистов Huawei подробную информацию о линейках маршрутизаторов Quidway, число установок которых в мире превысило 500 тыс. портов, и LAN-коммутаторов (установлено около 35 млн портов), разработанных поставщиком для корпоративных пользователей.

Мейнстрим широкой полосы,

заданный разработчиками и производителями, поддержали системные интеграторы, подтверждая, что и в технологических сетях связи – будущее за мультисервисом.

«Оптимальные Коммуникации» сфокусировались на отечественных решениях для магистральных сетей передачи данных. Оптические мультиплексоры «Акула» обеспечивают совместную передачу потоков E1 и Ethernet (пропускная способность 155 и 520 Мбит/с) между двумя или несколькими (до 132) пунктами связи по одному или двум оптическим одномодовым или многомодовым волокнам. Оборудование WiMIC стандарта WiMAX (IEEE 802.16-2004) для беспроводных линий (5725–6425, 5650–5725, 3400–3550 МГц) предназначено для построения сетей «точка-много точек» с количеством абонентских станций до 200 и скоростью передачи до 37 и 67 Мбит/с на сектор.

РКК продвигала новинки голландской фирмы Rohill (цифровые системы подвижной радиосвязи стандарта TETRA), испанской Sitre Telecom (универсальный интерфейсный коммутатор M.I.C.C.), Kathrein (базовые антенны), а также сетевые решения на базе аппаратуры широкополосного доступа (протокол 802.16, Motorola Canopy, MESH) и др.

В портфолио **Iskrateling** IP-телефоны: IP 10S – двухлинейный, с полным набором функций и поддержкой MGCP, H323v4, SIP; CT 310i – для вызовов на сети пакетной коммутации, совмещает функции аналоговых, цифровых и даже системных телефонов.

«Оптима-Интеграция» продвигает решения для обеспечения контроля на объектах и защиты информационно-телекоммуникационных систем.

Оборудование от **«КБ Кроникс»** использует в своих системах спутниковой связи компания Telintech. Оно входит в состав решений **Telintech** для организации спутниковой связи наряду со спутниковыми модемами производства Comtech EF Data и Advantech AMT. Эти модемы, поставляемые Telintech в Россию, и демонстрировались на стенде компании. Продукция Comtech EF Data – это выпускаемые серийно цифровые спутниковые модемы CDM-570, CDM-570L, CDM-600, а также модульный многоканальный спутниковый модем L-диапазона CDM-Qx (в его стандартный 19-дюймовый корпус высотой 1U можно установить 1 или 2 модема, до 4 модуляторов и до 4 демодуляторов). Спутниковые модемы от Advantech AMT – это почти штучная работа, они изготавливаются в соответствии с потребностями конкретных заказчиков. На стенде Telintech были представлены модели Advantech AMT-30RL, AMT-34RL и AMT-75. Последний из них поддерживает узкополосные системы связи, работающие по стандарту DVB-S2, и позволяет более эффективно использовать имеющуюся спутниковую емкость (в том числе для прямой трансляции видео высокой четкости).

Ракурс выбирали И. БОГОРОДИЦКАЯ, Е. ВОЛЫНКИНА, А. КРЫЛОВА