Исследование

РЫНОК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

+ Обзор рынка информационной безопасности Украины

2013

СОДЕРЖАНИЕ

1. Предисловие 3

2. Некоторые выводы исследования 5

3. Авторы разделов 6

4. Рынок систем сетевой безопасности, аппаратных средств двухфакторной аутентификации и инструментальных средств анализа защищенности 7

5. Рынок систем контентной фильтрации 17

6. Рынок систем антивирусной защиты 19

7. Рынок PKI 22

8. Рынок систем сбора и корреляции событий (SIEM) 25

9. Рынок систем идентификации и аутентификации (IDM) 28

10. Рынок систем защиты информации (СЗИ) от несанкционированного доступа (НСД) 31

11. Интеграторы в области ИБ 34

12. Рынок консалтинга ИБ 37

13. Рынок аудита информационной безопасности 39

14. Рынок услуг по сертификации продукции по требованиям информационной безопасности 44

15. Рынок услуг по обучению вопросам информационной безопасности 48

16. Мероприятия по информационной безопасности 52

17. Интегральная оценка рынка ИБ 57

18. Bonus. Рынок информационной безопасности Украины (обзор) 59

Приложение А. Методика и подход 66

ПРЕДИСЛОВИЕ

Евгений ЦАРЁВ

Острый недостаток информации о рынке информационной безопасности (ИБ) на рубеже 2007–2008 годов к сегодняшнему моменту сменился ее избытком. Сегодня все участники рынка сталкиваются с проблемой получения адекватных данных по российскому рынку ИБ.

Каковые реальные позиции того или иного вендора?

На чем реально зарабатывают те или иные интеграторы?

Какие решения по секторам пользуются большим спросом?

И т.п.

На эти и многие другие вопросы даже активные игроки рынка не всегда могут дать ответ. Такой ответ могут дать только конкретные эксперты данного сегмента рынка и иногда только в частной беседе.

Маркетинговые деньги вендоров, дистрибьюторов и интеграторов существенно исказили представление участников рынка о реальном положении вещей.

Вывод нового продукта или активный выход на рынок новой компании, как правило, сопровождается активным вливанием денежных средств в маркетинг. Как результат у участников рынка формируется представление об этом продукте или компании как о лидере, хотя по факту все может быть иначе.

Учитывая то, что российский рынок информационной безопасности значительно отличается от западного и общемирового, использовать иностранные источники в большинстве случаев не имеет смысла. Более того, информация по российскому рынку ИБ, которую выдают некоторые западные аналитические агентства, вовсе не соответствует действительности и зачастую абсурдна.

В результате небольшой инициативной группой было принято решение подготовить обзор/исследование российского рынка информационной безопасности. Каждый конкретный раздел готовят конкретные эксперты рынка (каждый по своему сегменту). Отличительной особенностью данного исследования является тот факт, что к его разработке приглашались не маркетинговые службы компаний и не руководство компаний, а конкретные эксперты, которые хорошо знают и понимают свой сегмент рынка. Работа велась исключительно на некоммерческой основе.

Естественно, не все эксперты соглашались принять участие в проекте, основным условием которого является непредвзятость. Ссылаясь на корпоративную этику своих работодателей, они отказывались. Также были случаи, когда эксперты были явно необъективны, и такие разделы/данные не были включены в итоговый документ. По этой причине некоторые сегменты рынка не нашли отражения в настоящем исследовании. Однако в результате более чем полугодичной работы нам удалось разработать итоговый документ, который содержит экспертную оценку всех основных сегментов рынка ИБ в России. Также был подготовлен небольшой обзор по рынку ИБ Украины.

Настоящее исследование не ставило своей целью «посчитать рынок ИБ» или «назвать точные

обороты игроков». Основная задача – сформулировать адекватную оценку рынка и ответить на вопрос: «Что такое российский рынок ИБ на самом деле?»

Важным является тот факт, что эксперты работали **независимо друг от друга и не могли влиять на результаты своих коллег**. По этой причине они не могут отвечать за все исследование целиком.

В рамках подготовки своих разделов эксперты имели возможность отойти от шаблона и дать информацию в том виде, в котором считают нужным. Полученный документ является уникальным. Авторы исследования не знают фактов проведения изысканий подобного рода. В результате почти 8 месяцев работы мы получили качественный срез по рынку ИБ, который не способно получить ни одно аналитическое агентство. Применяемый подход к проведению работы позволяет получать доверенные данные из первых рук без права ссылки на источник. С одной стороны это противоречит правилам проведения исследований, с другой является весьма эффективным, а в российских реалиях единственным, способом получения доверенной информации. В этом заключается ценность данного документа.

Итоговый документ передан всем участникам проекта без ограничений на распространение.

ВНИМАНИЕ! Возможно активное противодействие результатам данного отчета со стороны маркетинговых служб некоторых западных компаний, которые вкладывают в западные исследования серьезные деньги и не желают допускать независимые оценки.

НЕКОТОРЫЕ ВЫВОДЫ ИССЛЕДОВАНИЯ

- **41% российского рынка ИБ представлено решениями отечественного происхождения**
- **29% российского рынка ИБ представлено решениями по антивирусной защите**
- **70% российского рынка ИБ представлено решениями по антивирусной защите и сетевой безопасности**
- **Рынок аудита ИБ в России весьма незначителен (около 1%)**
- **Рынок консалтинга не превышает 5–10% от всего рынка ИБ**
- **Рынок ИБ имеет очевидную тенденцию к росту**
- **Российский рынок ИБ имеет явную специфику, в первую очередь по составу игроков и соотношению долей игроков**
- **Рынок ИБ находится под серьезным регулятивным влиянием, в первую очередь через инструмент сертификации и законодательство**
- **Рынок консервативен, некоторые международные тенденции вроде активного развития облачных сервисов безопасности пока неактуальны для России**
- **Флагманские «западные» темы, вроде MDM, защиты виртуализации, безопасности АСУ ТП развиваются в Росси очень медленно. В частности рынок таких решений в России фактически отсутствует**
- **Совокупный объем рынка ИБ составляет 1 399 млн долл. в год**

АВТОРЫ РАЗДЕЛОВ

Рынок систем контентной фильтрации	**Сергей Трещалин**
Рынок систем сетевой безопасности, аппаратных средств двухфакторной аутентификации и инструментальных средств анализа защищенности	**Михаил Романов**
Рынок систем антивирусной защиты	**Илья Шабанов**
Рынок PKI	**Дмитрий Артеменков**
Рынок систем сбора и корреляции событий ИБ (SIEM)	**Владимир Емышев**
Рынок систем идентификации и аутентификации (IDM)	**Александр Санин**
Рынок систем защиты информации (СЗИ) от несанкционированного доступа (НСД)	**Алексей Комаров**
Интеграторы в области ИБ	**Евгений Царев**
Рынок консалтинга ИБ	**Евгений Царев**
Рынок аудита информационной безопасности	**Илья Медведовский**
Рынок услуг по сертификации продукции по требованиям информационной безопасности	**Дмитрий Левиев**
Рынок услуг по обучению вопросам информационной безопасности	**Игорь Хайров**
Мероприятия по информационной безопасности	**Игорь Елисеев**
Интегральная оценка рынка ИБ	**Евгений Царев**
Bonus. Рынок информационной безопасности Украины	**Екатерина Ляшенко**

Отзывы, комментарии и предложения, а также запросы по дополнительной информации, в частности по контактам авторов разделов, просьба отправлять на адрес: **ISRussiaResearch@gmail.com**

РЫНОК СИСТЕМ СЕТЕВОЙ БЕЗОПАСНОСТИ, АППАРАТНЫХ СРЕДСТВ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ И ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ АНАЛИЗА ЗАЩИЩЕННОСТИ

Михаил РОМАНОВ

Российский рынок систем сетевой безопасности объединяет в себе большое количество различных решений и технологий. В настоящий момент существует множество подсистем информационной безопасности, поэтому в рамках данного раздела выделены только конкретные виды, относящиеся к рынку средств сетевой безопасности или не вошедшие в другие разделы исследования. В рамках раздела исследовались корпоративные средства безопасности, исключая средства защиты для домашних сетей и т.п.. Были выделены следующие типы устройств:

1. UTM/Firewall;
2. VPN;
3. IPS (IDS);
4. DDoS;
5. средства аутентификации и авторизации пользователей;
6. NAC.

Также в разделе рассмотрены следующие сегменты рынка ИБ:

1. рынок аппаратных средств двухфакторной аутентификации;
2. рынок инструментальных средств анализа защищенности.

Как видно, в состав рынка сетевой безопасности не вошли средства контентной фильтрации, например, Blue Coat и прочие, которые подробно рассмотрены в другом разделе. Также не рассматривались персональные межсетевые экраны и HIPS, поскольку они учитывались в разделе по средствам антивирусной защиты.

Подготовка количественной оценки российского рынка сетевой безопасности является достаточно сложной задачей, поскольку существующие методы, используемые некоторыми агентствами (например, опрос интеграторов о занимаемой ими доле рынка информационной безопасности), не могут достаточно достоверно определять рынок, так как у каждого интегратора существует соблазн несколько приукрасить действительность. Тем более, что в общем объеме продаж крупного интегратора информационная безопасность (далее ИБ), как правило, занимает не более 30%, и, соответственно, существует большой простор для показа «правильных» цифр, которые чаще всего предоставляют маркетологи данных интеграторов. Кстати, зачастую правильно посчитать оборот по ИБ у интегратора просто невозможно, поскольку работы и поставка оборудования ИБ являются частью крупных ИТ-договоров.

В свою очередь, специализированные агентства типа IDC предлагают собственную версию российского рынка, странным образом разделяя аппаратные и программные средства. В 2012 году отчет IDC (аж на 8 страницах), который компания предла-

гала за 1000 долл., немало удивил специалистов своим подходом. Например, как можно разделить межсетевой экран на программную и аппаратную часть, если это единое целое? Кроме того, у многих специалистов вызвали сомнение отдельные цифры в отчете, например, по компании Juniper Networks. Никто «не видит эту компанию у клиентов» (в части решений по ИБ), а цифры такие, что компания просто обязана быть везде, учитывая еще и фактически отсутствие сертификатов ФСТЭК и ФСБ России. Помимо этого, темпы роста российского рынка ИБ, указанные в документе, также вызвали легкое недоумение у специалистов. Кстати, вопросы к компании возникают не только в части ИБ, эта же организация из года в год обязательно предсказывает Microsoft очень большие доли рынка в мобильном мире. Однако прогнозы почему-то никак не сбываются. Например, здесь один из аналитиков подозревает IDC в завышении прогнозов по компании Microsoft. Таким образом, есть «красноречивые намеки» с разных сторон о «некоторой неточности» такого отчета.

Несомненно, многим бы хотелось получить цифры, более объективно оценивающие российский рынок ИБ, поэтому нужен другой подход.

Более достоверные цифры можно увидеть у специализированных системных интеграторов, занимающихся именно ИБ и самих вендоров. На основании объемов продаж вендоров можно оценить и объем рынка сетевой безопасности.

Для оценки рынка опрашивались специалисты, работающие в вендорах, дистрибьюторах и интеграторах, а также использовались различные системы типа СПАРК и аналоги. Далее, зная, какие скидки даются партнерам (выводим среднее значение), и, принимая во внимание, что на инсталляционные работы по проекту обычно выделяется сумма от 8 до 25% от стоимости контракта, можно вычислить итоговый объем рынка сетевой безопасности. В результате, мы имеем более достоверные цифры, чем в других случаях, однако в этих оценках не учитываются объемы некоторых рынков (ЗГТ, государственных специальных или закрытых проектов).

Российский рынок сетевой безопасности представлен большим числом как российских, так и зарубежных производителей оборудования. К сожалению, достаточно сложно оценивать объемы продаж отдельных российских вендоров, например, по продукции типа «Атликс», «Ручей», «Форпост» и др., так как они практически никогда не появлялись на конкурентном рынке. Такие решения, как правило, ставятся по умолчанию в закрытые проекты, где используется строго «назначенное» оборудование ИБ. Это же относится и к оборудованию, предназначенному для защиты гостайны. Объемы таких проектов могут быть достаточно большими, а по защите гостайны – очень большими, однако получить по ним информацию, как правило, не представляется возможным. Однако, и смысла в подобной информации нет. Рынок таких устройств является практически полностью изолированным от общего рынка сетевой безопасности, поэтому повлиять и показать какие-либо тенденции, тренды и пр. он попросту не может.

В отчете также рассматривался только ограниченный круг вендоров, который, по мнению автора, составляет основную (подавляющую) долю рынка. Ввиду вышесказанного, в рамках настоящего раздела учитывались данные по следующим производителям:

- Cisco Systems
- Check Point
- Juniper Networks
- Stonesoft
- Imperva
- ИнфоТеКС
- С-Терра СиЭсПи
- Код Безопасности
- АМИКОН (ФПСУ-IP, SSL)
- Sophos
- Fortinet
- McAfee
- HP (Tipping Point)
- WatchGuard Technologies
- Arbor Networks
- Radware
- Элвис Плюс (Застава)
- IBM Internet Security Systems
- ФАКТОР-ТС (семейство Дионис)

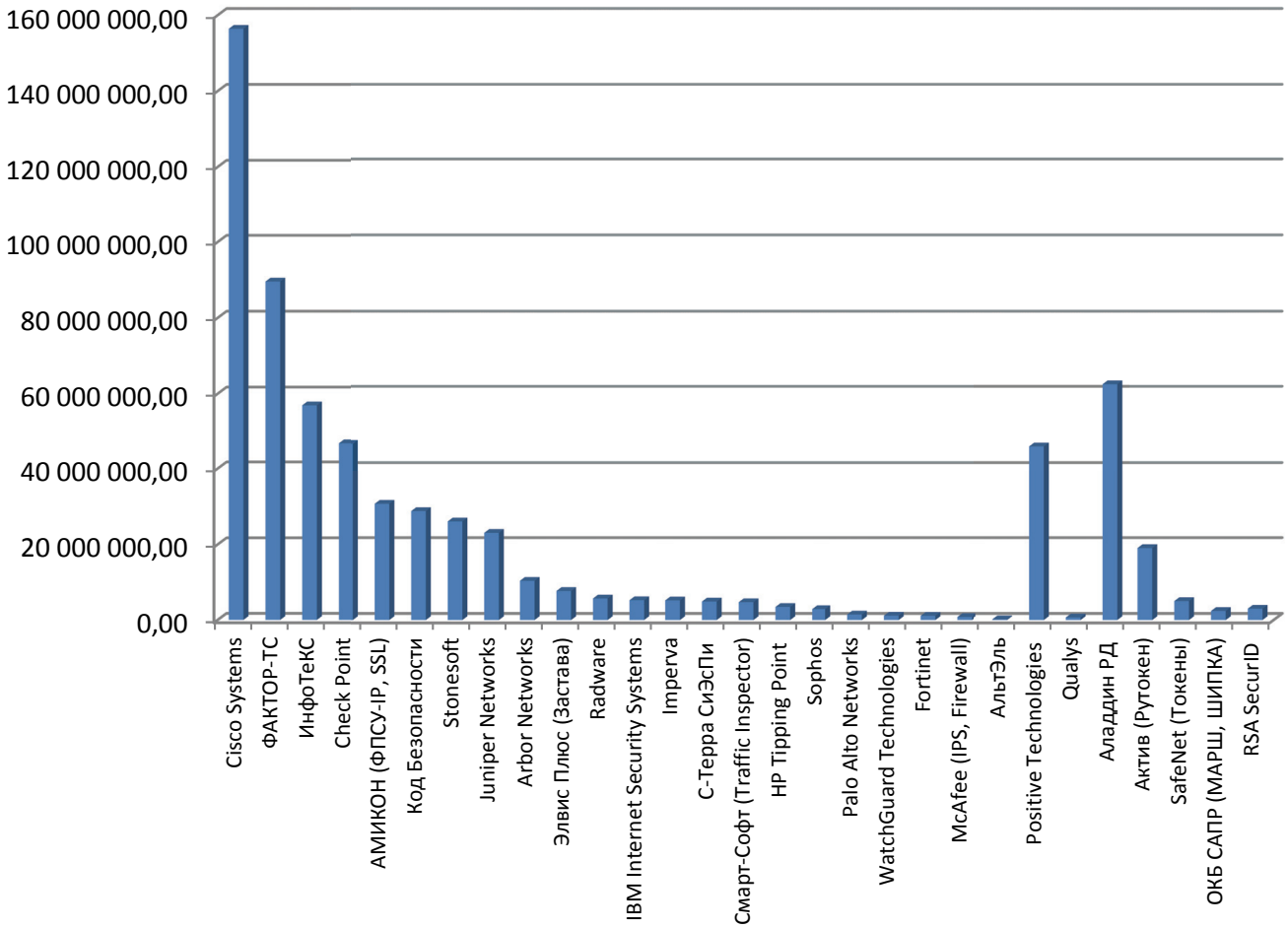
- АльтЭль
- Palo Alto Networks
- Смарт-Софт
- Positive Technologies
- Qualys
- Аладдин Р.Д. (Токены + ПО управления, лицензии)
- Актив (Рутокен)
- SafeNet (Токены)
- ОКБ САПР (МАРШ, ШИПКА)
- RSA (RSA SecureID)

Ограничения и допущения

Из раздела исключены такие вендоры, как D-link, Zuxel и некоторые другие, поскольку они, как правило, используются для защиты домашних сетей. Такие вендоры, как правило, работают с ритейл-сетями, то есть оперируют объемами отгрузок партнерам, и подсчет реальных продаж клиентам в этом случае является делом неблагодарным. При этом вендоры, попавшие в обзор, продают решения корпоративному рынку или рынку услуг, а это, как правило, проектный бизнес с четкими сроками реализации. Также, не проводилось исследование небольших вендоров, продающих решения типа ССПТ (продается в основном в государственные проекты типа Таможенного комитета и др., поэтому реальный объем оценивать сложно), и некоторых других вендоров, которые имеют определенные объемы продаж, но не очень большие, поэтому в итоговых таблицах их доля будет крайне мала.

Некоторые вендоры имеют в своем составе большое количество продуктов. Мы старались исключить продукты, не относящиеся к сетевой тематике или учтенные в других разделах (Антиспам, Антивирус и др.). А также постарались исключить сервисы и объемы, относящиеся к НИОКР и прочим непрофильным работам.

В целом по России объемы продаж по вендорам (долл.), рассматриваемым в настоящем разделе, выглядят следующим образом:



Результаты исследования

Основным поставщиком решений по сетевой безопасности в России является компания Cisco Systems. Причина такого результата понятна. Cisco Systems – это компания №1 в мире (и в России) по сетевым технологиям. Кроме того, по объемам поставок информационной безопасности данная компания также лидирует в мире. Она одной из первых пришла на российский рынок, ее сетевое оборудование стоит практически в каждой организации, соответственно, нет ничего необычного в том, что решения по сетевой безопасности также заказывают у этой компании. Кроме того, Cisco Systems ведет очень грамотную деятельность по продвижению своей линейки безопасности на российском рынке. И в настоящий момент ни одна компания не может сравниться с Cisco Systems по уровню работы с рынком, как в маркетинговом плане, так и в плане работы с партнерами, госорганизациями, регуляторами и пр. Остальные вендоры пока в своей массе не желают или не могут себе позволить такие затраты на специалистов, маркетинг и прочее. Необходимо отметить, что данная компания уделяет очень большое внимание вопросам сертификации по российским требованиям, тратя на них намного больше, чем другие западные вендоры, что также способствует сохранению лидирующего положения на российском рынке.

С другими западными вендорами, как показывают графики, все не так, как, например, на североамериканском рынке. В частности, компания McAfee, являющаяся ранее фактически стандартом антивирусных решений в российских банках и входящая в группу лидеров на американском рынке, в настоящий момент имеет в России крайне небольшую долю рынка, не проявляя достаточных «признаков жизни». Кроме того, имеется большое количество российских вендоров, которые показывают значительные объемы в России. Тут можно сделать вывод, что очень важное значение имеет сертификация.

Если внимательно посмотреть на рынок средств безопасности и проанализировать, какие места занимают, например, российские вендоры, то получается интересная картина:

1. Российских вендоров, имеющих более или менее значительные доли рынка, можно условно поделить на две группы – это VPN–вендоры и те вендоры, которые изготавливают различного вида токены или средства защиты от НСД (если посмотреть в другие разделы отчета, то у нас еще есть антивирусные вендоры).
2. Все вошедшие в обзор VPN-вендоры, имеющие значительные доли рынка, присутствуют, как правило, на неконкурентном рынке (различные государственные структуры), где требуется сертификат ФСБ России на СКЗИ. Например, «ФАКТОР-ТС» – это МВД и Федеральная налоговая служба, АМИКОН (ФПСУ-IP, SSL) – Сбербанк и Банк России (80% всех поставок), «ИнфоТеКС» – Пенсионный фонд, РЖД, ФОМС, «Ростелеком» и различные министерства и ведомства (данная компания наиболее широко представлена в государственных структурах).
3. Все российские производители токенов также связаны с разработками СКЗИ и необходимостью сертификации, где конкурируют в основном между собой.
4. На рынке практически отсутствуют межсетевые экраны российского производства, которые более или менее соответствуют современным требованиям, не говоря про экраны нового поколения (NGFW) – такие отсутствуют пока как класс. Сертифицированных средств много, можно назвать тот же ССПТ или «АльтЭль». Однако объемы продаж даже на неконкурентном рынке показывают их крайне скромные возможности. Даже если учесть, что за 2013 год, например, «АльтЭль» резко поднимет обороты, но опять же это будет продажа в основном VPN-решения. Можно посчитать межсетевыми экранами наши VPN-продукты, такие как «Континент-К», S-Terra и прочие. Они формально сертифицированы как МЭ, но автор пока не видел в данных решениях функциональности выше, чем пакетный фильтр. Можно возразить, что в них есть варианты со встроенным антивирусом Лаборатории Касперского, однако, во-первых, можно почитать отзывы в Интернете по таким ре-

шениям, а во-вторых, как показывает практика, антивирус надо еще суметь внедрить так, чтобы он корректно работал.

5. Фактически отсутствуют конкурентоспособные IPS-решения российского производства. Автору известны только три российских решения данного типа: «Аргус», «Форпост» и «РУЧЕЙ-М» (не позиционируется как IPS). Найти «Аргус» или «РУЧЕЙ-М» в Интернете и купить не представляется возможным. Решение «Форпост» производства компании РНТ, позиционируется как сертифицированное решение, полностью основанное на коде SNORT (и этого разработчики не скрывают). Разработчик не предоставляет свое решение на тестирование, продукт никак не продвигается на рынке, то есть создается впечатление, что РНТ продвигает его только в собственные проекты. Соответственно, увидеть эффективность этого решения не представляется возможным.
6. Отсутствуют российские решения NAC, UTM (исключением можно назвать «АльтЭль»), почти отсутствуют российские системы аутентификации (имеется в виду система аутентификации в целом, а не ее часть с токенами). Тут, свою роль играет законодательство, продвигаемое нашими регуляторами, которые в основном признают только один вид аутентификации: аутентификация по сертификатам. Соответственно развитие получили продукты позволяющие создать удостоверяющие центры, и криптобиблиотеки, обеспечивающие процесс аутентификации по сертификатам.

Если говорить о системах централизованного управления безопасностью, то можно отметить, что полноценные системы российского производства практически отсутствуют. Можно говорить о таких системах только в плане управления VPN-шифраторами, чаще всего – управления ключевой системой. Тут наши вендоры лучше всех (и это не сарказм). Однако пользователям нужно еще управлять другими параметрами и функционалом. Хотя в последние три года такие работы начали вести все основные российские вендоры. Одной из причин, по крайней мере для некоторых из них, является появление на российском рынке компании Stonesoft с одной из лучших в мире систем централизованного управления, а также с похожим уровнем сертификации по ФСБ и, в определенных случаях, превосходящим уровнем сертификации по ФСТЭК.

