kaspersky

CNews Analytics

КУРС НА ОБЛАЧНУЮ БЕЗОПАСНОСТЬ В РОССИИ – 2024

ДЕКАБРЬ 2024
CNews

Оглавление

Исследование на тему:

«Курс на облачную безопасность в России — 2024»

ВВЕДЕНИЕ

В сентябре 2024 года «Лаборатория Касперского» и CNews Analytics провели совместное исследование распространения облачных технологий в России и обеспечения облачной безопасности, в том числе рабочих облачных нагрузок. Нашей целью было получить актуальную картину рынка в вопросах использования облачной среды, сложившегося восприятия различных типов инфраструктуры в аспекте безопасности, популярности различных инструментов киберзащиты и планов по их внедрению. В рамках исследования был проведен телефонный опрос 111 респондентов, отвечающих за информационные технологии и информационную безопасность в компаниях таких отраслей, как ИТ, производство, банки, финансовые и страховые услуги, торговля и добыча полезных ископаемых.

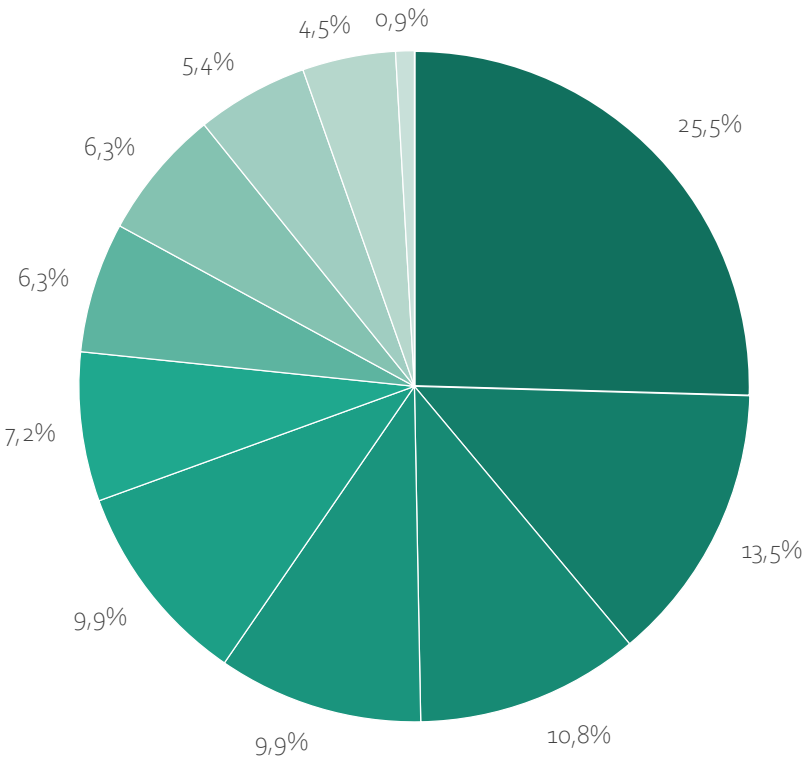
Ключевые результаты исследования

- 64% респондентов применяют облака в своей инфраструктуре.
- 54% респондентов продолжают пользоваться локальной инфраструктурой наравне с облачной, лишь 10% — только облачной.
- 70% компаний переносят в облачную инфраструктуру ИТ-системы и базы данных. Перенос таких систем, как CRM, анализ данных и продаж, ERP и расчета заработной платы осуществляется более низкими темпами.
- У 35% компаний на облако приходится от 60% до 100% рабочей нагрузки.
- 80% компаний планируют расширять применение облачных технологий для создания и развертывания приложений в облаке в перспективе ближайших трех лет.
- Среди подходов, которые применяются в ИБ-стратегии приложений в организации, чаще всего упоминали Zero trust (52,2%) и DevSecOps (43,5%).
- Для защиты облачной инфраструктуры чаще всего используют встроенную защиту провайдера облака (73,9%), защиту виртуализации (63%) и решения для защиты конечных устройств или EPP-платформы (54,3%).
- 34% компаний готовы инвестировать в решения для безопасности облаков на основе ИИ и ML, а 45% — в инструменты анализа уязвимостей и реакции на инциденты.

ПОРТРЕТ УЧАСТНИКОВ ИССЛЕДОВАНИЯ

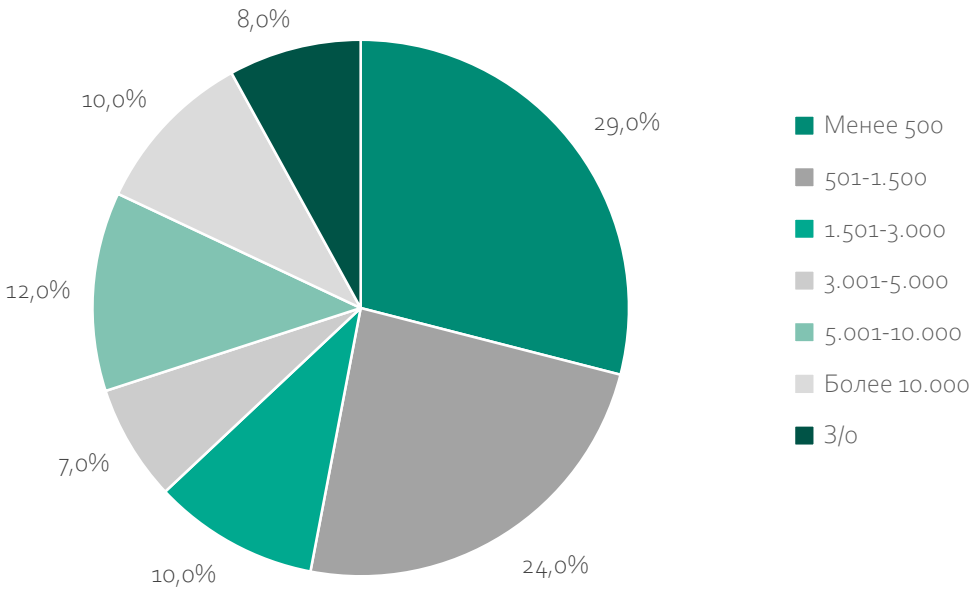
Четверть компаний (25%), участвовавших в исследовании, относятся к сфере ИТ, 14% – к производству, 11% – к банковским, финансовым и страховым услугам. Примерно равные доли пришлись на сферы торговли, добычи полезных ископаемых – около 10% соответственно, а также на сферы телекоммуникаций и здравоохранения – по 6%. Туризм, транспорт и логистика составили 7%, медиа и развлечения – 5%, государственный сектор – 5%, наука и образование – 1%.

