

Презентация исследования

Рынок информационной безопасности 2007- 2008

Москва, 2008

Об исследовании

LETA IT-company представляет второй экспертный отчет «Навстречу переменам: рынок информационной безопасности 2007-2008». Первый отчет был выпущен в начале 2007 года и многие его оценки стали признанными фактами на рынке информационных технологий.

Данное исследование посвящено рынку ИБ в России. Под рынком ИБ в рамках настоящего исследования подразумевается рынок всех средств и услуг, обеспечивающих информационную безопасность сетей, оборудования и систем государственных и коммерческих организаций.

Особо следует подчеркнуть, что авторы не ставили перед собой задачу осветить все аспекты, связанные с ИБ в России. Так, в исследовании не были подробно рассмотрены ряд сегментов рынка, например сетевая безопасность, web-безопасность, и т.д. Также сузить выбор сегментов LETA была вынуждена в связи с ограниченностью ресурсов и информации.

Информация для данного исследования получена путем опроса участников рынка методом экспертных интервью, а также анализа публикаций в СМИ и иных открытых источниках. Мы также пользовались открытыми данными ведущих исследовательских компаний — IDC, Gartner, PWC, Ernst&Young и др.

Все числовые данные являются экспертными оценками журналистов, участников рынка и аналитиков LETA IT-company. В исследовании использованы оценки из источников, имеющих высокий уровень достоверности: ведущие деловые и специализированные СМИ, представители крупнейших компаний и т.д.

Тенденции и прогнозы рынка ИБ сделаны на основании тенденций и прогнозов развития экономики РФ в целом, развития ИТ-рынка и рынка ИБ в России и в мире, а также оценок и расчетов аналитиков Департамента маркетинга LETA IT-company.

Оглавление

ОБ ИССЛЕДОВАНИИ	2
ОГЛАВЛЕНИЕ.....	3
СПИСОК ИЛЛЮСТРАЦИЙ.....	3
ОСНОВНЫЕ ВЫВОДЫ.....	4
ВВЕДЕНИЕ	5
ОБЪЕМЫ РЫНКА И СТРУКТУРА РЫНКА ИБ	7
Объем рынка ИБ	7
Структура потребления средств ИТ	10
Основные игроки на рынке ИБ	12
ОСНОВНЫЕ ФАКТОРЫ, ВЛИЯЮЩИЕ НА РАЗВИТИЕ РЫНКА ИБ	15
Соответствие стандартам и нормативным актам	15
<i>Развитие применения стандартов.....</i>	<i>15</i>
<i>Развитие законодательного регулирования.....</i>	<i>16</i>
Развитие новых систем ИБ	19
<i>DLP системы</i>	<i>19</i>
<i>Системы комплексной безопасности</i>	<i>20</i>
Применение «экономического» подхода	21
Легализация и развитие применения средств ИБ	23
<i>Рынок антивирусных средств.....</i>	<i>23</i>
<i>Усложнение задач, решаемых ИБ.....</i>	<i>25</i>
ТЕНДЕНЦИИ РАЗВИТИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СО СТОРОНЫ ВНЕШНИХ ВОЗДЕЙСТВИЙ.....	26
<i>Развитие бот-сетей.....</i>	<i>26</i>
<i>Скрытность вредоносного ПО</i>	<i>27</i>
<i>Угрозы для мобильных устройств</i>	<i>28</i>
<i>Новые технологии воздействия и поиск новых уязвимостей</i>	<i>29</i>

Список иллюстраций

Таблица 1. Основные сегменты потребления средств ИБ в %	11
Таблица 2. Ранкинг российских компаний, продвигающих услуги в области ИБ	14
Таблица 3. Сертифицированные СУИБ на начало 2008 года	15
Таблица 4. Общее количество ПК в России	24
Таблица 5. Тройка лидеров на рынке антивирусных средств	25
Рисунок 1. Факторы роста рынка ИБ в среднесрочной перспективе	6
Рисунок 2. Структура рынка информационной безопасности	8
Рисунок 3. Структура «открытого» рынка ИБ в \$млн.	9
Рисунок 4. Динамика роста всего рынка ИБ	9
Рисунок 5. Потребители ИБ в %	11
Рисунок 6. Доли игроков на рынке в %	13

Основные выводы

1. Объем «открытого» рынка информационной безопасности (ИБ) – 431 \$млн¹.
2. Объем всего рынка информационной безопасности, включая скрытый рынок – 912 \$млн.
3. Среднегодовые темпы роста рынка ИБ в 2007 году 45 – 50%, в то же время, рост ИТ – 6%, что означает, что он стагнирует
4. На программное обеспечение пришлось 65% «открытого» рынка, на аппаратное обеспечение - 6%, на услуги - 29%
5. Главное разочарование рынка – отсутствие роста широкого применения международного стандарта ISO 27001. По оценке LETA, внедрение стандарта будет идти «снизу», от частных политик
6. В 2007-2008 гг. произошло усиление внимания государства к вопросам защиты конфиденциальной информации, за это время было выпущено ряд нормативных актов
7. Крупные корпорации и самая прогрессивная часть из компаний SMB сектора стали все больше прибегать к услугам ИБ-компаний; сторонниками самостоятельных внедрений остаются средние компании.
8. Главная удача рынка – активный рост сегмента DLP (Data Leak Prevention), на 2007 – 2010 годы это будет самый быстрорастущий сегмент рынка ИБ
9. Объем средств потраченных в 2007 году на антивирусные средства составил около 110 \$млн.
10. К главным тенденциям развития угроз информационной безопасности со стороны внешних воздействий относятся:
 - ✓ Развитие бот-сетей
 - ✓ Скрытность вредоносного ПО
 - ✓ Угрозы для мобильных устройств

¹ Доллар США – среднегодовой курс по данным ЦБ РФ

Введение

Рынок информационной безопасности (в дальнейшем ИБ) остается одним из самых быстрорастущих сегментов российского ИТ-рынка.

В целом по данным агентства CNews Analytics и по предварительным оценкам IDC, объем российского ИТ-рынка по итогам 2007 года составил \$16 млрд. при росте 18% к предыдущему году. Министерство информационных технологий и связи РФ оценивает продажи на рынке ИТ в \$17,6 млрд. При пересчете роста в рублевый эквивалент оказывается, что рынок практически стагнирует: его реальный рост составил около 6%.

Но при этом рынок ИБ показывает совсем другие темпы роста, и это не только российская тенденция. Практически во всех странах рост затрат на ИБ превышает рост затрат на ИТ, по данным независимых исследований затраты на ИБ в среднем выше на 20 - 30%.

Общей тенденцией является рост угроз, но в разных странах и экономиках этот рост имеет разное основание. В России же главными двигателями роста являются:

1. Сам рост рынка за счет увеличения потребления, в том числе и легализация. Это, прежде всего, касается средств антивирусной защиты (в данном случае и далее под антивирусами подразумевается класс систем Secure Content and Threat Management,- SCM. Данный термин еще не стал общеупотребимым, поэтому в исследовании будет употребляться термин «антивирусная защита»)
2. Требования регуляторов и стандартов. На данный момент в России пока нет обязательных стандартов, но, тем не менее, все большее число организаций начинают тратить средства на полное или частичное соответствие требованиям регуляторов и/или стандартов
3. Появление новых сегментов. За последние несколько лет на рынке ИБ появился ряд новых технологий (часть из них будет рассмотрена в исследовании) и новых компаний, которые эти технологии предлагают. При этом эти технологии востребованы рынком как на данный момент, так и в среднесрочной перспективе (NAC, DLP, compliance и т. д.)
4. Повышение доступности ИБ. Использование средств ИБ, прежде всего, для малых и средних компаний упростилось. Как производители, так и компании интеграторы предлагают стандартные, несложные в настройке и эксплуатации решения. За счет типизации подобных решений стало возможно адаптировать решения по ИБ для малого и среднего бизнеса, доступные по цене. Это привело к тому, что организации, ранее пренебрегавшие средствами ИБ из-за их сложности и дороговизны, стали тратить средства на новые системы.

5. ИБ постепенно становится не просто одним из средств ИТ, а методом снижения рисков и повышения эффективности бизнеса. Этот подход пока не стал общеприменимым, но все большее число компаний начинают использовать ИБ не просто как набор технико-организационных мер, а как средство для управления бизнесом.

