ИБ виртуализированных ИКТ-сред: современное состояние

ВАЛЕРИЙ ВАСИЛЬЕВ

Несмотря на то что среди корпоративных ИКТ-ресурсов остаются такие, которые пользователи не виртуализируют по соображениям их критической важности или из-за принципиальной технической невозможности применения к ним этой технологии, роль виртуализации становится все более значимой и даже необходимой по мере распространения сервисной модели потребления ИКТ, поскольку без использования ее возможностей провайдерам ИКТ-услуг технически сложно и финансово накладно обеспечивать клиентам требуемые надежность и оперативность услуг и одновременно обеспечивать эффективность своего бизнеса.

ОБЗОРЫ

В нашем тематическом обзоре мы рассмотрим нынешнее положение дел с организацией защиты виртуализированной ИКТ-инфраструктуры, оценим наиболее актуальные из возникающих при этом проблем и возможные пути их решения, обсудим изменения, происходящие в области регулирования обеспечения информационной безопасности виртуализированных ИКТ-сред.

Направленность развития методов и инструментов защиты

Руководитель направления инфраструктурных ИБ-решений Центра информационной безопасности компании "Инфосистемы Джет" Юрий Черкас выделяет три технологических вектора, по которым развивается защита виртуализированных сред сегодня.

Первый — защита доступа к платформе виртуализации. Он, как правило, по его мнению, строится на привычных средствах сетевой защиты.

Второй — контроль доступа, прежде всего административного, к виртуализированной инфраструктуре. В привычной физической среде за сетевые коммутаторы отвечает один администратор, за операционную систему — другой, за базы данных — третий и т. д., и для нее в принципе многие ИБ-задачи могут решаться организационными методами. У администратора же виртуальной инфраструктуры полномочия гораздо шире, и потому контроль его доступа к ресурсам стоит особенно остро.

Третий — защита виртуализированных ИКТ-сервисов, для чего используются специально созданные под виртуализированные среды ИБ-технологии (антивирусные, технологии IDS/IPS, точек на дюйм и т. п.), поскольку использование традиционных средств защиты здесь чаще всего неэффективно.

Постепенно набирающая силу парадигма виртуализации ИКТ-среды через программное конфигурирование ИКТ-ресурсов (технологии SDN, SDS, SDDC), которая нацелена на поддержку сервисно-ориентированной модели предоставления ИКТ, как отмечает Юрий Черкас, стимулирует перевод на сервисную модель и механизмов обеспечения ИБ.

В целом, как считает директор по развитию продуктов компании "Код Безопасности" Константин Пичугов, ИБ виртуализации продолжает развиваться по тем же направлениям, которые обозначились сразу после того, как эта технология вышла на уровень массового использования, — антивирусная защита, сетевая безопасность, обеспечение целостности информации, специфические угрозы конфиденциальности данных... Эти направления обусловили появление широкого спектра ИБ-продуктов и решений: специализированных безагентных антивирусов для виртуальных машин (ВМ), средств резервного копирования и репликации ВМ, виртуальных межсетевых экранов и систем IDS/IPS, средств защиты от несанкционированного доступа...

Вместе с тем, по мнению ведущего инженера Центра комплексных услуг и проектов компании "ЭЛВИС-ПЛЮС" Павла Власова, ИБ-вендоры попали в зависимость от вендоров средств виртуализации. Развитие технологий и средств виртуализации находится сегодня в активной фазе: архитектура решений постоянно совершенствуется, появляются новые механизмы, упрощающие решения ИТ-задач... Это затрудняет производство универсальных ИБ-продуктов: ИБ-вендорам приходится учитывать изменения при переходе на новые версии ПО виртуализаторов, с которыми могут меняться интерфейсы на уровне ядра, что делает ранее реализованные ИБ-инструменты неэффективными.

Менеджер компании InfoWatch по развитию направления Mobile Security Management Андрей Арефьев в качестве первоочередных в сегодняшней практике обеспечения ИБ виртуальных сред рассматривает требования к хостинг-серверам, на которых работают ВМ, и к серверам, на которых хранятся их имиджи. Обеспечивая защиту всех ВМ именно на хостинг-серверах, специализированные решения для защиты ВМ, по его мнению, могут экономить системные ресурсы.

