IT - COMPANY

Презентация исследования

Рынок информационной безопасности 2009: начало эпохи compliance

LETA IT-company

Россия, 109129, Москва, ул. 8-я Текстильщиков, д. 11, стр. 2
Тел./факс: +7 (495) 921-14-10; e-mail: info@leta.ru, URL: www.leta.ru

Оглавление

LETA IT-company

Россия, 109129, Москва, ул. 8-я Текстильщиков, д. 11, стр. 2
Тел./факс: +7 (495) 921-14-10; e-mail: info@leta.ru, URL: www.leta.ru

Список иллюстраций и таблиц

LETA IT-company

Россия, 109129, Москва, ул. 8-я Текстильщиков, д. 11, стр. 2
Тел./факс: +7 (495) 921-14-10; e-mail: info@leta.ru, URL: www.leta.ru

Об исследовании

LETA IT-company представляет четвертый экспертный отчет по рынку информационной безопасности: «Рынок информационной безопасности 2009: начало эпохи compliance». Первый отчет был выпущен в начале 2007 года, второй — в середине 2008 года, третий — в середине 2009 года, и многие оценки этих исследований стали признанными фактами на рынке информационных технологий.

Данное исследование посвящено рынку ИБ в России. В исследовании дана информация о его объеме, структуре и основных игроках. Под рынком ИБ в рамках настоящего исследования понимается 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 подробно осветить все сегменты рынка ИБ в России. Так, в исследовании не был подробно рассмотрен ряд сегментов рынка, в частности, сетевая безопасность, веб-безопасность и т.д. Сузить выбор сегментов LETA IT-company была вынуждена в связи с ограниченностью ресурсов и информации по некоторым сегментам.

Особое внимание в данном исследовании уделено проблематике защиты персональных данных как самому важному явлению на рынке ИБ в 2009 году.

Информация для данного исследования получена путем опроса участников рынка методом экспертных интервью, а также анализа публикаций в СМИ и иных открытых источниках. Авторы 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 LETA IT-company.

Особенностью данного исследования является то, что в нем будут представлены авторы статей, с которыми можно будет связаться, если у читателей возникнут вопросы, предложения и замечания.

Автор	Компания	Тематика
Крохин Валентин	LETA Group	Научный редактор
Санин Александр	LETA IT-company	Защита персональных данных
Царев Евгений	LETA IT-company	Стандарт Банка России
Зенин Николай	LETA IT-company	DLP, compliance
Артеменков Дмитрий	LETA IT-company	Защита персональных данных
Сачков Илья	Group-IB	Расследований инцидентов информационной безопасности
Акатьева Мария	LETA IT-company	ISO/IEC 27001:2005
Железняков Вячеслав	LETA IT-company	ISO/IEC 27001:2006

Основные выводы

1. В 2009 году родился новый современный рынок ИБ в России. Это связанно с успешным стартом перового общероссийского масштабного проекта по compliance – реализация требований Федерального закона «О персональных данных».

2. Объем «открытого» рынка в 2009 году составил $561 млн. В целом рост рынка в ближайшие два года будет сохраняться на уровне 8 - 12%. Рост по сравнению с 2008 г составил менее 2% (по уточненным данным объем рынка в 2008 г. - $552 млн.)

3. В первой половине года рынок ИБ в отличие от рынка ИТ упал «всего» на 15% по сравнению с 2008 годом, а во второй половине года начался рост. На рост рынка в условиях кризиса влияют следующие факторы: требования регуляторов, возросший уровень угроз, в том числе появление новых. В результате рынок стагнировал в положительной зоне.

4. С начала кризиса многие компании основной моделью потребления продуктов и услуг информационной безопасности выбрали самостоятельное внедрение систем ИБ. Но всё изменилось с принятием закона «О персональных данных».

5. 2009 год подтвердил тенденцию, заключающуюся в том, что с развитием рынка постепенно меняется структура потребителей. Соответственно, на рынке будет наблюдаться: увеличение доли госорганов, снижение доли крупного бизнеса, рост сегмента SMB, рост сегмента частных потребителей.

6. В сегменте компаний-интеграторов бизнес развивается успешно. Но в сегменте российских производителей средств ИБ наблюдается кризис. Ориентируясь на узкий участок рынка, а не на массового потребителя, отечественные разработчики создали продукты с ограниченным функционалом, который сложно развернуть на большие масштабы. Скатывание в узкие ниши может совсем «убить» таких производителей, так как работа в нише не подразумевает больших денежных потоков, без которых невозможно развивать продукт.

7. Наибольший рост за последнее время демонстрируют два крупных направления злоумышленной деятельности – прямое вымогательство небольших сумм денежных средств и формирование баз данных учетных записей (как с аутентификационной информацией, так и без нее) для последующей продажи.

8. Целью атак практически всегда является исполнение вредоносного кода, внедренного в обрабатываемый объект, и, как следствие, получение привилегий учетной записи, от имени которой запущено атакуемое программное обеспечение.

9. Можно с уверенностью констатировать, что спрос на услуги по приведению ИСПДн в соответствие с требованию регуляторов в течение 2010 года будет расти. Затраты составят $110 млн.

10. Скорое согласование регуляторами новой версии Стандарта Банка России и признания его требований достаточными для выполнения требований 152-ФЗ и требований регуляторов, приведет к тому, банковское сообщество получит адекватные и адаптированные для отрасли документы, которые позволят выполнять работы по защите персональных данных в рамках СТО БР ИББС. По нашим оценкам с 2011 по 2013 года банки затратят более $60 млн. на внедрение требований стандарта. Также успешный старт этого стандарта несомненно усилит тенденцию разработки других отраслевых стандартов.

11. Внедрение систем автоматизации управления политиками ИБ станет важным направлением развития рынка ИБ начиная с 2010 года.

12. Прошедший год показал, что СУИБ, как целостный комплекс процессов, оказался менее востребованным, чем отдельные его элементы.

13. Объем рынка АВЗ в России в 2009 году составил $195 млн.

14. Объем рынка DLP в России в 2009 году составил $33 млн.

Основные характеристики рынка ИБ

Объем рынка ИБ

2009 год стал одним из важнейших периодов в развитии всего рынка информационной безопасности (ИБ). Можно смело утверждать, что именно в 2009 году родился новый современный рынок ИБ.

Но в начале 2009 года ничто не указывало на то, что этот год станет переломным. Перешедший в активную фазу в середине 2008 года мировой финансовый кризис очень сильно отразился на применении информационных технологий (ИТ).

В кризисных условиях компании всех секторов и всех размеров, не только в России, но и во всем мире, стали сокращать издержки, напрямую не влияющие на основные бизнес-процессы. Сокращение издержек на ИТ стало одним из способов уменьшения затрат. В России падение было существенным. Так, по данным Минкомсвязи, рынок ИТ упал на 13,8%; по данным же IDC, он упал на 43% (что представляется более адекватной оценкой). Так, по некоторым сегментам в первой половине года падение составило до 70% (это касается прежде всего поставок аппаратного обеспечения).

Рынок информационной безопасности не мог не начать сокращаться вслед за ИТ-рынком. Однако большого сокращения не произошло, рынок просел не намного, а во второй половине года начался рост.

Сравнительно небольшое сокращение, которое наблюдалось в первой половине года, можно объяснить тем, что бюджеты на безопасность сокращались в последнюю очередь. 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 информационные активы стали важнейшей частью любой организации, то и затраты на защиту информационных активов остались важнейшей статьей в бюджетах организаций и частных пользователей.

Но, несмотря на все положительные факторы, рынок все-таки просел. На это повлияли следующие факторы:

1. *Общее уменьшение затрат для сокращения бюджетов организаций на обслуживающие технологии, в том числе на ИТ и ИБ.*
2. *Замедление обновлений*. Компании практически не тратили средства на развитие и обновление тех систем, которые уже эксплуатировались.
3. *Перераспределение работ от интеграторов к внутренним службам*. Услуги интеграторов и внешних консультантов были востребованы только в тех случаях, когда собственная ИТ- и ИБ-служба не могла решить поставленные задачи (не хватает компетенций или область регулируется нормативными документами).

Вместе с тем не оправдался прогноз по следующим факторам:

1. *Усиление пиратства*. Все-таки за несколько лет рынок ИБ прошел большой путь, и соотношение пиратского ПО и лицензионного осталось практически на прежнем уровне.
2. *Переход на «бесплатные» и open source продукты*. Некоторые эксперты прогнозировали, что в условиях нехватки средств корпоративный сектор может начать массово переходить на «бесплатные» и open source продукты. Но этого не произошло. И если часть домашних пользователей действительно перешла на «бесплатные» и open source продукты, то корпоративный сектор посчитал, что риски, связанные с переходом, не оправданы.

В результате в первой половине года рынок ИБ в отличие от рынка ИТ упал «всего» на 15% по сравнению с 2008 годом. И это падение произошло в основном за счет компаний SMB-сектора, из его нижней части.

Удержать рынок ИБ от падения помогли следующие факторы:

1. *Возросший уровень угроз, в том числе появление новых*. В условиях кризиса криминальные риски растут, а значит, увеличиваются затраты на преодоление этих рисков. При этом сами риски могут меняться, возникают новые угрозы; старые угрозы, о которых успели позабыть, снова становятся актуальными. Так, например, выросла угроза со стороны своего персонала.

При сокращении численного состава персонала и фактическом уменьшении доходов лояльность сотрудников падает, поэтому можно ожидать как фактов саботажа, так и утечки конфиденциальной информации.

Также на сжимающихся рынках возросла конкуренция, что привело к ужесточению конкурентной борьбы. А одним из проявлений этой борьбы стали атаки на различные корпоративные электронные ресурсы.

2. *Требование партнеров*. Эта тенденция не ослабила своего влияния, наоборот, она усилилась в связи с увеличением количества угроз. Так как, несмотря на кризис, бизнес-отношения не прекратились, обострилась проблема взаимного доверия.

   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.

3. *Повышение значимости ИБ*. Информационная безопасность для всех крупных и многих средних компаний, которые прошли период массового внедрения ИТ, вышла из прикладной дисциплины на уровень бизнеса. В ИТ-системе стали храниться и обрабатываться действительно важнейшие данные, необходимые для существования и выживания бизнеса. В результате для многих компаний вопрос сохранения информации и поддержания целостности ИТ-систем и ИТ-инфраструктуры из второстепенных задач превратился в наиважнейшую, а сокращение затрат стало невозможным.

4. *Требование* регуляторов. В первой половине года многие компании до конца не понимали, что делать с требованием регуляторов, поэтому не предпринимали активных шагов. В основном это был период повышения компетенций. Такая же выжидательная позиция была и по квазиобязательным документам.

Но в середине года пришло осознание того, что выполнение требований закона «О персональных данных» будет обязательным и при этом довольно затратным. Также для выполнения требований всех выпущенных к этому времени подзаконных актов компаниям – операторам персональных данных — придется привлекать не только специалистов в области ИБ и ИТ, но и юристов, а также специалистов по управлению персоналом и специалистов по реинжинирингу бизнес-процессов. В результате проблема, которая до этого касалась, по сути, только специалистов по информационной безопасности, вышла на уровень бизнеса.

Этот переход проблематики ИБ на уровень бизнеса и стал переломным моментом для рынка. В России все нулевые годы специалисты по информационной безопасности постоянно стремились доказать не только значимость своей работы, но и значимость ИБ в целом для бизнеса. И казалось, у них были все инструменты, ведь именно в эти годы информационные технологии стали одной из основ бизнеса. К тому же на руках у специалистов по ИБ был международный опыт, который включал в себя и стандарты, и лучшие практики, и способы оценки рисков. Так что специалисты по ИБ могли говорить на одном языке с бизнесом. Об этом шла речь в прошлых исследованиях LETA.

За очень редким исключением в некоторых крупных и средних компаниях информационная безопасность не смогла занять должного места в системе корпоративного управления, так как воспринималась еще одной из поддерживающих систем, подобных АХО. Во многих компаниях не было выделенного менеджера по ИБ и функции по защите информации выполняло ИТ-подразделение. А политики в области ИБ были экзотикой. Однако во второй половине нулевых ситуация стала постепенно выправляться, правда, очень медленными темпами.

Работы, начавшиеся в 2009 году, в области защиты ПДн не только позволили поднять ИБ на уровень бизнеса, но и способствовали повышению интереса бизнеса к тому, что реально делает информационная безопасность. В результате значимость ИБ для компаний в целом повысилась, что привело к росту затрат, так как в условиях повышенного внимания специалистам по ИБ, обладающим соответствующими знаниями, стало проще мотивировать затраты на внедрение и эксплуатацию как

средств ИБ, так и различных стандартов и систем управления. Следствием этого процесса было то, что решения в области ИБ стали рассматриваться как стратегические, а значит, планирование по их внедрению перешло из краткосрочных решений в среднесрочные, что также привело к увеличению затрат.

Вторым важнейшим последствием роста интереса бизнеса к ИБ стал бум разработки отраслевых стандартов, прежде всего в области защиты персональных данных (в частности стандартов, разрабатываемых в отраслях связи, медицины, образования и банковской сферы, негосударственных пенсионных фондах). И в дальнейшем можно ожидать, что стандарты в области защиты персональных данных перейдут в стандарты по информационной безопасности.

Имея стандарты, проще обосновывать затраты на ИБ и прежде всего на организационные меры. Это означает, что ИБ постепенно перестает быть только технической проблемой, какой она довольно часто воспринималась. Соответственно, внедрение организационных мер – это затраты рынка ИБ и значительный рост доли консалтинговых услуг. В конце концов российский рынок придет к тому же состоянию, что и в развитых странах, где затраты на организационные меры и консалтинг в проектах по ИБ достигают 40—50%. Следует отметить, что процесс внедрения правильных организационных мер в российских условиях не будет быстрым (если в ближайшее время не появятся новые стандарты), традиция пока еще сильна, но сам процесс уже не остановить. Так, например, за 2009 год, по нашим оценкам, в 80% компаний с количеством ПК более 300 появились менеджеры, ответственные за информационную безопасность.

Необходимо подчеркнуть, что массовое появление менеджеров по ИБ привело к тому, что резко повысился интерес к образованию в этой области. Ведь довольно часто на эти должности назначаются сейчас не ИБ-специалисты, которых де-факто мало. Благодаря увеличению количества квалифицированных и образованных специалистов в области ИБ начнет расширяться рынок и, соответственно, затраты компаний на ИБ, так как эти специалисты смогут применять лучшие практики. По нашим оценкам, ИБ во многих компаниях и организациях либо недофинансировалась, либо работы по ИБ финансировались в рамках других проектов (так называемый

скрытый рынок). В докризисный период в тех компаниях, где существовал организованный и обученный персонал, затраты на ИБ были больше, чем в тех, где его не было (за счет применения внутренних стандартов и политик, которые реализовывал обученный персонал).