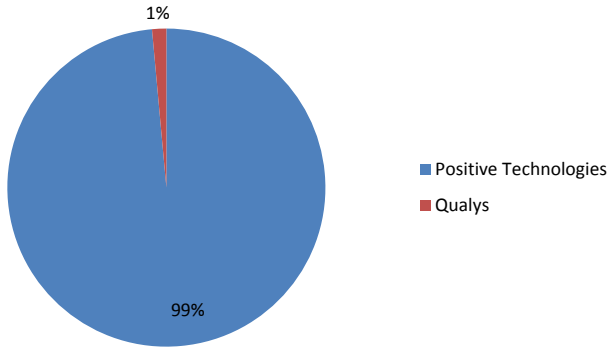
На конференциях сейчас часто можно увидеть, как, например, менеджер продуктов от компании Security Code в обязательном порядке старается посетить выступления западных вендоров с зеркальным фотоаппаратом (последняя конференция «Рускрипто» не являлась не исключением). Это уже давно стало предметом различных шуток о том, что идеи черпать больше не откуда.

В целом автор видит в этом позитивный момент: наконец-то российские производители VPN-решений начали понимать, что просто шифрующие коробки давно не нужны бизнесу, а нужны серьезные, мультифункциональные решения, с мощной системой управления, которая позволяет управлять не только ключевой системой.

Рынок инструментальных средств анализа защищенности

Рынок «сканеров безопасности» является не большим по количеству игроков. Что отрадно, на российском рынке подавляющее большинство поставок сканеров безопасности осуществляет компания Positive Technologies. Правда, на рынке практически отсутствуют другие вендоры. Заметную долю пока занимает только компания Qualys.

Доли игроков рынка инструментальных средств анализа защищенности



Российский рынок инструментальных средств анализа защищенности сейчас оценивается примерно в 47 млн. долл.

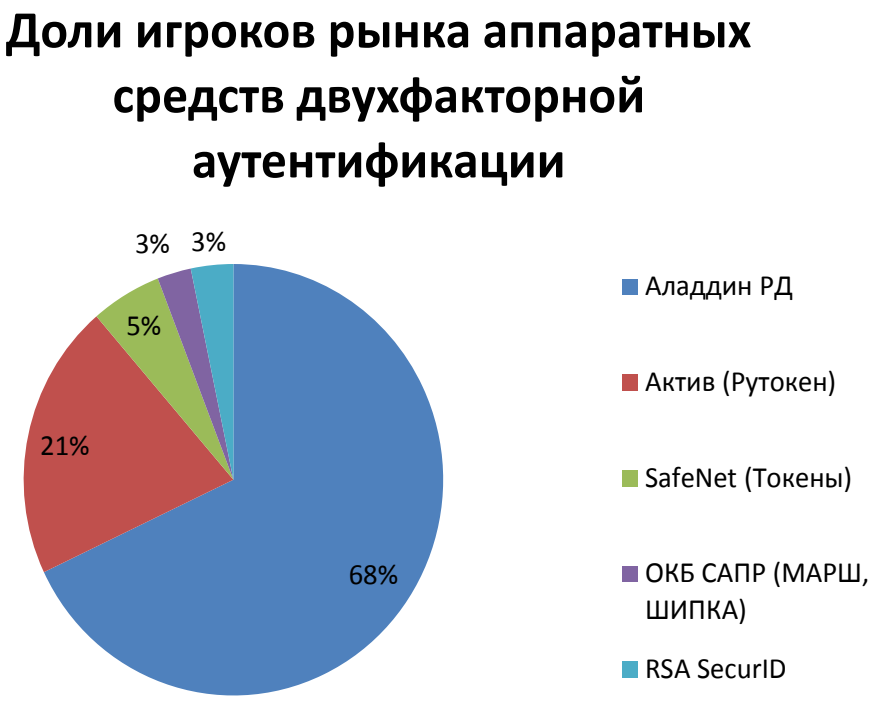
В ближайшей перспективе в плане смены игроков или потрясений на этой части рынка серьезных изменений не предвидится. Во-первых, мало игроков. Во-вторых, модель предоставления сервисов, которую предлагают западные вендоры, не устраивает наших регуляторов и, соответственно, является в нашей стране недостатком. Следовательно, у Positive Technologies сейчас практически нет серьезных конкурентов в реалиях нашей страны.

Из западных вендоров более или менее серьезно присутствует только Qualys. Остальные вендоры либо не торопятся на российский рынок, либо имеют откровенно слабые решения. Например, компания Fortinet имеет в своем составе систему анализа уязвимостей Forti Scan, но судя по тому, что данная функциональность даже на родном для компании рынке не является конкурентом более или мене заметным игрокам (Qualys, Outpost 24 и др.), этот продукт и на российском рынке не сможет добиться какой-либо заметной доли рынка. А, например, у вендора Outpost 24 грандиозные «наполеоновские» планы, и они выглядят гораздо более соответствующими рынку, но только этого может оказаться недостаточно для завоевания своей доли.

Рынок средств двухфакторной аутентификации

Рынок средств аутентификации в нашей стране также выглядит интересно. Если говорить о Западе, то там более распространены технологии одноразовых паролей в различных вариациях (в том числе и в токенах). RSA – далеко не единственная компания, которая предоставляет такие решения. В нашей стране, видимо под определенным давлением регуляторов и в сложившихся обстоятельствах, главным средством аутентификации является сертификат. Соответственно, большую роль играют аппаратные токены, где и хранятся сертификаты.

Опять же, на рынке аппаратных устройств последние годы происходили серьезные изменения. В результате слияний и поглощений компания SafeNet является основным поставщиком решений на российский рынок. Компания «Аладдин Р.Д.», закупая, скажем, базовые токены в данной компании (оригинальную компанию Aladdin купила компания SafeNet), обеспечивает основные их продажи на российском рынке под маркой eToken. «Аладдин Р.Д.» обеспечивает купленные токены собственным доработанным ПО, сертифицируя их у регуляторов, а также обеспечивает техническую поддержку. Есть ряд банков использующих токены непосредственно от компании SafeNet.

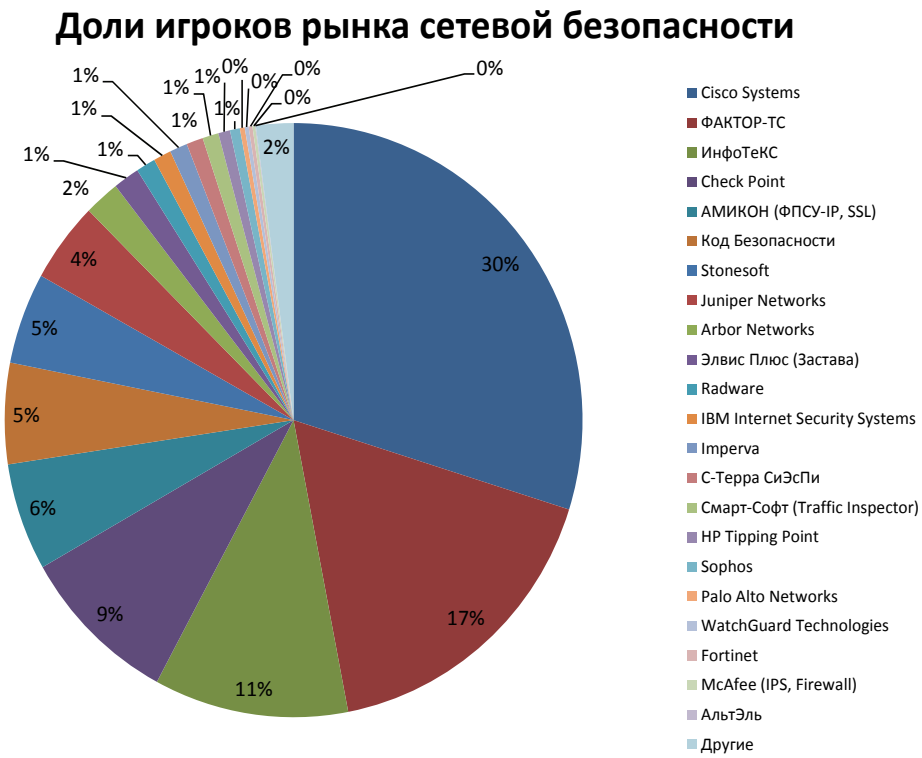


Таким образом, достаточно заметными игроками на рынке аутентификации в России являются компании «Аладдин Р.Д.», «Актив» (продукт «Рутокен»), ОКБ САПР (продукты МАРШ, «Шипка»). Ну и, конечно же, SafeNet, который имеет часть продаж, консолидированных с другими вендорами («Аладдин Р.Д.»). На графике показана доля без учета продаж другим вендорам. Также на рынке достаточно активно присутствует RSA со всем известным продуктом RSA SecurID. Известно, что на рынке присутствуют и другие вендоры, например Active Identity, однако получить какие-либо достоверные данные по ним не удалось.

В целом российский рынок аппаратных средств двухфакторной аутентификации оценивается примерно в 91 млн. долл.

К сожалению, не представляется возможным показать срезы рынка VPN, FW, IPS по отдельности, ввиду того что продукты сильно интегрированы и разделить, например, межсетевой экран и VPN не представляется возможным (за исключением продуктов российских вендоров, позиционируемых как VPN-концентраторы). Можно лишь констатировать, что среди межсетевых экранов в любом случае лидирует Cisco Systems, а безусловный вендор №2 – Check Point. Третье место, скорее всего, принадлежит Juniper Networks и далее Stonesoft. А вот на рынке продаж чистых IPS-решений тройка лидеров выглядит следующим образом: Cisco Systems, Stonesoft, IBM Internet Security Systems (если брать во внимание также и продажи обновлений для уже установленных сенсоров). Повторюсь, данное деление основано на определенном опыте автора и данных основных вендоров. Компания Check Point продает свои IPS в основном как блейд к основному МЭ, поэтому она не попала в тройку лидеров по этой части рынка.

Распределение долей по рынку сетевой безопасности выглядит следующим образом:



Можно также сделать следующие интересные наблюдения, показывающие способы продвижения российских вендоров на рынке сетевой безопасности.

Некоторые российские вендоры попросту «сидят» на определенных заказчиках, и зачастую эти вендоры для них и создавались (например, «АМИКОН», «ФАКТОР-ТС» и некоторые др.). С одной стороны, в этом нет ничего плохого. С другой, мы видим, что с протяжением времени производимые ими решения практически не развиваются относительно базового функционала. Особенно, если смотреть на продукцию других вендоров, работающих на конкурентном рынке. Можно посмотреть на большинство продук-

тов десять лет назад и сейчас – и может случиться "дежавю".

Можно обвинить автора и показать какую огромную работу проводит вендор по улучшению продукта. Однако, каждый вендор делает эту работу, но с точки зрения пользователя видны только изменения и новый функционал. И вендоры работающие на конкурентном рынке также делают и внутреннюю работу, и внедряет новые возможности.

Однако есть другие вендоры, которые вроде бы и не заметны на рынке, но имеют заметные объемы, при этом интересны их методы продвижения на рынке.

Например, автора заинтересовал продукт под названием Traffic Inspector. Являясь, по сути, межсетевым экраном, продукт развивается от функциональности управления трафиком. То есть, создателям продукта удалось найти нишу, где продукт начал развиваться, при этом не противопоставляя себя именитым брендам (той же Cisco Systems), а дополняя их: обеспечивая, по сути, функционал расширенного прокси-сервера (если так можно сказать) и дополняя основные системы безопасности полезным функционалом. Результаты очень интересные: за 9 лет компания продала 55 тыс. лицензий на свое серверное ПО!!! И в 2012 году ее продажи в рыночной доле (методику оценки рыночной доли см. выше) сравнимы, с некоторыми хорошо известными VPN вендорами (например S-terra).! Компания уделяет много времени вопросам сертификации по требованиям ФСТЭК России, развивает функционал и уже достаточно давно выпускает продукт в виде программно-аппаратного комплекса с предустановленным ПО. Сейчас продукт можно смело назвать нормальным межсетевым экраном, отвечающим современным требованиям. Опять же, не замахиваюсь на категорию NGFW. Согласитесь, интересный пример того, как построить бизнес, не имея друзей в определенном министерстве или большой компании, которая станет донором для обеспечения развития компании и продукта в целом.

Другое интересное наблюдение: практически половина дохода, а в некоторых случаях и больше, у отдельных вендоров (например, «АМИКОН», «ИнфоТеКС») приходится на VPN-клиентов! Такое в западном мире немыслимо, почти все международные вендоры, в основном, раздают VPN-клиентов бесплатно. Однако для России в этом нет ничего удивительного. Пока в составе Linux или Windows нет встроенных российских криптоалгоритмов, не будет изменений и в этой сфере. В части ОС Android или iOS тенденции показывают, что там почти все клиенты VPN и др. будут платными. Соответственно, судя по темпам, продажи VPN-клиентов будут только расти.

Краткие выводы

Таким образом, российский рынок сетевой безопасности имеет объем примерно 570 млн. долл. №1 на российском рынке по продажам в этом сегменте безусловно является компания Cisco Systems. Второе место, неожиданно для всех, занимает компания «ФАКТОР-ТС», затем Check Point, далее «ИнфоТеКС», «АМИКОН» и др.

Если брать во внимание только западных вендоров, второе место – Check Point, третье – компания Stonesoft, делящая его с компанией Juniper Networks. Справедливости ради стоит отметить, что получить достоверные данные по компании Juniper Networks не удалось, она старается не предоставлять данных. Со слов отдельных представителей компании, их объем порядка 20 млн. долл., однако автору не известны проекты с оборудованием безопасности этой компании, кроме проектов в УФСИН, ряде ФОМС, ЛУКОЙЛе (в роли антивирусного шлюза и в «ЛУКОЙЛ Оверсиз») и небольшом количестве других организаций. Остальные вендоры, как показало исследование, пока имеют относительно небольшие объемы продаж, серьезно отставая от лидеров.

№1 среди российских вендоров, судя по результатам, является компания «ФАКТОР-ТС». Наиболее распространенной и занимающей уверенное второе место среди российских вендоров является компания «ИнфоТеКС».

Если оценивать рынок со стороны экспансии западных вендоров, то картина достаточно интересная.

Отрадно видеть, что во многих организациях сохранились люди, способные думать и анализировать, которые не принимают квадраты Гартнера на веру и тестируют про-

дукты. Именно поэтому в России позиции вендоров не совпадают с североамериканским рынком, к результатам которого нас так пытаются приучить отдельные вендоры (конечно, из США). С другой стороны, отчетливо видно, что все российские продукты, имеющие более или менее серьезные продажи, находятся, можно сказать, в «защищенных» от конкуренции нишах, и, видимо, поэтому по функциональности и возможностям сильно уступают западным аналогам. Нет конкуренции – нет серьезного развития.

Кроме того, например, ни у одного вендора VPN-решений автор не увидел стремления сделать продукт мирового класса и завоевывать международный рынок. Скорее их поведение говорит о стремлении получить кусочек рынка в России и никого туда не пускать. Это, к сожалению, рано или поздно может привести к полной деградации.

Рынок, по мнению вендоров, растет, и в среднем большинство вендоров увеличили свой объем в 2012 году в сравнении с предыдущим на 20–25%. Некоторые вендоры росли быстрее рынка, например, Check Point и Stonesoft.

Рынок инструментальных средств анализа защищенности сейчас оценивается примерно в 47 млн. долл.

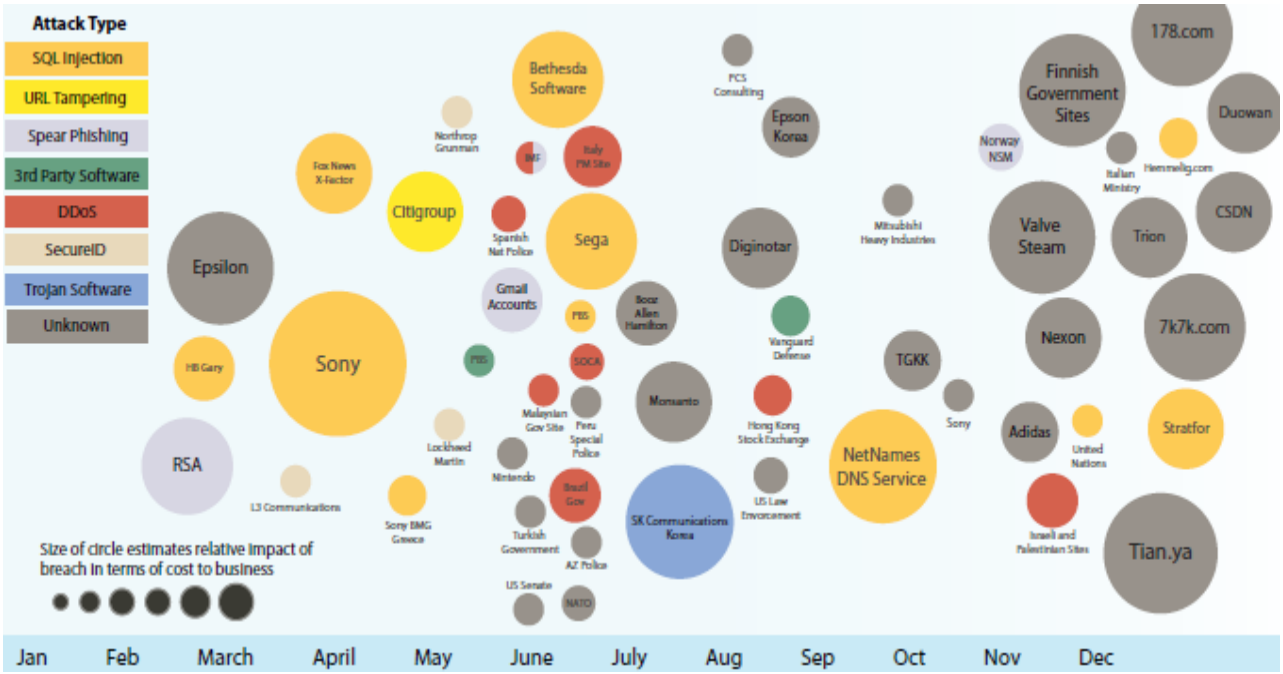
В целом рынок аппаратных средств двухфакторной аутентификации оценивается примерно в 91 млн. долл.

Основные тенденции рынка

Основным двигателем рынка в последние годы выступало законодательство по персональным данным, PCI DSS. В ближайшее время двигателем рынка, скорее всего, останется законодательство по персональным данным, дополнительным драйвером может стать закон о национальной платежной системе и желание российского правительства обеспечить защиту от кибератак.

Интересно, что за контроль над средствами IPS и другими подобными системами постоянно борется ФСБ, и в случае полной победы нас ожидают очередные затяжные войны сертификатов уже на рынке реальной безопасности.

Если смотреть на исследования различных групп безопасности (IBM X-Force, Symantec и др.), рынок безопасности становится все более серьезным. Последние известные взломы очень известных организаций (NASA, Sony, RSA, Lockheed Martin, Gazprom), где вопросы безопасности рассматриваются очень серьезно и где на момент взлома стояли очень популярные в США и в мире продукты безопасности, четко показывают, что необходимо переходить на новые принципы, и, видимо, средства безопасности нового поколения. Этот постулат хорошо иллюстрирует слайд из документа IBM X-Force



IBM X-Force 2012 trend and risk report

Серым цветом помечены взломы, которые неизвестно как были сделаны. Другими словами, средства безопасности не увидели атак и не зарегистрировали никакой «плохой» активности.

Таким образом, рынок безопасности вступает в эпоху кибервойн, когда все способы и арсеналы средств из государственных сфер и области действий разведок будут применяться и уже начинают применяться как в области конкуренции между различными организациями и фирмами, так и для дезорганизации какого-либо производства (например, иранская ядерная программа).

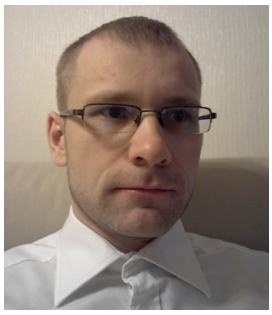
Динамика сектора

Стоит отметить, что из года в год системы безопасности делают значимые шаги вперед, становясь необходимым ИТ-инструментом современных предприятий. Связано это со многими факторами. Во-первых, репутационные риски и риски отказа в обслуживании клиентов многократно возросли. Все большая часть населения начинает использовать Интернет и информационные технологии в повседневной жизни. Люди все чаще делают покупки через Интернет, получают услуги/госуслуги и пр. Пока это небольшая часть населения нашей страны, но из года в год эта доля растет в геометрической прогрессии. Компании больше не могут позволить себе децентрализованные системы, когда над одной и той же задачей в разных регионах, в разных филиалах компании трудится большое количество сотрудников. Происходит централизация ресурсов, некоторые начинают использовать облачные сервисы и услуги, что сильно изменяет бизнес-процессы, а соответственно, и ИТ-инфраструктуру компаний. Меняются подходы к системе информационной безопасности, а также ее инфраструктура. Также сохраняется тенденция к использованию программно-аппаратных комплексов, а не программных решений.

Если посмотреть на рынок сетевой безопасности в мире по состоянию на 7–10 лет назад, то можно сказать, что была определенная эпоха застоя. Шло сращивание функционала (появлялись UTM-решения) в межсетевых экранах, но не с точки зрения потребностей, это были маркетинговые «фишки». Совершенствовались средства безопасности (добавлялись по 2–3 новые функции в новой версии). Сейчас ситуация совсем иная. Атаки стали целевыми на конкретные организации, вредоносная активность трансформируется из просто засорения компьютеров в инструмент зарабатывания денег, саботажа, политической и конкурентной войны.

Соответственно, стоит ожидать поступательного увеличения рынка сетевой безопасности, появления новых вендоров, адаптированных уже под новые реалии. Уже присутствующие вендоры вынуждены будут изменять и дополнять новым функционалом свои продукты, и это уже происходит на рынке.

РЫНОК СИСТЕМ КОНТЕНТНОЙ ФИЛЬТРАЦИИ



Сергей
ТРЕЩАЛИН

Рынок решений контентной фильтрации составляют решения, обеспечивающие безопасность входящих и исходящих интернет-соединений организаций от множества угроз, существующих в сети Интернет сегодня. Это вирусы, шпионские программы, фишинг-атаки и многие другие. Данные решения представлены в различных вариантах развертывания: программное обеспечение, программно-аппаратные комплексы, облачные сервисы, а также гибридные решения.

Игроки

На рынке средств контентной фильтрации представлено немало игроков, как уже зарекомендовавших себя, так и абсолютно новых. Если разделить рынок по потребителям, то решения представлены на всех уровнях, как на уровне телеком-операторов, так и на уровне домашних пользователей, которые в свою очередь также могут являться пользователями услуг телеком-оператора. При всем при этом некоторые из компаний имеют как широко масштабируемые решения для стремительно развивающихся компаний, так и решения для домашних пользователей.

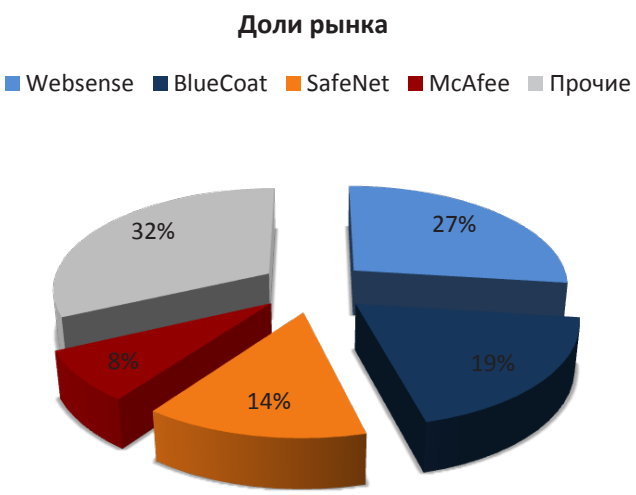
Последние годы на рынке контентной фильтрации можно назвать периодом поглощений. Изначально решения контентной фильтрации в ряде компаний развивались в качестве единичных «флагманских» продуктов. Однако такой подход значительно ограничивал как возможности развития самих продуктов, так и их присутствие на рынке. Достаточно отметить несколько компаний, подвергшихся такому поглощению: SurfControl, Secure Computing, Internet Security Systems, Aladdin, IronPort.

Отметим основных игроков на данном рынке:

- BlueCoat;
- Websense;
- SafeNet;
- McAfee.

Далее идут так называемые нишевые игроки:

- Cisco;
- Symantec;
- TrendMicro;
- Microsoft;
- PaloAlto;
- Sophos;
- Fortinet;
- Barracuda Networks;
- Zscaler;
- PineApp.