Рисунок 1. Факторы роста рынка ИБ в среднесрочной перспективе



Источник: LETA IT-company, Ernst&Young, IDC, PwC

Влияние приведенных факторов на рост рынка будет рассмотрено в рамках данного исследования.

Отдельная глава будет посвящена проблемам развития направления технических угроз.

Объемы рынка и структура рынка ИБ

Объем рынка ИБ

В 2007 году рынок информационной безопасности продолжил свой рост. Как и в 2006 году, его рост значительно опережал рост рынка ИТ. При этом ИБ не демонстрирует снижения темпов роста, как это прогнозировалось аналитиками LETA и ряда независимых агентств на 2007 год. В результате разрыв в темпах роста рынков ИБ и ИТ в краткосрочной перспективе будет только увеличиваться.

В первом исследовании, проведенном LETA IT-company, было выявлено, что рынок ИБ в России недостаточно прозрачен, его структура не отвечает мировым тенденциям. Хотя существует и другой факт: все остальные сегменты ИТ-рынка очень хорошо вписываются в мировые тенденции.

В ходе дополнительного опроса в 2006 – 2007 годах аналитики LETA сделали вывод о существовании «скрытого» рынка. По данным первого исследования объем рынка ИБ был равен \$250 млн., что составляет 1,8% от всего ИТ-рынка. Это не соответствует мировой практике, где рынок ИБ занимает от 8 до 9% от рынка информационных технологий.

В результате, без учета доли «скрытого» рынка, российский рынок ИБ явно не дотягивает до среднемировых показателей. И действительно, по данным независимых экспертов, от 3 до 8% стоимости проектов по внедрению КИС или ИТ-инфраструктуры приходится на работы по ИБ, которые обычно не выделяют в отдельную статью расходов.

Отдельно в первом исследовании было существование так называемого «серого» рынка ИБ, к которому относится потребление сегментами SOHO (малый и домашний офис) и частными пользователями пиратских продуктов ИБ. Их потенциальная доля оценивалась как небольшая, до 20%. Но взрывной рост продаж антивирусов в рознице в 2007 году, когда продажи Лаборатории Касперского в ритейле выросли в 4 раза, а продажи ESET – в 10 раз, отчасти подтверждает притязания этого сегмента на небольшую долю на рынке ИБ (до 10%) уже сегодня.

В результате был сделан вывод о том, что в целом, включая «серую» зону, рынок ИБ в 2006 году занимал около 5% от всего ИТ-рынка, что в денежном эквиваленте составляет около \$700 млн.

Развивая в 2007 году методологию исследования рынка ИБ, аналитики LETA убедились, что вывод о существовании «скрытого» и «серого» рынка правильный; респонденты (представители ИТ и ИБ рынка) подтверждали это. Но, в ходе дальнейших исследований, была уточнена структура скрытых и открытых сегментов. Следует подчеркнуть, что данное исследование не отменяет выводов предыдущего, а дополняет и углубляет его положения.

В 2007 – 2008 годах на основе совместно выработанной методологии компания IDC предоставила LETA данные по продажам софтверных решений в России. На основе этих данных стало возможным просчитать объем видимого рынка.

К нему относятся:

1. Продажи легального ПО
2. Продажи специализированного аппаратного обеспечения
3. Объем сервисов по внедрению и обслуживанию (техническая поддержка) средств ПО и АО.

Рисунок 2. Структура рынка информационной безопасности

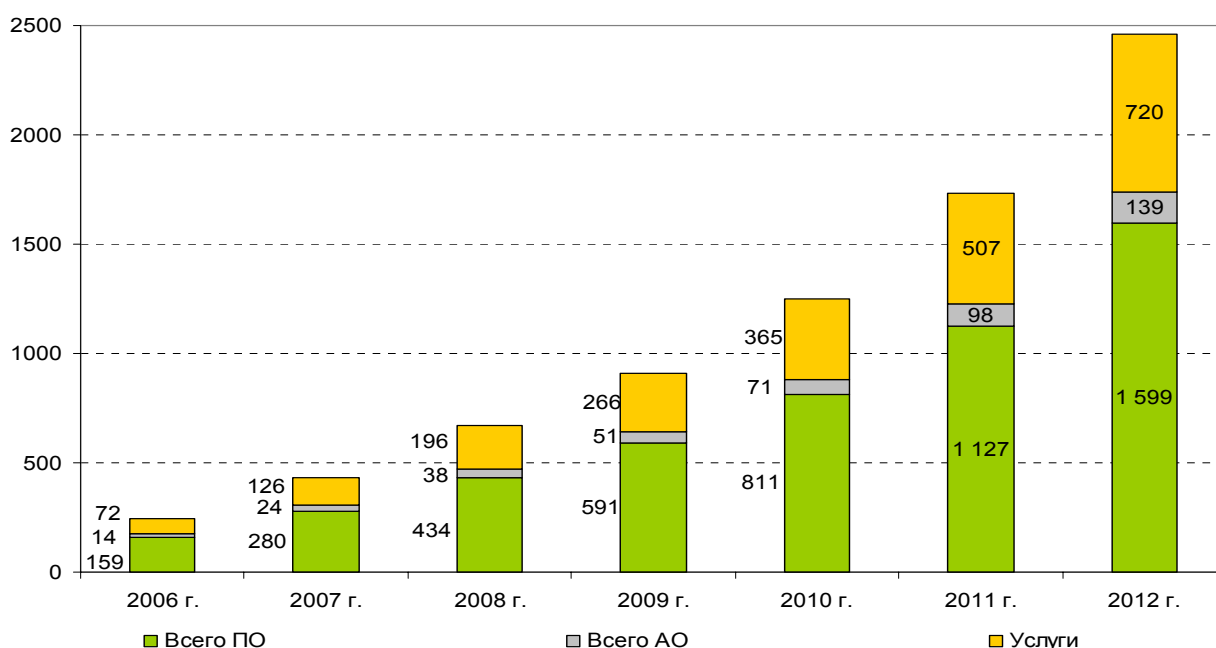


Источник: LETA IT-company

В результате удалось выделить реальный открытый объем рынка ИБ. Но, тем не менее, «скрытый» рынок продолжает существовать и занимать большую долю в рынке ИБ:

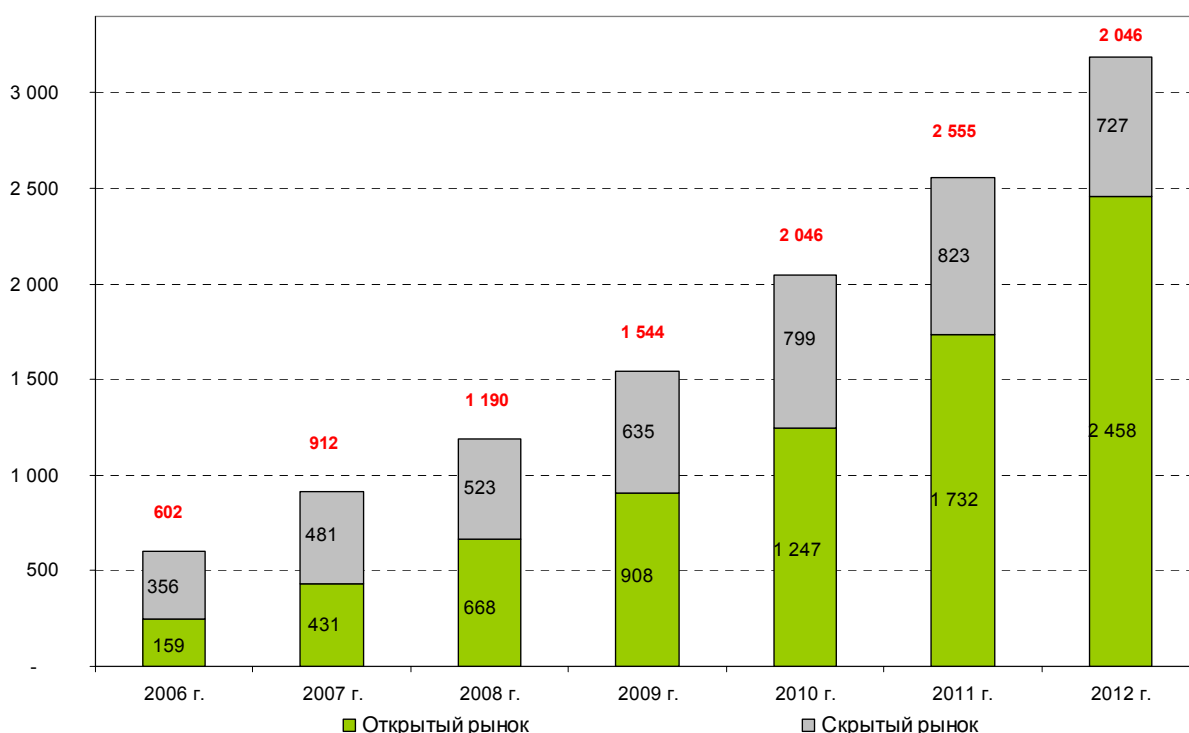
1. Пиратство. Практически 50% используемого на рынке ИБ ПО - пиратское. Значительная часть пиратского ПО приходится на сегмент SoHo и частных пользователей.
2. Работы, связанные с обеспечением информационной безопасности, но при этом не учитываемые как прямые затраты. Это, прежде всего, создание политик разных уровней, контроль их исполнения, обучение. То есть это затраты на организационные мероприятия. Именно они и занимают существенную часть скрытого рынка, при этом чаще всего затраты на эти действия (если это не внешний проект) не учитываются.
3. Затраты на ИБ в рамках внедрения и эксплуатации информационных систем. Системные администраторы, внедренцы и консультанты постоянно решают задачи, связанные с безопасностью. Это как настройка для безопасной работы различных ИТ-систем (от инфраструктуры до бизнес и промышленных приложений), так и их эксплуатация.