Изменения, которые принял ФСТЭК (подробнее об этом читайте в соответствующих главах), не приведут к замедлению роста рынка защиты ИСПДн. Наоборот, только поддержат его, так как новые требования более разумны и выполнимы. А это означает, что всё большее число компаний, для которых ранее риск неисполнения старых требований превышал все затраты на приведение ИСПДн в соответствие с требованиями регуляторов, начнут проекты по защите своих систем в соответствии с новыми требованиями.

Таким образом, можно сказать, что первый масштабный проект в России по compliance успешно стартовал, и в России, с опозданием в несколько лет по сравнению с развитыми странами, началась эпоха compliance.

Помимо обозначенных выше причин роста рынка в среднесрочной перспективе, необходимо отметить следующие:

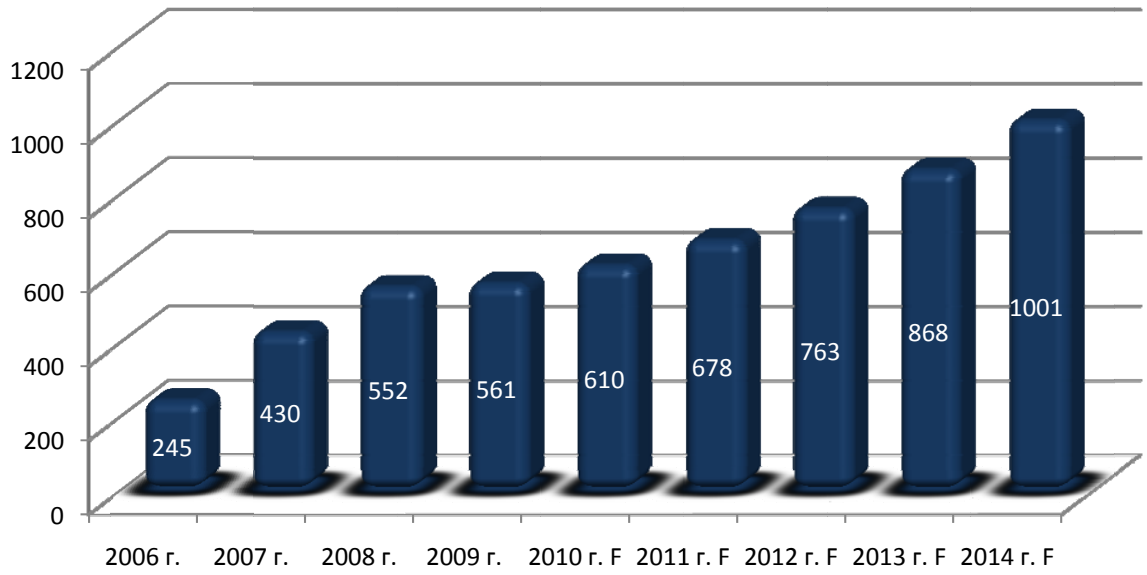
1. *Восстановление экономики*. Рост потребления средств ИТ как в домашнем сегменте, так и в бизнес- и госструктурах.
2. *Изменение закона «О электронной цифровой подписи»*. В середине этого года будет принят новый закон, регулирующий правовой статус электронной цифровой подписи. Предыдущий закон оказался неработоспособным. Те версии закона, которые сейчас обсуждаются, выглядят более логичными и применимыми на практике. А это означает, что возможен резкий рост использования ЭЦП, что приведет к расширению внедрения соответствующих ИБ-систем. Особо следует подчеркнуть, что согласно проекту закона, могут быть внедрены не только российские, но и зарубежные системы.
3. *Внедрение требований PCI DSS. Срок – к 2011 году*. Осенью этого года истекает время, когда пользователи VISA должны привести свои системы в соответствие с требованиями стандарта PCI DSS. Но на начало 2010 года члены VISA в России пока не предпринимают больших усилий по приведению своих систем в соответствие с PCI DSS. По нашим оценкам, бум PCI DSS

начнется с 2011 года, после начала применения штрафных санкций.

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 в том, 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, а значит, более доступными прежде всего для малых и средних компаний, упростилось их внедрение и использование.
6. *Развитие технологий, появление новых решений*. Прежде всего необходимо отметить следующие технологии, которые могут стать драйверами роста рынка в России:
   - защита виртуальных сред;
   - системы управления инцидентами;
   - системы, помогающие соответствовать требованиям регуляторов и стандартов;
   - защита АСУ ТП.
7. *Активная рекламная политика производителей*. Ни для кого 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.
8. *Возникновение новых угроз*. Действительно, за последние годы возникли новые угрозы, с которыми компаниям необходимо бороться. Чаще всего это означает увеличение затрат на ИБ.
9. *Усложнение задач, решаемых ИБ*. С ростом и с усложнением ИТ-систем растут и затраты на ИБ.

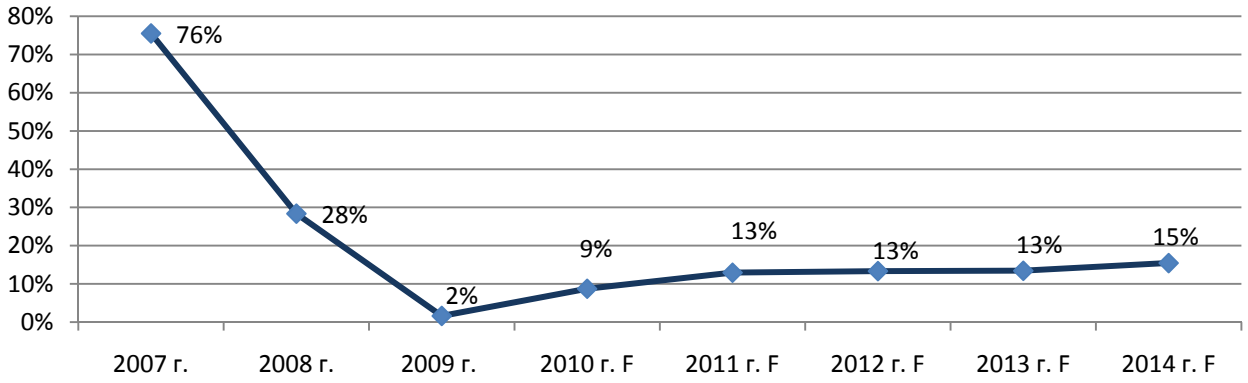
Опираясь на этот обширный список, можно сделать вывод, что на рост рынка ИБ влиял не один и не два, а целая группа факторов.

Рисунок 1 Объем «открытого» рынка ИБ в $млн



Источник: LETA IT-company

Рисунок 2 Темпы роста «открытого» рынка ИБ в %



Источник: LETA IT-company

В целом, рынок не сможет уже повторить свой бурный рост, так как, несмотря на все факторы, которые обеспечивают рост рынка, определяющим является состояние экономики. По всем оценкам, в ближайшие пять лет рост экономики если и будет, то составит минимальное значение. Но все остальные факторы обеспечат ему рост на 10—15%.

Благодаря исследованиям, проведенным LETA IT-company, выяснилось, 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 2009 году составили чуть более $1,1 млрд.

Структура потребления средств ИБ

С начала кризиса многие компании основной моделью потребления продуктов и услуг информационной безопасности выбрали самостоятельное внедрение систем ИБ, что было обусловлено сокращением расходов. Переход оказался довольно резким, что свидетельствует о том, что эта тенденция не на один год. Необходимость реализации требований закона «О персональных данных» выявила проблему крайне низкой осведомленности ИБ-персонала в большинстве компаний России. Действительно, собственный персонал компаний мог выполнить проекты по базовым требованиям безопасности, но на сложный проект с консалтинговой составляющей квалификации уже не хватало. В результате основные затраты в рамках ИБ в 2009 году пришлись на решение проблемы защиты персональных данных, что привело к резкому росту спроса на профессиональные услуги внешних консультантов. И поскольку внедрение различных обязательных стандартов в этой области будет только увеличиваться, то и доля консультантов в проектах будет расти.

Если еще несколько лет назад ИТ- и ИБ-отделы (или аутсорсинговые компании) крупных корпораций и компаний верхнего сегмента SMB предпочитали самостоятельно внедрять ИБ-решения, то с усложнением технологий, появлением новых требований, 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 чаще прибегать к услугам ИБ-компаний.

Средний бизнес предпочитал самостоятельное внедрение, часто даже не выводя ИБ в самостоятельные проекты. Учитывая, что компании SMB сектора составляют большинство в экономике России, то доля консалтинга оставалась небольшой, так как эти компании крайне редко обращались к консультантам.

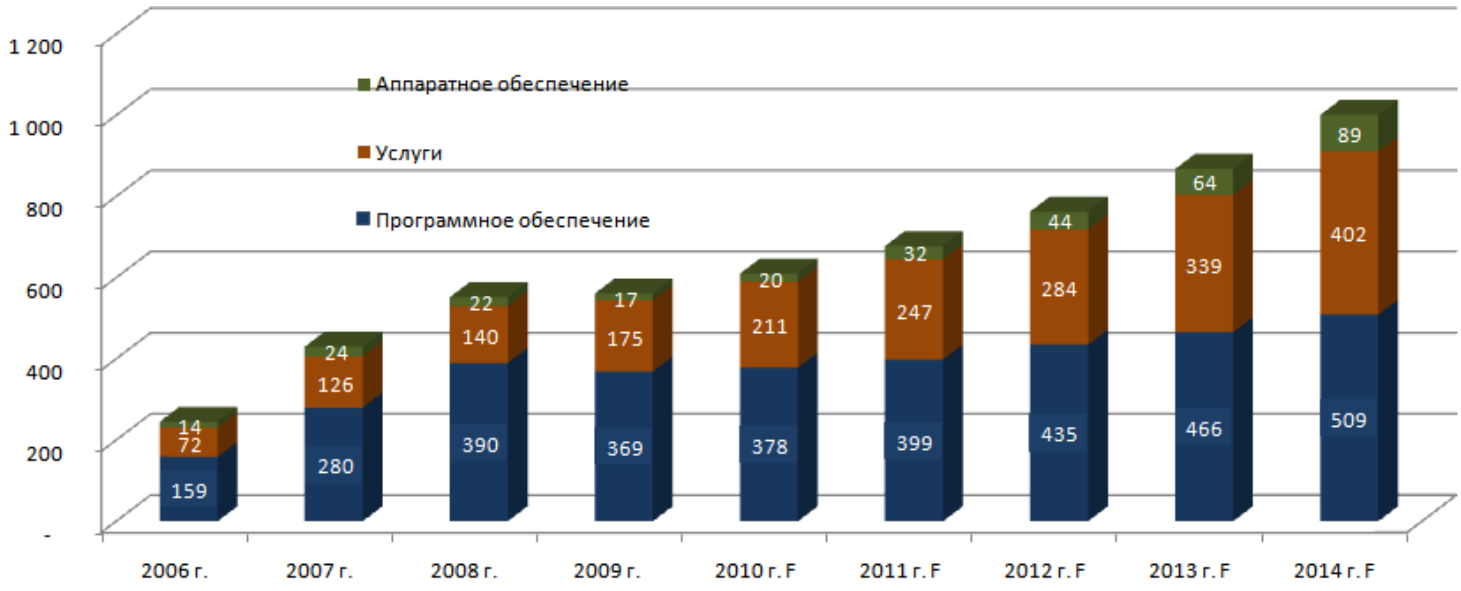
Но всё изменилось с принятием закона «О персональных данных». Крупные компании теоретически могли проводить работы по приведению

собственных ИСПДн в соответствие с требованиями регуляторов самостоятельно, но, как показывает практика, чаще все равно обращались к профессиональным консультантам. А компании среднего бизнеса в большинстве своем не могли иметь необходимых компетенций. Поэтому многие из них ограничивались только обследованием ИСПДн своими силами или внедряли необходимое ПО с минимальными организационными мероприятиями. Но при этом большая часть компаний все-таки привлекала внешних консультантов. В основном это были небольшие проекты, но их было достаточно много по всей России.

Малые компании в основном игнорировали требования регуляторов, так как требования, содержащиеся в первом варианте документов, были фактически невыполнимыми. Но тем не менее они закупали софт.

В результате тенденция преобладания продаж продуктов в 2009 году была сломлена, а это значит, что говорить о консервативности рынка уже нельзя.

Рисунок 3 Основные сегменты потребления средств ИБ в $млн



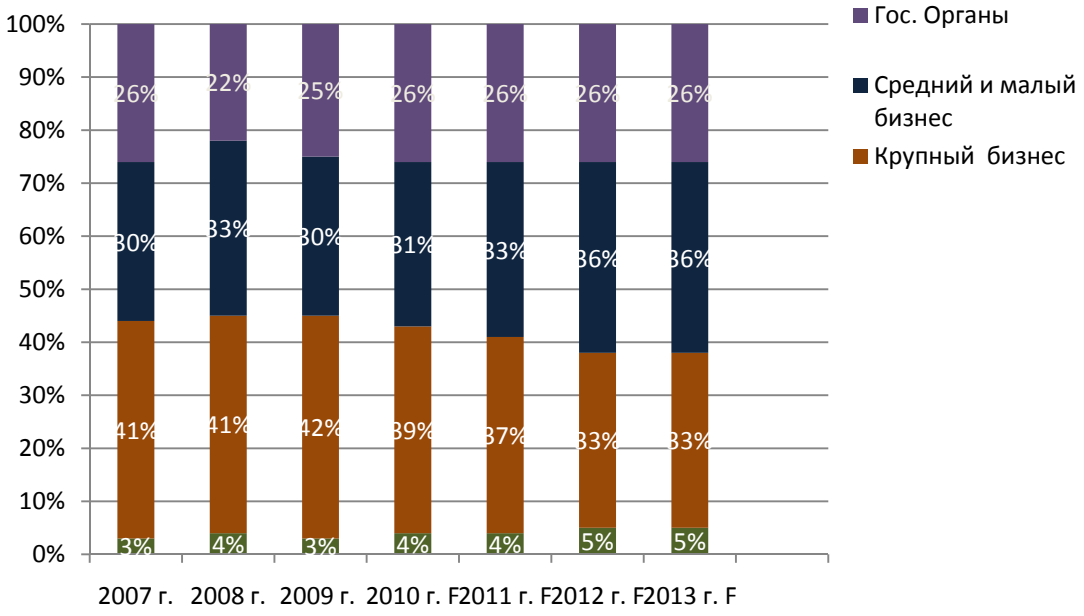
Источник: LETA IT-company

Таблица 1 Основные сегменты потребления средств ИБ в %

	ДОЛЯ ПО (в %)	ДОЛЯ УСЛУГ (в %)
2006 г.	65	29
2007 г.	65	29
2008 г.	71	25
2009 г.	66	31
2010 г. F	62	35
2011 г. F	59	36
2012 г. F	57	37
2013 г. F	54	39
2014 г. F	51	40

Источник: LETA IT-company

Рисунок 4 Потребители ИБ в %



Источник: LETA IT-company

2009 год подтвердил тенденцию, заключающуюся в том, что с развитием рынка постепенно меняется структура потребителей. Соответственно, на рынке будет наблюдаться:

- увеличение доли госорганов;
- снижение доли крупного бизнеса;
- рост сегмента SMB;
- рост сегмента частных потребителей.