Причем это не все игроки данного рынка, а лишь малая часть, создающая основное предложение на рынке. Такое обилие создает немалые трудности при выборе решений, как для потребителей, так и для поставщиков.

Тенденции

Стремление в облако. Решения по контентной фильтрации – одни из немногих на рынке средств ИБ, которые могут быть предложены в виде сервиса, а не программного обеспечения или программно-аппаратного комплекса. Такой сервис позволяет снизить ТСО предприятия, однако немногие компании пока что готовы передавать средства ИБ на внешнюю поддержку.

Расширение функционала. Обилие предложений на рынке подталкивает производителей на создание уникальных предложений. Во-первых, многие уже привыкли, что контентный фильтр – это база категорий ресурсов сети Интернет и сетевых протоколов, однако сейчас это потоковый антивирус, удаление активного контента, контроль полосы пропускания, проксирование приложений, контроль утечек информации, верификация сертификатов. Во-вторых, некоторые производители стали дополнять свои решения средствами контентной фильтрации (Stonesoft, Juniper, Zyxel, WatchGuard).

Контентный фильтр для телеком-оператора. Все больше телеком-операторов дополняют свои портфели услугами по фильтрации входящего интернет-трафика. Первопричинами для данных действий являются стремление расширения портфеля услуг оператора и попытка повышения ARPU.

События

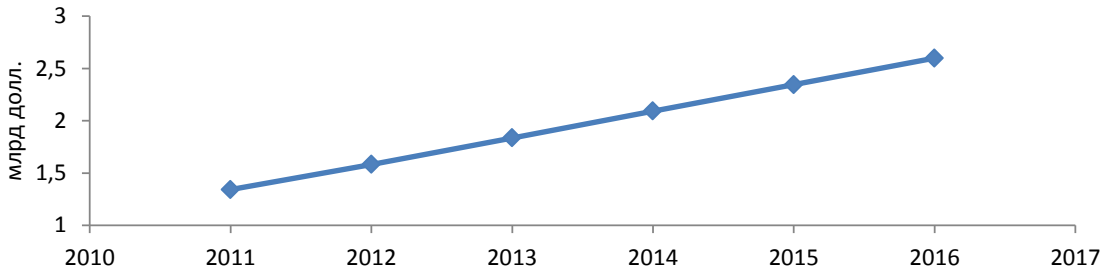
Рынок решений контентной фильтрации обычно небогат на события, достойные освещения в новостных колонках. Чаще всего новости ограничиваются информацией о поглощениях. Однако в 2012 году главным источником событий на рынке стало Правительство РФ. Во-первых, в рамках программы информатизации учебных заведений возникли потребности в фильтрации доставляемого интернет-контента в учебные учреждения. Во-вторых, правительство внесло изменения в Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации». Данный закон вводит требования к операторам по ограничению доступа к запрещенным ресурсам. Телеком-операторы не заставили себя ждать, что выразилось в явном повышении спроса на решения по контентной фильтрации операторского класса. На помощь Правительству РФ с целью обеспечения исполнения данных законодательных инициатив пришли представители российского бизнеса, мгновенно представив на рынке отечественные решения контентной фильтрации (МФИ софт, NetPolice Solutions).

Динамика

Рынок решений контентной фильтрации России и стран СНГ повторяет общемировые тенденции развития. Локомотивами остаются рынки России и Казахстана, на них приходится основной объем продаж решений данного класса. На мировом рынке заметны тенденции к плавному снижению темпов роста, однако к 2017 году этот рынок может достигнуть отметки в 3 млрд долл.

В 2012 году объем российского рынка решений контентной фильтрации составил примерно 10% от мирового, что составило приблизительно 500 млн руб.

Прогноз мирового рынка средств контентной фильтрации (The Radicati Group, Inc.)



РЫНОК СИСТЕМ АНТИВИРУСНОЙ ЗАЩИТЫ

Илья ШАБАНОВ

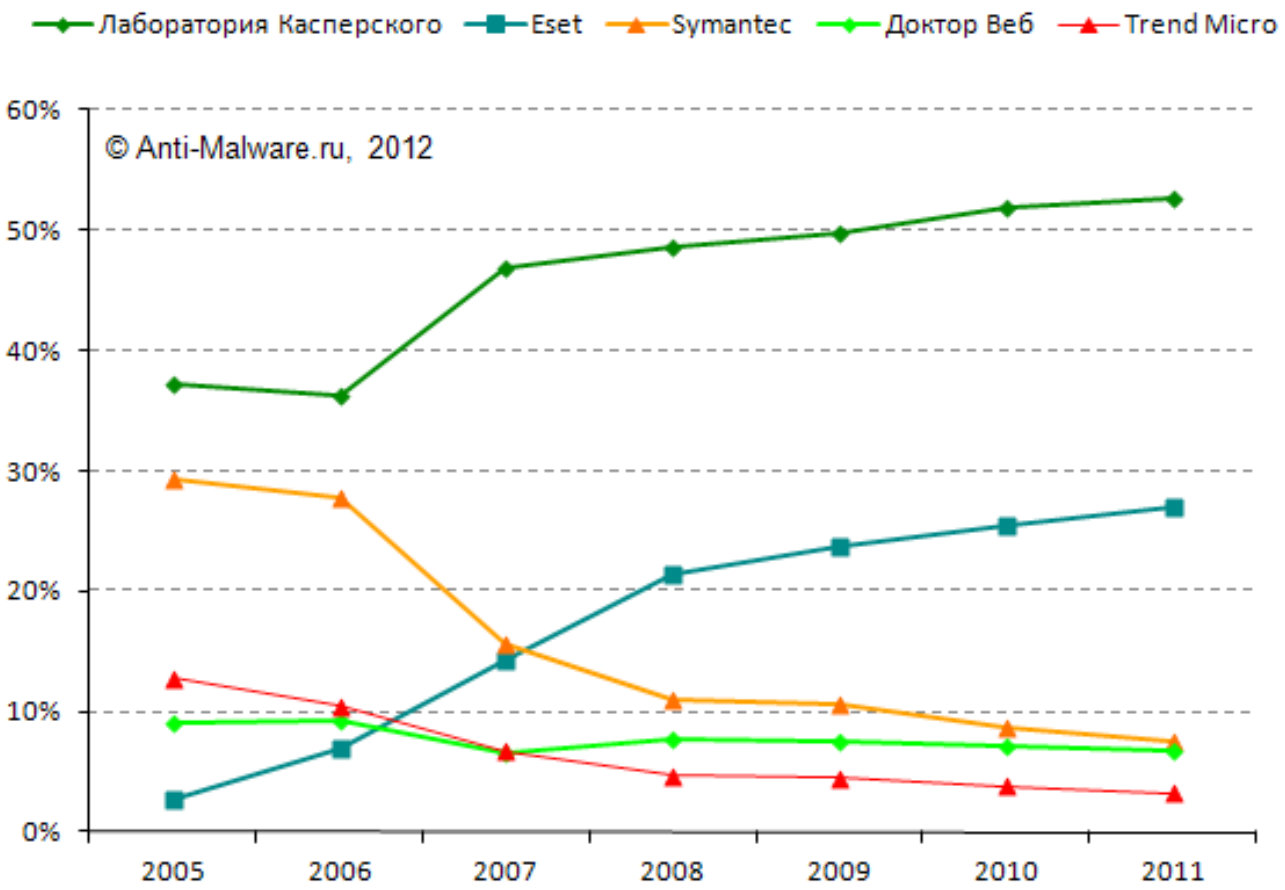
В настоящий момент антивирусный сегмент российского рынка информационной безопасности является самым крупным и опережает другие сегменты (например, сегмент сетевой безопасности) как минимум в несколько раз. Согласно нашим исследованиям, совокупный оборот этого рынка в 2011 году составил 334 млн долл., а в 2012 году, по предварительным данным, достиг 400 млн долл. При этом сохраняет тенденцию к росту. Это происходит на фоне сокращения аналогичного сегмента в некоторых странах Евросоюза, в частности в Греции, Италии и Испании (до 20% в год).

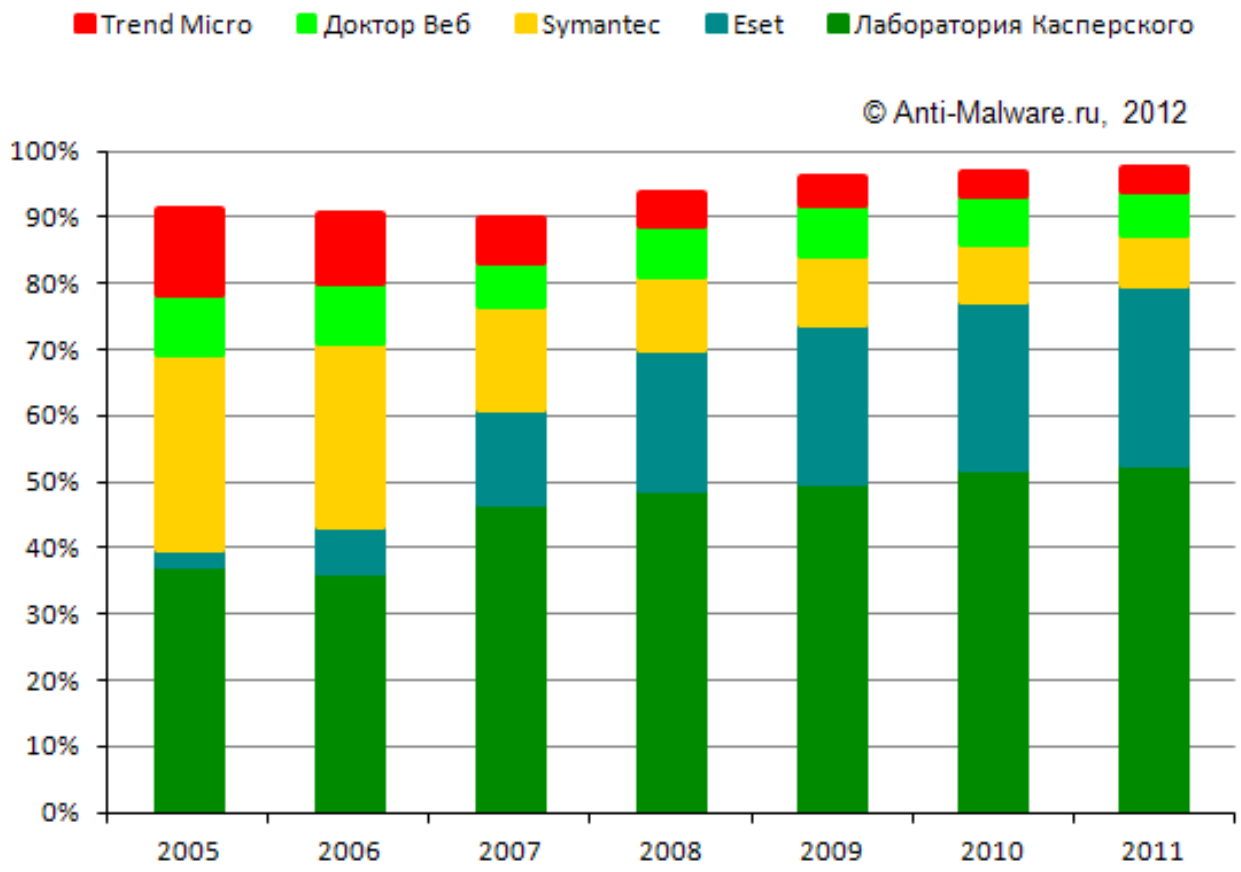
Основные игроки

Основными игроками рынка являются:

- «Лаборатория Касперского»;
- Eset;
- Symantec;
- «Доктор Веб»;
- Trend Micro.

Доли рынка каждого из пяти производителей:





Как видно из графиков, доли компаний «Лаборатория Касперского» и Eset стабильно растут, в то время как остальные производители теряют позиции. Причем, в отличие от Eset, который за время наблюдения всегда увеличивал продажи и свою долю рынка, для «Лаборатории Касперского» стал переломным 2007 год. Именно тогда компания сумела сломать негативный для себя тренд в России и включиться в ралли роста. В противном случае рыночные позиции этой компании были бы существенно ниже.

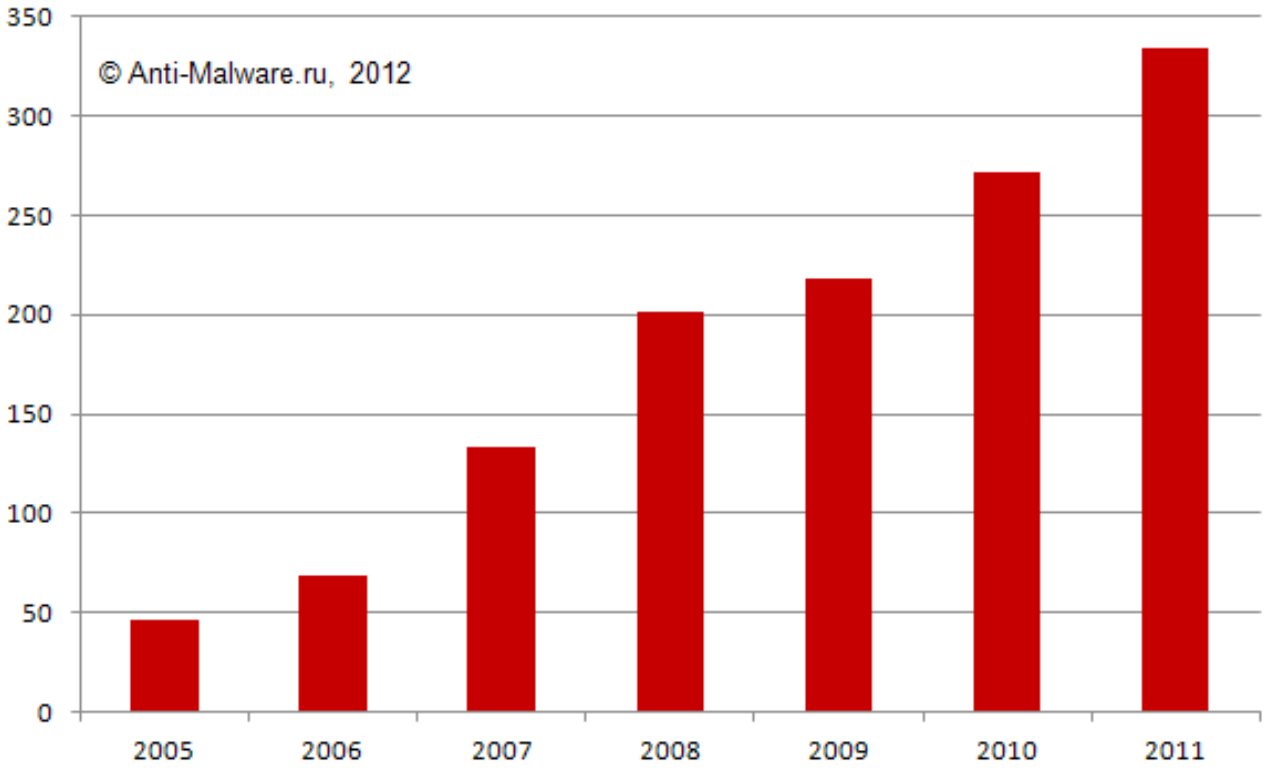
Для остальных игроков 2007 год оказался ключевым в негативном смысле. С этого момента Symantec и Trend Micro стали стабильно терять позиции, а «Доктор Веб» потерял потенциальные возможности для быстрого роста.

Если подводить некоторый итог по данным наблюдения за семь лет, то нельзя не отметить главное. *Российский антивирусный рынок обладает высокой степенью зрелости, основными игроками на котором являются «Лаборатория Касперского» и Eset, в окружении слабых конкурентов.*

Данные общего объема антивирусного рынка в России за период с 2005 по 2011 год включительно.

Среднегодовой рост рынка за этот период составил 42%. Пик роста пришелся на 2007 год, когда рост составил рекордные 94%. В период кризиса в 2009 году рост почти прекратился и составил меньше 9%, но затем продолжился с новой силой на 23–24% ежегодно.

По техническому анализу пока еще рано говорить о насыщении рынка или существенном замедлении его роста. Если не будет очередного витка глобального экономического кризиса, то антивирусный рынок в ближайшие несколько лет может спокойно продолжить расти на 15–25% ежегодно.



Дмитрий
АРТЕМЕНКОВ

Основные игроки сектора рынка

На сегодняшний день российский электронно-цифровой рынок представляет собой стремительно развивающуюся отрасль. Лидирующие места на нем занимают удостоверяющие центры (УЦ) отечественных разработок на основе асимметричного алгоритма ГОСТ-Р 34.10-2001, западные решения занимают лишь определенную нишу УЦ, используемых во внутреннем документообороте коммерческих организаций.

Такую специфику обуславливают, конечно же, жесткие требования ФСБ России к шифровальным средствам и электронно-цифровой подписи.

Согласно приказу № 796 ФСБ России от 27 декабря 2011 года, а также «Положению о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» устанавливаются требования к средствам УЦ в части их разработки, производства, реализации и эксплуатации.

Нельзя отрицать, что в ряде организаций имеются УЦ, развернутые не на ГОСТ, но они применяются лишь во внутрикорпоративном электронном документообороте и их доля очень мала.

В настоящее время в России насчитывается около 200 организаций, оказывающих услуги удостоверяющих центров. Значительная доля рынка приходится на несколько крупных компаний, таких как «СКБ Контур» или «Калуга-Астрал».

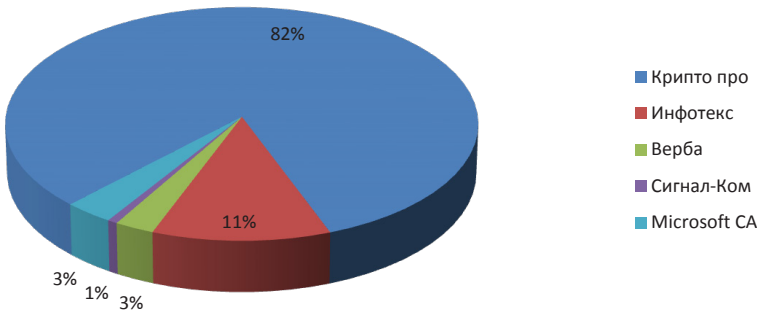
Существующие основные игроки на рынке производителей криптосредств, используемых в удостоверяющих центрах в России:

- ООО «Крипто-Про»;
- ОАО «Инфотекс»;
- ЗАО «Сигнал-Ком»;
- ЗАО «МО ПНИЭИ».

Некий возможный анализ использования удостоверяющих центров в юридически значимом документообороте можно провести по данным аккредитованных УЦ на портале уполномоченного федерального органа в области использования электронной подписи.

По этим данным доли рынка можно распределить следующим образом (добавленные данные по использованию Microsoft CA взяты из среднестатистических данных):

Распределение рынка



Безоговорочным лидером который год подряд является компания «Крипто-Про» со своим одноименным продуктом. Она давно захватила лидирующие позиции среди сертифицированных УЦ и с каждым годом лишь укрепляет свои позиции на российском рынке.

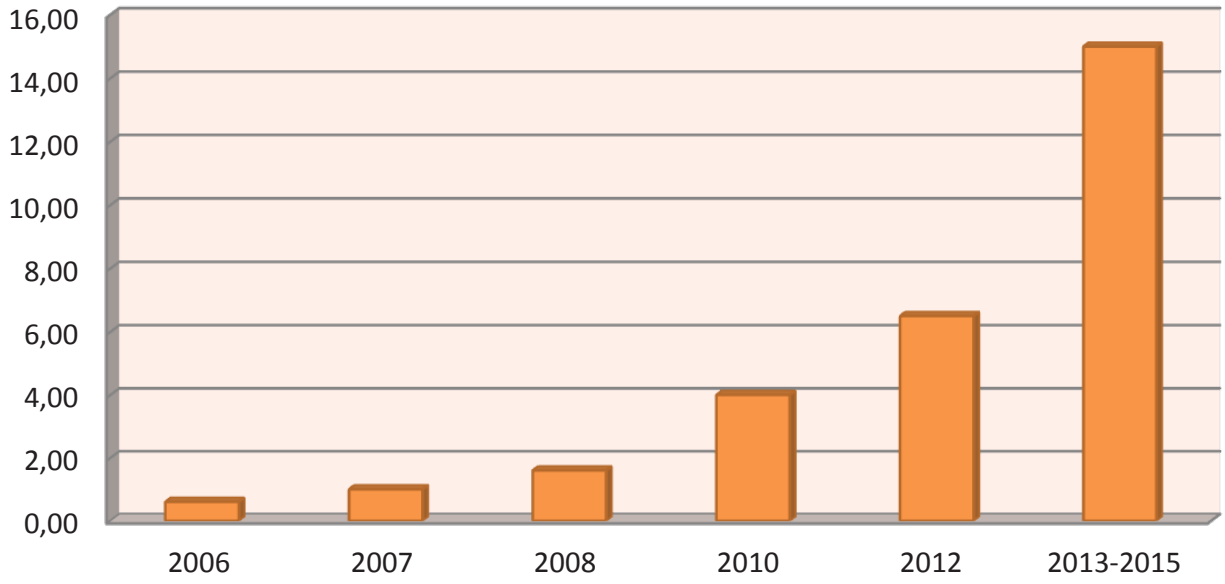
Ближайший преследователь – компания «Инфотекс». Она имеет более широкую линейку продуктов, использует криптобиблиотеки собственной разработки. Ее продукт ViPNet CUSTOM одновременно может выполнять роль не только удостоверяющего центра, но и служить средством построения защищенных сетей. Однако стать лидером компании так и не удается.

Динамика сектора

Главный потребитель услуг УЦ – юридические лица, использующие ЭЦП для нужд своей организации.

Рынок ЭЦП отличает устойчивый рост в течение нескольких лет. Увеличивается количество как организаций, получающих электронно-цифровую подпись, так и выданных сертификатов на одну организацию.

Количество выданных сертификатов, млн



Главным образом на это повлияло изменение российского законодательства, регламентирующего несколько направлений применения ЭЦП:

- перевод электронных торгов на основные федеральные торговые площадки (такие как Сбербанк-АСТ, РТС-тендер или ЭТП ММВБ «Госзакупки»). В связи с появлением специальных выделенных федеральных торговых площадок резко увеличилось количество выдаваемых ЭЦП;
- увеличение количества сдачи электронной отчетности в контролирующие органы – налоговую службу, Пенсионный фонд и страховые организации. Около 80% всех российских юридических лиц в 2012 году уже передают свои отчеты именно в электронном виде;
- появление возможности использовать электронно-цифровую подпись для заключения договоров и осуществления юридически значимого документооборота между организациями (также можно отметить все больший переход на системы электронного документооборота в связи с информатизацией предприятий как таковых).

После утверждения форматов электронных учетных документов (таких как счета-фактуры) и порядка их предоставления можно прогнозировать еще большую интеграцию электронных документов в документооборот и тем самым увеличение использования ЭЦП.

Колоссальный рост рынка ЭЦП можно ожидать от использования ЭЦП физическими лицами в госуслугах и осуществления электронных платежей (интернет-банкинг). Пока этот рынок практически не освоен.

РЫНОК СИСТЕМ СБОРА И КОРРЕЛЯЦИИ СОБЫТИЙ (SIEM)

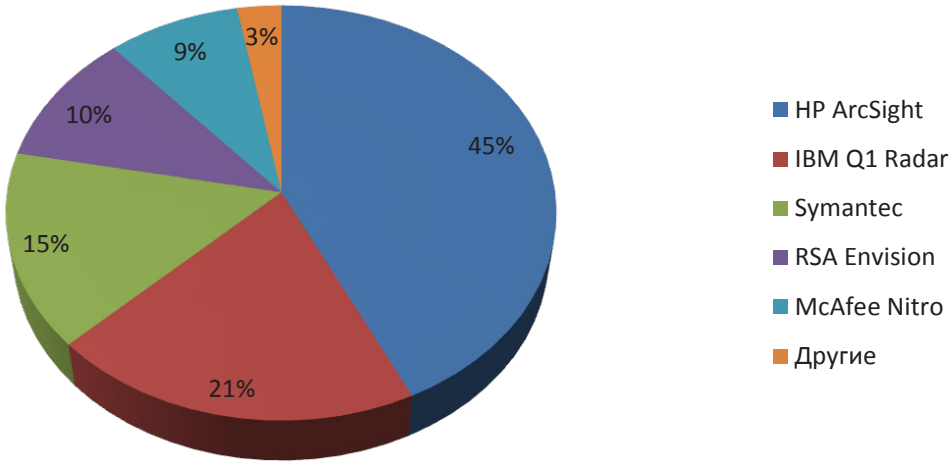
Владимир ЕМЫШЕВ

На сегодняшний день на российском рынке представлено достаточно большое количество SIEM-систем – систем мониторинга, управления, анализа и хранения информации и событий информационной безопасности. Основные игроки на рынке-2012:

- IBM Q1 Radar;
- HP ArcSight;
- Tibco Loglogic;
- McAfee Nitro;
- Symantec;
- RSA Envision;
- Splunk.

