КОНКУРЕНТНАЯ ЭКОСИСТЕМА И ДРУЖЕЛЮБНОЕ СОПЕРНИЧЕСТВО НА РЫНКЕ АНТИВИРУСНОГО ПО

Интервью с Александром Ерофеевым, руководителем управления маркетинговых исследований ЗАО «Лаборатория Касперского»
(e-mail: eemeapr@kaspersky.com)

«Лаборатория Касперского» — международная группа компаний с центральным офисом в Москве, специализирующаяся на разработке систем защиты от вредоносного и нежелательного ПО, спама и хакерских атак. Компания входит в четверку ведущих мировых производителей программных решений для обеспечения информационной безопасности.

Александр, как правильно называется рынок, на котором функционирует компания «Лаборатория Касперского», — рынок антивирусного программного обеспечения?

— Не совсем правильно, поскольку наш рынок не ограничивается лишь производством антивирусного программного обеспечения (ПО)[1], однако нет какой-то красивой формулировки, которая бы называла этот рынок. В западной литературе обычно используется понятие не «антивирус» (*antivirus*), а «антималвэр» (*antimalware*[2]) — более точная формулировка. Для обозначения этого рынка можно употреблять словосочетание «рынок борьбы с вредоносным кодом» или «рынок управления защитой контента» (*Security Content Management, SCM*) — так его определяет аналитическое агентство *IDC*[3]. Но для России привычнее звучит «антивирус», поэтому в интервью мы можем обозначать рынок, на котором мы функционируем, как рынок антивирусного ПО.

[1] Свободная энциклопедия «Википедия» определяет антивирусное программное обеспечение (антивирус) как любую программу для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом. (Все сноски в интервью — *прим. ред.*)

[2] От *malicious software* — вредоносные (злонамеренные) программы, т. е. любые программы, действующие против интересов пользователя или владельца компьютерной системы, например вирусы, черви, троянцы, шпионящее ПО и др.

[3] *IDC* является ведущей международной компанией, специализирующейся на исследованиях рынков *IT* и консалтинге.

Какие товарные сегменты можно выделить на рынке антивирусного ПО?

— Можно выделить несколько основных сегментов. Первый — **защита контента** *(Information Content Security, ICS)* всеми способами: проактивная и реактивная защита контента, защита от утечки на корпоративном уровне, защита контента на персональном компьютере, защита контента компьютерной сети, защита контента во время пересылки сообщения, защита веб-трафика, защита веб-приложений, шифрование данных. Иногда шифрование данных выделяют в отдельное направление, считая, что это даже не *IT*-технология, но я с этим не согласен.

Второй сегмент, но в основном корпоративный, — **управление правами доступа** *(Identified Access Management, IAM).* Когда вы начинаете пользоваться каким-то компьютерным ресурсом, для проверки права доступа у вас запрашивают учетную запись, в принципе, это некий прототип *IAM*, в каком-то смысле альтернативная парадигма первому направлению, возможно, в будущем это станет единым направлением.

Третий сегмент — **управление инцидентами в системе безопасности** (*Security Incidents Management, SIM).* Подход состоит в том, что хорошая безопасность достигается за счет профилактики. Сейчас на рынке доминирует парадигма, что с существующими опасностями невозможно бороться, нужно лишь стремиться минимизировать вред, который они несут, т. е. последствия реализации этих опасностей. В отличие от первого и второго направления, которые не предполагают минимизацию опасности, а нацелены исключительно на защиту от них, третий подход заключается в воздействии на сами опасности. Предполагается, что если делать хороший софт, поддерживать его в порядке, не устанавливать сомнительные программы, то к вам никто и ничто проникнуть не сможет. Этот подход, как и второй, бывает только на корпоративном уровне.

«Лаборатория Касперского» занимается всеми направлениями?

— Мы пока занимаемся только первым направлением — защитой контента, да и в целом сегодня на рынке наблюдается специализация. Вместе с тем у нас есть технологии и решения в рамках наших корпоративных продуктов, связанные с управлением инцидентами в системе безопасности (*SIM)*, и мы активно развиваем эти технологии. В области управления правами доступа *(IAM)* мы пока отдельных продуктов не делаем, хотя некоторыми технологиями обладаем. Другие ведущие игроки не имеют таких технологий или они находятся в зачаточном состоянии, поскольку разработки в этой сфере требуют от компаний дополнительных особых компетенций.

Возможно, когда-то можно будет наблюдать конвергенцию всех трех направлений, которая произойдет за счет перехода большого количества компаний и процессов к облачным вычислениям, виртуализированным машинам или ресурсам, в результате чего все три сегмента будут объединены. По факту мы сейчас наблюдаем гетерогенизацию *IT*-среды, полного замещения одного типа деятельности другим не происходит. Постоянно увеличивается количество операционных систем, усложняется обмен информацией, появляются новые варианты использования виртуальных сред, в частности из-за активного использования смартфонов и мобильных телефонов, их соединения с компьютерами. Так происходит усложнение пользовательской инфраструктуры, и пока неясно, к чему именно оно приведет. Одно можно сказать точно, что конвергенция рано или поздно произойдет.

Какие типы компаний функционируют на рынке антивирусного ПО?

— Все компании нашего рынка мы разделяем на три эшелона. Это условное деление. Первый эшелон — пятерка компаний, суммарная доля которых состав-

ляет около 70–75% мирового рынка антивирусного ПО, который оценивается в 10–12 млрд долл. Российский рынок — чуть меньше 200 млн долл. Первый эшелон включает следующие компании: *Symantec* (США), *McAfee*[4] (США), *Trend Micro* (Япония), «Лаборатория Касперского» (Россия), *Sophos* (Великобритания)[5]. Это пятерка ведущих мировых разработчиков программного обеспечения. По данным IDC, доля нашей компании на розничном потребительском рынке в Западной и Восточной Европе, США и на Ближнем Востоке составляет 25–30%. Мы стремимся войти в тройку мировых производителей защитных решений и уже недалеки от цели.