Рисунок 3. Структура «открытого» рынка ИБ в \$млн.



Источник: LETA IT-company, IDC

Рисунок 4. Динамика роста всего рынка ИБ



Источник: LETA IT-company

В результате среднегодовые темпы роста рынка ИБ будут составлять 45 -50%, в то время как рынок ИТ фактически стагнирует.

Таким образом, дальнейшее развитие рынка будет характеризоваться двумя направлениями:

- ✓ Рост открытого рынка. Некоторые тенденции будут описаны ниже

- ✓ Сокращение «скрытого рынка». Сокращение же «скрытого рынка» будет происходить за счет:
 - Снижения пиратства
 - Увеличение рынка консалтинговых услуг в области ИБ, прежде всего, по построению как всего СУИБ, так и его отдельных элементов.
 - Увеличение числа проектов, где все работы по ИБ будут проходить отдельной строкой в бюджете затрат.

В результате в ближайшие 5 лет мы ожидаем конвергенцию так называемого «скрытого» рынка ИБ и классического ввиду эволюции последнего.

Структура потребления средств ИТ

На сегодняшний день основной моделью потребления остается самостоятельное внедрение систем ИБ. Но тенденции 2006 года нашли свое продолжение и в 2007 году. Все больше компаний обращается за профессиональными услугами. При этом постепенно меняется ситуация в крупных компаниях.

Если еще несколько лет назад ИТ и ИБ-отделы (или аутсорсинговые компании) крупных корпораций и компаний верхнего сегмента SMB предпочитали сами внедрять ИБ-решения, то с усложнением технологий, появлением новых систем, началом применения стандартов, в этих отделах стало не хватать персонала на то, чтобы охватить весь спектр решений. В результате внедрение стали проводить специализированные компании, а за собственными структурами осталось сопровождение.

Поэтому именно крупные компании стали все больше прибегать к услугам ИБ-компаний. Также традиционно к услугам специализированных компаний прибегают малые компании, у которых нет собственного персонала. Интересно отметить, что сторонниками самостоятельных внедрений остаются средние компании. Сами представители этих компаний объясняют это тем, что стандартный набор сервисов по ИБ могут оказать собственные сотрудники, которые и должны этим заниматься. Но и среди данного типа компаний растет понимание, что многие специализированные сервисы в области ИБ требуют специализированного подхода. В дальнейшем это приведет к росту запросов к ИБ-интеграторам, соответственно, к росту затрат на ИТ-услуги.

Таблица 1. Основные сегменты потребления средств ИБ в %

Сегменты	Доля
Всего программное обеспечение	65%
Всего аппаратное обеспечение	6%
Услуги	29%

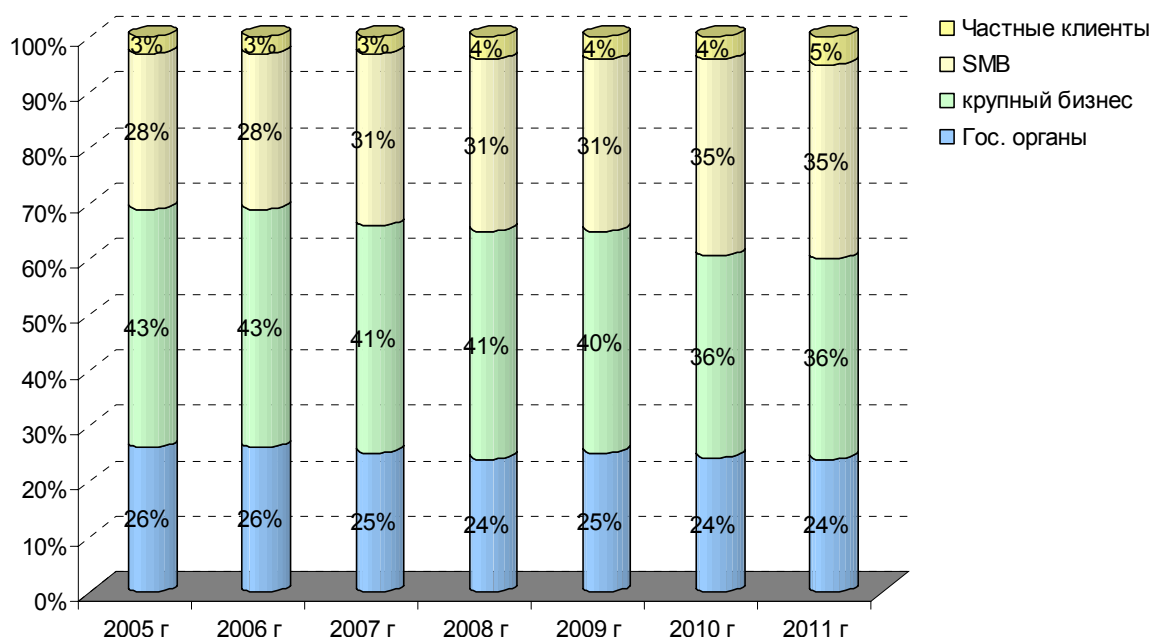
Источник: LETA, IDC

В ходе исследования было выявлено четыре основные группы потребителей.

Но, несмотря на рост продаж услуг, основное потребление приходится на поставку программных решений.

Такое преобладание продаж продуктов связано с тем, что пока рынок ИБ все еще консервативен. Многие организации, как коммерческие, так и государственные, воспринимают системы ИБ как наиболее критические, доступ к которым должен быть максимально ограничен. Поэтому не допускают к работе с ними внешних специалистов и внедряют все силами своих специалистов, то есть используют подход – «все делаем сами».

Рисунок 5. Потребители ИБ в %



Источник: IDC, LETA, РБК, РwC.

2008 год подтвердил тенденцию того, что с развитием рынка структура потребителей будет постепенно меняться. Для рынка будет характерно:

- Снижение доли госорганов
- Снижение доли крупного бизнеса
- Рост сегмента SMB
- Рост частных потребителей

Снижение доли госорганов. Обусловлено постепенным общим снижением затрат госорганов на автоматизацию. В 90-е и в начале 2000-ых годов именно госорганы были основными потребителями ИТ, но с развитием рынка и постепенным насыщением государственных органов современными ИТ, средства, выделяемые на закупку ИТ (в том числе и безопасность) будут сокращаться. Это приведет к постепенному сокращению их доли. Увеличение доли госорганов возможно, если на ИТ начнут выделяться деньги в рамках национальных проектов.

Снижение доли крупного бизнеса. Причины сокращения доли крупного бизнеса аналогичны. В основном эти компании уже прошли этап большой автоматизации, и, соответственно, как мы уже отмечали, их доля будет постепенно сокращаться.

