

Презентация исследования

Рынок информационной безопасности: Эпоха кризиса.

Москва, 2009

Об исследовании

LETA IT-company представляет третий экспертный отчет «Рынок информационной безопасности: Эпоха кризиса». Первый отчет был выпущен в начале 2007 года, второй в середине 2008 года и многие оценки этих исследований 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
ОСНОВНЫЕ ХАРАКТЕРИСТИКИ РЫНКА ИБ.....	5
ОБЪЕМ РЫНКА ИБ	5
СТРУКТУРА ПОТРЕБЛЕНИЯ СРЕДСТВ ИБ.....	9
ОСНОВНЫЕ ИГРОКИ НА РЫНКЕ ИБ	12
УГРОЗЫ БЕЗОПАСНОСТИ В 2008 - 2009 ГОДАХ	14
ТЕХНИЧЕСКОЕ НАПРАВЛЕНИЕ	14
НАПРАВЛЕНИЕ «СОЦИАЛЬНОЙ ИНЖЕНЕРИИ»	17
ЦЕЛИ АТАК	18
ИТОГИ И ПРОГНОЗЫ РАЗВИТИЯ УГРОЗ	19
РАЗВИТИЕ РЕГУЛИРОВАНИЯ РЫНКА ИБ	20
РАЗВИТИЕ НАЦИОНАЛЬНЫХ СТАНДАРТОВ	20
ИСПОЛНЕНИЕ ФЗ РФ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»	21
ПЕРСПЕКТИВЫ СТАНДАРТИЗАЦИИ БАНКА РОССИИ	27
ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ МЕЖДУНАРОДНЫХ СТАНДАРТОВ	29
ПРИМЕНЕНИЕ «ЭКОНОМИЧЕСКОГО» ПОДХОДА	30
РАЗВИТИЕ НЕКОТОРЫХ СЕГМЕНТОВ СРЕДСТВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ.....	32
РЫНОК АНТИВИРУСНЫХ СРЕДСТВ	32
СИСТЕМЫ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ	34
DLP СИСТЕМЫ	35
ДРУГИЕ ТЕХНИЧЕСКИЕ СЕГМЕНТЫ РЫНКА ИБ	39

Список иллюстраций

Таблица 1. Основные сегменты потребления средств ИБ в %	10
Таблица 2. Ранкинг (по алфавиту) российских компаний, продвигающих услуги в области ИБ.....	13
Таблица 3. Сертифицированные СУИБ на начало 2009 года	29
Таблица 4. Тройка лидеров на рынке антивирусных средств	32
Таблица 5. Краткое описание самых распространенных в России DLP систем	37
Рисунок 1 Структура «открытого» рынка ИБ в \$млн.	8
Рисунок 2. Потребители ИБ в %	10
Рисунок 3. Доли игроков на рынке в %	12
Рисунок 4. Рост рынка DLP в \$млн.	39

Основные выводы

1. Рынок информационной безопасности пострадал от кризиса меньше всех остальных сегментов ИТ рынка. Рынок информационной безопасности еще раз доказал, что безопасность во всех своих проявлениях остается базовой потребностью, даже если это касается информационных технологий.
2. Объем рынка в 2008 году составил \$581 млн. В целом рост рынка в ближайшие два года будет сохраняться на уровне 25 - 30%
3. На рост рынка в условиях кризиса влияет: возникновение новых угроз, требования регуляторов, требования партнеров, выход ИБ из прикладной дисциплины на уровень бизнеса.
4. Структура потребления средств ИБ не претерпела существенных изменений.
5. Рынок ИБ обладает в условиях кризиса самой большой инвестиционной привлекательностью. И именно в нем можно ожидать крупнейшие M&A сделки
6. В качестве объектов атак из области офисного ПО лидирующее место по-прежнему с большим отрывом занимают продукты компаний Microsoft и Adobe
7. Доля удаленных уязвимостей в сетевом ПО снизилась, уступив место браузерным уязвимостям и уязвимостям в офисном ПО
8. Социальные сети стали основным местом действия для методов социальной инженерии.
9. В 2008 – 2009 году усилилась роль регулирующих органов и был выпущен ряд стандартов.
10. Исполнение ФЗ РФ «О персональных данных» будет основным двигателем рынка в 2009 – 2010 годах
11. В 2008 – 2009 годах ожидается фактическое отсутствие применения серии стандартов ISO 27001.
12. Объем рынка АВЗ в России в 2008 году составил \$175 млн. «Лаборатория Касперского» и ESET в сумме контролируют более 80% продаж в ритейле. Лаборатория Касперского, ESET, Symantec, DrWeb контролируют до 80% от всего рынка АВЗ.
13. На конец 2008 года в России лидером рынка DLP являлась InfoWatch (около 50% всех внедрений). Но эта ситуация в ближайшие несколько лет может измениться. Уже сейчас в России представлены и начали продаваться продукты компании Websense, McAfee и мирового лидера Symantec DLP (Vontu), на западные решения с начала года приходится подавляющая часть новых продаж и внедрений.
14. Лидерами рынка сетевой безопасности остаются Cisco, Check Point и Microsoft. Остальные решения, которые в мире имеют существенную долю рынка, в России занимают незначительные доли.

Основные характеристики рынка ИБ

Объем рынка ИБ

В начале 2008 года рынок информационной безопасности продолжил свой рост (как и в 2007 году, его рост значительно опережал рост рынка ИТ), затем наступил резкий спад, связанный с кризисом. Но падение во второй половине было не столь жестким, как у всего ИТ рынка.

Рынок информационной безопасности еще раз доказал, что безопасность во всех своих проявлениях остается базовой потребностью, даже если это касается информационных технологий. И в условиях нестабильности безопасность последнее, чем может пожертвовать организация, а учитывая, что ИТ стали важнейшей частью любой организации, то и затраты на защиту информационных технологий остались важнейшей статьей в бюджетах организаций и частных пользователей.

2008 год стал годом состоящим из двух не равных частей: до сентября и после сентября. Поэтому, рассматривая любой рынок, необходимо понимать, что тенденции, работавшие в первой половине года и объяснявшие происходящее на рынке, во второй половине года кардинально поменялись. Но именно тенденции второй половины года, то есть кризиса, будут определять движение рынка в краткосрочной и среднесрочной перспективе.

На тенденции второй половины 2009 года и будет сделан основной упор в данном исследовании.

До середины 2008 года рынок ИБ оставался одним из самых быстрорастущих сегментов российского ИТ рынка.

До сентября рост рынка ИТ составлял 20% в годовом измерении, а рост рынка ИБ составлял до 70% годовых. На этот рост влияли, прежде всего, следующие факторы:

1. Рост экономики, а значит рост потребления средств ИТ, как в домашнем сегменте, так и бизнес и гос. структурах
2. Легализация. Это, прежде всего, касается средств антивирусной защиты.
3. Требования регуляторов и усиление их роли, появление обязательных (закон о персональных данных) документов и квазиобязательных: стандарт ЦБ, рекомендации ФСТЭК. Также следует отметить, что гос. структуры с середины 2000 – х стали обращать свое пристальное внимание на рынок ИБ. К категории квазиобязательных можно отнести и стандарт PCI DSS.
4. Требования партнеров, мировая тенденция, пришедшая к нам с опозданием в несколько лет, когда партнер, защитив данные у себя, передавая свои конфиденциальные данные (например, персональные данные), должен быть уверен, что у другой организации они будут защищены не хуже, чем у него. На эту тенденцию отвечает во многом серия стандартов ISO – 27 00X. За последние несколько лет интерес к сертификации по этому стандарту сильно увеличился. А сама сертификация помимо, внедрения организационных требований, приводит к тому, что в компании внедряются новые ИТ средства

5. Повышение доступности ИБ: технологии стали более понятными и значит более доступными, прежде всего, для малых и средних компаний.
6. Развитие технологий, появление новых решений. За 10 лет появился ряд новых классов решений (NAC, DLP, compliance, антивирусные «комбайны» и т. д.), и эти решения стали широко известны.
7. Проникновение ИБ на уровень бизнеса. Так как ИТ стали фактически кровеносной системой современного бизнеса, сейчас трудно найти компанию, которая бы не использовала хотя бы почту. Поэтому и защита этих критических для бизнеса систем стала задачей не просто для неких абстрактных «айтишников» или «ибешников», а для руководителей бизнес-уровня
8. Активная рекламная политика производителей. Не секрет, что производители средств ИБ тратили значительные средства на рекламу, в том числе, и на излишнее «запугивание» клиентов. Это позволяло поддерживать высокий уровень продаж
9. Возникновение новых угроз. Действительно, за последние годы возникли новые угрозы, с которыми компаниям необходимо бороться, а чаще всего это означает увеличение затрат на ИБ
10. Усложнение задач, решаемых ИБ. С ростом и с усложнением ИТ систем растут и затраты на ИБ.
11. Наличие у компаний свободных финансовых ресурсов, которые позволяли им экспериментировать с новыми технологиями. Многие компании в условиях, когда у них были средства, бессистемно закупали ИТ и ИБ средства, эти закупки не приводили к большей защищенности.

Из этого обширного списка видно, что на рост рынка ИБ влияли ни один, ни два, а большая группа факторов.

Но с началом кризиса многие из этих факторов потеряли свою актуальность, что привело к тому, что тенденция к росту рынка прекратилась. Но, тем не менее, рынок ИБ существует и даже развивается. Поэтому мы выделили ряд тенденций, которые и в условиях кризиса помогают рынку существовать и даже немного расти в рублевом исчислении.

1. Возникновение новых угроз. В условиях кризиса криминальные риски растут, а значит растут и затраты на преодоление этих рисков, но сами риски могут при этом меняться, возникают новые угрозы, или старые, которые были неактуальны становятся важными. Так, например, выросла угроза со стороны своего персонала. При его сокращениях и фактическом уменьшении доходов лояльность персонала падает, поэтому можно ожидать как факты саботажа, так и утечки конфиденциальной информации
2. Требования регуляторов и усиление их роли, появление обязательных (закон о персональных данных) и квазиобязательных документов. В условиях сокращения бюджетов на обязательные мероприятия деньги будут выделяться всегда.
3. Требование партнеров. Эта тенденция снизит свое влияние, но останется. Так как, несмотря на кризис, бизнесотношения не

прекратились, поэтому проблема «взаимного доверия» осталась. В условиях кризиса, когда взаимное доверие между участниками экономической деятельности сильно подорвано, фактор доверия на уровне передачи и хранения конфиденциальной информации наоборот возрастает. Для многих компаний информационная безопасность стала дороже денег.