Актуальные задачи обеспечения ИБ виртуализации и связанные с ними бизнес-риски

Для бизнеса в первую очередь важно обеспечить непрерывность своей деятельности, что в нашем случае означает надежную работоспособность информационных систем. При этом бизнес не готов переплачивать за ИКТ- и ИБ-ресусы.

По оценкам Павла Власова, для небольших компаний сегодня проще и дешевле воспользоваться обслуживанием по модели IaaS, которое предоставляют облачные сервис-провайдеры: клиент арендует виртуализованную ИКТ-среду, оставляя за провайдером базовые сервисы по управлению ИКТ-инфраструктурой, а также обеспечение ИБ, оговаривая условия обслуживания в соглашении об оказании услуг (SLA). При этом, оценивая риски, клиент должен помнить, что SLA не дает гарантии по защите коммерческой тайны и не освобождает от ответственности по обеспечению безопасности информации, отнесенной законодательством нашей страны к сведениям, подлежащим защите, регламентируемой законом (к таковой, например, относятся персональные данные).

Клиент, как считает г-н Власов, должен быть уверен в том, что работает в доверенной среде: его виртуальная ИКТ-среда изолирована от сред других клиентов облака провайдера и защищена от несанкционированного доступа системных администраторов провайдера; в ней используются доверенные средства виртуализации; для хранимых в облаке данных обеспечивается установленный режим тайны. Решить эти задачи без тесного сотрудничества провайдеров с вендорами средств виртуализации, по его мнению, крайне трудно, поскольку доверенная среда требует применения средств доверенной загрузки и обеспечения целостности по цепочке от гипервизора до ВМ. Поэтому, заключает он, основная задача по обеспечению ИБ при использовании облачных технологий и технологий виртуализации заключается в формировании доверенной среды для функционирования информационных систем.

По мнению Константина Пичугова, наиболее актуальные задачи ИБ сегодня лежат именно на стыке технологий виртуализации и облачных сред — решений, в которых заказчик арендует часть ИКТ-инфраструктуры (или всю инфраструктуру) в облаке. Наибольшую озабоченность у заказчиков в этом варианте, как он отмечает, вызывает безопасность данных, размещенных на стороне провайдера.

Актуальной задачей также остается предоставление заказчику прозрачных и доверенных инструментов контроля состояния и управления ИБ. Ждет своего часа также проработка вопросов соответствия нормативным и законодательным требованиям распределения ответственности за обеспечение ИБ данных в облачной модели между всеми сторонами, участвующими в предоставлении и потреблении ИКТ-сервисов.

Бизнес-риски, подчеркивает руководитель отдела информационной безопасности системного интегратора IBS Platformix Джабраил Матиев, напрямую зависят от бизнес-процессов, завязанных на ИКТ-системы, размещенные в виртуализованной ИКТ-среде, ИБ-угрозы для которой ведут к нарушению непрерывности бизнес-процессов, а также конфиденциальности или целостности информации, циркулирующей в информационных системах.

Наиболее актуальными задачами в процессе обеспечения ИБ виртуализованных ИКТ-сред г-н Матиев считает сегодня следующие:

- обеспечение отказоустойчивости и приемлемых показателей восстановления виртуализованной ИКТ-среды;
- обеспечение контроля с целью недопущения несанкционированного доступа внутри виртуализованной ИКТ-среды;
- применение адаптированных для виртуальной среды решений для комплексной защиты конечных точек;
- реализацию сетевой защиты внутри виртуализованной ИКТ-среды.

Несмотря на различия в моделях угроз для виртуальной среды и среды физической, задачи ИБ, как полагает менеджер по продуктам "Лаборатории Касперского" Матвей Войтов, в обоих случаях практически не различаются именно из-за схожих бизнес-рисков — компрометации данных, нарушений работы сервисов вплоть до отказа работы ИКТ-инфраструктуры, затрат на восстановление... Специфику в организации ИБ, по его мнению, нужно рассматривать с позиции сценариев применения виртуализации. Так, при виртуализации рабочих станций возникает задача применения к ним корпоративных ИБ-политик (например, ограничения доступа к веб-ресурсам) к ВМ, и ИБ-решение должно решать в числе прочих и эту задачу.

