Не было бы счастья, да несчастье помогло

У отечественных разработчиков хорошие перспективы благодаря тренду на импортозамещение

На вопросы «БИТа» отвечают эксперты ведущих ИТ-компаний

1. **В каком направлении в 2015 году будут развиваться технологические разработки в сфере информационной безопасности?**
2. **Технологии BYOD и облачные вычисления, получающие все более широкое распространение, выдвигают новые требования к информационной безопасности. Каковы пути их реализации?**
3. **Каковы возможности и перспективы отечественных платформ и систем?**
4. **Действительно ли заканчивается век антивирусов? Да/нет и почему?**

Рустэм Хайретдинов, CEO компании Appercut Security

1 В первую очередь в кризисное время инвестиции направляются на защиту ключевой информации, составляющей основу конкурентоспособности компании – интеллектуальной собственности, коммерческих секретов, клиентских баз. В защите будут нуждаться бизнес-системы, генерирующие прибыль (CRM-системы, интернет-магазины) или сокращающие издержки (ERP-системы, интернет-банк и др.). Производители откликаются на изменение спроса технологиями защиты приложений, системами противодействия целенаправленным атакам (APT) и атакам на веб-ресурсы. Наибольшим спросом будут пользоваться системы, обеспечивающие доступность информации и ИТ-ресурсов (например, решения защиты от DDoS-атак) и автоматизированные интегрированные системы защиты, сводящие к минимуму человеческий фактор.

2 Концепция BYOD постепенно замещается на PYOD/CYOD (Pick/Choose You Own Device) – компании предлагают сотрудникам выбор из узкого ассортимента мобильных устройств, обычно одно-два устройства на системах Android или Windows. Невозможность поддерживать любые личные мобильные устройства сотрудников сегодня стала очевидной, а навесные MDM-системы не могут решить проблему безопасности на системном уровне. В облаках основным трендом будет миграция пользователей из-за нового российского законодательства в российские облачные сервисы и российские дата-центры зарубежных компаний.

3 Импортозамещение не по «зову сердца», а из-за курса рубля набирает обороты – многие компании сейчас просто не могут себе позволить купить западные решения. Их взоры обращаются на российские решения, при этом они уже готовы снижать требования к функционалу. Российские производители, которые поймают эту волну, смогут существенно переделить рынок, получить от клиентов не только средства, но и пользовательский опыт, что позволит им развиваться опережающими темпами, приближая качество продуктов к общемировым стандартам.

4 От антивирусных решений сейчас и вообще нельзя отказаться, как, например, нельзя отказаться от ремней безопасности в автомобиле. Как и ремни, антивирусы сегодня не являются всеобъемлющим решением в области безопасности, они просто ушли на второй план, не имея возможности защитить от всех угроз. Принципиально другие решения (в автомобиле – подушки безопасности, датчики сближения, АБС и т.п.) позволяют решить проблемы безопасности на дальних подступах, оставляя базовую безопасность, которой являются ремни и антивирусы, на крайний случай.

Александр Санин, коммерческий директор компании «Аванпост»

1 Из основных трендов развития и роста в ИБ на 2015 год можно выделить несколько направлений: курс на импортозамещение, ИБ «Интернета вещей», безопасность мобильного доступа и BYOD.

Поэтому, если говорить о развитии современных технологических разработок в России, в первую очередь необходимо смотреть на тренд импортозамещения. Я считаю, что все отечественные разработчики программного обеспечения в области ИБ, имеющие на текущий момент продукт, способный конкурировать с западными аналогами, получат серьезный толчок для роста. Да и наверняка мы увидим появление совершенно новых продуктов, ранее на рынке не присутствовавших.

2 Рано говорить, что тренд BYOD стал уже действительно массовым в России. Сегодня схема работы программного обеспечения для безопасности мобильного доступа фактически разделена на два типа. К первому относится ПО, которое обеспечивает на мобильном устройстве некое доверенное пространство, за пределы которого информация не может быть передана. Ко второму типу относится такое ПО, которое встраивается на более низком уровне и позволяет практически полностью контролировать мобильное устройство пользователей. Это программное обеспечение пока вполне справляется с поставленными задачами.