По результатам проведенного исследования с привлечением специалистов, работающих в вендорах и дистрибьюторах решений SIEM, доли рынка распределились следующим образом.

Доли игроков на российском рынке



Безоговорочным лидером является HP Arcsight. Компания одной из первых пришла на наш рынок и, несмотря на возрастающую конкуренцию, продолжает удерживать лидирующие позиции в своем сегменте.

Идущие следом вендоры предлагают широкую линейку продуктов, известную российскому рынку, имеют представительства, вкладываются в развитие своих продуктов, что в совокупности приводит к росту продаж и увеличению доли рынка.

К «другим» относятся такие вендоры, как Splunk и Tibco Loglogic, имеющие качественные продукты и специализирующиеся исключительно на SIEM. Данные вендоры делают первые шаги на российском рынке, но ценовая политика, функционал и линейка, рассчитанная на организации любого размера, позволяют данным производителям рассчитывать на успешное продвижение.

Основные тенденции рынка

Долгое время SIEM-системы могли позволить себе только крупные компании с хорошим годовым ИТ-бюджетом.

Однако в последние годы появились системы all-in-one. В данных продуктах механизмы сбора, хранения, поиска, нормализации и корреляции информации реализованы в рамках одной коробки. Такие продукты, как HP ArcSight express, Tibco Loglogic MX, McAfee Nitro ESM, QRadar 2100 All-In-One Appliance, обеспечивают функционал SIEM, исходя из потребностей небольших и средних по величине компаний.

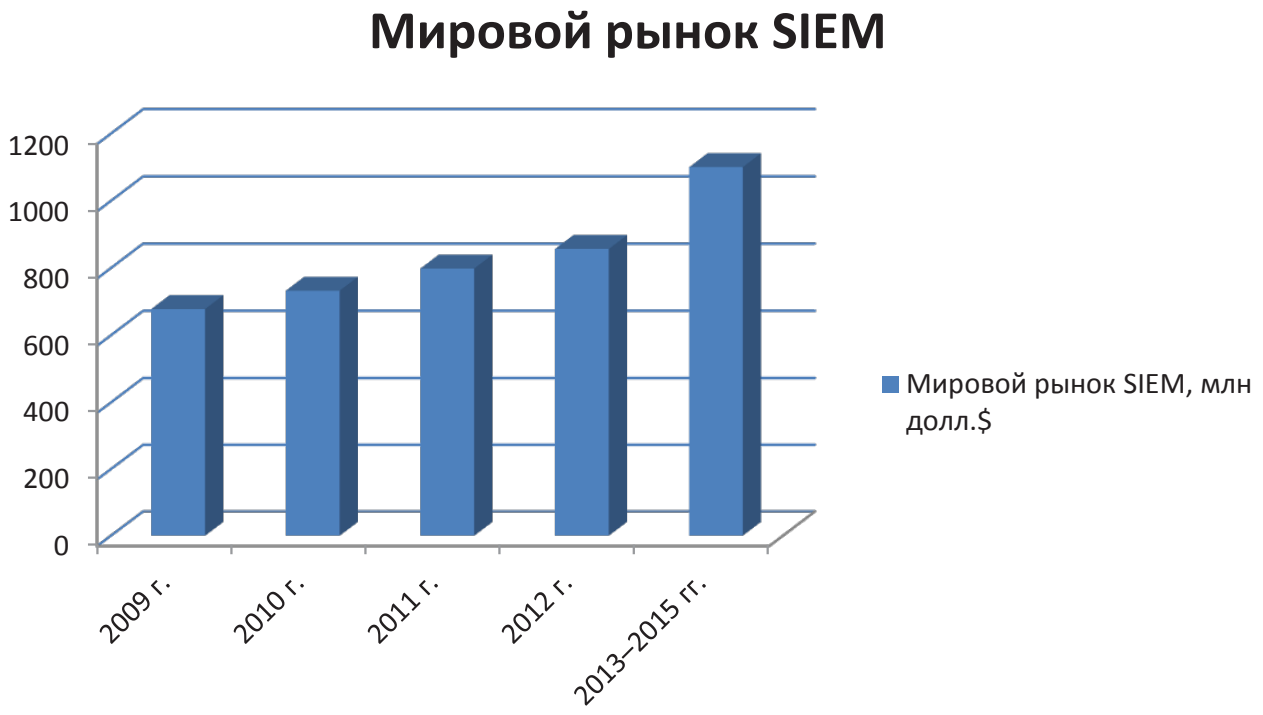
Также в этом году произошло много громких слияний. Это обусловлено тем, что изначально системы делились на SEM и SIM и, следовательно, тяготели к соответствующему функционалу, частично реализуя другой. В 2011–2012 годах крупные игроки SIEM-рынка старались максимально наполнить свои SIEM-системы функционалом SIM и SEM.

McAfee поглотила Nitro и усилила свою SIEM-систему функционалом SEM. Лидер рынка ИТ-технологий HP приобрел Arcsight, инвестируя новые средства в продукты этого вендора, с целью поддержания лидерства на рынке. В продукты IBM гармонично влился Q1 Radar, придя на смену устаревшей линейке Tivoli. Tibco приобрел Loglogic, внеся в функционал SIEM новые аналитические возможности, визуализируя все происходящее в сети и позволяя расследовать инциденты информационной безопасности в режиме реального времени.

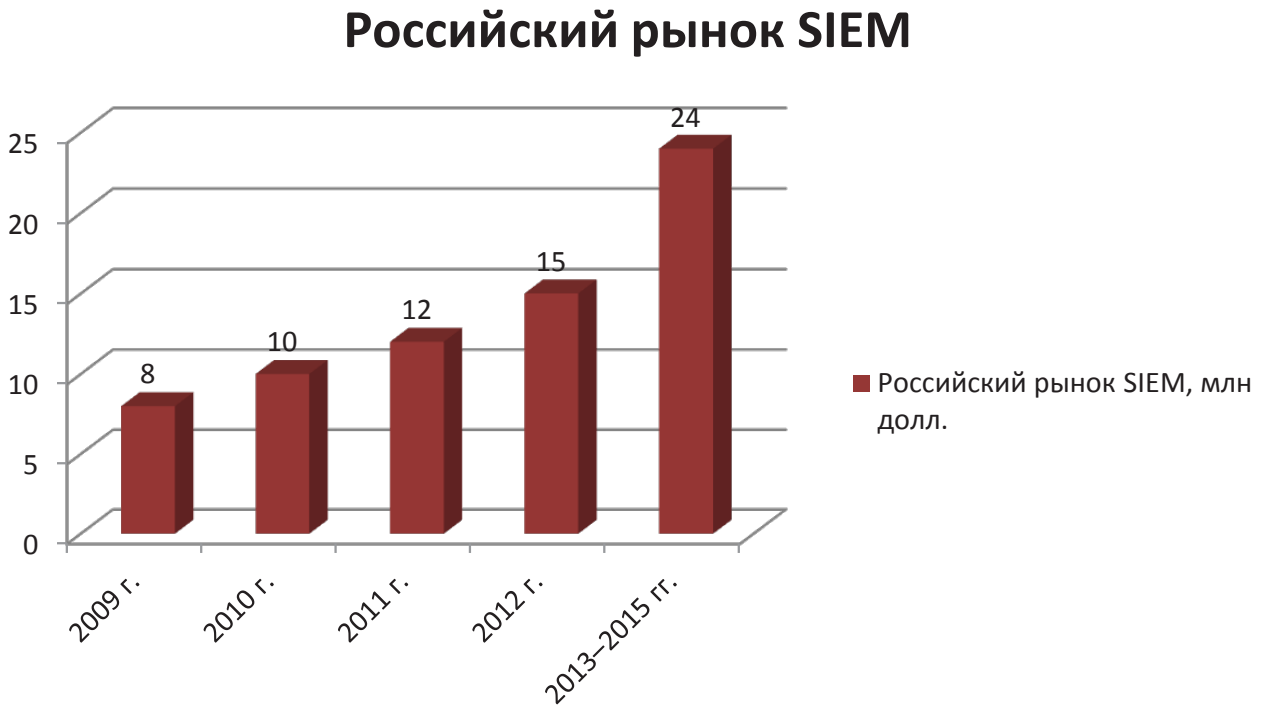
Динамика сектора

Стоит отметить, что из года в год SIEM-системы делают значимые шаги вперед, становясь необходимым ИТ-инструментом современных предприятий. Связано это прежде всего с двумя векторами, по которым идет развитие ИТ-технологий в целом: централизацией и виртуализацией. SIEM-системы централизуют хранение информации о событиях, происходящих в ИТ-инфраструктуре, и управление ею, также многие производители предлагают версии, доступные для развертывания в виртуальной среде.

По отчету аналитического агентства Frost & Sullivan за 2011 год, мировой рынок SIEM-решений с 2009 по 2015 год возрастет практически вдвое.



Положение дел на мировом рынке вполне проецируется на российский рынок.



РЫНОК СИСТЕМ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ (IDM)

Александр САНИН

ВМЕСТО ВВЕДЕНИЯ

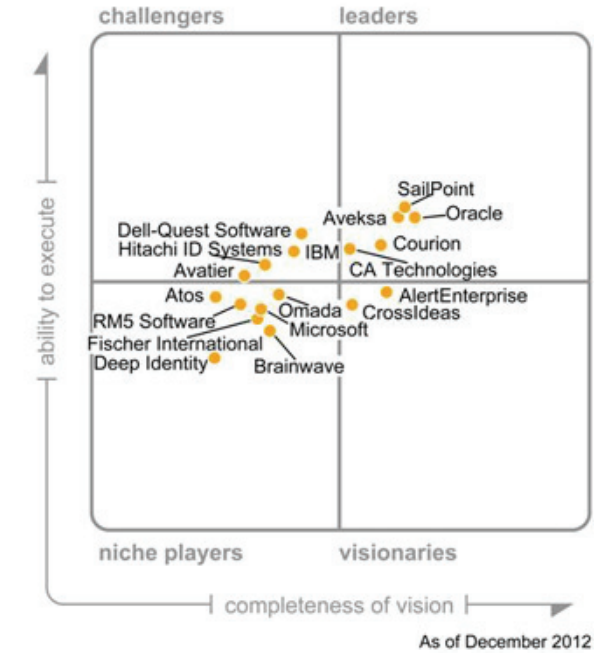
Данный материал носит обзорный характер, целью его являлось дать первичное представление о рынке, основных игроках, объемах и трендах.

История развития рынка

Развитие ИТ-систем и бизнес-приложений послужило толчком к развитию IDM-решений (или, в более широком смысле, IAM-решений) -- решений, призванных автоматизировать процессы управления доступом. На Западе (в Европе и США) бурное развитие данного класса решений началось ориентировочно в 2002–2003 годах. К этому времени там уже существовал более-менее очерченный рынок со своими игроками. Примерно в 2006–2007 годах западный рынок IDM-решений начал так называемый процесс консолидации, т.е. произошли крупные сделки-поглощения небольших разработчиков решений IDM крупными игроками, такими как Oracle, Sun и SAP. Ну а к 2007–2008 годам рынок практически приобрел те привычные очертания, что мы видим сегодня на «магических квадрантах» Gartner:

Магический квадрант Gartner по состоянию на декабрь 2012 года:

Figure 1. Magic Quadrant for Identity and Access Governance



Source: Gartner (December 2012)

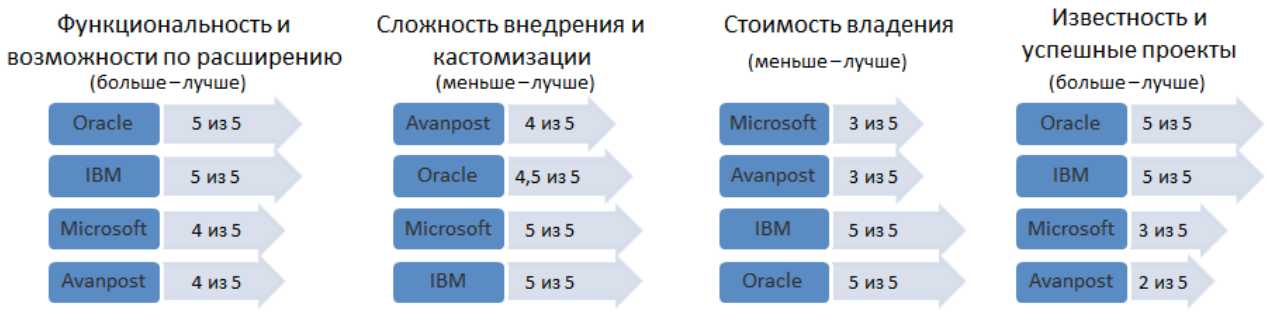
Последние пару лет Gartner стал делать квадранты по еще более широкому классу решений – IAG (Identity and Access Governance). Суть такого расширения в том, что многие решения уже технологически развились далеко за рамки одного только процесса управления учетными записями. И возможно, еще через несколько лет мы совсем перестанем использовать аббревиатуры

IDM или IAM и будем говорить IAG. Пока же мы будем оперировать более привычными и понятными терминами.

Российские реалии и основные игроки

Российский рынок IDM-решений отчасти повторяет западные очертания, за несколькими исключениями. Во-первых, развитие российского рынка IDM по объективным причинам отстает от западного ориентировочно на 3–4 года. Во-вторых, на российском рынке широко представлены далеко не все игроки, а только крупнейшие западные бренды: Oracle, IBM, Microsoft. Решения от таких компаний, как Novell, Quest Software и Courion, встречаются только в единичных случаях, и говорить об их широком распространении не приходится. В качестве еще одной специфической черты российского рынка необходимо отметить появление в 2012 году нового (на сегодняшний день единственного) сугубо отечественного игрока – Avanpost. Хотя это игрок относительно новый, мы все же включили в данный обзор эту линейку продуктов, подробно изучив заявленные характеристики продукта, а также несколько успешных бизнес-кейсов.

В рамках подготовки к написанию данного обзорного материала было проведено краткое исследование с опросом нескольких экспертов российского рынка IDM. Кроме того, было произведено небольшое функциональное и ценовое сравнение решений. Исследование основывалось на экспертных оценках участников рынка, а также на информации из открытых источников. Краткие результаты этого исследования представлены ниже:



Как видно из полученных оценок, есть два технологических лидера в данном сегменте – это Oracle (усиливший свое влияние после поглощения Sun) и IBM. Тем не менее эксперты сошлись во мнении, что и остальные решения хоть и находятся в статусе догоняющих, но показывают неплохие результаты. В целом те или иные функциональные особенности, которые реализованы в продуктах, могут приниматься как действительно существенные только в очень специфичных проектах. Базовый же функционал довольно схож. Основные отклонения появляются лишь в графах стоимости и известности, что в общем тоже вполне поддается логическому объяснению – ценовые политики у всех компаний разные, а что касается известности, то налицо фактор времени. Кто появился на рынке раньше, тот и обладает большим количеством бизнес-кейсов в России.

Динамика и объем рынка

Объем мирового рынка IDM-решений в 2012 году оценивается аналитиками ведущих мировых агентств (Gartner и Forrester примерно сходятся в оценках, IDC говорит о несколько меньшем объеме рынка) ориентировочно близ отметок в 10–11 млрд долл. Большую часть этого рынка занимают США (чуть более 40%), следом идут Западная и Центральная Европа (около 30%). Специальных оценок конкретно по России, естественно, нигде в отчетах нет. Но, по мнению экспертов, участвовавших в исследовании, мы можем говорить о цифрах близ отметок в 0,5% от мирового объема, следовательно, мы можем говорить о цифрах в пределах 50–60 млн долл. в рамках 2012 года.

Объем российского рынка на фоне мирового, конечно, крайне мал, и этому есть объяснение, ведь российская специфика наблю-

дается и тут. Так, если в США и Европе IDM-решения применяются минимум в 80% бизнеса уровня Enterprise (т.е. 4 из 5 Enterprise-компаний применяют подобные решения), что частично продиктовано требованиями различных нормативных актов, то в России этот показатель не достигает и 20%. Более того, средний и малый бизнес в России вовсе не использует подобные решения в силу их стоимости. Ну а главной причиной таких результатов является отсутствие в России явных и жестких указаний на наличие подобных решений в рамках нормативной базы по информационной безопасности. Хотя предпосылки уже появляются, и это явно двигает рынок вверх.

Что касается динамики роста мирового рынка, в целом она оправдывала прогнозы последних лет. Так, в период с 2003 по 2007 год мировой рынок IDM-решений рос поступательно с ежегодным увеличением примерно на 8–9%. Мировой экономический кризис 2008 года внес в этот тренд сильные корректировки, но после того, как все оправились, стало наблюдаться возвращение тренда и стабилизация его на тех же уровнях (ежегодный прирост примерно на 10%).

Новые тренды и прогнозы

Как мы уже отмечали в начале данного материала, в последние пару лет наблюдается один интересный тренд – расширение самого понятия рынка IDM. Многие компании-разработчики наряду с потребителями подобных решений начинают рассматривать такие системы как неотъемлемую составляющую более широкого понятия – IAG. А это в свою очередь приводит к некоторой трансформации направления, обобщению ее с другими смежными темами из области управления доступом, такими как SSO и PKI, слиянию с тематикой риск-менеджмента и т.п. Именно поэтому, например, Gartner в рамках своих магических квадрантов начал рисовать именно квадранты по IAG – Identity and Access Governance.

Еще один интересный тренд, начинающий набирать обороты, – IDM-решения для широкого рынка, включая сегмент SMB. В целом такое движение понятно и оправдано, ведь автоматизация процессов в современных реалиях является необходимой и неотъемлемой составляющей любого бизнеса в погоне за увеличением прибыльности и сокращением издержек. Да и на рынке, ограниченном только Enterprise-сегментом, бесконечный рост просто невозможен. Осознавая данный постулат, многие компании-производители заговорили о реальном расширении рынка IDM и переходе его в том числе в сектор SMB.

Начали появляться и осторожные заявления о возможности работы IDM в облачной среде. Сначала западные лидеры рынка начали говорить о потенциальной возможности перехода в облака. Теперь уже звучат более прямые заявления: IDMaaS (IDM as a Service) – это не просто возможность, а скорее будущая необходимость. Впрочем, отечественные разработчики также подхватили данный тренд и активно заявляют о начале разработок в данной области. Время покажет, что из этого получится, ведь потенциально данный вид сервиса действительно может быть востребован, а вкупе с тенденцией расширения рынка на средний и мелкий бизнес это может стать действительно переломной вехой в развитии тематики IDM.

Ну и как следствие можно назвать еще одну тенденцию – в погоне за расширением рынка компании-разработчики начали сталкиваться с необходимостью серьезного изменения своих схем лицензирования и собственно стоимости. Говорить о каких-то существенных изменениях в рамках 2012 года еще рано. Мировые лидеры из числа Oracle и IBM пока не сделали каких-то видимых шагов в данном направлении. Но вот компании поменьше уже серьезно нацелились на сегмент среднего и малого бизнеса как на потенциальных покупателей, что явно отражается в их лицензионной политике. Так, например, компания Avanpost уже заявила о планах расширения российского рынка IDM в 10 раз за ближайшие 5 лет. Но вот оправдается ли эта тенденция, покажет только время.

РЫНОК СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ (СЗИ) ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (НСД)

Алексей КОМАРОВ

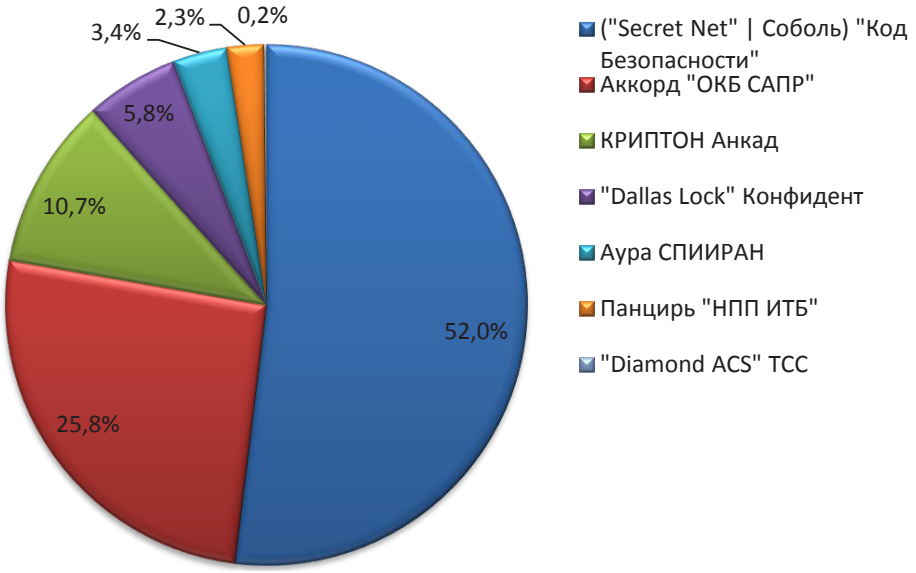
Основные игроки сектора рынка

В настоящее время среди основных игроков рынка СЗИ от НСД можно выделить следующие продукты (в скобках указан разработчик):

- Secret Net и «Соболь» («Код Безопасности»);
- «Аккорд» (ОКБ САПР);
- Dallas Lock («Конфидент»);
- «Панцирь» (НПП ИТБ);
- «Криптон» («Анкад»);
- СЗИ «Аура» (СПИИРАН);
- Diamand ACS (ТСС).

СЗИ от НСД по своему исполнению можно разделить на программные и программно-аппаратные, а по сфере применения – для защиты персональных данных и конфиденциальной информации (1Г) и для защиты гостайны и конфиденциальной информации высокого уровня (1Б-1В). Упрощенно будем называть «для ИСПДн» и «для гостайны».

Игроки сектора рынка	Тип	Предназначение
Secret Net + плата	программно-аппаратный	гостайна
Secret Net + TBL	программный	гостайна
Secret Net «Вариант К»	программный	ИСПДн
Dallas Lock 7.7	программный	гостайна
Dallas Lock 8.0-К	программный	ИСПДн
«Панцирь-С»	программный	ИСПДн
«Панцирь-К»	программный	ИСПДн
ПАК Аккорд + Аккорд-АМДЗ	программно-аппаратный	гостайна
«Криптон-Щит» + «Криптон-Замок»	программно-аппаратный	гостайна
СЗИ «Аура»	программный	гостайна
СЗИ «Аура 1.2.4»	программный	ИСПДн
Diamond ACS + плата	программно-аппаратный	гостайна
Diamond ACS	программный	ИСПДн



Основные тенденции сектора рынка

Согласно исследованию компании «Б-152» (разработчик автоматизированной системы защиты персональных данных), решающими факторами при защите персональных данных являются страх потерять деньги на штрафах от регуляторов (63% опрошенных) и чистота перед законом (41%). При этом при выборе подрядчика для решения вопроса о выполнении требований закона №152-ФЗ «О персональных данных» большинство опрошенных ориентируется на стоимость услуг (59%), вторым приоритетом является быстрота реализации проекта (49%).

Ситуация с решениями для защиты гостайны во многом представляется аналогичной.

Стоит разделять коммерческих заказчиков (например, аттестующих рабочие места для получения лицензии ФСБ или выполняющих требования по защите ПДн) и государственные организации.

Можно с уверенностью утверждать, что для коммерческих клиентов при выборе СЗИ от НСД наиболее важно следующее:

- формальное выполнение требований РД ФСТЭК (реализуется всеми сертифицированными СЗИ от НСД);
- совместимость с ОС компьютера, который будет аттестован (совместимость должна быть не просто реализованной, но и прописанной в сертификате);
- слабое влияние на компьютер в процессе работы (можно проверить с помощью демо-версии, поэтому чем легче ее получить, тем лучше);
- стабильность программного обеспечения (косвенно опять-таки можно определить с помощью демо-версии либо получить представление по отзывам других пользователей на форумах и пр.);
- отсутствие дополнительных средств, затрудняющих установку и эксплуатацию;
- минимальная цена.

