Ведущая темы
Лилия ПАВЛОВА

ждет ваших комментариев
в своем блоге на
www.iksmedia.ru

Информационная безопасность как услуга оператора для массового и корпоративного абонента – новый тренд российского рынка.

С одной стороны, число и уровень угроз растут, и защита от них становится насущной потребностью пользователей. Распространенные угрозы безопасности информационных ресурсов предприятий – DDoS-атаки, угрозы корпоративным брендам в Интернете, кибермошенничество, компьютерные вирусы. Частным интернет-пользователям, особенно детям, все сложнее самостоятельно защититься не только от вирусов и спама, но и от контента сомнительного или преступного характера.

С другой стороны, ради безопасности собственных сетей и информационных систем операторы уже давно используют решения для защиты от вредоносного кода, DDoS-атак, средства контентной фильтрации. И если до недавнего времени они были заняты в первую очередь наращиванием абонентской базы и «не замечали» массовый рынок услуг информационной безопасности, то сейчас ищут возможности «поделиться безопасностью» со своими клиентами, как корпоративными, так и частными. Дополнительные сервисы безопасности пока больших денег операторам не приносят, однако сами они считают, что у этого бизнеса хорошее будущее.

Есть и третья сторона – вендоры ПО информационной безопасности и системные интеграторы, часто выступающие в качестве движителей рынка и воспитателей спроса. Вендоры продают свои решения и стремятся выступать и в качестве провайдеров услуг ИБ; системные интеграторы выступают и как самостоятельные поставщики услуг ИБ, и как посредники в цепочке продаж этих услуг от вендоров конечным клиентам.

Возможен ли эффективный «тройственный союз» в противостоянии киберугрозам? Насколько готовы все участники рынка (вендоры, системные интеграторы, операторы, пользователи) к внедрению и развитию услуг информационной безопасности от оператора? Что представляет собой «базовый пакет» операторских услуг безопасности и какие сервисы могут войти в «дополнительный пакет»? Эксперты «ИКС» оценивают оперативную обстановку, дают прогнозы, генерируют идеи.

Новый тренд набирает силу.

Фокус
26
Со щитом или на щите

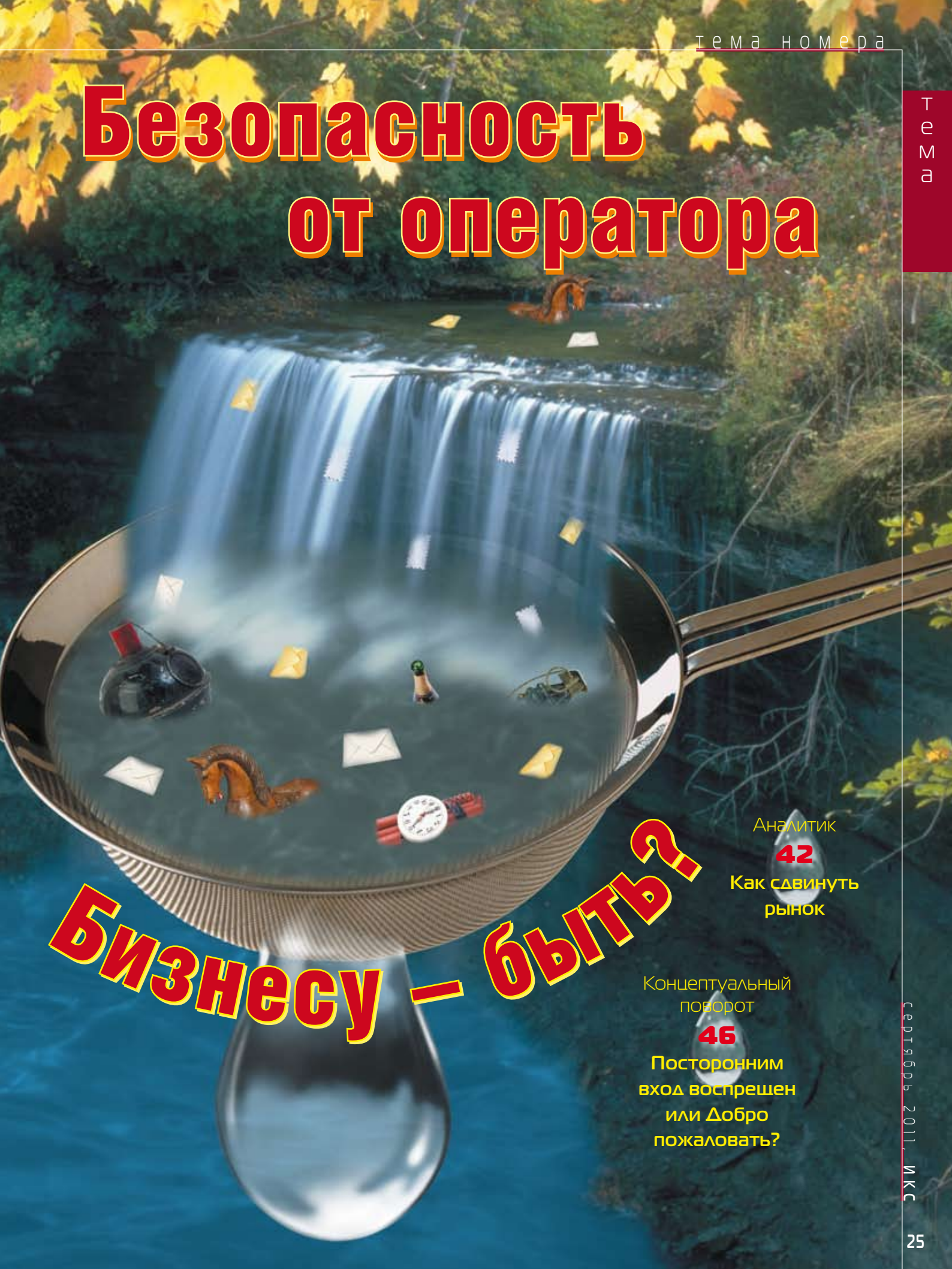
Проекты
29
Такие услуги обязаны быть прибыльными

Модель
33
Якорная услуга – результат R&D

Дискуссионный клуб
35
В одной упряжке

Подробности
40
Security as a Service

Безопасность от оператора



Бизнесу — быть?

Аналитик
42
Как сдвинуть рынок

Концептуальный поворот
46
Посторонним вход воспрещен или Добро пожаловать?

фокус

Со щитом или на щите

Информационная безопасность как провайдерская услуга для массового пользователя – еще не бизнес в России, но уже не экзотика; для корпоративного – уже не новость, но еще не рынок. За этот сегмент ИБ начинается битва партнеров-конкурентов, из которой кто-то выйдет со щитом, кого-то вынесут на щите.

В классе MSS

Услуги информационной безопасности от оператора связи относятся к классу аутсорсинговых услуг Managed Security Services (MSS). Характерная особенность модели MSS – постоянство. Это не разовые проекты по оказанию тех или иных услуг ИБ – напротив, клиент передает сторонней организации на обслуживание постоянные функции/процессы обеспечения безопасности своей информационной инфраструктуры. К классу MSS относят услуги анализа интернет-трафика и веб-фильтрации, защиты от спама, антивирусной защиты, контентной фильтрации трафика, защиты от DDoS-атак, а также управления – межсетевыми экранами, системами обнаружения и предотвращения вторжений, системами аутентификации и авторизации, криптографическими системами, включая построение VPN и инфраструктуры открытых ключей.

Аналитики прогнозируют рост рынка услуг класса MSS во всем мире: в Северной Америке – с $1,3 млрд в 2007 г. до $2,8 млрд в 2012 г. (IDC), в Европе – с $576,3 млн в 2006-м до $2,1 млрд к 2013 г. (Frost & Sullivan), в Азиатско-Тихоокеанском регионе – с $604 млн в 2008-м до $1,1 млрд к 2012 г. (IDC), в Латинской Америке – с $84,8 млн в 2009 г. до $298,6 млн к 2014-му (Frost & Sullivan). Игроки класса MSS представлены тремя группами компаний: вендоры ПО информационной безопасности, операторы связи, системные интеграторы. Конкуренция в классе существует и по горизонтали, и по вертикали: вендоры стремятся играть роль провайдеров услуг ИБ; операторы связи и системные интеграторы выступают и как самостоятельные поставщики услуг ИБ, и как посредники в цепочке продаж этих услуг от вендоров конечным клиентам. Выделить «операторскую долю» в выручке от услуг MSS крайне сложно, однако в этой тотальной конкуренции у операторов есть свои преимущества.

Забота о безопасности своей сети, по которой передается информация клиентов, – родовое свойство телекома. Кроме того, любой оператор основательно занимается защитой своей ИТ-инфраструктуры, поскольку от этого напрямую зависит его бизнес. Логично будет, если оператор – в порядке аутсорсинга – «поделится» безопасностью со своими клиентами.

К услугам, «заточенным» под бизнес оператора, эксперты «ИКС» отнесли защиту от DDoS-атак, шифрование каналов связи, веб-фильтрацию, PKI, AAAS, защиту от вирусов и спама, управление VPN. «В принципе в рамках операторского бизнеса возможна реализация любых решений MSS», – считает Д. Костров (МТС). Зарубежные операторы давно и успешно развивают этот рынок, в России же он находится в стадии формирования. При этом, как замечает А. Бугаенко («Синтерра»), активно формируют его сейчас именно операторы связи.

Бизнес на низком старте

На самом деле уже несколько лет крупные магистральные операторы при предоставлении своим корпоративным пользователям услуг IP VPN наделяют их дополнительными сервисами ИБ, а также предоставляют услуги защиты от DDoS-атак, веб-фильтрации и др. Однако российские телекомы оказывают услуги ИБ своим клиентам в порядке дополнительных опций (как правило, в целях повышения их лояльности и собственной конкурентоспособности) – и ни один оператор не готов назвать сумму выручки от этих услуг.

Тем не менее, по оценкам экспертов, именно операторский сегмент MSS должен «выстрелить» в ближайшие годы и начать приносить ощутимые доходы по-

ставщикам услуг. Это обусловлено набирающим силу встречным движением.

С одной стороны, этап наращивания клиентских баз ШПД рано или поздно завершится – и тогда рост операторского бизнеса будет возможен в основном за счет развития дополнительных услуг, в том числе ИБ. С другой стороны, растет спрос на услуги сетевой безопасности. Особенно остро нуждается в профессиональной защите от вирусов, фишинга, троянов, спама и нежелательного контента массовый сегмент, поскольку, как отмечает Д. Огородников (INLINE Technologies), большинство абонентов не обладают достаточным уровнем технических знаний, чтобы обезопасить себя в полном объеме. До недавнего времени, по признанию Д. Кострова, и сами операторы считали, что защита абонентов – дело рук самих абонентов. Сейчас они обратили внимание на частных пользователей – их же миллионы!..

Операторы, уже внедрившие на своих сетях системы контентной фильтрации и защиты от вредоносного кода, сами начали искать возможности предоставлять новые услуги безопасности. «Операторы связи не хотят быть «трубой», а хотят наиболее полно решать проблемы клиентов, быть MSSP, – комментирует операторскую позицию Д. Костров. – Это могут быть даже просто имиджевые услуги, на которых много не заработаешь, но когда есть два оператора и у одного можно заказать услугу «чистого Интернета», а у другого нет, то для пользователя выбор очевиден». Поэтому, считает П. Антонов (Cisco), услуги ИБ – как и любые другие дополнительные по отношению к услугам связи – станут для операторов основными источниками роста объемов выручки и способами удержания клиентской базы в ближайшие годы.

В корпоративном сегменте рост спроса, по мнению Д. Огородникова, обусловлен стремлением снизить операционные издержки и получить доступ к высокопроизводительным и современным системам ИБ за приемлемую цену. Даже крупные предприятия, способные самостоятельно решать задачи информационной безопасности, видят, что делать это своими силами далеко не всегда экономически более выгодно, чем отдать ту или иную задачу на аутсорсинг, замечает П. Антонов. Пресловутый «российский менталитет» (недоверие крупных организаций к аутсорсингу в принципе) постепенно отступает перед экономическими аргументами.

Кроме того, есть услуги ИБ, за которыми любой корпоративный клиент, независимо от размера бизнеса, придет к оператору. Самая известная такого рода услуга – защита от DDoS-атак. Однако доходы, которые эта услуга приносит крупнейшему магистральному оператору, его топ-менеджер называет «копеечными», поскольку главная роль услуги – не зарабатывание прибыли, а придание дополнительной привлекательности основным видам бизнеса.

Что касается предприятий SMB, особенно малого бизнеса, то здесь эксперты отмечают не меньшие перспективы для операторов, чем в массовом сегменте. Поскольку самые простые вопросы обеспечения ИБ у малого бизнеса оказываются практически нерешенными, его потребности охватывают огромный спектр услуг – от антивирусной защиты и антиспама до защиты от DDoS-атак, веб-фильтрации, защиты границы сети и т.д.