Однако именно в среде крупного бизнеса происходят основные изменения структуры потребления. В этом сегменте наиболее востребованы услуги, связанные с аудитом ИТ, а также с защитой ранее незащищенных областей, внедрением систем централизованного управления.

То есть основные затраты в области ИБ будут приходиться на поддержание ИБ-систем. И при переходе самой компании на более высокий уровень менеджмента будут появляться затраты на внедрение политик, регламентов, работы на соответствие стандартам и нормативным актам, внедрению средств ИБ более высокого уровня сложности. В перспективе это может стать одной из самых значительных статей расходов на ИБ

Рост сегмента SMB. В связи с тем, что именно в сегменте SMB наблюдается основной рост потребления ИТ, соответственно, в этом сегменте будет наблюдаться и наибольший рост средств ИТ-защиты. Особенностью данного сегмента в ближайшее время будет то, что в нем будут потребляться самые «простые» средства, без использования которых нормальное бесперебойное функционирование ИТ невозможно. Это, прежде всего, средства защиты периметра.

Рост сегмента частных потребителей. Частные клиенты начинают «обелять» свое ПО; закупка оригинальных средств защиты будет постепенно возрастать. Также росту данного сегмента способствуют OEM-программы, когда частный покупатель вместе с компьютерной техникой приобретает уже инсталлированные средства защиты.

В целом, именно рынок средств защиты наименее «пиратский». По мнению опрошенных экспертов, это связано с огромной скоростью появления все новых угроз. Для корпоративных и частных пользователей защита данных — одна из первостепенных задач, а использование «пиратских» средств не дает возможность противостоять эволюционирующим угрозам. Поэтому именно рынок средств защиты первым стал выходить из «тени».

Основные игроки на рынке ИБ

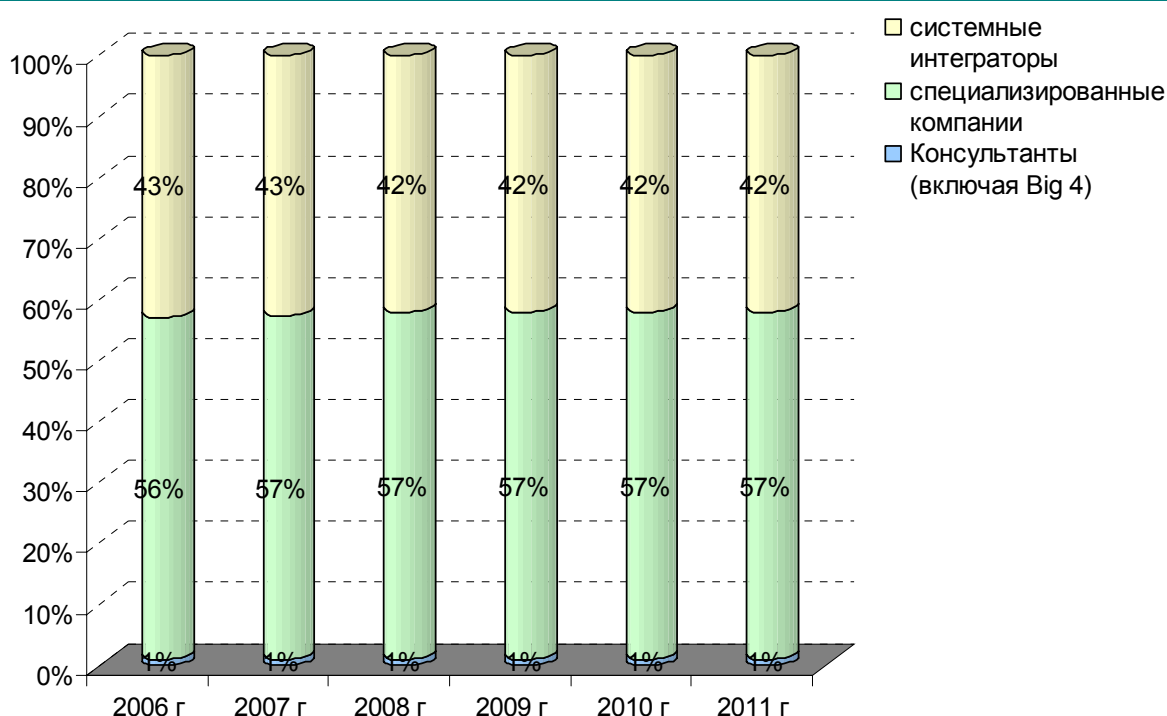
В 2008 году подход «делаем все сами» все еще характерен в целом для отрасли. Но с расширением применения средств безопасности ИТ, а также с распространением программных и

аппаратных средств со сложным внедрением, доля работ, выполняемых сторонними организациями, будет только расти. Это будет связано прежде всего с изменениями в структуре потребления как ИТ-услуг, так и услуг в ИБ.

В результате, доля услуг на рынке ИБ будет стремиться к той доле, которую занимают услуги на корпоративном рынке ИТ.

Особенностью рынка является и то, что нельзя выделить компаний-лидеров. Практически все ИТ-компании продают или внедряют средства защиты.

Рисунок 6. Доли игроков на рынке в %



Источник: LETA

При этом крупнейшие российские интеграторы не делали ставку на развитие у себя направления ИБ. Но за 2007 год большинство из крупных компаний или выделили у себя направление ИБ, или усилили уже существующее. В результате конкуренция на этом перспективном рынке будет только увеличиваться.

Специализированные ИБ-интеграторы пока имеют важное преимущество: более высокий уровень компетенции, который и позволяет им осуществлять сложные технические и консультационные проекты. Также важным преимуществом является опыт сложных проектов по ИБ, соблюдение и использование все необходимых нормативных актов и стандартов

Еще одним фактором влияния на развитие рынка служит то, что крупные ИТ-компании столкнулись с проблемой работы в SMB-сегменте. Крупные системные интеграторы изначально работали с корпоративным сектором и госструктурами, но последние изменения на рынке ИБ, где все большую роль играют SMB-компании, показали, что сегодняшним «крокодилам»

чрезвычайно сложно приспосабливаться к новым условиям. Подробнее об изменениях в среде ИТ-компаний см. третью главу.

В свою очередь, специализированные компании отлично разбираются в технологических основах ИБ, но при этом хуже ориентируются в «экономическом» подходе.

В результате, на рынке смогут полноценно работать только те компании, которые предложат заказчикам как «экономический»² подход, так и хорошую техническую базу.

Таблица 2. Ранкинг российских компаний, продвигающих услуги в области ИБ

Название компании
Информзащита
LETA IT-company
УСП КомпьюЛинк
ICL-КПО
Ланит
Инфосистемы Джет
Крок
Энвижн Груп
TopS BI
Элвис-Плюс

Источник: LETA, CNEWS

Усиление конкуренции на рынке ИБ побуждает ведущие компании, продвигающие ИБ-услуги, развивать необходимые рынку компетенции, разрабатывать современные типизированные услуги. Немаловажным фактором успеха на рынке становится также кадровая политика и серьезные финансовые ресурсы. При этом фактор лидерства будет обеспечиваться скорее умением решать бизнес-задачи клиентов, а не техническими свойствами решений.

Изменения, прежде всего, внедрение «экономического» подхода, на данном рынке приведут к тому, что многие ИТ-компании, которые ориентированы только на технологические решения, не смогут адекватно отвечать запросам клиентов, уже осознавших необходимость новых подходов к ведению бизнеса.

В результате возможно сокращение числа компаний, способных оказывать востребованные услуги, и появление новых компаний, ориентированных именно на «процессный» подход и оказание типизированных услуг. Также в результате изменений на рынке увеличится доля консалтинговых компаний.

² Подробнее о «экономическом» походе см. исследование ["Основные тенденции в области защиты конфиденциальных данных от утечки информации ILDP на российском рынке"](#)

Основные факторы, влияющие на развитие рынка ИБ

Соответствие стандартам и нормативным актам

Одной из потенциальных движущих сил рынка постепенно становится соответствие регулирующим правилам - как нормативным актам, так и различным стандартам. Но, на данный момент, соответствие нормативным актам продвигается более быстрыми темпами, чем внедрение стандартов.