Юрий Черкас разделяет мнение г-на Войтова, полагая, что характер ИБ-рисков при переходе в виртуализированные ИКТ-среды остался прежним: злоумышленники охотятся за теми же данными — паролями, логинами, записями в базах данных, используя при этом прежние методики. Изменились разве что некоторые технические аспекты ИБ-угроз — скажем, появились новые векторы атак, например на гипервизор.

В принципе же использование виртуализированных ИКТ как таковых, по мнению г-на Черкаса, позволяет существенно снизить бизнес-риски, поскольку виртуализация помогает сократить сроки запуска новых сервисов и обеспечить их высокую отказоустойчивость и доступность.

ИБ встроенная или наложенная?

У каждого из этих подходов, считают наши эксперты, есть как преимущества, так и недостатки, но применяться они должны только вместе.

Бесспорным преимуществом встроенной защиты для потребителя ИКТ, полагает Константин Пичугов, является отсутствие необходимости что-то дополнительно покупать и устанавливать, за исключением случаев, когда та или иная функция платформы виртуализации требует отдельного лицензирования.

Из преимуществ наложенных средств он прежде всего выделяет более полное обеспечение требований российских регуляторов, поскольку зарубежные средства виртуализации не учитывают специфику российской регулятивной базы. Наложенные средства отличаются более широкой функциональностью и гибкостью: если для разработчика платформы виртуализации антивирусная защита, резервное копирование или, например, усиленная аутентификация вторичны, то для производителей соответствующих средств защиты — это основной продукт, за качество которого они борются.

Отмечая положительную динамику ИБ, встроенной в ИКТ-продукты (в том числе со встраиванием в них движков зарекомендовавших себя наложенных ИБ-продуктов), Юрий Черкас в то же время напоминает, что разработчики этих продуктов ориентированы прежде всего на наиболее полную реализацию основного функционала. К примеру, ролевую модель доступа, функцию журналирования событий и некоторые других стандартные ИБ-функции можно считать стандартом для платформ виртуализации, однако патчи, защищающие, к примеру, от атак с использованием уязвимостей нулевого дня, вендоры платформ выпускают гораздо позднее, чем это делают разработчики виртуальных патчей (virtual patching), способных перехватывать вредоносные коды, использующие эти уязвимости. Для этого нужны отдельные компетен-

ПРОДОЛЖЕНИЕ НА С. 18 ▸

Наши эксперты

АНДРЕЙ АРЕФЬЕВ, *менеджер по развитию направления Mobile Security Management, InfoWatch*

ПАВЕЛ ВЛАСОВ, *ведущий инженер Центра комплексных услуг и проектов, "ЭЛВИС-ПЛЮС"*

МАТВЕЙ ВОЙТОВ, *менеджер по продуктам, "Лаборатория Касперского"*

ДЖАБРАИЛ МАТИЕВ, *руководитель отдела информационной безопасности, IBS Platformix*

КОНСТАНТИН ПИЧУГОВ, *директор по развитию продуктов, "Код Безопасности"*

ЮРИЙ ЧЕРКАС, *руководитель направления инфраструктурных ИБ-решений Центра информационной безопасности, "Инфосистемы Джет"*

Рынок виртуализации: новые возможности и новые риски

Технологии виртуализации приобретают всё бо́льшую популярность: крупные компании виртуализируют свои локальные серверы и строят частные "облака", малый и средний бизнес активно пользуется облачными сервисами и арендует ресурсы в ЦОДах. Применение технологий виртуализации приносит бизнесу массу преимуществ, но имеет и оборотную сторону — увеличение информационных рисков. Почему так происходит?