Поле под распашку

Облачные вычисления – это бизнес-шанс для телекоммуникационных провайдеров на рынке ИБ, считают эксперты «ИКС». Целевая аудитория публичных «облаков» – SMB, самая не охваченная услугами информационной безопасности территория. По словам А. Прокудина («АйТи»), это «непаханое поле» для желающих предоставить новый спектр услуг и заработать на них. П. Антонов уверен: наблюдая, как все больше и больше ИТ-сервисов предприятий в последнее время «переезжает в облака», операторы связи, естественно, не могут оставить без внимания этот рынок. В. Андреев (ИВК) также считает, что безопасность облачных сервисов, будучи «чисто инфраструктурной ИБ», это, «без натяжек, чисто операторская услуга» (хотя пока скорее перспективная, а не реальная). При этом, как отмечает К. Керценбаум (IBM), если провайдер сам же является оператором облачного сервиса, то защита – это его основная прерогатива, а не средство зарабатывания денег, поскольку ни один клиент не пойдет к облачному провайдеру, который потребует дополнительной платы за защиту информации заказчика. «Впрочем, можно получать прибыль, предлагая дополнительные услуги, чтобы повысить уровень защиты», – считает эксперт.

Но насколько сам рынок готов к модели Security as a Service? По мнению К. Керценбаума, к внедрению услуг готовы вендоры и операторы, но не клиенты, что связано «с определенным уровнем недоверия» и к первым, и ко вторым. При том что большинство экспертов наиболее высоко оценили уровень готовности к SaaS в вендорском и операторском лагерях, сомнения есть и здесь: каков потенциальный спрос и возможные объемы продаж, кто должен продвигать услуги, как выстроить модель взаимоотношений «вендор – интегратор – провайдер», есть ли целесообразность в привлечении «третьей стороны» (специализированной компании) для предоставления сервисов? Вопросов больше, чем ответов. По мнению В. Андреева, телеком все же имеет определенные преимущества перед ИТ-компаниями, поскольку доверие к нему у клиентов выше. В. Ткачев (SEC) видит возможный конфликт интересов операторов и системных интеграторов, поскольку задача оператора – сделать решение унифицированным, максимально «повторяемым», а задача системного интегратора – полностью удовлетворить именно специфичные требования заказчика и на длительный срок стать безальтернативным поставщиком услуг. Д. Савченко («Микротест»), напротив, считает, что для интеграторов это дополнительная возможность развивать свой бизнес: «Мы будем предоставлять услуги по проектированию и внедрению таких решений, но не конечным пользователям, а операторам связи, которые на базе этого будут уже реорганизовываться в SaaS-модели по предоставлению услуг пользователям».

В подобных спорах лучший советчик – опыт. Но его-то как раз на российской почве явный дефицит. Рынок ловит информацию о стартапе компании ТТК, запустившей в

ноябре прошлого года на базе облачной инфраструктуры компании Zscaler сервис очистки трафика Интернета WebProtection, который позиционируется как услуга для клиентов ТТК – коммерческих и государственных структур любого (!) масштаба. Но относительно подписчиков на сервис компания нигде не проговорилась...

Защита дома на столе, защита в кармане

Второй тренд, побуждающий к развитию ИБ как услуги от оператора, захватывает еще более массовую, чем SMB, аудиторию – собственно массовый рынок. По данным исследования российского рынка ИБ, проведенного компанией Leta, в 2010 г. наблюдался всплеск спроса на антивирусные решения со стороны домашних пользователей и в нынешнем году эта тенденция укрепляется. Десятки интернет-провайдеров, причем не только крупных (как «Комстар», МГТС, «ВымпелКом», «Центральный телеграф», бывшие МРК), но и городского масштаба, уже предоставляют своим абонентам подписные услуги «Антивирус», «Антиспам», «Родительский контроль», «Удаленная флэшка». Но если пользователи домашних ПК уже «дозрели» до такого рода аутсорсинга ИБ, то за мобильных абонентов операторам еще предстоит побороться.

По экспертным оценкам, в зарубежных странах операторские услуги антивирусной защиты для населения востребованы примерно у 15% абонентов мобильной связи. В России дополнительные услуги информационной безопасности для массового рынка пока редкость. «Российскую специфику» эксперты «ИКС» объясняют, во-первых, неготовностью абонентов платить за необязательные, с их точки зрения, услуги. «Редко кто из друзей, коллег или знакомых говорит о том, что у него телефон «убит» вирусом, скорее аппараты теряются, ломаются и т.п. На Западе практически та же самая ситуация – просто там больше процент бизнес-пользователей, использующих коммуникаторы в рабочих целях. У нас же такие устройства используются в основном для развлечения», – отмечает А. Трошин («Манго Телеком»). Вторая причина – незаинтересованность (до недавнего времени) самих операторов. «Чтобы обеспечить как увеличение числа пользователей, заинтересованных в данных услугах, так и заинтересованность операторов связи в их продвижении, необходимо определить максимально эффективную модель продаж услуг информационной безопасности», – считает А. Машков («Центральный Телеграф»). По мнению Д. Огородникова, дальнейшее формирование этой модели зависит в первую очередь от вендоров, которые должны изменить политику продаж, сдвигаясь от продажи «коробок» к разделению прибылей и рисков.

Между тем мобильные (теперь универсальные) операторы уже вошли в эту воду. «ВымпелКом» вывел на рынок в нынешнем году собственное провайдерское решение ИБ для частных абонентов (→ с. 29), МТС через свой магазин приложений предоставляет абонентам доступ к сервисам антивируса, спам-фильтрации и др. Их перспективность не подвергается сомнению, а с началом массовых продаж незрелость рынка из фактора риска трансформируется в потенциал его роста. Как заметил А. Машков, в наш небезопасный век спрос на операторские сервисы ИБ можно хорошо организовать («ведь нет ничего невозможного для людей с интеллектом») – и выигрыш при этом будет очевидным.

Не исключено, что даже можно будет посчитать его объем. ИКС

Есть идея!

Рынок бурлит идеями. Помимо привычных операторских услуг ИБ (защита от вирусов, спама, нежелательного контента, DDoS-атак и др.) эксперты «ИКС» вскрывают порой самые неожиданные возможности заработать на ИБ (а также минимизировать риски и сократить затраты на внедрение услуг).

Вот они:

- Вкладываться в R&D, создавать нужный рынку продукт – а потом зарабатывать и на продукте, и на услугах.
- Использовать модель Security as a Service.
- Для продвижения услуг использовать модель MVNO.
- Выступать в качестве канала продаж услуг ИБ, дополняя предложения провайдеров облачных услуг.
- Выстраивая партнерские отношения с несколькими специализированными вендорами, быстро запускать целый спектр новых услуг с минимальными затратами и, соответственно, минимальными рисками в случае, если какая-либо услуга «не пойдет».
- Привлекать к проектам «третью сторону» (специализированную компанию), значительно сокращая время вывода услуги на рынок и снижая затраты.
- Применять сервис-ориентированную модель: оператор конструирует услуги для различных категорий потребителей, создает инфраструктуру (на этом этапе средства уходят вендору и интегратору) и, опираясь на нее, продает свои услуги (эта составляющая остается у оператора и может со временем значительно превысить инвестиции).
- Защищать персональные данные клиентов компаний с территориально распределенной инфраструктурой в соответствии с требованиями ФЗ-152.
- Легализовать (в пределах требований СОРМ) право анонимного доступа в Интернет.
- Предоставлять услуги, связанные с использованием электронно-цифровой подписи.
- Предлагать на массовом рынке виртуальные системы хранения информации (стоимость хранения частной информации не должна быть выше стоимости записи информации на какой-либо жесткий носитель).
- Предоставлять корпоративным клиентам услуги электромагнитной безопасности*.

* В одном из ближайших номеров «ИКС» планирует публикацию статьи об электромагнитном нападении как новом виде угрозы ИБ и способах защиты от него.

проекты

«Такие услуги обязаны быть прибыльными»

С проектом «Родительский контроль и сетевой антивирус» компания открывает первую главу нового бизнеса, уверен Дмитрий УСТЮЖАНИН, руководитель департамента информационной безопасности компании «ВымпелКом».

Дмитрий УСТЮЖАНИН

– Во второй половине года «ВымпелКом» планирует запуск в коммерческую эксплуатацию сервиса «Родительский контроль». Что сподвигло вас заняться предоставлением услуг информационной безопасности частным клиентам?

– Интернет играет все большую роль в жизни людей, и люди все сильнее зависят от проблем, которые существуют в Интернете. Но самостоятельно установить приложение для защиты информации даже на домашний компьютер может не каждый. А как быть, если человек к тому же пользуется для доступа в Интернет смартфоном или планшетом? Устанавливать на эти устройства средства специализированной защиты очень сложно. Мы считаем, что эту задачу следует решать на операторском уровне, никто другой лучше и проще для пользователя это не сделает. Человек просто ставит «галочку» в «Личном кабинете» и получает максимально возможную защиту как услугу от своего оператора за некоторую дополнительную плату – на любое устройство, которым он пользуется для доступа в Интернет.

Вторая беда Интернета – контент сомнительного или даже преступного характера. Большинство пользователей Всемирной сети не способны самостоятельно оградить себя и, главное, детей от этой грязи. В 2009 г. по заказу «ВымпелКома» в пяти городах России (Москве, Нижнем Новгороде, Санкт-Петербурге, Екатеринбурге, Новосибирске) было проведено исследование «Безопасный Интернет» – и из 1000 опрошенных интернет-пользователей 55% высказали уверенность, что провайдер должен обеспечить защиту от вирусов, 70% считают наиболее полезной услугой от провайдера фильтрацию контента и 74% полагают, что провайдер должен предоставлять решения для обеспечения безопасности в Интернете и взрослых и детей.

– В Интернете можно найти множество предложений по ограничению доступа в сеть, чаще всего они так и называются – «родительский контроль». Чем от них отличается сервис «ВымпелКома»?

– Есть очень простое решение, которое сразу делает Интернет безопасным. Вы его просто почти отключаете: оставляете ребенку два-три сайта, и у вас получается замечательное решение «родительского контроля». Другое дело, что такое решение годится, наверное, только для самых маленьких детей. Ведь по большому счету оно убивает саму сущность Интернета как свободной среды общения и инструмента поиска информации.

Мы искали решение, которое сохраняло бы «вкус» Интернета для пользователей и при этом по возможности выметало оттуда всю грязь. В итоге у нас «Родительский контроль» оперирует сотней категорий блокировки контента, которые подразделяются на возрастные – до 7 лет, от 7 до 12, старше 13 лет. Используемая база данных уже сейчас содержит около 70 млн сайтов более чем на 100 языках мира. База ежедневно обновляется и пополняется; интернет-фильтры позволяют категоризировать более 100 тем, потенциально опасных или не рекомендуемых к использованию детьми, в зависимости от возраста. К слову, один из компонентов проекта – категоризация Рунета. На самом деле мы внесли в это существенный вклад, для чего пришлось вложить деньги, провести серьезное исследование. В итоге категоризируется более 3 млн российских сайтов.

О проекте

В рамках проекта «Родительский контроль и сетевой антивирус» на сети ОАО «ВымпелКом» внедрена система анализа и контроля интернет-трафика для абонентов «Билайн». Техническое решение основано на платформе Symantec NGNP (Next Generation Networks Protection). Поставщик платформы DPI – Nokia Siemens Networks (NSN). Интегратор – компания Bell Integrator. Сетевое решение анализирует интернет-трафик абонентов фиксированной связи, подключенных по технологии FTTB, и абонентов мобильной связи 3G/EDGE/GPRS.

Пожалуй, мы одни из первых в мире, кто смог построить такое решение на единой платформе. Для этого нам пришлось провести серьезную реорганизацию внутренней инфраструктуры предоставления пользователю доступа в Интернет – и в мобильной и в фиксированной сети. Вторая задача, которую потребовалось решить, – масштабируемость системы как по количеству абонентов, так и по объемам обрабатываемого трафика. Сейчас ее общая пропускная способность – 60 Гбит/с, это много. Но у нас миллионы абонентов мобильной сети, многие из них пользуются Интернетом, и маркетинговые прогнозы говорят о том, что количество подключений к Интернету будет постоянно расти.

– «Родительский контроль» – это социально направленная услуга, или имиджевая, или все же оператор может на этом заработать?

– Социальная направленность этой услуги очевидна. Конечно, нам важно, что такая услуга повышает лояльность клиента. Но не секрет, что для всех услуг существуют бизнес-кейсы, и эта не исключение. Мы рассчитываем, что компания заработает на услуге. Это стартующий практически с нуля бизнес, но он имеет, на мой взгляд, очень высокий потенциал роста, и я уверен, что это будет коммерчески успешный проект. Такие услуги информационной безопасности просто обязаны быть прибыльными, поскольку потребность в них огромна и расти будет постоянно. В конце концов, это должно стать гигиенической нормой для каждого пользователя Интернета (как, например, услуги дворников, убирающих грязь вокруг нашего дома). К слову, в нашем решении помимо защиты от нежелательного контента осуществляется и сетевое антивирусное сканирование трафика, поступающего на компьютер пользователя. Система выступает как сетевой фильтр, который «вырезает» вредоносное ПО, – с точки зрения реальной защиты это не менее важно, чем блокировка нежелательного контента. А все вместе это дает «чистый Интернет». Я лично оба сервиса обязательно подключу.