3 Тут все мы должны понимать одну простую вещь – перспективы есть. Важно лишь отдавать себе отчет, что невозможно за год с нуля написать свою операционную систему уровня Windows 8 или даже 7. И неважно, сколько у вас на это будет денег и ресурсов разработчиков. Подобное системное программное обеспечение создается и тестируется годами.

Ну а касательно программного обеспечения в области ИБ: у отечественных разработчиков есть хорошие перспективы пережить кризисные времена и увеличить свое присутствие на рынке благодаря тренду на импортозамещение. Конечно, я говорю лишь о тех компаниях, которые реально обладают конкурентоспособным продуктом.

4 Я не считаю, что век антивирусов заканчивается. Антивирусы стали практически неотъемлемой частью любого компьютера, активно развиваются на рынке мобильных устройств. Тут можно говорить о том, что заканчивается век классических схем продажи и распространения антивирусов. Тут семимильными шагами набирает рост распространение через предустановленные версии. Кроме того, мы видим увеличение активности интернет-провайдеров, встраивающих услуги антивируса в свои тарифы и подписки.

Сергей Вахонин, директор по решениям ЗАО «Смарт Лайн Инк»

2 Главная проблема ИБ, связанная с распространением модели BYOD, заключается в том, что модель информационной безопасности в этой сфере основывается на том, что фактическую ответственность за безопасность данных, попавших на личные устройства, несет сам пользователь. В случае с «корпоративными облаками» невозможен физический контроль доступа к эксплуатируемым ИТ-компонентам и данным, размещенным в арендуемых хранилищах. Здесь же стоит упомянуть еще и о «персональных» облачных файлообменных сервисах, когда все решения о способах и уровне авторизации, аутентификации и доступа к данным, размещенным в облачном хранилище, принимает пользователь, который при этом далеко не всегда является владельцем данных, будучи сотрудником какой-либо организации.

Для повышения уровня защиты данных, размещаемых на мобильных устройствах, рынок чаще всего предлагает решения класса MDM, однако они, будучи безусловно полезными и необходимыми, не являются надежным и гарантированным способом противодействия утечкам с персональных устройств. Альтернативным решением по защите данных в концепции BYOD является предоставление доступа к информационным активам компании через удаленное подключение. В этом случае BYOD-устройство использует корпоративные данные без локального хранения их на устройстве, строго в рамках терминальных сессий с подключением к размещенным в офисе или в облаке серверам компании, которые, в свою очередь, защищены DLP-системой, функционирующей на удаленном сервере или в виртуальных Windows-средах, доступных в терминальной среде. Такой подход называется Virtual Data Leak Prevention (Virtual DLP) и реализован в DLP-комплексе DeviceLock DLP Suite. Совместное использование Virtual DLP и MDM-решений позволяет создавать действительно безопасную BYOD-модель в корпоративной среде.

DLP-система может быть использована также для проактивного предотвращения утечек за счет применения технологий Discovery, когда производится автоматическое сканирование данных, размещенных на рабочих станциях внутри и вне корпоративной сети, внутренних сетевых ресурсах и внешних системах хранения данных.

Игорь Корчагин, руководитель группы обеспечения безопасности информации, компания ИВК

1 Развитие технологий информационной безопасности в 2015 году скорее всего будет направлено на те же ИТ-тренды, которые набирали популярность в предыдущие годы, в особенности:

- обеспечение безопасности среды виртуализации и облачных вычислений;
- обеспечение безопасности мобильных технологий (в том числе и ИБ BYOD);
- системы управления событиями и информацией о безопасности (SIEM);
- системы управления контролем идентичности и прав доступа (IAM).

Данные направления развития в сложившихся условиях стремления к расширению импортозамещения особенно актуальны для рынка отечественных ИБ-решений, которые только начинают осваивать данные технологии. Стоит отметить, что в 2015 году также вероятен повышенный интерес к теме обеспечения безопасности АСУ ТП.