Зачастую компании осуществляют проекты по виртуализации серверов без привлечения специалистов по безопасности и соответственно без учета специфики технологий виртуализации. Виртуальная инфраструктура отличается от физической двумя элементами: гипервизором — прослойкой между аппаратной и программной частью, которая исполняет виртуальные машины, и средством управления — инструментом, позволяющим централизованно управлять гипервизорами. Важность этих элементов чрезвычайно высока, так как при компрометации гипервизора будут скомпрометированы исполняемые им виртуальные машины, а если скомпрометировано средство управления, то и вся инфраструктура находится под угрозой. В связи с этим наиболее типичные риски в проектах по виртуализации серверов связаны:

- с отсутствием инструментов контроля администраторов виртуальной инфраструктуры;
- с невозможностью применения традиционных средств для защиты виртуальной инфраструктуры;
- с консолидацией приложений и информации разных уровней значимости на одном физическом сервере без обеспечения их достаточной изоляции;
- с уязвимостями и недокументированными возможностями в платформе виртуализации.

Требования регуляторов к защите технологий виртуализации

Процесс формирования лучших практик по защите виртуализации и регулятивной базы начался несколько лет назад и продолжается до сих пор. Одним из первых свои рекомендации по защите технологий виртуализации издал Национальный институт стандартов и технологий США (NIST). Сейчас международная

Рис. 1. Компрометация виртуальных машин со стороны управления инфраструктурой

организация Cloud Security Alliance выпустила уже третью редакцию руководства по безопасности облачных сред. Отраслевые рекомендации для финансовых организаций и индустрии платежных карт разрабатывает PCI Council.

В нашей стране пионером по контролю безопасности виртуализации является ФСТЭК России, в 2013 году издавший приказы № 17 и № 21. В этих документах, в частности, дан перечень мер защиты, обязательных при использовании виртуальных сред в государственных информационных системах и информационных системах персональных данных. При этом особое внимание уделяется необходимости применения сертифицированных средств защиты виртуальной среды.

Помимо этого в скором времени может появиться государственный стандарт серии ГОСТ Р "Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Основные положения", который также готовится по инициативе ФСТЭК России.

Данные документы регуляторов помогают потребителям определить, какие действия необходимо предпринять для снижения информационных рисков и обеспечения безопасности применения технологий виртуализации.

vGate — сертифицированная защита для виртуализации

Разработанный компанией "Код Безопасности" продукт vGate — одно из наиболее популярных сертифицированных средств защиты информации для виртуальных платформ VMware vSphere и Microsoft Hyper-V. Продукт учитывает специфические особенности защиты информации в виртуальной среде и предоставляет службе безопасности предприятия инструменты контроля и противодействия злоупотреблениям при ее использовании.

Основное преимущество продукта vGate – возможность контроля всех действий по управлению виртуальной инфраструктурой и доступу к данным виртуальных машин. Одной из наиболее актуальных угроз для виртуальных инфраструктур является наличие суперпользователя, когда администраторы виртуальной инфраструктуры могут выполнять манипуляции с виртуальными машинами со своих рабочих мест и делать это бесконтрольно. Кроме того, виртуальную машину (в отличие от физической) можно скопировать, удалить или исказить, поэтому традиционные методы защиты (например, опечатывание корпуса, АПМДЗ, ограничения физического доступа и т. п.) для защиты виртуальной инфраструктуры не применимы.

vGate позволяет разграничить доступ администраторов к виртуальной инфраструктуре и контролировать их действия.

Администратор информационной безопасности имеет возможность ограничивать манипуляции с виртуальными машинами. Любые изменения в их конфигурации и расположении не вступят в силу без его подтверждения. Администратор также может сегментировать виртуальную инфраструктуру и самостоятельно решать, на каком хосте будут исполняться те или иные виртуальные машины. Это позволит снять проблему консолидации виртуальных машин разных уровней конфиденциальности в пределах одного и того же хоста.

Уязвимости самих платформ виртуализации, несомненно, исправляются их производителями, но не все используют последние версии платформ и тем более не все настраивают свою инфраструктуру в соответствии с рекомендациями производителя. Эти рекомендации, как правило, предоставляются вендорами в виде отдельного документа с инструкциями, которые нужно выполнить на хостах. vGate позволит автоматизировать этот процесс и выбрать для инфраструктуры наиболее безопасную конфигурацию, а также отслеживать ее неизменность. vGate также журналирует все события безопасности в режиме реального времени, оповещает администратора информационной безопасности о нарушениях, а также предоставляет мощный механизм отчетов о состоянии инфраструктуры.

vGate сертифицирован ФСТЭК России, и его использование поможет привести виртуальную инфраструктуру в соответствие требованиям регуляторов при обработке персональных данных, конфиденциальной информации, а также сведений, относящихся к гостайне.

