КОД БЕЗОПАСНОСТИ

Защита виртуальной инфраструктуры

Аналитическое исследование
Март 2018 г.

Содержание

Резюме

- Больше половины используемых российскими компаниями серверов виртуализованы;
- Треть отечественных заказчиков рынка собираются переходить на российские гипервизоры;
- **70%** российских компаний хранят и обрабатывают на виртуальных машинах конфиденциальную информацию;
- **74%** заказчиков корпоративного сектора не переходят на конвергентные платформы и продолжают использовать традиционные архитектурные компоненты виртуализации;
- **56%** респондентов считают вопросы безопасности основным барьером для использования «облаков»;
- **23%** участников исследования не используют виртуализацию для информационных систем, требующих аттестации;
- Ключевыми параметрами информационной безопасности виртуальной инфраструктуры (ВИ) заказчики считают резервное копирование, антивирусную защиту, мониторинг событий безопасности ВИ, разграничение доступа внутри виртуальной инфраструктуры и защиту данных внутри виртуальных машин;
- Две трети компаний опасаются ущерба, нанесенного действиями администратора ВИ, причем как умышленными, так и неумышленными;
- Чаще всего российские предприятия используют технологии виртуализации применительно к файловым ресурсам **(76%)**, средствам коммуникации **(76%)** и бухгалтерским программам **(64%)**;
- Лишь **7%** российских компаний используют специализированные средства шифрования для виртуализации;
- Основными факторами, затрудняющими использование различных средств защиты информации виртуальной инфраструктуры, для респондентов стали влияние СЗИ на работу виртуальной инфраструктуры **(38%)**, сложности настройки и администрирования **(37%)** и необходимость переконфигурирования ВИ **(34%)**.

АННОТАЦИЯ

Технологии виртуализации в настоящее время являются одним из ключевых компонентов современной ИТ-инфраструктуры организаций. Сейчас уже сложно представить построение нового серверного узла компании без использования технологий виртуализации. Они помогают оптимизировать бизнес-процессы компаниям, и топ-менеджмент получает больше возможностей для развития бизнеса. Причинами такой популярности являются экономия денег и времени, оптимизация трудозатрат. Чтобы повышение эффективности использования вычислительных ресурсов за счет виртуализации происходило не в ущерб надежности и безопасности, не стоит забывать про важность защиты информации в виртуальных инфраструктурах.

Аналитики компании «Код Безопасности» провели исследование, оценили текущее состояние и перспективы развития этого сегмента рынка, чтобы предложить наиболее эффективный подход к построению системы защиты виртуальной инфраструктуры.

Методика сбора данных и анализа

Исследование проводилось по России. Использовался количественный метод в форме онлайн-опроса на сайте компании «Код Безопасности» (www.securitycode.ru). В исследование включена информация на основе ответов 305 специалистов по информационной безопасности, работающих в компаниях 10 отраслей: госсектор, здравоохранение, IT, образование, промышленность, строительство, телекоммуникации, топливно-энергетический комплекс, услуги, финансы.

При обработке полученных результатов компании были классифицированы по численности сотрудников на малые (до 100 чел.), средние (101–1000 чел.) и крупные (более 1000 чел.).

Респонденты

По размеру компании

По должностям

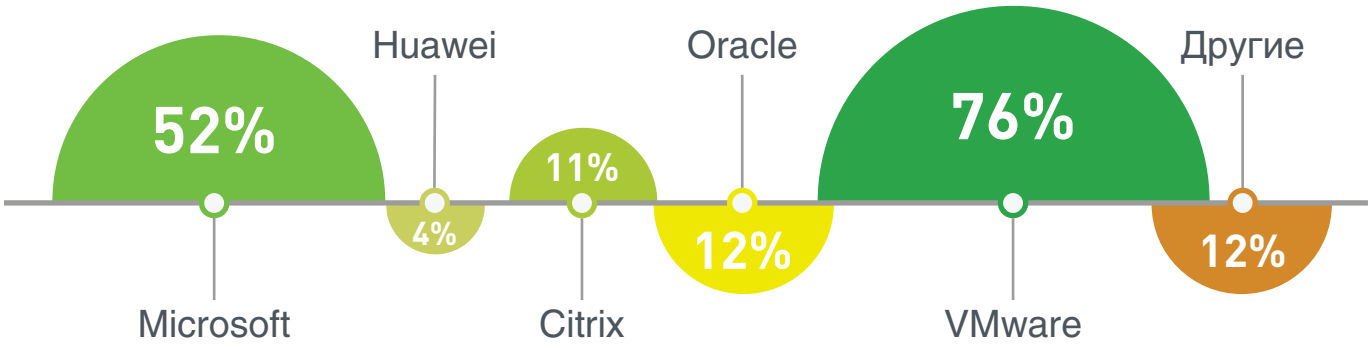
IT-директора, ведущие инженеры, специалисты по защите информации, руководители направлений информационной безопасности.