Отрасль организации (%)



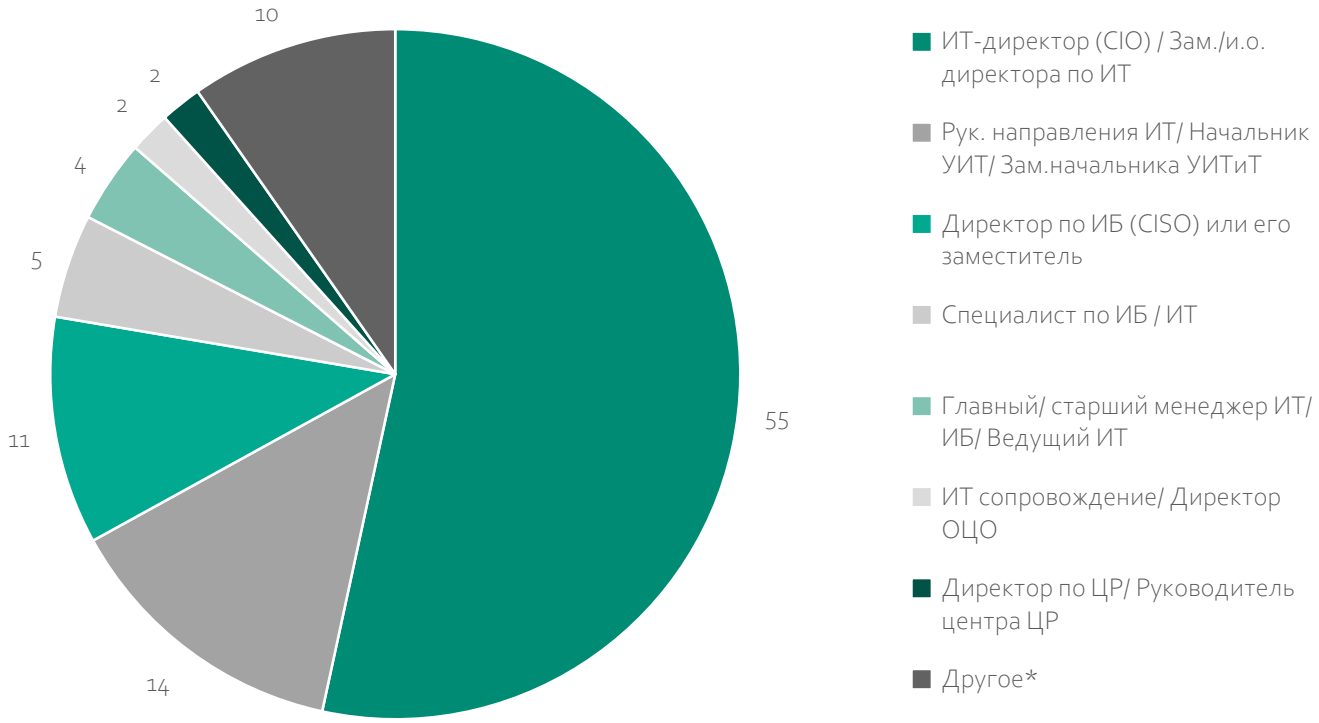
У более четверти опрошенных компаний (29%) на момент проведения исследования (сентябрь 2024 г.) штат насчитывал 500 сотрудников, еще у 24% компаний – от 500 до 1500 чел., у 12% – от 5000 до 10 000 чел. Равные доли компаний имеют персонал численностью более 10 000 чел. и от 1500 до 3000 чел. (по 10% соответственно). 7% компаний – от 3000 до 5000 чел., остальные 8% затруднились ответить.

Структура респондентов по численности сотрудников компании (%)



Большая часть респондентов является ИТ-директорами, руководителями или заместителями руководителя управления информационных технологий - 69%, 11% - директоры или заместители по ИБ, 5% являются специалистами по ИБ или ИТ, 4% - менеджеры по ИБ или ИТ верхнего или среднего звена.

Должности респондентов (%)



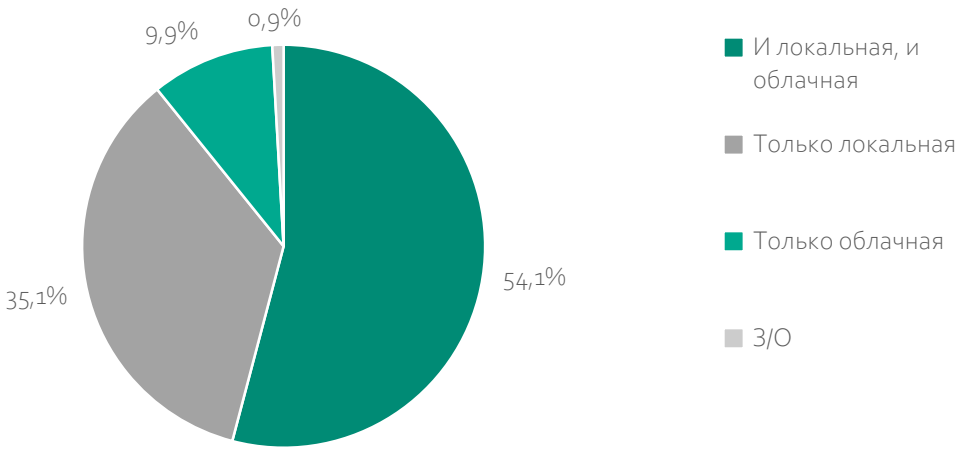
*Другое:

- СТО
- Директор по ИТ-архитектуре и управлению данными
- Директор по развитию цифровых сервисов
- ИТ и ИБ
- Руководитель IT-инфраструктуры
- Рук. направления платформенных решений
- Рук. направления платформенных решений
- Архитектор IT
- Вице-президент по IT
- Нач. отдела администрирования прикладного ПО и СУБД
- Нач. управления сервисами ИТ-инфраструктуры

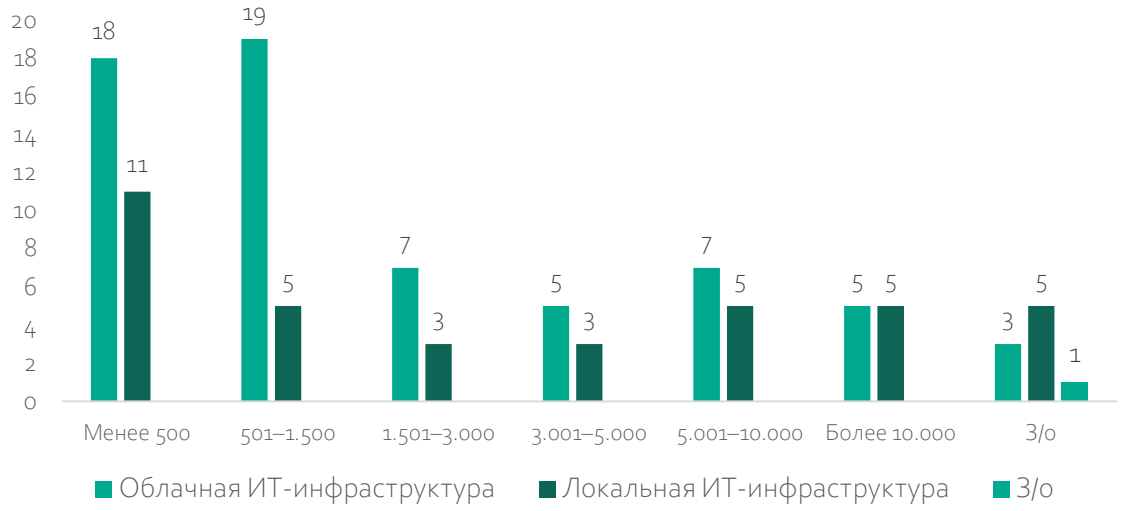
РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

64% респондентов применяют облака в своей ИТ-инфраструктуре. Из них 46,5% респондентов используют гибридное облако, 31% - публичное облако, 21,1% — частное облако, 1,4% — гособлако.
Большинство респондентов используют и локальную, и облачную ИТ-инфраструктуру (54%), более трети используют только локальную (35%), лишь 10% – только облачную. Исследование показало, что и крупные, и небольшие компании используют облачную ИТ-инфраструктуру.