2 Внедрение в своей ИТ-инфраструктуре технологии BYOD или облачных вычислений всегда должно в первую очередь сопровождаться проработкой стратегии их внедрения и применения на всем жизненном цикле как в части вопросов общей автоматизации, так и в части вопросов информационной безопасности, например, какие ресурсы будут обрабатываться с применением новых технологий, как и кто будет иметь к ним доступ, как изменится модель угроз безопасности информации, риски применения новых технологий, какие платформы и решения будут выбраны, необходимо ли соответствие выбранных решений требованиям законодательства и т.д.

3 В последнее время заметно стал расширяться рынок отечественных ИБ-решений, представляющих собой реализацию не только классических методов защиты, вроде наложенных средств защиты от НСД или межсетевых экранов, но и новые перспективные направления, в том числе защищенные операционные системы. Но зачастую многие новые разработки являются переработкой Open-Source-решений, что, с точки зрения ИБ, обязательно должно предполагать тщательное изучение разработчиком заимствуемого кода.

4 Век антивирусов как узкоспециализированных решений конкретных задач защиты от вредоносного ПО, можно считать, заканчивается. На смену им приходят целые программные комплексы, объединенные в рамках одного продукта, которые, помимо защиты от вредоносного программного обеспечения, предоставляют целый набор дополнительных функций защиты вычислительных устройств, таких как персональный межсетевой экран, родительский контроль, контроль использования различных устройств, поиск уязвимостей и другие.

Вячеслав Медведев, ведущий аналитик отдела развития компании «Доктор Веб»

1 В 20015 году не предвидится резких технологических прорывов. Будут улучшаться существующие технологии. Практика показывает, что функционал существующих продуктов избыточен и зачастую даже сложен для многих пользователей.

И хотя следующий прогноз повторяется из года в год, но все же: в итоге преимущество получат продукты, сочетающие качество работы и понятность интерфейсов.

2 Я бы не сказал, что эти требования новы. Чем с точки зрения безопасности облачные системы отличаются от систем эпохи мейнфреймов? Удаленные серверные и пользователи по всему миру. Да, технологии изменились, но проблемы и подходы к их решению остаются прежними.

Новые требования выдвигают не сами по себе облачные технологии, а переход от хранения данных в пределах одной сети к их доступности из любой точки Интернета, расширение списка людей, имеющих доступ к данным компании (при том, что большая часть этих людей проверки служб безопасности компании не проходила), большая простота доступа к этим данным, возможность перехвата трафика компании и т.д.

Техническая часть проблем решаема – шифрование трафика, установка дополнительных решений безопасности, в том числе антивирусных шлюзов. Но вот проблема доступности данных для сотрудников подрядчиков, проблемы ответственности за простои и потери на сегодняшний день не имеют однозначного решения.

3 К сожалению, весьма печальные, за исключением нескольких весьма узких секторов (антивирусов и систем шифрования в первую очередь). Отсутствие широкого спроса не позволяет построить политику долгосрочного инвестирования. Более того, формальное выполнение требования об импортозамещении вызывает к жизни (за редчайшим исключением) не проекты по созданию новых систем, а замену продуктов на якобы отечественные.

4. Про «смерть» антивирусов я слышу уже, наверно, лет 15. Есть задачи, которые никто, кроме антивирусов, выполнить не может. Более того, надвигающийся мир вещей – это вызов, причем вызов, который мы приняли.

Александр Лямин, руководитель Qrator Labs

1 В сфере информационной безопасности имеется целый ряд перспективных и прорывных направлений исследования и разработки, однако их бессмысленно обсуждать с практической точки зрения, потому что потребитель этих разработок – бизнес – достаточно инертен и не стремится внедрять даже то, что было разработано еще пять–десять лет назад. Традиционным двигателем практических разработок в сфере ИБ станет деятельность специалистов, занимающихся поиском уязвимостей. 2014 год в сфере информационной безопасности прошел под знаком SSL: начало положил Heartbleed, потом в криптографических протоколах был обнаружен еще целый ряд уязвимостей. Уязвимости, которые будут обнаружены в новом году, зададут направление новых разработок.