Увеличение доли госорганов.

В 2008 году казалось, что началось постепенное общее снижение затрат госорганов на автоматизацию. В 90–е и в начале 2000-х 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 уменьшению их доли. Однако увеличение доли госорганов все же возможно.

В 2009 году фактически стартовал новый проект по внедрению ИТ в госорганах и их затраты снова пошли вверх, прежде всего это касается G2C (Government-to-Citizen) систем и соответствующих веб-приложений. С ростом затрат на ИТ будут увеличиваться и затраты на ИБ.

Также госорганы будут вынуждены тратить значительные средства на приведение своих ИСПДн в соответствие с требованиями регуляторов.

Снижение доли крупного бизнеса

Большой бизнес в основном прошел этап большой автоматизации, и, соответственно, больших затрат на ИБ не будет. Следует учитывать также и тот факт, что многие системы ИБ в крупных компаниях изначально строились с учетом требований регуляторов и различных стандартов. Именно крупные компании, как наиболее подверженные рискам проверок, первыми внедряют требования регуляторов.

В этом сегменте наиболее востребованы услуги, связанные с аудитом ИТ, а также с защитой ранее незащищенных областей, внедрением систем централизованного управления, систем защит АСУ ТП. 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, внедрение средств ИБ более высокого уровня сложности. В перспективе это станет одной из самых значительных статей расходов на ИБ.

Рост сегмента SMB

Компаниям SMB приходится решать две проблемы: соответствие требованиям регуляторов и внедрение действенных систем защиты, которые должны защищать критичные ИТ-системы. А учитывая то, что именно компании SMB-сектора будут трать на внедрение ИТ значительные средства в ближайшие пять лет, то и им понадобятся соответствующие решения по ИБ.

Рост затрат будет обусловлен тем, что компании SMB-сектора не тратили средства на защиту своих ИСПДн по первой версии требований регуляторов. Вторая версия более исполнима, что приведет к тому, что компаниям проще выполнить новые требования, чем нести риски неисполнения.

Также с ростом экономики ИТ-системы будут все усложняться и решать новые задачи, а значит, пропорционально будут расти и затраты на их защиту.

Рост сегмента частных потребителей

Частные клиенты начинают «обелять» свое ПО; объемы закупок оригинальных средств защиты будут 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 является одним из наименее «пиратских». Это связано с высокой скоростью появления новых угроз. Для корпоративных и частных пользователей защита данных — одна из первостепенных задач, а использование «пиратских» средств не дает возможность противостоять эволюционирующим угрозам. Именно поэтому рынок средств защиты первым стал выходить из тени.

Основные игроки на рынке ИБ

Тот факт, что рынок ИБ в условиях кризиса не только не упал, но на нем даже появились новые сегменты (прежде всего работы, связанные с соблюдением требований регуляторов), свидетельствует о том, что рынок стал еще более привлекательным для большинства игроков.

На рынке появилось много новых специализированных ИБ-компаний, при этом большинство «больших» и «средних» системных интеграторов открыли у себя ИБ-подразделения. В России на конец 2009 года практически не осталось ни одной крупной ИТ-компании, которая бы не заявила о том, что в ее линейке есть услуги по ИБ.

Такой резкое увеличение ИБ-подразделений не привело, к сожалению, к росту профессионализма среди интеграторов. За редким исключением, количество не перешло в качество, и в начале 2010 года многие их тех, кто заявлял об оказании услуг по ИБ, стали от них отказываться. Это связано с тем, что компании-заказчики в большинстве своем консервативны и предпочитают заказывать такие критичные услуги у компаний, которые уже имеют определенный вес на рынке ИБ. Поэтому существенного перераспределения сил среди лидеров не произошло, а это значит, что конкуренция на этом перспективном рынке будет только усиливаться.

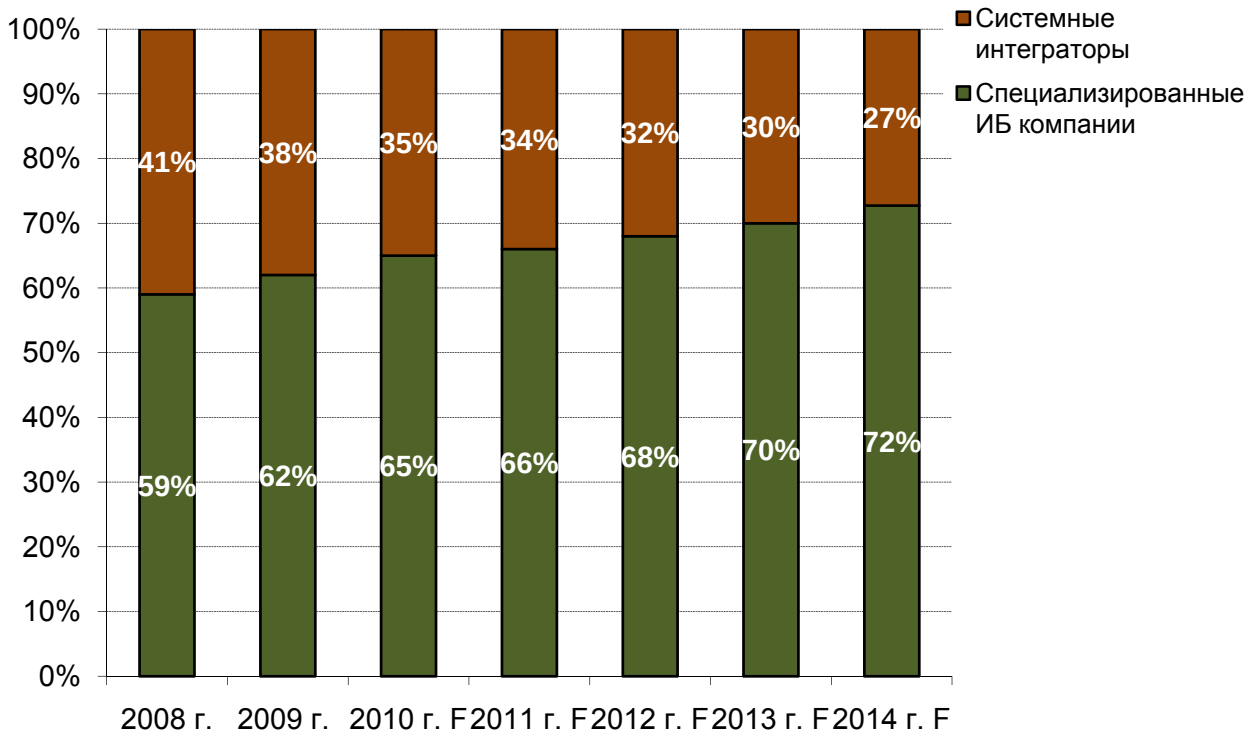
При этом особенностью данного рынка является и то, что невозможно определить, какие компании являются технологическими, а какие идейными лидерами. Практически все ИТ-компании продают или внедряют средства защиты. На рынке нет компаний, которые бы задали тон всему рынку, но можно ожидать, что они появятся.

По своим формальным признакам рынок ИБ является инвестиционно привлекательным, однако на нем (за редким исключением) не происходит сделок по слиянию и поглощению. Во многом это объясняться консервативностью самих компаний и их владельцев.

Также необходимо отметить, что с рынка ИБ фактически ушли «чистые» ИТ-компании. Ни одна крупная консалтинговая компания не открыла ИБ–направление, хотя многие об этом заявляли. Именно необходимость получения лицензии ФСТЭК России для оказания услуг по информационной

безопасности (и прежде всего по защите персональных данных), а также нехватка свободных и доступных специалистов и стали причиной того, что консалтинговые компании так и не открыли у себя это направление.

Рисунок 5 Доли игроков на рынке в %



Источник: LETA IT-company

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

Еще одним фактором, оказывающим влияние на развитие рынка, является то, что крупные ИТ-компании столкнулись с определенными трудностями в SMB-сегменте. Крупные системные интеграторы изначально работали с корпоративным сектором и госструктурами, но последние изменения на рынке ИБ, где все большую роль начинают играть SMB-компании,

показали, что сегодняшним «крокодилам» чрезвычайно сложно приспосабливаться к новым условиям.

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

Таким образом, на рынке смогут полноценно работать только те компании, которые предложат заказчикам как «экономический»1 подход, так и хорошую техническую базу.

Таблица 2 Список (по алфавиту) российских компаний, продвигающих услуги в области ИБ

Название компании-интегратора
ICL-КПО
LETA IT-company
ReignVox
АМТ-ГРУП
ГК Информзащита
Инфосистемы Джет
Крок
НПО «Эшелон»
Орбита
РНТ
СКБ Контур
Элвис-Плюс

Источник: LETA IT-company

[1] Подробнее об «экономическом» походе см. исследование «Основные тенденции в области защиты конфиденциальных данных от утечки информации ILDP на российском рынке».

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 значительные 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 своевременно и полностью удовлетворять потребности 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 и компаний оказывающих типизированные услуги.

За последние несколько лет ряд «больших» и «средних» интеграторов предложили рынку типизированные услуги, «услуги в коробке». Этот подход получил признание среди специалистов ИБ, так как основан на уже апробированных на мировом рынке стандартах и политиках. А так как рынок ИБ движется в сторону построения ИБ на стандартах и политиках, то и типизированные услуги, которые в том числе позволяют четко прогнозировать полученный результат их внедрения и использования, получают все большее распространение.

Но если в сегменте компаний-интеграторов бизнес развивается успешно, то в сегменте российских производителей средств ИБ наблюдается кризис, который начался задолго до экономического кризиса.

Российских производителей средств ИБ можно условно разделить на две неравные группы. К первой группе относится небольшая часть компаний, которая старается строить свой бизнес, основываясь на лучших мировых практиках. Это означает, что разработка средств ИБ идет в рамках стандартов, которые включают в себя современный продукт: менеджмент,

нормальное тестирование и последующую техподдержку. Также эти компании строят работу по классической схеме «вендор – партнер (дистрибутор, реселлер, интегратор) – клиент». Компании этой группы ориентируют свои продукты на массовый рынок. К этой группе можно отнести следующие компании:

Таблица 3 Список (по алфавиту) крупнейших российских вендоров

Название компании-вендора
Dr.Web
InfoWatch
Positive Technologies
SecurIT
Инфотекс
Код безопасности
КриптоПро
Лаборатория Касперского
С-Терра СиЭсПи

Источник: LETA IT-company

Ко второй группе относятся многочисленные разработчики средств ИБ, ориентированные на соблюдение требований гос. регуляторов. Эти компании обладают неплохими технологиями, но постепенно «тянут» российскую разработку вниз, в никуда.

Разработки компаний второй группы долгое время не получали существенной доли на рынке. Для их продвижения у производителей не хватало ресурсов (финансовых и организационных). Также следует признать, что зачастую функционал отечественных решений был хуже, чем у зарубежных аналогов.

У отечественных решений было одно преимущество, они были сертифицированы как ФСТЭК России, так и ФСБ России. Долгое время это

не играло существенной роли, так как, за некоторым исключением, компании вполне могли применять иностранные несертифицированные средства; в крайнем случае отдельные партии иностранных средств сетевой защиты проходили сертификацию.

Таким образом, произошло разделение рынка: для реальной защиты применялись зарубежные средства или средства компаний из первой группы; для соответствия требованиям регуляторов – средства компаний из второй группы.

В результате, ориентируясь на узкий участок рынка, а не на массового потребителя, отечественные разработчики создали продукты с ограниченным функционалом, который сложно развернуть на большие масштабы. Эти продукты недостаточно хорошо описаны и не имеют серьезной технической поддержки.

Но ситуация могла измениться с введением первой версии документов ФСТЭК России по защите персональных данных. Согласно этим требованиям компаниям необходимо было использовать в основном сертифицированные средства российского производства. В результате продукты компаний из второй группы попали на массовый рынок, но так как они не были для него приспособлены, то в большинстве своем оказались невостребованными.

Сами производители ПО надеялись на то, что из-за необходимости соблюдения требований ФСТЭК России потребители будут вынуждены покупать их продукты. И действительно, интерес к ним резко возрос. При этом сами производители не предприняли каких-либо шагов по улучшению как качества самих продуктов (в основном потребители были недовольны отсутствием совместимости данных продуктов с другими системами), так и уровня их поддержки. Многие из них действовали по принципу «берите что дают, все равно другого нет».

Результатом такой политики стало массовое отторжение рынком этих продуктов. Это стало причиной того, что многие операторы персональных данных стали требовать внесения изменений в документы ФСТЭК Росии, которые бы позволили им использовать другие разработки. Одновременно с этим по российским производителям был нанесен еще один удар.

Западные вендоры научились лицензировать свои продукты. Хорошим примером могут служить компании ESET и Stonesoft. В результате многие компании потеряли свое преимущество и скатились в совсем узкую нишу – защиту систем по гостайне или по другим системам, требующим сложной сертификации.

Скатывание в узкие ниши может совсем «убить» таких производителей, так как работа в нише не подразумевает больших денежных потоков, без которых невозможно развивать продукт.

Еще одной проблемой для многих российских производителей средств ИБ является то, что они выпускают монопродукты или строят свою политику вокруг своего флагманского продукта. Эта схема была популярна и у западных производителей десять лет назад, но сейчас они применяют совсем другую политику. Ведущие вендоры стремятся предложить максимально возможный набор, в том числе скупая внешних разработчиков. Российские же компании в основном находятся в другом цикле, что также в краткосрочной и среднесрочной перспективе может помешать им конкурировать с иностранными производителями.

Что касается государственных заказов, то они могут быть весьма значительными. Примером может служить тендер, проведенный в 2009 году МВД (210,35 млн руб.). Но они единичны, и на них нельзя построить долгосрочную стратегию развития.