СПЕЦПРОЕКТ КОМПАНИИ "КОД БЕЗОПАСНОСТИ"

ИБ...

ПРОДОЛЖЕНИЕ СО С. 17

ции и средства — специализированные исследовательские центры, специалисты, собирающие и анализирующие информацию об уязвимостях ПО со всего мира с высокой оперативностью.

Павел Власов предлагает разделять множество ИБ-функций, которые должны быть реализованы в комплексной ИБ-системе, на несколько классов, обосновывающих сочетание встроенных механизмов защиты с наложенными.

ИБ-функции уровня аппаратных платформ. К ним г-н Власов относит контроль аппаратной среды, доверенную загрузку ПО виртуализации, аппаратное шифрование данных в системах хранения данных (СХД). Наложенные средства на этом уровне возможны, но накладывают неприемлемые ограничения. Например, модули доверенной загрузки российского производства рассчитаны на применение в классических серверах и неприменимы на серверах-лезвиях, а наложенное средство шифрования данных в СХД может снизить скорость обмена до неприемлемой для пользователя.

ИБ-функции уровня ПО виртуализации. На этом уровне, как отмечает г-н Власов, должны выполняться базовые ИБ-функции, которые одновременно являются неотъемлемой частью самой технологии виртуализации. Основная из них — разграничение доступа к данным, обрабатываемым в ВМ, и изоляция ВМ. На этом уровне также должны решаться задачи:

- по управлению виртуальной инфраструктурой с применением мандатно-ролевого принципа доступа к объектам (ВМ, другому виртуальному оборудованию и т. п.) и субъектам доступа (администраторам виртуальной инфраструктуры, оркестраторам и т. п.);
- контроля целостности ПО виртуализаторов;
- доверенной загрузки образов ВМ;
- межсетевого экранирования (контроль трафика на сетевом уровне);
- контроля миграции образов ВМ.

Часть этих функций безопасности может быть решена и уже решается наложенными средствами, но логичнее возложить их реализацию на вендоров ПО виртуализации. Такой подход позволит избежать проблем встраивания наложенных средств защиты информации (СЗИ) в системы, упростит и, скорее всего, удешевит создаваемую систему ИБ.

ИБ-функции, которые могут быть выполнены наложенными средствами. Среди них г-н Власов видит СЗИ, которые напрямую не связаны с технологией виртуализации, но тем не менее должны учитывать ее особенности. Это антивирусы, системы IDS/IPS, выполнение криптографических функций, системы DLP. При этом ПО виртуализации для снижения нагрузки на вычислительные ресурсы должно предоставлять стандартизированные программные интерфейсы для встраивания ИБ-продуктов третьих производителей. Наличие таких интерфейсов позволит применять безагентные технологии.

На необходимость кооперации производителей платформ виртуализации и производителей СЗИ указывает также и Матвей Войтов, напоминая, что ведущие разработчики средств виртуализации идут именно по этому пути. В качестве примера он приводит компанию VMware, предлагающую инструментарий для интеграции сторонних ИБ-решений в свою платформу, что обеспечивает тем самым возможность создавать специализированные продукты для защиты платформ VMware (ту самую безагентную защиту).

В то же время с помощью безагентного ИБ-инструментария, отмечает г-н Войтов, можно создавать только платформно-зависимые решения, накладывающие к тому же некоторые ограничения на ИБ-технологии. Чтобы избежать этого, он рекомендует использовать решения, не зависящие от платформы виртуализации, способные к тому же реализовывать самые продвинутые ИБ-технологии.

Констатируя необходимость развития как встроенной, так и наложенной защиты, Юрий Черкас отмечает, что российские компании сегодня располагают довольно развитой собственной ИБ-инфраструктурой, весомой частью которой являются наложенные средства, как по отношению к ИКТ-инфраструктуре, так и по отношению к бизнес-приложениям. Этот фактор будет играть свою роль в организации ИБ виртуализированных ИКТ-сред на протяжении нескольких лет.