Характеристика виртуальной инфраструктуры российских компаний

Популярные платформы виртуализации

Технология виртуализации подразумевает наличие в инфраструктуре дополнительного компонента – гипервизора, который контролирует работу приложений во всех виртуальных средах. Ключевыми игроками на рынке виртуализации, согласно данным опроса, являются VMware и Microsoft.
Платформу виртуализации компании VMware используют 76% респондентов, платформу виртуализации компании Microsoft – 52% респондентов. Менее популярны среди опрошенных такие платформы, как Oracle, Citrix и Huawei. В группу «Другие», которая составила 12%, вошли такие вендоры, как KVM, Proxmox, Xen, РусБИТех, Parallels.
Ряд компаний используют в своей инфраструктуре решения сразу нескольких производителей программного обеспечения для виртуализации одновременно. Как распределились приоритеты участников опроса при выборе платформ, отражено на следующем графике:

Популярность платформ виртуализации (по вендорам)



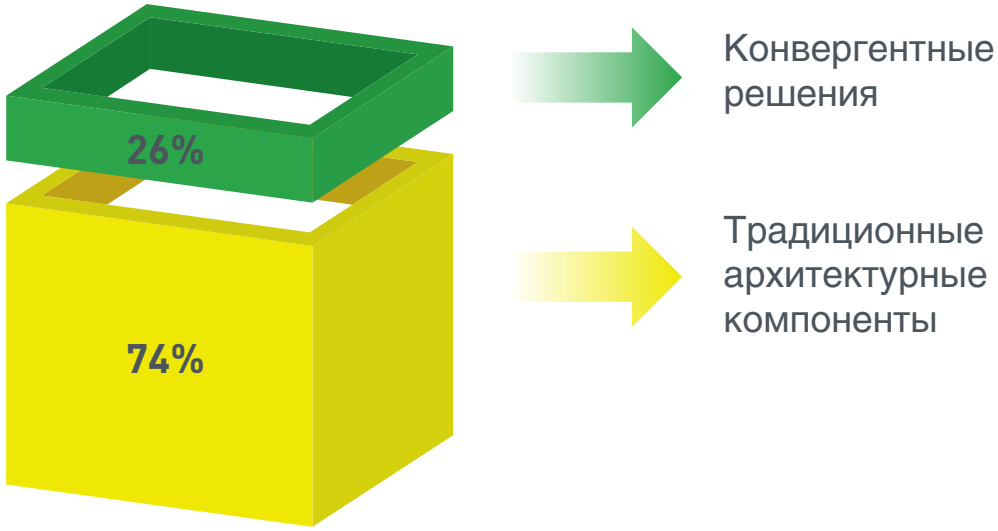
Конвергентные платформы vs традиционная архитектура

Постепенное «взросление» технологий виртуализации и распространение облачных решений дало толчок появлению нового способа организации эффективной ИТ-инфраструктуры. Появляются так называемые конвергентные системы. Главная идея конвергентных решений состоит в интеграции разрозненных аппаратных и программных элементов в единый комплекс и предоставлении заказчику всего, что необходимо для работы: вычислительных мощностей, ресурсов хранения, сетевой поддержки, средств виртуализации, программного администрирования, обслуживания приложений. Конвергентный тип инфраструктуры представляет собой готовое «коробочное» решение. Насколько же популярен такой формат среди отечественных заказчиков?

Опрос показал, что только четверть российских компаний – участников исследования применяют конвергентные решения. Остальные 74% респондентов используют для создания виртуальной инфраструктуры традиционные архитектурные компоненты.