4. Четвертой тенденцией, которая продолжит влиять на развитие рынка, останется то, что сейчас ИБ вышла из прикладной дисциплины на уровень бизнеса. В ИТ системе стали храниться и обрабатываться действительно важнейшие данные, необходимые для существования и выживания бизнеса. И бизнесу все равно придется защищать свои информационные системы, а значит тратить средства на ИБ.

Необходимо отметить, что первый испуг от кризиса и резкого сокращения бюджетов, который пришелся на конец 2008 года, быстро прошел, когда стало ясно, что кризис - это надолго. И в 2009 году компании под влиянием вышеперечисленных факторов возобновили финансирование ИБ, но конечно, в меньших объемах.

Но в условиях кризиса необходимо учитывать и тенденции, которые станут отрицательно воздействовать на рынок.

1. Общее снижение затрат для снижения бюджетов организаций на обслуживающие технологии, в том числе на ИТ и ИБ
2. Замедление легализации и обновления. Компании будут меньше тратить средств на развитие тех систем, которые уже работают.
3. Рост пиратства и рост использования «бесплатного ПО». Несомненно, в домашнем потреблении и в сегменте SMB снова начнет расти пиратство. Основной прирост - у домашних пользователей и в малом бизнесе. Задачи по защите ИТ никуда не денутся, но, в связи с сокращением затрат, у предприятий останется два выбора: или пиратство или «свободное» ПО.
4. Перераспределение работ от внешних организаторов к внутренним службам. Услуги интеграторов и внешних консультантов стали востребованы только в тех случаях, когда собственная ИТ и ИБ служба не может решить (не хватает компетенций или область регулируется нормативными документами)

Существует еще одна тенденция, влияние которой на рынок пока не ясно. Это тенденция – нацеленность компаний на защиту отдельных критически важных областей. Если до кризиса многие компании хотели полного обеспечения ИБ, то в условиях кризиса выбираются отдельные сегменты. В результате растет спрос на специализированные средства.

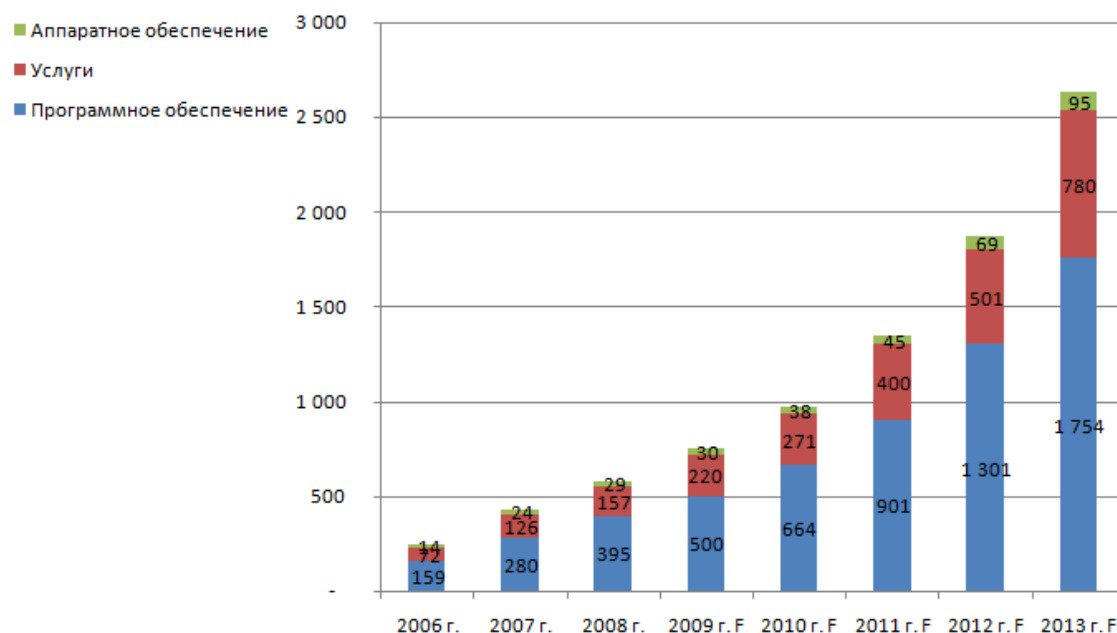
Но у каждой компании эти сегменты разные и общей тенденции пока не наблюдается, хотя есть большая вероятность, что во время кризиса будет выделено несколько направлений, которые и будут доминировать в последующие годы. По мнению IDC, такими направлением могут стать DLP, WAF, а такое направление, как защита баз данных наоборот практически уйдет с рынка. В результате, в зависимости от доли «прорывных» технологий, они или смогут положительно повлиять на рынок или, если их доля останется небольшой, их влияние не будет заметно, и рынок продолжит стагнировать.

Еще одной важной характеристикой рынка ИБ, которая не позволила ему упасть так глубоко, как рынку ИТ, является относительная краткость проектов. В среднем проект по ИБ не длится больше шести-семи месяцев (исключение только проекты по ISO 27001), что позволяет увидеть отдачу от него также в сжатые сроки. В результате ИБ проекты более прозрачны для компании, чем многие ИТ проекты

В исследованиях, проведенных 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 предыдущих исследований было выявлено существование «скрытого рынка» затрат на ИБ. В него входят пиратские затраты и иные затраты, не поддающиеся классификации. С учетом «скрытого рынка» затраты на ИБ в 2008 году составили чуть более \$1,1 млрд¹

Рисунок 1 Структура «открытого» рынка ИБ в \$млн.



Источник: LETA IT-company

¹ Подробнее о структуре «скрытого рынка» см. предыдущие исследования

Структура потребления средств ИБ

Несмотря на все изменения на конец 2008 и начало 2009 года основной моделью потребления остается самостоятельное внедрение систем ИБ. В первой, докризисной половине года, тенденция говорила о том, что все большее число организаций прибегает к услугам профессиональных ИБ компаний. Но с началом кризиса произошел откат к прежним позициям, как в средних, так и 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. И именно по проектам в крупных компаниях сильнее всего ударили кризисные явления. Многие проекты были или свернуты или остановлены. По нашим оценкам были «заморожены» в том или ином виде до 20% от всех реализуемых проектов.

Средние компании как были, так и остались сторонниками самостоятельных внедрений. Сами представители этих компаний объясняют это тем, что стандартный набор сервисов по ИБ могут оказать собственные сотрудники, которые и должны этим заниматься. В этом сегменте было заморожено до 30% проектов.

В результате основной причиной для большего и среднего бизнеса для развития ИБ систем стали законодательные требования и явные угрозы бизнесу.

Малые компании, к сожалению, также сократили свои затраты до 50%.

Но с окончанием кризиса можно спрогнозировать, что рынок не начнет с тех позиций, которые он занимал в середине 2008 года. Осознание того, что большую часть работ выгоднее перекладывать на профессиональные компании, уже никуда не уйдет. И с 2011 года можно ожидать, что рынок рывком перейдет в состояние, когда основные работы будут проводиться ИБ-компаниями.

Особо следует подчеркнуть, что в 2008 году резко вырос интерес к комплексным решениям, воплощенным в железе - appliance. Но пока этот интерес не перешел в потребление, хотя доля appliance решений на рынке выросла.

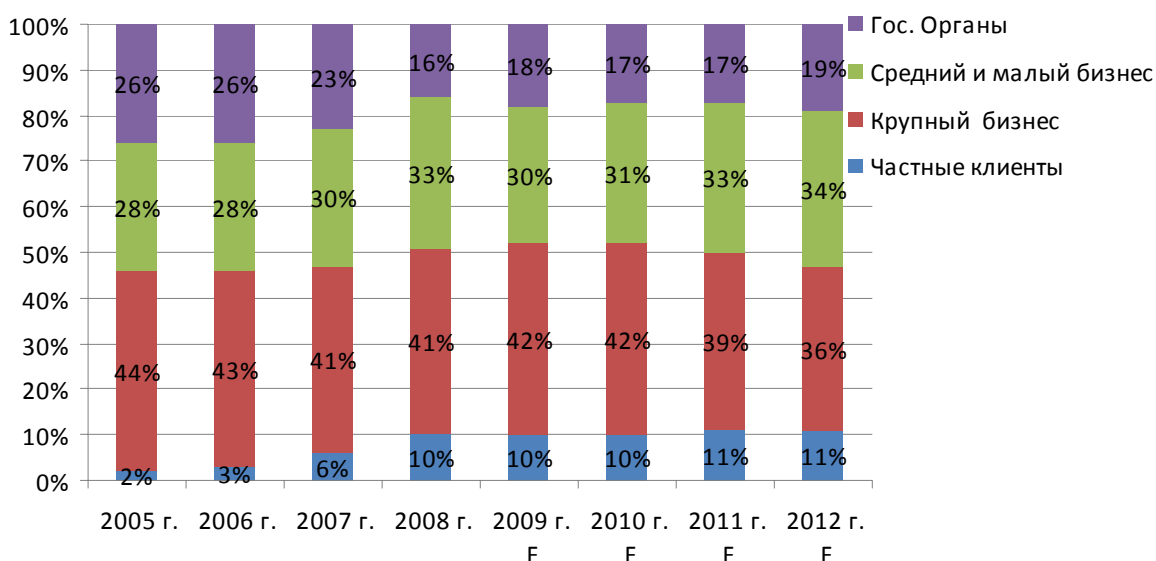
Такое преобладание продаж продуктов связано с тем, что пока рынок ИБ все еще консервативен. Многие организации, как коммерческие, так и государственные, воспринимают системы ИБ как наиболее критические, доступ к которым должен быть максимально ограничен. Поэтому не допускают к работе с ними внешних специалистов и внедряют все силами своих специалистов, то есть используют подход – «все делаем сами». В результате по итогам года доля услуг на рынке ИБ выросла не значительно, хотя развитие в первой половине года указывало на то, что доля услуг вырастет значительно

Таблица 1. Основные сегменты потребления средств ИБ в %

Сегменты	Доля	
	2008 г.	2009 г.
Всего программное обеспечение	68%	65%
Всего аппаратное обеспечение	5%	5%
Услуги	27%	30%

Источник: LETA, IDC

Рисунок 2. Потребители ИБ в %



Источник: IDC, LETA, РБК, PwC.

