# Защита систем виртуализации

Давно пора понять что каждая новая технология, которая появляется в области ИТ, приносит с собой все более новые угрозы. Причем развитие средств нападения, как правило, опережает средства обороны. А борьба снаряда и брони вечна, пока живет человечество.

Как показало исследование «Лаборатории Касперского», проводившееся совместно с агентством B2B International в 14 странах мира, включая Россию, 91% компаний сталкивались с внешними киберугрозами. В России этот показатель еще выше – 96%. Более того, ситуация становится только хуже: почти половина участников исследования утверждает, что количество кибератак за этот период увеличилось, и лишь 8% говорят о незначительном снижении их числа.

Перечисляя киберугрозы, которые представляются им самыми значительными, большинство участников исследования во всем мире ставят на первое место вирусы, шпионское ПО и другие вредоносные программы (61%). Спам назвали источником угрозы 56% респондентов. Третье место (36%) заняли фишинговые атаки, за ними идут сбои, вызванные проникновением в корпоративную сеть (24%), и DDoS-атаки (19%).

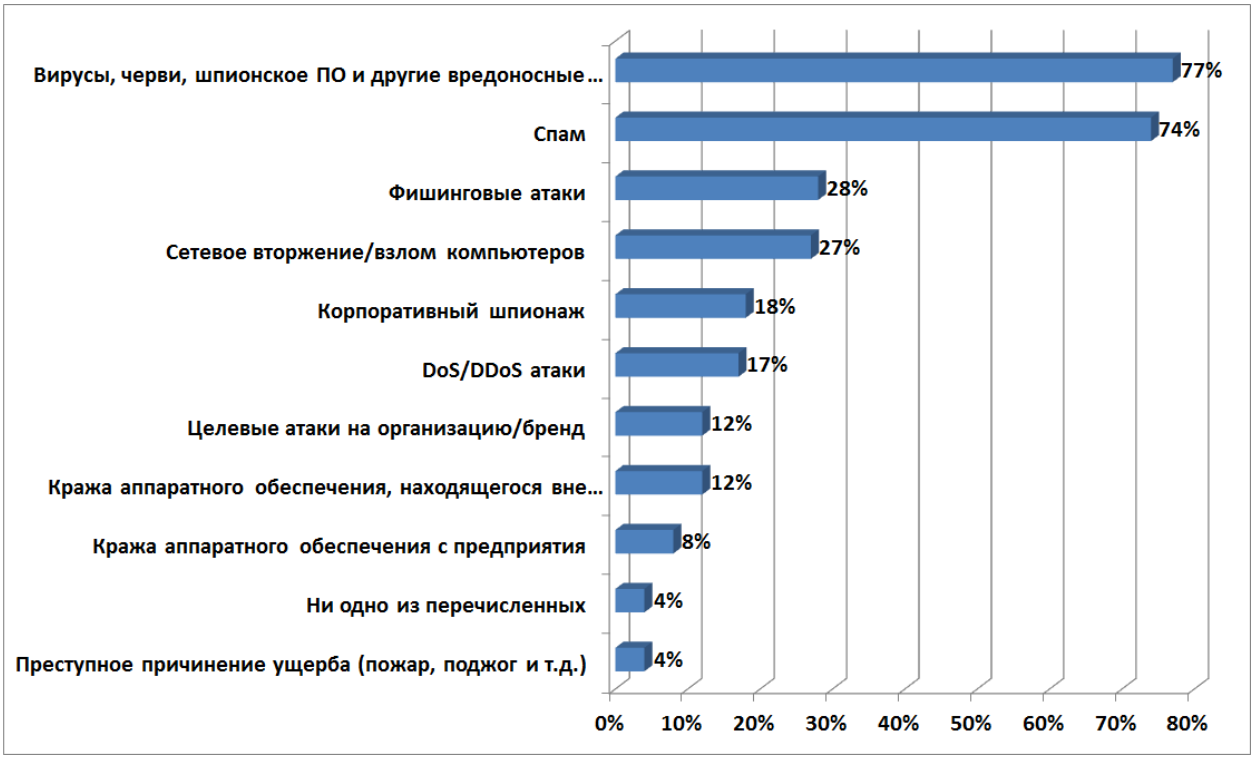


Рисунок 1 Типы внешних угроз, с которыми сталкивались российские компании

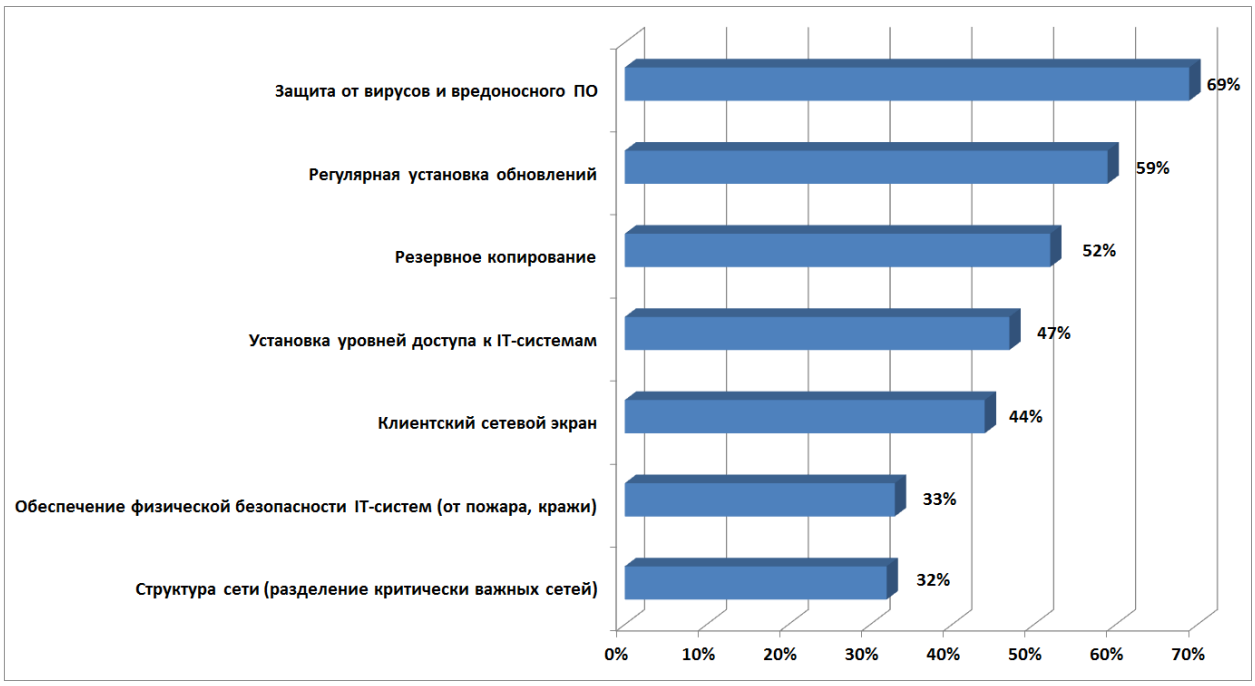


**Рисунок 2 Наиболее широко применяемые в России меры по обеспечению информационной безопасности**

Стоит отметить, что несмотря на то, что **защита от вредоносного ПО наиболее широко применяемая в России мера безопасности, все же 31% компаний до сих пор не применяет ее в полном объеме!**

В данной статье мы с вами рассмотрим риски одной из технологий, сравнительно недавно появившейся в нашем мире, но уже успевшей снискать повсеместную популярность – технологии виртуализации. А также поговорим о способах защиты машин в виртуальной среде: что в ответ на растущие киберугрозы нам готов предложить рынок, и с какими трудностями могут столкнуться компании при выборе защитного решения. Но вначале немного истории.

Понятие виртуализации появилось сравнительно недавно. В 2005 году она впервые была использована в целях консолидации рабочих нагрузок нескольких виртуальных машин (ВМ), размещаемых на одном физическом сервере в рамках процедур разработки и тестирования.

К 2008 году сформировалось второе поколение технологий, в котором основное внимание уделялось консолидации бизнес-приложений. Появились динамические функции, и применение виртуализации стало стремительно расширяться. Получила распространение и виртуализация рабочих станций – в частности, технология virtual desktop infrastructure (VDI), с помощью которой рабочие станции консолидировано размещаются на серверах в виде ВМ.

Сегодня IT всего мира вступают в третью «облачную» фазу. Для нее характерно развертывание внутри компаний систем с высокой степенью виртуализации и автоматизированным управлением.