Характеристика виртуальной инфраструктуры российских компаний

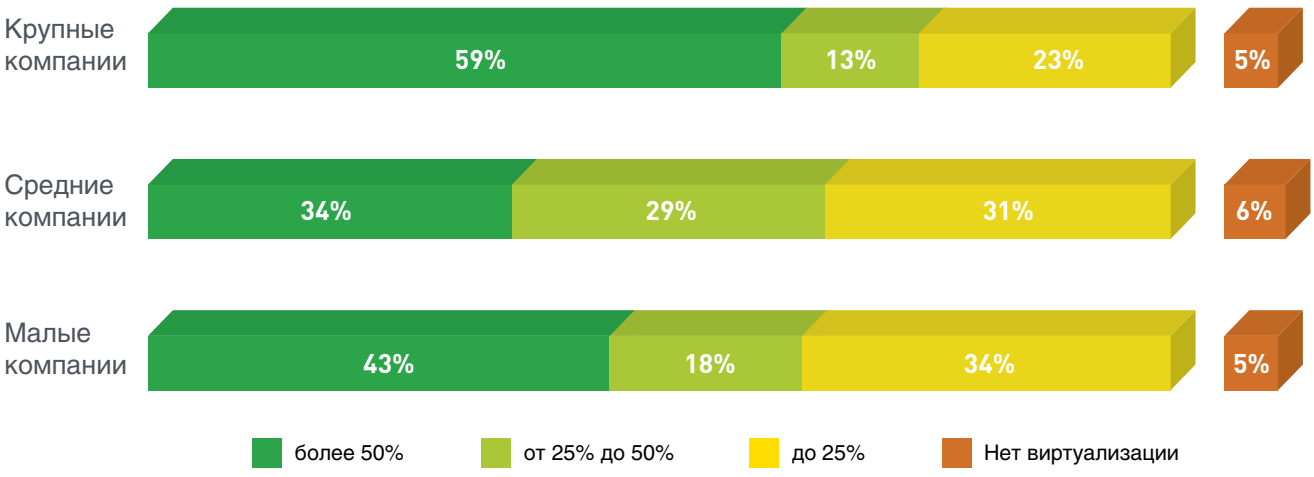
Архитектура виртуальной среды



Виртуализация серверной инфраструктуры российских компаний

Значительная часть организаций, независимо от масштабов их бизнеса, виртуализовали свою серверную инфраструктуру более чем на 50%. Это говорит о высоком уровне зрелости рынка виртуализации. Не виртуализованной остается серверная инфраструктура не более 6% российских компаний.

Доля виртуализованной серверной инфраструктуры

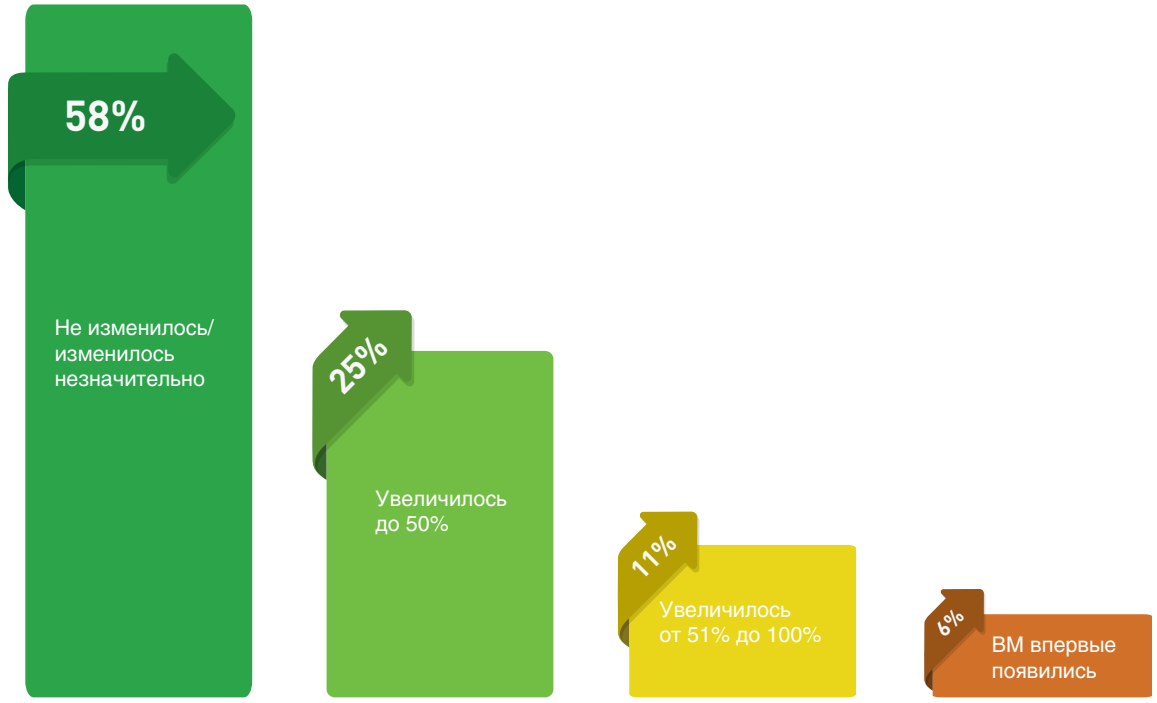


Характеристика виртуальной инфраструктуры российских компаний

Изменение количества используемых виртуальных машин

Виртуальная среда стала неотъемлемой частью ИТ-инфраструктур. При этом 58% опрошенных за последние два года не расширяли виртуальную инфраструктуру. Количество виртуальных машин в этих компаниях оставалось на прежнем уровне либо увеличивалось незначительно. Четверть компаний-респондентов увеличили количество виртуальных машин до 50%. Более чем на 50% возросло количество виртуальных машин у 11% респондентов. Впервые за последние два года появилась виртуализация у 6% опрошенных компаний.

Рост количества виртуальных машин (ВМ) за 2016-2017 гг.



Отношение опрошенных компаний к использованию сторонней арендуемой виртуальной инфраструктуры

Рынок облачных технологий продолжает расти и развиваться, стремясь удовлетворить потребности пользователей в оптимизации ресурсов и расходов. Помимо возможности виртуализовать ресурсы компании собственными силами сейчас существует альтернатива – переход в публичное облако. Самыми распространенными услугами являются SaaS (Software as a Service) и IaaS (Infrastructure as a Service). Как бизнес понимает данный формат и готов к использованию облачных услуг?