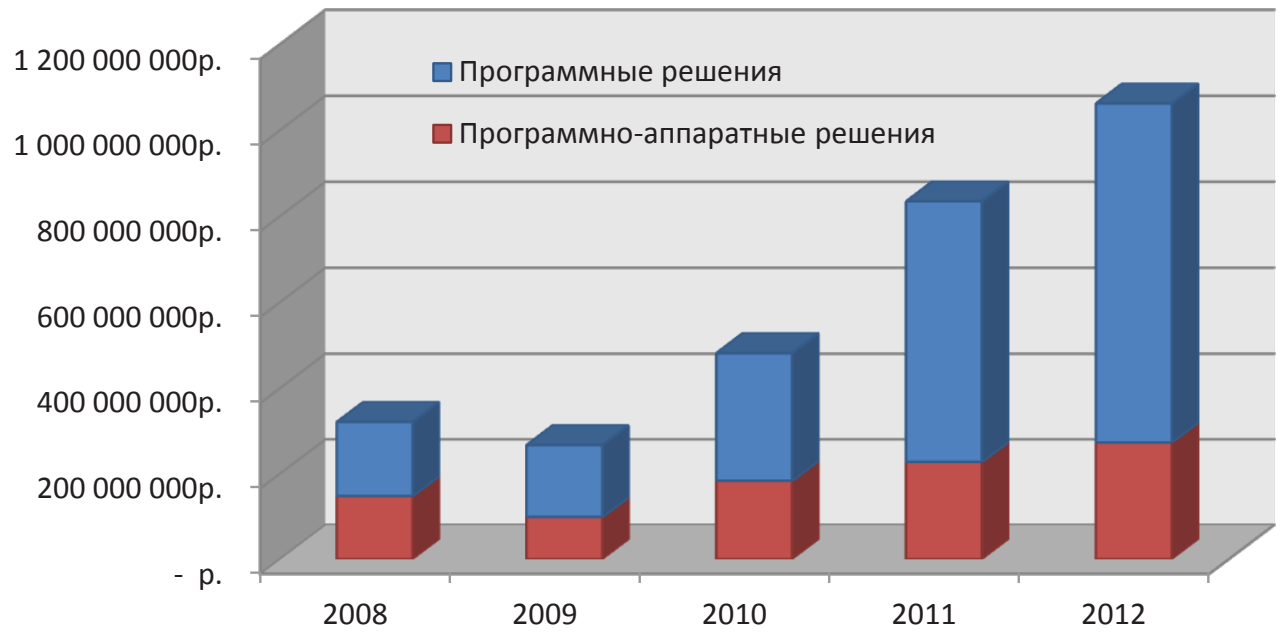
Для государственных заказчиков при выборе СЗИ от НСД важны те же факторы.

Динамика сектора

Согласно имеющимся данным, общий объем продаж средств защиты информации от несанкционированного доступа имел в 2008–2012 годах (на 2012 год приведен прогноз) динамику, представленную на диаграмме.

При этом в 2011–2012 годах объем рынка программно-аппаратных средств составил около 26% всех продаж СЗИ от НСД, а на долю чисто программных средств приходится соответственно примерно 74% рынка.

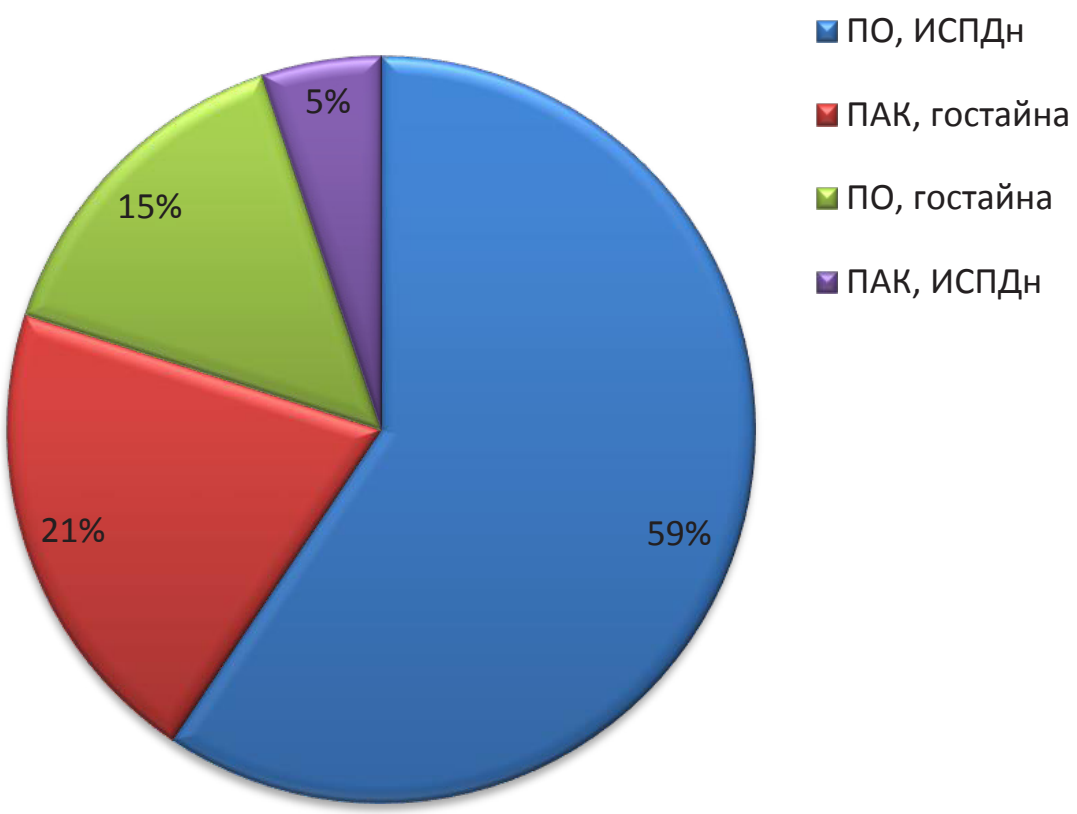
Важной тенденцией является также отсутствие значительной динамики роста аппаратных СЗИ, в частности вызванной увеличением числа ноутбуков и моноблоков, для которых использование аппаратных средств затруднительно.



Точных данных о распределении продаж СЗИ от НСД по сфере их применения (ИСПДн/гостайна) нет. С учетом того, что:

- требование об обязательности использования аппаратных плат «для ИСПДн» отсутствует,
- рынок гостайны консервативен и использование чисто программных средств является скорее исключением,

можно предположить, что не менее 80% рынка программно-аппаратных продуктов относится к категории «для гостайны», а из рынка чисто программных средств на долю «гостайны» приходится не более 15–20%.



ИНТЕГРАТОРЫ В ОБЛАСТИ ИБ

Евгений ЦАРЁВ

В рамках настоящего раздела рассматриваются только компании, оказывающие услуги в сфере информационной безопасности.

При этом мы не учитывали доходы интеграторов, которые были получены от реализации тех продуктов и услуг, которые не перечислены выше.

Также мы не учитывали доходы, полученные от дистрибуции собственных или сторонних решений. Это очень важно, например, для тех компаний, в состав которых входят как производители решений, так и дистрибьюторы.

Не рассматривались также компании-посредники, которые не оказывают услуги и не совершают поставки клиентам напрямую. Это ограничение необходимо для того, чтобы исключить из расчетов«двойныепродажи»/«двойной зачет» (перепродажи чужих проектов).

В отличие от схожих исследований и рейтингов мы не рассматривали в качестве участников рынка производителей, дистрибьюторов/реселлеров и консалтинговые компании, которые не имеют отношения к системной интеграции.

Интеграторский бизнес в области ИБ очень неоднороден.

По структуре бизнеса интеграторов можно разделить на следующие группы:

- ИБ – приоритетное направление;
- ИБ – второстепенное направление.

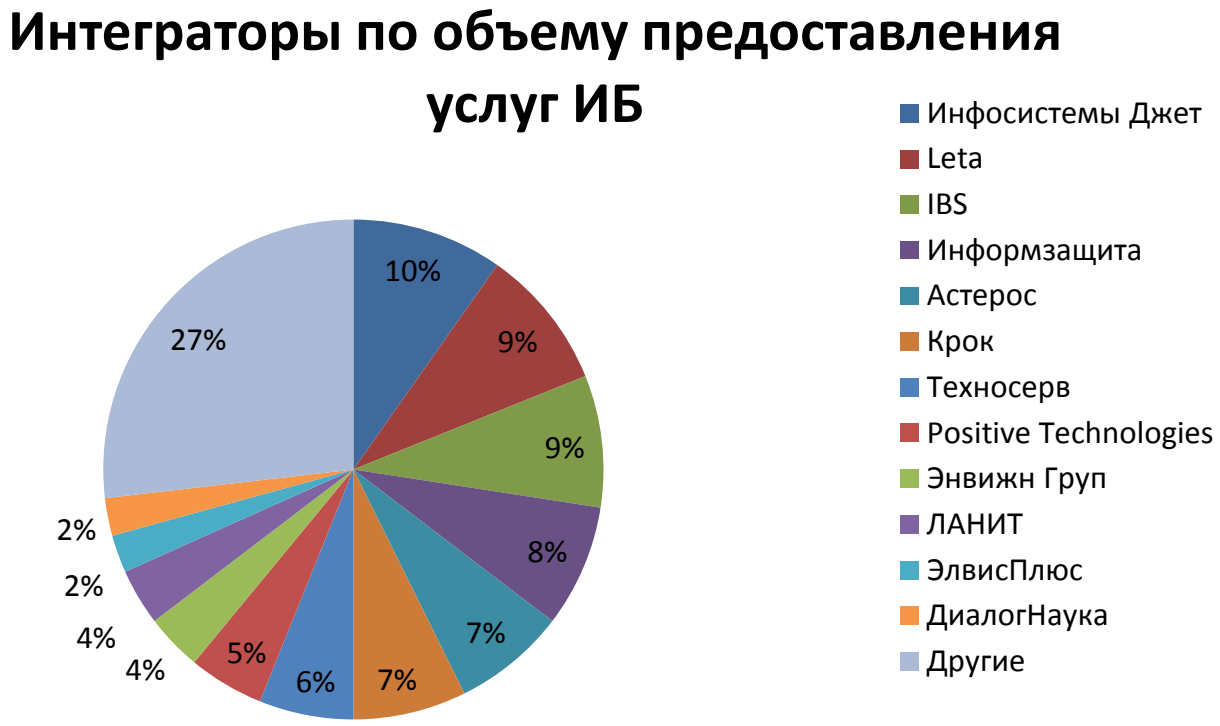
Подавляющее число крупных ИТ-интеграторов не выделяют бизнес ИБ в качестве приоритетного. Однако именно они обеспечивают самые высокие обороты по направлению ИБ.

По структуре выручки интеграторов можно разделить так:

- основа бизнеса – ИБ-услуги;
- основа бизнеса – ИБ-поставки оборудования и его ПНР.

	Приоритет ИБ		Основа бизнеса ИБ	
	Высокий	Низкий	Услуги	Поставки
1. Ай-Теко				
2. Астерос				
3. ДиалогНаука				
4. Информзащита				
5. Инфосистемы Джет				
6. Leta				
7. Крок				
8. Техносерв				
9. ЭлвисПлюс				
10. Энвижн Груп				
11. IBS				
12. ЛАНИТ				
13. Positive Technologies				
14. Digital Security				
15. АМТ				
16. РНТ				

Объем продаж услуг ИБ:

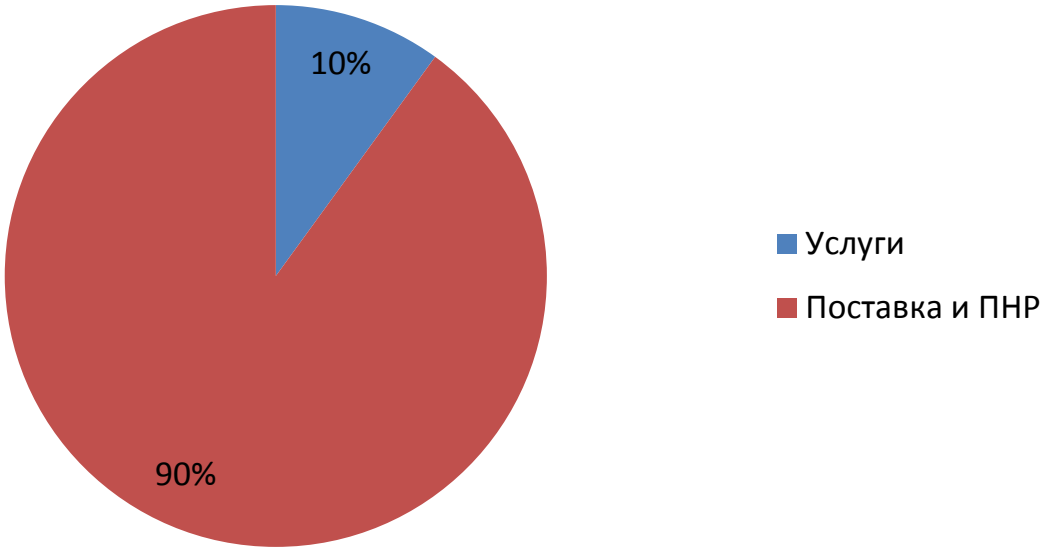


Объем продаж оборудования и ПО (включая ПНР):

Специфика российского рынка такова, что крупнейшие интеграторы обеспечивают высокие обороты за счет крупных поставок оборудования крупным корпоративным заказчикам и в государственный сектор. Именно такие заказчики обеспечивают 80% интеграторского рынка.

По структуре выручки интеграторов по направлению ИБ на услуги ИБ приходится около 10% всех приходящих денежных средств.

Структура выручки интеграторов по направлению ИБ



Необходимость ведения консалтингового направления бизнеса в первую очередь обусловлена поддерживающей функцией для поставок своих технических решений.

Также необходимо отметить, что на рынке действуют десятки компаний, которые специализируются исключительно на предоставлении услуг ИБ. При этом если взглянуть на рынок в целом, то их обороты будут незначительны.

Выводы:

- Основные обороты по направлению ИБ делают крупные ИТ-интеграторы.
- В общей выручке интеграторов по направлению ИБ услуги ИБ составляют около 10%, более 90% – поставки технических решений.
- Крупнейшими ИБ-интеграторами, имеющими сильные позиции, как по направлению поставок, так и по направлению услуг, являются «Информзащита» и «Инфосистемы Джет».

Евгений ЦАРЁВ

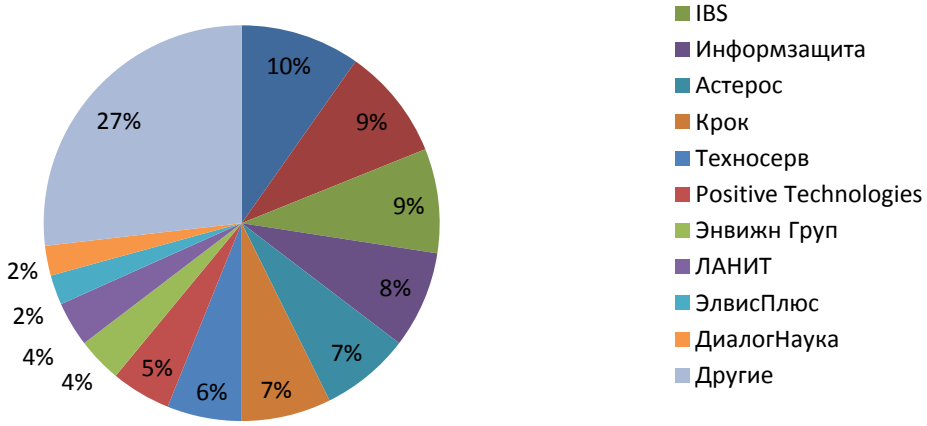
Традиционно под консалтингом на рынке ИБ понимаются услуги ИБ. Такое тождество не совсем корректно, однако терминология устоялась.

Основные направления консалтинга ИБ:

- защита персональных данных;
- защита коммерческой тайны;
- помощь в лицензировании (ФСТЭК и ФСБ);
- нормативное обеспечение в рамках технических внедрений (разработка документации);
- проектирование СОИБ;
- обследование на предмет обеспечения безопасности;
- аутстаффинг специалистов по ИБ;
- поддержание в актуальном состоянии СОИБ;
- обеспечение непрерывности бизнеса/деятельности;
- анализ рисков;
- СУИБ;
- СТО БР ИББС;
- PCI DSS
- НПС;
- расследование преступлений.

Основные игроки

Интеграторы по объему предоставления услуг ИБ



Нужно учитывать, что рынок консалтинга ИБ весьма неоднороден. Проекты по ИБ можно условно разделить на:

«рыночные»;

«высокомаржинальные».

К «рыночным» относятся те проекты, которые мы в основном и видим на рынке. Например, проект по обследованию по персональным данным с подготовкой отчета и организационно-распорядительной документации за 1,5 млн руб. в компании из 500 сотрудников. Стандартная маржинальность составляет около 40%.

К «высокомаржинальным» относятся проекты по поддержанию в актуальном состоянии

СОИБ в государственном ведомстве силами 5 консультантов интегратора за 33 млн руб. в год. Очевидно, что маржинальность такого проекта исчисляется сотнями процентов.

«Рыночные» проекты

Традиционно консалтинг ИБ воспринимался системными интеграторами как средство продажи технических решений. Фактически для большинства интеграторов продажа, например, услуги по обследованию информационных систем не имеет ценности сама по себе. Эту услугу зачастую продают по себестоимости, а иногда и в убыток, с целью дальнейшей продажи собственных технических решений. Фактически в рамках обследования готовится обоснование необходимости применения тех или иных технических мер.

При этом на рынке информационной безопасности регулярно появлялись компании, которые в качестве основной специализации выбирали консалтинг ИБ. Однако специфика консалтингового бизнеса такова, что без притока денежных средств с продажи технических решений велика вероятность возникновения кассовых разрывов. Как результат цены на услуги таких компаний должны быть значительно выше среднерыночных. Конкурировать с крупными компаниями, у которых цены на консалтинг ниже, весьма непросто.

Основываясь на производственных мощностях интеграторов в части консалтинга ИБ, совокупный объем рынка «рыночных» консалтинговых проектов оценивается в 39 млн долл. в год.

«Высокомаржинальные» проекты

«Традиционные» и крупные заказчики у крупных интеграторов зачастую покупают консалтинг с заложенной маржинальностью значительно выше 40%. Например, проект на 40 млн руб. с маржинальностью в 1000% – распространенная практика. Число таких «высокомаржинальных» проектов очень невелико (не более 70–100 в год). Основываясь на имеющейся информации о таких проектах за прошедший 2012 год, примерная оценка оборота интеграторов по таким проектам составляет около 43 млн долл. в год.

Итого совокупный объем рынка консалтинга оценивается в 82 млн долл. в год.

РЫНОК АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Илья МЕДВЕДОВСКИЙ

В рамках настоящего раздела не рассматриваются аудиты на соответствие требованиям по защите персональных данных. Также не рассматривается рынок аудита на соответствие ISO 27xxx, так как зарождающийся рынок умер в 2008 году и сейчас за год проходит всего несколько таких проектов.

Весь остальной рынок аудита можно условно разделить на 4 части:

- аудит защищенности (тесты на проникновение);
- PCI DSS;
- PA-DSS;
- СТО БР ИББС.

Итак, прежде всего, **в РФ (и в целом в СНГ) не существует и никогда не существовал рынок аудита ИБ как услуги, которая массово интересна заказчикам и подрядчикам**.

В последние 10 лет для 99% подрядчиков в РФ этап аудита защищенности ИС представляет собой не более чем первый промежуточный этап процесса выхода на интеграцию, на которой, собственно, до сих пор и зарабатываются основные деньги в СНГ. Впрочем, если раньше заказчики стремились выделять аудит в отдельный предварительный этап, то сейчас они сразу выбирают интегратора. Поэтому в отличие от Запада, где рынок аудита (как отдельной специализированной услуги) давно сформирован, активно развивается и ключевые позиции на нем занимают узкоспециализированные компании-консультанты, в РФ его практически нет. Исторически так сложилось, что интеграторы в свое время «каннибализировали» его и в итоге практически полностью уничтожили. Что же от него осталось? Только банковский сектор, да и то с большими оговорками. Плюс толком еще не сформированный рынок аудита бизнес-приложений и АСУ ТП.

На рынке аудита есть только два исключения – компании, не являющиеся интеграторами, которые специализируются на технических аспектах защищенности. Это Positive Technologies и Digital Security.

Компания Positive Technologies всегда являлась и сейчас является классическим горизонтальным вендором (продукт анализирует всевозможные компоненты любых ИС) и только в последнее время стала заниматься консалтинговыми услугами в этой области, в основном для пресейла или поддержки своего продукта. Обороты продаж продукта Positive Technologies и услуг по аудиту несопоставимы, однако этот факт скорее просто указывает на общий вектор, приоритетный для компании.

Компания Digital Security является консультантом, хотя также несколько лет назад создала дочернюю компанию ERPScan – вертикального вендора (разработчика специализированного продукта по анализу и мониторингу защищенности SAP).

Обе эти компании сейчас обращают внимание на зарождаю-

щийся сегмент аудита анализа защищенности АСУ ТП, развивая компетентность в этой области. Хотя, как показывает прошлый опыт, это не имеет большого практического смысла с точки зрения бизнеса, так как в итоге этот рынок полностью займут интеграторы и история с обычными аудитами ИС в точности повторится и для аудитов АСУ ТП. Однако разработки в области обеспечения безопасности АСУ ТП со стороны технически развитых российских компаний – тенденция положительная, так как итогом работы станут практические наработки по оценке реального уровня защищенности АСУ ТП.

Итак, **в РФ нет чистых компаний-аудиторов** («большую четверку» мы сразу выносим за скобки – они решают совершенно другие задачи). А те, кто близок к ним, – или вендоры, или «полувендоры». Потому что бизнес-перспектив для чистой компании-аудитора в РФ нет.

Все остальные игроки рынка – это все имеющиеся на рынке интеграторы.

1. АУДИТ ЗАЩИЩЕННОСТИ (ТЕСТЫ НА ПРОНИКНОВЕНИЕ)

Рынок тестов на проникновение (аудит защищенности) в последнее время развивается в основном за счет банковского сектора. Здесь востребованы следующие услуги:

- тесты на проникновение, обязательные для соответствия PCI DSS;
- аудит ДБО.

Тесты на проникновение, обязательные для соответствия PCI DSS, не представляют собой полномасштабную проверку систем. Рыночная цена такого теста невысока, в результате этот этап является сугубо формальным на пути к PCI compliance. Пентесты по PCI DSS в РФ обычно выполняют сами QSA-компании в общем комплексе услуг по PCI. Почти никто из них не является экспертом в этой области, поэтому качество такой услуги невелико. Но в любом случае наличие необходимости в такой услуге оказывает позитивное влияние на этот рынок.

Аудит ДБО. В настоящий момент сложилась тяжелейшая ситуация с уязвимостями в системах ДБО, которые одновременно являются желанной целью для злоумышленников и представляют жалкую картину с точки зрения безопасности. Банки постепенно начали осознавать необходимость квалифицированного аудитора (хакера), который будет регулярно проверять их системы ДБО. Банки стали понимать, что, находясь один на один со своим разработчиком ДБО, они не в состоянии решить проблемы безопасности. Хотя надо отметить, что российские системы ДБО ничем не хуже любых западных аналогов. Просто они на виду – на первой линии криминального огня.

Ситуация по результатам исследований и аудитов ДБО близка к катастрофической. Применяемые российскими банками системы ДБО чрезвычайно уязвимы.

Основные причины:

- нежелание и неумение разработчиков системно подходить к процессу безопасной разработки (это долго и дорого);
- нулевая ответственность разработчика перед банком за уязвимости;
- невозможность для банка самому найти уязвимости без приглашения эксперта;
- нежелание и неспособность разработчика вносить изменения во все кастомизированные сборки всех заказчиков

и т.п.