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

Но кризис немного переключил эту картину. Не произошло существенного роста доли сегмента SMB. Но при этом рост в первой половине года обеспечил общий рост частного потребления, хотя, конечно, во второй половине года рост существенно сократился

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 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 один из наименее «пиратских». 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 возможности противостоять эволюционирующим угрозам. Поэтому именно рынок средств защиты первым стал выходить из «тени».

Основные игроки на рынке ИБ

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.

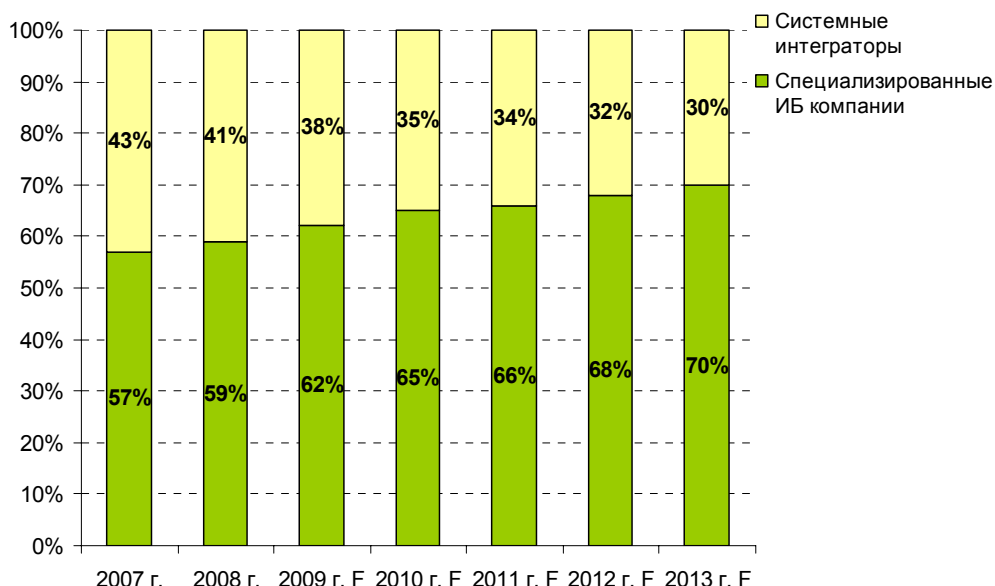
В результате, доля услуг на рынке ИБ будет стремиться к той доле, которую занимают услуги на корпоративном рынке ИТ. А это означает значительные поступления от консалтинговых услуг.

Это приводит к тому, что рынок стал привлекателен для большого числа игроков. В результате на рынке появилось большое число новых специализированных ИБ компаний, а также большинство «больших» и «средних» системных интеграторов открыли у себя ИБ подразделения.

При этом особенностью рынка является и то, что нельзя выделить компаний - технологических и идейных лидеров. Практически все ИТ-компании продают или внедряют средства защиты. На рынке нет компаний которые бы задали тон всему рынку. Это также дает дополнительные инвестиционные возможности для тех игроков у которых появятся действительно новые востребованные решения.

Инвестиционная привлекательность рынка должна была привести к началу M&A сделок, появлению больших компаний. Первой такой сделкой могло стать слияние компаний «ГК Информзащита» и ОКБ САПР, но эта сделка сорвалась. Тем не менее, следует ожидать, что в ближайшее время можно ожидать новых сделок.

Рисунок 3. Доли игроков на рынке в %



Источник: LETA IT-company

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 всех необходимых нормативных актов, стандартов и лицензий

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 (по алфавиту) российских компаний, продвигающих услуги в области ИБ

Название компании	
Интеграторы	Производители ПО
ICL-КПО	Agnitum
LETA IT-company	Dr.Web
TopS BI	InfoWatch
ГК Информзащита	Securit
Инфосистемы Джет	АНДЭК
Крок	ГК Информзащита
Ланит	Инфосистемы Джет
Орбита	Инфотек
УСП КомпьюЛинк	КриптоПро
Элвис-Плюс	Лаборатория Касперского

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» подходе см. исследование "[Основные тенденции в области защиты конфиденциальных данных от утечки информации ILDP на российском рынке](#)"

Угрозы безопасности в 2008 - 2009 годах

Как и в предыдущие годы, целью разработчиков вредоносного ПО в 2008 году было расширение сферы влияния. И, как и раньше, вектор усилий разделился на два основных направления: техническое и социальное. Следует, забегая вперед, отметить, что оба направления были честно "отработаны" и принесли ощутимые плоды и, по-видимому, немалые доходы хакерскому сообществу.

Техническое направление

В 2008 году наблюдались следующие основные тенденции эксплуатации уязвимостей:

1. доля удаленных уязвимостей в сетевом ПО снизилась, уступив место браузерным уязвимостям и уязвимостям в офисном ПО;
2. внутри категории браузерных уязвимостей на фоне существенного спада в количестве программных ошибок собственно в ядре браузера наблюдался резкий рост уязвимостей в разнообразных плагинах и интерфейсных модулях;
3. наметившийся в 2007 году рост эксплуатации ошибок в офисном ПО получил еще большее развитие в 2008 году;
4. среднее количество вновь обнаруживаемых удаленных и локальных уязвимостей собственно в коде операционных систем существенно не изменилось;
5. еще более пристальное внимание в качестве объектов поиска уязвимостей злоумышленники стали уделять устройствам сетевой инфраструктуры и средствам защиты сетей.

В качестве объектов атак из области офисного ПО лидирующее место по-прежнему с большим отрывом занимают продукты компаний Microsoft и Adobe, что, несомненно, объясняется их распространенностью.

Среди офисных продуктов Microsoft наиболее высокие риски имеют обладатели пакета Office 2003. Семейство Office 2000, несмотря на сравнимое в относительных цифрах с Office 2003 количество уязвимостей среднего и критического уровней уже имеет гораздо меньший процент инсталляций на рабочих местах, что в том числе сдерживает распространение вредоносного кода, эксплуатирующего его уязвимости. Из положительных тенденций хотелось бы отметить, что семейство Office 2008 на текущий момент демонстрирует очень низкий уровень подверженности классическим методам атак. Следствие ли это недостаточной исследованности его программного кода злоумышленниками или же действительно заслуга разработчиков, активно внедряющих методики и средства повышения качества выпускаемого ПО, – ответа на этот вопрос пока нет.

Программное обеспечение от компании Adobe для просмотра и редактирования цифровых документов и мультимедиа к сожалению сохранило и даже ухудшило за прошедший год свое реноме в отношении устойчивости к уязвимостям. Так несколько раз в нем были обнаружены очень серьезные уязвимости, в т.ч. до уровня возможности загрузки и исполнения вредоносного программного кода на компьютер жертвы. При

этом ошибкам оказался подвержен очень широкий спектр продуктов, как по функционалу так и по версиям.

Конкуренция "на рынке" браузеров также оказывает все более заметное влияние на вектор поиска уязвимостей злоумышленниками. Так, объектами успешных эксплуатаций уязвимостей все чаще становятся пользователи Firefox, Opera, Safari. Резкий рост интереса злоумышленников к ошибкам в программном коде Mozilla Firefox к счастью нивелируется очень оперативной реакцией разработчиков на обнаруженные уязвимости. Вкупе с системой практически "принудительного" автообновления, встроенной в данный браузер, это позволяет держать количество реальных взломов на очень низком уровне.

При этом, как отмечают многие аналитики, прошедший год с запасом побил рекорды в отношении среднего времени между публикацией уязвимости и внедрением ее на практике во вредоносном коде, распространяющемся по сети Интернет.

Все больший интерес проявляют разработчики вредоносного кода к объектам сетевой инфраструктуры: маршрутизаторам, DSL-модемам, DHCP-серверам и т.п. Сразу для нескольких семейств маршрутизаторов и модемов, функционирующих под управлением одного из клонов Linux, была разработана удаленная атака, позволяющая получить полный контроль над устройством и использовать его для дальнейшего распространения этого же кода. Для известной линейки файрволов PIX/ASA от компании Cisco была опубликована уязвимость и программный код, позволявшие внешнему злоумышленнику переводить устройство в неработоспособное (до перезагрузки) состояние. По-прежнему пристальное внимание злоумышленниками уделяется протоколу SSH и его конкретным реализациям.

Технология внедрения фальшивых DHCP-серверов в локальную сеть все чаще и успешнее эксплуатировалась в 2008 году. Основной целью злоумышленников при этом являлась подмена DNS-серверов и, как следствие, открытие широких возможностей для фишинга и перехвата конфиденциальной информации.

Не остались без внимания исследователей и беспроводные сети. После некоторого периода затишья, характеризовавшегося фразой "WEP абсолютно ненадежен, WPA ненадежен только в случае использования слабых паролей", появились сообщения, с описанием алгоритмов частичного обхода средств защиты WPA и для случаев применения стойких паролей. Основная цель подобного рода атак состоит во взломе ключа аутентификации пакетов на базе прослушивания пакетов с хорошо известным содержимым (например, ARP-запросов). Ключевая идея при этом состоит в использовании для подбора ключа подканалов с другими значениями приоритета (Quality of Service), в которых порядковый счетчик отправленных пакетов еще не достиг значения, записанного в перехваченном пакете.