Надо заметить, что решения с функционалом «родительского контроля» представляют интерес и для бизнеса, поскольку позволяют значительно уменьшить расходование интернет-ресурсов и рабочего времени сотрудников, которое они используют вне профессиональной деятельности.

Вообще, информационная безопасность – такая специфическая профессиональная сфера деятельности, доверить которую можно не каждому. Операторам – можно, потому что «внутри себя» они умеют это делать, они прекрасно понимают требования регуляторов в этой области, у них есть хорошая команда, профессионально обученная, и они вполне могут донести эту услугу до клиентов, в том числе корпоративных. У операторских сервисов безопасности, я считаю, большое будущее, а у самих операторов – особая роль. Если сервисы информационной безопасности продвигаются со стороны оператора связи – это самый простой вход на пока еще не вспаханное поле. ИКС

Госзапрос на безопасность

Когда мы говорим об информационной безопасности применительно к мобильным телефонам, чаще всего на ум приходят антивирусные решения для мобильных операционных систем. Однако возможности операторов сотовой связи по предоставлению сервисов ИБ далеко не ограничиваются «технологическими» рамками, укрепляясь на территории безопасности собственно человеческой жизни.

Чрезвычайные ситуации – стихийные бедствия, техногенные аварии, катастрофы и теракты – увы, стали неотъемлемой частью нашей жизни. Как минимизировать потери в результате ЧС? Следует воспользоваться возможностями мобильной связи, считает «МегаФон» (тем более, что госструктуры стали требовать от мобильных операторов устойчивой связи вне зависимости от ситуации).

Первый в России ситуационный центр мобильной связи федерального масштаба, обеспечивающий при ЧС взаимодействие с оперативными дежурными МЧС, Минкомсвязи и других ведомств, был открыт в «МегаФоне» в апреле 2010 г. Одна из задач центра – оповещение абонентов о чрезвычайных ситуациях. По данным Галины Беловой, директора Федерального центра управления и мониторинга «МегаФона», с этой целью оператор впервые в мире начал применять «точечную» технологию SMS-оповещения населения в случае ЧС в локальной зоне заданного радиуса. «Уникальность технологии в том, что в онлайн-режиме наша система может определить количество абонентов, находящихся в любой зоне в любой точке страны, – и в соответствии с заявкой выполнить информирование населения именно в заданной локальной зоне, – подчеркнула Г. Белова на круглом столе, посвященном мониторингу и предупреждению ЧС с помощью сетей мобильной связи. – При этом каждый абонент, который попадает в зону (их может быть всего два, а может быть тысяча), получит SMS-оповещение». Эту технологию наряду с известной в мире технологией SMS-оповещения CellBroadcast оператор активно применял в прошлом году: через центр было сделано 48 оповещений о неблагоприятных погодных явлениях, 73 – о техногенных авариях, 20 – о пожарах, 7 – о катастрофах, 5 – о терактах. Таким образом, основная часть оповещений была связана с погодными явлениями и техногенными авариями (нередко – последствиями погодных явлений). Очевидно, что от их четкого прогнозирования во многом зависит и минимизация вызванных ими угроз.

Ставка больше, чем ИБ

Основное свойство абонентского терминала мобильной связи — мгновенная и адресная передача информации – делает его идеальным устройством для предупреждения об опасности в чрезвычайных ситуациях, что может значительно сократить число жертв ЧС. Например, для мест большого скопления людей операторы предлагают системы уведомления о пожарах, террористических угрозах и т.п., когда все находящиеся в определенном месте люди получают так называемые флеш-смс, предупреждающие о необходимости покинуть помещение или содержащие иные инструкции. Одновременно с этим система информирует экстренные службы. Для ее активации необходимо вызвать специальный короткий номер, подобный тому, что сообщает абоненту о балансе счета. Такие системы, разумеется, могут быть задействованы и в более крупных масштабах, чем офисный центр, завод или университет. С другой стороны, сегодня любой оператор поддерживает вызовы на номера экстренных служб – и, по экспертным оценкам, количество звонков о чрезвычайных ситуациях, сделанных с мобильных телефонов, значительно превышает число таких звонков со стационарных аппаратов. Это существенно сокращает промежуток времени от возникновения чрезвычайной ситуации до ее устранения вызванными специалистами.

В обыденной жизни тоже становятся привычными информационные сервисы, поддерживающие безопасность в широком понимании. Так, хорошо известен сервис определения местоположения телефона (и, соответственно, его обладателя), которым охотно пользуются родители школьников начальных классов, родственники пожилых людей. Зарубежные операторы активно продвигают услугу «умного дома», в рамках которой с мобильного телефона можно сделать звонок на устройство, передающее видеосигнал, и увидеть все закоулки своего жилища и состояние находящихся в нем электроприборов (отличное решение извечной проблемы рассеянных людей: выключил ли я утюг, выходя из дома?). Учитывая, что мобильное устройство хранит в себе массу персональной информации, которая может быть очень интересна злоумышленникам, мобильные операторы также вывели на рынок услугу удаленного блокирования телефона. Все это новые услуги в области безопасности, которые они могут предоставить своим абонентам.

Приходится признать, что российские операторы несколько отстают от западных коллег, но движутся в том же направлении. Но на самом деле все это лишь начало предстоящего интернет-бума. Сегодня соотношение цены и качества мобильного Интернета не выдерживает никакой критики. Но на подходе мощные скоростные каналы передачи данных для мобильной связи, которые сделают Интернет доступнее и географически, и по цене – а значит, откроют новые возможности для пользователей и операторов. И чем более доступным будет быстрый мобильный Интернет, тем активнее люди будут пользоваться дополнительными услугами, в том числе и в области информационной безопасности, – это произойдет естественным образом. А те операторы, которые раньше других смогут предложить своим пользователям такие услуги, получат шанс обойти конкурентов.

Алексей ДЕМИН, управляющий продажами в корпоративном секторе G Data Software в России и СНГ

Задачу прогнозирования «МегаФон» решает в рамках нового проекта «МетеоФон», предполагающего создание сети автоматических метеорологических станций на территории России в дополнение к существующей сети Росгидромета. Цель проекта – создание базы метеоусловий, предоставление фактических метеоданных организациям и другим пользователям, возможность предотвращения погодных рисков и страхования от них.

Метеостанции предлагается установить на базовых станциях «МегаФона», сеть которых имеет высокую плотность покрытия территории страны. Это более 20 тыс. площадок, где уже существуют системы сбора данных, необходимых для жизнеобеспечения БС. Подключив дополнительное оборудование, с тех же станций можно получать и метеоданные, которые будут использоваться для составления детальных прогнозов и предотвращения чрезвычайных ситуаций (пожаров, наводнений, паводков). Как отметил Тигран Погосян, заместитель генерального директора «МегаФона» по стратегическим проектам, ежегодно наша страна теряет порядка 700 млрд руб. только из-за лесных пожаров – и хотя оператор мобильной связи бороться с ними напрямую не должен, но он может дать специальным организациям оперативную информацию для быстрого реагирования, что, несомненно, поможет сократить эти колоссальные потери.

По словам Т. Погосяна, «МегаФон» готов реализовать проект технологически, однако вопросы территориального размещения метеостанций, их лицензирования и сертификации, законодательной поддержки ускоренного согласования для строительства таких сооружений, корректировки руководящих документов по данной тематике (погодные риски, страхование погодных явлений и др.) необходимо решать коллегиально. «Сложность подхода к решению проблемы заключается в том, что она затрагивает целый ряд ведомств – не только Минкомсвязи, но и МЧС, Росгидромет и целый ряд других, – считает Александр Крупнов, глава Инфокоммуникационного союза. – Кроме того, проблему следует рассматривать не только на федеральном, но и на региональном уровне взаимодействия с губернаторами». Для реализации проекта, по мнению А. Крупнова, понадобятся разработка государственной программы и выпуск соответствующего правительственного постановления.

Для решения технологических вопросов предлагается сформировать рабочую группу с участием представителей всех универсальных операторов, а для организационных – межведомственную рабочую группу, которая могла бы подготовить правительственное постановление. Принятие подобных документов – дело не одного месяца, однако с необходимостью госпрограммы согласны также представители МЧС, Росгидромета, администраций Московской, Тверской и Ивановской областей.

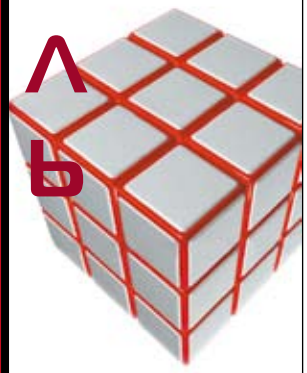
«МегаФон» уже начал обкатку проекта в пилотных зонах. Сейчас они развернуты на олимпийских объектах в Сочи (восемь метеостанций и две видеокамеры; до конца этого года количество метеостанций планируется довести до 30) и в Московской области. В дальнейшем авторы проекта планируют установить метеооборудование на своих вышках в 12 крупнейших городах России, а также создать сеть метеостанций, покрывающую все 28 685 км федеральных трасс на территории страны. ИКС

Модель

Операторы становятся MSSP

Бизнес-модель MSSP (Managed Security Service Provider) известна достаточно давно. В России рынок как раз переживает момент, когда и операторы и клиенты «созрели» для этих сервисов: операторы внедряют новые платформы и прорабатывают Service Level Agreement (SLA), клиенты стали больше доверять операторам.

Дмитрий КОСТРОВ, директор по проектам департамента информационной безопасности МТС



MSSP – оператор, предоставляющий сервисы безопасности, которые клиент не может сам себе предоставить. Скажем, при аренде помещения мы не думаем о том, чтобы обеспечить себе газ, воду и свет, поскольку это делают специализированные компании. Точно так же, выходя в Интернет, можно не думать о безопасности (антивирусе, антиспаме и т.д.), поскольку ее обеспечивает специализированная компания. В этом качестве, как правило, выступает именно оператор связи. Ведь в числе активов оператора – не только «труба» для передачи данных, но и, что более важно, клиентская база, которой могут быть интересны новые сервисы.

Спектр основных услуг безопасности от оператора – фильтрация веб-трафика, PKI, AAAS, сетевой антивирус, антиспам, защита от DDoS, managed VPN и т.д. В принципе, в рамках операторского бизнеса возможна реализация любых решений безопасности. В России «чистых» MSSP пока нет, однако большинство операторов уже осваивают эту модель. Оператор оценивает рынок, востребованность услуг информационной безопасности, проводит мониторинг предложений вендоров – и после этого развертывает техническое решение на своей сети. В рамках реализации услуги необходимо постоянно повышать компетенцию собственных сотрудников или работать в режиме кобрендинга с вендором.

У МТС есть такие продукты: наш магазин приложений предоставляет абоненту доступ к программам информационной безопасности, антивирусным сервисам и т.п.

Наиболее привлекательным нам представляется сегмент SMB. В базовый пакет для него обычно включают межсетевое экранирование, антивирус, антиспам. Эти же услуги входят и в базовый пакет MSSP для массового рынка, а любые другие чаще всего позиционируются как дополнительные сервисы. Но это зависит от конкретного заказа потребителя. Например, при реализации услуги FMC компания МТС обеспечивает абоненту защиту вне зависимости от способа связи и выхода в Интернет, поддерживая принцип конвергенции и мобильности «откуда угодно, когда угодно».

Надо признать, что у интернет-пользователей сетей мобильной связи интерес к дополнительным услугам информационной безопасности намного ниже, чем у подписчиков фиксированного ШПД. Одна из основных причин – отсутствие культуры потребления таких услуг. Многие абоненты не уделяют внимания вопросам безопасности; некоторые полагают, что это слишком накладно. Да и сами операторы до недавнего времени считали, что проблема безопасности – это проблема абонента. Сейчас многое поменялось, оператор должен использовать схему TELCO 2.0 в высококонкурентной среде. Так что безопасность – это проблема не только абонента, но и оператора. И поэтому он старается объяснить абоненту все преимущества использования систем безопасности уже на этапе заключения соглашения.

В целом сервисы безопасности, предлагаемые операторами в виде дополнительных услуг, достаточно перспективны. Однако делать конкретные прогнозы роста в силу незрелости рынка пока рано. ИКС

Якорная услуга – результат R&D

Цены на услуги защиты от DDoS-атак для клиентов ЗАО «Синтерра» Андрей БУГАЕНКО, директор по информационным технологиям компании, называет «копеечными» – но готов мириться с этим обстоятельством, поскольку услуга оказалась якорной для основного бизнеса оператора.