Весь этот рынок сохраняет статус-кво только за счет того, что злоумышленники пока стараются атаковать клиентов: это проще и практичнее. Но совсем скоро они узнают, что серверы ДБО представляют собой легкую и очень лакомую добычу, и рынок взорвется. Однако стоит еще раз повторить, что сами разработчики ДБО с точки зрения ИБ не лучше и не хуже своих западных коллег.

А что кроме банковского сектора? Практически ничего. Есть еще аудит бизнес-приложений, веб-приложений, АСУ ТП и т.д., но обороты здесь пока несущественны, а вход крайне сложен из-за необходимости иметь очень серьезную квалификацию. Оба этих фактора приводят к тому, что каждый работает или пытается работать со своими постоянными клиентами, но рынка при этом нет.

Да и в банковский сектор новым компаниям проникнуть со стороны практически невозможно: чужие здесь не ходят. И нет смысла проникать: по сравнению с общим годовым оборотом сумма, о которой идет речь на этом рынке, настолько неинтересна для мас-

сы наших интеграторов, что они не пытаются играть существенную роль на рынке аудитов ДБО. Ведь на интеграцию через эту услугу не выйдешь, а профессиональный опыт требуется очень серьезный.

Выводы

Основной драйвер рынка – страх перед злоумышленниками.

Основные игроки рынка – Digital Security и Positive Technologies.

2. АУДИТ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ PCI DSS

Рынок аудита PCI DSS крайне специфичен. Этот рынок имеет одну простую закономерность: кто первый пришел, тот и победил.

Все компании в СНГ, обладающие статусом PCI QSA и играющие сколь-либо существенную роль на этом рынке, являются интеграторами. Исключение одно – Digital Security. Аналогия с аудитами защищенности ИС здесь полная – банки (а именно они были и являются главными потребителями данной услуги) заинтересованы в проектах «под ключ», когда аудитор и интегратор – это одна компания. На Западе это не так, а в СНГ именно так.

Поэтому банковский сектор поделен между компанией «Информзащита», которая сильно опережает конкурентов, и компанией «Инфосистемы Джет», за ними (возможно, с небольшим отрывом) идут все остальные. Причем сам аудит на соответствие PCI DSS как услуга интеграторов не интересует. Им интересна именно интеграция.

Второй класс заказчиков по PCI DSS – это небольшие процессинги и платежные шлюзы. Они неинтересны интеграторам, так как таким заказчикам нужны только консалтинг и аудит, а на интеграции здесь ничего не заработаешь. Здесь лидируют Digital Security и «Информзащита». Остальные QSA-компании проигрывают с большим отрывом.

Итак, по общему числу проектов в год абсолютный лидер – «Информзащита», второе место ориентировочно делят «Инфосистемы Джет» и Digital Security, далее еще ряд старых QSA, а остальные новые QSA-компании (2011 года «изготовления») идут с большим отставанием.

Российские компании, которые получили статус в 2011 году (это был последний всплеск интереса к получению статуса QSA), за эти два года выполнили примерно 1–2 проекта и получили полностью убыточное направление бизнеса. Дело в том, что к концу 2010 года рынок был полностью сформирован, поделен, предельно конкурентен и начал впадать в фазу стагнации.

Этот рынок принадлежит компаниям, получившим статус в 2007–2008 годах, и перспектив для успешного выхода на него у новых игроков нет. Все банки давно поделены между интеграторами, первыми получившими статус, и новых банков на рынке не появляется. Новых небольших процессингов и платежных шлюзов, которые нуждаются в сертификации, сейчас крайне мало, и они или по недоразумению попадают к одному из многочисленных QSA-интеграторов (коих сейчас около 10), или к Digital Security, которая объективно наиболее привлекательна для этого класса заказчиков по целому ряду причин – начиная от того, что DSec не является интегратором, и заканчивая активной пропагандой PCI DSS (организованный в 2009 году и на сегодня единственный по теме PCI DSS в СНГ информационный портал PCIDSS.RU, опять же единственная на сегодня в СНГ ежегодная конференция PCI DSS Russia). Кстати, полное отсутствие какой-либо рекламы или пропаганды PCI DSS со стороны других QSA после 2010 года также подтверждает факт стагнации этого рынка – все основные события на нем отгремели как раз до 2010–2011 годов, когда раздел рынка был окончательно завершен. Например, «Информзащита» прекратила поддерживать свой портал по PCI DSS как раз в начале 2011 года.

Также важно отметить, что привязка заказчика к аудитору крайне сильна и случаи перехода к другому аудитору очень редки, поэтому новым игрокам закрепиться на этом рынке практически невозможно. Кроме того, сам рынок услуг по PCI DSS весьма невелик (если исключить из него интеграцию) и делится более чем на дюжину действующих в РФ QSA-аудиторов (включая ряд зару-

бежных компаний). Так что рынок для новых игроков закрыт.

Выводы

Основной драйвер рынка – требования Visa и MasterCard.

Основные игроки рынка (по числу проектов) – «Информзащита» (с традиционно большим отрывом), «Инфосистемы Джет», Digital Security.

3. АУДИТ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ PA-DSS

Говоря про «рынок» PA-DSS, надо сразу честно признать, что в РФ этого рынка нет и не предвидится. Дело в том, что нет жесткого контроля со стороны Международных платежных систем (Visa и MasterCard). Дедлайн прошел полгода назад, однако МПС не требуют от банков-эквайеров применения карательных мер к разработчикам, потому что крупные разработчики ПО для процессингов уже давно сертифицированы, а мелкие разработчики разнообразного софта, попадающего под PA-DSS, имеют массу возможностей уйти от сертификации, для них процедура крайне затратна, сложна и избыточна. Поэтому рынка нет – есть только единичные проекты.

Кроме того, не следует переоценивать значимость аудита на соответствие PA-DSS с точки зрения безопасности.

Вывод

Перспектив появления рынка в РФ нет.

4. АУДИТ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ СТО БР ИББС

Тема рынка аудита на соответствие требованиям СТО БР ИББС имеет очень давнюю историю, уходящую корнями в далекий 2004 год – год рождения СТО БР ИББС. С тех пор продолжаются постоянные попытки создать рынок в этой области. И при всем, безусловно, положительном влиянии, которое оказал стандарт на всю банковскую сферу РФ, за что перед его создателями нам всем надо снять шляпу, в том числе и за их поистине титанические усилия по продвижению этого стандарта в широкие банковские массы, создать именно рынок услуг в этой области никому так и не удалось за 8 лет с момента его появления.

Стандарт, который так и не стал обязательным, очень четко показал, что на добровольной основе в РФ крайне сложно сформировать какой-либо рынок аудита. Нет никакого сомнения, что аналогичная судьба ожидала бы в РФ и PCI DSS, который без давления МПС не нашел бы своего применения. Именно это случилось и с ISO 27001, который так и не стал популярным в РФ и рынок по которому так и не сформировался.

В случае же СТО БР ИББС ситуация несколько иная. Сам стандарт популярен и в итоге длительной работы ЦБ РФ и АБИСС добровольно принят многими банками в качестве внутреннего стандарта. Однако есть одно важное «но»: единицы банков пользуются услугами внешних аудиторов, аккредитованных АБИСС. Честно говоря, вообще плохо понятна позиция интеграторов, которые бегом бежали становиться аудиторами по этому стандарту. Он достаточно высокоуровневый (в отличие от того же PCI DSS), и выйти через него на столь интересную им интеграцию не такая и тривиальная задача. Общий вывод: пока рынка нет, и без жесткой позиции ЦБ РФ в отношении обязательных независимых аудитов вряд ли он появится. Тем более с учетом более чем 30 (!) организаций-аудиторов – членов АБИСС и несколько изменившегося в последнее время отношения ЦБ РФ к АБИСС. Возможно, что-то поменяется с учетом принятого закона об НПС, но это покажет лишь время (и ЦБ РФ). Ситуация также могла бы измениться из-за появления 382-П, однако и здесь недавно озвучена позиция регулятора: внешний независимый аудит не является обязательным.

Вывод

На текущий момент рынка нет.

Теперь давайте подведем итог «успехам» и «перспективам» рынка аудита ИБ в РФ.

Итого, что мы имеем? **Зачатки рынка аудита, оцениваемые в 1% от общего рынка ИБ**, из которых добрая треть, если не половина, относится к обязательному PCI DSS. Речь идет именно о рынке, а не о кулуарно получаемых контрактах на аудит ИБ по сво-

им аккаунтам, хотя и здесь, вероятнее всего, общая сумма в год немногим превысит упомянутые сотые доли процента. В связи с этим говорить о каком-то целенаправленном интересе серьезного бизнеса и зарождении рынка услуг в области аудита ИБ в РФ в ближайшее время не представляется возможным. По этой же причине в РФ нет и серьезных исследований в области ИБ, за исключением, например:

- Digital Security с 2007 года (ДБО, Oracle, SAP, АСУ ТП, мобильные приложения);
- Elcomsoft примерно с 1999 года (защита ПО и данных);
- «Лаборатория Касперского» и Eset (вирусная тематика);
- Positive Technologies с 2012 года (Web, АСУ ТП).

Выступлений российских специалистов на ведущих западных хакерских конференциях тоже почти нет (исключения – Digital Security, «Лаборатория Касперского», Eset, Elcomsoft и Positive Technologies): бизнесу это просто не нужно. Правда, наметился один позитивный сдвиг – получив за прошедшие два года опыт выступлений на ZeroNights и PHDays, российские независимые исследователи буквально ринулись выступать на западных конференциях – этой весной в Европе на HITB и BlackHat буквально яблоку будет негде упасть от российских белых шляп – хакеров-исследователей. Однако все это пока, к сожалению, никак не влияет на бизнес.

Должно смениться целое поколение руководителей ИБ, и, когда на смену придет новое поколение менеджеров, вышедших из технарей, воспитанных на ZeroNights и PHDays, ситуация, может быть, и начнет меняться в лучшую сторону. Тогда регулярный аудит защищенности станет, как и на Западе, нормой, а не ненужным промежуточным этапом перед интеграцией. Тогда на рынке появятся специализированные российские компании, основным бизнесом которых станет качественное предоставление услуг в этой области, а не продажа продуктов и в довесок, для пресейла продукта, услуг. Тогда же появятся исследования и выступления российских специалистов различных компаний на ведущих западных конференциях. Все это взаимосвязано. Но это будет еще очень не скоро…

В РФ на сегодняшний день не созданы условия для формирования специализированных консалтинговых компаний – технических аудиторов по ИБ. Слишком высокие требуются технические компетенции, и слишком мал рынок. Эти два фактора в совокупности не оставляют шансов для изменения ситуации в перспективе ближайших нескольких лет.

С другой стороны, дорогу осилит идущий. Компании – технологические лидеры на этом рынке обязаны его развивать, обязаны брать на себя инициативу и заниматься миссионерством. Развивать технические компетенции, вести глубокие исследования и презентовать их на Западе, создавать и развивать сложные технологические продукты и услуги и вести их на Запад, перенимать западный опыт и приносить все это в РФ. Предлагать своим заказчикам в РФ передовые разработки и услуги, популяризировать технические аспекты ИБ, проводить технические конференции и развивать техническое комьюнити профессионалов – это миссия лидеров, которые обязаны видеть будущее и тем самым двигать индустрию за собой.

РЫНОК УСЛУГ ПО СЕРТИФИКАЦИИ ПРОДУКЦИИ ПО ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дмитрий ЛЕВИЕВ

Сертификация продукции по требованиям информационной безопасности на основании сведений из открытой печати проводится в системах безопасности федеральных органов исполнительной власти:

- средства защиты информации ФСБ России;
- криптографические средства защиты информации ФСБ России;
- средства защиты информации ФСТЭК России;
- средства защиты информации МО РФ.

В силу ведомственных ограничений и наличия информации, относящейся к государственной тайне, сертификация в ФСБ России и МО РФ не имеет открытых источников.

Перечень сертифицированных средств защиты информации ФСТЭК России содержит информацию не только о сертифицированных решениях, но также о заявителе и компаниях, принимавших участие в процессе сертификации.

Порядок проведения сертификации приведен на рисунке 1.

Сроки сертификации прини-

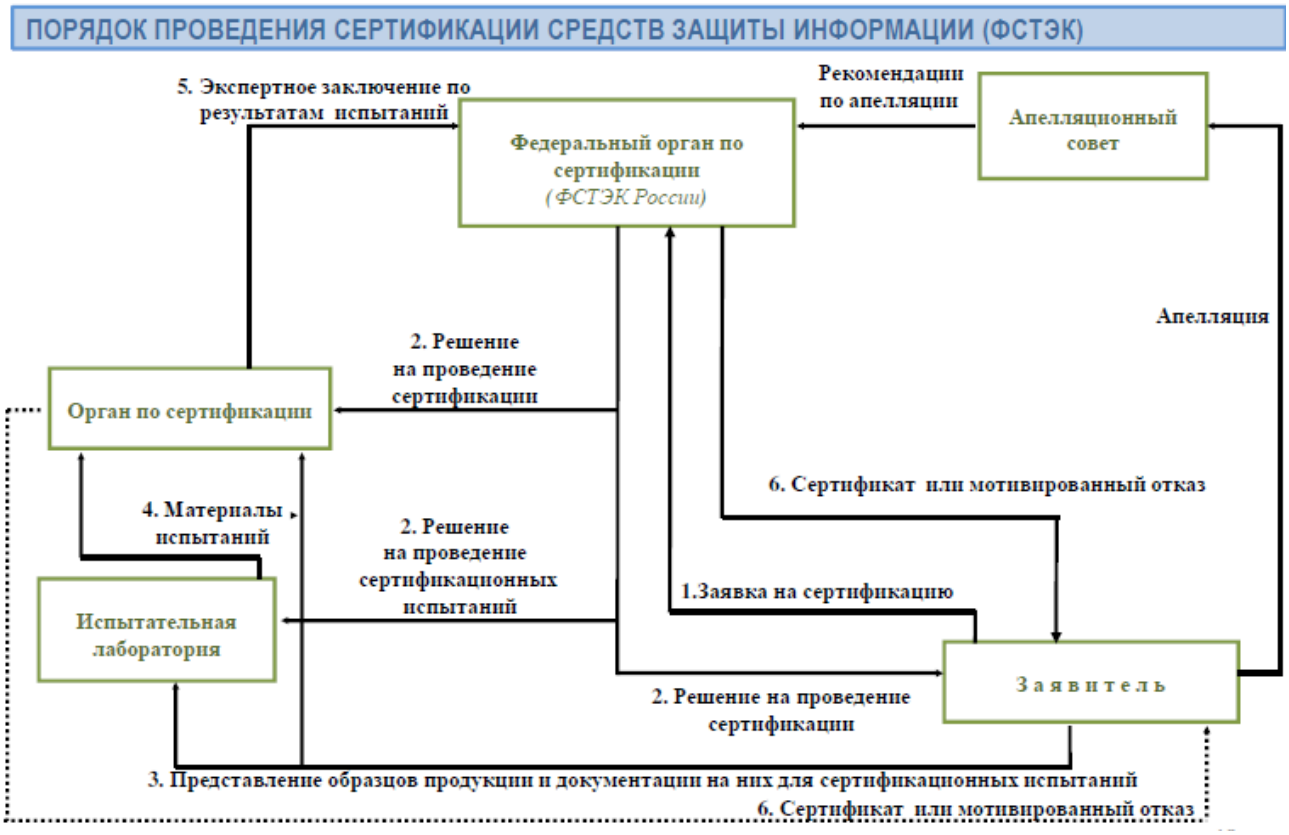


Рисунок 1. Порядок проведения сертификационных мероприятий

маются усредненно равными 6 месяцам на протяжении анализируемого периода.

Официальным источником публикации перечня сертифицированных средств защиты информации ФСТЭК России является официальный сайт ФСТЭК России в сети Интернет www.fstec.ru. Однако с января 2013 года при опубликовании списка сертифицированных средств опубликована версия файла от декабря 2009 года.

Остальные выводы базируются на анализе Перечня сертифицированных средств защиты информации ФСТЭК России, актуального на октябрь 2012 года, полученного из архива официального сайта www.fstec.ru системы резервного копирования значимой информации компании ООО «НПО «Спецремонт».

Методика анализа представляет собой оценку участия компаний в сертификационном процессе в следующих условиях:

Сертификация серий: испытательная лаборатория, орган по сертификации.

Сертификация партий, в том числе единичных образцов: испытательная лаборатория, орган по сертификации.

При выполнении всех работ одной компанией участие засчитывается как испытательной лаборатории, так и органу по сертификации.

При наличии нескольких компаний при сертификации соответствующие работы засчитываются каждой организации отдельно с весом 1.

Из расчета отдельно вынесены специальные сертификации в системе ФСТЭК России для атомной промышленности и железнодорожного транспорта и для расчета объема работ не принимают участия.

Анализ проводится:

- базовый год – год окончания сертификации 2005
- год сравнения – год окончания сертификации 2011
- год развития – год окончания сертификации – для 10 месяцев 2012 года

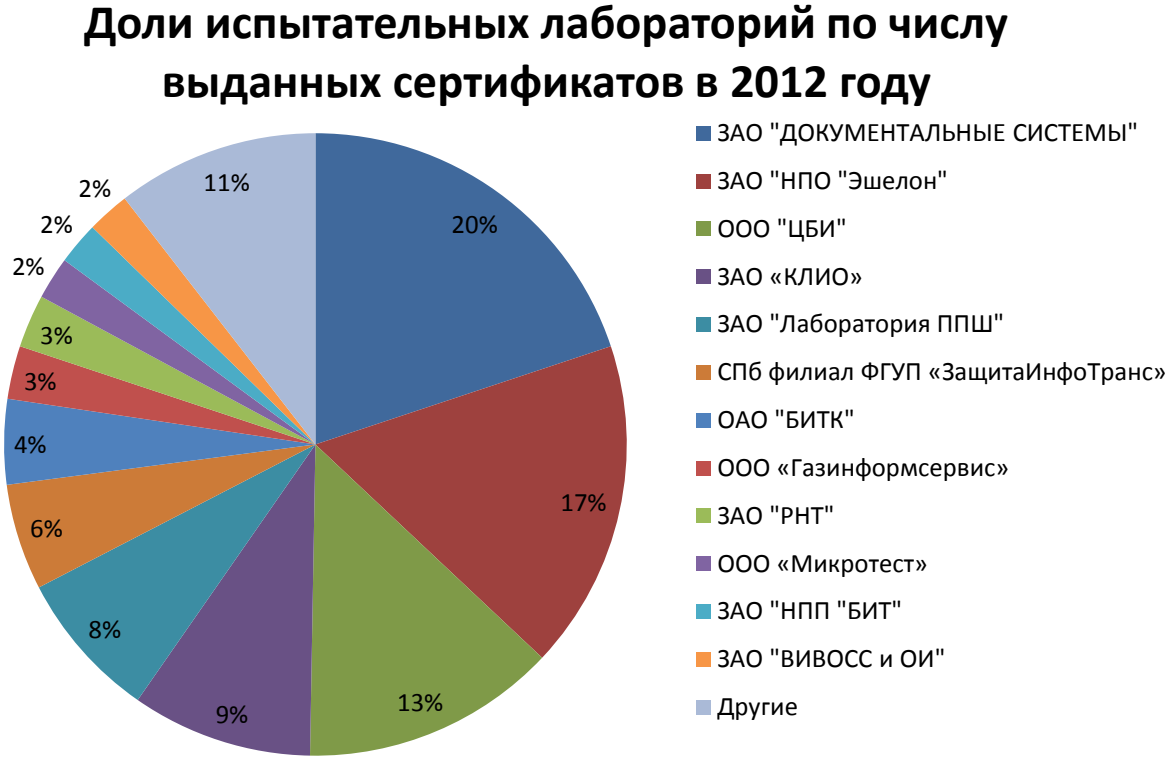


Рисунок 2. Распределение долей испытательных лабораторий в 2012 году*

* за 10 месяцев 2012 года.

В категорию «Другие» включены:
- ФГУП «ЗащитаИнфоТранс»
- ФГУП «Гостехстрой»
- СПб НТЦ ФГУП «НПП «Гамма»
- ООО «ГИЦ ПС ВТ»
- ОАО «Синклит»
- МОУ «ИИФ»
- ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
- ООО «НПО ВС»
- Пензенский филиал Научно-технического центра «Атлас»
- ЗАО «Королевская лаборатория информационных объектов»
- ЗАО «НПП «Гамма»
- ОАО «Информакустика»

Рисунок 3. Распределение долей органов сертификации в 2012 году**

** за 10 месяцев 2012 года.

Рисунок 4. Тренд общего объема сертификации

Совокупный объем рынка сертификации в системе ФСТЭК России оценивается в 250–300 млн руб. в год.

РЫНОК УСЛУГ ПО ОБУЧЕНИЮ ВОПРОСАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Игорь ХАЙРОВ

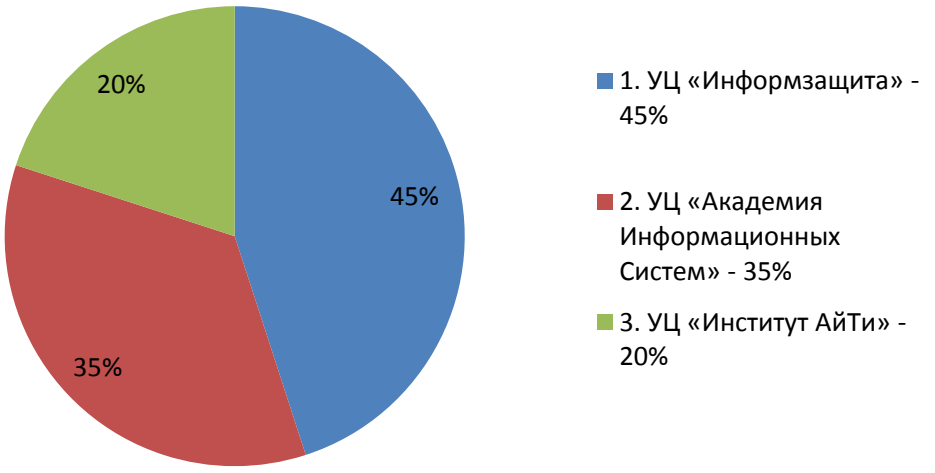
Настоящее экспресс-исследование затрагивает исключительно вопросы обучения по защите информации конфиденциального характера, но не касается тем, связанных с обучением по защите государственной тайны, т.к. это в России большой рынок, который заслуживает отдельного исследования.

На российском рынке работают десятки учебных центров, которые специализируются на подготовке специалистов в области защиты конфиденциальной информации (далее – информации). Лидерами этого рынка являются следующие три компании:

- АНО ДПО «Учебный центр «Информзащита» (*УЦ «Информзащита»*);
- НОУ ДПО ЦПК «АИС» (*УЦ «Академия информационных систем»*);
- НОУ ДПО «Институт «АйТи» (*УЦ «Институт АйТи»*).

В части курсов по защите информации среди этих трех компаний соотношение по оборотам денежных средств в 2012 году следующее:

Соотношение по оборотам денежных средств в 2012 году среди трех УЦ



Большинство остальных учебных центров либо перепродают курсы вышеприведенных компаний, либо имеют достаточно ограниченную линейку курсов по защите информации в своем собственном арсенале.

При этом нужно учитывать, что помимо указанных трех учебных центров, которые вместе составляют более 50% (среди учебных центров) всего рынка образовательных услуг по информационной безопасности,

действуют другие учебные центры, такие как:

- «Ланит»;
- «Микротест»;
- «Эшелон»;
- ЦБИ;
- «Маском»

и т.п.

Также большинство интеграторов включают в свои проекты обучение специалистов и самостоятельно его проводят. От интеграторов не отстают и вендоры, которые также зачастую самостоятельно проводят обучение по своим продуктам.

Распределение образовательных услуг между игроками рынка по типу компании:

Общий оборот по курсам ИБ в 2012 году можно оценить более чем в 700 млн руб.

Большую часть указанного оборота составляют курсы и тренинги по продуктам различных разработчиков и производителей средств и систем защиты информации. Также необходимо учитывать достаточно большой объем курсов, проводимых высшими учебными заведениями в рамках дополнительных занятий для студентов старших курсов.