Результатом атаки при типовых настройках параметров протокола WPA является возможность для злоумышленника в среднем 1 раз в 10 минут отправлять 1 фальшивый пакет в сторону клиента якобы от имени точки доступа, при этом аутентичность пакета будет подтверждена криптографической подсистемой. При такой относительно невысокой скорости наиболее вероятными целями фальсификации будут активные

атаки класса ARP-spoofing, DNS-spoofing и т.п.. В целом, сам факт (хотя бы частичного) взлома очередной подсистемы безопасности WiFi, казавшейся еще недавно абсолютно надежной, на фоне растущего интереса к беспроводным сетям заставляет в очередной раз задуматься о необходимости постоянного контроля за ситуацией в области WiFi-безопасности и внедрении многоуровневых систем защиты при использовании беспроводных систем доступа.

Также совершенствовались и гибридные технологии распространения вредоносного кода, объединявшие зачастую совершенно разные пути проникновения на компьютер-жертву. Примером подобного подхода можно назвать модификацию вируса Virut, после заражения встраивавшего вредоносные ссылки в найденные на компьютере и сетевых ресурсах HTML, ASP и PHP страницы – в случае, если инфицированные страницы оказывались частью какого либо WWW-сервера, под угрозой кроме самого владельца страниц оказывались и все его посетители.

Не обошелся прошедший период и без принципиально новых идей и методик в техническом плане. Наибольший прирост "новинок" пришелся на методики внедрения вредоносного кода на все более и более низких уровнях (новые разновидности руткит-технологий, внедрение в BIOS, в микрокод процессора и т.д.). Цель разработчиков подобных методик состоит в получении контроля над компьютером до загрузки антивирусного ПО с целью пассивного или активного противодействия ему (соответственно – либо скрытия своего кода от анализатора либо нейтрализации подсистем антивируса, в т.ч. например, службы обновления вирусных баз). Кстати, следует отметить, что увеличение распространенности руткит-троянов сразу отразилось на повышении интереса к антивирусным загрузочным дискам (LiveCD), наиболее надежно сражающимся с подобным вредоносным кодом.

Заметно возросло активное противодействие троянских программ в отношении установленных на заражаемом компьютере антивирусных продуктов. Почти все "успешно" распространившиеся модификации вирусных программ умеют полностью или частично отключать антивирусное ПО, блокировать сайты автообновлений вирусных баз, противодействовать запущенным антивирусным процессам. С учетом подтвержденных фактов активного развития за последние годы рынка автоматических средств сокрытия (шифрования, мутаций, полиморфизма) вредоносного кода наблюдающиеся процессы уже можно расценивать как настоящие столкновения в киберпространстве между экземплярами "белого" и "черного" программного кода.

В целом, обстановку в области поиска и эксплуатации новых уязвимостей и подходов к заражению компьютеров можно охарактеризовать как довольно сложную. Открыто публикуемая часть потока информации о новых и новых ошибках в широко распространенном ПО нисколько не уменьшает своих объемов. А это кроме того позволяет формировать и неутешительные прогнозы о масштабах скрытой части айсберга "черного рынка" уязвимостей, доступного только участникам закрытых хакерских групп.

Направление «социальной инженерии»

В тех случаях, когда технические уязвимости не помогали злоумышленнику добраться до цели, почти всегда оставался путь социальной инженерии. За последние годы со вполне предсказуемым снижением среднего уровня компьютерной грамотности у новых пользователей сети он развился в индустрию, сравнимую с индустрией поиска уязвимостей.

Основными направлениями социальной инженерии в 2008 году стали:

- рассылки в адрес "друзей" со взломанных аккаунтов социальных сетей и ICQ;
- фишинг по электронной почте с ложными уведомлениями о новых сообщениях в социальных сетях;
- подделка интерфейсов популярных развлекательных, новостных и медийных сайтов с предложением установки фальшивых кодеков или плагинов для просмотра;
- фальшивые сообщения о якобы имеющихся на компьютере жертвы угрозах безопасности с предложением установки фальшивых антивирусных продуктов;
- фальшивые сообщения о бесплатных обновлениях программных продуктов.

Социальные сети, как и прогнозировали эксперты по информационной безопасности, оказались "раем" для методов социальной инженерии. Запоминающийся на подсознательном уровне интерфейс, WWW-технология, очень широкий процент пользователей со средним и откровенно низким уровнем компьютерной грамотности – всё это привело к расцвету кибермошенничеств в социальных сетях. Как выяснилось, доля перехода даже по явно подозрительным ссылкам и загрузкам, пришедшим по каналам социальных сетей от хорошо знакомого человека, в разы превышает показатели, характерные для обычного Web-серфинга. Уровень угроз со стороны социальных сетей вырос за прошедший год настолько сильно, что даже лояльные к web-серфингу своих сотрудников работодатели, стали адекватно относиться к требованиям служб ИБ полностью блокировать социальные сети на офисных компьютерах.

Ситуация с фальшивыми кодеками и плагинами для web-просмотра медийного контента также называется многими ведущими экспертами как первоочередная проблема прошедшего года. Причем проблема эта скорее объективная, чем субъективная. Современные программные продукты, использующие web-технологии планомерно приучают пользователей к необходимости время от времени получать постоянные обновления для корректного отображения все новых и новых спецификаций медийного контента. На этом фоне злоумышленники, обнаружившие нишу фальшивых кодеков и плагинов, сделали беспроблемный шаг. Даже опытному пользователю ПК не всегда под силу отличить поддельный сервер-источник предложения об обновлении. Негативным моментом является то, что в настоящее время решительных мер по снижению подобных рисков со стороны ни одного из заинтересованных участников не наблюдается.

К подобному же классу уловок социальной инженерии относятся WWW-сообщения о якобы обнаруженных на персональном компьютере сервера

вирусных программах, заполонившие "серые" сайты. Последующими рекомендациями доверчивому пользователю будет предложение загрузить и установить уникальное современное антивирусное ПО, вслед за чем собственно и произойдет инсталляция вредоносного кода. Уровень риска по данному классу угроз может эффективно снижаться своевременной и качественной образовательной программой "минимума знаний по ИБ" пользователю ПК. Однако, к сожалению, на текущий момент масштабы заражений по данной схеме огромны.

Новый подход к фишингу, доведенный в 2008 году до работоспособных инцидентов, был продемонстрирован симбиозом разработчиков вредоносного кода и специалистов по "раскрутке" сайтов (SEO). Суть его заключается в искусственном поднятии рейтинга качественно сделанных фальшивых промо-сайтов в результатах поисковых систем по тому или иному ключевому слову. Не секрет, что поисковые системы являются одним из основных путеводителей пользователей к впервые посещаемым сайтам, а высокий рейтинг фальшивого сайта дает дополнительную подсознательную уверенность в том, что сайт является безопасным. Итогом чаще всего является уже описанное выше предложение установки инфицированных плагинов или кодеков.

Изложенные факты и схемы позволяют сделать вывод о том, что за последнее время социальная инженерия превратилась в мощнейший инструмент разработчиков вредоносного кода и на текущий момент находится на этапе своего активного развития.

Цели атак

Какими были основные мотивы злоумышленников при захвате ими персональных компьютеров в 2008 году? – Деньги и еще раз деньги.

Ключевыми источниками доходов, и как следствие, целями заражения стали:

- использование зараженных компьютеров для спам-рассылок;
- кража сохраненных на компьютере реквизитов платежных онлайн-систем (в первую очередь – банковских);
- прямое вымогательство денег (например, шифрованием файлов или блокированием работы компьютера);
- кража реквизитов социальных сетей или программ обмена мгновенными сообщениями для фишинговых рассылок по списку контактов;
- использование зараженных компьютеров для DDoS-атак с целью вымогательства денег.

Действительно серьезным изменением, произошедшим в 2008 году, стало перераспределение схем "монетизации" криминальных доходов с учетом появления новой "удобной для всех" схемы – платных SMS. Очевидно, рост денежных потоков через платные SMS является следствием определенного попустительства со стороны организаций, призванных контролировать размещение платного и дополнительного контента в сетях сотовых операторов. Но факт остается фактом – схема оказалась жизнеспособной и выгодной для злоумышленников, кроме того, она оказалась как никогда ранее доступной для жертвы. А это в свою очередь еще более склонило чашу весов в сторону исхода, при котором владелец

зараженного ПК заплатит вымогателю посредством SMS и через несколько минут получит код разблокировки, нежели прибегнет к помощи специалиста по удалению вредоносного ПО или системного инженера компании (в т.ч. уже из боязни репрессивных мер со стороны работодателя). Неудивительно, что на новую схему активно переключились разработчики шифровальщиков файлов, блокировщиков работы системы, авторы фишинговых рассылок.

Итоги и прогнозы развития угроз

Общая ситуация в сфере вредоносного кода в целом продолжает тренды предыдущих лет и описывается двумя ключевыми терминами "профессионализация" и "монетизация". По глобальной сети в каждый момент времени распространяются сотни уникальных, достаточно проработанных, свежих (не определяемых сигнатурными методами) экземпляров вредоносного кода, формируя массивы зараженных рабочих станций и серверов (ботнеты). Наиболее успешные из них (например, Storm, Conficker) успевают в пике своего распространения контролировать сотни тысяч и по некоторым оценкам даже миллионы компьютеров. Подавляющее большинство из них умеет распространяться одновременно по нескольким различным схемам, временно нейтрализовать антивирусное ПО и подключаться к центрам контроля за инструкциями и "свежим" программным кодом.

Черный рынок вредоносного ПО содержит предложения по продаже массивов зараженных ПК, описаний неопубликованных уязвимостей, программ-шифровщиков для защиты от сигнатур антивирусного ПО, программ автоматической генерации "комбайнов" из кода, собственно эксплуатирующего уязвимость, и вредоносного наполнения. Разработчики антивирусного ПО сокращают, насколько это возможно, время реакции на новые экземпляры вирусов, однако, сигнатурный подход принципиально является реактивным, а проактивные (в т.ч. эвристические) методы до сих пор не дают желаемого соотношения уровня обнаружений к проценту ложных срабатываний. При этом высокая пропускная способность каналов связи и отточенные за последние годы алгоритмы распространения в глобальных сетях, позволяют вредоносному коду захватывать огромные парки компьютеров за считанные часы и дни.

Все это позволяет вновь охарактеризовать ситуацию с вредоносным кодом как довольно сложную, а прошедший год как, к сожалению, не принесший каких-либо ощутимых положительных методик в борьбе с ним.