Андрей БУГАЕНКО

– На внедрение комплекса защиты от DDoS-атак на сети «Синтерра» в 2009 г. компания потратила около $2 млн. Насколько они соотносятся с доходами от услуг, которые вы оказываете клиентам с помощью этой системы?

– Система основана на двух решениях разных вендоров – Arbor Networks и российского «МФИ-Софт». Надо сказать, что других «тяжелых» и реально работающих решений для магистральных операторов на рынке нет. Разработку «Периметра» компания «МФИ-Софт» выполнила по нашему заказу, функционально он соответствует продукту Arbor и даже превосходит зарубежный аналог: например, на основе композиции анализа транзитного трафика и сигнатур вредоносных приложений, выявляемых в нем, наш продукт умеет строить свою внутреннюю точную карту бот-сетей по всему миру, выявлять центры управления бот-сетями, гарантированно не содержит недокументированных возможностей и т.д. Изначально мы предполагали, что система будет защищать только нашу сеть, но потом поняли, что это нужно и нашим клиентам.

Начав работы по созданию собственного продукта совместно с партнерами в 2008 г., в 2009-м мы уже использовали тестовые образцы «Периметра». Примерно в то же время у нас стартовала программа «40x40» (объединение 40 ЦОДов по всей России 40-гигабитными магистралями) – и мы решили предложить нашим клиентам услугу защиты от DDoS-атак в дополнение к размещению их ресурсов в ЦОДе. Стоит такая услуга около 250 руб. за 1 Мбит/с, т. е. за 10 Мбит/с клиент платит 2500 руб. в месяц плюс инсталляционный платеж, за канал 1 Гбит/с – 100 тыс. руб. в месяц. При этом услуга подразумевает круглосуточную поддержку и ограниченную возможность обращаться к нашим экспертам в области информационной безопасности.

Видя тот объем задач, которые мы выполняем для наших клиентов, я считаю, что она должна быть дороже, но это мое личное убеждение. Сейчас затраты на внедрение Arbor уже окупились; инвестиции в «Периметр» более длинные, но зато эта система должна принести нам дополнительную прибыль за счет ее продаж и возможности использования нашей разработки в интересах спецпотребителей. Когда она была впервые представлена на широком рынке (это произошло на «Связь-Экспокомме» в нынешнем году), мы увидели живой интерес ряда операторов связи, госзаказчиков, банковского сообщества.

– Так кто будет продавать этот продукт – «Синтерра» или «МФИ-Софт», и чей это продукт – ваш или разработчика?

– Это наш продукт. Но поскольку его захотели купить и другие компании (а мы как оператор продаем инфокоммуникационные услуги, но не аппаратное обеспечение или проекты по внедрению), мы уполномочили «МФИ-Софт», компанию-разработчика, продавать этот продукт. Продажи в существующей модели бизнеса одинаково выгодны и нам и партнеру. Продукт получился действительно нужный рынку, поскольку DDoS-атаки происходят все чаще, они все мощнее, изощреннее, целенаправленнее, все больше влияют на деловую активность.

Отдельная история, почему система интересна оператору. Для нас как магистрального оператора защита от DDoS-атак – лишь небольшая область ее применения, и только ради этого нет смысла покупать настолько дорогостоящее оборудование. А вот то, что система «видит» всю маршрутизацию трафика на узлах сети, позволяет вести мониторинг сетевой активности – с учетом вредоносной – на магистралях и клиентских окончаниях, дает нам неоценимый результат с позиций оптимизации затрат.

Кстати, и вопрос о справедливом разделении доходов между участниками рынка средств и услуг обеспечения ИБ, на мой взгляд, с включением оператора и его партнеров в создание технологий решается очень просто. Сейчас на рынке командуют вендоры: например, за

сколько хочет Arbor продать – столько и запрашивает, а хочет, естественно, максимум, и максимум может подниматься выше уровня целесообразности по отношению к цене страховки от рисков ИБ. Цена справедливая – но на монопольном рынке. У покупателей выбора нет. Кто мешает оператору вкладываться в R&D, создавать нужный рынку продукт – и зарабатывать потом и на продукте, и на услугах? Я считаю, мы сделали выгодное вложение, у продукта хорошие перспективы.

– Услуги ИБ от оператора – это уже рынок или только его возможность?

– Скорее начало его формирования. Каждый универсальный оператор в нашей стране сейчас старательно формирует рынок этих услуг. Он может предложить клиенту действительно комплексную телеком-услугу в пакете с сервисами ИБ. Клиенту легче и о цене договориться с одним поставщиком услуг, и снять с себя головную боль в виде тендеров на создание или модернизацию собственной инфраструктуры со средствами безопасности, в виде операционных затрат на обслуживание, капитальных затрат на развитие и т.п.

На мой взгляд, в «базовый пакет» услуг ИБ от оператора должно входить то, без чего корпоративный клиент не может обойтись в принципе. А он не может обойтись без VPN, без защиты персональных данных в соответствии с ФЗ-152 (я убежден, что это должна быть услуга оператора для предприятий с территориально распределенной инфраструктурой), без защищенной голосовой связи. В ЦОДах, которые есть у всех операторов, клиентам требуются услуги предотвращения внешних воздействий и их устранения (системы IPS/IDS), защиты от спама и от вредоносного ПО. Ну и, конечно, интернет-ресурсы клиентов надо защитить от DDoS-атак.

– Вы считаете цены на услуги защиты от DDoS заниженными. Почему не повысите?

– Вопрос, наверное, больше к маркетологам и коммерсантам. Лично я готов мириться с этим, потому что оператору можно и нужно зарабатывать не на борьбе с DDoS-атаками, а на основных видах бизнеса – инфокоммуникационных услугах. При этом у нас есть как минимум три существенных преимущества на этом рынке. Во-первых, мы можем предложить клиенту систему мониторинга качества предоставляемых нами услуг (SLA) – и готовы на штрафные санкции со стороны заказчика, если качество не соответствует заявленному уровню. Во-вторых, мы готовы предложить в дополнение к услугам связи защиту от кибератак. В-третьих, мы развиваем российские продукты, что дает нам преимущества в глазах спецпотребителей основных услуг. Дополнительная недорогая услуга увеличивает привлекательность основного бизнеса – не было случая, чтобы клиент отказался от такого предложения.

Так что не надо «в лоб» обеспечивать окупаемость сервисов ИБ, надо делать их якорными услугами, которые позволяют продать больше основных услуг с более высоким качеством. ИКС

Защита платного контента – это плохо, хорошо или правильно?

«Есть мнение», что весь контент, производимый медиаиндустрией, должен быть в свободном доступе, а технические средства его защиты (DRM) – это зло и препятствие всеобщему удовольствию. Конечно, это крайность, однако трудно спорить с тем, что люди хотят более свободного и гибкого использования премиум-контента. Как найти «соломоново решение» – баланс между желанием потребителей получать контент везде, на любом устройстве, и стремлением компаний, вложивших средства в производство контента, получать за него плату?

Киноиндустрия с многомиллиардными бюджетами, к примеру Голливуд, недавно начала предоставлять контент для мобильных платформ с использованием DRM (это необходимо производителям контента для гарантированного возвращения инвестиций). Мир приложений сейчас устроен следующим образом: если вы покупаете электронную книгу, например, на Amazon, впоследствии вы можете ее использовать на любом устройстве, поддерживающем платформу Kindle от компании Amazon, или на приложении Kindle на смартфоне на базе Apple, Android и Windows. Иными словами, если пользователь меняет устройство, его контент следует за ним. При переходе к другому провайдеру для доступа к этому контенту нужно будет просто открыть другое приложение, использующее DRM. Провайдеры видео- и музыкального контента все чаще прибегают к аналогичной модели. Подписка, скажем, на ресурсы Love Film или Sportify, подразумевает неограниченный доступ к этим сервисам на весь период подписки, и пользоваться им можно на самых разных устройствах, включая ПК, ТВ, смартфоны и планшеты.

Теперь Голливуд и производители бытовой электроники пошли дальше – навстречу желанию потребителей «купить единожды и использовать где угодно». В конце этого года разработанная ими технология UltraViolet будет запущена в США и Великобритании. Эта инициатива позволит приобретать бессрочное право на контент и получать его на любом устройстве, поддерживающем UltraViolet. Если файл контента потерялся или потребитель приобрел другое устройство, файл можно передать или скачать снова без дополнительных затрат. Если электронный «поставщик», у которого был приобретен контент, вышел из бизнеса, потребитель все равно всегда получит доступ к своему контенту, поскольку его право на этот контент зарегистрировано в централизованной глобальной базе данных.

Сидящему внутри всех нас ребенку хотелось бы думать, что мы должны получать все бесплатно; но мир устроен не так и никогда не был так устроен. То, что ценно, должно продаваться по соответствующей цене. То, что драгоценно, должно быть защищено. Технология защиты контента – и есть выражение этого базисного принципа.

Кристофер ШАУТЕН, старший директор маркетинговых решений компании Irdeto

Дискуссионный клуб «ИКС»

В одной упряжке

Выясняем: как распределяется труд при предоставлении оператором услуг ИБ и как он вознаграждается, какие модели партнерства существуют и какие – оптимальны.

Затратно, неприбыльно... Выгодно!

«ИКС»: Как соотносятся затраты операторов на внедрение услуг безопасности и прибыль от их предоставления?

Александр ТРОШИН, технический директор, «Манго Телеком»: Вопрос непростой. Если система ИБ построена грамотно и «обширно», то это достаточно дорогостоящий проект, и чтобы он окупился, нужно продавать этот ИБ-сервис либо очень дорого, либо довольно большому числу клиентов. А на это, по моим расчетам, нужно около двух лет. Да и то если рассматривать эту систему только по одному параметру эксплуатации (например, «угрозы»). Система состоит из активных компонентов: сети передачи данных, анализа трафика, аналитических инструментов, средств хранения информации и прочего. По сути дела, это комплексная система, на которую может быть возложена и иная роль – скажем, отработка примитивных правил маршрутизации. Иными словами, как таковое каналообразующее оборудование может рассматриваться сервис-провайдером как часть модернизации инфраструктуры в целом. И к тому же на этих узлах он может уже строить систему ИБ.

А. МАШКОВ

Алексей МАШКОВ, директор по ИТ, «Центральный Телеграф»: Соотношение затрат на внедрение услуг безопасности и прибыли, получаемой при последующем предоставлении этих услуг, зависит от ряда факторов. Во-первых, от наличия необходимого оператору связи решения у системных интеграторов/вендоров. При наличии такого решения основные затраты связаны с покупкой необходимого оборудования, лицензий на программное обеспечение, а также с работами по внедрению и техническому обслуживанию. При его отсутствии – возникают дополнительные затраты на его разработку. В том случае, если базовая услуга уже реализуется на вычислительных мощностях оператора связи, основные затраты производятся единовременно при внедрении новой услуги либо при модификации существующей. Если же оператор использует для реализации услуги арендованные мощности, получается, что его затраты распределены по времени. Тем не менее в настоящий момент приходится скорее говорить не о прибыли оператора связи от внедрения услуг безопасности, а о необходимости иметь данные услуги в стандартном пакете, в том числе и для того, чтобы оставаться конкурентоспособным на рынке.

П. АНТОНОВ

Павел АНТОНОВ, инженер-консультант, Cisco: До принятия решения о запуске той или иной услуги операторы связи просчитывают ROI, оценивая такие основные показатели, как NPV*, срок окупаемости и время вывода на рынок. Если сравнивать два подхода к запуску новой услуги – партнерство со специализированным провайдером услуги и самостоятельный запуск, – то в большинстве случаев срок окупаемости и время запуска услуги существенно ниже у партнерской модели. А если риски, связанные с запуском услуги и успешностью ее продаж, невелики, то NPV может оказаться выше при самостоятельной реализации.

*NPV, net present value – чистая приведённая стоимость. – *Прим. ред.*

Кирилл КЕРЦЕНБАУМ, представитель по продажам решений по безопасности, IBM в России и СНГ: Насколько можно судить, большой выручки операторам услуги по обеспечению ИБ не приносят. Это связано с низким спросом. Велики затраты на технологии информационной безопасности, особенно если они используются на широких каналах связи, дорого обходится оборудование. Однако несмотря на то что прибыль пока мала, перспективы развития этого сервиса значительны. Провайдеры все больше инвестируют в сферу ИБ, понимая, что им нужно защищать и свои каналы, а в будущем они смогут передавать эту защищенную платформу заказчикам.