В 2013 году ожидается незначительный рост объема образовательных услуг за счет дополнительного регулятивного воздействия со стороны государства на этот рынок.

Основные тренды (направления обучения) в 2012 году:

1. *Вопросы обработки и защиты персональных данных*. Данное направление обучения было лидером начиная с 2008 года и вплоть до конца 2011 года.

2. *Обеспечение безопасности информации с использованием шифровальных (криптографических) средств*. Данное направление, также как и защита персональных данных, пользуется большим спросом в последние 4 года. Это связано в первую очередь с ужесточением требований к компаниям, оказывающим услуги по криптографической (с помощью шифровальных средств) защите информации, и их персоналу, а также с требованиями к персоналу компаний, которые используют шифровальные средства для собственных нужд.

3. *Обеспечение информационной безопасности в кредитно-финансовых учреждениях (включая требования отраслевого стандарта по безопасности банковской системы РФ СТО БР ИББС-1.0 и обеспечение безопасности при дистанционном банковском обслуживании)*. Сильным драйвером обучения по данному направлению в последние несколько лет стал Банк России и так называемое письмо шестерых.

4. *Повышение осведомленности в области информационной безопасности*. Данное обучение имеет стабильный большой интерес среди компаний, т.к. позволяет значительно снизить количество случайных инцидентов безопасности.

5. *Обеспечение безопасности и непрерывности бизнеса по требованиям международных стандартов ISO27001 и ISO22301*. Данное обучение в России было одним из лидеров в 2006–2007 годах, а также в 2010–2011 годах. Финансовый кризис 2008 года свел обучение по данному направлению практически к нулю.

6. *Вендорские курсы* всегда пользовались и будут пользоваться большим спросом и стабильным интересом.

Еще раз отметим, что в 2012 году значительно вырос спрос на курсы повышения квалификации (свыше 100 часов) и на курсы профессиональной переподготовки (свыше 500 часов) по обеспечению безопасности с использованием шифровальных (криптографических) средств. Это обусловлено в первую очередь усилением требований со стороны исполнительных органов государственной власти к защите информации ограниченного доступа.

Прогнозируемые основные тренды (направления обучения) в 2013 году:

1. *Защита мобильных систем, платформ и приложений*.

2. *Обеспечение безопасности при переводе денежных средств в рамках Национальной платежной системы*.

3. *Обеспечение безопасности облачных вычислений и приложений*.

4. *Расследование инцидентов и случаев мошенничества в глобальных сетях*.

5. *Обеспечение экономической безопасности и защита коммерческой тайны*.

6. *Безопасность АСУ ТП*.

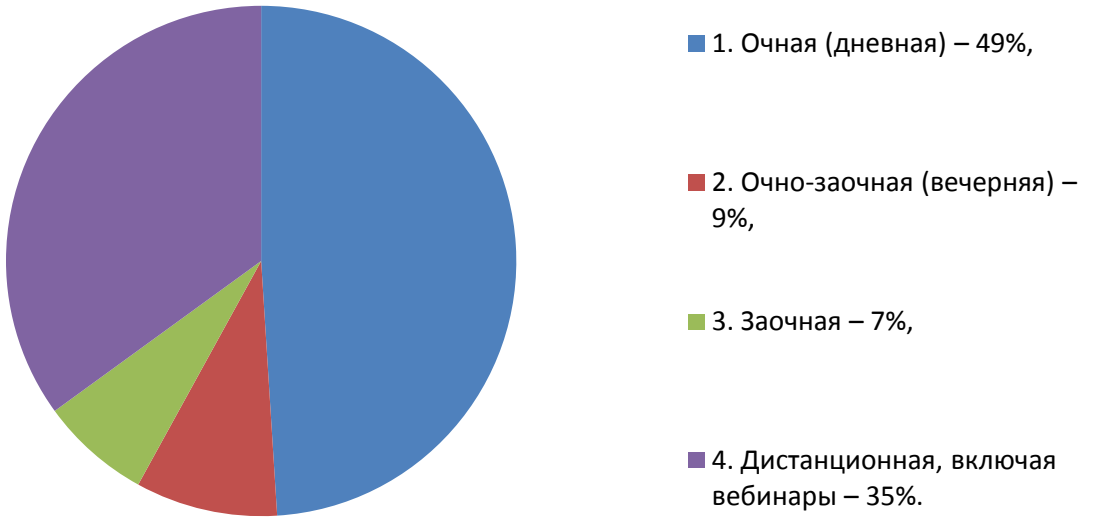
7. *Комплексные программы повышения квалификации и профессиональной переподготовки руководителей компаний и подразделений по защите информации по MBA в области информационной безопасности*.

В 2013 году ожидается всплеск интереса российских специалистов к международным сертификациям, таким как CISSP, CISM, CGATE и CRISC.

Что касается форм обучения, то подавляющее большинство слушателей предпочитают проходить обучение в очном формате. Здесь нет ничего удивительного, т.к. очное обучение позволяет прививать практические навыки и является наиболее эффективным.

Однако использование дистанционных технологий, включая вебинары и видеоконференции, позволяет проходить обучение без отрыва от производства и вне зависимости от географического расположения лектора/тренера и обучающихся.

Формы обучения



Начиная с 2013 года соотношение между очным и дистанционным обучением будет меняться в пользу последнего. Также будут развиваться интерактивные формы обучения в виде двусторонних телеконференций.

Основной вывод

Несмотря на экономическую ситуацию в стране и в мире, спрос на квалифицированные кадры будет расти, а значит, обучение в области защиты информации будет пользоваться возрастающим спросом. Во все времена информация была, есть и будет одним из важнейших активов любой компании (как коммерческой, так и государственной), а ее нужно правильно защищать!

МЕРОПРИЯТИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Игорь ЕЛИСЕЕВ

На российском рынке ИБ сложилась довольно устойчивая группа мероприятий, проводимых ежегодно на регулярной основе. Если не рассматривать выставки и конференции регионального уровня, то можно насчитать почти два десятка отраслевых форумов общефедерального значения, собирающих представителей из Москвы и различных регионов страны. Примерно 70% от общего числа отраслевых мероприятий по ИБ постоянно дислоцируется в Москве. Но также в списке мест проведения фигурируют Сочи, Казань, Йошкар-Ола и Санкт-Петербург.

Совокупный объем рынка мероприятий по ИБ в России оценивается в 10 млн долл.

В годовом цикле отраслевых мероприятий явно прослеживаются два сезонных «пика активности» – весенний (с февраля по май) и осенний (сентябрь-ноябрь). Сводная таблица регулярных конференций и выставок, посвященных тематике ИБ, приведена ниже:

Название	Время	Место	Организаторы	Сайт
«Инфофорум»	Февраль	Москва	НП «Инфофорум»	infoforum.ru
«Информационная безопасность банков»	Февраль	Магнитогорск	«Авангард-Центр»	Ib-bank.ru
«Технологии безопасности»	Февраль	Москва	«Гротек»	Tbforum.ru
IDC IT Security Roadshow	Март	Москва	IDC	idc-cema.com
Russian CSO Summit	Весна	Москва	«Форт-Росс»	cso-summit.ru
«РусКрипто»	Март	Подмосковье	Академия информационных систем, ассоциация «РусКрипто»	ruscrypto.ru
Форум директоров по ИБ	Апрель	Москва	Infor-media	infosecurity-forum.ru
PH Days	Май	Москва	Positive Technologies	phdays.ru
IT & Security Forum	Май-июнь	Казань	ICL КПО, НПО «Вычислительные системы»	itsecurityforum.ru
«Информационная безопасность. Региональные аспекты. ИнфоБЕРЕГ»	Сентябрь	Сочи	Академия информационных систем	Vipforum.ru
DLP Russia	Сентябрь	Москва	Ассоциация DLP Expert	dlp-expert.ru
PKI-Forum	Осень	Санкт-Петербург	«Авангард-Центр»	pki-forum.ru
Infosecurity Russia	Сентябрь-октябрь	Москва	«Гротек»	infosecurityrussia.ru
InfoBez	Сентябрь-октябрь	Москва	«Рестэк»	infobez-expo.ru
Охрана и безопасность IS.CS	Ноябрь	Санкт-Петербург	«Примэкспо»	sfitex.primexpo.ru

Название	Время	Место	Организаторы	Сайт
«Электронная Россия: торги, документооборот, электронная подпись»	Ноябрь	Йошкар-Ола	«Цифровые технологии»	trusted.ru
ZeroNights	Ноябрь	Москва	Digital Security	zeronights.ru
Antifraud Russia	Ноябрь-декабрь	Москва	Академия информационных систем, ТПП РФ	antifraudrussia.ru

Все регулярные мероприятия по ИБ, проводимые в России, можно разделить на несколько условных категорий в зависимости от их направленности:

Отраслевые выставки-конференции, охватывающие все аспекты развития информационной безопасности и все продуктовые категории. Это прежде всего две осенние выставки Infosecurity Russia и InfoBez, которые проводятся друг за другом с разрывом менее чем в один месяц. К сожалению, такая лобовая изматывающая конкуренция не идет на пользу ни одному мероприятию – их тематика и аудитория очень схожи, поэтому посетителям и участникам приходится выбирать в пользу одной из выставок. Деловая программа довольно размазана по направлениям, что еще больше усложняет выбор слушателя, на какую секцию и в какой день стоит приходить.

Если судить по текущему году, как выставка, возможно, несколько впереди Infosecurity, а конференционная часть интереснее у InfoBez. Но в целом ни одно из мероприятий не растет ни качественно, ни количественно, как бы организаторы ни заверяли в обратном.

Также к этой категории относится февральский форум «Технологии безопасности» и осенняя выставка в Санкт-Петербурге «Информация: техника и технологии защиты», которая проводится в рамках более крупного международного форума «Охрана и безопасность – SFITEX». А февральский форум «Технологии безопасности» в отличие от осенних выставок в Москве охватывает всю тематику комплексной безопасности объектов и инфраструктуры (видеонаблюдение, контроль доступа, пожарная безопасность, транспортная безопасность и т.д.), уделяя собственно вопросам ИБ не более 10–15% экспозиции и продолжительности выступлений докладчиков.

Название	Плюсы	Минусы
«Технологии безопасности»	Обсуждение широкого спектра вопросов, связанных с обеспечением безопасности	Размазанность программы; отсутствие фокуса на проблемах ИБ; разношерстная аудитория
Infosecurity Russia	Выставка и конференция на одной площадке; весь спектр вопросов, связанных с ИБ	Прямая конкуренция с InfoBez примерно в одно и то же время; нет собственной изюминки; слабо структурированная деловая программа; выставочная часть имеет тенденцию к сокращению
InfoBez	Выставка и конференция на одной площадке; весь спектр вопросов, связанных с ИБ	Прямая конкуренция с Infosec примерно в одно и то же время; нет собственной изюминки; слабо структурированная деловая программа; выставочная часть имеет тенденцию к сокращению
IS.CS	Обсуждение широкого спектра вопросов, связанных с обеспечением безопасности; удобно для представителей СЗФО	Обо всем понемногу; нет фокуса на проблематике ИБ

Конференции с упором на вопросы государственной кибербезопасности. В первую очередь это ежегодные конференции «Инфофорум» (проводится в феврале) и «Инфофорум – Евразия» (июнь). Отличаются широким присутствием государственных органов власти,

очень незначительным влиянием бизнес-сообщества на формат и программу мероприятия, которое по сути больше напоминает отчетно-выборное собрание времен СССР, чем полноценный диалог заинтересованных участников рынка.

Название	Плюсы	Минусы
«Инфофорум»	Широкое участие ФОИВов; большая аудитория >500 человек	Схожесть с отчетно-выборным собранием; отсутствие реального диалога бизнеса и власти; малое влияние бизнес-сообщества на программу мероприятия

Научно-технические конференции по ИБ, ориентированные на узкопрофильных специалистов, разработчиков технологий, научных сотрудников и студентов технических вузов. Это мартовская конференция «РусКрипто», проводимая в Подмосковье, майский форум PH Days и ноябрьский ZeroNights. Основной упор в этих мероприятиях – на технические средства защиты информации, включая криптографию, анализ уязвимостей, новые сетевые угрозы, защиту от взлома, тесты на проникновение и т.п. Довольно большой процент вузовской молодежи среди слушателей. Самое научно-ориентированное среди перечисленных мероприятий – конференция «РусКрипто». Доклады ее участников публикуются в журнале, рекомендованном Высшей аттестационной комиссией (ВАК). Также проводится конкурс докладов среди студентов и аспирантов, победители которого получают возможность выступить перед аудиторией конференции наравне с профессионалами рынка ИБ. Поскольку мероприятие проводится несколько дней в ближнем Подмосковье, его участники имеют уникальную возможность сочетать работу на конференции «без отрыва от основного производства», неформальное общение с партнерами и коллегами и отдых.

Форум PH Days – самый амбициозный российский проект, имеющий целью консолидировать вокруг себя движение этичных хакеров и, разумеется, продвинуть на рынок компетенции и услуги организатора форума – компании Positive Technologies. Как PH Days, так и ZeroNights отличаются неформальной средой, фокусированием внимания на молодых специалистов, перспективные разработки и приглашением к участию большого количества зарубежных экспертов-докладчиков. Пожалуй, единственный минус обеих конференций – слабое внимание к ним со стороны отраслевых регуляторов ИБ, которые сильнее определяют направление движения отечественного рынка, чем глобальные тренды.

Название	Плюсы	Минусы
РусКрипто	Научно-практическая направленность; широкое участие молодых специалистов и разработчиков; публикации работ в журнале ВАК; совмещение деловой программы с неформальным общением и активным отдыхом	Небольшой процент участников от бизнеса
PH Days	Крупнейшее мероприятие для технических специалистов по ИБ; стильный и современный дизайн; много зарубежных экспертов; разнообразная мультиформатная программа	Ориентация на интересы компании-организатора
ZeroNights	Много зарубежных экспертов; разнообразная программа; широкое участие молодых специалистов	Уступает по масштабу PH Days; небольшой процент бизнес-участников

Специализированные конференции, нацеленные на углубленное обсуждение по конкретным направлениям ИБ: информационная безопасность банков, удостоверяющие центры, защита электронной торговли или борьба с компьютерным мошенничеством. Например, февральский форум «Информационная безопасность банков» в Магнитогорске или международная конференция Antifraud Russia (Москва, конец ноября), PKI-Forum (осень,

Санкт-Петербург) или ноябрьская конференция «Электронная Россия: торги, документооборот, электронная подпись», которая проводится в Йошкар-Оле. В общем, названия мероприятий говорят сами за себя. Их участники получают, как правило, глубокую и исчерпывающую информацию по той тематике, которой они посвящены. Из года в год собирают довольно устойчивую аудиторию, в составе которой поначалу преобладают заказчики, но со временем становится все больше интеграторов и поставщиков услуг ИБ. Но в любом случае альтернативы такого рода конференциям для руководителей и специалистов, интересующихся данными конкретными проблемами, нет.

Название	Плюсы	Минусы
«Информационная безопасность банков»	Крупнейшее мероприятие по ИБ в банковском секторе; широкий состав профессиональных участников (более 300); активное участие бизнеса и регуляторов	Высокие цены на участие; необходимость отрыва от основного производства почти на неделю; тенденция к перекосу в пользу интеграторов и поставщиков решений
PKI-Forum	Крупнейшее мероприятие для представителей УЦ и поставщиков решений	Относительно узкая тематика; первую скрипку среди регуляторов играет почему-то не ФСБ, а Роскомнадзор
«Электронная Россия: торги, документооборот, электронная подпись»	Полезное и удобное мероприятие для представителей Центрального и Приволжского ФО; интересная деловая программа; поддержка регуляторов	Относительно небольшая аудитория участников (менее 200); не совсем удобное место проведения
Antifraud Russia	Крупнейшее мероприятие по борьбе с компьютерным мошенничеством в СНГ; международный формат; широкое участие регуляторов и правоохранительных органов	Очень плотная программа с параллельными секциями; тесная площадка, с трудом вмещающая всех участников

Общеотраслевые конференции, рассчитанные на обсуждение широкого круга вопросов, связанных с ИБ (от регуляторных до технических), и адресованные представителям всех игроков рынка – заказчикам, разработчикам, ИТ-интеграторам, консультантам, исследовательским лабораториям. Сюда можно отнести IDC IT Security Roadshow, Russian CSO Summit (оба мероприятия проводятся в Москве), казанский IT & Security Forum и всероссийскую конференцию «Информационная безопасность. Региональные аспекты. ИнфоБЕРЕГ» в Сочи. В эту же категорию окончательно перешла конференция DLP Russia, раньше позиционирующая себя как мероприятие, посвященное технологиям защиты от утечек конфиденциальной информации.

Самое слабое звено в данной группе – IDC IT Security Roadshow, это попытка пробежаться «галопом по Европам», тогда как участники ждут более глубокого обсуждения проблем, связанных с регулированием отрасли, вопросами лицензирования, сертификации и соответствия требованиям государственных органов. Саммит директоров по ИБ Russian CSO Summit изначально был хорошей идеей собирать на одной площадке лиц, принимающих решения, и рассказывать им о том, как решение проблем ИБ влияет на бизнес предприятий. Но в итоге идея выродилась в крайне коммерциализированное мероприятие, где продается все, вплоть до базы данных участников. Соответственно, содержательное наполнение программы с каждым годом все больше оставляет желать лучшего. По инерции ИБ-руководители и многочисленные спонсоры пока не оставляют Russian CSO Summit совсем за скобками своего графика.

IT & Security Forum, напротив, стабильно набирает вес. Организаторы смогли придать мероприятию формат крупного действа, соответствующего международным стандартам проведения отраслевых конференций, вместе с тем не выплеснув за борт российскую специфику рынка. Одним словом, при невысокой плотности отраслевых мероприятий в конце весны – начале лета IT & Security Forum – то событие, которое стоит посетить.

Сочинская конференция «Информационная безопасность. Региональные аспекты. ИнфоБЕРЕГ» традиционно более 10 лет открывает новый деловой сезон и представляет собой уни-

кальную возможность погрузиться в проблематику развития отрасли после сезона отпусков. А для некоторых участников «ИнфоБЕРЕГ» – это еще и возможность продлить летний отпуск, совместив отдых на море с деловой программой и бизнес-общением. Конференцию отличает достаточно стабильный состав участников, присутствие основных регуляторов и многочисленное участие лицензиатов ФСБ России и ФСТЭК России.

Название	Плюсы	Минусы
IDC IT Security Roadshow	Участие экспертов-аналитиков рынка; компактная деловая программа	Оторванность от российских реалий рынка ИБ; отсутствие регуляторов; относительно небольшая и разношерстная аудитория слушателей
Russian CSO Summit	Большой состав участников (более 400); обсуждение вопросов взаимодействия бизнеса и служб ИБ	Сильная коммерциализация; продается все, в т.ч. базы данных участников; качество организации и программы с каждым годом хуже
IT & Security Forum	Очень крупное и солидное мероприятие; все аспекты развития ИБ; большой состав участников и регуляторов	Пока не замечено
DLP Russia	Большой состав участников; интересные эксперты; удобное место проведения	Ориентация на бизнес-интересы компании-организатора; пока слишком узкая программа, чтобы быть общеотраслевой конференцией по ИБ
«ИнфоБЕРЕГ»	Активное участие представителей бизнеса и регуляторов; разнообразная деловая и культурная программа; широкие возможности для неформального общения и активного отдыха	Необходимость отрыва от производства на 4–5 дней; небольшой процент бизнес-заказчиков

Следует отметить, что каждый год появляются и другие мероприятия, так или иначе связанные с тематикой информационной безопасности. Но они либо не набирают достаточного веса на рынке и после одной-двух не очень удачных попыток проведения исчезают, либо представляют собой частную инициативу каких-то участников рынка и не претендуют на то, чтобы стать регулярным ежегодным центром притяжения отраслевой аудитории.

ИНТЕГРАЛЬНАЯ ОЦЕНКА РЫНКА ИБ

Евгений ЦАРЁВ

При подготовке настоящего исследования не удалось получить раздел по рынку средств контроля утечек (DLP).

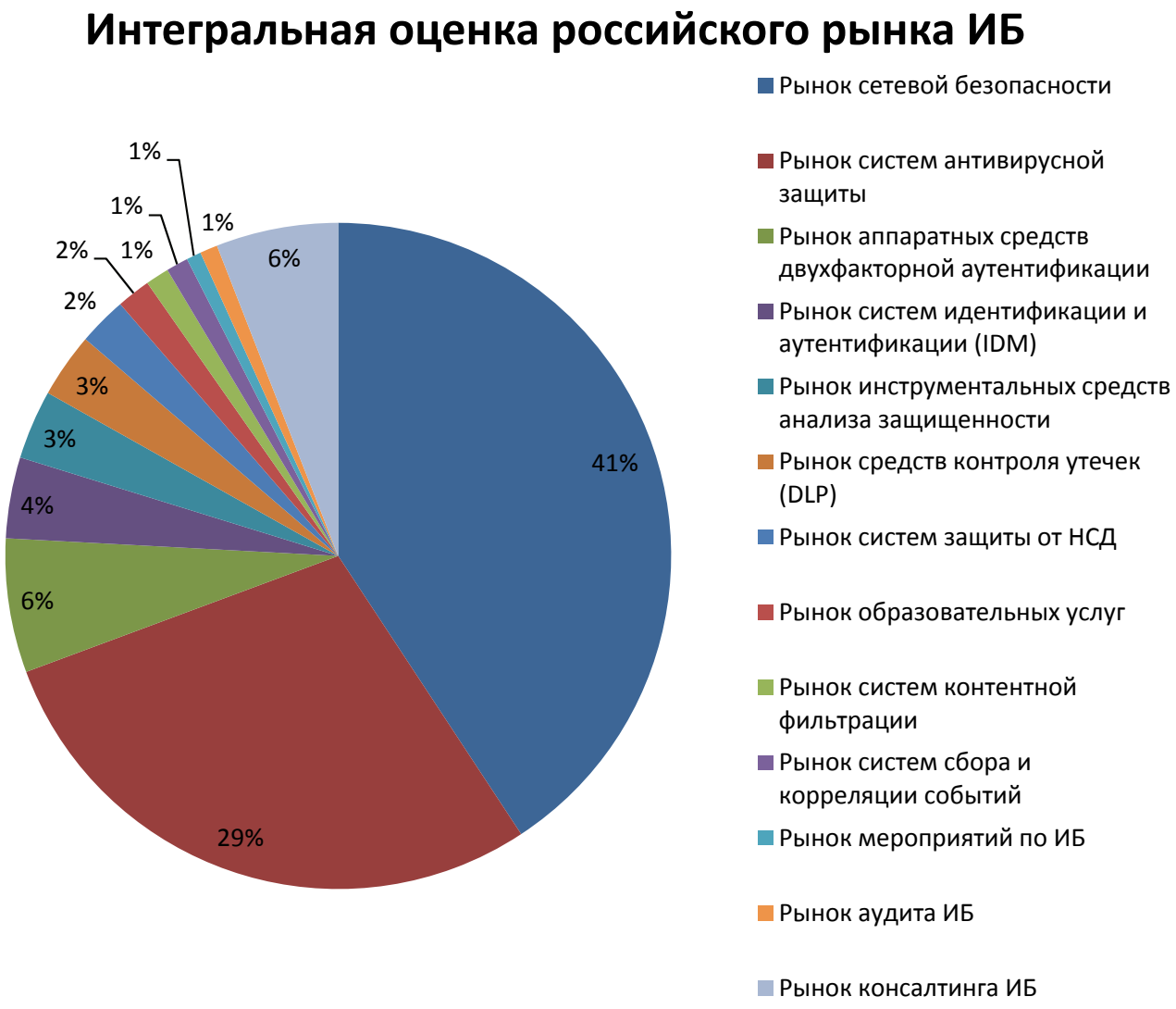
Однако для подготовки раздела с интегрированной оценкой рынка ИБ был проведен анализ открытых данных из доступных источников по основным игрокам этого рынка, их оборотам и составу выручки. Также был проведен опрос экспертов, которые помогли оценить объем по данному сегменту. В результате рынок средств контроля утечек (DLP) был предварительно оценен в 44 млн долл. в год. Однако необходимо подчеркнуть, что данная цифра является оценочной и не является результатом проведения полноценного исследования.