Второй эшелон — около дюжины компаний, функционирующих на мировом рынке, но имеющих относительно небольшую долю, а также национальные компании, имеющие существенную долю на крупнейших региональных рынках. К этой группе относятся такие производители, как Webroot (Webroot, США[6]), Beijing Rising International Software (Китай), Panda Security (Китай), BitDefender SRL (Румыния), Agnitum (Россия), *QuickHeal* (Индия) и др.

Третий эшелон — национальные компании, которые работают на своих небольших региональных рынках и за их пределы не выходят. В данной группе, например, «ВирусБлокАда» (Белоруссия), «Доктор Веб» (Россия), *MKS* (Польша), второстепенные китайские компании: Джибинк, Кейсофт. Они производят продукты исключительно для своего рынка. Их основные конкурентные преимущества — не инновационный продукт высокого качества, а хорошее знание каналов продаж и умение продвигать продукцию на своем региональном рынке. Типичный владелец такой компании — человек, который 10 лет назад создал компанию, продукт, нашел клиентов, например среди местных госструктур. Однако конкурентная среда изменилась, и в современных условиях ему трудно конкурировать, поскольку у него нет ни передовых технологий, ни финансовых ресурсов, ни потенциала для увеличения доли на местном рынке и выхода на мировой рынок. Единственное, что его спасает сегодня, — знание своего родного национального рынка и умение «давить» на патриотизм. Для него это стратегический рынок, и отступать ему некуда.

Можно ли выделить географический рынок, который для «Лаборатории Касперского» является стратегическим?

— Непростой вопрос, наверное, для нас — весь мир. Мы видим для себя большой потенциал роста на рынке США, это самый большой в мире рынок, где мы быстро растем сейчас. Там есть определенные сложности, но очень много возможностей. Также перспективными, на наш взгляд, являются рынки Ближнего Востока и Африки — там происходит бурная первичная компьютеризация. Уровень жизни в странах этого региона невысокий, но мы привыкли работать в государствах с ВНП на душу населения около 1500 долл. Не так давно к ним относилась и Россия, а многие страны постсоветского пространства и сегодня недалеко продвинулись по этому показателю. Мы знаем, что на таких рынках можно неплохо зарабатывать, знаем, как именно это делать. Еще один очень перспективный рынок — Юго-Восточная Азия, там есть сильные местные игроки, более проблемный язык, больше местной регуляции, более закрытые рынки, например рынки Китая и Южной Кореи достаточно закрыты. Но, в отличие от рынка арабских и африканских стран, все понимают, что эти рынки перспективны.

[4] 19 августа 2010 года *McAfee* была приобретена компанией *Intel* за 7,68 млрд долл.

[5] В скобках указано расположение штаб-квартир компаний и их историческая страновая принадлежность, сегодня компании первой пятерки являются глобальными.

[6] Рынок антивирусного ПО США — крупнейший региональный рынок в мире.

Российский рынок не является для вас стратегическим?

— Мы не выделяем российский рынок отдельно, потому что он достаточно небольшой, в доходах компании его доля составляет ниже 15%. Вместе с тем российский рынок не сильно отличается от рынков других стран, входящих с ним в одну группу, чтобы говорить о нем как об особенном. Все страны мира, где работает наша компания, мы разделяем на группы.

Александр, какие группы стран вы выделяете?

— Мы разделяем страны на четыре группы.

Первая группа — развитые страны, к которым мы относим Западную Европу и Северную Америку. Вторая группа — развивающиеся страны: Восточная Европа, Ближний Восток, Африка, Латинская и Южная Америка. Они достаточно однородны, к примеру, разница между Казахстаном и Чили невелика, если не касаться политической системы. Есть языковые различия — в Казахстане почти все население говорит на русском, в Чили — на испанском, но это достаточно массовые языки, не китайский с множеством наречий и не суахили. Население стран примерно похоже. Обе страны сырьевые. Стремятся к экономической модернизации. Не являются лидерами в своем регионе, но при этом и находятся не на последнем месте. Третья группа — это Юго-Восточная Азия, которую мы рассматриваем отдельно от развивающихся рынков, поскольку там своя специфика. Прежде всего это относится к Китаю. Четвертая группа — Япония, поскольку, несмотря на то, что японский рынок развит, он не похож на развитые рынки первой группы. Япония — другая планета со своими особенностями выхода на этот рынок и работы на нем. Поэтому мы не можем объединить японские операции с операциями в странах первой группы. Еще раз отмечу, что это наше внутреннее деление.

В чем специфика российского рынка по сравнению с другими рынками этой же группы?

— Разница, конечно, есть, но какой-то особенной специфики нет. Среди его особенностей можно выделить следующие.

Первая особенность заключается в высокой роли государства в России. Хотя это не единственная страна, где государство играет значительную роль, она так же велика, например, в странах Ближнего Востока. Вторая особенность — цикличность рынка, его рост сильно зависит от роста цен на сырье. Так, в 2008 году цены на сырье упали, и российский рынок антивирусного ПО также снизился в долларовом выражении примерно на 15%, в то же время во всем мире рынок рос. Третья особенность — для «Лаборатории Касперского» российский рынок является родным, мы его знаем лучше других, здесь наша штаб-квартира, здесь мы национальный бренд.

Четвертая особенность — поскольку российский язык для нас родной, в отличие от зарубежных компаний нам не нужно преодолевать языковые барьеры входа, переводя техническую документацию на русский язык и русифицируя наши продукты.

Как вам удается удерживать лидирующую позицию на российском рынке, и насколько она устойчива?

