Ну что, коллеги — поТОПали в 2013 год?

Роман Кобцев
Директор Департамента развития и маркетинга ОАО «ЭЛВИС-ПЛЮС»

Чем ближе к новому году, тем больше как из рога изобилия лились различные прогнозы. Давайте теперь посмотрим на некоторые из них.

Для начала я предлагаю взглянуть на тренды информационных технологий (ИТ) в целом, т.к. информационная безопасность (ИБ) является все-таки частью этого рынка. Аналитическая компания Forrester Research провела под конец ушедшего года интересный вебинар «2013 Tech Trends For Europe And The World». Аналитики Forrester выделяют ТОП-4 ИТ-вызова следующего года, которые будут с разной степенью воздействовать на бизнес:

1. Облачные вычисления.
2. Мобильность.
3. СМАРТ-компьютинг.
4. ИТ-консьюмеризация.

Общий рост глобального ИТ-рынка, по мнению аналитиков Forrester, составит в 2013 году примерено 4%. И если по сегментам (аутсорсинг, консалтинг, ПО, коммуникационное и компьютерное оборудование) рост его будет примерно одинаковым, то по регионам рынок будет расти неравномерно – США больше, Европа меньше. В Европе лидерами роста будут являться Швеция, Великобритания, Франция и Германия, а страны Южной Европы ждет серьезное снижение. А вот сегмент ИБ, по мнению уже, правда, Gartner, будет расти быстрее, чем рынок ИТ в целом – рост составит примерно 8%. Эта тенденция, конечно, не может не радовать игроков рынка безопасности. А какие тренды будут его двигать в 2013 году?

Аналитики компании Gartner в своем вебинаре (примерно в тот же период) «Top Security Trends and Takeaways for 2012-2013» назвали ТОП-10 ИБ-трендов следующего года:

1. Безопасность сетей.
2. Безопасность данных.
3. Мониторинг безопасности.
4. Консьюмеризация / мобильность.
5. Управление идентификацией и правами доступа.
6. Облачные вычисления.
7. Непрерывность бизнеса и восстановление после сбоев.
8. Безопасность персональных данных и частной информации.
9. Управление информацией и информационной безопасностью.
10. Программы развития безопасности.

Свою версию ТОП-7 вызовов безопасности в 2013 году дает аналитический интернет-портал «Help Net Security»[1] правда, по всей видимости, ориентируясь только на исследования одной антивирусной компании:

1. Конец интернету, каким мы его знаем.

[1] http://www.net-security.org/secworld.php?id=14120

2. За инцидентами утечек будет больше обнаруживаться след государственного шпионажа.
3. Рост коммерческого интереса криминального бизнеса к развитию вредоносного кода для мобильных устройств.
4. Рост вредоносного кода для MAC-сред.
5. Смарт-ТВ станет мишенью хакеров.
6. Развитие шпионских программ для мобильных устройств.
7. Широкое распространение бесплатных планшетных компьютеров с открытыми «экосистемами».

Прогноз ТОП-6 вызов ИБ от FortiGuard Labs (компания Fortinet)[2]:

1. Нацеливание APT(advanced persistent threat)-атак индивидуально (например, на руководителей) посредством их мобильных устройств.
2. Замена простой парольной защиты на двухфакторную аутентификацию в моделях информационной безопасности.
3. Нацеливание эксплойтов на M2M (машина-машина) коммуникации.
4. Развитие эксплойтов, обходящих «песочницы».
5. Развитие кросс-платформенных бот-сетей.
6. Количество и «качество» вредоносных программ для мобильных платформ догонит «десктопы».