Используемая ИТ-инфраструктура (%)



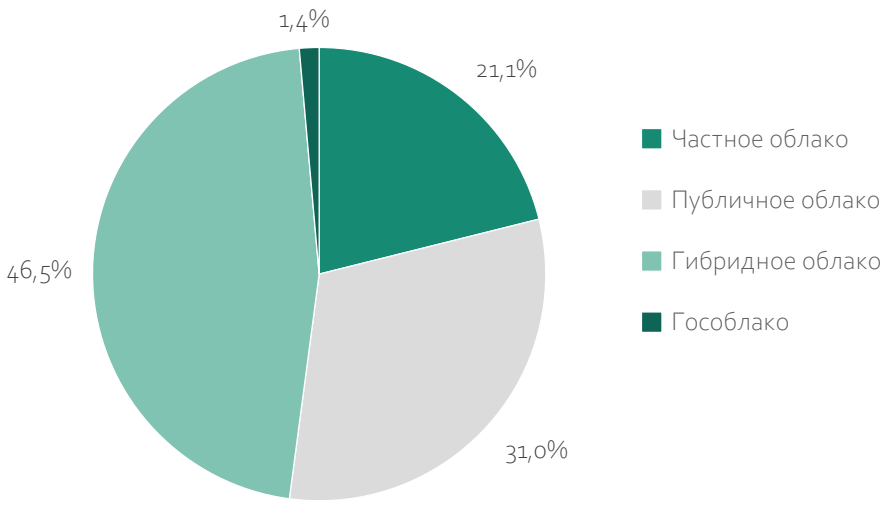
Соотношение размера компании и используемой ИТ-инфраструктуры (%)



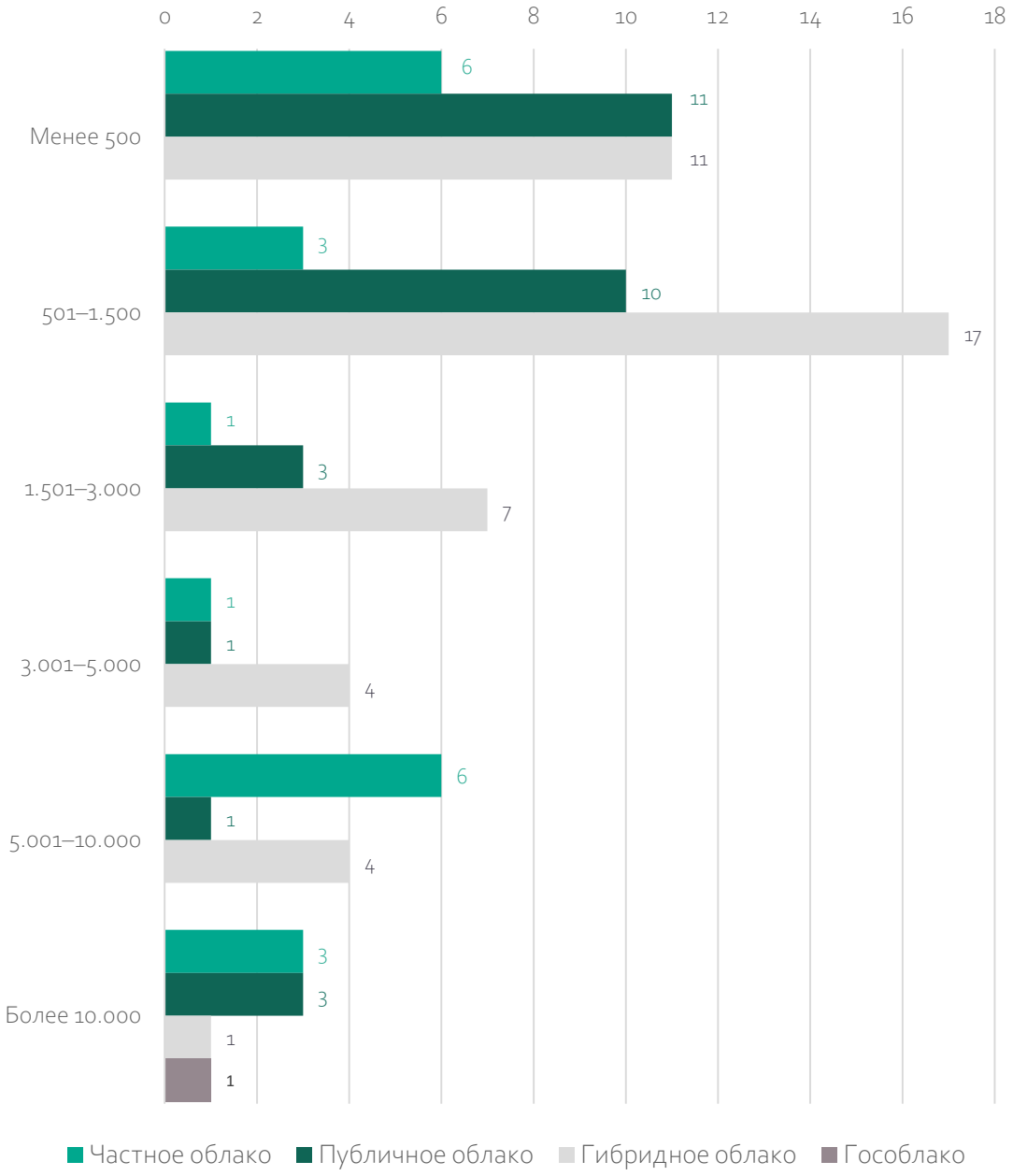
ИТ-инфраструктура компаний-респондентов

64% компаний в качестве ИТ-инфраструктуры используют либо только облачную, либо и локальную, и облачную. Почти половина из них использует гибридное облако (46,5%), 31% – публичное облако. Еще 21,1% – частное облако, 1,4% – гособлако. Небольшие компании отдают предпочтение в основном гибридному облаку, крупные компании – как частному, так и публичному облаку.