Характеристика виртуальной инфраструктуры российских компаний

При переходе к хранению данных у внешнего провайдера у российских компаний возникает ряд сложностей – снижается возможность контролировать доступ к своим данным и встает вопрос об обеспечении их безопасности. Исследование показало, что 91% опрошенных пока не используют арендуемую виртуальную инфраструктуру. И в первую очередь это обусловлено опасениями, связанными с рисками ИБ (56%). 21% компаний не видит преимуществ в облачном подходе. 10% отказались от технологии из-за завышенной цены.

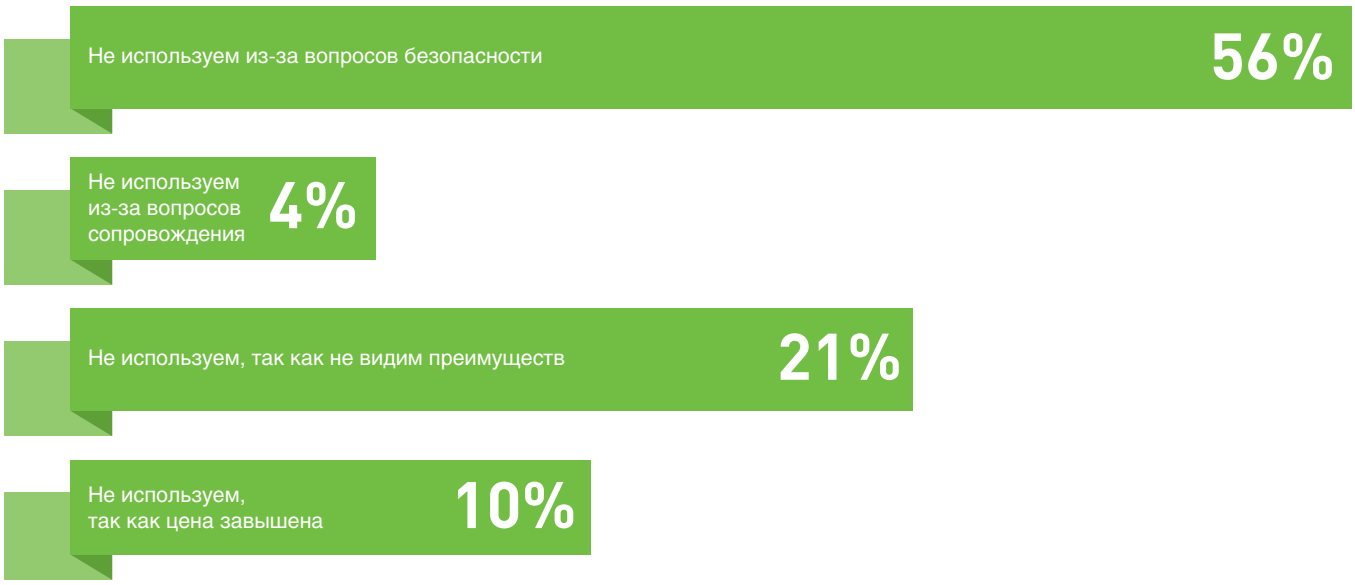
Использование арендуемой ВИ

91% Не используем арендуемую виртуальную инфраструктуру

7% Используем IaaS

2% Используем SaaS

Причины отказа от использования сторонней виртуальной инфраструктуры

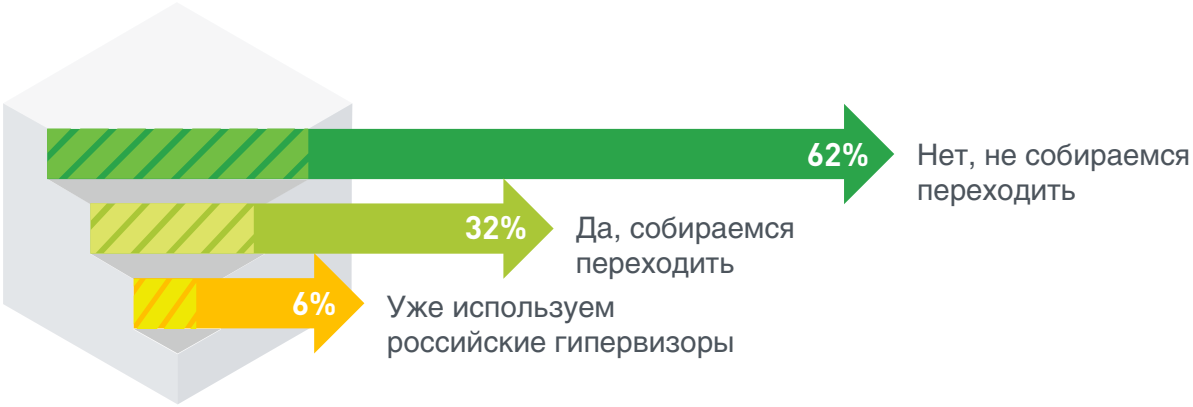


Характеристика виртуальной инфраструктуры российских компаний

Импортозамещение гипервизоров

Долгие годы лидерами виртуализации на российском рынке были закрытые решения западных вендоров. После введения санкций ситуация с присутствием продуктов зарубежных производителей стала меняться. Предложение российских игроков стало пользоваться бóльшим спросом, однако подавляющее большинство (94%) респондентов отметили, что продолжают использовать иностранные гипервизоры, и только треть планируют переходить на российские. А 6% респондентов уже используют российские продукты.