В данной ситуации выходом для многих российских вендоров могло бы стать слияние. В России есть несколько компаний, которые бы могли стать центрами объединения производителей. Это прежде всего «ГК Информзащита», «Лаборатория Касперского», «Инфотекс» и «КриптоПро». Известно, что некоторые компании предпринимают попытки к объединению вокруг себя независимых производителей, но пока больших прорывов не было. Если в ближайшие годы российское вендоры не найдут внутренних сил для создания крупных компаний, в том числе путем M&A, то российский рынок займут западные компании.

Угрозы безопасности в 2009 - 2010 годах

Уязвимости в программном обеспечении

После определенного "затишья" в сфере обнаружения уязвимостей "критического" уровня, наблюдавшегося в 2008 году, второе полугодие 2009 и начало 2010-го года отметились целым списком проблем, присутствующих практически у всех разработчиков, занимающих значимую долю в сфере клиентского программного обеспечения.

В подавляющей массе выявленные критические уязвимости относятся к атакам классов "переполнение буфера", "целочисленное переполнение" и "небезопасные преобразования над указателями". Целью практически всегда является исполнение вредоносного кода, внедренного в обрабатываемый объект, и, как следствие, получение привилегий учетной записи, от имени которой запущено атакуемое программное обеспечение.

В 2009 году в списках критических уязвимостей отметились:

- целый спектр программного обеспечения от компании Adobe, предназначенного как для отображения PDF-документов, так и для воспроизведения мультимедийного контента (как минимум дважды за прошедший год, крупнейшие исследовательские центры по компьютерной безопасности выпускали рекомендации полностью запретить обработку недоверенных PDF-документов до момента выпуска обновления, устраняющего уязвимость, что является очень серьезным фактом как для формата, получившего такое широкое распространение, так и для его разработчика);
- офисный пакет от компании Microsoft, несколько раз за прошедший год (в том числе один раз – во всей линейке Microsoft Office от 2000 до 2007) пострадавший от уязвимостей, позволяющих исполнять вредоносный код, включенный в недоверенные DOC, XLS и PPT документы, за счет ошибок на этапе его разбора;
- встроенные средства операционной системы Microsoft Windows (системные процедуры визуализации графических форматов, исполнения .NET-кода, анализа URL-ссылок, компоненты

декодирования видео-файлов); при этом вызывает озабоченность то факт, что новое поколение операционных систем от компании Microsoft (Vista/2008) привносит новые (не имевшие места, например, в Windows XP) уязвимости в такие, казалось бы, тщательно проработанные процедуры, как предоставление доступа к общим файлам и принтерам по локальной сети или стек протоколов TCP/IP;

- виртуальная машина Java (JRE) и включенная в нее технология Java Web Start (JWS), предназначенная для загрузки из сети полнофункциональных Java-приложений и запуска их на компьютере вне процесса браузера; при этом одна из уязвимостей JWS, пожалуй, относится к хрестоматийным: разработчики ядра предусмотрели возможность (наиболее вероятно – в целях тестирования и отладки) замены (с помощью параметров запуска) библиотеки, реализующей функции виртуальной машины с указанием полного пути к альтернативной библиотеке, а программисты, осуществлявшие собственно реализацию JWS для операционных систем семейств Windows и Linux не уделили внимания фильтрации данных параметров при запуске; как результат злоумышленники получили возможность заставить ядро JWS скачать и выполнить с высокими привилегиями в системе любую библиотеку, в т.ч. потенциально содержащую вредоносный код;
- компоненты декодирования видео Apple QuickTime, позволяющие из-за ошибки в обработке целых чисел осуществить переполнение буфера с последующим исполнением вредоносного кода, внедренного в обрабатываемый файл.

Ситуация с уязвимостями в web-браузерах за прошедший год практически не изменилась, несмотря на то, что безопасность пользования позиционируется как наиболее приоритетное направление в рекламных акциях почти всех представителей этого класса программного обеспечения. В списках уязвимостей по-прежнему отмечаются все наиболее популярные браузеры, и по-прежнему, по мнению авторов, наиболее активную политику, направленную на устранение обнаруживаемых уязвимостей ведут создатели Mozilla Firefox.

Компания Microsoft в этом году, к своей чести, открыто поддержала движение (первоначально спонтанно инициированное web-разработчиками) по доведению до сведения широкого круга пользователей недостатков морально устаревшего браузера Internet Explorer 6. В настоящее время большинство уязвимостей, обнаруживаемых в браузерах этой компании, приходится на долю до сих пор официально поддерживаемой 6-ой версии (ее доля по разным оценкам составляет от 15% до 20% всего объема используемых в мире браузеров). Однако, и последняя 8-ая версия также "отметилась" в прошлом году уязвимостью, позволяющей исполнить произвольный код на компьютере, посетившем вредоносный сайт.

Отдельное внимание хотелось бы обратить на уязвимость службы автоматического поиска и настройки беспроводных сетей в ОС Microsoft Windows Vista/2008. Данная уязвимость реализуема при возможности со стороны злоумышленника установки фальшивой точки доступа в пределах радиодоступности WiFi-сети от атакуемой системы и формирования ее программным обеспечением искаженных служебных пакетов. Результатом атаки, которая не зависит от действий пользователя (в т.ч. возможна в его отсутствие), является переполнение буфера и исполнение вредоносного кода на атакуемой системе. На практике атака может быть проведена извне физического периметра охраны предприятия.

Отметившаяся ранее тенденция роста интереса исследователей к ошибкам и уязвимостям собственно в средствах защиты сохранилась и в прошедшем году. В отношении программных продуктов сразу нескольких производителей межсетевых экранов и виртуальных частных сетей (в т.ч. одного из лидеров этого рынка – компании Cisco Systems) были опубликованы методы вывода из строя либо частичного отказа в обслуживании (DoS). Сразу несколько известных антивирусных программных продуктов и спам-фильтров оказались уязвимыми на этапе обработки анализируемых файлов (а спам-фильтры – в т.ч. и на этапе обработки заголовков письма).

Вектора распространения

Вектора распространения вредоносного кода практически не претерпели изменения:

- размещение вредоносного кода на "собственных" сайтах с получением тем или иным способом посещений потенциальных жертв;
- взлом популярных (обычно тематических) сайтов и форумов с целью дополнения их стартовых страниц малозаметными вредоносными вставками;
- рассылки как кода, так и ссылок на него посредством почты, ICQ, и, особенно –блогов и социальных сетей, которые уверенно выходят на лидирующие позиции по активности пользователей последнее время;
- мошенничества с фальшивыми окнами антивирусной деятельности, фальшивыми требованиями активации установленного ПО или учетных записей на игровых серверах и серверах блогов и социальных сетей;
- использование уязвимостей с удаленной эксплуатацией;
- автозапуск на сменных носителях информации.

Несмотря на то, что б**о**льшая часть уязвимостей, обнаруженных за прошедший год, официально исправлялась производителями до даты публикации технических подробностей уязвимости в открытом доступе, масштабы вирусных эпидемий, использовавших уже закрытые уязвимости, и даже, уязвимости с 2-х и 3-х летней давностью, поражают своими объемами. Так, до сих пор по состоянию весны 2010 года доля вируса Conficker (Kido), эксплуатирующего уязвимость, устраненную компанией Microsoft в октябре 2008 года, находится в пределах 6-9% от всех регистрируемых антивирусными компаниями заражений.

Цели злоумышленников

Наибольший рост за последнее время демонстрируют два крупных направления злоумышленной деятельности – прямое вымогательство небольших сумм денежных средств и формирование баз данных учетных записей (как с аутентификационной информацией, так и без нее) для последующей продажи.

Вымогательство и мошенничество

Вирусы, реализующие различного рода блокирование рабочего стола с требованием покупки кода разблокировки через SMS-сообщения, приобрели такое широкое распространение, что о них в настоящий момент, знает, пожалуй, любой пользователь работающий в сети Интернет либо на своем опыте, либо из разговоров знакомых. Практически повсеместно "для усиления эффекта" заблокированный экран дополняется сообщениями и фотографиями, якобы свидетельствующими о фактах посещения жертвой сайтов фривольного, а иногда и откровенно криминального содержания. Это стимулирует пользователя компьютера, особенно в офисной среде, постараться "разрешить ситуацию" скорее путем откупа небольшой денежной суммой, чем с привлечением компьютерных специалистов и внимания руководства.

Конечно, подобное дополнительное психологическое воздействие играет на руку злоумышленнику, но кроме того, что гораздо опаснее для организации – оно стимулирует к сокрытию произошедшего инцидента нарушения информационной безопасности сотрудником. Более того, в долгосрочной перспективе успешный факт такого откупа формирует еще одну угрозу ИБ организации. Во-первых, он прививает персоналу ложную уверенность в том, что некоторые инциденты безопасности не обязательно требуют рассмотрения со стороны специалистов по ИБ, а во-вторых, подталкивает к попыткам решения любых нештатных ситуаций на рабочем компьютере частным порядком без уведомления руководства и службы ИТ или безопасности.

Примерно по аналогичному пути, но с другой мотивацией идут вирусы и троянские программы, осуществляющие фишинговые атаки на популярные сайты по следующей схеме. При очередной попытке входа на сайт,

которым пользователь активно пользуется, например, в социальную сеть или бесплатную онлайн-игру, в браузере появляется интерфейс, в точности повторяющий целевой, с сообщением о том, что посещение сервера стало платным, и для активации учетной записи требуется отправить SMS небольшой стоимости на указанный короткий номер.

Базы данных пользователей сети

Черный рынок баз данных пользователей сети уверенно занял свое место в сфере несанкционированного доступа. Примерная стоимость подобной информации в настоящее время в части, касающейся отечественных пользователей, сведена в таблице:

Таблица 4 Стоимость баз данных

Вид информации	Примерная стоимость	Единицы измерения
Учетные данные (с аутентификационной информацией)		
Яндекс-Деньги, WebMoney (в зависимости от сумм на счете)	500-3000 р.	за 1 шт.
Skype (в зависимости от сумм на счете)	100-300 р.	за 1 шт.
банковские (пластиковые) карты (с кодами для Интернет-покупок)	100-200 р.	за 1 шт.
банковские (пластиковые) карты	50-100 р.	за 1 шт.
сканированные копии паспортов граждан	20-60 р.	за 1 шт.
"голоса" социальной сети ВКонтакте	3 р.	за 1 шт.
учетные записи ВКонтакте	700-1000 р.	за 1000 шт.
почтовые ящики сервера mail.ru	150-250 р.	за 1000 шт.
Списки без учетных данных (для рассылок, спама и		

т.п.)		
сотовые номера	20-50 р.	за 1000 шт.
почтовые адреса (в зависимости от наличия тематической привязки)	5-20 р.	за 1000 шт.
номера ICQ	5-10 р.	за 1000 шт.

Источник: LETA IT-company

Иные цели

Всё большую активностью и разнообразие целей стали демонстрировать троянские программы, ориентированные на кражу банковских реквизитов (системы Клиент-Банк, Интернет-Банк и аналогичные). В начале текущего года один из ведущих отечественных разработчиков банковских систем предупредил своих пользователей об обнаружении в сети вирусной программы, способной осуществлять целенаправленную кражу ключей для обмена с банком, если для их защиты не используются аппаратные средства хранения (токены). Более того, следует учитывать, что даже в случае применения токенов угроза удаленного управления рабочим столом (а подобный функционал становится нормой для современных троянских программ) может быть реализована злоумышленником вручную с целью перевода денежных средств.

По-прежнему высока доля умышленных и неумышленных воздействий на ИТ-активы организаций со стороны сотрудников. Недовольные грядущими увольнениями, сокращениями, а иногда и просто отношениями на работе, сотрудники:

- осуществляют копирование внутренних документов и сведений из баз данных "на черный день";
- уничтожают или выводят из строя компоненты информационных активов;
- разрабатывают и внедряют черные ходы для удаленного управления компьютерами после увольнения;

- в некоторых случаях устанавливают скрипты-закладки, срабатывающие на уничтожение или искажение данных через определенный период времени.

Особенно высок риск подобных действий со стороны ИТ-специалистов, досконально знающих устройство инфраструктуры организации и ее уязвимые места.

Итоги

Анализ даже только открыто опубликованной части эксплуатируемых уязвимостей приводит к неутешительному выводу о том, что технология разработки программного обеспечения, как в корпоративном, так и в пользовательском сегментах, как для коммерческих, так и для open-source продуктов так и не смогла выйти на сегодняшний день на требуемый уровень качества и безопасности кода. Практически ни один программный продукт не может быть застрахован от наличия уязвимостей, становящихся реальными угрозами в определенных обстоятельствах.

В этой ситуации только многоуровневый комплекс как проактивных так и реактивных мероприятий может позволить организации снизить риски, возникающие вследствие автоматизации бизнес-процессов до приемлемого уровня.

Среди проактивных мероприятий с наилучшими показателями соотношения "затраты/результат" с учетом современной специфики атак на информационные системы следует выделить:

- принудительную, актуальную и контролируемую политику обновлений программного обеспечения (в т.ч. микропрограмм в аппаратном обеспечении);
- агрессивную фильтрацию и экранирование входящих и исходящих потоков информации, в первую очередь – WWW-трафика и эл.почты;
- политику минимизации прав отдельных пользователей, как в пределах рабочей станции, так и в корпоративной информационной системе, с целью снижения потенциальных потерь в случае реализации угроз ИБ.
- Среди реактивных мероприятий следует отметить:
- политику достоверного и полного журналирования и мониторинга значимой для бизнес-процессов активности пользователей и систем;
- тщательный квалифицированный анализ инцидентов в области ИБ с целью не только устранения последствий инцидента и угроз, вызвавших возможность его реализации, но и поиска

концептуальных недочетов на этапах проектирования, внедрения и поддержки проектов и обеспечения их информационной безопасности.

В целом, неуклонно повышающаяся квалификация (чаще всего за счет узкой специализации) создателей вредоносного кода и мошеннических схем с одной стороны, и готовность криминального рынка пользоваться результатами их разработок с другой, формируют состояние высокого уровня рисков в области безопасности информационных технологий. Данный факт, в свою очередь, объективно требует от организаций реализации защитных мероприятий в области ИБ для обеспечения сохранности и непрерывности своего бизнеса.

Развитие регулирования рынка ИБ

№ 152-ФЗ «О персональных данных» - старт работ

Как таковые, работы по защите персональных данных выделились из спектра работ по ИБ-консалтингу в отдельное направление сравнительно недавно. Довольно длительное время после вступления в силу № 152-ФЗ «О персональных данных» практически никто не считал данное направление одним из самых перспективных. Мнения экспертов в области информационной безопасности разнились, и большинство рассматривало работы по защите персональных данных в первую очередь как один из видов всевозможных compliance услуг, таких как приведение в соответствие со Стандартом 27001, PCI DSS, СТО БР ИББББС и др. Однако практика показала, что количество инициированных проектов по защите персональных данных в разы превосходит количество проектов по всем остальным compliance услугам вместе взятым!