Развитие регулирования рынка ИБ

Соответствие стандартам и нормативным актам есть соответствие регулирующим правилам - как нормативным актам, так и различным стандартам. На данный момент соответствие нормативным актам продвигается более быстрыми темпами, чем внедрение стандартов.

В 2008 году пристальное внимание рынка безопасности было сосредоточено как на особенностях развития и гармонизации новых национальных стандартов информационной безопасности, так и на надлежащем исполнении Федерального Закона РФ от 27 июля 2006 года №152-ФЗ «О персональных данных». Также следует отметить повышенный интерес отечественных кредитных организаций к развитию комплекса документов в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации" (БР ИББС).

Развитие национальных стандартов

В 2008 году продолжился последовательный процесс разработки и гармонизации национальных стандартов информационной безопасности. Количество национальных стандартов ИБ увеличилось до сорока. При этом международных стандартов ИБ насчитывается порядка 170.

В 2008 гг. были введены в строй следующие гармонизированные национальные стандарты ИБ:

- ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасности информации»
- ГОСТ Р ИСО ТО 13569 «Финансовые услуги. Рекомендации по информационной безопасности»
- ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3
- ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»
- ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем»
- ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»
- ГОСТ Р ИСО/МЭК 27006 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности»
- ГОСТ Р ИСО/МЭК 18028-1 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности»

- ГОСТ Р ИСО/МЭК ТО 24762 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения»

В 2009 году планируются выйти:

- ГОСТ Р ИСО/МЭК 21827 «Информационная технология. Проектирование систем безопасности. Модель зрелости»
- ГОСТ Р ИСО/МЭК 27000 «Информационная технология. Методы и средства безопасности. Системы менеджмента информационной безопасности. Обзор и словарь»
- ГОСТ Р ИСО/МЭК 27002 «Информационная технология. Методы и средства безопасности. Практические правила менеджмента информационной безопасности»
- ГОСТ Р ИСО/МЭК 27005 «Информационная технология. Измерения менеджмента информационной безопасности»
- ГОСТ Р «Защита информации. Автоматизированные системы и базы данных. Требования по обеспечению безопасности информации»
- ГОСТ Р «Защита информации. Оценка безопасности информации, циркулирующей в автоматизированных системах. Общие положения»
- ГОСТ Р «Защита информации. Техника защиты информации. Требования к формированию баз синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»
- ГОСТ Р «Система обеспечения информационной безопасности сети связи общего пользования. Методика оценки риска причинения ущерба сетям и системам связи»

Отличительной особенностью современного этапа стандартизации в области информационной безопасности является развитие существующих требований по защите информации с уклоном от чисто технических аспектов в сторону аспектов управления, аудита и оценки ИБ.

Исполнение ФЗ РФ «О персональных данных»

Первые шаги в направлении защиты персональных данных, были сделаны Россией еще в 1995 году, когда был принят Федеральный закон от 20 февраля 1995 г. №24-ФЗ «Об информации, информатизации и защите информации», несколько позже Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», была сделана попытка конкретизировать, какие именно персональные данные относятся к сведениям конфиденциального характера и соответственно подлежат защите. Самым первым пунктом было написано, что к сведениям конфиденциального характера относятся «Сведения о фактах, событиях

и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях».

Только спустя 5 лет, а именно в 2002 году, был принят нормативно-методический документ Гостехкомиссии (ФСТЭК) «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), в рамках которого, требования к защите персональных данных были определены уже более конкретно. Класс защищенности автоматизированных систем, обрабатывающих персональные данные, который был определен данным документом, являлся одним из самых низких. Документ носит статус обязательного для защиты государственных информационных ресурсов и рекомендательный для защиты конфиденциальной информации содержащейся в негосударственных информационных ресурсах.

Споры по его поводу не утихают до сих пор, т.к. СТР-К не был зарегистрирован в Минюсте. Необходимо также отметить то, что кроме СТР-К были приняты соответствующие изменения/дополнения ряда законодательных актов, в отношении личной и семейной тайны, как то был принят ряд статей Гражданского, Уголовного, Трудового кодекса, а также федеральные законы «О банках и банковской тайне», «О связи» и т.д.

Фактически только Федеральный Закон РФ от 27 июля 2006 года №152-ФЗ «О персональных данных» положил начало актуализации ранее сформированной концепции защиты персональных данных.

Под действие закона подпадает обработка персональных данных, как с использованием средств автоматизации, так и без их использования. Одним из важных положений закона является то, что к 1 января 2008 года оператор персональных данных в определенных случаях обязан был направить в Роскомнадзор необходимое уведомление.

Федеральный Закон РФ от 27 июля 2006 года №152-ФЗ «О персональных данных» направлен на реализацию конституционных положений, закрепляющих право каждого на неприкосновенность частной жизни и свободу информации. Этот закон ориентирован на выполнение международных обязательств Российской Федерации в соответствии с Федеральным Законом от 19 декабря 2005 года №160 «О ратификации конвенции Совета Европы защите физических лиц при автоматизированной обработке персональных данных». Федеральным Законом «О персональных данных» предусматриваются:

- унифицированные требования к сбору и обработке персональных данных (ПДн) физических лиц во всех сферах, где используются эти данные
- принципы трансграничной передачи ПДн
- меры государственного контроля за деятельностью государственных органов, органов местного самоуправления, юридических и физических лиц, связанной с обработкой ПДн.

Срок, к которому организации должны привести свои информационные системы, обрабатывающие персональные данные в соответствие был определен – 1 января 2010 года.

При этом если в Законе «Об информации, информационных технологиях и о защите информации» говорится о том, что именно надо защищать и что конкретно является объектом конфиденциальной информации, то Закон «О персональных данных» раскрывает состав ПДн и предусматривает применение технических и организационных мер и средств для обеспечения защиты.

В сферу действия Федерального закона "О персональных данных" попадают все юридические и физические лица, которые обрабатывают или организуют обработку ПДн граждан. Согласно статьи 19 Федерального Закона «О персональных данных», оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры. В том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Для разъяснения действия закона был выпущен ряд подзаконных актов. Если рассмотреть все подзаконные акты, которые в той или иной части затрагивают данные вопросы, то их можно условно разбить на две группы:

1. Открытые документы;
2. Документы, доступ к которым ограничен.

Наибольший интерес представляют документы по защите ПД, введенные в действие 2008г., и регламентирующие защиту персональных данных, обрабатываемых с использованием средств автоматизации. Т.к. на настоящий момент именно эти документы являются самым большим камнем преткновения для большинства компаний в вопросах защиты персональных данных.

Это документы:

1. утвержденные ФСТЭК России. Доступ к ним ограничен, носят гриф «Для служебного пользования»;
2. утвержденные ФСБ России. Являются открытыми.

Если говорить о документах регламентирующих защиту ПДн, утвержденные ФСТЭК России, то это четыре документа:

1. «Основные мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн» - содержит рекомендуемые для выполнения работы, применительно к каждой стадии создания системы защиты ПДн;
2. «Рекомендации по обеспечению безопасности ПДн при их обработке в ИСПДн» - определяет порядок организации обеспечения безопасности ПДн при их обработке в элементах информационных систем;
3. «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн» - является основой для разработки модели угроз в соответствии с Методикой определения актуальных угроз безопасности ПДн;
4. «Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн» - предназначена

для формирования перечня актуальных угроз безопасности ПДн, при их обработке в информационных системах.

Каждая компания может получить данные документы, достаточно официально обратиться в территориальные подразделения ФСТЭК по месту нахождения организации.

Если говорить о документах регламентирующих защиту ПДн, утвержденных ФСБ России, то это два документа:

1. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств ... в случае их использования для обеспечения безопасности персональных данных при их обработке в ИСПДн» - определяет организационно-технические меры для развертывания и эксплуатации информационных систем ПДн, защищенных с использованием шифровальных (криптографических) средств;
2. «Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации» - предназначен для формирования модели угроз и нарушителей, а также определения требуемого уровня защиты ПДн.

Данные документы ФСБ, можно найти по ссылке <http://www.rsoc.ru/main/directions/874/916.shtml>. По данной ссылке можно также найти ряд других открытых документов по ПДн, а также документы Роскомнадзора, регулирующие порядок регистрации оператора персональных данных (компании обрабатывающей или организующей обработку персональных данных)

Рассмотрев документы, регламентирующие защиту персональных данных, как утвержденные ФСБ России, так и утвержденные ФСТЭК России, можно выделить ряд основных положений:

- Защита персональных данных должна строиться из организационного, инженерно-технического обеспечения и из процессов обеспечения системы защиты персональных данных;
- Работы по разработке и внедрению системы защиты персональных данных должны осуществляться только специализированными организациями, обладающими соответствующими лицензиями ФСТЭК России и ФСБ России;
- Защита персональных данных должна производиться только сертифицированными в ФСБ России или ФСТЭК России средствами защиты информации;
- Информационные системы 1 и 2 класса, обрабатывающие персональные данные, должны быть аттестованы на соответствие требованиям ФСТЭК России;
- Организации эксплуатирующие информационные системы персональных данных, должны получить соответствующие лицензии ФСТЭК России или ФСБ России.

После прочтения документов регуляторов, изданных в поддержку закона №152-ФЗ, у многих сложилось мнение, что невозможно, за оставшийся срок до конца 2009 года привести в соответствие информационные системы персональных данных организации. Действительно, если просто

посмотреть данные документы, то может сложится такое ощущение, но при более тщательном их изучении, достаточно просто сформировать четкий план выполнения работ. Он будет включать как стадии технического направления, так и стадии направление «нетехнической» защиты.