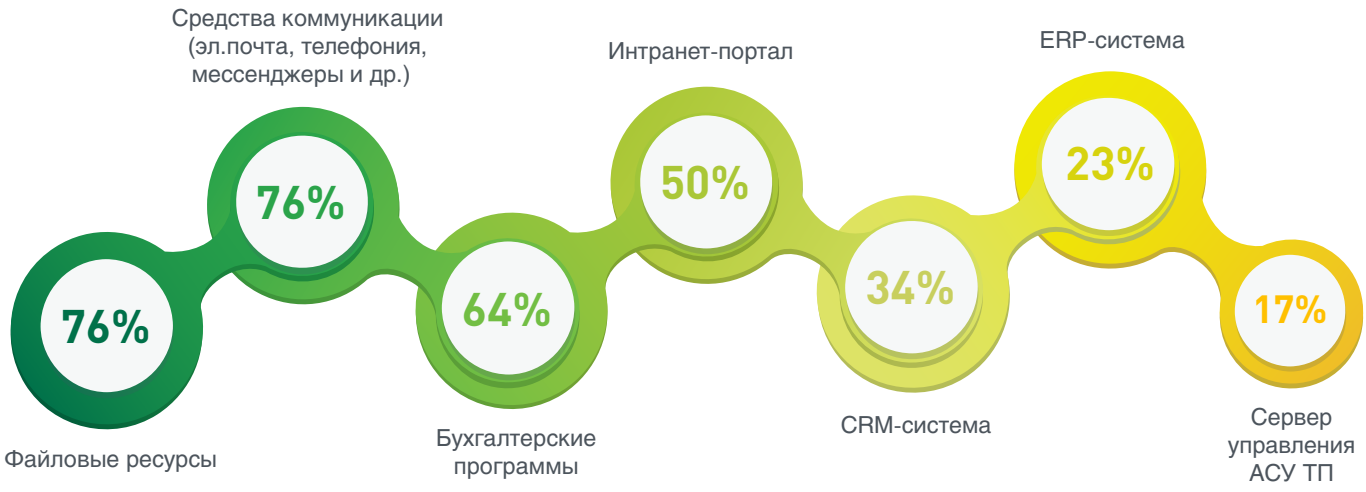
Переход на российские гипервизоры



Сервисы в виртуальной среде

Чаще всего российские предприятия используют технологии виртуализации применительно к файловым ресурсам (76%), средствам коммуникации (76%) и бухгалтерским программам (64%). Менее значимую долю сервисов, работающих в виртуальной среде, заняли интранет-портал (50%), CRM-система (34%), ERP-система (23%) и сервер управления АСУ ТП (17%).

Сервисы в виртуальной среде



Характеристика виртуальной инфраструктуры российских компаний

Какая информация обрабатывается на виртуальных машинах

Исследование продемонстрировало, что конфиденциальную информацию обрабатывают на виртуальных машинах 70% российских компаний-респондентов.
Наибольшую долю хранящихся на виртуальных машинах данных (76%) составляет общедоступная информация. И лишь 3% компаний обрабатывают сведения, содержащие государственную тайну.
Следует также отметить, что в виртуальных инфраструктурах компаний присутствуют системы разных классов и одновременно хранятся и обрабатываются разные типы данных.

Типы информации, обрабатываемой в ВИ

76%

70%

3%

общедоступная

конфиденциальная

информация, содержащая гостайну

Компании, обрабатывающие в ВИ разные типы данных одновременно

47%

Актуальные угрозы информационной безопасности в виртуальной среде

Источники угроз

В настоящее время технологии виртуализации используют множество крупных, средних и небольших российских компаний, обеспечивая не только экономию ИТ-бюджетов, но и существенное увеличение гибкости ИТ-инфраструктуры. Какие проблемы при выборе подхода к обеспечению информационной безопасности стоят перед компаниями?
Независимо от размера компании, основной опасностью при использовании виртуализации респонденты назвали умышленные/неумышленные действия администратора ВИ. Особо остро это ощущают малые компании: представители 66% из них отметили опасность действий администратора. Эти опасения подтвердили коллеги из средних (65%) и крупных компаний (55%). Действий злоумышленников извне опасаются в среднем лишь 38% российских компаний.

Опасения российских компаний относительно безопасности ВИ

Применение виртуализации дает возможность оптимизировать ресурсы компании, но несет в себе и опасность – появляется дополнительный канал для проникновения злоумышленника и повышается вероятность потери конфиденциальных данных, хранящихся и обрабатывающихся в ВИ. Однако опрос показал, что две трети компаний считают основным источником угроз в среде виртуализации действия именно администратора ВИ, а не злоумышленника извне. Особенность эксплуатации ВИ такова, что непоправимый вред могут нанести действия администратора, причем как умышленные, так и непреднамеренные.