Основываясь на информации, полученной из предыдущих разделов, получаем следующие оценки объема рынка ИБ:

Сегмент рынка ИБ	Оборот, млн долл.*
Рынок сетевой безопасности	570
Рынок систем антивирусной защиты	400
Рынок аппаратных средств двухфакторной аутентификации	91
Рынок систем идентификации и аутентификации (IDM)	55
Рынок инструментальных средств анализа защищенности	47
Рынок средств контроля утечек (DLP)	44
Рынок систем защиты от НСД	33
Рынок образовательных услуг	23
Рынок систем контентной фильтрации	16
Рынок систем сбора и корреляции событий	15
Рынок мероприятий по ИБ	10
Рынок аудита ИБ	12
Рынок консалтинга ИБ	83
Итого	**1399**

* – для конвертации принималось 1 долл. США = 30 руб.

Графическое представление:



Итоговый объем рынка ИБ оценивается в 1 399 млн долл.

BONUS. РЫНОК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УКРАИНЫ (ОБЗОР)

Екатерина ЛЯШЕНКО

До принятия Закона Украины «О защите персональных данных» вопросами информационной безопасности в глобальном смысле этого термина были озадачены две категории организаций: государственные учреждения и банки.

У большинства других предприятий информационная безопасность ассоциировалась в большей степени со средствами охранной и пожарной сигнализации, а также видеонаблюдения.

На сегодняшний день, особенно после принятия Закона Украины «О защите персональных данных», ***основными специалистами в области защиты информации*** в силу возложенных на них функциональных обязанностей ***стали представители кадровых служб*** предприятий. Именно они отвечают за выполнение требований законодательства относительно вопросов защиты персональных данных.

Предприятия, существующие на рынке Украины, можно поделить на три категории:

1. Small. Предприятия, численность персонала которых составляет не более 15 человек, отсутствует информационно-телекоммуникационная система (ИТС), информация обрабатывается как в электронном, так и в бумажном виде.
2. Middle. Предприятия, численность персонала которых составляет от 15 до 100 человек, данные обрабатываются в пределах одной информационно-телекоммуникационной системы.
3. Large. Предприятия, численность персонала которых составляет более 100 человек, данные обрабатываются в нескольких информационно-телекоммуникационных системах и в силу особенностей бизнес-процессов могут передаваться из одной системы в другую.

Так как речь идет о коммерческих организациях, то в этом случае существует всего один вопрос: ***как законодательство Украины регулирует вопрос защиты информации в информационно-телекоммуникационных системах?***

Согласно Закону Украины «Об информации» выделяется два *вида информации*: *открытая и информация с ограниченным доступом*. Информация с ограниченным доступом, в свою очередь, делится на:

- конфиденциальную,
- служебную,
- составляющую государственную тайну.

В законе делается особый акцент на понятии конфиденциальной информации в отношении данных о физическом лице. Так, например, пункт 2 статьи 21 этого же закона говорит о том, что конфиденциальной является информация о физическом лице, а в статье 11 дается более четкое определение, какие именно данные о физическом лице являются конфиденциальными:

«К конфиденциальной информации о физическом лице относятся, в частности, данные о национальности, об образовании, о семейном положении, религиозных убеждениях, состоянии здоровья, а также адрес, дата и место рождения».

Также имеет смысл обратить особое внимание на такой документ, как «Правила обеспечения защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах», утвержденные постановлением Кабинета министров Украины от 29.03.2006 № 373 (далее – Правила). Можно сказать, что данный документ известен достаточно узкому кругу специалистов, занимающихся непосредственно вопросами технической защиты информации, построением комплексных систем защиты на предприятии. Однако Правила дают четкий ответ на вопросы относительно того, какая же информация, по мнению государства, подлежит защите и что подразумевается под словом «защита». Так, например, в пункте 4 этого документа говорится следующее:

Защите подлежит:

1. ***Открытая информация***, которая является собственностью государства и в определении Закона Украины «Об информации» принадлежит к статистической, правовой, социологической информации, информации справочно-энциклопедического характера и используется для обеспечения деятельности государственных органов или органов местного самоуправления, а также информация о деятельности указанных органов, если она публикуется в Интернете, других глобальных информационных сетях и системах или передается телекоммуникационными сетями (далее – открытая информация);

2. ***Конфиденциальная информация***, которая является собственностью государства или требование относительно защиты которой установлено законом, в том числе конфиденциальная информация о физическом лице (далее – конфиденциальная информация);

3. Информация, составляющая государственную или другую предусмотренную законом тайну (далее – ***секретная информация***).

Далее в этом же документе идет речь о том, что для обеспечения защиты информации в системе должна создаваться комплексная система защиты информации, которая предназначается для защиты информации от утечки по техническим каналам, от несанкционированных действий с информацией, в том числе с использованием компьютерных вирусов, от специального воздействия на средства обработки информации. Данная часть документа перекликается со статьей 8 Закона Украины «О защите информации в информационно-телекоммуникационных системах», в которой говорится о том, что информация, которая является собственностью государства, или информация с ограниченным доступом (конфиденциальная), требование относительно защиты которой установлено законом, должна обрабатываться в системе с применением комплексной системы защиты информации, подтвержденной соответствием. Подтверждение соответствия осуществляется по результатам государственной экспертизы в порядке, установленном законодательством.

Комплексная система защиты информации (КСЗИ) представляет собой взаимосвязанную совокупность организационных и инженерно-технических мероприятий, средств и методов защиты информации.

Для создания комплексной системы защиты информации используются средства защиты информации, которые имеют сертификат соответствия или положительное экспертное заключение по результатам государственной экспертизы в сфере технической и/или криптографической защиты информации.

Рассмотрим основных сертифицированных игроков на рынке информационной безопасности.

Согласно данным, представленным на официальном сайте Государственной службы связи и защиты информации Украины, лидирующие позиции занимает компания *Cisco Systems* (США), имеющая на рынке Украины более 70 сертифицированных продуктов. Стоит также отметить, что на украинском рынке IT компания Cisco имеет порядка 340 партнеров.

На втором месте находится французская компания *Alcatel-Lucent*, сертифицировавшая около 40 единиц продуктов.

Третье место по количесту продуктов (22–27), соответствующих требованиям нормативних документов Украины в области технической защиты информации, делят *Quintum Technologies* (США), *Hewlett-Packard* (США) и *Hangzhou H3C Technologies* (Китай).

Далее следует компания-представитель Китайской Народной Республики *Huawei* с 11 еди-

ницами сертифицированного оборудования.

И замыкает список компания *ZTE* (Китай), имеющая в своем арсенале 6 сертификатов соответствия.

В процентном соотношении информация представлена на рисунке 1.

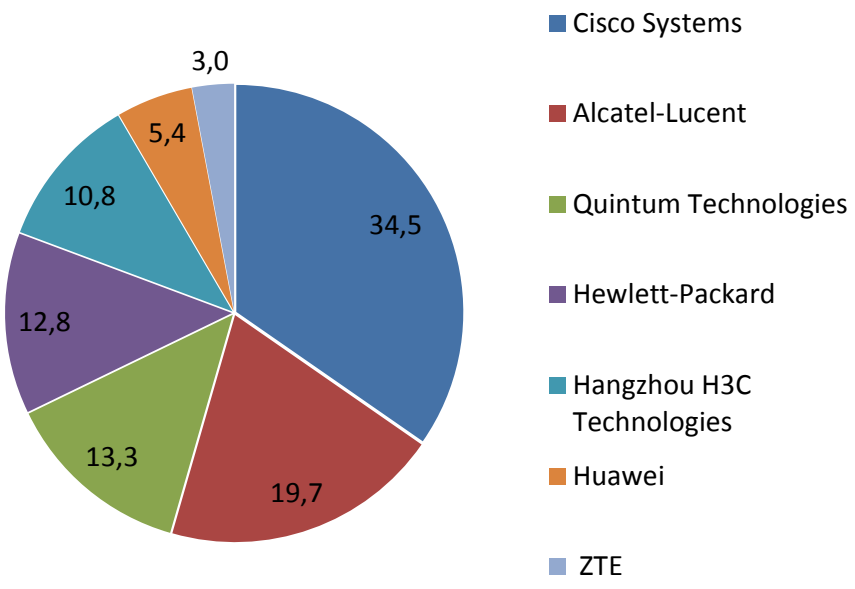


Рисунок 1. Количество (%) сертифицированных средств общего назначения, которые разрешены для обеспечения технической защиты информации, необходимость охраны которой определена законодательством Украины

Если говорить о программном обеспечении, то на рынке Украины аттестаты соответствия имеют:

Антивирусное программное обеспечение (рис. 2):

а) ESET, Словакия;
б) «Лаборатория Касперского», Россия;
в) «Доктор Веб», Россия.

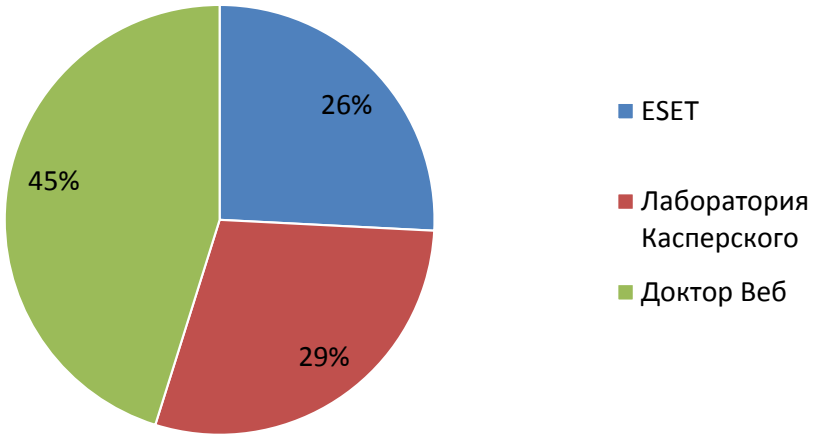


Рисунок 2. Доли рынка сертифицированного антивирусного программного обеспечения

Специализированное программное обеспечение:

а) система автоматизации управления предприятием «Парус-Корпорация»;
б) программный комплекс «1С: Предприятие, версия 8.2»;
в) система документооборота «Мегаполис»;
г) система документооборота «ДОК ПРОФ 2.0»;
д) программный комплекс «ABBYY FlexiCapture, версия 10.0»;
е) Microsoft Windows 7 Enterprise Edition-Service Pack 1 (32-bit и 64-bit);
ж) Microsoft Windows Server 2008 R2Enterprise Edition Service Pack; и др.

Еще одним важным моментом является то, что согласно Правилам ***передача конфиденциальной информации из одной системы в другую должна осуществляться в зашифрованном виде или по защищенным каналам связи*** в соответствии с требованиями законодательства по вопросам технической и криптографической защиты информации. В основе всех сертифицированных в Украине средств криптографической защиты информации лежит алгоритм симметричного шифрования, ГОСТ 28147-89.

Порядок проведения работ по созданию КСЗИ описан в одноименном документе: НД ТЗИ 3.7-003-05 «Порядок проведения работ по созданию комплексной системы защиты информации в информационно-телекоммуникационной системе». Согласно этому документу создание комплекса средств защиты от несанкционированного доступа осуществляется во всех ИТС, где обрабатывается информация, являющаяся собственностью государства, относится к отдельным видам информации, необходимость защиты которой определена законодательством, а также в ИТС, где такая необходимость определена собственником информации.

Порядок создания КСЗИ в ИТС является единым независимо от того, создается КСЗИ в ИТС, которая проектируется, или в действующей ИТС, если возникла необходимость обеспечения защиты информации либо модернизации уже созданной КСЗИ.

Из всего сказанного можно сделать следующие **выводы**:

Государственные органы, если у них есть информационно-телекоммуникационная система и они имеют информационный ресурс в сети Интернет, обязаны в любом случае строить комплексную систему защиты информации.

Коммерческие организации, если они обрабатывают конфиденциальную информацию о физическом лице (в частности, данные о национальности, об образовании, о семейном положении, религиозных убеждениях, состоянии здоровья, а также адрес, дату и место рождения) в информационно-телекоммуникационной системе, также должны строить КСЗИ.

При построении КСЗИ необходимо использовать сертифицированное оборудование и программное обеспечение. Если же в ИТС присутствует оборудование, не имеющее аттестата соответствия, то либо его необходимо заменить на сертифицированное, либо провести процедуру оценки его соответствия требованиям национальных стандартов в области технической защиты информации на этапе государственной экспертизы комплексной системы защиты информации.

Где этому учат?

На сегодняшний день ***повышение квалификации*** персонала в области информационной безопасности проходит ***в двух направлениях***:

- изучение требований международного стандарта ISO 27001;
- получение разъяснений относительно требований Закона Украины «О защите персональных данных».

Разъяснительные семинары в области защиты персональных данных на регулярной основе проводит Государственная служба Украины по вопросам защиты персональных данных. Основными потребителями данных семинаров являются менеджеры по персоналу.

Что касается ISO 27001, то на данный момент на рынке Украины существует два учебных центра, которые проводят данный курс. Стоит отметить, что особой популярностью среди слушателей пользуются мос-

ковские лекторы. Однако тенденция такова, что за последние два года ***количество слушателей сократилось примерно на 50%.*** Упор делается преимущественно на корпоративное обучение.

Производными от ISO 27001 являются тренинги на тему «Управление информационными рисками (IT-рисками)» и «Внедрение системы управления информационной безопасностью (СУИБ) на основе отраслевого стандарта информационной безопасности СОУ Н НБУ 65.1 СУИБ 1.0:2010». Национальный банк Украины переработал ISO 27001, и как результат появился Стандарт организации Украины «Методы защиты банковской деятельности. Система управления информационной безопасностью. Требования» (сокращенно – СОУ Н НБУ 65.1 СУИБ 1.0:2010).

Кто выступает регулятором в вопросах обеспечения информационной безопасности?

Как уже ранее упоминалось, главным регулятором в вопросах информационной безопасности выступает ***Государственная служба специальной связи и защиты информации Украины***, основными задачами которой являются:

- формирование и реализация государственной политики в сфере защиты информационных, телекоммуникационных и информационно-телекоммуникационных систем;
- определение требований и порядка создания, развития систем технической и криптографической защиты информации, являющейся собственностью государства, или информации с ограниченным доступом, требование относительно защиты которой установлено законом;
- разработка и осуществление мероприятий по развитию телекоммуникационных сетей, улучшение их качества, обеспечение доступности и устойчивого функционирования;
- содействие интеграции сфер телекоммуникаций, пользования радиочастотным ресурсом Украины в мировое информационно-коммуникационное пространство.

Однако в вопросах защиты персональных данных уполномоченным органом является ***Государственная служба Украины по вопросам защиты персональных данных***, основными задачами которой являются:

- внесение предложений по формированию государственной политики в сфере защиты персональных данных;
- реализация государственной политики в сфере защиты персональных данных;
- контроль над соблюдением требований законодательства о защите персональных данных;
- осуществление международно-правового сотрудничества в сфере защиты персональных данных.

Кто представляет IT-индустрию в Украине?

Ведущие позиции в области системной интеграции занимает «Инком».

На втором месте – «БМС Консалтинг».

Далее:

- ITodor;
- S&T Ukraine («Эс энд Ти» Украина);
- «ТехноСерв Украина»;
- «Приоком»;
- NetWave;
- OSIS;
- «Ситроникс ИТ Украина»;
- IBA Group;
- Integrity Vision;
- SI BIS;
- RIM2000;
- Space IT;
- Triasystems;
- «Инлайн Груп Запад»;
- Астерос Украина и др.

Согласно данным Госстатистики, ***оборот телекоммуникационного оборудования*** за первый квартал 2012 года составил 568 436,9 тыс. гривен (примерно ***71 млн*** долларов США), за первое полугодие 2012 года – 1 288 045,4 тыс. гривен (примерно ***161 млн*** долларов США).

Начиная с 2005 года продажи компьютерного оборудования и другой вычислительной техники возросли в 5,3 раза. С 2008 по 2009 год наблюдается спад показателей до

уровня 2007 года, этот период совпадает с экономическим кризисом в стране. На рисунке 3 представлены данные по обороту компьютерного оборудования за 2005–2011 годы.

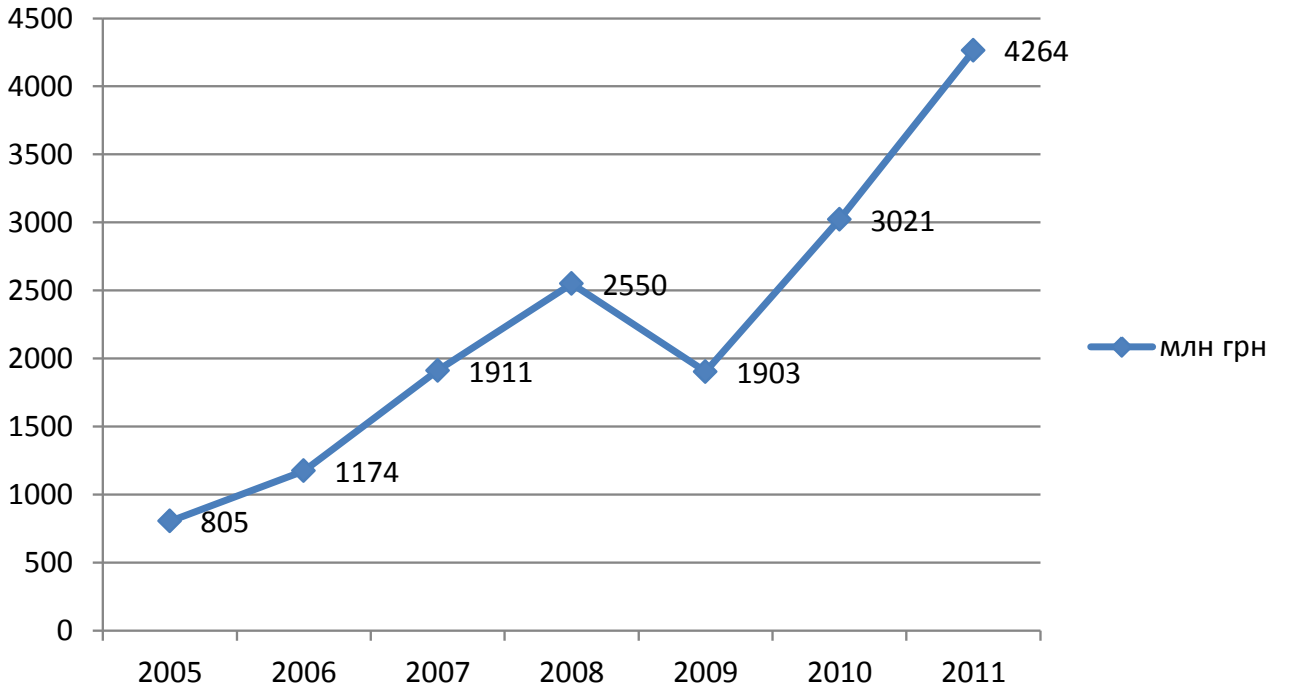


Рисунок 3. Оборот компьютерного оборудования и другой вычислительной техники

О выставках и конференциях

На регулярной основе в Украине проходят:

• Международная конференция «Банковские системы и безопасность информационных технологий», на которой преимущественно рассматриваются вопросы информационной безопасности в банках;

• Международная конференция Computer Forensics Ukraine, посвященная вопросам компьютерной криминалистики и информационной безопасности;

• Конференция McAfee Security Day in Ukraine, на которой обсуждаются тенденции развития киберпреступности и методы борьбы с ней.

В 2012 году впервые была проведена Международная конференция «Защита персональных данных: право, практика, надзор». В ней приняли участие представители Группы уполномоченных органов по вопросам защиты персональных данных стран Центральной и Восточной Европы.

Что касается выставок, то их всего две:

Cisco Expo – выставка, посвященная продуктам и технологиям Cisco.

«Безпека» – выставка, которая представляет комплекс систем, средств и услуг для обеспечения безопасности предприятия, офиса, дома и человека.

Если первая интересна с точки зрения информационной безопасности и телекоммуникационных систем, применения современных решений при обработке и передаче данных, то вторая достаточно статична и сосредоточена исключительно на вопросах физической защиты.

Итоги

1. Рынок информационной безопасности Украины условно можно поделить на следующие сегменты:
2. Обеспечение информационной безопасности в автоматизированных (компьютерных) и телекоммуникационных системах (локальные сети предприятия, телефония).

3. Обеспечение информационной безопасности путем шифрования и/или использования инфраструктуры открытых ключей (электронно-цифровая подпись).
4. Обеспечение информационной безопасности путем физической защиты помещений, систем, сетей и комплексов обработки информации, в том числе биометрическая система защиты.

Консалтинг, аудит информационной безопасности, а также повышение квалификации.

Если для государственных организаций и банков ответ на вопрос относительно необходимости защиты информации очевиден, то для всех остальных предприятий он все еще остается открытым по двум причинам:

1. Финансовая.
2. Организационная.

Причем эти причины взаимосвязаны.

Но несмотря на существующие сложности, украинский рынок информационной безопасности продолжает развиваться, предпринимаются попытки адаптировать и интегрировать в жизнь лучшие мировые практики в области информационной безопасности и информационных технологий.

Приложение А. МЕТОДИКА И ПОДХОД

Цель исследования

Дать читателю наиболее адекватное представление о рынке информационной безопасности Российской Федерации с указанием качественных и количественных характеристик по секторам.

Понятие рынка информационной безопасности

Информационная безопасность (ИБ) – это процесс обеспечения интересов стейкхолдеров путем управления бизнес-рисками, связанными с информационными потоками и технологиями.

Рынок информационной безопасности – рынок продуктов и услуг, направленных на обработку бизнес-рисков, связанных с информационными потоками и технологиями.

В рамках рынка информационной безопасности необходимо отдельно рассматривать рынок продуктов и рынок услуг. Рынок продуктов включает в себя как поставку оборудования, так и пусконаладочные работы (ПНР). Рынок услуг включает в себя проектирование, выработку интеграторских решений и консалтинг ИБ.

Для исключения двойного учета продуктов ИБ в рамках интеграторских решений проводится нормировка. В результате рынок услуг не включает в себя рынок продуктов ИБ.

В данном исследовании под продуктами ИБ понимаются технические решения следующих классов:

1) системы защиты от несанкционированного доступа;
2) средства обеспечения сетевой безопасности;
3) средства контентной фильтрации;
4) средства криптографической защиты информации;
5 технические решения резервного копирования и восстановления данных;
6) инструментальные средства анализа защищенности;
7) средства защиты удаленного доступа;
8) средства сбора и корреляции событий ИБ (SIEM);
9) системы идентификации и аутентификации (IDM);
10) средства контроля утечек (DLP);
11) средства антивирусной защиты.

К услугам по информационной безопасности относятся следующие:

1) аудит информационной безопасности;
2) консалтинг в области информационной безопасности;
3) услуги по сертификации продукции по требованиям информационной безопасности;
4) образовательные услуги;
5) мероприятия по ИБ.

В рамках настоящего исследования рынок ИБ представляется как ряд секторов рынка, включающих в себя указанные выше классы технических решений и услуги.

В исследовании разрабатывается раздел «Рынок PKI». Рынок PKI хоть и имеет непосредственное отношение к рынку ИБ, тем не менее не является его составной частью. По этой причине в разделе с итоговой оценкой рынка он не рассматривается как сегмент рынка ИБ.

Также в рамках исследования готовится «Обзор рынка информационной безопасности Украины», который также не влияет на итоговую оценку рынка ИБ.

В рамках исследования авторами представляются качественные и количественные оценки по секторам рынка, а также выдается интегральная оценка.

Применяется методика, основанная на опросе респондентов, анализе данных из открытых источников, а также экспертного мнения исследователя. В качестве единственного источника информации не могут приниматься данные, представленные коммерческими компаниями. В случае если такие данные являются основными, в обязательном порядке должна проводиться нормировка посредством использования экспертных оценок участников рынка. В качестве респондентов могут привлекаться только эксперты, знакомые с конкретным сектором рынка.

Каждый раздел исследования должен содержать следующую информацию:

- Основные игроки сектора рынка. Качественные и количественные характеристики.
- Основные тенденции сектора рынка. Качественные и количественные характеристики.
- Основные события и изменения в рамках данного сектора рынка за 2012 год.
- Динамика сектора с 2005 года по настоящий момент плюс прогноз на три года (если возможно).

Требования по наличию конкретных подразделов отсутствуют. ■