Развитие применения стандартов

Основной неудачей 2007 года является слабое развитие применения серии стандартов ISO 27001. Предполагалось, что российские компании станут активно применять и внедрять этот стандарт, так как именно применение стандартов является основным вектором развития. Но этого не произошло. По результатам опроса компании пока не готовы внедрять этот стандарт целиком. Основной причиной является то, что компании пока не видят в полноценном внедрении стандарта очевидного экономического эффекта

Но, тем не менее, все большее число компаний начинает использовать в своей практике частные политики. Как показывает опрос, опыт нашей компании и наших партнеров, российские компании готовы вводить организационные меры для части бизнес-процессов и активов, но пока не готовы тратить деньги на полноценный СУИБ, так как не могут пока оценить его экономическую эффективность.

Можно ожидать, что будет постепенный переход количества в качество. С накоплением частных политик по различным аспектам в области ИБ компании будут приходить к тому, что накопленный опыт и знания позволят строить им полноценный СУИБ. В результате движение будет идти от частного к общему. Но на начало 2008 года насчитывалось всего 8 аудированных СУИБ, хотя по некоторым оценкам уже более 60 компаний привели свои СУИБ в соответствии со стандартом, но, по различным мотивам, на сертификацию не вышли.

Таблица 3. Сертифицированные СУИБ на начало 2008 года

Компания	Аудитор	Стандарт
1 Bank24.ru, Ekaterinburg	Bureau Veritas Certification	ISO/IEC 27001:2005
2 CMA Small Systems AB	BSI	BS 7799-2:2002
3 CROC Incorporated, Moscow	BSI	ISO/IEC 27001:2005
4 Lukoil-Inform, LLC	BSI	ISO/IEC 27001:2005
5 Luxsoft, Moscow	LRQA	ISO/IEC 27001:2005
6 Multiregional TransitTelecom	BSI	ISO/IEC 27001:2005
7 Rosno, SC	BSI	ISO/IEC 27001:2005
8 TransTeleCom	SGS	ISO/IEC 27001:2005

Источник: International Register of ISMS Certificates

Основным движущим фактором использования стандарта будет то, что клиенты и партнеры компании хотят гарантий того, что их

конфиденциальная информация защищена надлежащим образом, и они могут требовать юридического закрепления данного факта в контрактах. Доказательством этого является наличие подтвержденных политик информационной безопасности компании. Правильно разработанные и реализованные политики и регламенты безопасности позволяют уменьшить время недоступности сервисов, вызванных компьютерными инцидентами, таким образом, увеличивая показатель устойчивости компании. Так как политики в рамках ИБ являются ключевыми в непрерывности бизнеса, введение их является доказательством намерений компании относительно качества информационной безопасности. Что интересно, контрагентов, партнеров и клиентов, как правило, интересуют именно эти “намерения”, а не технические средства, которыми они могут быть достигнуты.

Сертификация по стандарту подтверждает необходимый уровень обеспечения непрерывности бизнеса и информационной безопасности для защиты информации и бизнес-процессов. Например, в настоящее время фокус создания продуктов и услуг смещается из стран с дешевой рабочей силой. Одним из доказательств компаний из этих стран того, что они смогут адекватно защитить ту информацию, которую им передают производители, является сертификация на соответствие требованиям стандартов по информационной безопасности, например, ISO 27001.

Уже сейчас любая внешняя аудиторская проверка обращает внимание на необходимость формализации всех бизнес-процессов. В том числе, особое внимание уделяется наличию политик информационной безопасности. В 2007 году аудиторы стали обращать внимание на наличие метрик безопасности и непрерывности, так называемых KPI, согласованных с высокоуровневыми KPI ведения бизнеса. В целом наблюдается повсеместное усиление внимания к формализации систем управления компаниями для постановки и решения задач анализа и оптимизации бизнес-процессов.

Также необходимо отметить, что для выхода на международные рынки российские компании вынуждены были обратить свое внимание на лучшие международные стандарты и практики BS ISO/IEC 27001:2005, BS 7799-2:2005, COSO, CobiT 4.1, ITIL v3 (ISO/IEC 20000), BS 25999 для подготовки систем управления к наметившимся изменениям.

Все это, по нашим оценкам, приведет к тому, что применение стандарта будет увеличиваться.

Развитие законодательного регулирования

В 2007-2008 гг. произошло усиление внимания государства к вопросам защиты конфиденциальной информации, главным образом, к защите персональных данных и усиление контроля за режимом обеспечения конфиденциальности в органах исполнительной власти, ФГУПах, а также в коммерческих компаниях, связанных с исполнением работ со сведениями,

содержащими конфиденциальную информацию. В связи с этим требования ФСБ, ФСО, ФСТЭК и Минсвязи к лицензиатам и проверяемым предприятиям (в области их методического и технического уровня) регулярно повышаются.

Создана сеть федеральных удостоверяющих центров и соответствующие технические регламенты. Начался процесс предоставления юридически значимых государственных услуг с помощью государственных порталов на основе ЭЦП и цифровых сертификатов.

В целом движение рынка происходит в сторону ужесточения требований к организации режима конфиденциальности на предприятиях, усложнению методик аттестации и сертификации и требований к техническому обеспечению лабораторий, ужесточению требований к аттестационным органам, что привело к определенному переделу рынка защиты информации. Требования к аттестации дополняются требованиями необходимости специальных проверок, обследований помещений и проведения экспертиз объектов защиты на противодействие иностранным техническим разведкам.

В начале 2008 года существенно пополнилась нормативная база по технической защите персональных данных в автоматизированных системах (АС). В феврале 2008 года приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 утвержден «Порядок проведения классификации информационных систем персональных данных». ФСТЭК России подготовила «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Документ был разработан на основании Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Существенно, что в перечисленных документах обоснован комплекс мероприятий по обеспечению безопасности персональных данных в ИС, который предлагается проводить на основе результатов оценки опасности угроз и определения класса ИС персональных данных. При этом определены мероприятия по:

1. Выявлению и закрытию технических каналов утечки персональных данных в ИС персональных данных на основе анализа и оценки угроз безопасности персональных данных;
2. Защите персональных данных от НСД и неправомерных действий:
 - ✓ Управление доступом;
 - ✓ Регистрация и учет;
 - ✓ Обеспечение целостности (преимущественно ОС и СУБД);
 - ✓ Контроль отсутствия недеklarированных возможностей (в большинстве случаев на базе СУБД, СЗИ, антивирусных средств защиты информации);
 - ✓ Антивирусная защита;

- ✓ Обеспечение безопасного межсетевого взаимодействия ИС персональных данных;
 - ✓ Анализ защищенности;
 - ✓ Обнаружение вторжений.
3. Установке, настройке и применению средств защиты.

Существенно, что тем самым “легализовались” средства защиты от вирусов и вредоносных программ, а также средства анализа защищенности и системы обнаружения вторжений, которые до этого не имели четко сформулированных требований и соответствующих руководящих документов.

В 2007 – 2008 гг. году можно отметить следующие основные вехи

1. Март 2007 г. – вступил в силу N 152-ФЗ "О персональных данных"
2. 17 ноября 2007 г. - Постановлением Правительства Российской Федерации N 781 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
3. 29 декабря 2007 г. - Постановление Правительства Российской Федерации N 957 "Об утверждении Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами"
4. 9 января 2008 года Приказ министра Мининформсвязи №1 "Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации".
5. 17 марта 2008 Указ Президента РФ N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
6. Методические документы, необходимые для выполнения требований, предусмотренных Положением, утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007г. №781 (подготовлены ФСТЭК России во исполнение пункта 2 постановления, утверждены 15 -18 февраля 2008 г.)
 - ✓ Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных
 - ✓ Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных
 - ✓ Основные мероприятия по организации и техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
 - ✓ Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
7. Ряд закрытых документов ФСБ

Отдельно необходимо отметить, что в 2007 году продолжилось развитие деятельности Банка России по повышению уровня информационной безопасности как самого Банка, так и организаций банковской системы Российской Федерации на

основе серии стандартов “Обеспечение информационной безопасности организаций банковской системы Российской Федерации”. Большинство из стандартов носят рекомендательный характер и сформировались как лучшая практика соответствующих профессиональных сообществ и организаций. Практическая ценность названных стандартов заключается в значительной экономии ресурсов при разработке нормативных документов безопасности компаний.

Также нужно подчеркнуть, что в 2008 году в структурах министерства здравоохранения постепенно началось прорабатывание вопроса введения стандарта защиты информации, аналогичное американскому HIPAA (Health Insurance Portability and Accountability Act). Можно ожидать, что первые документы появятся не ранее 2009 года, поэтому пока рано говорить о том, что именно будет использоваться.