— На российском рынке нам удается удерживать лидирующую позицию по двум причинам. Во-первых, мы давно работаем на этом рынке, начали работать здесь в конце прошлого века, когда рынок не представлял интереса ни для кого, кроме российских компаний. Тогда было три мифа о России: 1) отсутствие компьютеров и Интернета; 2) стопроцентное пиратство; 3) плохая экономическая ситуация, которая не будет улучшаться. Любой аналитик 15 лет назад сказал бы, что в России нечего делать. Но у нас не было другой возможности, кроме как работать здесь. Теперь мы знаем российский рынок лучше, чем кто-либо еще.

Во-вторых, у нас очень сильная команда. К нам часто приходят, и от нас редко уходят. Мы достаточно конкурентоспособны на рынке труда, входим в четверку крупнейших компаний и предлагаем хорошие условия для работников. Ключевая команда наших разработчиков находится в России, хотя у нас есть центры разработки и эксперты за рубежом. В общей сложности в компании работает около 2300 человек.

Каковы конкурентные преимущества «Лаборатории Касперского» на мировом рынке?

— Первое конкурентное преимущество — наша идеология анализа не существующих, а будущих угроз. Никто не может знать будущее. Но в стремлении понять, какие угрозы могут возникнуть, мы уделяем внимание эвристическим технологиям, позволяющим определить будущую угрозу еще до ее возникновения, идентификации и изучения. Таким образом, мы прогнозируем будущие вредоносные действия на основе анализа существующих проблем в *IT*-системах. Следствие этого — наша антивирусная экспертиза, носящая проактивный характер и основанная на хорошем знании вредоносного кода, глубоком понимании того, как он работает, что позволяет обеспечивать для наших пользователей более высокий уровень защиты.

Второе конкурентное преимущество заключается в том, что абсолютное большинство используемых нами технологий — наши разработки. Данное преимущество обеспечивает несколько положительных моментов. Во-первых, это позволяет добиваться более высокого качества защиты наших продуктов, поскольку мы не собираем его из разных чужих алгоритмов и технологий, полученных на условиях лицензирования, делая тем самым сборный конструктор. Во-вторых, и это не менее важно, указанное преимущество позволяет нам эффективно контролировать издержки, поскольку мы практически не зависим от других компаний, нам не нужно платить за чужие технологии. В-третьих, наличие большого количества собственных технологий обеспечивает большую безопасность — нашу и наших клиентов.

Третье конкурентное преимущество — это наш бренд. Я имею в виду не положительный имидж, а именно сильный бренд. Положительный имидж — немного расплывчатое понятие, предполагающее хорошее, доброе отношение. Бренд — это то, что вызывает доверие, а на нашем рынке доверие является очень важным ресурсом, поскольку мы имеем дело с безопасностью. В данном случае бренд выступает в роли знака качества, обеспечивая доверие к нам.

Можно ли выделить какие-либо особенности конкурентного поведения на рынке антивирусного ПО?

— Можно. Эти особенности обусловлены тем, что ***IT*-бизнес представляет собой особую экосистему**, отличную от других систем, например, от ритейла или пассажирских авиаперевозок, где наблюдается низкий уровень взаимодействия и высокий уровень взаимозаменяемости. Если одна из авиакомпаний разоряется или отказывается от какого-то маршрута, ее место занимает другая компания. Потребитель ничего не потеряет (мы не говорим о доминирующем положении и монопольном сговоре), он выберет другую компанию со схожим уровнем цен и сервиса и будет летать на тех же самолетах, что и раньше. В приведенном примере нет такой сложной экосистемы, как у нас, где связи между компаниями более тесные, и эффекты экосистемы проявляются в большей степени.

Александр, какие эффекты экосистемы Вы имеете в виду?

— Это эффект взаимозависимости и эффект синергии. **Эффект взаимозависимости** заключается в том, что зависимость между компаниями изменяет конкуренцию между ними, порождая уважение и толе-

рантность друг к другу. Нередко компании нашей отрасли используют чужие технологии, лицензируя их друг другу. «Лаборатория Касперского» не испытывает необходимости в покупке чужих технологий, поскольку обладает собственными ресурсами для их развития. Мы лицензируем свои технологии многим известным компаниям, в том числе конкурентам, которые считают, что изобретение собственной технологии потребует у них значительных временных затрат и средств, но не обязательно приведет к хорошим результатам.

Взаимозависимость как бы преломляет конкуренцию, выводит ее на новый уровень, делает менее конфликтной, порождает уважение к прямому конкуренту, который предоставляет важную технологию.

Более сложным эффектом нашей экосистемы является **эффект синергии**. Он заключается в том, что ни одна компания в одиночку не сможет противостоять всем угрозам. А несколько компаний, образуя целую экосистему защиты информации, где каждая из них имеет свою специфику, могут. Одни компании умеют хорошо шифровать данные, другие — определять вредоносный код и сортировать его на правильный и неправильный, третьи — уничтожать вредоносный код.

Только вместе эти компании могут должным образом понизить общий уровень компьютерной угрозы, ограничивая распространение вирусов во всем мире. Здесь можно провести аналогию — представьте город, в котором есть большая медицинская клиника. Для того чтобы жители были здоровы, в клинике должны работать разные врачи: терапевты, хирурги, окулисты, отоларингологи, неврологи и т. д. Врачи только одного профиля не помогут людям.

Но, делая общее дело, мы все равно конкурируем. Конкурируя, стремимся делать наши продукты лучше: дешевле, удобнее, но самое главное — надежнее, чтобы они лучше защищали. Если это дешево и удобно, но не защищает, то оно никому не нужно даже бесплатно. Как следствие — конкурентная экосистема способствует снижению уровня компьютерных угроз, окружающих нас. Без этой экосистемы уровень угроз был бы значительно выше. Снижение конкуренции за счет сильного сокращения количества конкурентов или раздела ими рынков внесет негативные изменения в экосистему и в конечном итоге может привести к неблагоприятным последствиям, которые можно охарактеризовать как ***IT*-апокалипсис**.