Актуальные угрозы информационной безопасности в виртуальной среде

Угрозы для виртуальной инфраструктуры

Бизнес во всем мире испытывает большие потери из-за инцидентов в виртуальной среде. Какие угрозы при эксплуатации виртуальной инфраструктуры актуальны для российского бизнеса? В ходе исследования аналитиками «Кода Безопасности» были выявлены группы, включающие актуальные угрозы, и произведена оценка критичности угроз внутри каждой группы.

Угрозы при эксплуатации виртуальной инфраструктуры

Актуальные угрозы информационной безопасности в виртуальной среде

Самой многочисленной стала группа угроз несанкционированного доступа. Внутри группы для 42% компаний актуальна угроза несанкционированного доступа к консоли управления виртуальной инфраструктурой; 38% респондентов отметили актуальность угрозы несанкционированного доступа к системе хранения данных и 36% – угрозы несанкционированного доступа к гипервизору.

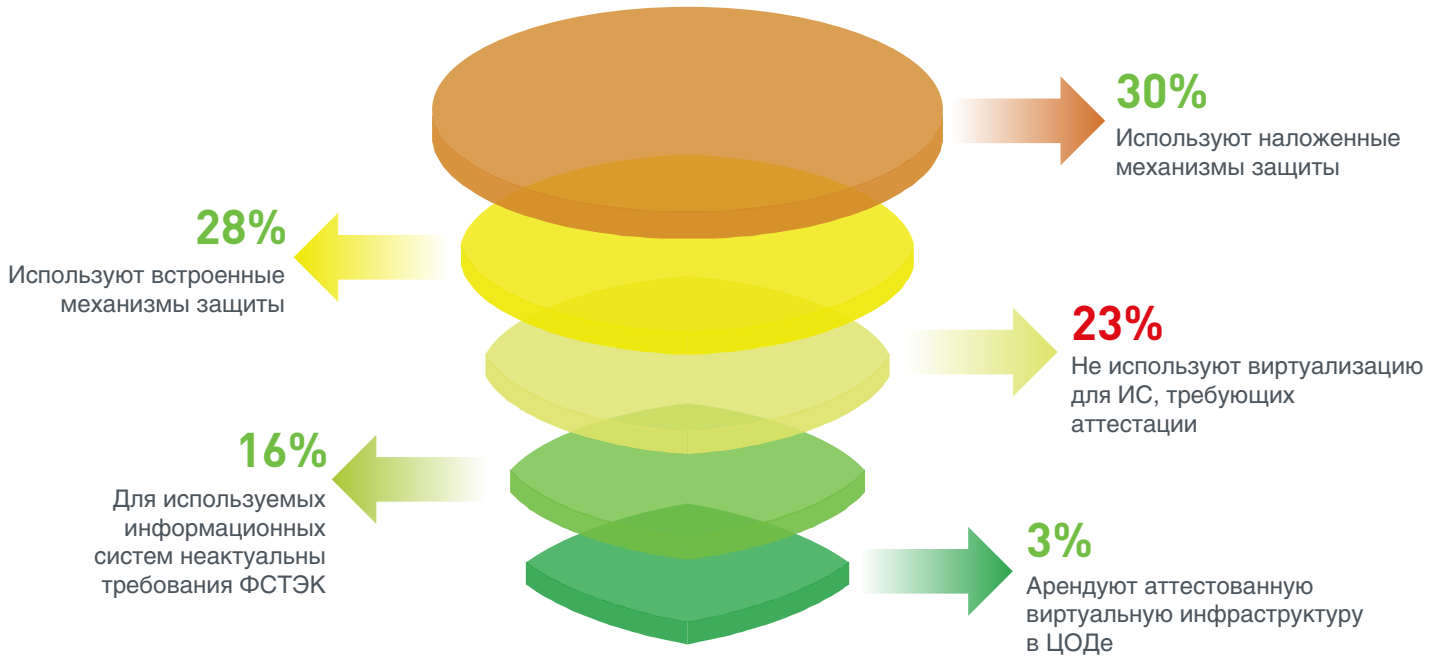
Наибольшее опасение у корпоративного сектора вызывает угроза нарушения процедуры аутентификации субъектов виртуальной инфраструктуры – ее отметили 44% пользователей. Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов актуальна для 42% предприятий. 40% респондентов отметили важность угрозы использования новых плохо защищенных виртуальных машин из группы угроз «Ошибки архитектуры виртуальной инфраструктуры».

Вопросы безопасности при эксплуатации виртуальных инфраструктур

Выполнение требований ФСТЭК России по защите виртуальной инфраструктуры

Вопрос о том, что к защите ИТ-инфраструктур, построенных с использованием технологий виртуализации, должен применяться особый подход, стал подниматься не сразу. Причины – и в отсутствии специальных требований со стороны регуляторов, и в популярном заблуждении о том, что виртуализация делает ИТ-инфраструктуру безопаснее и надежнее. Включение мер по защите виртуализации в нормативные документы ФСТЭК России стало шагом к стандартизации вопросов защиты виртуальных инфраструктур.