В начале 2009 года в области защиты персональных данных наблюдался небольшой информационный кризис. Было понятно, что нужно что-то делать, но как именно это делать, оставалось за гранью общественного понимания. Это было связано в первую очередь с тем, что нормативные документы ФСТЭК России по защите персональных данных, так называемое «четверокнижие», носили гриф ДСП (для служебного пользования). Кроме того, ходили слухи о том, что эти документы еще до конца не утверждены в самой ФСТЭК России, и после их финального утверждения с них будет снят гриф ДСП. Приводились даже примеры того, что в разное время по официальным запросам во ФСТЭК операторы персональных данных получали разные версии «четверокнижия». Все это способствовало такому явлению, как «отложенный спрос», когда компании-операторы персональных данных не спешили во что бы то ни стало начинать проекты «прямо сейчас», решив дождаться окончательных и четких требований со стороны регуляторов.

Тем не менее тенденция оставалась неизменной – спрос на услуги по защите персональных данных начал стремительно набирать обороты. С чем это было связано? В первую очередь с тем, что № 152-ФЗ «О

персональных данных», в отличие от всех других compliance в области информационной безопасности, обязателен для любого юридического лица, работающего на территории Российской Федерации. Естественно, никто из операторов персональных данных не хочет попадать под санкции Роскомнадзора, ФСТЭК России и ФСБ России, и именно данный риск спровоцировал рост спроса на подобные услуги.

К концу второго – началу третьего квартала 2009 года спрос стал настолько высоким, что многие ИТ- и ИБ-интеграторы решили расширить штат своих специалистов по направлению защиты персональных данных. Никогда еще у специалистов в области информационной безопасности, имеющих опыт работы по защите персональных данных, не было такой свободы выбора на рынке труда. Специалисты требовались всем и в большом количестве. Отчасти данная тенденция несколько скорректировала и компенсационное обеспечение подобного рода специалистов, вернув зарплаты на докризисный уровень. Параллельно с этим проблематика защиты персональных данных начала довольно широко освещаться на всех мероприятиях, связанных с информационной безопасностью. В итоге рынок стал воспринимать данное направление чуть ли не как первоочередную задачу ИБ на ближайший год – полтора.

Не стояли в стороне от этого процесса и ассоциации, представляющие интересы различных отраслей деятельности. Первыми, по понятным причинам, были представители банковской отрасли. Именно тогда серьезные позиции начала отстаивать Ассоциация Российских Банков, предлагая внести изменения в стандарт СТО БР ИББС в части, касающейся защиты персональных данных. Причем данная инициатива была встречена представителями банковской отрасли как самая приемлемая и удобная. Суть инициативы заключалась в том, чтобы законодательно закрепить те положения, при которых организации банковской отрасли при внедрении у себя новой версии стандарта СТО БР ИББС автоматически бы покрывали требования по защите персональных данных. Фактически это означало бы то, что рекомендательного характера стандарт СТО БР ИББС превращался в обязательный. Кроме того, представителей банковского сообщества совсем не радовала перспектива появления еще двух регуляторов для банков (Роскомнадзора и ФСТЭК России). Кстати сказать, в настоящее время данная

инициатива практически доведена до логического завершения (осталось лишь согласовать и подписать межведомственный приказ, закрепляющий данную инициативу).

Немаловажным фактом в планомерном развитии спроса на услуги по защите персональных данных стало то, что уже к середине второго – началу третьего квартала 2009 года компании, предоставляющие подобного рода услуги, смогли выстроить свою модель ценообразования таким образом, что рынок выровнялся. Перестали появляться предложения типа «сделать то, не знаю что, за много-много денег». Т.е. цены на консалтинговые услуги по защите персональных данных стали адекватными и обоснованными.

Упомянутый ранее «отложенный спрос» на услуги по защите персональных данных стал реализовываться в полной мере в начале четвертого квартала 2009 года. Именно в данный период времени практически все специализированные интеграторы ощутили нехватку собственных ресурсов для реализации такого количества проектов. Ходили слухи даже о длинных очередях, в которые выстраивались операторы персональных данных, дабы начать проект у определенных интеграторов. На этой волне появилось очень много непрофильных компаний - поставщиков услуг по защите персональных данных. Это несколько снизило напряженность в части спроса, но и сказалось на качестве предоставления услуг. Тем не менее именно четвертый квартал 2009 года стал, с точки зрения спроса, пиковым. Именно тогда была заключена бóльшая часть контрактов по проектам защиты персональных данных.

Нельзя не отметить также и одно из самых знаковых событий начала четвертого квартала 2009 года – парламентские слушания на тему «Актуальные вопросы развития и применения законодательства о защите прав граждан при обработке персональных данных», которые состоялись в Государственной думе 20 октября 2009 года. Основной целью данного мероприятия был анализ существующей обстановки в области защиты персональных данных. Кроме того, свои позиции озвучили представители операторов персональных данных, столкнувшихся с проблемами при реализации требований законодательства в области защиты персональных данных. Именно на данном мероприятии впервые прозвучали

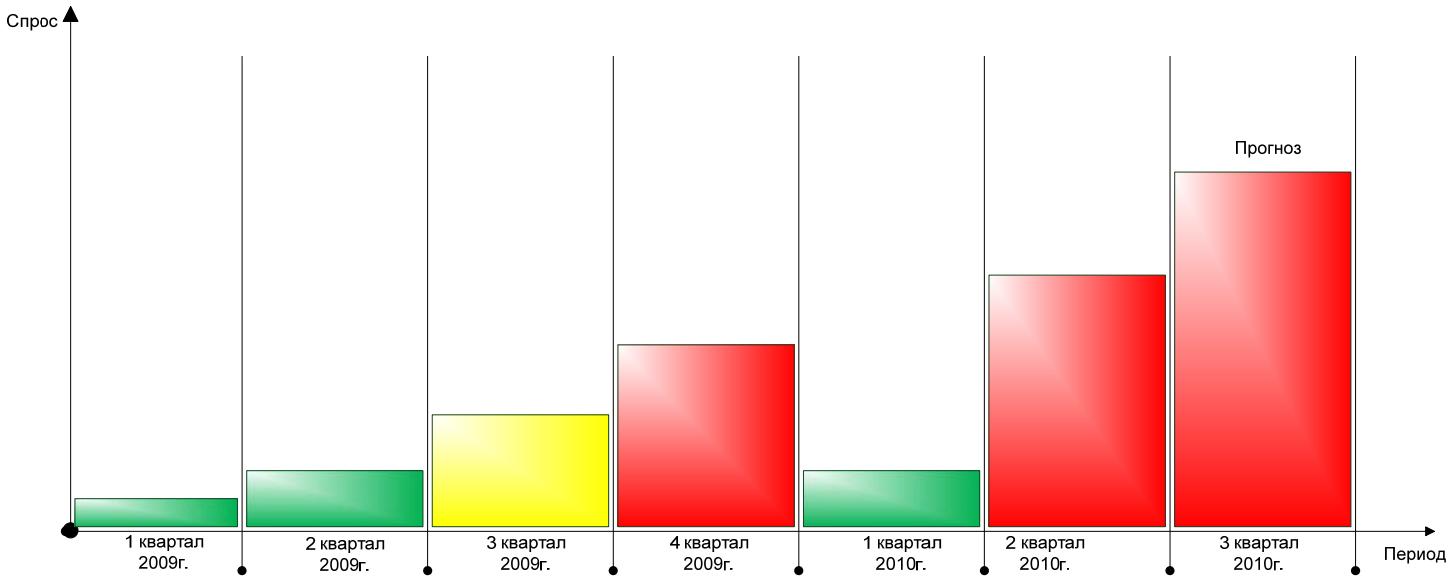
предложения об отсрочке срока 01.01.2010 (именно к этому сроку согласно № 152-ФЗ «О персональных данных» компаниям необходимо было привести все свои информационные системы персональных данных в соответствие с требованиями законодательства). Причем высказывались предложения о переносе данного срока как на один год, так и на целых три. И это случилось. В конце четвертого квартала 2009 года вышеупомянутый срок был передвинут на один год, и теперь deadline значится на отметке 01.01.2011. Многие операторы персональных данных вздохнули с облегчением, теперь спешка была ни к чему.

Начало 2010 года прошло уже в более спокойной обстановке. Длительные январские каникулы вкупе с переносом срока deadline на один год привели к резкому снижению спроса на услуги по защите персональных данных. Но стоит отметить, что не надолго. На этот раз новости пришли со стороны регуляторов – из ФСТЭК России. В начале 2010 года именно это ведомство официально сняло с нормативных документов по защите персональных данных гриф ДСП. А немного позже был издан приказ ФСТЭК России № 58 и решение ФСТЭК России. Суть данных событий сводилась к тому, что требования, предъявляемые к операторам в части защиты персональных данных, были снижены. ФСТЭК России упразднила два своих документа из «четверокнижия», заменив их приказом № 58. Наверное, в первую очередь это было следствием серьезного давления со стороны операторов персональных данных. Да и, к слову сказать, многие существовавшие требования реально были избыточными и финансово необоснованными. Так или иначе, именно данные события способствовали тому, что спрос на услуги по защите персональных данных начал возвращаться на уровень четвертого квартала 2009 года.

Второй квартал 2010 года, с точки зрения спроса, полностью перекрыл четвертый квартал 2009 года и даже частично превзошел его. С одной стороны, это обуславливалось снижением требований, с другой стороны, многие операторы, не успевшие начать проекты в конце 2009 года, начали активно работать в этот период. Таким образом, наблюдаемый на рынке рост спроса на услуги по защите персональных данных в 2010 году в целом является продолжением тенденции, начавшейся еще в 2009 году. Но есть одно существенное отличие: количество инициированных проектов в 2010

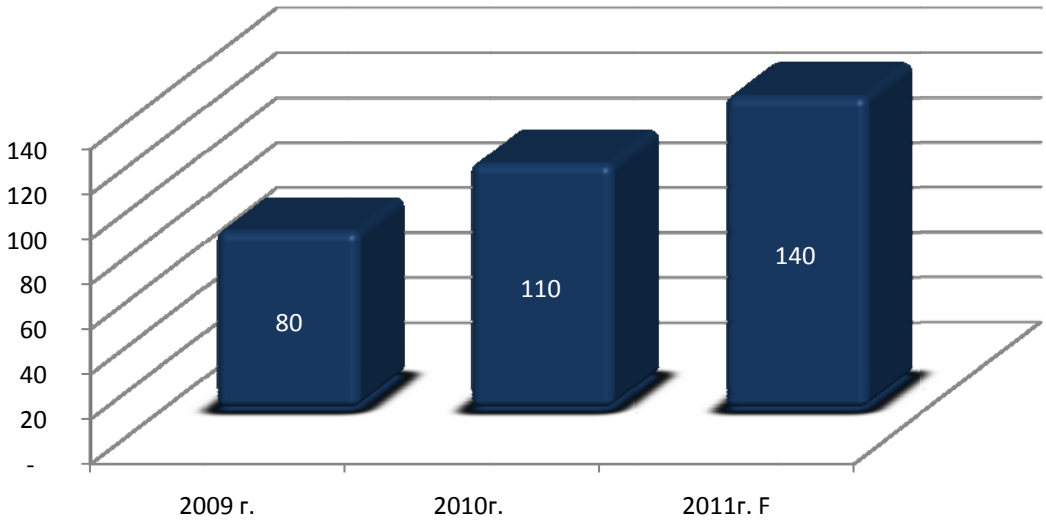
году обещает быть гораздо бóльшим. Если представить показатель спроса в графическом виде, то получится следующая схема:

Рисунок 6 Схема роста инициированных проектов по зашите персональных данных



Источник: LETA IT-company

Рисунок 7 Рост затрат российских организаций на защиту персональных данных ИБ в $млн



Источник: LETA IT-company

В настоящее время высказываются разные мнения касательно того, как будет развиваться спрос на услуги по защите персональных данных в 2011 году. Но все это лишь домыслы, сейчас же можно с уверенностью констатировать, что спрос на подобные услуги в течение 2010 года будет расти.

Стандарт Банка России

Мощное развитие получил отраслевой стандарт по информационной безопасности Банка России. В основном это связано с появлением требований по защите персональных данных в доработанном проекте СТО БР ИББС. Работы по поиску решений соответствия кредитных организаций требованиям 152-ФЗ начались весной 2009 года. Очевидного решения этой задачи не существовало. В рамках нескольких рабочих групп Ассоциации Российских банков была инициирована работа по подготовке поправок в 152-ФЗ и доработке СТО БР ИББС.

Менее чем за год активной работы были доработаны существующие и разработаны принципиально новые документы. Проекты документов новой версии стандарта можно найти на сайте Ассоциации Российских банков http://www.arb.ru/forums/conf152FZ/2/docs.php.

Новые документы, входящие в Комплекс БР ИББС:

- Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации;
- Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций БС РФ.

А также методические документы:

- Рекомендации по выполнению законодательных требований при обработке персональных данных в организациях БС РФ.

В своей сути документы разъясняют спорные положения федерального законодательства, постановлений правительства и требований регуляторов, а также содержат методические рекомендации по созданию адекватной СЗПДн.

Все документы согласуются с приказом ФСТЭК №58 и со стандартом ISO по защите персональных данных, который разрабатывался на основе ISO/IEC 27002-2005.

Примечательно, что в предлагаемых методических рекомендациях присутствуют положения, которые значительно упрощают приведение информационных систем персональных данных (ИСПДн) в соответствие требованиям регуляторов. Например, положение о том, что далеко не все автоматизированные системы, в которых обрабатываются персональные данные, являются ИСПДн, а только те, целью работы которых является обработка персональных данных. В соответствии с этим положением, например, Автоматизированные банковские системы не являются ИСПДн со всеми вытекающими положительными для оператора персональных данных последствиями.

В настоящий момент (весна 2010 года) новая версия стандарта не согласована с регуляторами в области защиты персональных данных (Роскомнадзор, ФСТЭК, ФСБ). В случае согласования новой версии стандарта и признания его требований достаточными для выполнения требований 152-ФЗ и требований регуляторов, банковское сообщество получит адекватные и адаптированные для отрасли документы, которые позволят выполнять работы по защите персональных данных в рамках СТО БР ИББС.

По факту окончания согласования начнется процедура создания саморегулируемой организации (СРО). Данная структура призвана выполнять функции гражданской организации-регулятора, в задачи которой будет входить регулирование вопросов защиты прав субъектов персональных данных в рамках вступивших в нее организаций. Пропуском в эту структуру будет ввод всей системы документов СТО БР ИББС, обязательной к исполнению. Дело в том, что все стандарты в РФ носят рекомендательный характер и обязательными могут стать только в случае введения внутренними приказами обязательности их исполнения.