Александр, расскажите подробнее об IT-апокалипсисе.

— Представьте некую очень популярную операционную систему, которая длительное время не испытывала угроз со стороны конкурентов, или конкурентные угрозы находились на очень низком уровне. Стимулов к развитию и защите от конкурентов не было, нарастало расслабление, не возникало мыслей: «Если ты этого не сделаешь, то это сделает твой конкурент», а были другие мысли: «Когда будет угроза — я это сделаю». Нужно понимать, что все современные компьютерные технологии сетевые, и скорость распространения вируса в них очень высока и приближается к скорости света с небольшим замедлением сети, в отличие от биологических вирусов, которым нужны время и особая среда.

Предположим, что кто-то знает, как сделать «плохой» файл, чтобы взломать эту популярную, но плохо защищенную операционную систему и выложить его на профильный сайт в Интернет, чтобы все, кому это нужно, могли его скачать, опробовать в деле и рассказать о своем успехе другим. Нетрудно представить, что будет, если практически одновременно на профильных сайтах в Интернете будут размещены сотни или тысячи аналогичных «плохих» файлов. Если бы антивирусные компании работали в неконкурентной или низкоконкурентной среде, это могло бы привести к тому, что большинство из них оказались несостоя-

тельными перед таким «плохим» файлом, т. е. у десятков тысяч людей во всем мире в течение нескольких дней сгорел (или заблокировался) жесткий диск, украли деньги, взломали аккаунт в соцсети и стали рассылать с него разные компрометирующие сообщения, требуя заплатить деньги за то, чтобы оставить аккаунт в покое. Пользователи поймут, что они не защищены, полиция не будет справляется с потоком потерпевших, ставших жертвой киберпреступников, парламентариев будут винить в том, что они допустили такую ситуацию.

Результатом описанного *IT*-апокалипсиса, возможно, станет прекращение существования Интернета в том виде, в каком он существует сегодня. Пользователям выдадут электронные паспорта, все сайты будут проходить обязательную сертификацию и станут жестко привязанными к национальной юрисдикции, международный трафик будет закрыт, поскольку на своей территории проще принять необходимые меры и обеспечить безопасность. Но эти меры могут оказаться неэффективными в решении проблемы, поскольку интернет-пространство едино. Так, в случае недавней атаки на российские сервера *Livejournal*[7], по словам представителя этого сервиса Светланы Иванниковой[8], не использовалось ни одного российского ботнета[9] (англ. *botnet* от *robot* и *network*). Атака велась с территории таких стран, как Индия, Китай, Йемен, Южная Корея и даже Япония, Пакистан, усложняя противодействие ей тем, что российским правоохранительным органам нужно осуществить правосудие на территории чужих стран. Это осложняется, например, тем, что законодательство в Пакистане по происхождению англосаксонское, а написано на урду[10], там другой язык и другая этическая система. К тому же нужно пробудить интерес у правоохранительных органов Пакистана к помощи правоохранительным органам России — Пакистану никакого ущерба нанесено не было. Здесь выручит только налаженное сотрудничество между правоохранительными органами и международная дружба стран. В упомянутом случае сотрудничество налажено не было.

Это один из сценариев *IT*-апокалипсиса, есть и другие. Предугадать истинные последствия не представляется возможным, но можно утверждать, что последствия будут весьма плачевны и сильно ощутимы. Мы не просто так говорим о конкурентной множественной экосистеме антивирусного программного обеспечения. На наш взгляд, эта система не просто удобна. Возможно, комфортнее было бы одной компании-победителю, когда все остальные компании ушли с рынка, а она заполучила весь рынок. Но экосистема, включающая многие компании, является необходимой составляющей среды нашего бизнеса, без которой возможность его существования и развития была бы поставлена под сомнение.

---

[7] Около 16 часов 30 марта 2011 года началась *DDoS*-атака на Живой журнал — как выяснилось, мощнейшая в истории этого ресурса. На несколько часов *LiveJournal* оказался практически недоступен для пользователей и вернулся к более-менее нормальной работе только после полуночи — подробнее см. http://lenta.ru/articles/2011/03/31/battleofevermore/.

[8] http://www.bbc.co.uk/russian/russia/2011/04/110406_livejournal_ddos_attack. shtml.

[9] Ботнет — это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на компьютере жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера. Ботнет обычно используется для нелегальной или неодобряемой деятельности — рассылки спама, плохого кода, перебора паролей на удаленной системе, направления множественных запросов на сайт до тех пор, пока сайт не перестанет работать, и других атак.

[10] Урду — индоевропейский язык, родственный хинди, возникший в XIII веке. Урду является одним из двух официальных языков в Пакистане (второй — английский), несмотря на то, что лишь 7% населения считает его родным языком.

Можно ли говорить о каком-то оптимальном для описанной Вами экосистемы числе компаний-производителей антивирусного ПО на рынке?

— Две компании на этом рынке явно недостаточны. Присутствие на рынке, например, только двух компаний приведет к деградации экосистемы, росту цен и падению качества. Предположу, что и экосистема, и рынок, и потребители выиграют, если на рынке будет несколько компаний — пять–шесть. Это обеспечит конкуренцию, и, соответственно, более низкие цены и высокое качество. При меньшем числе компаний не будет достаточного обмена идеями, достаточной исследованности области компьютерной безопасности, разнообразия взглядов и подходов к защите, пользы от того, что мы делаем. Это становится особенно важным в динамичной, быстроменяющейся среде, например в области изучения биологических вирусов работает много разных команд, как и в нашей сфере. В некотором роде мы являемся научно-исследовательским институтом, и лучше, чтобы их было несколько, тогда будут разные школы мысли. Мы, к примеру, анализируем угрозы не так, как *Trend Micro*.