Развитие новых систем ИБ

DLP системы

Самым быстрорастущим новым сегментом рынка является DLP (Data Leak Prevention). Но, как всякий новый рынок, DLP еще до конца не структурирован. Разные компании и вендоры понимают под ним совершенно разные решения. Об этом говорит и тот факт, что иногда этот сегмент называют ILDP (Information Leak Detection and Prevention), а недавно IDC ввело новый термин IPC (Information Protection and Control). Но, по сути, все системы, которые попадают под это определение, выполняют одну главную функцию - защищают от утечек данных по различным каналам.

LETA предлагает следующее определение Системы защиты от утечек данных: автоматизированное средство, позволяющее распознавать и/или блокировать перемещение конфиденциальной информации за пределы защищаемой информационной системы по всем каналам, используемым в повседневной работе. В дальнейшем будет использоваться аббревиатура DLP, как наиболее часто применяемая.

При анализе описания данного сегмента необходимо подчеркнуть, что к DLP при определенных обстоятельствах могут относиться и следующие смежные системы:

1. системы управления правами
2. системы мониторинга и архивирования почтовых сообщений
3. решения по контролю операций с внешними устройствами
4. контроль над перемещением содержания полей баз данных,
5. мониторинг SQL- запросов к базам данных.

Также тенденцией последнего времени стало включение в DLP криптографических средств. Например, это сделали InfoWatch с продуктом InfoWatch CryptoStorage. Также криптография используется в продуктах VONTU, McAfee. В результате при

определении объема рынка необходимо учитывать и часть криптографических средств.

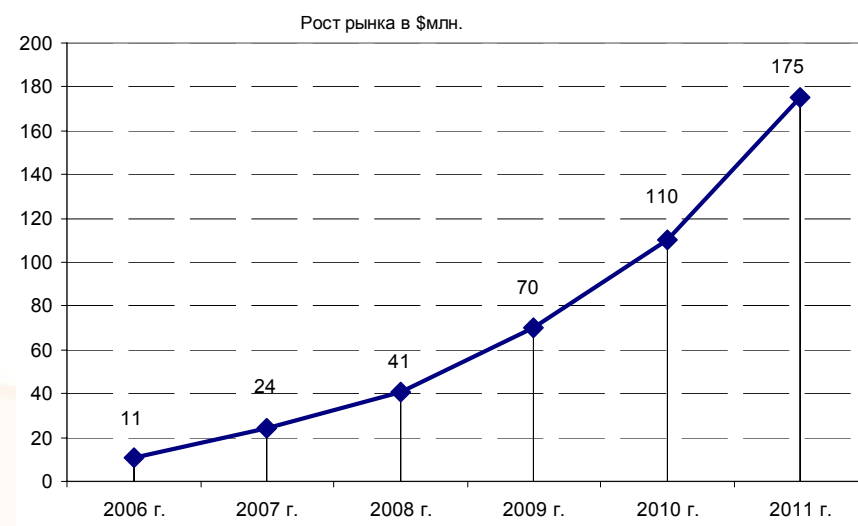
На начало 2008 года в России лидером рынка в денежном выражении являлась российская компания InfoWatch со своими продуктами. Но эта ситуация в ближайшие несколько лет может измениться. Уже сейчас в России представлены и начали продаваться продукты компании Websense, McAfee. В середине 2008 года ожидается появление в России VONTU. Конкуренцию сможет поддержать еще один российский разработчик - Perimetrix (ведущие менеджеры ранее работали в InfoWatch). Таким образом, на этом рынке ожидается серьезная борьба. Тем более, что потребление подобной системы будет расти большими темпами.

Интересно отметить, что пока именно на рынке DLP наибольшую долю составляют консалтинговые услуги.

На рост рынка будут влиять следующие факторы:

1. Развитие нормативной базы:
 - а. выход инструкций ФСБ и ФСТЭК о применении положений закона о защите персональных данных;
 - б. продвижение Стандарта ЦБ РФ СТО БР ИББС-1.2-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».
2. Переход управления задач борьбы с инсайдерами от ИТ к Управлению рисками для бизнеса
3. Выход компаний на IPO за пределами России требует соответствие требований SOX и прочих норм.

Рост рынка DLP



Источник: LETA

Системы комплексной безопасности

Вторым перспективным рынком может стать рынок систем комплексной безопасности.

Системы комплексной безопасности – вполне прогнозируемая эволюция разрозненных ИБ-решений, объединяемых вендорами под централизованным, а главное, унифицированным центром

управления; в различных сочетаниях подобные продукты содержат межсетевой экран, антивирусное и антишпионское ПО, средства контроля политики доступа, криптосредства защиты конфиденциальных документов, подсистемы журналирования действий сотрудников, средства контроля за доступом к внешним портам рабочих станций, беспроводным сетям и т.п. О выпуске подобных комплексных решений либо работе в этом направлении заявило большинство игроков рынка продуктов ИБ. Главной особенностью данных систем является централизованное управление событиями ИБ, сбор и анализ событий ИБ.

Но пока они не получили в России большого распространения. Большинство российских компаний не готовы к их внедрению. Также в профессиональном сообществе до конца не сформировалось отношение к данным системам; против их использования выдвигается довольно большое число аргументов.

Но можно ожидать, что через два-три года именно данные системы станут «хитами» на рынке ИБ.

Применение «экономического» подхода

2007 год подтвердил тенденции того, что все больше компаний начинают задумываться о стоимости информации, а значит, и о стоимости ее защиты.

При первоначальном построении систем ИБ клиенты и поставщики решений ориентировались, в первую очередь, на построение инфраструктуры защиты. Решались, прежде всего, технические проблемы.

Но, все большее число организаций при построении ИБ-систем компании уже ориентируются не на инфраструктуру, а на соответствие ИТ бизнес-задачам и бизнес-процессам в организациях. Используется так называемый «экономический» подход.

Под «экономическим» подходом понимается ориентация на экономическую отдачу. То есть все действия должны быть прозрачны и экономически оправданы. При этом используется взвешенная система оценки проектов, основанная на принципах возврата инвестиций и управления рисками.

На рынке ИБ в 2005–2006 годы также начались проекты, ориентированные на «экономический» подход. В 2007 году их стало еще больше. Клиенты начинают понимать такие термины, как ROI (Return on Security Investment — оценка эффективности инвестиции в безопасность)³ и KPI (Key Performance Indicator) систем безопасности.

В 2008 году все большее число потребителей придет к пониманию новых подходов. Во многом это будет связано с общими изменениями в работе российских организаций, где уже сейчас «экономический» подход де-факто является стандартом для большинства бизнес-единиц, в том числе, и для ИТ. Так как отношение к безопасности в целом, и к ИБ в частности, — самое

³ Подробнее о расчете ROI см. исследование "[Основные тенденции в области защиты конфиденциальных данных от утечки информации ILDP на российском рынке](#)"

консервативное, то и новые подходы будут внедряться самыми последними. Но следует отметить и недостаточность знаний среди ИТ и ИБ персонала по данной тематике. Многие слышали об этих подходах, но, в силу необученности, не знают где, как и что применять. Тем не менее, данный подход стал одинаково применяться как в больших компаниях, так и в SMB секторе.

В результате сами поставщики решений в области ИБ уже ориентируются в своих материалах не только на свой технический функционал, но и на то, насколько экономически выгодно использовать данную систему.

Также и к компаниям-интеграторам заказчики стали предъявлять новые требования – экономический расчет проектов по ИБ. Но пока подобным опытом обладает только ряд специализированных компаний в области ИБ.



Легализация и развитие применения средств ИБ

Рынок антивирусных средств

Рынок антивирусных средств (АВЗ) - традиционно наиболее крупный сегмент на рынке информационной безопасности. За лидерство именно на нем идет сражение между российскими и международными вендорами.

Но, к сожалению, достоверных данных по продажам антивирусных средств нет. Во многом это связано с особенностью российского рынка, а именно, наличием крупных отечественных вендоров. Если западные компании сотрудничают с исследовательскими организациями, то отечественные компании долгое время адекватно не раскрывали статистику своих продаж. Впрочем, ситуация начала постепенно меняться. По данным совместного исследования с IDC, объем рынка антивирусов в конечных ценах по данным вендоров составляет \$140 млн, а по данным дистрибуторов - \$90-100 млн. Эта оценка была сформирована и посчитана по методологии IDC. Мы считаем методологию расчета не совсем корректной, что косвенно подтверждается существенным расхождением в расчетах.