Если используете облачную ИТ-инфраструктуру, то какую именно? (%)



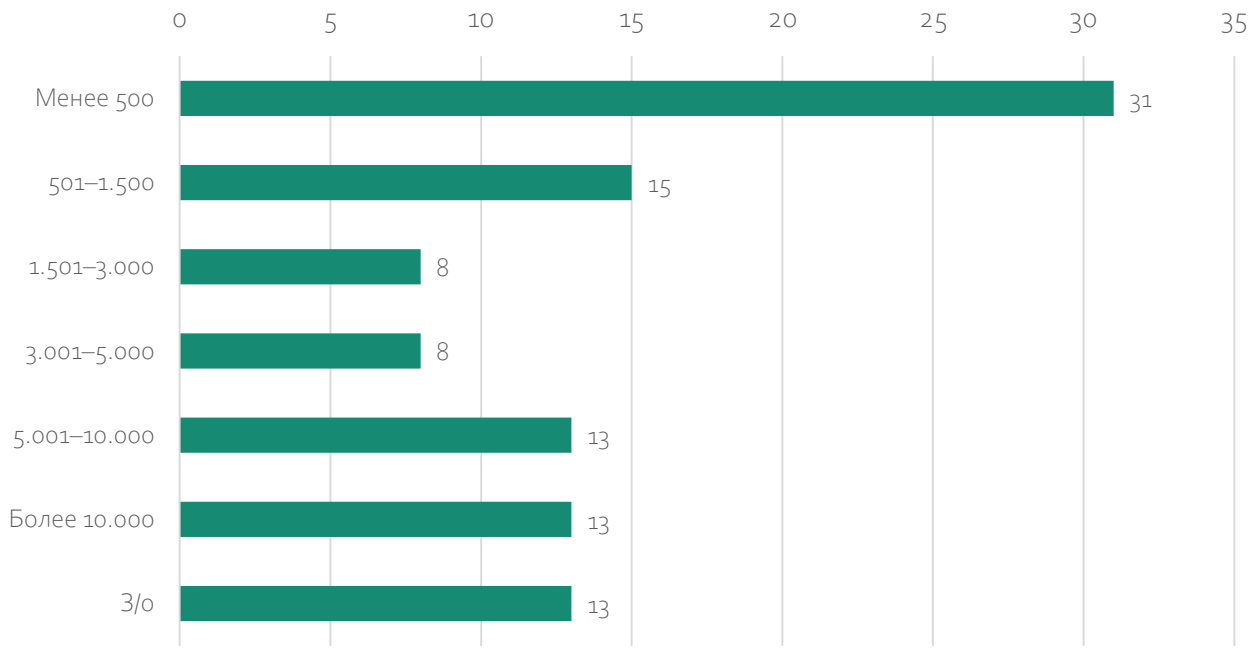
Соотношение размера компании и используемой облачной ИТ-инфраструктуры (%)



Мнение респондентов, не использующих облака

Как выяснилось в ходе исследования, 35,1% компаний используют только локальную ИТ-инфраструктуру, из них 92,3% не планируют переносить рабочую нагрузку в облако.
Из тех, кто планирует перенести рабочую нагрузку в облако (5,1%), доли тех, кто выбрал для этого частное облако и гибридное, равны.

Соотношение размера компании и используемой локальной ИТ-инфраструктуры (%)



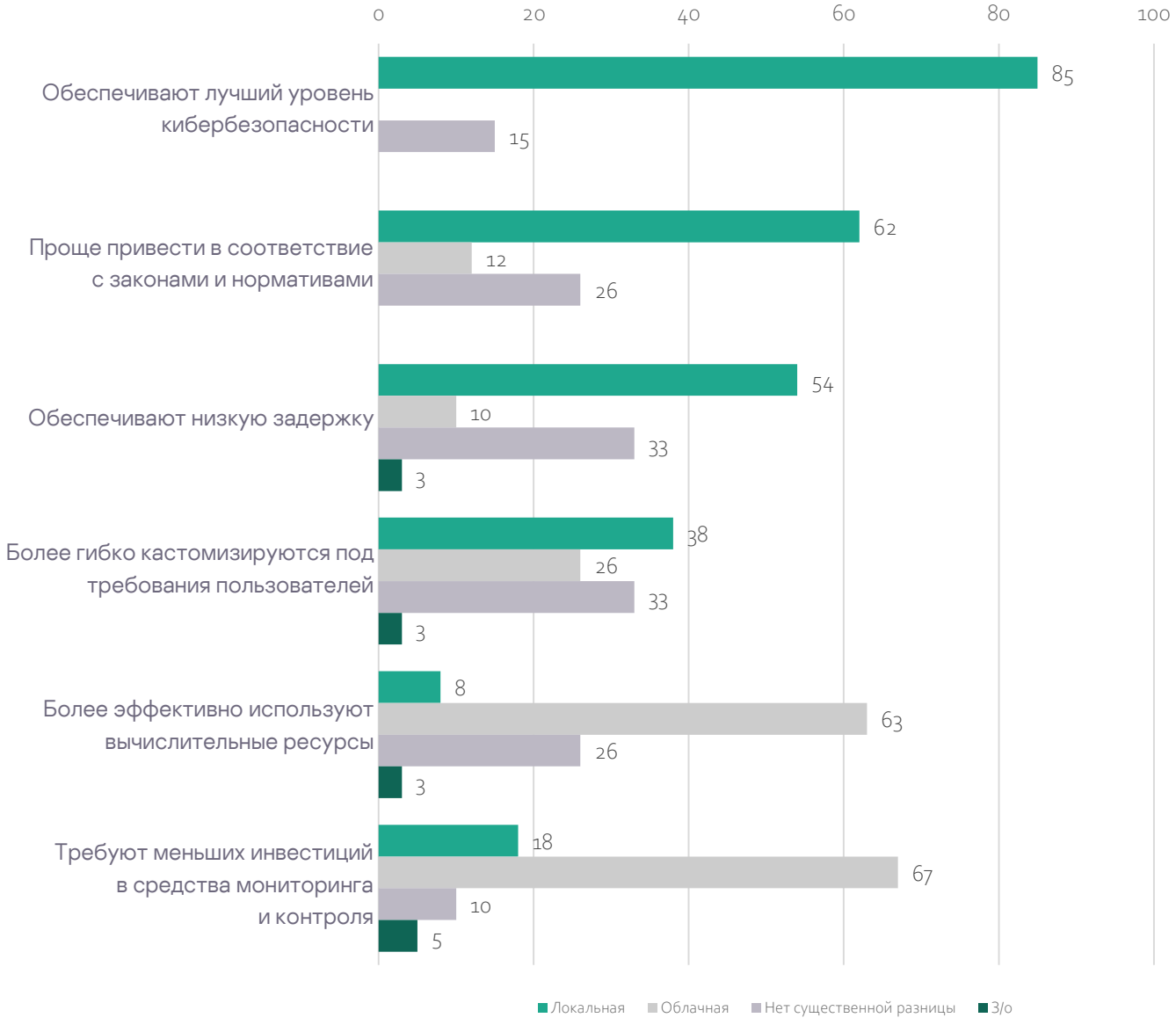
Исследование показало, что те респонденты, которые используют только локальную инфраструктуру (35,1%), отмечают ее существенные преимущества по таким параметрам как:

- Более высокий уровень кибербезопасности (85%);
- Простота приведения в соответствие с законами и нормативами (62%);
- Низкая задержка (54%);
- Гибкость кастомизации под требования пользователей (38%).