В данном случае, признание СТО БР ИББС обязательным к исполнению позволяет кредитной организации значительно сократить проблемы с

созданием СЗПДн и одновременно запустить процесс приведения в соответствие признанному отраслевому стандарту.

Мы ожидаем, что факт принятия регуляторами по защите персональных данных новой версии СТО БР ИББС значительно увеличит число кредитных организаций, которые инициируют работы по обеспечению информационной безопасности в соответствии с данным стандартом. В результате стандарт банка России станет де–факто обязательным и начнется его массовое внедрение. Что приведет также к значительному росту консалтинговых услуг на рынке ИБ и увеличению затрат на ИБ. По нашим оценкам с 2011 по 2013 года банки затратят более $60 млн. на внедрение требований стандарта. Также успешный старт этого стандарта несомненно усилит тенденцию разработки других отраслевых стандартов.

Развитие применения систем менеджмента информационной безопасности

Состояние рынка систем менеджмента ИБ в соответствии с требованиями ISO 27001:2005 в 2009 году претерпел значительные изменения. Если раньше внедрение систем по большей степени преследовало цель маркетинговых выгод для компании, то в прошедшем году кризис внес свое коррективы: стали внедряться и реализовываться только «жизненнонеобходимые» для бизнеса системы.

Спустя более чем 5 лет с момента первой реализации в России СУИБ в соответствии с ISO 27001:2005 за последний год значительно вырос общий уровень понимания принципов управления в части ИБ, что нашло свое отражение в множественных запросах на построение комплексных систем информационной безопасности. Фактически в каждом тендерном запросе на комплексное обеспечение ИБ наряду с техническими подсистемами в один ряд встали требования на реализацию систем управления ИБ, в том числе и в соответствии с ISO 27001:2005.

2009 год явно обозначил границы и подходы к реализации систем управления исходя из фактической необходимости обеспечения ИБ и получения сертификата соответствия требованиям. На рынке в 2009 году сертификат был выдан или продлен компаниям, которым действительно критично для бизнеса наличия международного сертификата ISO 27001:2005, одновременно с этим с арены российского рынка сертифицированных компаний ушли те, для бизнеса которых поддержания сертификации стало невыгодной с точки зрения затрат на поддержания сертификации. Кризис, как естественных отбор в природе, оставил наиболее необходимые для выживания на рынке свойства компаний, те, которые оказались ненужными для выживания были убраны.

Прошедший год показал, что СУИБ, как целостный комплекс процессов, оказался менее востребованным, чем отдельные его элементы. Внедрение полномасштабной системы стало невыгодно с экономической точки зрения, что привело к фрагментарной реализации отдельных элементов управления: системы управления рисками, системы управления

инцидентами, системы повышения осведомленности, управления эффективностью внедренных решений по ИБ.

Свои коррективы внес и закон 152 ФЗ. Последний квартал 2009 – первый квартал 2010 год был отмечен достаточно сложными запросами на реализацию СУИБ не только в соответствии с международным стандартом, но и одновременно с учетом требований № 152-ФЗ.

Таблица 5 Сертифицированные СУИБ на начало 2010 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
15	IBS DataFort	LRQA	ISO/IEC 27001:2005

16	HandyBank	VNIIS	ISO/IEC 27001:2005

Источник: International Register of ISMS Certificates

Большинство компаний РФ и СНГ остаются преданными бренду BSI MS.

Оставаясь лидерами российского рынка сертификации, BSI MS диктует новые модные тренды на 2010 год. Уже сейчас мы наблюдаем появления новой линейки курсов по тематикам:

- Управление рисками информационной безопасности в соответствии с рекомендациями международного стандарта ISO/IEC 27005;
- Обеспечение непрерывности IT и коммуникаций в соответствии с рекомендациями британского стандарта BS 25777, в том числе и в рамках финансовых организаций с точки зрения реализации 242-П;
- Управление рисками организации. Стандарт BS 31100;
- Сертификация продукции на соответствие Директивам ЕС и т.д.

На текущий момент наблюдается пробуждение рынка как в части подготовке к сертификации, так и организации фактической информационные безопасности в соответствии с ISO 27001:2005. На текущий момент все большее число компаний приходит к пониманию, что СУИБ разумнее внедрять «снизу», сначала организовав базу из процессов обеспечения ИБ (управления активами, управления уязвимостями, изменениями, инцидентами), а уже после выстраивания этих процессов в компании внедрения полноценного анализа рисков ИБ.

Данный подход в 2010 году будет набирать обороты, потому что многие компании, реализовавшие у себя анализ рисков, без сопутствующих процессов ИБ, осознали на своем горьком опыте, что анализ рисков без актуальной информации об угрозах, уязвимостях, инцидентах, всех изменениях в бизнес-процессах не имеет никакого прикладного смысла ни для ИБ, ни для бизнеса компании в целом.

В 2010 году все больший спрос будет наблюдаться на автоматизацию процессов управления ИБ и организацию полноценной интеграции уже имеющихся средств ИБ для получения реальных механизмов управления

ИБ, об этом в частности свидетельствует выход и постепенное распространение на рынке новых программно технических систем по управлении ИБ и решений по их интеграции друг с другом. Сейчас подобные решения предлагают все крупнейшие вендоры рынка ИБ. Первым шагом в построении процессно-ролевой модели управления системы ИБ будет составление и анализ БД управления конфигурацией (CMDB — configuration management database), содержащей описание таких ресурсов компании, как ПО, технические средства, сотрудники и процедуры).

Все большая потребность в интеграции систем и выборе подходящего подхода по внедрению СУИБ привело к тому, что недавно был выпущен новый стандарт ISO / IEC 27003:2010 «Информационные технологии. Руководство по осуществлению системы менеджмента информационной безопасности». Использование данного стандарта в 2010 году снимет ряд вопросов по внедрению СУИБ. ISO/IEC 27003:2010 охватывает процесс СУИБ от начала производства до реализации, как разработать и спланировать проект СУИБ для обеспечения его успешной реализации.

Однако прямое использование моделей и стандартов ISO/IEC 27001 и ISO/IEC 17799:2005 для построения СУИБ затруднительно. Либо они слишком конкретизированные, а в любой организации, как правило, уже существует определенная система процессов, ролей, организационно-распорядительных документов информационной безопасности, которые необходимо интегрировать в систему управления ИБ. При этом не определяются приоритеты, так называемые «веса директив», которые обычно применяются в стандартах аудита. Либо, напротив, рекомендации носят слишком общий характер. Например, стандарты содержат либо набор контрольных директив, либо общий подход к системам менеджмента, то есть определяют, что нужно сделать, но не определяют, как это сделать.

2010 год будет направлен так же на интеграцию принципов ISO 27001:2005 и рекомендаций в частности ITIL (Information Technology Infrastructure Library, библиотека лучшего мирового опыта в области организации работы ИТ-службы), получивших достаточно широкое распространение

среди российских компаний. Данная необходимость продиктована еще и тем, что на российском рынке очень большое количество компаний, в которых подразделения информационной безопасности входят в департаменты ИТ.

Развитие некоторых сегментов средств технической защиты

Особенности использования сертифицированных средств при защите персональных данных

С момента выхода Федерального закона № 152-ФЗ «О персональных данных» и так называемого «четверокнижия» прошло уже достаточно много времени для того, чтобы операторы, обрабатывающие персональные данные, и системные интеграторы смогли в полной мере проанализировать данные документы и разработать необходимую методику по организации защиты персональных данных.

Большая часть положений № 152-ФЗ касается выполнения именно технических требований по защите персональных данных. Стоит отметить, что часть операторов уже построили систему защиты персональных данных в соответствии с данными требованиями. Системные интеграторы, со своей стороны, определили для себя некую «корзину» основных технических средств защиты информации, которые покрывают необходимые требования регулирующих органов для защиты персональных данных.

Существующие положения были достаточно жесткими, и в начале 2010 года произошли изменения, затрагивающие проекты по защите персональных данных:

05 февраля 2010 г. был издан приказ ФСТЭК России № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»;

05 марта 2010 г. было обнародовано решение ФСТЭК России, согласно которому были упразднены два методических документа ФСТЭК России, входящие в старое «четверокнижие»: «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Основные мероприятия по организации и техническому обеспечению безопасности персональных

данных, обрабатываемых в информационных системах персональных данных».

Каждый желающий, решившись ознакомиться с приказом № 58 и приложением к нему, сразу же прочтет следующее: «В настоящем Положении не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также вопросы применения криптографических методов и способов защиты информации».

Это как раз и не удивительно – криптография всегда была, есть и будет вотчиной именно ФСБ России. Так что при выборе средств, где задействована криптография (например, при создании канала связи, обеспечивающего защиту передаваемой информации), оператору или системному интегратору необходимо пользоваться регламентирующими документами ФСБ России.

Что касается требований к применению сертифицированных средств защиты информации, то согласно новому Положению использование средств защиты информации (СЗИ), прошедших оценку соответствия на отсутствие недекларируемых возможностей (НДВ), является обязательным только для информационных систем персональных данных (ИСПДн) класса К1. Для ИСПДн остальных классов использование СЗИ, прошедших данный вид оценки соответствия, является необязательным и оставляется на усмотрение оператора.

С классом К1 всё более или менее понятно. Что касается ИСПДн класса К2 и К3, то согласно тексту приказа № 58 средства защиты должны проходить в установленном порядке процедуру оценки соответствия. Согласно Федеральному закону «О техническом регулировании» существует три формы оценки:

- обязательная сертификация;

- добровольная сертификация;

- декларация соответствия.

Согласно Положению и приказу № 58 оператор, обрабатывающий персональные данные класса К2 и К3, для построения системы защиты может использовать любые СЗИ, прошедшие сертификацию ФСТЭК России по ТУ, что в значительной мере расширяет возможность выбора СЗИ. Тем не менее при выборе СЗИ необходимо руководствоваться требованиями, описанными в Приложении 1 к Положению о методах и способах защиты информации в информационных системах персональных данных.

Если говорить более простыми словами, то эту же мысль можно выразить так: если для защиты персональных данных в системах класса К2 и К3 заявлено некое средство защиты, то оно должно иметь сертификат, свидетельствующий о том, что данное средство выполняет те самые необходимые функции, о которых было заявлено.

Это значительно упрощает выбор и расширяет перечень технических средств, которые могут быть использованы при построении систем защиты персональных данных.

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 по-прежнему, к сожалению, достоверных данных по продажам антивирусных средств нет. Эта ситуация не изменилась и в 2009 году. Жесткая конкуренция между вендорами приводит к тому, что собственная статистика продаж используется компаниями как метод борьбы, поэтому полностью доверять опубликованным данным об объемах продаж нельзя.

Во многом это объясняется особенностью российского рынка, а именно наличием крупных отечественных вендоров. Если западные компании сотрудничают с исследовательскими организациями и как публичные компании раскрывают свои данные, то отечественные компании долгое время старались не раскрывать полностью статистику своих продаж, поэтому даже в опубликованных данных можно легко найти много противоречий.

Впрочем, ситуация начала постепенно меняться. В начале 2010 года основные игроки на российском рынке представили отчеты, которые более адекватно отражают действительную картину и соотносятся с другими источниками, такими как данные дистрибьюторов и опросы, проводимые различными социологическими компаниями, методология, которая была использована компанией LETA в прошлом исследовании.

Сопоставив различные источники, можно определить, что объем рынка АВЗ в России в 2009 году равнялся $195 млн, в 2008 году он составлял $175 млн.

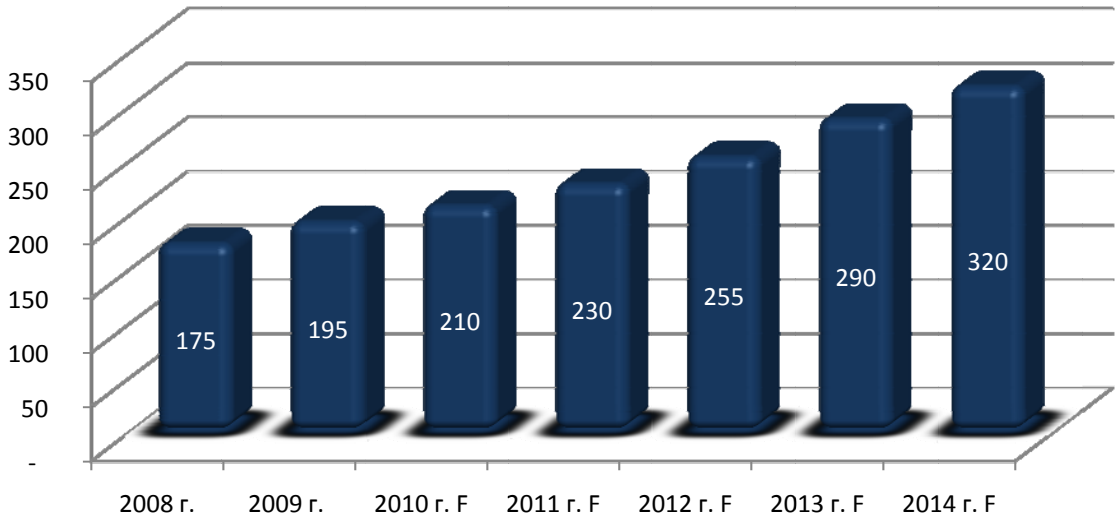
Независимо от разных оценок можно выделить тройку лидеров по проданным лицензиям.

Таблица 6 Тройка лидеров на рынке антивирусных средств

Лаборатория Касперского
ESET
Symantec

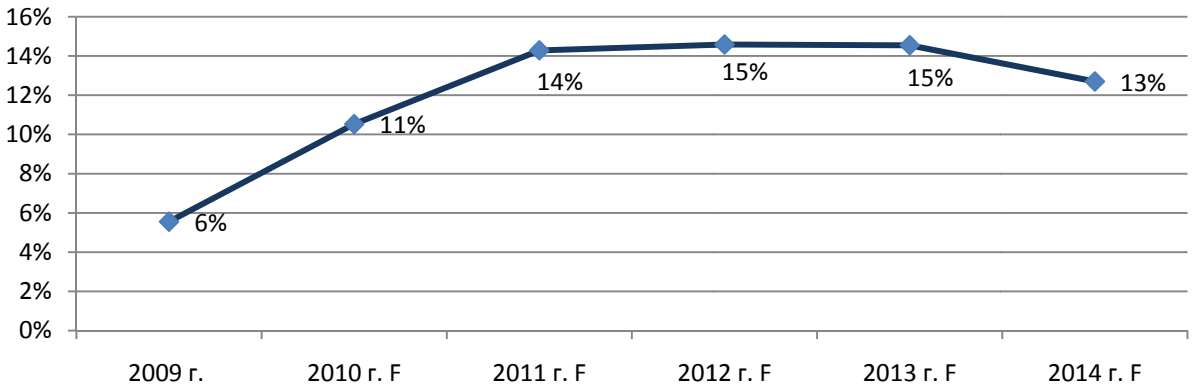
Источник: LETA IT-company

Рисунок 8 Роста рынка средств антивирусной защиты в $млн



Источник: LETA IT-company

Рисунок 9 Темы роста рынка средств антивирусной защиты в %



Источник: LETA IT-company

По оценкам LETA IT-company за 2009 год не произошло существенно перераспределения долей вендоров. Первенство удерживает «Лаборатория Касперского»,доля рынка этой компании за год практически не изменилась. ESET прочно занял второе место и увеличивает свою долю, в основном за счет игроков второго эшелона.