Основная проблема этой оценки заключается в том, что и сами вендоры не обладают информацией о своих канальных продажах. Досконально вендор знает собственные продажи, знает продажи дистрибуторов. Но именно эти данные и не разглашаются. Также есть проблема того, что часть денег не учитывается дистрибуторами. В результате нельзя пересчитать рынок и через дистрибуторов, хотя именно это оценка и может быть наиболее близкой к истине.

Брать же данные по рынку, которые озвучивают вендоры, в том числе, данные IDC по продажам через дистрибуторов, неправильно потому, что не учитываются следующие аспекты:

- ✓ Прямые поставки вендора крупным корпоративным клиентам и OEM-партнерам
- ✓ Легальные госконтракты, в которых «специальная» низкая цена делает цену за рабочее место существенно ниже публично объявленной стоимости
- ✓ Отдельно надо понимать, что в крупных гостендерах невозможно определить стоимость различных составляющих одного лота, соответственно погрешность расчетов может составлять до 50%
- ✓ OEM-поставки, в которых контракт заключает иностранный производитель АВЗ с иностранным производителем ПК и ноутбуков. Но при этом сами ПК продаются в России
- ✓ OEM-поставки или поставки в ритейл, в которых существенная часть цены возвращается продавцу, например, через обязательный маркетинговый фонд

- ✓ Контракты с ISP, мобильными операторами, интернет-порталами (пример: Dr Web и Corbina, Лаборатория Касперского и МТС, Яндекс). В данном случае непонятно как считать конечную стоимость для клиента, ведь вендор передает свой продукт бесплатно или условно-бесплатно.

Все эти факторы ставят под сомнение те цифры, которые объявляют российские вендоры. Второй классический метод оценки рынка - это расчет денег, которые были потрачены конечными пользователями. То есть расчет объема рынка идет не со стороны производителя, а со стороны потребителя. Сами производители ориентируются на эти цифры, а не изобретают свои. Для этого есть специальные методики, прежде всего, так называемые «панельные исследования». Но таких исследований по рынку антивирусов не проводилось. Поэтому для оценки рынка аналитики LETA использовали схожую модель, которая основывается на оценке затрат пользователей на антивирусные средства.

Для правильной оценки затрат на АВЗ нужно знать:

- ✓ число ПК;
- ✓ средние затраты на АВЗ на один ПК в год;
- ✓ уровень пиратства.

Все данные взяты из достоверных и проверенных источников и публично доступны.

По данным IDC и Мининформсвязи, общее количество ПК в России в 2007 году составило 31,2 млн. штук. При этом распределение по потребителям следующее:

Таблица 4. Общее количество ПК в России

Всего ПК	31 200 000
У населения	14 000 000
Корпоративный сектор	17 200 000

Источник: LETA

По данным НЭСТ и Business Software Alliance, уровень пиратства у домашних пользователей находится на уровне 85%, в корпоративном секторе - 65%. Также нужно учитывать, что около 10% домашних пользователей используют бесплатные программы; в корпоративном секторе таких 1%.

Таким образом, можно получить цифру: сколько ПК используют платный антивирус. (в расчете учтены и затраты на серверные продукты).

По экспертным оценкам, домашний пользователь тратит на АВЗ 30 долларов в год (с учетом продлений), а корпоративный – 15 (в расчете учтены и затраты на серверные продукты). Но необходимо учитывать, что в среднем 30% всех типов пользователей покупают «комбайны». И затраты на антиспамы, файрволы также необходимо учитывать при анализе данных рынков. В результате весь антивирусный рынок составляет 110 млн. долларов, что составляет 36% от рынка ПО в области безопасности.

При этом, если подобную методику экстраполировать на предыдущие годы, то разница между двумя подходами останется 40%. Нам представляется, что оценка финальных затрат пользователей в 110 млн. более адекватна.

Вне зависимости от разных оценок, можно выделить тройку лидеров:

Таблица 5 Тройка лидеров на рынке антивирусных средств

Лаборатория Касперского
ESET
Symantec

Источник: IDC

В ближайшие несколько лет предстоит борьба за лидерство на этом рынке.

Усложнение задач, решаемых ИБ.

Первоначально при построении систем информационной безопасности организации ориентировались на защиту периметра, и в ее рамках делали упор на антивирусную защиту. Однако укрупнение бизнеса и появление новых видов угроз требует усложнения защиты, внедрения новых программных и аппаратных средств. Все острее в последние годы встает вопрос защиты от внутренних угроз.

Таким образом, в оборот входят все новые продукты, которые требуют внедрения и сопровождения, что также влияет на рост рынка. Организации, уже создавшие ИТ-инфраструктуру, начинают внедрение более серьезных средств, защищающих ранее незащищенные области.

Тенденции развития угроз информационной безопасности со стороны внешних воздействий

С середины 2006-го года специалисты в области ИБ начали озвучивать весьма серьезное и пугающее наблюдение: текущий период является переломным в развитии угроз информационной безопасности – процесс меняет свой характер с экстенсивного пути на интенсивный. 2007-ой год не только подтвердил прогнозы, но и продемонстрировал эти тенденции в полном объеме.

При практически не изменившихся с 2006-го года количественных показателях (как по объему найденных уязвимостей, так и по количеству опубликованных инцидентов в области ИБ), сложность методик реализации атак, схем воздействий на основе социальной инженерии, алгоритмов централизованного управления возросла чрезвычайно. Некоторые зарубежные аналитики оценивают рост черного рынка киберпреступности в 2007-ом году в цифры от 70% до 200%.

Основными целями злоумышленников в зафиксированных инцидентах стали:

- ✓ инсталляция на сервера и рабочие станции элементов управляемого вредоносного кода (в т.ч. на WWW-серверах – с целью дальнейшего распространения за счет подключающихся к серверу абонентов);
- ✓ вывод из строя онлайн-сервисов компаний либо каналов передачи данных к ним (атаки класса "переполнение буфера", "DDoS – распределенный отказ в обслуживании", получение привилегий администратора сервера с дальнейшим отключением сервиса и др.);
- ✓ идентификационные данные к ресурсам различного рода (серверам электронной почты, служб мгновенных сообщений, WWW-серверов интернет-банкинга, онлайн-игр, социальных сетей и т.п.).

Кроме того, нельзя не упомянуть стремительный рост за рубежом количества инцидентов, связанных с кражами или распространением в результате неумышленного раскрытия массивов персональных данных, что, очевидно, связано с формированием в этих странах коммерческого спроса на эту информацию.

Аналитики компании LETA составили обзор тенденций в технической составляющей компьютерных атак и средствах защиты информации, разрабатываемых в настоящее время.

Развитие бот-сетей

Практически все исследователи называли 2007-ой "Годом бот-сетей". Несомненно огромное и даже пугающее по некоторым оценкам проникновение во всех секторах ИТ (государственном, коммерческом, образовательном, личном), десятки волн спам-рассылок, вскрытые антивирусными специалистами, подробности о механизмах управления бот-сетями – всё это заставило

признать проблему бот-сетей одной из двух ключевых на сегодняшний день.

Ключевыми качественными изменениями в технологиях бот-сетей стали:

- ✓ появление схем децентрализованного управления (отсутствие центрального управляющего компьютера не позволяет ИБ-специалистам после дизассемблирования кода отключить сеть путем его изоляции);
- ✓ разделение бот-сетей, даже построенных на основе одного и того же вредоносного кода, на независимые сегменты с отдельными серверами и ключами управления, что также усложняет их обнаружение и уничтожение;
- ✓ увеличение доли вредоносного кода с управлением по протоколам и схемам, наиболее схожими с легитимным трафиком (например, посредством HTTP-запросов в псевдослучайные моменты времени к хаотично, на первый взгляд, расположенным WWW-серверам, что чрезвычайно затрудняет их обнаружение на корпоративных прокси-серверах).