А облачная инфраструктура, по их мнению, имеет преимущество по следующим параметрам:

- Требование меньших инвестиций в средства мониторинга и контроля (67%);
- Более эффективное использование вычислительных ресурсов (63%).

Какая инфраструктура имеет существенное преимущество по следующим параметрам? (%)

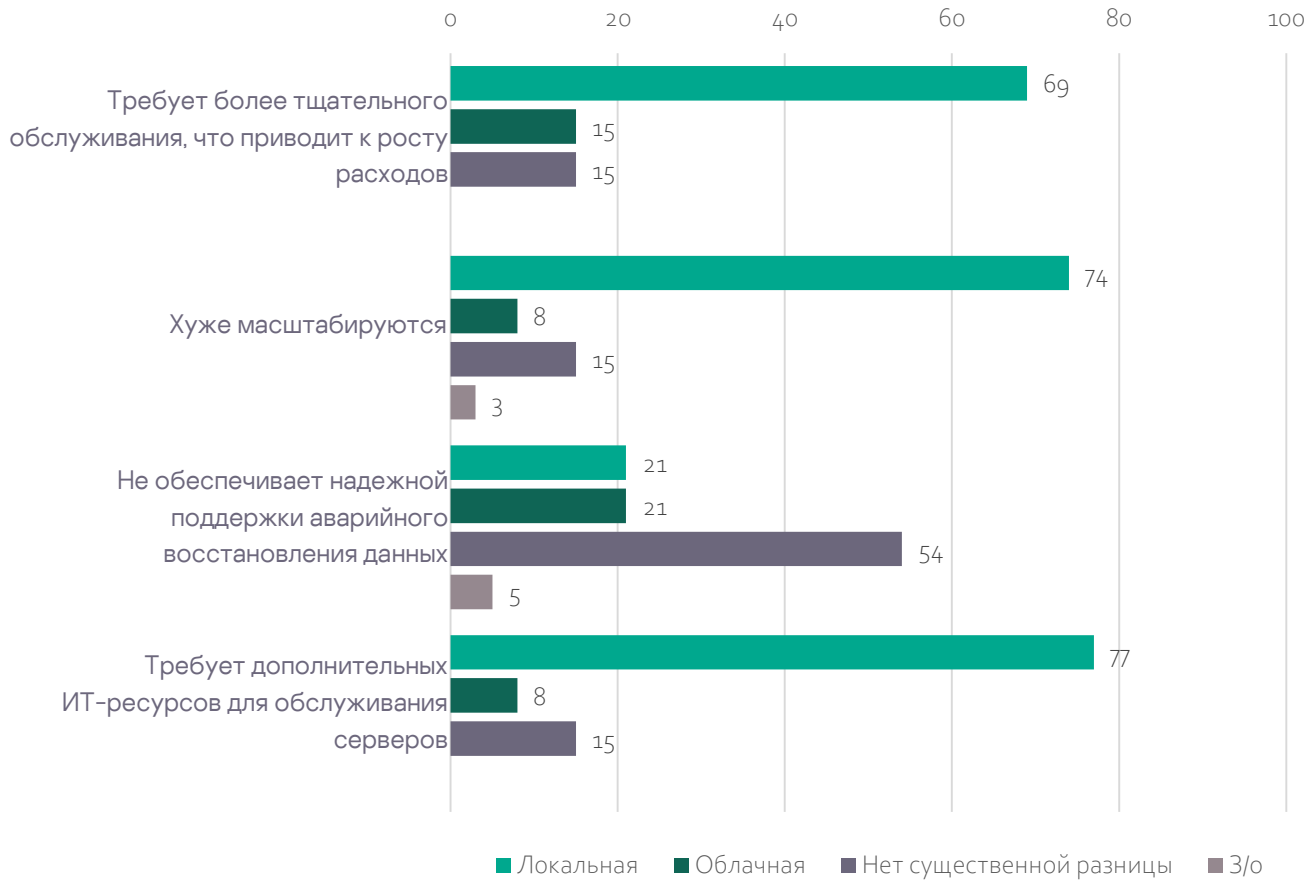


По мнению респондентов, не использующих облака (35,1%), локальная инфраструктура проигрывает облачной по следующим параметрам:

- Требует дополнительных ИТ-ресурсов для обслуживания серверов (77%);
- Хуже масштабируется (74%);
- Требует более тщательного обслуживания, что приводит к росту расходов (69%).

По такому параметру, как "Не обеспечивает надежной поддержки аварийного восстановления данных" больше половины (54%) отметили, что нет существенной разницы между инфраструктурами. Голоса оставшихся разделились примерно поровну между локальной и облачной инфраструктурой.

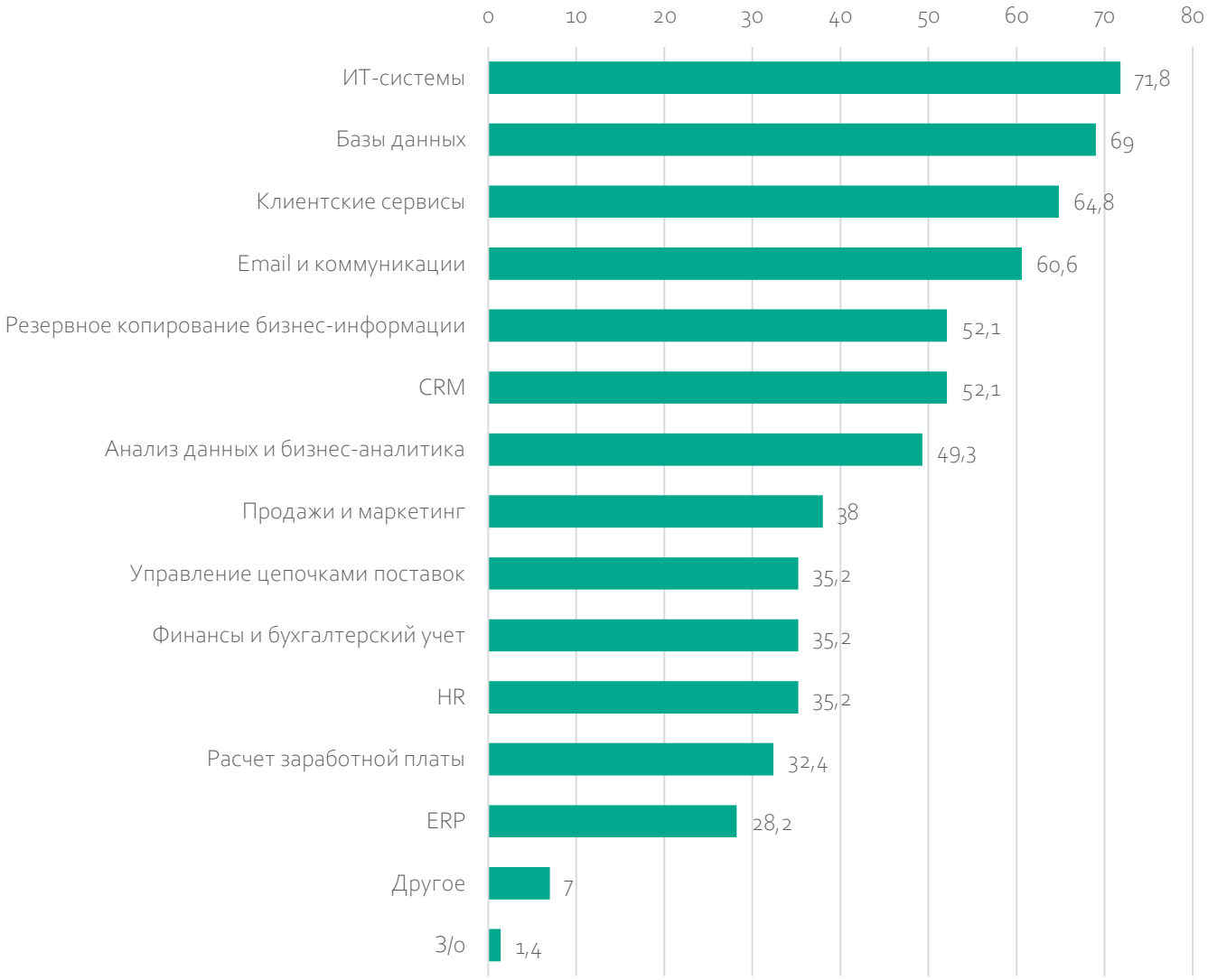
Какая инфраструктура существенно проигрывает по следующим параметрам? (%)