В наше время виртуализация стала привычным явлением. По данным IDC[1], сейчас большинство развертываемых серверов являются виртуальными. В конце 2009 г. число физических и виртуальных серверов сравнялось, и с тех пор это соотношение неуклонно меняется в пользу

[1] The IDC Technology Spotlight, Новый взгляд на безопасность виртуальных сред, 2012 г.

последних. По прогнозам IDC, к 2014 г. оно превысит 2:1, то есть среди развертываемых серверов виртуальных будет вдвое больше, чем физических.

К концу 2010 г. более половины приложений и сервисов было перенесено в виртуальную среду. По прогнозам IDC, к 2013 г. эта доля превысит 2/3.

Российские компании этот общемировой тренд также не обошел стороной. По данным исследования «Лаборатории Касперского», 40% организаций в России уже применяют серверную виртуализацию, и еще 19% планируют перейти к этой технологии в течение года. Чаще всего российские предприятия используют виртуализацию применительно к базам данных, электронной почте и ERP-приложениям. Причем, согласно проведенному опросу, большинство всех сервисов, запущенных в виртуальной среде, являются критически важными для бизнеса.

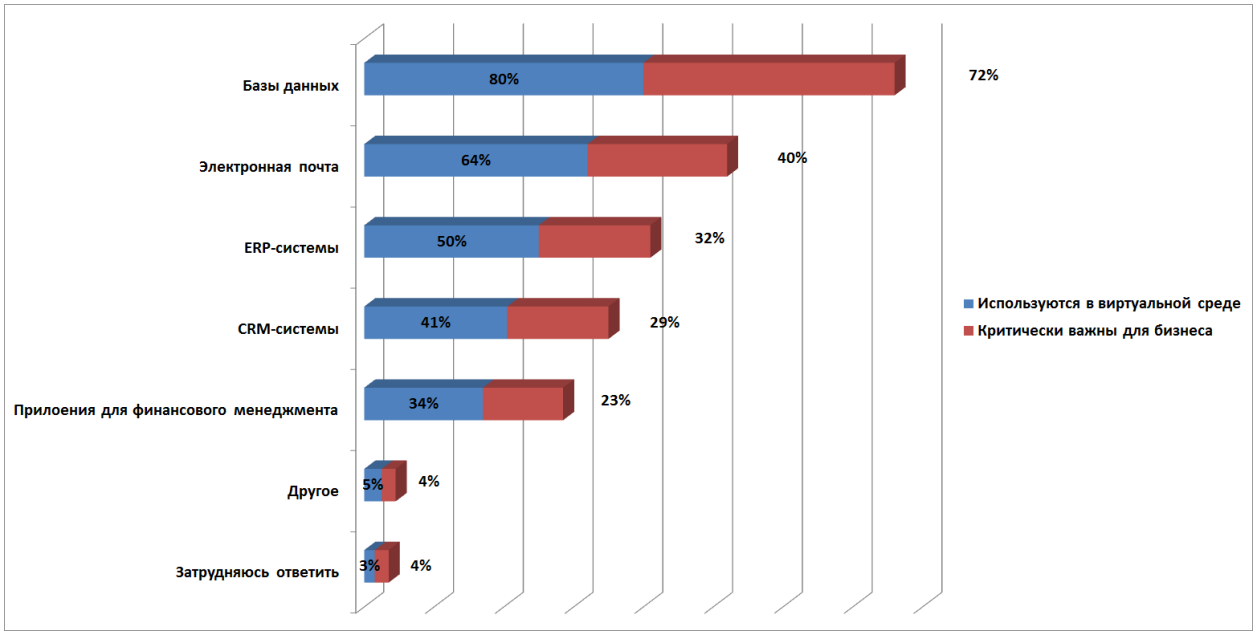


**Рисунок 3 Приложения, используемые в виртуальной среде в России**

Столь высокая популярность технологии не удивительна. Виртуализация действительно дает бизнесу немало преимуществ – от снижения капитальных затрат до повышения производительности и отказоустойчивости IT-инфраструктуры.

Вместе с тем стоит учитывать, что внедрение виртуализации приносит с собой и новые проблемы, затрагивая все аспекты деятельности центра обработки данных (ЦОД). И безопасность – одна из таких проблем. В условиях сосредоточения нескольких виртуальных машин на одном физическом компьютере появляются дополнительные риски, и инциденты безопасности могут иметь более серьезные последствия, т.к. заражение одной виртуальной машины представляет угрозу для всей виртуальной среды. Более того, если раньше вредоносные программы создавались только для физических систем, сейчас вирусописатели создают вредоносный код, предназначенный как для физических, так и для виртуальных машин. Некоторые вредоносные программы способны сохраняться на виртуальной машине, даже когда она неактивна, и возобновлять вредоносные действия при выходе ее из спящего режима.