Выполнение требований ФСТЭК РФ по защите ВИ



Вопросы безопасности при эксплуатации виртуальных инфраструктур

Как показали результаты исследования, для 84% опрошенных требования ФСТЭК России актуальны. Из них 30% компаний используют наложенные механизмы защиты; 28% компаний используют встроенные механизмы защиты ВИ; 23% участников рынка не используют виртуализацию для ИС, требующих аттестации.

Для информационных систем 16% респондентов требования ФСТЭК России неактуальны. В основном это компании сферы ИТ/Телеком.

Актуальные аспекты безопасности российских компаний

Популярность виртуализации меняет модель построения инфраструктуры информационной безопасности. На что компании обращают внимание в первую очередь при создании системы защиты виртуальной инфраструктуры, представлено на графике ниже.

Основные направления обеспечения безопасности виртуальной инфраструктуры

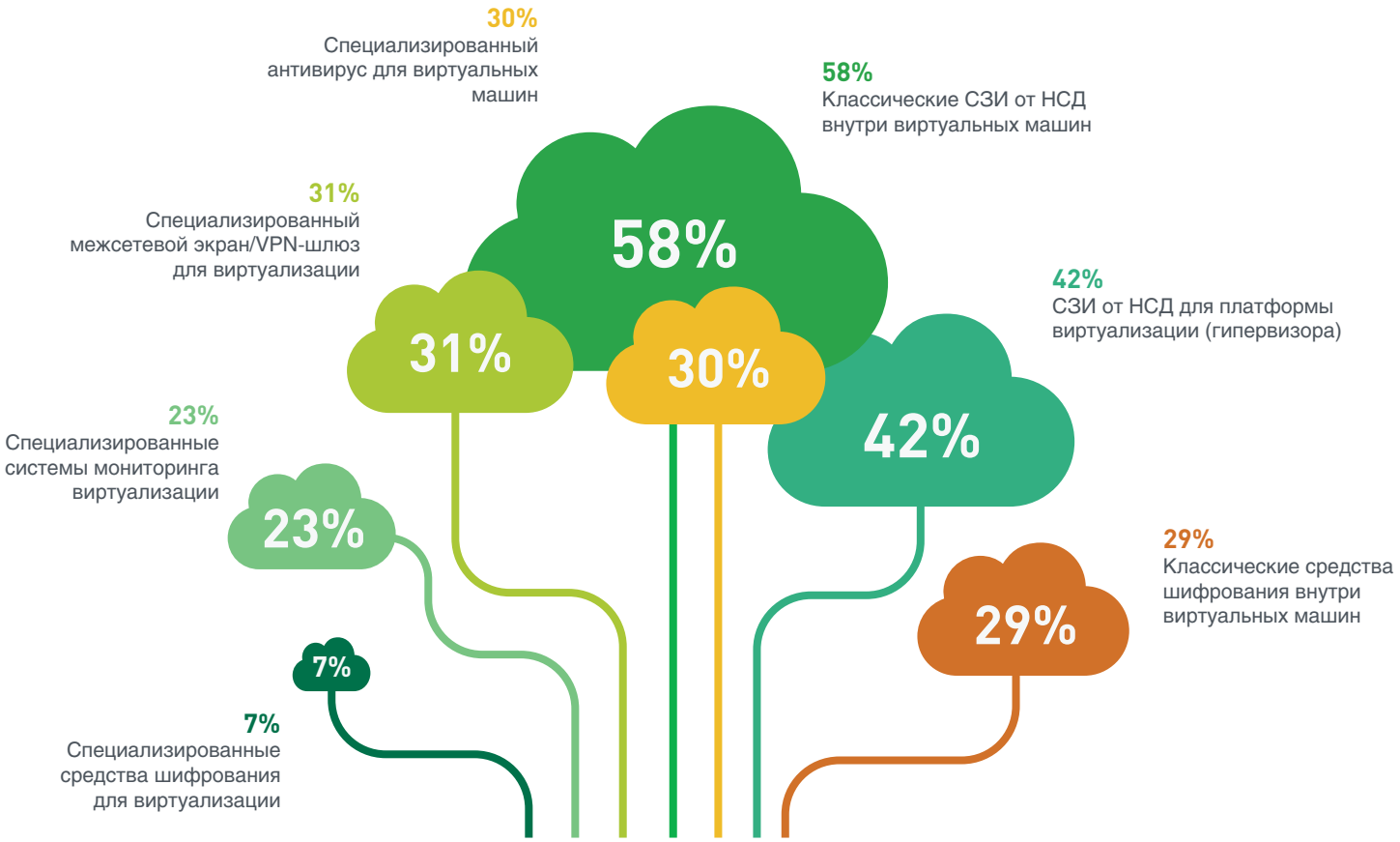
Вопросы безопасности при эксплуатации виртуальных инфраструктур

Ключевым параметром информационной безопасности ВИ заказчики считают резервное копирование виртуальных машин – его отметили 76%. Второе и третье место по значимости для бизнеса заняли антивирусная защита (67%) и мониторинг событий безопасности ВИ (60%). Такой аспект, как разграничение доступа внутри виртуальной инфраструктуры, актуален для 59% ИБ-специалистов, а защита данных внутри виртуальных машин – для 53%.