В. АНДРЕЕВ

Валерий АНДРЕЕВ, заместитель директора по науке и технологиям, ИВК: На мой взгляд, риски компрометации таким образом построенных систем ИБ существенно выше разумных (при любой цене вопроса). Поэтому рынок и развивается столь вяло. Кроме того, стандартные способы продвижения услуг, применяемые крупными операторами связи, вряд ли будут эффективны в сфере ИБ. И рынок более узкий, и способы убеждения, вероятно, иные. А глубокий анализ непонятного рынка (которого, возможно, даже не существует), разработка стратегий, создание альтернативных механизмов продвижения, наконец, создание инфраструктуры для новой услуги... Все это не очень вписывается в привычный бизнес крупных операторов. Да и риск неудачи велик, а ведь неудача бросит тень на бренд компании. Возможно, здесь могла бы работать модель виртуальных операторов, но реальных проектов в этой сфере, насколько я знаю, нет.

Алексей ИВАНОВ, руководитель проектов, Digital Design: Как и любой новый продукт, сервис безопасности, возможно, будет окупаться достаточно долго. Особенно сейчас, когда клиенты еще не до конца понимают, зачем этот сервис им нужен. Предстоит работа по продвижению и убеждению в его преимуществах. Но поскольку расширяемость предоставления сервиса достаточно высока (при наличии резерва мощностей), то в будущем – возможно, и не таком далеком – прибыль может вырасти.


А. ИВАНОВ

Дмитрий САВЧЕНКО, руководитель бизнес-направления по информационной безопасности, «Микротест»: На первом этапе, если оператор решил оказывать такие услуги, затраты у него будут очень большие. К примеру, хорошее фундаментальное решение для оперативного управления безопасностью будет стоить для оператора более полумиллиона долларов. В некоторых случаях оператор может распределить эти затраты на пользователей – к примеру, продавая им антивирус. Однако окупаемость таких внедрений будет достигаться также небыстро. Хотя есть варианты, когда оператор может договориться с владельцем антивируса и продавать этот антивирус совместно.


С. САВЧЕНКО

Аркадий ПРОКУДИН, заместитель руководителя отдела информационной безопасности, «АйТи»: Специфика России в том, что хочется все и сразу. Это утопическая идея. Если оператор назначит желаемую высокую цену – он не сможет продать сервис пользователям и не сможет окупить свои инвестиции. Однако тут следует сделать оговорку на коррупционную составляющую. Если продвигать пускай и дорогой сервис под гарантированно лояльного государственного или коммерческого пользователя, то все может получиться с высокой маржинальностью.

Разделение доходов: все довольны?

«ИКС»: Не секрет, что основную прибыль от присутствия на рынке услуг безопасности получают вендоры. Как «перераспределить потоки», чтобы предоставление этих услуг было выгодно другим игрокам (в частности, операторам)?

А. ПРОКУДИН: Вендор получает прибыль, большая часть которой в грамотных компаниях идет на развитие. Если вендоры не будут получать хорошую прибыль – им не имеет смысла заниматься развитием своих средств защиты. Операторы связи должны искать другие пути получения прибыли – не завышая стоимость услуг, которые они фактически перепродают от вендора, а расширяя спектр сопутствующих собственных услуг.


А. ПРОКУДИН

П. АНТОНОВ: Позволю себе не согласиться с самим утверждением, что вендоры зарабатывают больше, чем операторы связи. В партнерской модели разделение прибыли, как правило, зависит от популярности услуги конкретного вендора и размеров клиентской базы конкретного оператора связи. Кто больше – тот и (совершенно логично) забирает себе бóльшую часть выручки от продаж услуги. В случае же конкуренции, когда оператор связи сам продает свои услуги, а вендор свои, – да, можно сказать, что вендоры занимают бóльшую часть рынка, нежели операторы. Это совершенно логично: вендоры специализируются на услугах ИБ, а операторы – на услугах связи.

Мы же не пытаемся что-то сделать с тем фактом, что операторы связи продают услуги связи гораздо лучше, чем вендоры.

К. КЕРЦЕНБАУМ: Нельзя сказать, что основную прибыль получает вендор. Большинство поставщиков разработали схемы лицензирования продуктов, чтобы инвестиции провайдеров синхронизировались с потенциально получаемой выручкой. Это означает, что нет необходимости сразу вкладывать много средств, а потом несколько лет ждать результата. Прибыль, которую получают провайдеры от продажи услуг, равна затратам на использованные технологии. Именно поэтому нельзя сказать, что вендоры получают основную прибыль: все зависит от операторов и от тех компаний, которые предоставляют эти услуги (например, SaaS).


К. КЕРЦЕНБАУМ

Владимир ТКАЧЕВ, технический директор, Siemens Enterprise Communications в России и СНГ: Мнение о «доминировании» прибыли вендоров в области предоставления услуг ИБ зачастую ошибочно. Любой крупный вендор при выходе на рынок предоставления услуг через операторов в первую очередь фокусируется на смещении продаж с разовых и единичных контрактов на «повторяемый» объем бизнеса. При этом значимость прибыли для вендора уходит на второй план. Кроме того, нередко даже с разовыми контрактами перед их заключением требуется большая подготовительная работа со стороны квалифицированных партнеров, которыми могут выступать операторы. При такой схеме (проведение предварительных исследований, разработка концепции, формирование методических принципов применения норм ИБ, обучение персонала) доля самого продукта в стоимости общего решения уменьшается, поскольку все это требует дополнительных затрат.


В. ТКАЧЕВ

Д. САВЧЕНКО: Вендоры зачастую не предоставляют услуги, они предоставляют только свои продукты. С другой стороны, сейчас существуют вендоры, которые продают, к примеру, антивирусы, антиспам, URL-фильтры. Они тоже, по сути, зарабатывают на услугах. Но это делается не конкретно в России, так происходит во всем мире. Вендоры постоянно анализируют вирусы и под них разрабатывают антивирусы, а подписка на них стоит денег, и это тоже услуга, на которой зарабатывают профильные вендоры. Оператор либо какой-то центр по обеспечению оказания услуг безопасности никогда сам не будет вести такие разработки, скорее они будут приобретать подписки у тех же вендоров. В данной ситуации значительную роль играет добавочная стоимость. Мое мнение таково, что не надо пытаться забрать что-то у вендоров, это экономически неоправданно.

Дмитрий ОГОРОДНИКОВ, директор по направлению информационной безопасности, INLINE Technologies: Сам переход от модели поставки решений и коробок к модели предоставления услуг предусматривает перераспределение потоков. Операторы начинают наиболее полно задействовать оборудование ИБ, обслуживать максимальное количество клиентов, загружая оборудование «по максимуму». А поскольку клиент платит за услугу, то достаточно быстро капитальные затраты на внедрение окупаются, и поток прибыли идет в сторону оператора.

А. МАШКОВ: В настоящее время пока наблюдается устойчивая тенденция: вендор стремится самостоятельно продвигать и продавать конечному потребителю свой продукт даже в тех случаях, когда он работает через оператора связи. Используется стандартная агентская схема, в которой оператор связи является фактически агентом по распространению продукта вендора. В такой схеме вендор в любой момент имеет возможность заключить договор с заинтересовавшим его, но уже работающим абонентом напрямую, исключив из процесса оператора связи. Считаю, что более перспективна партнерская схема, в которой именно оператор будет выступать как полноценная точка предоставления услуг безопасности конечному абоненту и регулировать тарифную политику в рамках партнерского взаимодействия с вендором.

Тройственный союз: за и против

«ИКС»: Нужна ли для продажи операторских услуг «третья сторона» – специализированная компания?

В. ТКАЧЕВ: Правильный ответ на этот вопрос – да, для широкого рынка такая организация нужна. Но в большинстве компаний принят более традиционный подход, когда сам провайдер формирует собственное подразделение для предоставления ИБ-услуг. Причина этого – в отсутствии нормальной практики аутсорсинга на рынке в целом. Возможно, в ближайшем будущем начнут появляться узкопрофильные компании, предлагающие типовые решения ИБ, которые смогут их бесшовно интегрировать с иными пакетами услуг от провайдера, однако этот процесс не будет быстрым.

К. КЕРЦЕНБАУМ: На мой взгляд, «третья сторона» не требуется. Существует две схемы оказания услуг информационной безопасности. В первом случае предоставлять сервис может вендор. Во втором случае провайдером услуг может быть оператор – обычно это касается Интернета и каналов связи. Опера-

тор может заключать договор с производителем, устанавливать определенные технологии и предоставлять их клиентам.

П. АНТОНОВ: Нельзя сказать, что во всех 100% случаев оператору связи не обойтись без партнерства со специализированной организацией, провайдером услуг ИБ. На рынке есть много примеров, когда операторы самостоятельно запускают услуги ИБ, а не перепродают партнерские. Преимущество такого подхода в том, что не нужно делиться выручкой от продажи услуги с партнером. Но и недостатки есть – это и существенные затраты на запуск услуги, более длительное время вывода ее на рынок и риск, что услуга не окупит сделанные инвестиции.


Д. ОГОРОДНИКОВ

Д. ОГОРОДНИКОВ: Операторы заинтересованы в том, чтобы самостоятельно предоставлять основные услуги своим пользователям. Однако построение подобной инфраструктуры и обслуживание систем требует больших вложений. Операторы ожидают получить максимальную прибыль, в то время как пользователи – максимальное количество услуг. В интересах обеих сторон операторы могут предоставлять свою технологическую платформу третьей стороне – провайдерам контента и услуг – для организации специализированных сервисов. В основе взаимовыгодного сотрудничества – модель разделения прибыли, а также снижение рисков для обеих сторон: оператор связи не тратит средства и ресурсы на продвижение услуги, а сервис-провайдер использует уже готовую инфраструктуру и транспорт.


Д. КОСТРОВ

Д. САВЧЕНКО: «Третья сторона» не всегда необходима, хотя зачастую она более продуктивна. Например, сейчас на рынке есть компания Zscaler, которая оказывает услуги безопасности по принципу аутсорсинга. Zscaler специализируется на развертывании территориально распределенных ЦОДов, которые оказывают услуги безопасности корпоративным клиентам – антиспам, URL-фильтры, защита от DDoS-атак, управление корпоративной безопасностью. Иными словами, компания построила свой бизнес как третье лицо между конечными пользователями и операторами связи. Однако такой вид услуг достаточно затратен, поскольку нужно прилично вложиться в развитие инфраструктуры, необходимой для оказания подобных услуг.

А. ПРОКУДИН: Я считаю, что на данный момент большинство операторов связи в состоянии предоставить услуги по защите информации самостоятельно. Начинающим же операторам предпочтительно привлекать «третью сторону», которая уже, как говорится, «собаку съела» в этом вопросе.

А. МАШКОВ: Ответ на этот вопрос зависит от модели ведения бизнеса оператора связи. Однако сейчас распространена практика, когда «третья сторона» не только участвует во внедрении новой услуги на вычислительных мощностях оператора связи, но и в дальнейшем обеспечивает техническую поддержку реализованных решений. Возможен другой способ, при котором оператор связи арендует вычислительные мощности «третьей стороны» для оказания своим клиентам тех или иных услуг.

Дмитрий КОСТРОВ, директор по проектам департамента информационной безопасности, МТС: Привлечение к проекту третьей стороны-подрядчика позволяет оператору значительно сократить время вывода услуги на рынок и резко снизить затраты. Но в самом начале договоренностей с этой стороной важно прописать все условия по SLA. Для посредника было бы также целесообразно предоставлять сервис безопасности в виде security cloud. Наличие лицензий регуляторов приветствуется, но это не главное. Главное – это правильный SLA.

Оптимальное партнерство

«ИКС»: Существует ли оптимальная модель партнерства при предоставлении услуг ИБ оператором/провайдером?

В. АНДРЕЕВ: Оптимальной модели пока что нет – потому что не сформирована доверенная среда партнеров, которым можно безусловно доверять с точки зрения ИБ, основывая эту оценку на объективных критериях. Существует несколько компаний, которые на волне новой аутсорсинговой риторики пытаются позиционировать на рынке новую ИБ-услугу. Но здесь как раз очень кричать не надо. Все дело — в доверии. Телеком имеет определенные преимущества перед ИТ-компаниями, к нему доверие выше, он ведь практически государственный. У них могло бы пойти, если бы была хорошая цена и уровень защиты.


И. ЯРТЫМ

Игорь ЯРТЫМ, директор по развитию и маркетингу услуг ИТ-аутсорсинга, Tieto: Оптимальная модель партнерства заключается в том, что услуги по ИБ должны предоставляться специализированными ИТ-

компаниями – системными интеграторами, которые, в свою очередь, собирают под своим зонтиком и используют операторов и вендоров.

А. ТРОШИН: Все зависит от типа и размера конкретного бизнеса клиента, от его структуры. Если это средний и малый бизнес и если компания, например, пользуется выделенными серверами от каких-то провайдеров и от операторов, для них взаимодействие удобно в рамках единого договора по размещению и поддержке оборудования. В таком случае оператор связи либо дата-центр напрямую предоставляют и гарантируют определенный набор услуг в рамках ИБ. Так как у представителей SMB, как правило, не бывает своих экспертов (а по сути нет ни желания, ни времени заниматься экспертизой ИБ), эти компании полагаются целиком и полностью на компетенции сервис-провайдера. А в большом бизнесе интеграторы (эксперты) могут либо привлекаться для построения систем ИБ (если у крупной корпорации есть определенные бизнес-риски или если информация, исходящая от компании, имеет высокий уровень секретности, не стоит полагаться исключительно на услуги сервис-провайдеров), либо выступать «третьей стороной».