Увы, однако в связи с удобствами и преимуществами виртуализации проблемы безопасности нередко уходят на второй план. Однако сегодня стоит признать, что виртуальные машины

подвержены всем тем же угрозам, что и физические компьютеры, и одна зараженная ВМ может создать угрозу для всего дата-центра.

По мнению специалистов IDC, сегодня виртуальные среды весьма сложно защищать, так как для действительно эффективной защиты на предприятии нужно развернуть единую платформу, обеспечивающую управление и обеспечение безопасности всех - виртуальных, физических и мобильных - устройств в сети.

Стоит отметить, что в связи со все более широким применением виртуализации применение традиционных подходов, связанных с использованием антивирусных агентов, сталкивается с целым рядом проблем:

- Неэффективное использование ресурсов. На сервере оказывается большое количество антивирусных агентов, работающих независимо, что в свою очередь приводит к дефициту ресурсов сервера (несколько агентов могут начать одновременное сканирование соответствующих ВМ или начать одновременное обновление).
- Проблемы с выявление незащищенных ВМ (ведь в каждый момент времени какая-то часть ВМ может быть выключена).

Существует другой способ защиты виртуальных машин, без использования антивирусных агентов. Это позволяет решить следующие проблемы безопасности ВМ:

- Ресурсы ВМ, размещаемых на хост-сервере, используются куда более эффективно. На каждом сервере устанавливается один экземпляр антивирусного ядра, с помощью которого проверяются все ВМ на данном сервере на наличие вредоносного кода.
- При переходе ВМ из неактивного состояния в активное для каждой ВМ не нужно проводить обновление антивирусного ПО.
- Невозможен перерасход ресурсов во время обновления или сканирования, так как по умолчанию каждый раз данный процесс контролируется.

Типичным представителем данного класса ПО является Kaspersky Security для виртуальных сред, решение для защиты от вредоносных программ, не требующее установки антивирусного агента на каждую ВМ, созданное специально для виртуальных инфраструктур и тесно интегрированное с технологией vShield Endpoint.

Основные возможности:

- Интегрируется с решением VMware vShield Endpoint для обеспечения централизованной защиты всех виртуальных машин на хост-сервере vSphere или View без установки антивирусного агента на каждую ВМ (сервер или рабочую станцию).
- Работает на базе новейшего антивирусного ядра «Лаборатории Касперского». Частые обновления позволяют обеспечить высочайший уровень обнаружения угроз при минимальном использовании ресурсов сервера. При обнаружении вредоносного ПО угроза блокируется и удаляется, а администратор получает соответствующее уведомление.
- Поддерживает сканирование виртуальных машин по требованию, а также по расписанию. Благодаря кэшированию проверенные файлы не сканируются повторно, что позволяет экономить ресурсы.

Помимо этого, Kaspersky Security для виртуальных сред обладает следующими возможностями развертывания, управления и интеграции с VMware:

- Продукт поставляется в виде виртуального устройства безопасности, которое легко развертывается на хост-сервере и не требует дополнительной установки операционной системы и приложений.
- Kaspersky Security Center 9.0 обеспечивает централизованное управление задачами антивирусной защиты как для физических, так и для виртуальных и мобильных устройств из единой консоли, а также формирование отчетов.
- Взаимодействует с vCenter для получения сведений о виртуальной инфраструктуре VMware.
- Решение позволяет создавать профили безопасности для применения различных параметров безопасности к разным группам виртуальных машин. Политики продолжают действовать даже в случае переноса виртуальных машин на другой хост-сервер с помощью vMotion.

Исходя из вышесказанного стоит отметить, что виртуализация это технология, внедрение которой неизбежно, однако стоит понимать, что любая новая технология несет в себе новые риски и к ним нужно быть готовым заранее иначе проблемы с безопасностью сведут на нет все ваши успехи в технологии. И внедрение новой технологии без учета требований безопасности принесет только новую головную боль.

Достойный же уровень безопасности могут обеспечить только специализированные решения, потому что обеспечивать безопасность новой технологии старыми методами не удавалось еще никогда и никому.