Компании, которые планируют перенести рабочую нагрузку в облако (5,1%), для укрепления защиты облачной среды в ближайшие 3 года будут использовать в основном следующие решения:

- Инструменты для выявления аномалий в конфигурациях контейнеров в режиме реального времени;
- Средства сканирования и обеспечения безопасности реестра контейнеров;
- Решения для отслеживания нарушений нормативных требований в режиме реального времени и передачи предупреждений отделу ИБ.

Какие сервисы или рабочие нагрузки перенесли или планируете перенести в облако? (%, возможен выбор нескольких вариантов)



Плюсы переноса баз данных в облачную среду очевидны: облачные хранение и вычисления позволяют сократить капитальные затраты на оборудование и поддержку локальной инфраструктуры, что особенно актуально для баз данных, которые требуют значительных ресурсов для хранения и обработки.

Заметно, что перенос менее критических систем, таких как CRM, анализ данных и продаж, осуществляется с меньшими темпами. В свою очередь, относительно низкие показатели для таких систем, как ERP (28,2%) и расчета заработной платы (32,4%), могут быть связаны с тем, что они системы считаются более чувствительными и требуют более тщательной настройки безопасности и контроля доступа.

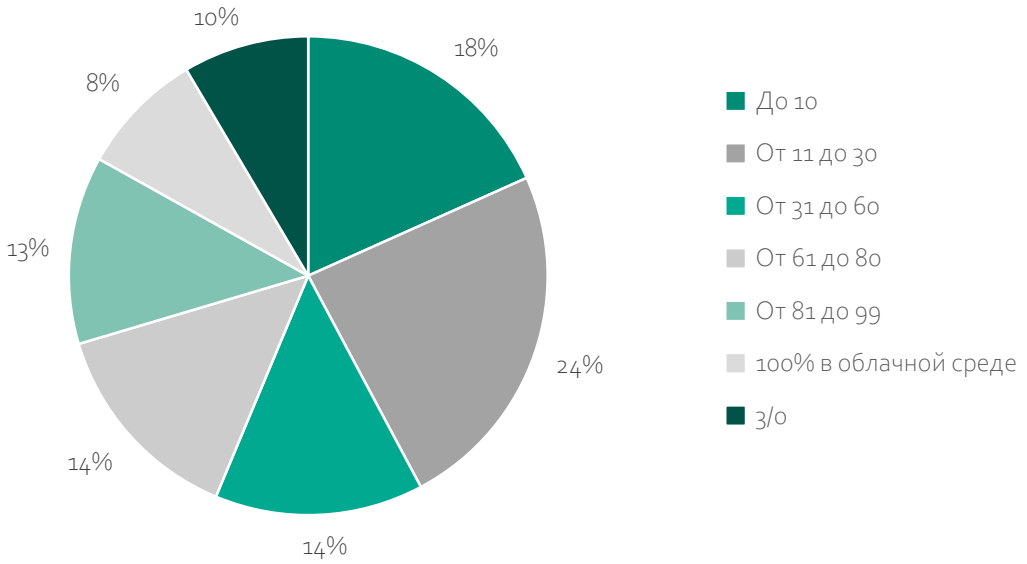
Общий тренд миграции ИТ-систем в облако подкрепляется явными преимуществами, которые облачные решения предоставляют по сравнению с традиционными локальными системами.

Мнение респондентов, использующих облака

У 42,2% компаний на облако приходится от 10% до 30% рабочей нагрузки, у 35% компаний на облако приходится от 60% до 100% рабочей нагрузки. Несмотря на растущую популярность облачных технологий, текущий уровень использования облачных решений все еще остается низким из-за множества факторов, включая низкую осведомленность, опасения по поводу безопасности, финансовые вопросы и существующие локальные решения. Для увеличения загрузки облаков компаниям необходимо создавать целостные стратегии по внедрению и осваивать преимущества миграции в облако. Это сложный затратный процесс, требующий не только написания самих стратегий, но и соответствующих организационных и культурных преобразований в компании. Для оптимизации процессов может понадобиться привлечь сторонних экспертов и провайдеров облачных услуг.

Владимир Золотов,
Директор по информационным технологиям АО «Гринатом»:
«*Российский рынок облачных сервисов находится в стадии активного развития, открывая перед собой новые перспективы. Адаптация к изменяющимся условиям и эффективное применение новейших технологий создают надежную основу для будущего роста и укрепления позиций отечественных провайдеров в области безопасности рабочих нагрузок в облаке. В последние годы мы можем наблюдать взрывной рост потребления таких сервисов, что ведет к увеличению потребности в обеспечении безопасности данных и приложений, работающих в облачных средах. Отсутствие крупных глобальных игроков создает уникальную возможность для развития отечественных облачных провайдеров, так как это способствует не только расширению их возможностей, но и стимулирует конкуренцию внутри страны. Еще одним ключевым фактором для ускоренного роста является наличие якорных заказчиков, готовых инвестировать в услуги российских провайдеров, что создает стабильный спрос и позволяет провайдерам усовершенствовать свои предложения, улучшая защиту от киберугроз и наращивая технологические компетенции. Защита облачных инфраструктур становится особенно актуальной в контексте импортозамещения и стремления к технологической независимости. Это подталкивает разработчиков к поиску своих собственных решений и технологий*».