В области защиты от DDoS-атак необходимо развитие более серьезных аналитических методов. Мы будем наблюдать дальнейшее эволюционное развитие поведенческого анализа запросов, который позволит более эффективно отличать ботов от реальных людей.

2 Во-первых, как и при прежней идеологии корпоративной IT-архитектуры, требуется тщательный подбор вендоров. Наличие облачной инфраструктуры упрощает работу компании, избавляет от необходимости держать штат администраторов, содержать парк оборудования, своевременно делать апгрейд. Но одно требование сохраняется: IT-инфраструктуру должны проектировать люди, которые знают, как это делается. Компании, которые предоставляют облачные сервисы, в основном устойчивы, но ключевое слово – «в основном». Всегда необходима система резервирования, которая позволит бизнесу оставаться на плаву, если проблемы облачного провайдера продлятся больше суток. Есть целый ряд факторов, которые могут повлиять на стабильность работы облачного сервиса. Это и сетевые проблемы, возникающие в сети Интернет стихийно из-за неправильно работающего транзитного оборудования. Это также и целенаправленные действия заинтересованных лиц. Облака в отличие от традиционных сервисов имеют распределенную топологию, что в целом повышает их устойчивость, однако при ошибках в проектировании этой топологии злоумышленник может вывести облачный сервис из строя. Существует заблуждение, что облако само по себе противодействует атакам. Это не совсем так. Облако обычно располагает мощными вычислительными ресурсами, но эти ресурсы стоят денег. Облачный вендор не будет отличать легитимную нагрузку от нелегитимной, а просто выставит счет. При серьезных атаках на облако работа с клиентом становится для облачного провайдера невыгодной, и тогда провайдер может просто отключить своего клиента. Поэтому, если в облаке размещаются публично доступные сервисы (сайты для работы с внешними заказчиками и пр.), то никто не снимает задачу их защиты от атак извне.

3 У целого ряда российских компаний есть наработки и продукты, позволяющие быть конкурентоспособными на мировом ИТ-рынке. Однако тут возникает целый ряд вопросов, смогут ли все эти компании не только выжить, но и активно развиваться в 2015 году. Мы надеемся, что российские ИТ-компании накопили достаточный запас прочности, чтобы пережить этот год.

4 Разговоры об этом ведутся последние лет десять. Они большей частью основываются на том, что растет число облачных сервисов, мобильных платформ, а продажи ПК падают. Однако мировой парк ПК все еще огромен, и, наблюдая стабильный рост размеров ботнетов, то есть рост числа зараженных компьютеров по всему миру, мы можем сделать вывод, что антивирусная тематика ни в коем случае не теряет актуальности.

Есть и другой важный момент. Теоретически проблема вирусов должна сойти на нет по мере развития мобильных ОС, допускающих установку только проверенного программного обеспечения из доверенных источников (App Store, Play Market и пр.). Но на практике мы видим достаточно пренебрежительное отношение со стороны производителей мобильных устройств к таким важным вещам, как обновление прошивок и встроенного ПО. Особенно это актуально для платформы Android. Производители не обновляют прошивки, поскольку тратят все силы на разработку новых моделей. В старых прошивках со временем обнаруживаются уязвимости, которые приводят к заражению устройств, и мы уже неоднократно наблюдали DDoS-атаки с зараженных телефонов и планшетов. Так что век антивирусов все никак не заканчивается. Однако все это не снимает проблему низкой результативности антивирусов. Согласно исследованию наших коллег из компании Group-IB, антивирусы справляются только с 40% угроз.

> Существует заблуждение, что облако само по себе противодействует атакам. Это не совсем так

Максим Захаренко, генеральный директор компании «Облакотека»

1, 2 Информационная безопасность следует за ИТ-технологиями, а те, в свою очередь, демонстрируют тенденцию «Сервер – в облако», «Клиент – на мобильное устройство», что продолжает размывать контур безопасности организации. Соответственно развитие средств безопасности будет идти в трех направлениях: защита клиента (MDM-технологии, endpoint защита устройства и т.д); в облачных средах будут развиваться средства защиты «от провайдера» при размещении ИТ-ресурсов на виртуализированных облачных платформах, а также удобная управляемая изоляция ИТ-ресурсов разных клиентов друг от друга; будут развиваться сервисы класса SecaaS, позволяющие не разворачивать средства безопасности у себя, а брать защиту в виде сервиса из облака; и, конечно, будут развиваться средства защиты канала между мобильным устройством и облаком, в том числе различные решения IDS/IPS, борьба с DDoS и т.д.