А. ТРОШИН

П. АНТОНОВ: Наиболее интересной моделью предоставления услуг ИБ, на мой взгляд, является партнерство оператора связи со специализированными провайдерами услуг ИБ и перепродажа этих услуг своим клиентам под своим брендом. Такая модель обладает рядом преимуществ для всех участвующих сторон. Во-первых, специализированный провайдер услуги, зачастую вендор, за счет партнерства с операторами связи получает прямой выход к широкой клиентской базе потенциальных потребителей услуги ИБ, которыми являются абоненты операторов. При этом вендор, отдав на аутсорсинг операторам процесс продаж, может сосредоточиться на развитии одной-единственной услуги, делая ее лучшей на рынке. Во-вторых, оператор связи за счет выстраивания партнерских отношений с несколькими специализированными вендорами получает возможность быстро запустить целый спектр новых услуг с минимальными затратами и, соответственно, минимальными рисками в случае, если какая-либо услуга «не пойдет». Наконец, в случае реализации такой модели оператором клиент может получать целый набор ИТ-услуг из одних рук, что, несомненно, удобнее, а в итоге и дешевле, чем иметь отношения с целым рядом провайдеров, специализирующихся каждый на одной услуге.

Где провести линию защиты

Олег ГЛЕБОВ,
продакт-менеджер,
компания
«Информзащита»

Среди решений для обеспечения информационной безопасности в сетях операторов сегодня наиболее перспективны системы, разработанные специально для защиты виртуальных сред и облачных инфраструктур. Многие эксперты рассматривают операторов как основных поставщиков сервисов SaaS, IaaS и PaaS в ближайшие годы. Именно такие критерии, как обеспечение безопасности услуги, подтверждение ее уровня и возможность контроля безопасности станут определяющими при выборе поставщика облачных услуг.

Для решения этих задач операторы предлагают специализированные продукты для защиты виртуальных сред, облачные антивирусы, специализированные системы обнаружения и отражения сетевых вторжений (IPS/IDS).

Особняком стоят решения, которые изначально разрабатываются под модель бизнеса операторов. В классическом проекте защита от DDoS-атак начинается с развертывания таких решений для собственных нужд оператора. Это защита как от внешних атак, так и от внутреннего DDoS, поскольку для оператора именно DDoS-атака из собственной сети (от клиентов) может быть крайне опасна. Целью ее могут стать внутренние серверы оператора, например почтовые или файловые хранилища, которые в случае успешной атаки окажутся недоступны для клиентов.

Текущая ситуация с законодательством, безусловно, ограничивает применение на стороне оператора специализированных решений для защиты персональных данных. Клиентам можно посоветовать устанавливать такие продукты в собственных сетях, не вынося критичные данные вовне. Это как минимум упростит прохождение проверок со стороны регуляторов. Тем более что в рамках законодательства и на практике невозможно пока регламентировать совместную обработку персональных данных и соразмерную ответственность оператора согласно стандартному SLA. Сейчас в России нет ни одного успешного проекта по защите «облака» сертифицированными средствами для обработки персональных данных.

Аналогично обстоит дело с системами противодействия утечке данных (DLP). Такие системы должны частично охватывать арендованную у оператора инфраструктуру, но управление ими и основной контроль трафика целесообразнее оставить в рамках собственной компании. При этом более крупные системы обнаружения уязвимостей и управления политиками доступа оператор может предложить клиентам именно на своей стороне. Внедрение таких систем станет одним из первых шагов к управляемой защите.

ПОДРОБНОСТИ

Security as a Service

В терминологии облачных вычислений услуга информационной безопасности называется Security as a Service, что подразумевает перевод антивирусов, спам-фильтров и других программ либо в частное облако самой компании, либо на аутсорсинг провайдеру, предоставляющему соответствующий сервис. При этом главные факторы, сдерживающие переход организаций к «облакам», – вопросы безопасности данных, хранимых в облачных средах. Как провайдер облачных услуг может защитить данные клиента? Чем для пользователя интересна эта услуга? Попробуем разобраться.

Что должен знать клиент

Алексей АРТЮХИН,
системный инженер
Digital Design

Чем это удобно

Любая организация может начать использовать Security as a Service, просто обратившись к провайдеру облачных вычислений. Тогда все работы по поддержанию работоспособности облачных систем безопасности берет на себя подрядчик, а организация только оплачивает предоставленные сервисы. Этот вариант наиболее подходит средним и малым компаниям. Крупному бизнесу может потребоваться развернуть частное облако, которое будет соответствовать жестким стандартам безопасности и другим корпоративным требованиям. В частности, для банков, государственных и финансовых структур предпочтителен именно такой вариант, который гарантирует, что конфиденциальная информация будет обрабатываться внутри организации.

Как это делается

Для получения доступа к сервисам в «облаке» со своего рабочего места пользователи, находящиеся за корпоративным брандмауэром, могут использовать браузер либо, при необходимости, специальные программы-агенты. Сотрудники компании могут также получать доступ к облачным сервисам вне офиса с мобильного или другого устройства, имеющего выход в Интернет.

Большая часть данных обрабатывается внутри «облака». Благодаря этому пользователи имеют дело только с отфильтрованной и безопасной информацией. Многие провайдеры облачных вычислений предоставляют также услугу поиска уязвимостей в сети компании, что дает клиенту взгляд извне на бреши в безопасности.

Удачным решением является размещение службы защиты от спама и DDoS за пределами организации, поскольку это существенно снижает нагрузку на корпоративную сеть – за счет уменьшения объема передаваемых данных. Перенос антивируса в «облако» позволяет переместить ресурсоемкие задачи с пользовательских компьютеров на мощные серверы в «облаке». Исчезает необходимость хранить локально базы сигнатур, объем которых растет с каждым днем, и заботиться об их своевременном пополнении. Благодаря этому удается быстрее и эффективнее вести поиск вредоносных программ и обнаруживать зараженные файлы.

Конечно, перенос всех расчетов с компьютера пользователя на сервер генерирует в сети дополнительный трафик. Но современные технологии помогают уменьшить нагрузку на сеть (например, при проверке на вирусы на сервер отправляется не весь файл, а только специально рассчитанная контрольная сумма, которая сравнивается с базой сигнатур).

Не рекомендуется переносить в «облако» брандмауэр, так как он требует непосредственного доступа ко всему трафику сети, что может снизить скорость для пользователей. Также следует учитывать, что зачастую необходимо устанавливать программы-агенты на каждый компьютер, с которого будет осуществляться доступ к сервисам безопасности в «облаке».

Основные решения

На сегодняшний день на рынке имеются решения для предоставления услуг Security as a Service от разных вендоров. Из наиболее известных назовем McAfee Security SaaS, Panda Security Cloud Protection, Symantec.cloud, Zscaler Cloud Services. Все решения примерно одинаковы по функционалу: они обеспечивают фильтрацию спама, поиск вредоносных программ, защиту от угроз из сети, блокировку нежела-

тельных сайтов, защиту от вирусов и решение других задач, необходимых для поддержания безопасности. Основные различия между ними – в стоимости программ, удобстве их администрирования и необходимости установки дополнительного ПО на компьютеры пользователей. ИКС

Что должен уметь провайдер

В обеспечении безопасности клиентских данных должны в той или иной мере участвовать и клиент (потребитель), и провайдер облачных услуг. «Распределение обязанностей» будет сильно зависеть от используемой модели – SaaS, PaaS или IaaS.

Как следует из свойств самих облачных моделей, провайдер несет тем большую ответственность за выполнение требований по защите данных, чем большую часть инфраструктуры облачного сервиса он контролирует. Например, в IaaS-модели провайдер контролирует лишь физическую и виртуальную среду, в которой работают виртуальные машины клиентов; он не занимается обслуживанием ОС и приложений, функционирующих внутри самих виртуальных машин.

Совсем иначе обстоит дело с SaaS-моделью, при которой провайдер облачной услуги полностью контролирует физическую и логическую инфраструктуру приложения, занимается его разработкой и обслуживанием, оставляя пользователю лишь возможность загружать свои данные и работать с ними. В этом случае на плечи провайдера ложится самая существенная часть задач информационной безопасности, а клиенту достается лишь разграничение и контроль доступа к приложению и данным.

В PaaS-модели разделение задач ИБ представляет собой нечто среднее между IaaS и SaaS – провайдер не только контролирует физическую и логическую среды выполнения программного кода, но и предоставляет разработчикам инструменты и механизмы создания собственных приложений. PaaS-провайдеру необходимо удостовериться, что инструментарий и API платформы разрабатываются с учетом требований и стандартов безопасности и не являются дополнительным источником уязвимостей. При этом сервис-провайдер должен обеспечивать комплекс организационных и технических мер, направленных на построение, поддержание и улучшение системы защиты своих активов и системы управления ИБ.

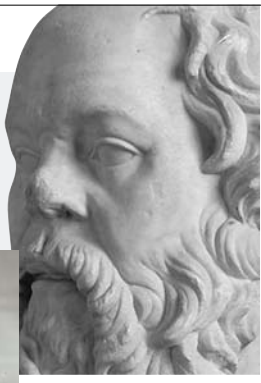
Меры обеспечения ИБ для облачных провайдеров

Технические	Организационные
■ Логическое разделение данных разных клиентов ■ Шифрование данных клиентов на разных ключах при хранении, а также их шифрование при передаче по сети ■ Использование систем обнаружения и предотвращения атак, в том числе позволяющих обнаруживать атаки на инфраструктуру виртуализации ■ Антивирусная защита и использование других средств выявления вредоносной активности ■ Межсетевое экранирование ■ Контроль физического доступа и усиленная аутентификация сотрудников при доступе в помещения ■ Управление логическим доступом сотрудников провайдера к информации клиентов, а также к инструментам, позволяющим манипулировать данными (например, клонировать диски виртуальных машин) ■ Использование систем предотвращения утечек данных (DLP) ■ Управление уязвимостями и своевременная установка патчей для всех ОС и систем	■ Наличие политики ИБ и прочих документов по управлению ИБ ■ Регулярные внутренние и внешние аудиты в соответствии с лучшими практиками, доступность их результатов клиентам провайдера ■ Регулярное проведение тестов на проникновение и сканирования на наличие уязвимостей, доступность их результатов клиентам провайдера ■ Поддержание контактов с правоохранительными органами в соответствии с требованиями законодательства ■ Инвентаризация активов и установление владельцев активов ■ Документирование процесса предоставления и авторизации доступа сотрудников к данным клиентов ■ Разделение и документирование обязанностей персонала ■ Проведение тренингов по осведомленности в области ИБ для персонала ■ Наличие плана реагирования на инциденты ИБ, отражающего разделение обязанностей между провайдером и клиентами ■ Наличие плана непрерывности бизнеса и восстановления после катастроф ■ Инвентаризация внешних поставщиков и проверка на наличие дублирующих поставщиков ■ Проверки (скрининг) персонала, имеющего доступ к данным клиентов

Наиболее экономически эффективным для провайдеров может оказаться использование решений, сочетающих в себе несколько подсистем ИБ: например, реализующих антивирусную защиту, межсетевое экранирование, обнаружение и предотвращение атак, виртуальный патчинг и управление уязвимостями, подсистему контроля целостности и модуль анализа журналов событий. С точки зрения оптимизации затрат на технические средства ИБ владельцам коммерческих облаков следует обратить внимание на те компании, которые предлагают модели лицензирования, учитывающие специфику бизнеса провайдеров.

Денис БЕЗКОРОВАЙНЫЙ, технический консультант Trend Micro Россия

аналитик



Как сдвинуть рынок

Услуги безопасности, предоставляемые операторами связи, в мире успешно развиваются, во многих странах их давно уже освоили как корпоративные, так и частные клиенты операторов. Россия к этому рынку совершенно не готова и готовится, к сожалению, очень медленно. Между тем целый ряд проблем обеспечения информационной безопасности не решить без оператора. Какие это проблемы и почему они не сдвигаются с мертвой точки?

Михаил ЕМЕЛЬЯННИКОВ, консалтинговое агентство «Емельянников, Попова и партнеры»

Массовый сегмент: инертность и невежество

С одной стороны, сами компании не спешат: внедрение и продвижение сервисов ИБ требует определенных инвестиций и, самое главное, больших маркетинговых усилий. С другой – пользователи, особенно частные клиенты, не готовы эти сервисы покупать. Нет уверенности, что при получении антивируса онлайн провайдер будет в полном объеме отвечать за безопасность. И эти сомнения во многом оправданны: каналы плохие, компьютеры старые... Конечно, очень многие люди понимают, что антивирус необходим, – и покупают (в лучшем случае) программу, устанавливают ее и настраивают самостоятельно, руководствуясь инструкциями вендора. И все же на уровне частного пользователя в абсолютном большинстве случаев все вопросы, связанные с безопасностью, решить нельзя.