На самом деле таких ТОПов от аналитических агентств и крупных вендоров очень много, и все приводить смысла нет. Главный вопрос, а что из всех этих поминаемых трендов окажет реальное воздействие на наш, российский, рынок информационной безопасности? Есть тренды, которые можно с уверенностью называть еще очень долго – усиление государственного регулирования сферы ИБ и рост угроз. Но это, как говорила одна киногероиня из культового советского фильма «Покровские ворота»: «Банально, Хоботов!»© Это понятно всем и так. Вообще вопрос трендов информационной безопасности 2013 года в нашей стране я бы делил на две неравные части. С одной стороны (большей) – теоретические вопросы развития технологий ИБ, с другой стороны – рынок ИБ. Т.е. говоря другими словами, с одной стороны то, о чем будут много говорить, а с другой – что активно будут внедрять.

Если говорить о первой составляющей, то здесь будет все тоже самое, о чем гудит мировое ИБ сообщество – безопасность информации в облачных вычислениях и в критических инфраструктурах, угрозы для мобильных платформ и кроссплатформенность вредоносных программ, рост киберпреступности и проблемы расследования компьютерных преступлений, ну и многое другое, что мы будем в наступившем году обсуждать, проводить круглые столы и семинары.

А вот с рынком, как это ни банально, все проще, и 2013 год больших сюрпризов рынку информационной безопасности не принесет. Я уверен, что по-прежнему наш рынок будет в основном ориентирован на государственный и крупный корпоративный секторы, а продажи в СМБ будут в гораздо меньшем объеме. Я думаю, что до 80% всех внедрений решений ИБ будут обусловлены выполнением обязательных требований по защите информации. Возможно нас, специалистов по безопасности, это коробит, и с точки зрения информационных рисков в свете роста ИБ-угроз это не правильно. Но если стать на сторону бизнеса и посмотреть на бизнес-риски,

[2] http://www.networkworld.com/news/2012/121412-fortinet-top-6-threat-predictions-265115.html?source=nww_rss&goback=%2Egde_38412_member_196409751

то все становится на свои места. Одним из главных бизнес-рисков для любого бизнеса из любой (практически) отрасли является несоответствие требованиям законодательства. В то время как риски связанные с безопасностью и конфиденциальностью данных входят в ТОП-10 бизнес-рисков только в двух отраслях (разработка новых технологий и банковская)[3]. Поэтому основным драйвером на 2013 год по-прежнему останется «волшебный регуляторский пинок»…

Для начала я пройдусь по тем громко мировым трендам, которые будут громко звучать, но пока, на мой взгляд, не окажут существенного влияние на наш рынок безопасности. Я для себя разделил их на две категории:

Наше «светлое завтра»

Расследование компьютерных преступлений. Очень хотелось бы серьезного развития этого направления, но боюсь, не в этом году. Наша правоохранительная система пока еще слаба для того, чтобы оказать всестороннюю поддержку в этом направлении. Хотя тема в отрасли будет горячая, полная обсуждений, но на рынок пока сильного влияния не окажет. По крайней мере, не на столько, чтобы считать ТОП-трендом.

Усиление внимания государственных регуляторов к безопасности информации в критических инфраструктурах. Вряд ли, глядя на американский опыт, в этом году уже можно ожидать сформированной нормативно-правовой базы, на основе которой можно было бы запустить государственные надзорно-контрольные функции «на всю катушку» (слишком много проблем как технических, так и правовых). Хотя благодаря тому, что тема остается второй год во внимании государства на самом высоком уровне, что подтверждается недавним указом Президента РФ о создании российской системы предотвращения кибератак, она станет одной из культовых на мероприятиях по ИБ. Тем не менее, без четких «правил игры» (требований, стандартов, порядка регулирования и т.д.) внедрение этих решений пока останется за узким сегментом компаний-новаторов из числа крупных предприятий ТЭК, которые могут себе позволить смотреть на проблему «глазами вечности».

Кроссплатформенность вредоносных программ и направленность на мобильные устройства. Оказывает серьезное влияние на антивирусный сегмент, заставляет шевелиться производителей средств аутентификации и сетевой безопасности, чем вносит, возможно, разнообразие в конкурентную среду. Однако существенного увеличения продаж СЗИ для мобильных устройств на российском рынке, на мой взгляд, пока не будет, по крайней мере не в этому году, т.к. частные пользователи смартфонов и планшетов еще не дозрели до этого в полной мере, а в корпоративном сегменте СЗИ на рабочих местах мобильных пользователей уже давно устанавливаются и так.