План работ будет выглядеть примерно так:

1. Подать заявку в территориальное подразделение ФСТЭК на получение экземпляров руководящих документов по защите ПДн.
2. Сформировать рабочую группу, ответственную за обеспечение защиты персональных данных и наделить ее соответствующими полномочиями.
3. Определить область, в которой будут проводиться работы по приведению процессов обработки персональных данных в соответствие закону. Это может быть как территориальное подразделение компании, так и какие-то ее типовые процессы.
4. В выделенной области работ, выделить и изучить технологические процессы, в которых присутствует обработка персональных данных.
5. Определение процессов позволит очертить перечень подразделений компании, и информационных систем участвующих в обработке персональных данных.
6. Изучить и провести доработку процессов обработки персональных данных без использования средств автоматизации, руководствуясь требованиями Постановления Правительства №687 от 15.09.08
7. Изучив информационные системы, участвующие в обработке персональных данных определить перечень обрабатываемых персональных данных и провести их категорирование
8. Руководствуясь категориями персональных данных, их количественной и качественной характеристикой, определить класс информационной системы ПДн.
9. Определить характеристики безопасности ПДн, которые необходимо обеспечить (конфиденциальность; защищенность от уничтожения, изменения, блокирования или иных несанкционированных действий).
10. Сформировать модель угроз для каждой информационной системы персональных данных в соответствии с руководящими документами ФСБ России и ФСТЭК России.
11. Сформировать требования к системам защиты персональных данных, обрабатываемых в информационных системах, руководствуясь ранее сформированными моделями угроз.
12. На основании требований к защите персональных данных, сформировать план работ по приведению информационных систем персональных данных в соответствие законодательству.
13. Провести необходимую подготовку организации к подаче заявки на получение лицензий ФСБ России и ФСТЭК России, если в этом есть необходимость.

14. Опираясь на требования к системе защиты ПДн, спроектировать ее.
15. На основании спроектированного решения, внедрить систему защиты персональных данных в рамках некоей выделенной пилотной зоны.
16. Провести опытную эксплуатацию сформированного решения.
17. Провести необходимые корректировки и доработки системы защиты персональных данных.
18. По окончании опытной эксплуатации принятого решения системы защиты, масштабировать на всю область работ.
19. Аттестовать информационные системы ПДн, если это определено требованиями руководящих документов ФСТЭК России.
20. Ввести приказом руководителя компании информационные системы ПДн в промышленную эксплуатацию.

Для того, чтобы составить корректное решение системы защиты персональных данных, необходимо знать, что руководящими документами регуляторов определено - используемые средства защиты ПДн должны обладать сертификатами ФСТЭК России или ФСБ России. К счастью, актуальные регулярно обновляемые реестры всех этих средств доступны на официальных сайтах ФСТЭК России и ФСБ России.

Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 (Реестр ФСТЭК России): http://www.fstec.ru/doc/reestr_sszi/reestr_sszi.xls.

Перечень средств защиты информации, не содержащей сведений, составляющих государственную тайну (Перечень средств ФСБ России): <http://www.fsb.ru/fsb/supplement/contact/lasz/perechen.htm>

В руководящих документах, для каждого класса информационной системы персональных данных определен необходимый набор требований по защите ПДн, который можно изложить в виде перечня необходимых к внедрению подсистем защиты. Приведем перечень подсистем защиты, характерный для информационных систем самого высокого класса. Данный перечень разобьем на две подгруппы:

- Подгруппа подсистем защиты от НСД, блокировки доступа, контроля целостности и криптографической защиты
- Подгруппа подсистем защиты информации от утечек по техническим каналам

Среди первой подгруппы несколько подсистем хорошо известных специалистам по информационной безопасности. Так же руководствуясь реестрами регуляторов приведем пример средств, которые могут составлять данные подсистемы:

- Подсистема антивирусной защиты (например - Антивирус Касперского вер. 6.0, Dr.Web вер.4.44, ESET NOD32 вер.3.0)
- Подсистема защиты от НСД (например – Панцирь-С, Secret Net 5.0 сетевая версия, Аккорд АМДЗ под управлением Аккорд-РАУ)
- Подсистема анализа защищенности и выявления уязвимостей (например – XSpider 7.0, Ревизор-Сети вер.2.0)

- Подсистема криптографической защиты информации (например – Панцирь-С, Crypton Personal 2.1, Верб-ВБ, Континент, Застава, VipNet Custom)
- Подсистема маршрутизации, коммутации и межсетевого экранирования (например – Cisco ASA 5520, Застава, VipNet)
- Подсистема обнаружения вторжений (например – Cisco ASA 5520 с установленным модулем IPS, Cisco IPS 4200)
- Кроме того данная группа содержит ранее не встречавшуюся подсистему:
- Подсистема противодействия программно-математическим воздействиям (Примеров сертифицированных средств нет. Данная подсистема получается путем выполнения определенных условий в отношении других подсистем защиты)

Ко второй подгруппе, относятся подсистемы хорошо знакомые государственным и около государственным организациям. Здесь также приведем пример средств, которые могут составлять данные подсистемы:

1. Подсистема защиты от утечек по цепям электропитания и заземления (пример - Соната-PC2, SEL SP-44, ЛГШ-221)
2. Подсистема защиты от утечек за счет ПЭМИН (пример – ГРОМ-ЗИ-4А, ГШ-2500, ГНОМ-3)
3. Подсистема защиты информации от утечки по акустическому (вибраакустическому) каналу (пример – Соната-АВ, Кабинет-С2, Барон S1)
4. Подсистема защиты информации от утечки за счет акустоэлектрических преобразований и высокочастотного навязывания (пример – МП-1Ц, МП-1А, КОРУНД, СИГНАЛ)

Необходимо понимать, что приведенные средства не являются исчерпывающим списком средств защиты персональных данных.

Кроме того, приятным является то, что ФСТЭК России идя на встречу операторам персональных данных проводит реструктуризацию своего реестра сертифицированных средств и указывает для какого класса информационной системы может быть использовано то или иное средство защиты.

Именно проекты по реализации закона о персональных данных позволят обеспечить стабильный рост рынка ИБ. По оценкам компании LETA проект по построению системы ЗПДн для средней компании может стоить от 3 до 4 млн. руб. (сюда включены затраты на обследование, создание нормативной документации и внедрение тех. средств. Сами работы могут проводиться как самими оператором, так и внешним консультантом). И учитывая, что в ближайшие четыре года (2009-2012), по нашим оценкам на затраты по ПДн будет затрачено более 13 млрд. рублей, то этот сегмент на рынке ИБ станет самым значительным.

Перспективы стандартизации Банка России

В 2008 году работа над стандартами и рекомендациями Банка России была продолжена. Появились новые обновленные редакции документов:

- Общие положения СТО БР ИББС – 1.0

- Аудит информационной безопасности СТО БР ИББС – 1.1
- Методика оценки соответствия СТО БР ИББС – 1.2
- Документы по обеспечению информационной безопасности РС БР ИББС – 2.0
- Руководство по самооценке РС БР ИББС – 2.1

По результатам работы в 2008 году можно перечислить основные тренды развития упомянутых документов.

В мае 2009 года начинает действовать новая третья редакция Стандарта СТО БР ИББС – 1.0. Упомянутая редакция была подготовлена на основе опыта внедрения предыдущих редакций Стандарта в Банке России и в кредитных организациях.

- К основным нововведениям третьей редакции Стандарта относятся:
- Значительная переработка и детализация терминов и понятий.
- Корректировка набора требований по обеспечению информационной безопасности.
 - появление более четких и однозначных формулировок требований;
 - исключение требований, связанных с реализацией;
 - добавление требований к дистанционному банковскому обслуживанию;
 - появление конкретных и детальных требований к СМИБ.
- Исключение из текста Стандарта раздела, посвященного Моделям зрелости процессов менеджмента ИБ

В Методике оценки соответствия информационной безопасности (СТО БР ИББС – 1.2) представлены наборы вопросов для проверки в точном соответствии с требованиями новой третьей редакции стандарта СТО БР ИББС – 1.0. В частности, в формах групповых показателей появился рекомендуемый частный показатель с оценкой либо "1", либо "н/о". Уточнены критерии оценки выполнения требований по обеспечению ИБ. При этом частные показатели, связанные с направлением "Осознание" рекомендуется рассчитывать на основе требований и рекомендаций к СМИБ, что позволяет производить оценку деятельности руководств кредитных организаций.

Методика оценки рисков нарушения ИБ (РС БР ИББС – 2.1) пока носит рекомендательный характер, т.е. имеет статус рекомендаций в области стандартизации Банка России. Предполагается, что результаты оценивания рисков безопасности будут использоваться в кредитных организациях для расширения базового набора требований Стандарта СТО БР ИББС – 1.0. При этом уровень допустимого риска каждой кредитной организации рекомендуется определять самостоятельно.

В Методике распределения ролей предложены рекомендации по формированию состава типовых ролей кредитной организации, связанных с непосредственным выполнением требований по обеспечению ИБ Комплекса БР ИББС. При этом предложены такие пути назначения и распределения ролей в кредитной организации, которые

полностью исключают недопустимую концентрацию полномочий в одних руках.

На данный момент пока не решено, когда этот стандарт станет обязательным.

Перспективы применения международных стандартов

Основной неудачей 2008 года является фактическое отсутствие 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. 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.

Пока сложно ожидать, что будет постепенный переход количества в качество. Несомненно, с накоплением частных политик по различным аспектам в области ИБ компании будут приходить к тому, что накопленный опыт и знания позволят им строить полноценный СУИБ. В результате движение будет идти от частного к общему.

Необходимость получения сертификата пока неочевидна, особенно в условиях кризиса.

Таблица 3. Сертифицированные СУИБ на начало 2009 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
9 LANIT, CSC	BSI	ISO/IEC 27001:2005
10 Rutenia, JSC	BSI	ISO/IEC 27001:2005
11 M-City	BSI	ISO/IEC 27001:2005
12 CBI	BSI	ISO/IEC 27001:2005
13 CB, Renaissance Capital	BSI	ISO/IEC 27001:2005
14 BTA Bank	BSI	ISO/IEC 27001:2005

Источник: International Register of ISMS Certificates

Возможно, основным движущим фактором использования стандарта после окончания кризиса будет то, что клиенты и партнеры компании захотят 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.