Другая проблема, которую без оператора устранить довольно сложно, – это опасности, подстерегающие детей в Интернете. Минимизировать их очень трудно без предустановленного на стороне провайдера продукта, который может автоматизировать категоризацию сайтов по уровню доверия. Понимания в обществе на этот счет нет. А нет понимания – нет услуги, нет и рынка. Чтобы услуга контент-анализа «родительский контроль» стала массовой, оператор должен, как минимум, очень сильно вложиться в повышение осведомленности общества.

Иногда операторы объясняют свое нежелание вкладывать деньги в запуск таких услуг их низкой маржинальностью. С одной стороны, маржинальность, безусловно, низкая. С другой – понятие маржи у наших операторов немножко оторвано от реальной жизни. Если во всем мире маржа в 3–10% считается хорошей, то у нас меньше чем за 30–40% операторы в принципе не хотят ничего делать.

Я бы рассматривал эти сервисы в другом ракурсе – как некое дополнение к основной услуге оператора, которое повышает его конкурентоспособность. Не просто доступ в Интернет, но безопасный доступ в Интернет. Уровень безопасности станет для пользователя сильным аргументом в пользу выбора того или иного провайдера, когда мы придем к насыщению рынка интернет-доступа и обострению конкуренции на нем – рано или поздно это произойдет. Войти на рынок интернет-доступа будет довольно сложно – значит, надо войти с чем-то новым. И этим новым может быть безопасность. Наверное, по этой причине «ВымпелКом» достаточно активно занялся продвижением на массовый рынок услуги, несмотря на ее невысокую прибыльность.

Вообще же, на мой взгляд, как не парадоксально это звучит, основным драйвером продаж услуг безопасности пользователям может оказаться сотовая связь. Сейчас iPhone – это фактически компьютер по функционалу, просто у него устройства ввода-вывода довольно специфические. Для кибермошенников это сигнал заняться разработкой вредоносных программ и попытаться заработать деньги. Вирусы и фишинговые программы для сотовой связи создаются и распространяются очень быстро, а на абсолютное большинство сотовых аппаратов поставить антивирусную защиту сейчас невозможно. Пользователь, прежде чем открыть MMS-файл, не имеет технической возможности проверить его безопасность – значит, об этом должен позаботиться оператор.

Корпоративный сегмент: беспечность и недоверие

DDoS – это колоссальная угроза для всех компаний, бизнес которых «развернут» в Интернет. Защищаться от нее самостоятельно бесполезно, если мощность атаки превосходит пропускную способность канала последней мили. Это должен делать провайдер – разумеется, за определенную плату. К слову, цены, которые заявляют московские провайдеры на своих сайтах, мне представляются сильно заниженными. Сомневаюсь, что за 1500 рублей в месяц можно обеспечить корпоративную защиту от DDoS-атаки. Скорее

всего, речь идет о каких-то других услугах, которые маскируются под защиту от DDoS. Оказание этой услуги требует от оператора связи очень больших инвестиций. Существующие решения вендоров весьма дороги, сложны, требуют высокой производительности, большой вычислительной мощности, резервирования каналов и пр. Поэтому компании, ведущие бизнес в Интернете, должны закладывать более реальные бюджеты на защиту от DDoS-атак.

Эта проблема будет, на мой взгляд, с каждым годом только обостряться, поскольку DDoS – это самый дешевый способ расправиться с конкурентами, к тому же безнаказанно. Но к осознанию масштабов угрозы и поиску средств защиты от нее бизнес в массе своей еще не пришел. Многие компании лишь на третий день DDoS-атаки обращаются в специализированные организации: «Не можем справиться, приезжайте, помогите». Поздно на третий день DDoS-атаки приезжать и помогать. Об этом надо было думать раньше – и думать вместе с оператором, без него не обойтись.

Следующая колоссальная проблема, которая сейчас возникает и которую без операторской услуги не решить, связана с облачными вычислениями. Все, что пользователь передает со своего компьютера в «облако», дальше принадлежит оператору/провайдеру. И если он не обеспечит безопасность – ни один конечный клиент самостоятельно ее не обеспечит. Однако у пользователя нет доверия к оператору, поскольку нет внятных соглашений об уровне обслуживания (SLA), не работает приемлемая для клиента система страхования рисков. Недавно с помпой была анонсирована очередная программа страхования информационных рисков, однако есть основания для скепсиса – после 12 лет разговоров на эту тему, ни к чему продуктивному не приводящих, когда дело доходит до возмещения понесенных убытков. Оператор связи предлагает в качестве возмещения, например, месяц бесплатного обслуживания. Зачем компании месяц бесплатного обслуживания, если за три дня простоя бизнеса она потеряла больше денег, чем заплатила бы оператору за 100 лет обслуживания?.. И в этом вопросе мы тоже не двинемся вперед, не потратив сил на продвижение услуги, на повышение осведомленности и убеждение клиентов, на формирование внятных SLA.

К слову, и к «обычной» (не SaaS) модели сервисов информационной безопасности, предлагаемых оператором, доверия у корпоративного клиента мало. Он часто не готов отдать операторам такие элементарные вещи, как антивирусная защита, антиспам, веб-фильтрация. Между тем самостоятельно решать эти задачи дорого и сложно, особенно среднему и малому бизнесу. Гораздо проще доверить это провайдеру и договариваться с ним.

Несомненно, рынок будет развиваться. Интуитивно он готов, технически никаких проблем, по большому счету, нет. Но в силу организационных, правовых и психологических аспектов рынок стоит. ИКС

Рынок «выстрелит» рано или поздно

В широком и пестром спектре компаний – возможных участников рынка услуг ИБ в России – степень готовности и мотивация у каждого своя. Основными игроками этого рынка видятся вендоры, операторы связи и корпоративные клиенты. Так, клиентов сейчас не назовешь активными игроками, формирующими рынок. Они скорее наблюдают за появлением интересных предложений и оценивают возможные преимущества и недостатки передачи процессов обеспечения ИБ «в чужие руки». Но принципиальная готовность пользоваться такими услугами у них уже есть, особенно если учесть главное преимущество для потребителя услуг ИБ – сокращение затрат.

Различие потребностей малых и крупных предприятий в тех или иных услугах ИБ обусловлено прежде всего тем, в состоянии ли они сами решить те или иные задачи в области обеспечения ИБ. Крупные предприятия способны и могут себе позволить самостоятельно решать все или почти все свои задачи, связанные с ИБ. Но бывают и исключения, когда технически или организационно задачу невозможно решить на стороне предприятия. Нельзя, например, защититься от DDoS-атак – каким бы продвинутым не было решение, будучи установленным на стороне клиента, оно не спасет от переполнения канала связи, предоставляемого оператором. Поэтому для защиты от DDoS-атак наиболее целесообразно приобрести услугу защиты у оператора связи.

Что касается малых предприятий, то бюджетов на приобретение дорогостоящего оборудования у них нет, штат специалистов держать дорого – и в результате самые простые вопросы обеспечения ИБ оказываются практически не решенными. Поэтому у малого бизнеса есть потребность в защите от самых распространенных угроз и, соответственно, в таких услугах, как защита от вирусов и спама, веб-фильтрация, защита границы сети и т.д. Такие услуги тоже могут предлагать операторы связи.

Рынок операторских услуг ИБ в России пока только начинает формироваться. Основная причина его отставания кроется в том, что на Западе операторы уже прошли переломный момент развития бизнеса – от увеличения клиентской базы к насыщению услугами. В нашей стране этап наращивания клиентской базы операторов связи только близится к окончанию – но уже все операторы понимают, что дальнейший рост бизнеса возможен в основном за счет развития дополнительных услуг.

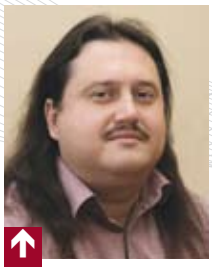
Помимо увеличения ARPU, колоссальное значение дополнительные услуги имеют и для удержания существующей клиентской базы. Когда клиент пользуется не только базовыми, но и получает от оператора еще целый ряд дополнительных услуг, решиться сменить оператора гораздо тяжелее: ведь смена единого поставщика нескольких ИТ-услуг может вскрыть целый пласт незаметных на первый взгляд нюансов и потребовать существенных инвестиций в сам процесс «переезда».

Поэтому услуги ИБ, как и любые другие дополнительные по отношению к услугам связи, в ближайшие годы станут для операторов основным источником роста объемов выручки и способом удержания клиентской базы. Но на переориентацию всех бизнес-процессов оператора связи с одной стратегии развития на другую потребуется некоторое время.

А вендоры, с оглядкой на объемы рынка услуг ИБ в Европе и США, стараются продвигать эти услуги и в России, не без оснований полагая, что рано или поздно этот рынок «выстрелит» и в нашей стране.

Павел АНТОНОВ, инженер-консультант Cisco

Безопасность по стандарту



Константин СОКОЛОВ,
директор департамента информационной безопасности АМТ-ГРУП

Тематика информационной безопасности в разрезе рынка услуг операторов связи в последнее время достаточно широко освещается. Тем не менее хотелось бы высказаться немного в другом русле, дистанцируясь от радужных прогнозов роста услуг информационной безопасности, особенно в формате SaaS.

На мой взгляд, услуги этого формата могут быть интересны в России в первую очередь физическим лицам, а также малому и среднему бизнесу (если исключить из рассмотрения филиалы и дочерние предприятия зарубежных компаний, имеющих привнесенную из-за рубежа корпоративную культуру работы с аутсорсингом и SaaS-услугами).

При работе с физическими лицами высока конкуренция с производителями антивирусного программного обеспечения (в первую очередь с «Лабораторией Касперского»). Впрочем, вступить здесь в конкурентную борьбу операторы даже не успели. Большинство услуг, которые они могут предложить, вполне заменяются широко разрекламированными программными продуктами отечественных производителей, имеющими к тому же больший функционал.

Проблемы же малого и среднего бизнеса лежат в большинстве своем не в информатизации, и тем более не в соблюдении режима информационной безопасности. Даже при 50%-ном проникновении услуг ИБ на рынок SOHO/SMB они вряд ли окупят вложения операторов – по причине незначительности самой абонентской базы. Рынки стран, демонстрировавших разумную окупаемость вложений в SaaS, характеризуются гораздо более высокой степенью развития информатизации общества и сегмента среднего и малого бизнеса.

Куда инвестировать оператору

В общем случае все вложения операторов в информационную безопасность можно разделить на три вида:

Комплекс защиты корпоративной ИТ-инфраструктуры

Компания АМТ-ГРУП выполняет полный комплекс работ по защите конфиденциальной информации, персональных данных (ПДн), ключевых систем информационной инфраструктуры, коммерческой и банковской тайны. Этот комплекс включает:

- технический и организационный консалтинг;
- проектирование, внедрение и сопровождение систем защиты информации;
- аудит существующих систем, обследование, тестирование на проникновение;
- расследование инцидентов;
- управление проектами;
- разработку корпоративных и отраслевых стандартов по ИБ;
- подготовку и проведение аттестации автоматизированной системы согласно требованиям ФСТЭК России;
- работы по обеспечению соответствия ИС стандартам и практикам СТО БР, BS/ISO 27001:2005, PCI DSS, BS25999.

Защита корпоративных информационных систем предполагает выполнение пилотных проектов на объектах заказчика со сравнительным анализом оборудования разных производителей и проведение всех стадий проектных работ (в соответствии с ГОСТом) в части создания комплексных систем информационной безопасности. Сюда включается предпроектное обследование, техническое задание, эскизное, системное, техническое, рабочее проектирование, разработка программы и методики испытаний; технический план миграции, эксплуатационная документация. После выполнения пусконаладочных работ проводятся приемо-сдаточные испытания (автономные, комплексные).

Проектирование, разработка планов миграции и внедрение систем защиты информации любой сложности охватывают такие виды защиты, как:

- защита периметра при подключении к Интернету (FW, UTM) и другим внешним сетям;
- криптографическая защита каналов связи (VPN);
- защищенный удаленный доступ (RA/SSL VPN, NAC);
- комплексная защита сегментов ЛВС/ЦОД (FW, IPS, NAC);
- защита рабочих станций (EndPoint Security);
- защита от атак типа «отказ в обслуживании» (DDoS) для операторов связи, банков, крупных корпоративных заказчиков;
- управление событиями и инцидентами ИБ (SIEM);
- безопасность Web и электронной почты;
- управление уязвимостями и соответствием требованиям регуляторов (vulnerability & compliance management;)
- защита от утечек данных (DLP);
- распределенная антивирусная защита;
- Web Application Firewall и безопасность БД
- SaaS, URL-фильтрация, фильтрация по регулярным выражениям;
- управление идентификационными данными и доступом пользователей (IDM).