3 Сноуден показал нам, чего на самом деле стоят «сертифицированные средства защиты». Единственный способ гарантировать отсутствие НДВ («закладок») – это контролировать весь цикл производства целиком: и железо, и ПО, и процедуры обновлений… В текущих политических условиях отечественные производители средств защиты имеют очень неплохие перспективы на внутреннем рынке (прежде всего госсектор и госкорпорации), но внешний рынок по тем же причинам будет закрыт для наших разработок, так что эффективные шедевры мирового уровня мы вряд ли произведем.

4 Мобильное устройство – достаточно «толстый» клиент, на котором могут заводиться «вредоносы». Если бы наблюдалась общая тенденция «облегчения» клиента (переход в терминальный режим, Chromebook), тогда можно было говорить о конце века антивирусов, но этого не происходит.

Михаил Башлыков, руководитель направления Информационной безопасности компании КРОК

1 В кризисное время спрос на решения по информационной безопасности возрастает, как и активность злоумышленников. Актуальные решения в сфере ИБ будут соотноситься с трендами этого года. Это в первую очередь облачные вычисления и виртуализация, бизнес-аналитика, мобильные устройства для удаленной и совместной работы и пр.

В связи с этим особое внимание будет уделяться защите виртуализированных и облачных сред, противодействию мошенничеству или так называемым antifraud-системам, защите от утечек конфиденциальной информации (DLP-системы), средствам контроля кода и анализа защищенности приложений и пр.

Но нужно иметь в виду, что вопросы экономии и оптимизации, как бизнес-процессов, так и бюджетов, будут идти отдельным лейтмотивом в развитии ИТ-рынка в целом. Все технологии, в том числе и в области информационной безопасности, будут проходить через призму текущей экономической ситуации и сокращения затрат. И поэтому вполне возможно, что на первый план выйдет оптимизация того, что есть, а не внедрение совершенно новых технологий.

2 Действительно, концепция BYOD становится все более популярной год за годом, а вместе с этим растет и необходимость обеспечить безопасный доступ к данным на личных устройствах пользователей. В первую очередь важно управлять мобильными устройствами, и, самое главное, той частью, где находятся корпоративные данные. Корпоративное мобильное приложение должно не только стабильно работать на любом типе мобильных устройств и быть удобным для пользователя, но и обеспечивать конфиденциальность данных, которые в нем содержатся либо пере-даются между устройством и офисом.

Что касается облачных вычислений, то нужно, во-первых, учитывать необходимость использования сертифицированных средств защиты при размещении в облаке персональных данных. Во-вторых, важно учитывать особенности виртуальной среды и тех сервисов, которые обеспечивает облачный провайдер, и максимально интегрировать их между собой таким образом, чтобы снизить риск утечки информации и обеспечить комплексную защиту, доступность и целостность размещаемых в облаке данных и ресурсов.

3 В России разрабатывается ряд базовых инструментов информационной безопасности – антивирусы, межсетевые экраны, DLP-системы, средства защиты от несанкционированного доступа, анализа защищенности приложений и другие. При этом у большинства из них есть сертификация на соответствие требованиям регуляторов, в частности, ФСТЭК и ФСБ. Однако потребности российского рынка на данный момент они закрывают примерно на 40%. В целом современная политическая обстановка может подстегнуть рынок, а необходимые квалифицированные кадры для этого у нас есть.