Применение «экономического» подхода

2008 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 на защиту от очевидных угроз, например от вирусов или внедрение систем разграничения доступа. Но с ростом компаний и ростом применения ИТ росли и угрозы, что привело к тому, что от ИБ стала восприниматься как одна из важнейших инвестиций. В результате от ИБ стали требовать считаемой эффективности 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 2005–2007 года также начались проекты, ориентированные на «экономический» подход. В 2008 году их стало еще больше. Клиенты начинают понимать такие термины, как ROSI (Return on Security Investment — оценка эффективности инвестиции в безопасность)³ и KPI (Key Performance Indicator) систем безопасности.

Кризис поможет внедрению этого подхода, так как с его помощью и «предварительной оценки рисков» станет возможно выделить те участки ИТ – инфраструктуры, которые надо защитить обязательно. В результате деньги, потраченные на ИБ, будут действовать действительно эффективнее.

В 2008 году большее число потребителей пришло к пониманию новых подходов. 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.

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

Развитие некоторых сегментов средств технической защиты

Рынок антивирусных средств

Рынок антивирусных средств (AB3) - 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. Эта ситуация не изменилась и в 2008 году. 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. В начале 2009 года основные игроки на российском рынке представили отчеты, которые более адекватно отражают действительную картину и соотносятся с другими источниками, такими как данные дистрибуторов и опросы, проводимые различными социологическими компаниями, методология, которая была использована компанией LETA в прошлом исследовании.

Сопоставив различные источники можно определить объем рынка AB3 в России в 2008 году в \$175 млн.

Вне зависимости от разных оценок, можно выделить тройку лидеров по проданным лицензиям.

Таблица 4. Тройка лидеров на рынке антивирусных средств

1	Лаборатория Касперского
2	ESET
3	Symantec

Источник: IDC

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

2008 и 2009 года можно смело назвать годом борьбы за ритейл. Именно через ритейл будут определяться лидеры рынка У ведущих вендоров доля ритейловых продаж доходит до 50%. Именно победители в этом сегменте и будут определять будущее лицо рынка AB3 в России. Основная схватка происходит между компаниями «Лаборатория Касперского», ESET, Symantec и DrWeb. Следует отметить, что борьба ведется довольно жесткими методами, но пока в рамках правил и в рамках российского законодательства.

Компании взяли на вооружение все инструменты, которые используют в своем продвижении товары класса FMCG, начиная от прямой рекламы на радио и наружной рекламы, заканчивая попытками выстраивания «особых» взаимоотношений с ритейлом. Таким образом, можно сказать, что AB3 стал первым товаром в России среди ПО, который стал по настоящему массовым товаром.

Лидерами в борьбе за частного покупателя стали «Лаборатория Касперского», ESET и DrWeb. При этом «Лаборатория Касперского» и ESET в сумме контролируют более 80% продаж в ритейле. Symantec

пока эту борьбу проигрывает, свое третье общее место он держит за счет корпоративных продаж.

DrWeb по результатам 2008 года можно назвать компанией «фениксом». Развитие в начале 2009 года только это подтверждает. Довольно продолжительное время DrWeb не предпринимал попыток к активному продвижению. Во многом это было связано с внутренними проблемами компании и отсутствии вменяемой современной линейки. Но, предприняв попытку возвращения через ритейл, DrWeb оказался прав. Этот бренд до сих пор узнаваем на российском рынке, что помогло ему занять, по сути, третье место среди компаний лидеров в ритейле.

Эта же тенденция наблюдается и в секторе средних и малых компаний, так как они в своем выборе довольно часто ориентируются на последние тенденции в ритейле.

За сегмент крупного бизнеса планировали биться в основном западные компании: Symantec, TrendMicro, MacAfee и «Лаборатория Касперского». Эта задачу должна была облегчена и тем, что за 2008 – начало 2009 года все основные компании открыли в России свои офисы. Но как показала практика, открыть офис и надеяться на известность своей компании мало для продвижения на российском рынке.

Так, за исключением Symantec ни одна из крупных компаний не начала программ масштабного продвижения и не создала в России своей службы технической поддержки, что для России чрезвычайно важно.

В результате лидерство в сегменте большого бизнеса осталось за лидерами рынка в целом: «Лаборатория Касперского», ESET, Symantec. И этот отрыв только увеличивается. В результате в 2008 году эта тройка и примкнувший к ним DrWeb контролируют до 80% от всего рынка АВЗ. И если другие компании не предпримут серьезных и капиталоемких программ продвижения, то можно констатировать, что ведущая четверка все дальше будет отрываться от конкурентов, и нынешняя структура рынка просуществует не менее 5 - 7 лет.

Системы комплексной безопасности

Еще в начале 2008 года перспективным рынком считались системы 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 средствами ИБ, сбор и анализ событий ИБ.

Но пока они не получили в России большого распространения. В условиях, когда бюджет экономится, большинство российских компаний не готовы к их внедрению. Так как данные системы довольно дороги, но интерес к ним значительный и после окончания кризиса можно ожидать стремительную реализацию отложенного спроса

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

DLP системы

Самым быстрорастущим новым сегментом рынка является DLP (Data Leak Prevention). Он и в условиях кризиса будет расти на 40 – 45 % ежегодно

Но пока на рынке нет устоявшегося понимания, что это за системы, какие подходят под это определение, какие нет. В России это дискуссия также чрезвычайно активна

Самые распространенные трактовки термина DLP:

- Data Loss Prevention (Предотвращение потери данных);
- Data Leak(age) Prevention (Предотвращение утечки данных).

Термин DLP совершенно не отражает сути рассматриваемых систем, — они ведь не могут в прямом смысле предотвратить все утечки информации! Правильнее было бы назвать такие решения системами контроля нежелательного перемещения информации (data move control), — но терминология DLP уже устоялась, и нам придется ей пользоваться.

Под DLP-системой подразумевается:

автоматизированное средство, позволяющее распознавать и/или блокировать перемещение существенных объёмов конфиденциальных данных за пределы защищаемой информационной системы по всем каналам, используемым в повседневной работе.

Чтобы понять, что система относится к DLP необходимо, чтобы она выполняла следующие операции:

(1) Система подготавливается к работе

- учится на примере данных, про которые уже известно, что они являются секретными;
- принимает к исполнению политику безопасности, в которой сказано, какие типы документов кому можно пересылать, а кому — нельзя;

(2) Система контролирует перемещения и хранение секретной информации

- выявляет (мониторинг) в потоке данных такие документы, которые похожи на защищаемые;
- реагирует на несанкционированную передачу конфиденциальных документов
- сканирует всевозможные залежи файлов (в корпоративной сети, на рабочих станциях) для поиска документов, похожих на секретные;

(3) Система отчитывается - сохраняет единую базу зафиксированных событий и выдает отчеты о произошедших инцидентах.

В настоящее время, в отсутствие специализированных систем противодействия утечкам, компании применяют следующие методы борьбы с утечками:

- Организационные меры — подписание сотрудниками положений по использованию корпоративной информации, прохождение инструктажа и контроль соблюдения норм;

- Физические ограничения — обращение с защищаемой информацией в замкнутом сегменте сети;
- Разграничение прав доступа — внедрение систем, блокирующих доступ к информации, не предназначенной для выполнения служебных обязанностей;
- Установка на локальные компьютеры программ, следящих за всеми операциями пользователей (перехват нажатий клавиатуры, снятия скриншотов, контроль операций с буфером обмена), например, StaffCop;
- Установка устройств, контролирующих количество распечатываемых и отправляемых по факсу документов, например Print Control;
- Внедрение систем архивирования исходящей почты с возможностью последующего разбора инцидентов, например Дозор Джет, InfoWatch Mail Storage, Symantec Ent.Vault;
- Внедрение серверных систем фильтрации трафика по ключевым словам (MIMESweeper, СКБТ Дозор Джет);
- Внедрение систем, собирающих и анализирующих все события информационной безопасности от всех, в том числе вышеперечисленных, систем, например Symantec Security Information Manager, ArcSight, Cisco MARS;

Ряд программных решений также используется для целей снижения рисков утечки информации совместно с DLP и при определенных допущениях они также могут быть отнесены к сегменту DLP:

- Средства контроля компьютерных портов ввода-вывода информации (DeviceLock, ZLock, Device Control и подобными);
- Системы шифрования устройств, дисков, файлов с управлением правами доступа к ним;
- Системы мониторинга запросов пользователей к корпоративным базам данных.

Тенденцией последнего времени стала широкая интеграция технологий DLP с несколькими классами инфраструктурных систем и систем информационной безопасности:

- Криптографические средства. DLP решения от InfoWatch, McAfee, Symantec, а также SecurIT позволяют выполнить шифрование в рамках решения от одного вендора;
- Системы управления цифровыми правами. DLP решения RSA Security, McAfee (совместно с Liquid Machines) и Symantec можно будет использовать для классификации данных «на лету» и применения к ним правильных политик;
- Системы управления идентификацией и доступом. Решения DLP от Computer Associates позволяют динамически классифицировать данные и применять к ним установленные политики доступа.
- Системы архивирования. Совместно с DLP решениями InfoWatch, Perimetrix, Symantec, а также SecurIT возможно сохранять историю

переписки пользователей последующего для ретроспективного анализа.

Отдельно следует подчеркнуть, что все ведущие мировые DLP компании за последний год, в том числе и во время кризиса, выпустили новые версии своих продуктов, которые существенно увеличивают доступный функционал.

На конец 2008 года в России лидером рынка в денежном выражении являлась российская компания InfoWatch со своими продуктами. По оценкам LETA на InfoWatch приходится до 50% от всех проданных DLP систем.

Но эта ситуация в ближайшие несколько лет может измениться. Уже сейчас в России представлены и начали продаваться продукты компании Websense, McAfee и мирового лидера Symantec DLP (Vontu).

Компания Perimetrix имела шансы и возможность занять существенную долю на рынке, но по состоянию на середину 2009 года ей это пока не удалось.

Отечественные решения по контент-чувствительному мониторингу перемещений информации более легкого класса, чем DLP (например, SearchInform, SecurIT Zgate, ТКБ Мониторинг), также могут претендовать на бюджет предприятий, отведенный под задачи защиты от утечек.

Таким образом, на этом рынке ожидается серьезная борьба. Тем более, что потребление подобных систем и в условиях кризиса будут расти большими темпами. Уже сейчас, на середину 2009 года можно сказать, что иностранные системы постепенно захватывают лидерство. Именно на них с начала года приходится до 75% новых продаж и внедрений. В результате InfoWatch начал терять лидерство.