Влияние и нынешняя готовность российской регулятивной базы к виртуализации ИКТ

Наши эксперты, констатируя, что регулирование рынка ИБ является одним из драйверов его развития, единодушно отмечают активизацию российских регуляторов в области регулирования организации защиты виртуальных сред — связанные с нею вопросы поднимаются на повестку дня ими в последнее время все чаще и чаще. К тому же, как подчеркивает Юрий Черкас, за последние два года отечественные регуляторы сильно продвинулись в направлении развития двустороннего диалога с российским ИБ-сообществом.

Виртуализация — это специфическая технология, и технические аспекты ее применения, включая возникающие при этом задачи защиты информации, как напоминает Павел Власов, должны регулироваться не напрямую законодательством, а сопроводительными документами технического уровня — стандартами, техническими и юридическими рекомендациями, издаваемыми органами государственной власти, уполномоченными регулировать деятельность в области защиты информации, и т. п.

На протяжении двух последних лет ФСТЭК России, напоминает Константин Пичугов, сформулировала и внесла в свои нормативные документы конкретные требования к защите среды виртуализации. Эти требования касаются защиты персональных данных в информационных системах персональных данных (ИСПДн), защиты данных в государственных информационных системах (ГИС). В ближайшее время, по его словам, следует ожидать появления подобных требований, предъявляемых к защите автоматизированных систем управления технологическими процессами (АСУ ТП).

Г-н Власов оценивает работу ФСТЭК над новыми документами, устанавливающими требования и рекомендации по защите информации при использовании для ее обработки технологий виртуализации, как достаточно активную. К числу уже действующих наиболее важных нормативных документов, устанавливающих обязательные требования в этой сфере, как он отмечает, относятся следующие:

- в области обеспечения безопасности персональных данных — приказ ФСТЭК России от 18 февраля 2013 г. № 21 (зарегистрированный Минюстом России, № 28375 от 14.05.2013), регламентирующий состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн;

• в области обеспечения безопасности информации ограниченного доступа, обрабатываемой в ГИС, — приказ ФСТЭК России от 12 февраля 2013 г. № 17 (зарегистрирован Минюстом России, № 28608 от 31.05.2013), определяющий требования к защите информации, содержащейся в ГИС и не составляющей государственную тайну; методический документ "Меры защиты информации в ГИС", разработанный ФСТЭК России (утвержден директором ФСТЭК России 11.02.2014).

Для банковской отрасли, подчеркнул г-н Власов, подготовлены и находятся в стадии обсуждения еще два полезных, по его оценкам, документа, которые будут носить рекомендательный характер: проект национального стандарта РФ ГОСТ Р "Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Общие положения" и проект рекомендаций в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Рекомендации по обеспечению информационной безопасности при использовании технологии виртуализации".

Введение в действие этих двух стандартов пока затягивается, что, как считает г-н Власов, свидетельствует о том, что готовность российской регулятивной базы к виртуализации ИКТ и влияние ее на направление пока еще недостаточны (за исключением аспектов защиты персональных данных и информации, обрабатываемой в ГИС). Однако он выражает надежду, что с введением в действие (в ближайшей перспективе) двух упомянутых стандартов ситуация улучшится.

Перечисленные выше документы устанавливают универсальные требования и определяют базовый набор мер по обеспечению ИБ при использовании технологии виртуализации для обработки защищаемой информации.

Эксперты также напоминают, что действующий (всё еще!) на территории нашей страны международный стандарт PCI DSS для платежных систем Visa и MasterCard еще несколько лет назад был усовершенствован в целях учета ИБ-угроз виртуализации и требований к защите виртуализированных сред. Для операторов этих платежных систем нынешний год является переходным от второй к третьей версии стандарта: если в нынешнем году еще можно сертифицироваться на соответствие второй версии, то начиная с 2015 г. — только на третью.