1) вложения в поддержание основного вида деятельности за счет снижения рисков, связанных с безопасностью, в первую очередь с DDoS-атаками и возможным выходом из строя аппаратуры;

2) вложения в SaaS – в большинстве случаев они обеспечивают паритет с другими операторами в конкурентной борьбе за клиента и имиджевые составляющие;

3) вложения в приведение систем и процессов в соответствие с требованиями международных стандартов и российских руководящих документов.

На третьей составляющей остановимся подробнее, хотя она важна в первую очередь для операторов, имеющих свои дата-центры и оказывающих на их базе различные услуги.

Безопасность и стандарты

Какие требования, касающиеся соответствия, предъявляются сегодня к ЦОДам? В первую очередь логично поинтересоваться, как оператор выполняет требования 152 ФЗ «О персональных данных» с учетом всех дополнений и нововведений. С одной стороны, инвестиции в эту сферу оператору необходимы, чтобы снизить издержки при проверке регулирующих органов, с другой – вложения позволят привлечь потенциальных клиентов, чья деятельность связана с обработкой значительного количества персональных данных.

Следующим пунктом стоит соответствие (подтверждаемое наличием сертификата) требованиям стандарта PCI DSS, который распространяется на компании и организации, обрабатывающие информацию о держателях платежных карт. Потребности в услугах ЦОДов для размещения информационных систем, связанных с обработкой, хранением и передачей карточной информации (процессинговых центров, хранилищ носителей резервных копий данных и т.д.), будут расти опережающими темпами. В этих условиях прохождение сертификации на соответствие требованиям PCI DSS станет заметным преимуществом.

Также представляется важным наличие у оператора сертификации систем менеджмента по международным стандартам, в первую очередь ISO 27001 и BS 25999. Вложения в сертификацию соответствующих систем менеджмента по ISO 27001 и BS 25999 помогут обеспечить следующие преимущества:

- наглядное представление потенциальным заказчикам эффективности внедренных мер защиты и обеспечения непрерывности бизнес-процессов;
- демонстрация защиты внутренних средств управления и соответствия лучшим отраслевым практикам;
- независимая демонстрация соблюдения действующих законов и нормативных и регулирующих актов;
- предоставление потенциальным заказчиком данных для аудитов, проводимых третьей стороной;
- независимое подтверждение того, что риски оператора должным образом выявлены, оценены и находятся под контролем, процессы формализованы, процедуры и документация, относящиеся к обеспечению информационной безопасности, разработаны и поддерживаются;
- демонстрация устойчивости к сбоям, наличие процесса постоянного повышения устойчивости оператора к сбоям и инцидентам;
- предоставление эффективных инструментов управления непрерывностью бизнеса для потенциальных заказчиков.

Таким образом, с точки зрения окупаемости и получения реальных конкурентных преимуществ представляются разумными капитальные затраты (CAPEX) на средства обеспечения информационной безопасности основной инфраструктуры операторов и операционные расходы (OPEX) – на подготовку и проведение сертификации организации на соответствие требованиям международных стандартов, в частности PCI DSS, ISO 27001 и BS 25999. Прочие затраты будут носить ярко выраженный имиджевый характер или будут связаны с соблюдением российского законодательства.

Сертификационное производство

В 2007 г. АМТ-ГРУП стала первой компанией на российском рынке, получившей право на серийный выпуск программно-технических средств защиты информации (ПТСЗИ), отвечающих требованиям Федеральной службы по техническому и экспортному контролю (на основе продуктов компании Cisco). Выпускаемое АМТ-ГРУП оборудование входит в Государственный реестр сертифицированных средств защиты информации ФСТЭК России.

Согласно требованиям российского законодательства, ПТСЗИ, использующиеся в системах обработки конфиденциальной информации и персональных данных, подлежат обязательной сертификации. Сертификация ПТСЗИ подтверждает, что законодательные требования и требования ФСТЭК данным оборудованием выполняются.

Наличие у АМТ-ГРУП данных сертификатов значительно сокращает время получения заказчиком сертифицированного оборудования и ввода автоматизированных систем в эксплуатацию.

Специалисты АМТ-ГРУП проводят испытания ПТСЗИ на соответствие требованиям ФСТЭК России и предоставляют заказчикам сертифицированные ПТСЗИ с комплектом документов, соответствующим российскому законодательству:

- ✓ заключение о результатах тестирования оборудования на соответствие требованиям ФСТЭК (заполняется для каждой единицы тестируемого оборудования);
- ✓ специальный защитный знак соответствия сертификату (голографический знак ФСТЭК России, нанесенный на фронтальную часть оборудования);
- ✓ копия сертификата ФСТЭК России с реквизитами отдела сертификационного производства;
- ✓ паспорт на ПТСЗИ.

Концептуальный поворот

Технологические сети операторов

Посторонним вход воспрещен *или* Добро пожаловать?

Операторы связи предлагают сегодня своим абонентам новые услуги, в том числе в области ИБ. Между тем их собственные технологические сети могут оказаться слабым звеном с точки зрения безопасности, считает Наталья БАТАЛОВА, руководитель направления по работе с телекоммуникационными компаниями Центра информационной безопасности компании «Инфосистемы Джет».

Наталья БАТАЛОВА

– Технологические сети операторов строились, эксплуатировались и развивались десятилетиями. Почему сейчас их безопасность оказалась под сомнением?

– Корпоративные сети и ИТ-системы операторов в основном уже «обнесены тройным забором», сейчас здесь скорее стоят задачи оптимизации и управления ИБ. Что же касается технологических сетей, на которых, собственно, и оказываются услуги связи, то ранее они были довольно закрытыми, поскольку в них применялись специализированные системы и протоколы, они были разделены и защищены от типичных угроз IP-сетей. С переходом на стандартные платформы и протоколы, с объединением сетей, их взаимодействием с Интернетом угрозы, характерные для IP-сетей, перекочевывают в технологические сети. Теперь при наличии определенных условий – уязвимостей элементов продуктивной сети – злоумышленник может добраться сначала до периметровых устройств, а затем до внутренних ресурсов и транспортных узлов оператора. Следует отметить и появление понятия «технический фрод» – это мошенничество, основанное на уязвимостях компонентов технологических сетей: манипуляции с системами оператора, несанкционированный доступ к абонентскому оборудованию и услугам (взломы call-центров, PBX и IP-PBX) и др.

– Это гипотетические угрозы, или имеют место реальные инциденты на сетях операторов?

– Аудиты на продуктивных сетях операторов во многих случаях показывают, что для таких инцидентов существуют довольно благоприятные условия. Вполне реальны (а иногда, к сожалению, воплощаются в жизнь) угрозы проникновения во внутреннюю сеть оператора со стороны абонентов (взломы точек Wi-Fi, перехват парольной информации и т.д.), получения доступа к оборудованию технологических сетей, нарушения доступности сетевой инфраструктуры и прекращения предоставления услуг физическим лицам и корпоративным клиентам, атак на критичные приложения, вмешательства в передачу информации абонентами (перехват конфиденциальной информации), получения доступа к учетным записям абонентов (манипуляции со счетами, блокирование доступа к услугам) и т.д. Риски и потери оператора сложно переоценить: ущерб репутации, отток абонентов, санкции со стороны регулирующих органов и, разумеется, финансовые потери. Последние, в соответствии с расчетами нашей компании, могут исчисляться десятками и сотнями тысяч долларов в час в зависимости от вида услуги: это недополученная выручка от оказания услуги, авральная работа call-центров по обработке претензий (до нескольких десятков тысяч звонков от абонентов в час), расходы на поиск причин и восстановление услуги, в том числе оплата работы сервисных и аварийных служб. По нашей информации случались сбои, длившиеся не один час. Потери от технологического фрода исчисляются близкими величинами.

Согласитесь, при таком масштабе возможных потерь разумно заняться их предотвращением. Все понимают, что техно-

логические сети – опора бизнеса операторов связи, что доходы операторов напрямую зависят от работоспособности и соответствия рыночным потребностям магистральных сетей, сетей мобильной и фиксированной связи. Для обеспечения их безопасности и защиты от мошенничества необходим системный подход, но реально проблемы пока решаются фрагментарно, по мере возникновения инцидентов безопасности и фактов мошенничества.

– И всему виной переход на IP?

– IP – это чисто техническая предпосылка, притом не единственная. В действительности причин уязвимостей сетей гораздо больше.

Технологические сети огромны по своему масштабу, разнообразию и количеству единиц оборудования (десятки и сотни тысяч), это очень сложный объект (а точнее, множество объектов) защиты как с технической, так и с организационной точки зрения.

Большинство крупных компаний-операторов, оказывающих сегодня разнообразные услуги мобильной и фиксированной связи, создавались путем слияний и поглощений более мелких. При объединении с сетями приобретенных компаний, зачастую имеющих более низкий уровень безопасности и защиты от мошенничества, угрозы перекочевывают в объединенную сеть, а проблемы с безопасностью одной сети влияют на работоспособность всей компании.

Гонка на опережение, в которой главное – поскорее запустить и анонсировать, скажем, новую услугу, вынуждает оставлять вопросы безопасности продуктивных сетей на втором плане. Быстрое развитие сетей, внедрение новых технологий, еще не исследованных с точки зрения безопасности, – головная боль для «безопасников». Ни компетенций, ни штата не хватает.

Дизайном и строительством сетей, поддержкой оборудования и управлением им (в том числе удаленно) занимаются множество подрядчиков, в телекомах внедряется практика передачи оборудования и целых сетей на аутсорсинг. И всё это создает дополнительные проблемы: нет гарантий безопасности и отсутствия «дыр», оставленных подрядчиками для своего удобства. Усугубляет ситуацию то, что вопросы строительства и обслуживания технологических сетей в регионах в ряде случаев технически слабо контролируются из центра.

Наконец, подразделения развития и эксплуатации технологических сетей и безопасности в большинстве случаев отделены друг от друга и не всегда находят общий язык.

В итоге в сетях бывает намешано всё – критичное и некритичное оборудование разного назначения, основное и вспомогательное; много не инвентаризированных, «забытых» устройств, физическое местонахождение и владельцы которых неизвестны; на критичном оборудовании работает устаревшее уязвимое ПО, используются «слабые» настройки либо настройки по умолчанию; в сетях работают устройства с незащищенными интерфейсами управления, открытыми портами; для администрирования оборудования применяются небезопасные способы и т.д.

Из-за отсутствия (в ряде случаев) единой системы инвентаризации возникают сложности со сбором информации о сетях, устройствах, конфигурациях, владельцах оборудования и др. Поэтому проблемы порой остаются без внимания годами, пока они не обнаружатся в процессе аудита или, что хуже, – не будут использованы злоумышленниками.

Очевидно, что проблема назрела, и сейчас операторы движутся в направлении безопасности своих продуктивных сетей.

– Какие задачи нужно решить для улучшения ситуации?

– В идеале требуется решить ряд задач, касающихся не только безопасности: это инвентаризация (поскольку без актуальной информации о структуре, составе, расположении элементов сетей подступаться к вопросам безопасности нереально); анализ дизайна сетей с точки зрения безопасности и оптимизации; оценка текущего уровня защищенности элементов данных сетей; контроль настроек оборудования с точки зрения безопасности и мошенничества; сбор, анализ и корреляция событий на критичном оборудовании, в том числе корректная отработка инцидентов безопасности в системах тикетинга; обеспечение правильно организованного, безопасного управления и администрирования, подключения абонентов и др. И это не только технические задачи – нужны также стандарты и регламенты по обеспечению безопасности технологических сетей. В их разработке и внедрении в жизнь, как уже понятно, должны участвовать не только подразделения ИБ, но и подразделения, ответственные за эксплуатацию и развитие технологических сетей.

Для слаженной и эффективной работы над решением такого огромного пласта задач необходимо, чтобы руководство телеком-компаний осознало существующие угрозы безопасности технологических сетей и, как следствие, угрозу бизнесу.

– Может ли оператор справиться с этими задачами самостоятельно, или потребуется привлекать экспертов?

– Как уже говорилось, огромный масштаб сетей, разнообразие и постоянное развитие технологий, обилие оборудования разных производителей означает, что службам безопасности просто нереально все это охватить. Полагаю, что операторам необходимо участие приглашенных экспертов по ИБ в проектах по построению/модернизации/развитию технологических сетей и их сегментов, систем мониторинга, управления, тикетинга, в работе над созданием системы контроля безопасности технологических сетей. Ценность системных интеграторов – наличие компетенций в нескольких областях, в данном случае – знание специфики технологических сетей операторов (применяемых технологий, протоколов, оборудования и ПО) с точки зрения безопасности, а значит, понимание того, где могут возникнуть проблемы, какие технологии, протоколы, типы устройств уязвимы. Особенная ценность интегратора в решении рассматриваемой проблемы – это способность наладить совместную работу служб ИБ и подразделений, ответственных за эксплуатацию и развитие технологических сетей, умение говорить и с теми и с другими на одном языке. ИКС