Какой процент существующей рабочей нагрузки приходится на облачную среду? (%)



Среди компаний, использующих облачную ИТ-инфраструктуру (64%), популярно мнение, что существенным преимуществом локальной инфраструктуры является более высокий уровень кибербезопасности (49%).

Максим Осорин, директор X5 Облака:

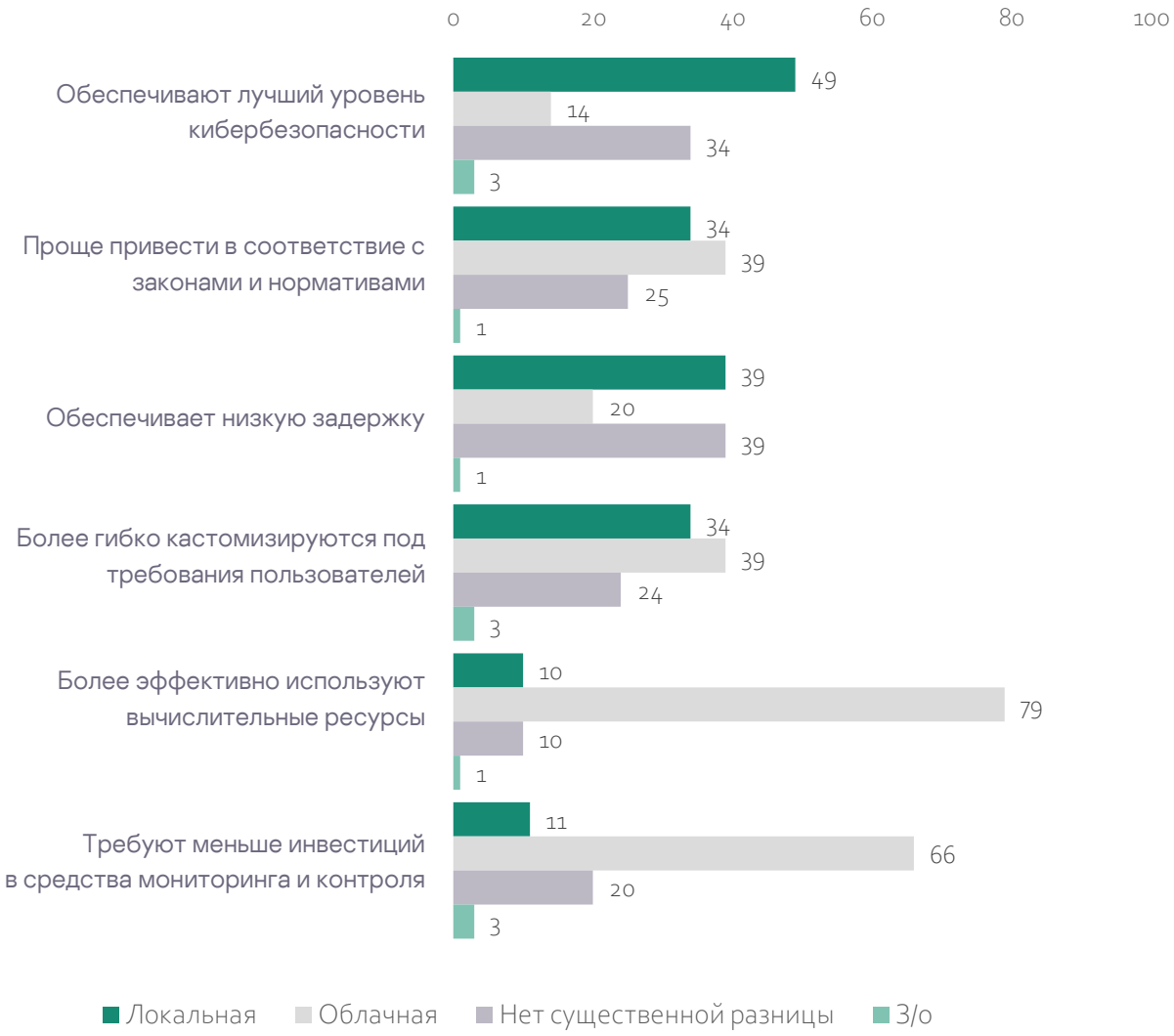
«*Современные частные облачные платформы предоставляют намного более высокий уровень безопасности пользовательских нагрузок по сравнению с традиционной ИТ-инфраструктурой предприятия*».

В свою очередь, существенными преимуществами облачной инфраструктуры её пользователи называют:

- Более эффективное использование вычислительных ресурсов (79%);
- Требование меньших инвестиций в средства мониторинга и контроля (66%);
- Простоту приведения в соответствие с законами и нормативами (39%);
- Гибкость кастомизации под требования пользователей (39%).

По такому параметру, как обеспечение низкой задержки, одинаково популярны ответы «преимущество у локальной инфраструктуры» и «существенной разницы между инфраструктурами нет» (по 39%).

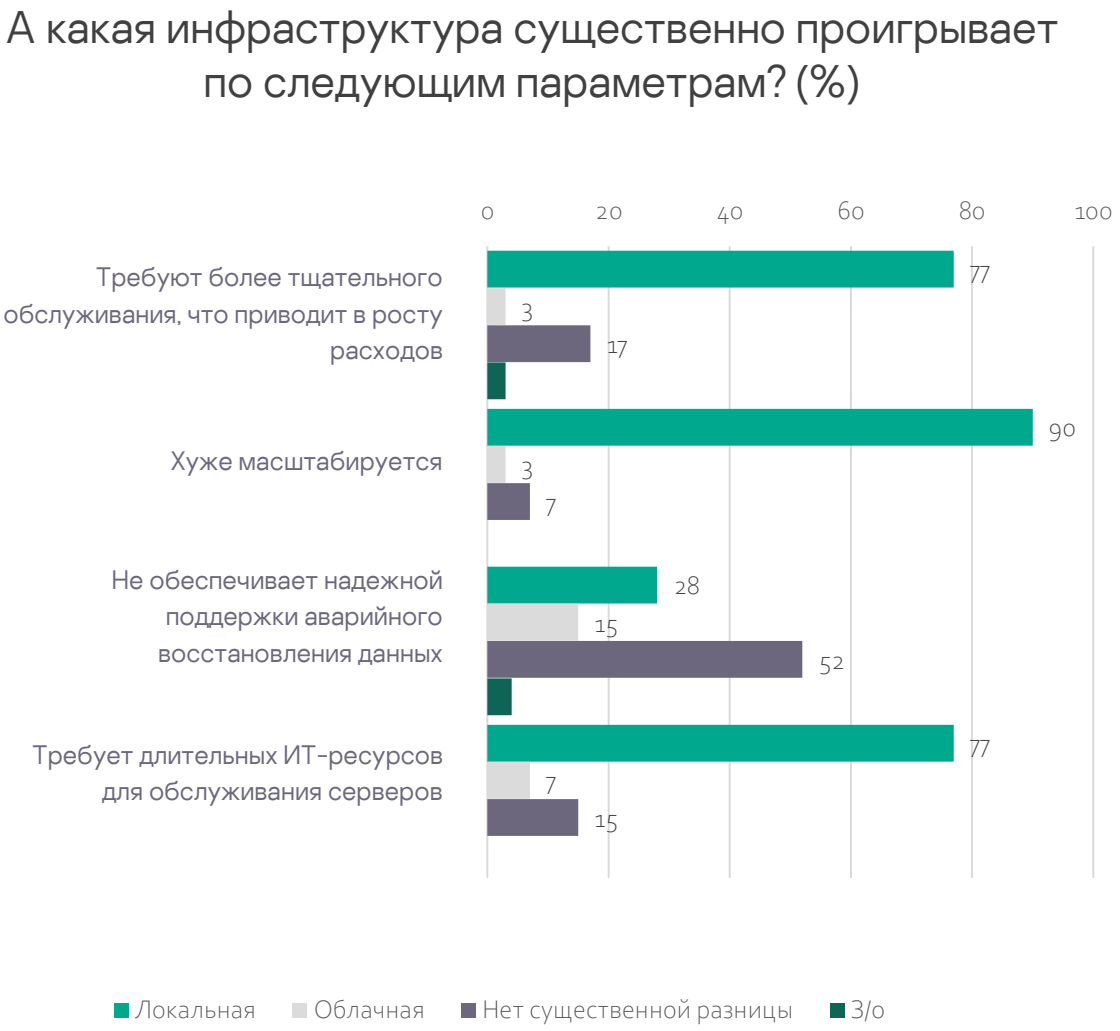
Какая инфраструктура имеет существенное преимущество по следующим параметрам? (%)