Дмитрий Титков, ведущий менеджер по работе с финансовым сектором Check Point Software Technologies

1 Как и в прошлом году, в 2015 году число угроз в сфере ИБ будет только расти. Естественно, в первую очередь целями киберпреступников являются большие компании, атака на которые может принести им внушительную прибыль и возможность завладеть информацией на миллионы долларов. Средний и малый бизнес часто используется хакерами как ступень на пути к крупным организациям – проникновения в их сеть осуществляются не напрямую путем взлома их систем, а через более мелкие компании-подрядчики.

Сегодня хакеры не используют какой-то один тип атак – они применяют комплексные каскадные атаки, то есть целый набор технологий и методов взлома. Для защиты от них требуется такая же многоуровневая система. Этого можно достичь за счет использования всей линейки средств, обеспечивающих защиту информации: антивирусов, межсетевых экранов, антибот-решений, средств криптографической защиты, DLP-систем, DDoS-протекторов и многих других. Поэтому в основе новейших систем безопасности лежит комплексный подход, объединяющий решения разных типов и даже от разных производителей.

Если ранее мы часто говорили о таком виде атак, как атаки «нулевого дня», то сегодня мы уже говорим о вредоносном ПО «нулевой секунды». Глобальная сеть сенсоров безопасности Check Point показала, что около трети компаний за 2013 год загрузили хотя бы один файл, зараженный неизвестным вредоносным ПО. Атаки «нулевой секунды» опасны тем, что они используют неизвестные вредоносные программы, и для защиты от них необходимо применять специально разработанные для конкретного случая средства предотвращения угроз. Поэтому по-прежнему будет востребована технология эмуляции угроз Threat Emulation.

С развитием облаков и облачных сервисов для обеспечения информационной безопасности компаний все больше будут использоваться различные решения класса «ПО как услуга» (SaaS). Поэтому в наступившем году можно ожидать повышения спроса на решения безопасности как сервиса (Security-as-a-Service). Это мультифункциональные решения, которые могут обеспечить защиту от многих угроз. Одновременно с этим будет расти спрос на аутсорсинг сервисов безопасности в публичных облаках.

Еще одна тенденция, которая продолжит свое развитие в 2015 году, связана с безопасностью использования мобильных устройств для работы. Согласно исследованию Check Point, проведенному в 2014 году среди 700 компаний по всему миру, 42% респондентов столкнулись с инцидентами мобильной безопасности стоимостью более $250 000. Более 80% участников подтвердили, что ожидают ухудшения ситуации в 2015 году.

2 Концепция BYOD подразумевает использование личных устройств сотрудников в рабочих целях, поэтому введение строгих правил и ограничений работы с мобильными девайсами не представляется возможным. Выходом в данной ситуации являются четкое разделение личных и корпоративных данных на устройстве и их защита. Сейчас наиболее эффективный подход, который использует, в том числе и Check Point, – это выделение внутри устройства изолированного контейнера для работы с корпоративными данными. Для доступа к контейнеру или капсуле необходимо ввести дополнительный пин-код, и через VPN-туннель пользователь получит возможность работать с почтой, календарем, адресной книгой, интранетом и приложениями.

Тем не менее не стоит забывать и о безопасности личной части устройства. Для этого рекомендуется использовать сервисы фильтрации интернет-трафика, не оставлять само устройство, пароли и коды от него в доступных для незнакомых людей местах, не подключаться к подозрительным публичным сетям и устройствам и т.д. Для достижения максимального уровня безопасности можно дополнить решение защитой на уровне документов. В этом случае даже если документ попадет в чужие руки, его содержимое останется в тайне. Аналогичный механизм можно применять и для работы с облачными хранилищами.

> // Действительно, век традиционных антивирусов уже подошел к концу

4 Действительно, век традиционных антивирусов уже подошел к концу. Как мы уже говорили выше, атаки стали намного более изощренными и, что важно, направленными. Вредоносное ПО в большинстве своем уже не пишется для использования на массовом сегменте. Сейчас над созданием вирусов работают целые команды разработчиков (как уже известно, иногда даже подобные разработки финансируются государствами), предшествует этому также огромная работа по поведенческому анализу персонала (для внедрения вируса внутрь периметра), а также анализ функционирующих в организации систем и их уязвимостей.