Средства защиты виртуальной инфраструктуры

Корпоративному бизнесу технологии виртуализации дают массу преимуществ. Однако важно грамотно подходить к выбору не только платформы виртуализации, но и решений для ее защиты.

Предпочтения российских компаний в выборе средств защиты виртуализации



Вопросы безопасности при эксплуатации виртуальных инфраструктур

По результатам исследования большинство компаний (58%) используют классические СЗИ от НСД внутри виртуальных машин, 29% компаний применяют классические средства шифрования внутри виртуальных машин. Специализированный антивирус для виртуальных машин и специализированный межсетевой экран для виртуализации используют 30% и 31% организаций соответственно. Лишь 7% российских компаний используют специализированные средства шифрования для виртуализации.

Сложности при использовании средств защиты виртуальной инфраструктуры

Перед каждой компанией, использующей виртуализацию, встает вопрос защиты виртуальной инфраструктуры и безопасного доступа к ней.

Основной «киберболью» для пользователей стало влияние СЗИ на работу виртуальной инфраструктуры – его отметили 38% респондентов. На второе место участники рынка поставили проблемы, связанные со сложностью администрирования и настройки – 37%. И 34% ИБ-специалистов назвали ключевым неудобство, связанное с необходимостью переконфигурирования ВИ при использовании СЗИ. Также некоторые респонденты отметили такие сложности, как значительные задержки в развертывании новых версий виртуализации из-за отставания выпуска средств защиты; недостаток квалифицированного персонала; необходимость приобретения дополнительных лицензий; небольшой список поддерживаемых гипервизоров. Лишь 3% респондентов не испытывают сложностей при использовании различных средств защиты виртуальной инфраструктуры.

Сложности применения средств защиты виртуализации

Заключение

Большинство российских компаний уже используют виртуализацию. О том, что технологии виртуализации позитивно воспринимаются рынком, свидетельствует перевод компаниями в виртуальную среду бизнес-критичных приложений, т.е. приложений, недоступность которых ведет к ощутимым негативным последствиям для бизнеса – вплоть до полной остановки деятельности. Российские компании размещают в виртуальной инфраструктуре системы разных классов; одновременно хранят и обрабатывают разные типы данных. Как уже упоминалось, **76%** опрошенных хранят в виртуальной среде общедоступную информацию, **70%** – конфиденциальную информацию; **3%** – информацию, содержащую гостайну.

Популярность виртуализации вполне понятна, ведь ее применение позволяет оптимизировать расходы на ИТ (обслуживание физических серверов, оплата электроэнергии, замена комплектующих, зарплата обслуживающего персонала). Для решения одних и тех же задач виртуализованная инфраструктура требует гораздо меньше ресурсов по сравнению с классическим подходом.

Однако распространение технологий виртуализации происходит намного быстрее, чем понимание необходимости применения особого подхода при обеспечении защиты виртуальных сред. Появляется ряд специфических угроз, не характерных для классической «железной» инфраструктуры. Поэтому и защиту виртуальных сред должны обеспечивать специализированные средства.

Исследование показало, что две трети компаний считают основным источником угроз в среде виртуализации не внешнего злоумышленника, а администратора виртуальной инфраструктуры. Особенность эксплуатации ВИ такова, что умышленные либо непреднамеренные действия администратора могут нанести непоправимый вред. Ошибки в эксплуатации могут быть разными – отсутствие backup, несвоевременное применение обновлений и патчей, ошибки конфигурации, исключение виртуальной инфраструктуры из зоны ответственности систем мониторинга, некорректная настройка журналирования или полное отсутствие логов. Предотвратить риски с точки зрения возможных утечек информации, снизить возможность угроз в виртуальных средах поможет комплексный и системный подход к защите.

Специалисты назвали ряд приоритетных требований при выборе решения для защиты виртуальной инфраструктуры:

- СЗИ не должно оказывать высокую нагрузку на виртуальную инфраструктуру и снижать ее производительность;
- Низкие требования к ресурсам виртуализации;
- Простота настройки и эксплуатации;
- Отсутствие необходимости переконфигурирования ВИ;
- Надежность и стабильность работы;
- Поддержка современных платформ виртуализации;
- Соответствие требованиям регулирующих органов.

Целостная система защиты ВИ должна включать три компонента:

- Система защиты виртуальных машин;
- Система защиты виртуальных сетей;
- Система защиты средств управления гипервизором:
  - Контроль настроек безопасности гипервизора;
  - Разграничение прав доступа администраторов ВИ к интерфейсу управления;
  - Контроль целостности и управление доступом к данным виртуальных машин;
  - Мониторинг безопасности ВИ.

КОД БЕЗОПАСНОСТИ

«Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, среды виртуализации, облачных сред, мобильных устройств, а также коммерческой и государственной тайны. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

Тел.: +7 (495) 982 30 20

analytics@securitycode.ru

www.securitycode.ru