В силу того, что это коммерческая деятельность, прямого обмена знаниями между компаниями нет, но по факту все равно мы видим, что, например, *Symantec* придумал такую-то технологию, мы думаем, почему они это сделали. *Или McAfee* видит, что «Лаборатория Касперского» начала заниматься тем-то и тем-то, они думают, зачем мы это делаем. Производители антивирусного ПО очень хорошо знают друг друга. Это связано с тем, что рынок достаточно взаимозависимый, и нередки случаи, когда мы видим продукты наших конкурентов, а они наши, а также с тем, что в сфере антивирусного ПО регулярно проходит множество конференций, панельных дискуссий, имеются и другие формы общения. Несмотря на то, что рынок конкурентный, компании достаточно открыты друг другу. В результате все выигрывают.

Наш рынок необычен — особенность заключается в том, что мы боремся с внешней неконтролируемой агрессивной и быстро меняющейся средой. Это фундаментальное отличие антивирусного бизнеса, например, от бизнеса по производству бухгалтерского программного обеспечения или его более продвинутого родственника *ERP*. Там компании-производители ни с какой средой не борются, они просто создают автоматизированное решение для определенного процесса. Мы находимся в ситуации, когда нас окружает большое количество разнородного, постоянно развивающегося вредоносного кода (*malware*) — социальных технологий облегчения ваших карманов, технологий компрометации, воровства данных и хулиганства. Здесь большее количество компаний лучше, чем меньшее.

Иногда можно услышать высказывания о том, что конкуренция — это война. При каких условиях конкуренция на вашем рынке может приобрести форму войны?

— На самом деле представление о конкуренции как о войне — очень узкий частный случай, как правило, связанный с тем, что рынок никуда не растет, и между сторонами накопились конфликты и противоречия, которые мирным путем не решаются. В реальности компании все-таки конкурируют не столько между собой, сколько за потребителей, стремясь в долгосрочной перспективе завоевать их сердца. И в таком смысле называть конкуренцию войной не совсем корректно. Что касается конкуренции на рынке антивирусного ПО, где функционирует «Лаборатория Касперского», то, я думаю, правильнее расценивать конкуренцию как интенсивное, но достаточно дружелюбное соперничество.

Описанный характер конкуренция имеет по следующим причинам. Во-первых, ни мировой, ни российский рынки пока не насыщены и продолжают достаточно интенсивно расти, причем растут и корпоративный, и потребительский секторы. Во-вторых, ме-

жду компаниями, которые на этом рынке работают, нет никаких фундаментальных противоречий. В-третьих, среда *IT*-бизнеса мало агрессивна по своей природе, и люди, которые хотят вести себя агрессивно, гораздо лучше реализуются в других сферах, здесь им будет трудно сделать карьеру.

На нашем рынке нет войн, хотя он достаточно конкурентный. Но, пока он растет, было бы неразумно выбрать военные действия в качестве эффективного способа достижения результатов. Очень мало компаний в нашем бизнесе ведут неэтичный бизнес. Компании имеют схожие продуктовые линейки, но у всех есть своя специфика, которая позволяет говорить о том, что компании растут в своих нишах.

Вы часто сталкиваетесь со случаями недобросовестной конкуренции?

— Недобросовестной рекламы в России, Европе и США в явном виде я не помню. Возможно, потому, что ее можно сделать только один раз, поскольку ее могут заметить не только конкуренты, но и государственные регуляторы, такие как ФАС России. В США по закону можно делать прямое сравнение конкурирующих продуктов, но там я тоже не помню таких примеров.

Некоторые компании не так давно активно использовали различные технологии антипиара своих конкурентов в Интернете через социальные сети, блоги, форумы, сайты компаний-производителей, используя разных «ботов» и «троллей». Однако, как я говорил, потребители обучаются и умеют отличать потребителей, оставляющих реальные отзывы, от специалистов, которым за эти псевдоотзывы платят. Сейчас таких случаев стало существенно меньше, а сегодняшний рынок — не настолько брутальный.

Насколько велика угроза со стороны пиратских антивирусов?

— Пиратский антивирус — игрушка для людей, у которых очень много свободного времени. Другие пиратские программы достаточно один раз установить для того, чтобы потом продолжительное время пользоваться, не обновляя их, поскольку после обновления они могут перестать работать. Наши программы не обновлять нельзя, поскольку антивирусная база очень быстро устаревает, и для того, чтобы быть защищенным, нужно обновлять ее несколько раз в день. Естественно, что с «пиратками» обновляться невозможно, там обновление не работает. Можно, конечно, рыскать по просторам Интернета в поисках пиратских ключей, но это требует немалого времени, а ключи к тому же имеют нехорошую особенность постоянно обнуляться — мы тоже не смотрим на нелегальное использование нашего ПО с излишней толерантностью и блокируем их. Ключ функционирует недолго и достаточно скоро перестает работать. Найти бесплатные пиратские ключи можно только на специальных сайтах. Но они представляют собой «вирусную помойку», нафаршированы разными вредоносными кодами, троянскими программами и фишинговыми ссылками. Чтобы их посещать, нужно иметь хороший антивирус и желательно заходить туда не со своего компьютера. Если вы идете на сайт за нелицензионным ключом, то очевидно, что у вас этого ключа нет, и вы не защищены от последних угроз. Иначе зачем вы туда идете? Вы демонстрируете уязвимость и становитесь легкой мишенью для кибернедоброжелателей[11].