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

В условиях кризиса рынок антивирусных средств поддерживало несколько факторов:

1. Ритейл. Как это ни парадоксально, но именно ритейл меньше всего пострадал от кризиса. Частные пользователи продолжили покупать и продлевать антивирусы. Опасение за безопасность данных на личных компьютерах превысило привычку ставить «пиратские» версии ПО. Поэтому можно с уверенностью утверждать, что рынок SOHO и домашних пользователей продолжит поступательное движение и в будущем.

2010 год можно назвать годом борьбы за ритейл. Именно через ритейл будут определяться лидеры рынка. У ведущих вендоров доля ритейловых продаж превысила 50%. Именно победители в этом сегменте и будут определять будущее лицо рынка АВЗ в России. Сегодня «Лаборатория Касперского» и ESET имеют долю рынка 80-85%, сколь либо заметные продажи в ритейле имеют также компании Symantec и DrWeb. В будущем неплохой потенциал роста в этом сегменте есть у компании Symantec.

Компании взяли на вооружении все существующие инструменты и теперь используют их в продвижении своих товаров, которые стали фактически FMCG. Используется широкий спектр способов продвижения, начиная от прямой рекламы на радио и наружной рекламы и заканчивая попытками выстраивания «особых» взаимоотношений с ритейлом. Таким образом, можно сказать, что АВЗ - первый в России среди ПО, кому удалось стать по-настоящему массовым товаром.

2. Требования регуляторов. Антивирусные средства являются неотъемлемой частью системы защиты ИСПДн. Но применение антивирусов в некоторых ИСПДн требует их сертификации по высоким классам. И в конце 2009 года развернулась «гонка сертификаций». ESET -

первый западный вендор, который получил сертификат ФСТЭК России класса «К1».

«Лаборатория Касперского», DrWeb и ВирусБлокАда заявили о том, что имеющеюся у них сертификаты можно отнести к этому классу и они могут быть использованы для защиты информации в ИСПДн до 1-го класса включительно. Остальные вендоры завили, что де-факто отказываются от этого рынка. Но новые документы, изданные ФСТЭК России, позволяют использовать простую сертификацию по ТУ для низкоуровневых ИСПДн. В начале 2010 года Symantec и TrendMicro подали документы на сертификацию по ТУ. Если они получат необходимые сертификаты, то можно будет говорить об окончании «войны сертификатов» и появлении двух групп вендоров: вендоров с «высокими» сертификатами и вендоров с «низкими» сертификатами.

Учитывая то, что ФСТЭК России готовит отдельные документы по антивирусной защите (а значит, важность сертификации только возрастет), то можно ожидать, что все вендоры, работающие в России, получат те или сертификаты. И наличие таких сертификатов будет определять место вендора на государственном и корпоративном рынке.

В сегменте крупного бизнеса заметны как западные компании: Symantec, TrendMicro, MacAfee, ESET, а также российская компания «Лаборатория Касперского».

За исключением Symantec, в 2009 году ни одна из крупных компаний не начала программ по масштабному продвижению и не создала в России своей службы технической поддержки, что для России чрезвычайно важно.

Но со сменой руководства в TrendMicro можно ожидать резкого прорыва данного вендора в России. Возможно, новый директор McAfee в России, назначенный в июне 2010 года, также усилит позиции этой компании.

В результате лидерство в сегменте большого бизнеса осталось за лидерами рынка в целом: «Лаборатория Касперского», ESET, Symantec. И этот отрыв только увеличивается. И если другие компании не реализуют в ближайшее время серьезных и капиталоемких программ продвижения, то можно

констатировать, что ведущая тройка и дальше будет отрываться от конкурентов, и нынешняя структура рынка просуществует не менее 5-7 лет.

Решения по обеспечению контроля соответствия требованиям ИБ

На российском рынке информационной безопасности (ИБ) за несколько прошедших лет сложилась скрытая проблема, связанная с его реактивным развитием. А именно, используемые на практике решения ИБ внедрялись в качестве незамедлительной реакции на возникшие локальные угрозы ИБ. Так, с появлением первых вирусов появились антивирусы, затем – средства межсетевого экранирования в ответ на необходимость противодействия внешним вторжениям. Не так давно были осознаны проблемы инсайдерских угроз, - и организации стали внедрять системы DLP. Реактивный подход к развитию системы ИБ, несомненно, упрощает обоснование соответствующих проектов и демонстрирует практические результаты на выбранных участках. Однако, в организациях, внедривших множество частных решений ИБ, подразделения, отвечающие за корпоративную политику безопасности и управления рисками, по существу, утрачивали контроль над выполнением комплекса требований ИБ. Рынок ИБ сложился излишне технологическим и слабо привязанным к деятельности бизнес-подразделений.

Иной подход проактивного развития системы информационной безопасности исповедуют лишь немногие организации. Данный подход подразумевает цельную картину состояния ИБ организации и заблаговременное (проактивное) внедрение мер по обеспечению безопасности. Обязательными элементами такого подхода являются:

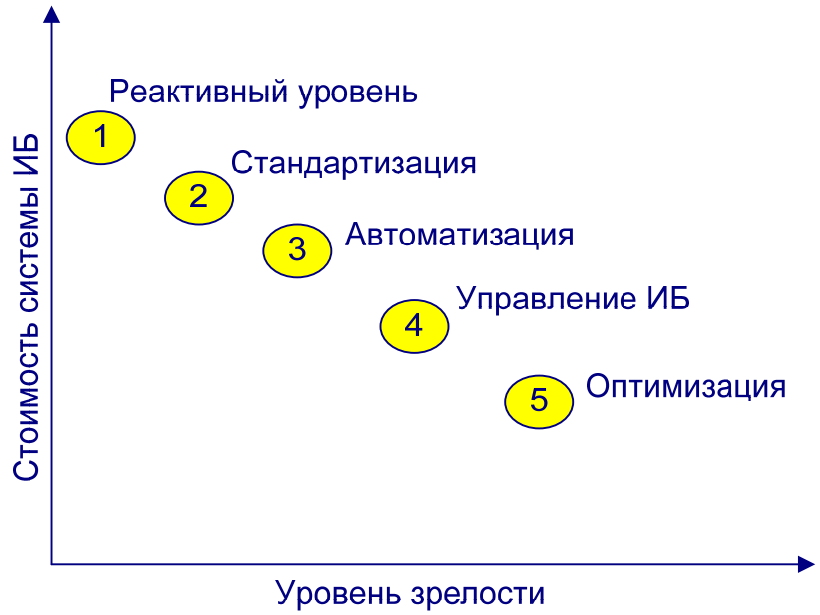
- Наличие действующей политики ИБ организации. Корпоративная Политика разрабатывается с учетом нормативных и законодательных требований ИБ.
- Наличие процессов контроля соответствия состояния ИБ требованиям корпоративной политики ИБ.
- Анализ результатов выполнения проверок на регулярной основе с оценкой и приоритезацией.
- Выполнение компенсирующих мер на основе риск-ориентированной оценки.

Проактивный подход подразумевает анализ не только существующих, но и возможных будущих угроз, и заблаговременное планирование и принятие компенсирующих мер. Несмотря на кажущуюся сложность организационной проработки вопросов ИБ, приверженность организации такому подходу обеспечивает сокращение капитальных и операционных издержек за счет нижеперечисленных факторов:

- Снижение затрат на выполнение мер по обеспечению совместимости с внешними требованиями ИБ.
- Меньшее количество недочетов по результатам аудитов ИБ. По сложившейся практике, в проектах подготовки и аттестации по требованиям ИБ каждая организация проходит ряд неудачных попыток. Затраты на исправление несоответствий существенно завышающих итоговую стоимость проекта.
- Непрерывность бизнес-процессов. При снижении общего уровня рисков перебои информационных систем, обеспечивающих бизнес, возникают существенно реже.
- Снижение рисков финансово-значимых утечек информации.

В 2010 году произойдет массовое движение организаций в сторону повышения уровня зрелости системы ИБ, обусловленное, прежде всего, экономическими показателями.

Рисунок 10 Общий уровень расходов на ИБ организаций различного уровня зрелости



Источник: LETA IT-company

Общий уровень расходов на ИБ организаций различного уровня зрелости.

В настоящее время большая часть организаций находится между 2 и 3 уровнем зрелости: применяются стандартизованные по предприятию в целом средства ИБ и инфраструктурные решения, но не во всех предприятиях автоматизированы процессы выполнения проверок на соответствие корпоративным требованиям. Используемые сканеры безопасности (например, MaxPatrol, Qualys) автоматизируют не только процессы нахождения уязвимостей, но и выполняют необходимые проверки настроек серверов, баз данных, активного сетевого оборудования.

Следующего, 4-го уровня зрелости достигли лишь немногие организации. В таких компаниях разработаны и действуют единые для всей компании политики безопасности. Управление политиками (их создание, распределение, контроль исполнения и принятие корректирующих мер)

как правило, выполняются в рамках специализированных технических решений.

На 5-м уровне зрелости предполагается выстраивание процессов управления ИБ таким образом, что используемое техническое решение выполняет не только проверку состояния защищенности, но и автоматически запускает процессы исправления обнаруженных уязвимостей (в том числе, установка обновлений систем ИБ, заведение заявки в ServiceDesk на исправление настроек сервера, удаление неактивных записей из каталога пользователей).

В 2010 году рынок ИБ России активно идет от 2,3-го к 4-му уровню зрелости, переходя к решению четкой высокоуровневой задачи в сфере управления рисками. «Под» данную задачу создается комплексное решение, рассматриваемое как часть внутрикорпоративной системы безопасности, и как элемент связности системы защиты информации в сети взаимодействующих предприятий. На этом пути ключевую роль начинает играть разработка и внедрение различных взаимоувязанных стандартов ИБ. Соответствие им станет главной долгосрочной тенденцией корпоративного рынка ИБ. Таким образом, наступает «Эпоха Compliance».

Для решения задач управления ИБ организациями используются различные инструменты для:

- создания политик безопасности (DS Кондор, Positive Technologies MaxPatrol , netIQ, Symantec, OpenPages, Acher, Numara, Paisley, Compliance Spectrum, Microsoft SharePoint),
- инвентаризации хранимых информационных ресурсов (Symantec, Websense, McAfee, RSA Security),
- выполнения технических проверок (Qualus, MaxPatrol, neqIQ, Symantec, tripware, RSA Security, McAfee, Configuresoft, DS Гриф),
- заполнения показателей состояния ИБ в виде вопросников и построения отчетов о соответствии стандартам (Symantec, Modulo, Agiliance, McAfee, Relational Security, Archer, Omanda),
- исправления обнаруженных несоответствий (Symantec ServiceDesk, HP Software, LANDesk, FrontRange, Remedy).

Не все решения распространены в России, не все интегрированы между собой. Поскольку разработку политик, инвентаризацию защищаемых активов, выполнение технических проверок, заполнение вопросников и исправление несоответствий (все операции, что особенно актуально для компаний 5-го уровня зрелости) удобнее всего вести на единой платформе; ожидается появление интегрированных решений одного или нескольких производителей, позволяющие выполнять весь комплекс описанных действий. По состоянию на середину 2010 года таким решением, имеющим практику использования в России, является продукт Control Compliance Suite единственной компании – Symantec.

Ввиду наложения ряда факторов:

- появления требований ИБ, исполнение которых становится обязательным для нескольких типов организаций (в частности, введение требований закона «О персональных данных» 152-ФЗ, требования к организациям – эмитентам платежных карт PCI DSS, стандарт Банка России СТО БР ИББС);
- послекризисные экономические условия, в которых организации стали обращать пристальное внимание на эффективность и долгосрочную отдачу от инвестиций;

внедрение систем автоматизации управления политиками ИБ приобретет одно из важных направлений развития рынка ИБ начиная с 2010 года.

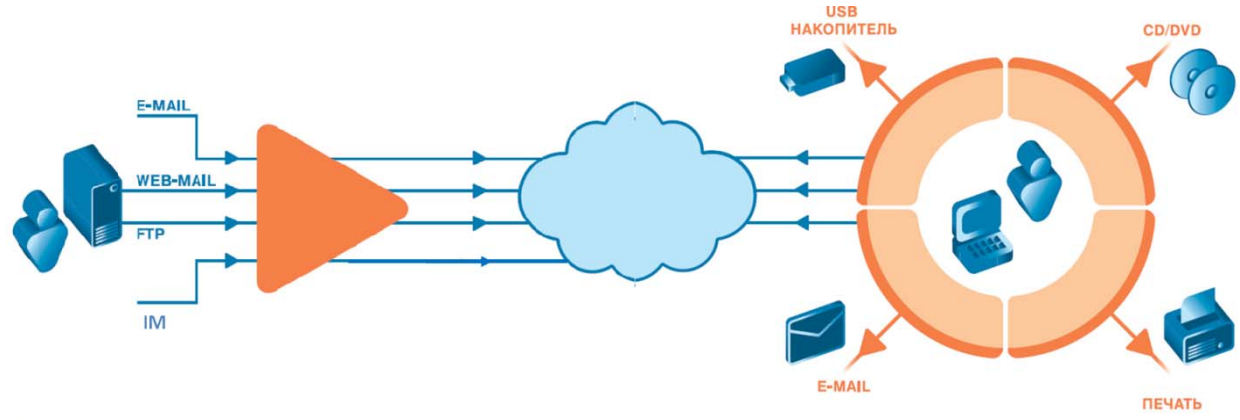
DLP системы

Самым быстрорастущим новым сегментом рынка является DLP (Data Loss Prevention). Но и в условиях кризиса он продолжил расти на 5%. Основной причиной роста является то, что в ходе развития собственно ИТ-рынка в ИТ-системы предприятий было переведено большое количество конфиденциальных данных, которые требует защиты прежде всего от утечек изнутри компании.