Качественные изменения, по свидетельствам специалистов, произошли и в самом underground-сообществе. Так, именно в прошлом году были опубликованы некоторые факты о чрезвычайно активной коммерциализации рынка бот-сетей. Их сегменты покупаются и продаются, сдаются в аренду (при этом на базе автоматизированных методик оплаты), им поручаются специфические задания "по желанию клиента" (т.к. практически все активно распространившиеся на сегодня популяции обладают возможностями загрузки дополнительного кода с центров управления).

Борьба с бот-сетями на сегодняшний день возможна как на стороне компьютеров конечных пользователей, так и на границе периметра. Однако всё усиливающееся стремление разработчиков маскировать трафик обмена с центром управления, ускоренное развивающейся внутренней конкуренцией, позволяет прогнозировать освоение бот-сетями моделей поведения, всё более близких по своим характеристикам к действительно случайным, а также переход на управление с элементами стеганографии. Если данная тенденция воплотится на практике, то это приведет к еще большему смещению акцента в борьбе с бот-кодом на сторону компьютеров конечных пользователей.

Скрытность вредоносного ПО

Активная коммерциализация компьютерного underground-а закономерно привела к еще одной специфической черте, проявившейся в последнее время: смещение ориентиров основной массы вредоносного ПО на как можно большую скрытность в зараженной системе. Действительно, чем дольше проживет код на компьютере жертвы, тем большую денежную сумму получит его владелец с одного факта успешного заражения.

Всё большее проникновение в троянские программы получает технология руткитов, позволяющая скрывать свое присутствие в системе от типовых методик сканирования. Постоянно демонстрируются новые схемы размещения вредоносного кода и методик перехвата системных функций. Появились сообщения о возрождении на новом витке эволюционной спирали загрузочных вирусов, совмещенных с руткитами, что позволяет им, загружаясь до операционной системы Microsoft Windows, получить несравнимые возможности по маскировке своего присутствия в системе. Сразу несколько ведущих антивирусных компаний назвали буткиты (экземпляры, реализующие данный подход) одним из возможно наиболее опасных классов вредоносного кода в ближайшие два года.

Высокотехнологичные методы проникновения, всё чаще реализуемые во вредоносном коде, приведут к очередному витку противостояния умов "черных шляп" и профессионалов-разработчиков антивирусного ПО, и, возможно, – к некоторому перераспределению весов на рынке антивирусного ПО. Потребителю в данной ситуации остается роль "наблюдателя с правом выбора".

Угрозы для мобильных устройств

Стремительное распространение персональных мобильных устройств с функционалом, сравнимым с персональными ПК пятилетней давности, всеобщая "мобилизация" пользователей привела сначала к плавному стиранию грани между офисным ПК, мобильным устройством и домашним компьютером (чье место всё чаще занимает ноутбук), а затем, вполне закономерно, к взрывному росту инцидентов, связанных с потерями и кражами конфиденциальной информации. В статистику потерь попадают адресные книги, корпоративные базы данных, личная и деловая переписка, электронные дневники, пароли доступа, сохраненные в клиентском ПО.

Причинами заметно ощущаемого отставания темпов внедрения средств защиты данных на мобильных устройствах от объективно требуемой скорости, следует назвать:

- ✓ консерватизм пользователей ("это" может случиться с кем угодно, но только не со мной – зачем себя утруждать какими-то паролями);
- ✓ недостаток унифицированных удобных в использовании технических решений;
- ✓ отсутствие во многих компаниях технических и организационных мер контроля за мобильными устройствами сотрудников (возможно, частично объясняемое тем, что именно здесь проходит граница между корпоративным и личным, а, следовательно, противодействие со стороны конечных пользователей максимально велико).

Сегмент средств контроля за мобильными устройствами продолжит свой рост. При нынешнем уровне проникновения мобильных устройств в повседневную жизнь противодействие

служб ИБ их использованию для различных рабочих задач, например, сотрудниками уровня начальников подразделений или руководства компаний, будет встречать всё большее непонимание. Кроме того, любая попытка внедрения или активации в мобильных устройствах того или иного защитного ПО будет оцениваться владельцами, в первую очередь, с позиций того, насколько сильно это "затруднит им жизнь". Как следствие, можно прогнозировать рост заинтересованности в области:

- ✓ разноплановых программных и аппаратных средствах защиты информации, хранимой и обрабатываемой на мобильных устройствах (в первую очередь прямо или косвенно основанных на криптографических схемах);
- ✓ средств контроля копирования классифицированной информации на отчуждаемые носители и внешние мобильные устройства;
- ✓ систем стойкой аутентификации и авторизации пользователей, доставляющих минимальные неудобства владельцу, например, токенов (USB-крипточипы) и биометрических (встраиваемые в мобильные устройства сканеры отпечатков пальца) и др.

Новые технологии воздействия и поиск новых уязвимостей

В 2007-ом году активно развивалось 3 вектора поиска уязвимостей:

- ✓ под прицелом оказалось офисное программное обеспечение (так, уязвимости уровня "Критичная" были найдены в Lotus Notes, Adobe Reader, а также в нескольких продуктах Microsoft Office, в т.ч. как общие для всего семейства, так и специфичные отдельно для Microsoft Access и Microsoft Excel);
- ✓ WWW-приложения сохранили темпы снабжения злоумышленников уязвимостями: по - прежнему по различным методикам подсчета на них приходится порядка 60%-80% уникальных сообщений об уязвимостях (хотя на практике такая высокая доля нивелируется малой распространенностью тех или иных уязвимых скриптов и кода);
- ✓ появилось новое, активно развивающееся направление – поиск уязвимостей в программном обеспечении, призванном защищать информацию; уязвимости были обнаружены в широко распространенных продуктах Symantec, TrendMicro, Cisco Systems, BitDefender, Clam Anti-Virus, Eset; при этом, если ранее злоумышленники ставили целью только вывод защитного ПО из строя, то в прошедшем году на первое место вышли уязвимости, приводящие к исполнению кода, а, следовательно, сами открывающие вредоносному коду вход в систему.

Непрекращающийся поток уязвимостей, которые, похоже, присущи всем классам программного обеспечения (в т.ч. даже изначально проектируемым как средства защиты) заставит производителей ПО совершенствовать системы автоматического обновления кода (в т.ч.

экстренного и, возможно, принудительного), а потребителей – во-первых, внедрять подобные подсистемы в своих сетях, а во-вторых, обращать всё большее внимание на системы инвентаризации и централизованного управления ПО в сети.

Среди новых технологий несанкционированного воздействия на компьютерную технику, впервые продемонстрированных либо заметно увеличивших частоту инцидентов в 2007-ом году, следует отметить:

- ✓ внедрение вредоносного кода в программное обеспечение с открытым программным кодом на этапе сборки, либо обновления версий, либо формирования/доставки модулей расширения (add-ons);
- ✓ взлом пароля экранной заставки в ОС Windows XP путем подключения внешнего FireWire-устройства (реализация драйвера протокола FireWire в ОС Windows предоставляет ему доступ к любой области памяти по запросу, что позволяет злоумышленнику с помощью специализированного ПО на внешнем устройстве найти программный код экранной заставки и отключить условный переход, проверяющий корректность введенного пароля, либо использовать другие технологии ее обхода);
- ✓ неоднократно наблюдавшиеся факты построения эксплоитов к программному обеспечению (в т.ч. ОС Microsoft Windows XP) на основе анализа программного кода обновления безопасности, закрывающего ту или иную уязвимость, что заставило нескольких исследователей ИБ призвать разработчиков ПО к совершенствованию процесса выпуска обновлений;
- ✓ методики выхода из виртуальной машины за счет ошибок в программном коде систем виртуализации, что позволяет злоумышленникам получить управление над сервером в целом и, как следствие, над всеми управляемыми им виртуальными компьютерами;
- ✓ наблюдавшиеся в нескольких странах случаи установки фальшивых WiFi точек доступа (хот-спотов) с целью кражи идентификационной информации (имена, пароли, cookies) к онлайн-сервисам на этапе передачи их между мобильным устройством и сетью Интернет.

Это далеко не полный список возможных новых технологий воздействий, но, по нашему мнению, приведенные выше имеют наибольшую опасность. В следующих исследованиях мы увеличим список угроз.

Компания LETA продолжит исследование российского рынка информационной безопасности. В дальнейшем будут выпущены исследования как по отдельным сегментам, так и по рынку в целом (2009 год). LETA IT-company надеется, что эти исследования, которые компания готовит для себя, будут востребованы всеми участниками ИТ и ИБ рынка.