Наше «светлое послезавтра».

Облачные вычисления. В вопросах безопасности информации в «облаках» до сих пор пока больше вопросов, чем ответов. Да, тема будет по-прежнему звучать, и скорее всего мы будем обсуждать ее еще глубже, чаще и т.д., но на рынок ИБ существенного влияния она не окажет – все будет как и было, т.е. эта тема останется пока прерогативой ИТ. Конечно, средства безопасности для виртуализированных сред будут развиваться, устанавливаться в ЦОДы, но ничего нового на

[3] Исследование «10 основных бизнес-рисков. Обзор отраслевых рисков, угрожающих международному бизнесу». Ernst&Young совместно с Oxford Analytica, 2010.

рынке не произойдет и назвать это прямо ТОП-трендом я не готов. Кстати, интересно отметить, что на ежегодно выпускаемом компанией Gartner графике Hype Cycle (кривая заблуждений[4]) for Emerging Technologies облачные технологии второй год уже как сползают с «пика раздутых ожиданий» в «яму разочарований», и Gartner прогнозирует 2-5 лет на выход данной технологии на «плато продуктивности».

Комплексное управление информационными ресурсами и информационной безопасностью предприятия на основе риск-ориентированного подхода., Необходимо отметить, что в той или иной степени фрагментарно решения, которые можно отнести к управлению информационной безопасностью, внедряется довольно активно. Но говорить именно о комплексном подходе, пока, к сожалению рано. Я думаю, мы начнем чаще говорить о подобном подходе, хотя подобных внедрений пока все еще будут единицы.

Мобильные устройства и BYOD в целом. Пока из разговоров со знакомыми людьми, руководящими ИБ сегодня, создается впечатление, что эта тема долго будет еще «светлым послезавтра» для российской ИБ. Т.е. пока мобильные устройства сотрудников не наносят заметного урона для безопасности – на них не обращают внимания, как только наносят – их просто тут же запрещают, и никакой интеграцией в общую архитектуру ИБ предприятия подавляющее большинство пока заниматься не собирается.

Ну а что же окажется паровозом для российского рынка ИБ в 2013 году?

Итак, наши «серые будни». *Моя версия ТОП-драйверов рынка информационной безопасности в 2013:*

Гостайна (и иже с ней «Государевы» информационные ресурсы). Кормила, кормит и будет кормить большой, закрытый сегмент рынка, многие участники которого даже не появляются в рейтингах аналитических обзоров. Кроме того, я прогнозирую рост данного сегмента в ближайшее время за счет, в первую очередь, оборонной промышленности. Я уже говорил на конференции ИБ в ОПК в прошлом году и повторю снова – оборонка (а в дальнейшем думаю и силовые структуры) будут вынуждены менять свое отношение к порядку обработки, хранения и защиты информации. Если раньше все, что касалось гостайны, максимально изолировалось от автоматизированной обработки, а если и обрабатывалось, то изолировалось от сети и т.д. Времена, когда для ОПК главными инструментами защиты информации были заборы, собаки и особисты прошли. Государство требует от предприятий конкурентоспособности на международных рынках, а конкурентоспособность требует активное внедрение новых технологий для проектирования и производства сложных изделий. Отсюда вытекают как минимум две проблемы – огромные объемы данных порождаемые современными САПР системами, требующие активного использования ЦОДов, а во вторых, необходимость совместной работы над проектами сразу нескольких предприятий, требующая активного сетевого взаимодействия. Ну и кроме того, кибервойны набирают обороты, развитые страны создают подразделения кибербезопасности в своих армиях и др. признаки говорят о том, что, сегмент безопасности государственных информационных ресурсов останется одним из основных драйверов рынка.