За 2009 год решения класса DLP стали повсеместно распространенными и на рынке окончательно сформировалось понимание, что стоит за DLP-системами. Согласно известному рынку представлению, основное назначение DLP – обеспечить защиту от случайного или намеренного распространения конфиденциальной информации со стороны сотрудников, имеющих доступ к информации в силу своих должностных обязанностей. Одновременно, любая DLP-система может быть настроена и для борьбы со злонамеренными инсайдерами.

Решение DLP объединяет в себе контроль над перемещением информации как на уровне коммуникаций с внешней сетью, так и на уровне оконечных устройств пользователей (рис. D1). А в дополнение, важной функцией классического решения DLP является возможность сканирования хранящихся файлов и баз данных для обнаружения мест расположения конфиденциальной информации.

Рисунок 11 Информационные потоки, контролируемые при помощи системы DLP



Источник: LETA IT-company

Каждый разработчик DLP решения предлагает свою собственную архитектуру развертывания, но, в общем, принципиальные модули системы следующие:

- перехватчики/контроллеры на разные каналы передачи информации;
- агентские программы, устанавливаемые на оконечные устройства;
- центральный управляющий сервер.

Перехватчики анализируют потоки информации, которая может быть выведена из периметра компании, обнаруживают конфиденциальные данные, классифицируют информацию и передают для обработки возможного инцидента на управляющий сервер. Перехватчики могут быть как для копии исходящего трафика, так и для установки в разрыв трафика. В последнем случае потенциальная утечка может быть остановлена системой DLP.

Контроллеры для обнаружения хранимых данных запускают процессы обнаружениях в сетевых ресурсах конфиденциальной информации. Способы запуска обнаружения могут быть различными: от собственно сканирования от сервера контроллера до запуска отдельных программных агентов на существующие серверы или рабочие станции.

Контроллеры для операций на рабочих станциях распределяют политики безопасности на оконечные устройства, анализируют результаты деятельности сотрудников с конфиденциальной информацией и передают данные возможного инцидента на управляющий сервер.

Агентские программы на оконечных рабочих местах замечают конфиденциальные данные в обработке и следят за соблюдением таких правил, как сохранение на сменный носитель информации, отправки, распечатывания, копирования через буфер обмена.

Управляющий сервер сопоставляет поступающие от перехватчиков и контроллеров сведения и предоставляет интерфейс проработки инцидентов и построения отчетности.

Таким образом, решения DLP нацелены на централизованный контроль за всеми инцидентами нарушения политик безопасности по отношению к конфиденциальной информации.

Очевидной тенденцией развития технологической платформы систем DLP стало то, что разработчики стали активно интегрировать свои DLP решения с другими подсистемами, такими как:

- Управления правами на документы (Enterprise Digital Rights Management). Яркие примеры – интеграция RSA DLP Suite и Microsoft AD RMS, интеграция Symantec DLP с рядом других решений в том числе Microsoft RMS, Liquid Machines, Oracle IRM. DLP отыскивает хранимые копии конфиденциальных документов и передает в систему EDRM инструкцию по обеспечению защиты.
- Криптографическая защита файлов и контейнеров. Типичные примеры – McAfee Endpoint Encryption и McAfee Host DLP, Symantec Endpoint Encryption и Symantec DLP, Verdasys.
- Подсистемы сбора и анализа событий безопасности и управления инцидентами. Примеры – Symantec DLP и Symantec SIM, RSA DLP Suite и RSA eNvision.
- Системы контроля соответствия требованиям безопасности. Пример – Symantec DLP и Symantec Control Compliance Suite (версии 10).
- Системы контроля доступа к портам рабочих станций и устройствам.

Как видно из примеров, ряд решений DLP интегрированы с решениями других разработчиков.

Другой тенденцией развития рынка DLP заключается в том, что заказчики стали уделять существенное внимание консалтинговой составляющей процесса построения системы противодействия утечки информации. Особенностью решений DLP является то, что в систему необходимо передать логику, на основании которой будет происходить классификация конфиденциальной / открытой информации. Встроенные механизмы DLP

позволяют максимально автоматизировать и облегчить процессы обучения системы благодаря используемым методам. Несколько лет назад существовало только два основных метода описания условий классификации:

1) грифование секретных документов (требовались простановка текстовой метки или изменение свойств каждого документа вручную);

2) подбор слов и выражений (подчас требовалась работа лингвиста для составления словаря характерных для бизнеса организации терминов, на основании которых должна реагировать система), а также регулярные выражения.

Сегодня в решениях DLP появился широкий набор комбинированных методов:

3) цифровые отпечатки документов и их частей (в систему вводятся сотни тысяч документов одной командой);

4) цифровые отпечатки баз данных (в систему вводятся выгрузки из баз данных клиентов и прочей структурированной информации, которую важно защитить от распространения);

5) статистические методы (повышение чувствительности системы при повторении нарушений).

Современные системы класса DLP включают в себя набор готовых правил реагирования на обнаружение, например, данных кредитных карт, российских паспортов, стандартных форм финансовой отчетности. Но наиболее значимым в системах DLP стал метод цифровых отпечатков, построенных на основе образцов конфиденциальных данных, имеющихся в обращении.

Если подходить к вопросу внедрения DLP масштабно, потребовалось бы выполнить классификацию и инвентаризацию конфиденциальной информации, находящейся в обращении. Другая крайняя сторона – ограничиться первоначальным набором выборки конфиденциальных документов (со временем такая настройка теряет актуальность, если не

обновлять выборку). Рабочим вариантом для многих заказчиков стал средний уровень проработки базы конфиденциальных документов:

- во-первых, при внедрении системы DLP выделяются наиболее критичные 1-3 бизнес-процесса, в рамках которых выделяют 2-4 наиболее критичных категории информационных ресурсов (например, персональные данные, стратегические разработки);
- затем процессы обращения выделенных групп информации описываются и прописываются во внедряемой системе;
- разрабатывается необходимая нормативная база для обеспечения процессов обновления базы обучения системы DLP;
- дополнительно устанавливается набор стандартных отраслевых шаблонов и правил реагирования для обнаружения других групп конфиденциальных документов.

Выполнение описанной консалтинговой подготовки к запуску системы DLP увеличивает объем работ в рамках проекта, зато появляется значительная и долгосрочная финансовая отдача от проекта построения системы DLP.

Таким образом, описанные две тенденции (интеграция DLP с другими классами решений и расширение консалтинговой составляющей), проекты построения систем противодействия инсайдерским угрозам будут комплексными, охватывать наиболее критичные для бизнеса угрозы.

Основными игроками рынка DLP на 2009 год стали более десятка мировых компаний, среди которых стоит выделить решения, присутствующие на российском рынке и уже используемые отечественными организациями:

– Symantec Data Loss Prevention;

– Websense Data Security Suite;

– McAfee Host Data Loss Prevention.

Кроме того, в российских организациях распространено использование DLP российского разработчика InfoWatch Traffic Monitor.

На конец 2009 года в России лидером рынка в денежном выражении являлась российская компания InfoWatch со своими продуктами.

Но ситуация с 2009 года радикально изменилась. Лидерами по новым внедрениям стали продукты компаний Symantec, Websense и McAfee. На их долю приходилось до 70% от всех новых проектов.

Особый интерес представляют решения для SMB сектора. Именно он станет драйвером роста, но пока за исключением McAfee Host Data Loss Prevention на рынке нет конкурентоспособных продуктов

Затраты российских организаций на DLP решения составили в 2009 году $33 млн. В дальнейшем рост рынка будет сохраняться на уровне 15% в год.

Расследование инцидентов информационной безопасности.

Бывает, что, несмотря на хорошую политику безопасности, подкреплённую современными техническими решениями, происходят утечка информации, хакерские атаки и другие инциденты. Сейчас вопрос «как защищать?» уже не столь актуален. Этой теме посвящено большое количество трудов, разработано множество теорий. А вот вопрос «что делать, если произошёл инцидент?» вызывает головную боль. Компьютерная преступность, преступления в информационном поле, инциденты в области информационной безопасности - вот о чём пойдёт речь в данной статье.

Термин «компьютерная преступность» появился впервые в США в начале 60-х годов. Именно тогда, соответственно, были совершены первые преступления с использованием информационных технологий. Основные признаки компьютерных преступлений были сформулированы в 1974 году на Конференции Американской ассоциации адвокатов в Далласе в 1979 году: Тогда были выделены три направления компьютерных преступлений:

- использование или попытка использования компьютера, вычислительной системы или сети компьютеров с целью получения денег, собственности или услуг;
- преднамеренное несанкционированное действие, имеющее целью изменение, повреждение, уничтожение или похищение компьютера, вычислительной системы, сети компьютеров или содержащихся в них систем математического обеспечение, программ или информации;
- преднамеренное несанкционированное нарушение связи между компьютерами, вычислительными системами или сетями компьютеров.

Шли годы, менялись термины: «информационные преступления», «преступление, совершённое с использованием информационных

технологий», «кибер преступление». Но суть оставалась прежней, и с каждым годом количество таких инцидентов увеличивалось в геометрической прогрессии. За последние 10 лет количество инцидентов увеличилось в 23 раза, но эта статистика раскрывает только зарегистрированные случаи. А, как известно, большинство компаний не стремятся сообщать о произошедшем нарушении. На данный момент также выделяют три направления компьютерных преступлений:

- преступления против информационной безопасности;
- преступления, в которых электронная информация является орудием или средством совершения другого преступления;
- преступления, совершаемые с использованием компьютерной и иной электронной техники.

Правительства западных стран быстро осознали, что компьютерные преступления представляют серьёзную угрозу национальной и экономической безопасности. Поэтому начиная с 70-х годов в западных странах в рамках органов внутренних дел создаются специальные подразделения по борьбе с компьютерной преступностью, в высших учебных заведениях в рамках курса криминалистики читают методики расследования информационных преступлений, ведётся научная работа.

Благодаря поддержке государства в виде больших инвестиций в исследования в области компьютерной криминалистики и поддержке законодательства в странах, таких как Германия и США, отделы по борьбе с кибер терроризмом вели и ведут эффективную работу.

Отдельно стоит затронуть и юридическую сторону вопроса. Так как разговор идёт о преступлениях, нарушения и инцидентах, то, естественно, что юридически должно быть оформлено и наказание. Поэтому одновременно с созданием подразделений на государственном законодательном уровне шла работа по созданию юридической базы. И действия законодательной власти были скоординированы настолько, что соответствующие законы появились достаточно быстро и сразу же начали работать.

Необходимо отметить, что за границей сильно развиты и коммерческие службы по расследованию информационных инцидентов. Отметим, хотя бы знаменитый FoundStone (www.foundstone.com), который на данный момент является подразделением McAfee. FoundStone стал образцом для организаций и специалистов по всему миру.

Россия по мнению экспертов отстаёт от Запада в компьютерной криминалистике на 5 лет. На данный момент анализ норм действующего в России уголовного, уголовно-процессуального и административного законодательств показывает отсталость, неточность и противоречивость нормативной базы. Такие же тенденции прослеживаются в научных, методических и учебных работах по уголовному праву, криминалистике, судебной экспертизе, оперативно-розыскной деятельности и информатике.

Но, тем не менее, нельзя не отметить и значительные сдвиги в этой области. Увеличивается финансирование органов внутренних дел Российской Федерации по борьбе с компьютерными преступлениями. Отдельное внимание уделяется повышению квалификации сотрудников и совершенствованию криминалистических методик. В рамках органов внутренних дел созданы отделы «К», которые специализируются именно на компьютерных преступлениях.

В Интернете можно собрать статистику по делам, раскрываемым органами внутренних дел: получается, что лишь 10% раскрытых преступлений – это «высокотехнологичные» преступления, которые совершили высококвалифицированные хакеры. В тоже время в Интернете существуют десятки фишинговых сайтов, постоянно ведутся DDOS атаки и т.д.

Хотелось бы обратить внимание на ещё одну проблему Российских государственных служб - большую вероятность появления информации об инциденте в прессе, что очень нежелательно для коммерческих компаний. Ведь информация о том, что компанию атаковали хакеры, произошла утечка конфиденциальной информации – это удар по престижу фирмы. Поэтому компании предпочитают замалчивать информацию о случившихся инцидентах, создавая у нарушителей чувство безнаказанности. Кроме этого, до сих пор некоторые компании продолжают использовать нелицензионное ПО, таким образом, они не могут позвать на помощь

государственные спецподразделения, пока не передут полностью на лицензионное программное обеспечение.

А что делать, если расследование нужно произвести незамедлительно или недопустимо афиширование инцидента, произошедшего в компании? Тогда на помощь могут прийти организации, которые занимаются расследованием компьютерных преступлений на коммерческой основе.

На Западе такие компании давно заняли свой сегмент в рынке безопасности, то в России ситуация выглядит несколько иначе. Гораздо выгодней внедрять системы безопасности, и получать гарантированные деньги, чем заниматься деятельностью, которая может и не принести результат. И деятельность эта требует огромных усилий с научно-исследовательской точки зрения. По сути, штат подобных организаций должен состоять из людей, знания и навыки которых аналогичны знаниям и навыкам людей, совершающих компьютерные преступления. Расследование может зайти в тупик, и становится непонятно каким образом рассчитывать сумму затрат на работы. А самое главное, что когда дело касается расследования по сути преступления, то речь уже идёт о контакте не с образом злоумышленника, о котором идёт речь при оценке рисков, а контакте с конкретным преступником \ нарушителем \ злоумышленником или группе таковых. А для этого нужна специальная подготовка.

Основными направлениями данного рынка в России и в мире являются:

- Реагирование на инциденты (Incident response)
- Расследование инцидентов (eDiscovery)
- Компьютерная криминалистика (Digital Forensic)
- Мониторинг инцидентов
- Юридическое сопровождение инцидентов

На данный момент на рынке России присутствует только один игрок, комплексно реализующий все направления этого рынка – Group-IB.

Анонс. Исследование по итогам 2010 года

Исследование, которые выйдет в середине 2011 года будет посвящено развитию рынка информационной безопасности и отдельных сегментов. В этом исследовании будут проанализированные старые и новые факторы, влияющие на рынок ИБ. Из новых факторов необходимо отметить:

- Закон «Об электронной цифровой подписи»
- PCI DSS

Также в новом исследовании специалистами LETA и других компаний будут проанализированы и описаны следующие сегменты рынка ИБ:

- защита виртуальных сред
- защита АСУ ТП
- сетевая безопасность

Специалисты LETA IT-company готовы принять предложения по новому исследованию. Если Вы или Ваша компания обладаете признанным авторитетом на рынке ИБ, знаниями о факторах и сегментах влияющих на развитие информационной безопасности, то LETA с удовольствием даст возможность принять участие в исследовании по итогам 2010 года.