Для корпоративного сегмента лицензионное программное обеспечение — единственный вариант обеспечения безопасности. В небольшой компании можно конечно поставить и «пиратки», но это плохо с точки зрения безопасности и нелегально с точки зрения закона. В крупной компании это еще более затруднительно. В частном сегменте

[11] По данным российской компании *Group IB*, занимающейся расследованием киберпреступлений, в 2010 г. российские хакеры похитили 1,3 млрд долл, мировой рынок киберпреступности в том же году оценивался в 7 млрд долл.

тоже нет тенденции использования пиратских лицензий.

Какую опасность для вас представляют бесплатные антивирусные программы?

— Компании, производящие бесплатные антивирусные программы, живут за счет бизнес-модели *Freemium*. Классический *Freemium* — базовый пакет услуг бесплатный, все остальное за деньги (апгрейд, звонки на телефоны, спецсервисы). Данная бизнес-модель предполагает два сценария. Хороший сценарий — компания начнет зарабатывать на этом бизнесе, плохой — не начнет зарабатывать, но создаст большую пользовательскую базу, которую можно будет кому-нибудь продать[12].

Freemium-продукты на нашем рынке живут по второму сценарию. Они замедляют наш бизнес, но в то же время мне неизвестны ситуации, когда из-за их присутствия мы стали терять долю рынка. Пользователи избирательны и склонны к обучению. Поставив себе бесплатный продукт и столкнувшись с тем, что он пропускает вирусы, работает с регулярными сбоями, они рано или поздно поймут, что это не лучший способ защитить свой компьютер. На наш взгляд, главный вред от этих компаний состоит в том, что они нарушают экосистему.

А технологии freemium-компаний не имеют ценности?

— В нашей сфере сначала появились платные компании, потом появился *freemium*. В отличие от *Skype'a*, который был инновационным *freemium*-продуктом, никаких инновационных технологий у большинства *freemium*-компаний на нашем рынке нет. Бизнес-модель *freemium* не предполагает больших затрат, поэтому антивирусные продукты, создаваемые в рамках такой модели, не являются инновационными и, как правило, обеспечивают недостаточный уровень защиты. Более того, ситуация постоянной нехватки денег, в которой они находятся до тех пор, пока не продались, вынуждает их сокращать издержки.

Основные направления сокращения издержек следующие.

Первое направление — экономия на каналах дистрибьюции. Например, продажа продуктов только через Интернет без красивых коробок.

Второе направление — экономия на поддержке. На ней экономят почти все *freemium*-компании. Если у вас стоит бесплатный антивирус, у вас что-то не работает, или вы не можете избавиться от вируса, вам некуда обратиться за помощью. Правда, есть форумы доброжелателей, на которых вам дадут совет, но совет любого качества, в том числе хакеры могут дать совет, удобный им самим.

Третье направление — экономия на качестве защиты. Это происходит по двум причинам. Первая — качественная защита достаточно сложная и громоздкая, компьютер будет «тормозить», поэтому у таких компаний есть соблазн делать продукт попроще — по аналогии с фильтром: чем больше отверстия, тем быстрее течет вода и хуже фильтрация. Вторая причина — снижение затрат как на собственные разработки, так и на покупку лицензий, в результате все сводится к тому, что данные компании используют только один алгоритм защиты. Однако, даже если это очень хороший алгоритм, он не позволяет обеспечить достаточный уровень защиты, и любой эксперт в области антивирусного ПО скажет, что нельзя защитить пользователей, используя, например, только сигнатурный анализ[13].

[12] Например, имея в базе 20 млн пользователей и договорившись «продать» каждого из них за 10 центов, владельцы бизнеса получат 2 млн долл.

[13] Сигнатурный анализ — это определение вируса по части кода программы путем сравнения этого кода с базой программных кодов вирусов. Это хороший метод, но он не является абсолютно надежным, поскольку не решает проблемы с новыми вирусами, которые еще не изучены, проблему с фишингом, проблемы в уязвимостях систем и др.

Бытуют мнения, что *freemium*-компании борются с жадностью производителей платного антивирусного ПО, являясь своего рода белыми рыцарями, которые спасают мир. Но, вникнув в проблему глубже, становится очевидной иллюзорность подобных взглядов — во *freemium*-компаниях нет подвижников, есть бизнесмены. В одних случаях такие компании финансируются инвестиционными фондами, в других являются придатками крупных *IT*-компаний, которые субсидируют другой свой бизнес, в третьих случаях — предприниматели, которые поздно зашли на рынок, поняли, что для них *freemium* — единственная возможность на этом рынке уцелеть.

Сложно ли сейчас выйти на рынок антивирусного ПО с бизнес-моделями, отличными от freemium?

— За последние два года никаких новых компаний в области антивирусного ПО на рынке не появилось. Причины просты: наш бизнес достаточно сложен. К примеру, можно открыть ресторан, если есть деньги. Создать бизнес будет не очень сложно, но если это ваш первый ресторан, и вы не гений ресторанного бизнеса, то, скорее всего, вы быстро прогорите. В антивирусном ПО все сложнее, потому что нужно заслужить доверие пользователей — они вряд ли будут пользоваться продукцией неизвестной компании. Кроме того, нужно обладать антивирусной экспертизой, поддерживать ее, к тому же рынок должен знать о вашей экспертизе и доверять ей.

Общая логика конкуренции такова, что первая компания, вышедшая на рынок, получает большую долю, чем вторая, а вторая — больше, чем третья и т. д. Стоимость входного билета возрастает в порядке очередности. И тем, кто заходит десятым, ничего не остается, кроме как начать раздавать продукт бесплатно в ожидании того, что все его оценят и будут готовы покупать его. Но это маловероятно, поскольку данный продукт десятый, и мало кто будет помнить десять названий антивирусного ПО. Можно вкладывать большие деньги в торговую марку, но для того, чтобы добиться мировой известности марки в объеме около 20%, нужно вложить в продвижение 50–100 млн долл. Вместо того, чтобы тратить такие деньги на маркетинг, можно просто начать раздавать продукт бесплатно, тогда, возможно, удастся потратить меньше и добиться большей эффективности.