Как отмечает Джабраил Матиев, все новые требования регуляторов к ИБ в обязательном порядке учитывают использование виртуализации в ИКТ. В качестве примера он приводит опубликованный для обсуждения в мае текущего года проект Федерального закона, разработанный Минкомсвязи России, "О внесении изменений в отдельные законодательные акты Российской Федерации в части использования облачных вычислений" (напомним, что в облачных вычислениях применение технологии виртуализации особенно эффективно). Хотя этот документ г-н Матиев оценивает как поверхностный, тенденцию, намеченную в нем регулятором, он расценивает как правильную.

Наши эксперты считают, что предпринятые регуляторами шаги пока лишь первые из конкретизирующих позицию государства и отраслевых регуляторов в области обеспечения ИБ виртуализированных ИКТ-сред. Они, как все российские пользователи ИКТ, ожидают от регуляторов новых уточняющих регулятивные требования документов и рекомендаций по их выполнению.

Ожидаемые технологические и организационные перемены

Эксперты довольно вяло отозвались на предложение нашего издания высказаться по поводу ожидаемых технологических прорывов и необходимых организационных перемен в области обеспечения ИБ виртуализированных ИКТ-сред. Возможно, это связано с замедлением роста российской ИТ-отрасли и общей стагнацией экономики у нас в стране. А может быть, ИКТ-потребители переживают сейчас период освоения довольно широкого спектра предложений в рассматриваемой области, и рынку нужно время для накопления опыта их применения.

Константин Пичугов отмечает насущную потребность в нашей стране в проработанной нормативной базе в области применения облачных технологий. Он считает, что нужны конкретные требования и разъяснения регуляторов о том, как распределяется ответственность между владельцем облаков, сервис-провайдерами и операторами персональных данных, как регламентировать доступ сотрудников ЦОДов и сервис-провайдеров к размещенным в ЦОДах данным клиентов, как решать вопрос трансграничной передачи данных, если ЦОД провайдера находится за границей…

С учетом сложной международной обстановки Павел Власов рекомендует стимулировать через создание соответствующих государственных программ разработку и производство в нашей стране собственного ПО и оборудования для построения ЦОДов (включая средства и решения по обеспечению ИБ), использующих технологии виртуализации.

В условиях, когда основные производители средств виртуализации находятся за рубежом, а в России только начата разработка нормативных актов, устанавливающих требования и рекомендации по защите информации при использовании для ее обработки технологии виртуализации, крайне важно, по мнению г-на Власова, представлять позиции в этой области регулирующих органов нашей страны на международных площадках. Это, с одной стороны, позволит зарубежным разработчикам средств виртуализации и СЗИ ознакомиться с правилами игры на российском рынке (прежде всего с учетом необходимости сертификации продукции), а с другой — российским регуляторам принять к сведению общие международные тенденции и оперативно корректировать нормативную базу в целях исключения противоречащих им (а порой невыполнимых и для внутреннего рынка) требований.

Главных изменений в области обеспечения ИБ виртуализации, по мнению Джабраила Матиева, нужно добиваться не столько через законодательство, регулирующее ее, сколько через сознание владельцев виртуализированных ИКТ-сред, и не дожидаться возможных массовых компрометаций технологии.

Одним из возможных механизмов, подходящих для этого, является обучение. Именно с ним Матвей Войтов в первую очередь связывает позитивные перемены в области ИБ виртуализации. Он считает, что обучение поможет тем компаниям, которые до сих пор используют в виртуальных средах традиционные ИБ-решения (а таких, по его оценкам, всё еще немало), перейти на специализированные, что позволит им решить проблемы совместимости инструментов, продуктов и решений, а самое главное — освободить нерационально расходуемые значительные вычислительные ресурсы и использовать их для бизнес-приложений.

На нехватку методических рекомендаций от производителей конкретных продуктов виртуализации и СЗИ для виртуальных сред, особенно на русском языке, обращает внимание Андрей Арефьев.

Однако с учетом всего, сказанного выше, по мнению Юрия Черкаса, в ряду насущных для нашей страны ИБ-проблем (которых, как он считает, немало) проблемы ИБ виртуализованных ИКТ-сред стоят далеко не на первом месте — есть гораздо более насущные проблемы.