Соответствие требованиям по защите персональных данных (Privacy в целом пока, к сожалению, для нас также пока только «светлое будущее»). Здесь все понятно. И жаркие отраслевые споры, и

[4] Этот и далее термины аналитической компании Gartner. Подробнее о данном методе исследования на сайте компании http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp

активная позиция, которую занимают Роскомнадзор и остальные регуляторы, еще раз подчеркивают, что эта тема останется одним из основных стимулов к внедрению систем защиты информации.

Соответствие требованиям безопасности информации в платежных системах. 161-ФЗ, наделивший Банк России регуляторными функциями теперь еще и в сфере ИБ, в частности платежных систем, а также последовавшее затем создание отельного департамента в структуре ЦБ и выпуск целого ряда подзаконных нормативных документов, стал дополнительным драйвером рынка. И хотя банковская сфера всегда была в передовиках по внедрению систем ИБ, приведение в соответствие с новыми документами потребует дополнительных усилий. Ведь самое главное, что требования по ИБ стали обязательными еще по одному параметру (раньше только в части ПДн). А для банков риск несоответствия законодательным требованиям является одним из ТОП-10 бизнес рисков[5]. И хотя введение «дамокловой» ст.9 161-ФЗ отсрочили на год, банковскому сообществу дали ясный сигнал, что отсрочивать до бесконечности (как это было с 152-ФЗ) никто не собирается, и значит через год риски ущерба от мошенничества в ДБО для банков значительно возрастут. Поэтому несмотря на то, что 2013 год станет еще установочным и в большей мере отладочным для безопасности НПС, ее можно смело записывать в ТОП-драйверы рынка ИБ.

Развитие СМЭВ и Закон Об электронной подписи. Эта тема также последние два года находится в пристальном внимании государства на самом высоком уровне, и в отличие от критических инфраструктур, с самого начала имеет четко обозначенные требования по ЭП и защите информации[6]. А поскольку развитие СМЭВ идет не так быстро, как того требует правительство, то сразу нескольким сегментам рынка ИБ еще не один год будет чем заняться, «не покладая рук». Процесс создания в России единого пространства доверия для безопасного использования электронной подписи идет тоже не без проблем, тем не менее, внимание к этой теме «на верху» не ослабевает – наконец утвердили правила обмена электронными счетами-фактурами. И хотя я не думаю, что за этот год удастся решить тот ворох правовых проблем, связанный с повсеместным развитием юридической значимости электронного документооборота и внедрением ЭП, эта тема все равно будет активным драйвером развития рынка ИБ.

Вот таким мне видится 2013 год. Я конечно сознательно дал множество поводов бросить в меня камнем, ибо в споре рождается истина, однако еще раз повторю, что я не отрицаю ни рост киберугроз, ни всех тех тенденций мирового киберпространства, о котором сейчас так много пишут и говорят эксперты. Просто так сложился российский бизнес, что большинство трендов еще долго будут жить только в умах и словах ИБ-экспертов и узкой группы «новаторов», которые по тем или иным причинам могут позволить себе проактивный подход к обеспечению безопасности. В большинстве случаев все наши предостережения бизнес видит пока еще «только в очень крупную лупу», и как я уже говорил, с точки зрения бизнес-рисков его сложно в этом упрекнуть. Сколько должно быть громких инцидентов в нашей стране, чтобы риски ИБ попали хотя бы в ТОП-20 бизнес рисков для большинства отраслей и предприятий? К сожалению, практика показывает, что пока у нас в умах преобладает метод латания дыр, а риск-ориентированный-подход сводится во многом к нашему великому «авось», двигателем рынка ИБ останется по прежнему только мощный инструмент государственного (либо иного) принуждения.

---

[5] Исследование «10 основных бизнес-рисков. Обзор отраслевых рисков, угрожающих международному бизнесу». Ernst&Young совместно с Oxford Analytica, 2010.

[6] Постановление Правительства Российской Федерации от 8 сентября 2010 г. N 697; Приказ Минкомсвязи от 27 декабря 2010 г. N 190; Постановление Правительства РФ 451 08 июня 2011 и другие документы.