В выборе бизнес-модели *freemium* определяющую роль играет стратегия компании. Для построения успешного рентабельного бизнеса на нашем рынке модель *freemium* малопригодна, работая по ней, можно лишь рассчитывать продать часть бизнеса (или весь бизнес) инвестиционным фондам, которые, вкладываясь в разные бизнесы, ожидают, что часть бизнесов прогорит, часть будет существовать, а один станет *Skype'ом*, принеся им тысячепроцентные доходы.

Наиболее реальный выход на наш рынок — через поглощение действующей компании. Именно по этому пути пошла *Intel*, поглотив 19 августа 2010 года *McAfee*, входящую в пятерку крупнейших производителей антивирусного ПО.

M&A-процессы — частое явление на мировом рынке антивирусного ПО?

— За последние два года на рынке было много поглощений[14]. Здесь можно наблюдать два варианта. Первый — выход через поглощения на наш рынок *IT*-компаний из смежных отраслей, сближающихся с нашей, например, уже упоминавшаяся покупка *Intel*'ом *McAfee*. Второй — поглощение компаниями первого эшелона компаний второго эшелона. Так посутпают *Symantec*, *Trend Micro* и *Sophos*. Для компаний второго эшелона такая интеграция является хорошей стратегией, поскольку они имеют мало шансов дорасти до первого эшелона самостоятельно.

Обычно поглощения происходят в случаях, когда есть ожидание, что рынок либо

[14] К недавним крупным сделкам можно отнести покупку компанией *Symantec* в апреле 2010 года компании *PGP* за 300 млн долл. и *GardiannEdge* за 70 млн долл.

будет очень быстро расти, либо находится на спаде, и компании разоряются. Применительно к антивирусной отрасли явно первый случай, т. е. рынок растет, и вместе с ним растут компании, но не все. «Лаборатория Касперского» растет. Доходы компании увеличились на 38% в прошлом году. Сейчас наблюдается некоторое замедление роста, что связано с размером бизнеса — чем больше бизнес, тем труднее поддерживать высокие темпы роста. Многие компании первого эшелона были прибыльны в прошлом году, и сейчас у них есть средства на поглощения.

Технологическая гонка, набирающая обороты на рынке защитных решений, активизирует поглощения узконишевых специализированных технологических компаний. Это эффективный способ достижения лидерства в технологиях, сокращения времени внедрения новой технологии. Возможно, когда всех «съедят» и возможности развития за счет расширения технологий будут исчерпаны, конкуренция изменится и рынок перейдет к прямой конфронтации на уровне розницы или реселлеров. Тогда конкуренцию можно будет действительно сравнить с военными действиями.

Кризис сильно повлиял на рост вашей компании?

— Кризис не очень сильно повлиял на мировой рынок антивирусного ПО. Сегмент защиты информации один из немногих, который не только не упал, но даже немного вырос. В России кризис оказал влияние на нашу отчетность, из-за значительного падения курса рубля объем рынка не снизился, но в долларовом выражении все-таки сократился. Это коснулось не только России, но и некоторых других стран. Например в Польше были схожие проблемы, только в меньших масштабах.

Планирует ли «Лаборатория Касперского» участвовать в M&A-процессах?

— Пока точно могу сказать одно: мы хотим участвовать в росте рынка. Для публичной компании M&A может быть самоцелью, поскольку это, с одной стороны, способ повышения акционерной стоимости компании, с другой — способ демонстрации бурной деятельности топ-менеджмента. Но в обоих случаях это весьма дорогостояще. Однако мы частная компания и не видим сейчас смысла в M&A. Возможность получить доступ к новым знаниям и технологиям при совершении M&A на нашем рынке представляется наиболее интересной, но мы имеем достаточно развитую собственную инженерную структуру, у нас много хороших разработчиков, и мы умеем делать свое дело хорошо. При покупке компании трудно удержать ее клиентов, что особенно характерно для горизонтальных поглощений. M&A имеет смысл, когда компании исчерпали возможности органического роста. Но ни мы, ни другие компании нашей отрасли, с которыми нам было бы интересно консолидироваться, такие возможности не исчерпали и надеются хорошо вырасти за счет своих ресурсов. Мы не находимся в активном M&A-поведении, и я думаю, что ситуация будет сохраняться, пока рынок растет.

Каким методам конкуренции «Лаборатория Касперского» отдает предпочтение?

— Мы стараемся избегать ценовой конкуренции, как любая компания, стремящаяся к лидерству. Во-первых, на растущем рынке ценовая конкуренция бессмысленна, во-вторых, она может привести к вымиранию экосистемы.

В целом рынок не находится в состоянии жесткого демпинга, а ценообразование зависит от конкретной страны и сегмента рынка. Где-то достаточно интенсивно идет ценовая конкуренция, где-то цены не очень эластичны. На большинстве рынков «Лаборатория Касперского» не является самой дорогой компанией, в то же время мы и не дискаунтеры. Есть рынки, на которых мы позиционируем себя как премиум-игроки, — конкурентные преимущества, о которых известно нашим конечным пользователям, позво-

ляют нам предлагать более высокую цену. Мы считаем, что наши технологии лучшие, и клиенты, немного доплачивая, получают более высокий уровень сервиса и защиты.