На данный момент в России представлены практически все основные мировые решения и ряд российских разработок по контролю утечек информации:

1. InfoWatch Traffic Monitor
2. Websense Data Security Suite
3. McAfee DLP Host
4. Symantec Data Loss Prevention
5. Trend Micro LeakProof
6. EMC / RSA Security / RSA DLP Suite
7. Дозор Джет
8. Perimetrix SafeSpace
9. SecurIT Zgate

Решения от InfoWatch, Websense, McAfee, Symantec – активно продвигают различные интеграторы, у которых есть специалисты, способные продемонстрировать и внедрить решение в крупном предприятии.

Таблица 5. Краткое описание самых распространенных в России DLP систем

Разработчик	Продукт	О решении
Websense	Data Security Suite	Лидирующее DLP-решение согласно авторитетным исследованиям 2008 года. Система интегрирована с продуктами web-безопасности и web-фильтрации.
InfoWatch	Traffic Monitor	Самое распространенное в России решение по борьбе с утечками на

		2008 год. Единственный из перечисленных продуктов, имеющий русский интерфейс.
Symantec	Vontu DLP	Признанное ведущими корпорациями из списка Fortune 100 решение, имеющее крупнейшую в мире базу инсталляций.
McAfee	Total Data Protection	Интегрированное в единую систему управления продуктами McAfee DLP-решение, осуществляющее анализ и блокирование запрещенных действий пользователя на конечной станции.
Trend Micro	LeakProof	Решение, выполняющее контроль над перемещением конфиденциальной информации на уровне агентов для рабочих станций. Будет выведено в продажную готовность в течение 2010 года

Источник: LETA IT-company

Решение Дозор Джет покрывает ограниченный набор каналов утечки (электронная почта, web). Его продвигают «Инфосистемы Джет» напрямую без партнерской сети.

Решение Zgate, разработанное в сентябре 2008, продвигает компания SecurIT через свою партнерскую сеть.

Западные продукты от Trend Micro и RSA DLP Suite доступны для продажи в России, но до настоящего времени производители не выделили достаточных ресурсов, чтобы продвигать свои DLP-решения в России.

Отечественные предприятия уже имеют достаточно представительный выбор технологических платформ для построения систем класса DLP.

По экспертной оценке LETA, к 2009 году до 30% крупных российских предприятий уже начали использовать у себя системы противодействия утечкам информации или отдельные модули этих систем. DLP уже стали восприниматься службами информационной безопасности как неотъемлемая часть строящейся системы управления информационной безопасностью. Согласно опубликованным отчетам по выполненным проектам и открытой информации, в 2008 году около 75% крупных западных предприятий (данные по США и Великобритании) уже используют у себя те или иные DLP-системы или другие специализированные системы противодействия утечкам.

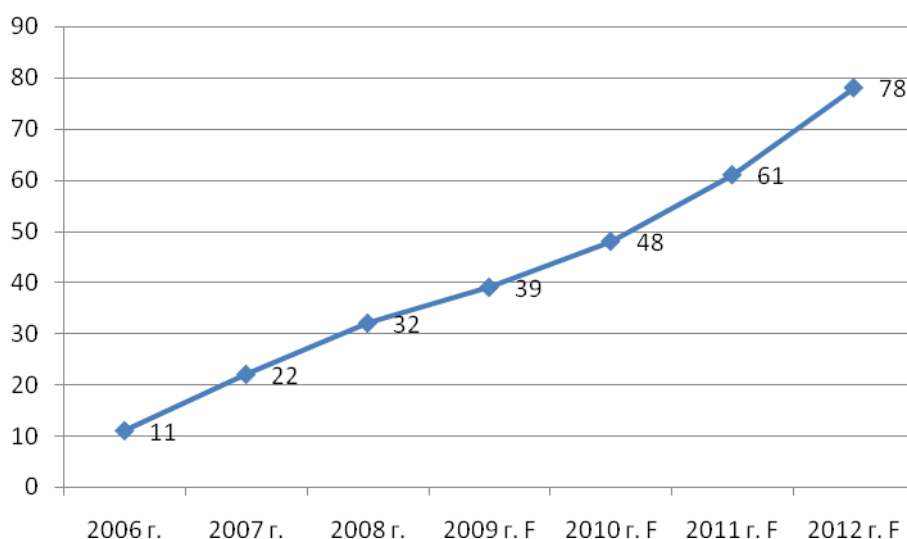
Эта же тенденция неизбежно постигнет и российский рынок с отставанием в 3-4 года.

В условиях кризиса и неуверенного состояния сотрудников и высокого уровня ротации кадров именно DLP-системы заслуживают внимания, поскольку позволяют комплексно проконтролировать как общее состояние с утечками информации по предприятию, так и проводить анализ конкретных инцидентов.

Аналитики LETA считают, что большая часть планировавшихся в DLP решения инвестиций не будет заморожена, и рынок DLP в России будет продолжать расти, хотя конечно, не такими темпами, как это было в докризисное время.

В прошлом исследовании была дана оценка роста рынка DLP в России, но в связи с началом кризиса, как и все прогнозные данные, эти оценки были пересмотрены.

Рисунок 4. Рост рынка DLP в \$млн.



Источник: LETA IT-company

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.

Другие технические сегменты рынка ИБ

После антивирусов, вторым большим сегментом на рынке ИБ являются средства сетевой безопасности: межсетевые экраны и т.д. В этом сегменте широко представлены как программные, так и программно-аппаратные решения. Этот сегмент вырос в среднем за 2008 год на 17 – 18%. И в дальнейшем будет расти в среднем на 15%. Тройка лидеров на нем не меняется уже много лет: первое место принадлежит Cisco, второе Check Point и третье место принадлежит семейству межсетевых экранов от Microsoft.

На тройку лидеров приходится до 70% от всего рынка.

Помимо иностранных разработок, в России есть собственные, отечественные МСЭ. Их доля на данный момент не превышает 5%. Эти разработки длительное время не получали существенной доли на рынке. Для их продвижения у производителей не хватало ресурсов (финансовых и организационных), и следует признать, что часто функционал отечественных решений был хуже, чем у зарубежных аналогов.

У отечественных решений было одно преимущество, они были сертифицированы как ФСТЭК, так и ФСБ. Долгое время это не играло существенной роли, так как, за исключением специальных случаев, компании вполне могли применять иностранные несертифицированные средства, в крайнем случае, отдельные партии иностранных средств сетевой защиты проходили сертификацию. Но с ростом вмешательства государства, прежде всего, с принятием закона о персональных данных потребность в сертифицированных, а значит, и потребность в российских решениях будет расти. По нашим прогнозам доля отечественных разработок на этом рынке может достигнуть 20% в денежном выражении к 2012 году. Уже первая половина 2009 года показала, что их доля начала расти.

Что касается подсегмента IDS/IPS, то и в нем лидирует в России Cisco и с большим отрывом, и пока не видно конкурента, который мог бы подвинуть компанию с этого места.

Классическим сегментом рынка ИБ является криптография. Но, к сожалению, достоверных данных по продажам в России этих средств нет. Во многом это связано с законодательными ограничениями на использование несертифицированной криптографии. В результате на многих предприятиях все равно используется иностранная криптография, часто встроенная в различные ИТ и ИБ системы. И, по факту, доля западной криптографии существенно больше, чем российской.

Как видно, практически во всех основных сегментах ИБ рынка лидируют западные решения. Исключение только рынок антивирусов и некоторые разработки компании «ГК Информзащита». Так, в России не было создано ни конкурентоспособного на международном рынке межсетевого экрана, ни системы криптографической защиты данных. Во многом это связано с тем, что при создании подобных ИБ систем компании-разработчики изначально ориентировались на внутренний рынок и на соответствие российским правилам и стандартам.

В результате, ориентируясь на узкий участок рынка и не на массового потребителя, отечественные разработчики создали продукты с ограниченным функционалом, который сложно развернуть на большие масштабы, эти продукты недостаточно хорошо описанные и не имеют серьезной технической поддержки. В результате, несмотря на хороший инженерный потенциал, рынок был проигран иностранным компаниям.

Но с началом массового применения российских средств в соответствии с законом «О персональных данных» можно надеяться на то, что российские компании получат опыт массового использования продуктов, маркетинговой и технической поддержки массовых продуктов. Итогом может стать появление конкурентноспособных ИБ продуктов.

Еще одной особенностью российского ИБ-рынка является то, что на нем реально представлено небольшое число ИБ продуктов. Так, за лидерами сетевой безопасности Cisco, Check Point и Microsoft идет фактически пустота. Хороший пример компания CA, в мире это один из лидеров, в России ее деятельность стремится к нулю. Остальные решения, которые в мире имеют существенную долю рынка, в России занимают незначительные доли. Но с увеличением рынка можно ожидать, что соотношение вендоров в России и мире будет сопоставимо.

Отдельно необходимо отметить линейку IBM ISS. Компания IBM с начала 2009 года стала проявлять большую заинтересованность в продвижении этой линейки. Таким образом, можно ожидать, что в скором времени ISS займет существенную долю рынка.

Еще одним небольшим сегментом, в котором может развернуться серьезная борьба это сегмент сканеров уязвимостей. На данный момент лидером является российская компания Positive Technologies с группой продуктов XSpider. Но в середине 2009 года на российский рынок вышли западные компании Qualys и Outpost24. Вполне возможно, что как и в случае с InfoWatch российский разработчик уступит лидерство иностранным компаниям.

В целом, рынок информационной безопасности показал, что он устойчив к изменениям внешней среды и способен развиваться в условиях кризиса. Практически все сегменты выросли в 2008, растут в 2009 году и по нашему прогнозу будут расти и в 2010.

Уже в 2009 год в России появились как новые российские разработчики и разработки, так и западные компании. В мире рынок ИБ также не стал стагнировать, там тоже выходят новые продукты, появляются новые идеи. В результате можно смело отметить, что системы безопасности для информационных технологий окончательно заняли место одних из базовых приложений, без которых само существование ИТ невозможно.