Цена для нас не является ключевым фактором успеха (КФУ), более того, мы не уверены, что она может быть таким фактором на технологическом рынке, особенно с постоянно изменяющейся средой. Если вы делаете электромоторы, то в конечном итоге научитесь делать их настолько дешево, насколько это технологически возможно. Для этого нужно найти самых дешевых рабочих, самое дешевое оборудование, самые дешевые материалы, затем добиться максимального качества. В нашем бизнесе это невозможно из-за постоянно меняющейся среды, находясь в которой нецелесообразно делать самый дешевый движок[15], поскольку компьютерная отрасль очень динамично развивается, меняются требования к компьютерным сетям, технологии быстро устаревают, и скоро придется делать его снова.

На нашем рынке практически отсутствует конкуренция за счет снижения издержек, нет товаров-субститутов, но есть системы-субституты, например, *Apple* утверждает, что для ее операционных систем не нужны антивирусы, поскольку система сконструирована так, что заражение ее вирусом практически невозможно. Однако на самом деле такая опасность все-таки существует, более того, есть риск возникновения небольшого апокалипсиса. Операционная система *Apple* неплохая, но не менее уязвимая, чем остальные. Разработчики, конечно, много сделали для того, чтобы было сложно запустить вредоносный код, но не невозможно, и система все равно поддается взлому, тем более соблазн ее взломать постоянно возрастает с течением времени и ростом числа пользователей.

Какие рынки являются смежными по отношению к вашему рынку, и представляет ли для вас интерес диверсификация в эти рынки?

— На сегодня никаких решений о выходе нашей компании на новые продуктовые рынки не принято. Смежными по отношению к рынку *IT*-безопасности являются рынок системного менеджмента, *B2B*-рынок, который связан с управлением *IT*-системой предприятия. Хороший пример многопрофильной компании — компания *Symantec*, которая начинала с компьютерной безопасности. Пойдем ли мы этим или другим путем или решим специализироваться — вопрос будущего.

Александр, каковы, на Ваш взгляд, основные тенденции развития рынка?

— Я вижу несколько ключевых тенденций. Первая — облачные вычисления, т. е. такая технология распределенной обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как интернет-сервис, программный код исполняется не на компьютере, на котором работает пользователь. Вторая тенденция — мобильность, когда многие пользователи начинают получать доступ в интернет через мобильные устройства. Третья тенденция — защита данных. Мы стремимся соответствовать данным тенденциям, разрабатывая решения для виртуальных сред, уделяя значительное внимание мобильной защите, предлагая разные решения в области защиты информации.

Какие стратегические риски, влияющие на состояние отрасли, могут реализоваться в ближайшие год–два?

— На мой взгляд, правильнее говорить не о стратегических рисках, а о группах угроз. Можно выделить три такие группы. Первая — это новые операционные системы *Mac OS*, *Android*, *Chrome*, для которых пока нет

[15] Движок — выделенная часть программного кода для реализации конкретной прикладной задачи. Как правило, прикладная часть выделяется из программы для использования в нескольких проектах, использование готового движка при разработке программы сокращает время разработки, позволяет уделить больше времени разработке других подсистем, например пользовательскому интерфейсу.

наработанной практики защиты — не до конца понятно, как именно и от чего защищаться. Лавинообразный рост данных операционных систем может привести к различным негативным последствиям от маленьких *IT*-апокалипсисов до серьезных эпидемий, аналогичных тем, что были в начале 2000-х годов. Это может повлиять на состояние отрасли позитивно, как бы цинично это ни звучало, хотя сейчас сложно предугадать истинные последствия этой эпидемии. Мы видим угрозу и стараемся не допустить ее реализации.

Вторая группа угроз связана с отношением государств к киберпространству — во многих странах сейчас создаются и активно развиваются различные киберкомандования. Так, в США прошлой осенью был создан *Cyber Command* — четвертое командование. Это не отдельная служба, она объединяет все киберструктуры американской армии, где служат десятки тысяч солдат и офицеров. Американцы объявили киберпространство четвертым театром боевых действий наряду с воздухом, водой и землей. Данный риск заключается в том, что на пространстве, где ранее были правоохранительные органы, компании, занимающиеся безопасностью, отдельные злоумышленники и их крупные группы, может появиться четвертый игрок — государство. Если в киберпространстве начнется война между странами, в отличие от конфликтов на земле, в воде и в воздухе, она будет носить глобальный характер. Отстраненно смотреть репортажи с мест боевых действий по телевизору, сидя в удобном кресле, не получится.

Третья группа угроз связана с тем, что законодательство и правоохранительные практики не успевают за развитием киберпреступности. Правда, нужно отметить, что некоторые успехи в борьбе с преступлениями в Сети. Так, в последние месяцы отмечается сокращение спама, что связано с активизацией борьбы правоохранительных органов с крупными спамерами и налаживанием трансграничного сотрудничества. В легенде у знаменитого американского мошенника эпохи гангстеров Уилли Саттона спросили, почему он грабил банки, он ответил: «Потому что там лежат деньги». Современные преступники знают, что сейчас деньги лежат не в банках, а в компьютерных сетях.

Сегодняшние киберпреступники зарабатывают на серых раскрутках, черной оптимизации поиска, контекстных ссылках, порнотрафике, краже денег. Теперь представьте, что произойдет, если в этой сфере появится криминальный венчурный капитал.

Таким образом, происходит обновление криминального мира в условиях отстающего законодательства. Сейчас киберпространство напоминает ситуацию с водным пространством XVIII века, когда в отсутствие морского законодательства все друг друга грабили. Даже «приличные» страны выдавали бандитам лицензии на грабеж кораблей других стран (каперский патент), причем это происходило не только во время войны. Практика пиратства прекратилась только к концу XVIII века, когда была сформирована достаточная правовая база. Однако стоит подчеркнуть, что в отличие от морей киберпространство общее.

Интервью провел
Денис Матвиенко