В вопросе о параметрах, по которым та или иная инфраструктура проигрывает, мнения тех, кто облака не использует и тех, кто использует, совпали. Локальная инфраструктура, как считают использующие облака респонденты, уступает по следующим параметрам:

- Хуже масштабируется (90%);
- Требует более тщательного обслуживания, что приводит к росту расходов (77%);
- Требует дополнительных ИТ-ресурсов для обслуживания серверов (77%).

По такому параметру, как "Не обеспечивает надежной поддержки аварийного восстановления данных" респонденты считают, что существенной разницы в инфраструктурах нет, причем в этом с ними согласны и те, кто облака не используют: в обоих категориях этот вариант набрал более 50% голосов. Однако 28% пользователей облаков все же считают, что локальная инфраструктура справляется с этим хуже.

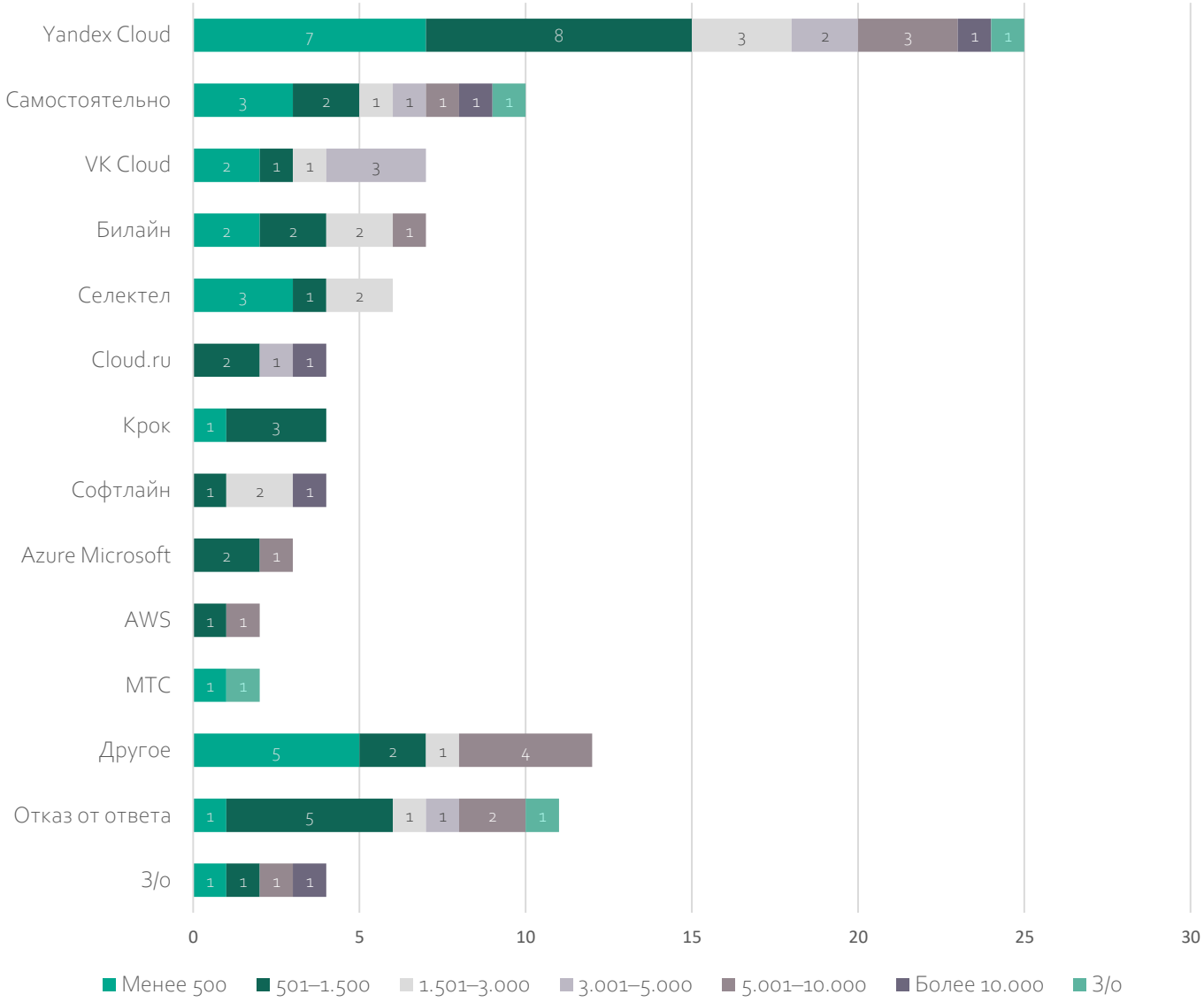


Самым популярным поставщиком, с которым респонденты, использующие облака, сотрудничают при переносе текущей рабочей нагрузки в публичное облако, является Yandex Cloud (25%). Часто обращаются к VK Cloud и Билайн (по 7% соответственно). 10% переносят рабочую нагрузку самостоятельно. Еще 6% обращаются к Селектел, по 4% соответственно к таким поставщикам, как Cloud.ru, Крок, Софтлайн.

Несмотря на геополитические риски, с Azure Microsoft продолжают сотрудничать 3%, с AWS – 2%. Доля последней на рынке такая же, как у МТС.

В категорию «Другое» вошли такие поставщики, как EdgeЦентр, Huawei Cloud, Инфосистемы Джет, Nubes, Майнд Софт, VMware, Айстек, Google Cloud Platform, ОНТС (NextCloud), Ростелеком, M1 клауд, ОБИТ, Облако ВТБ, Timeweb Cloud.

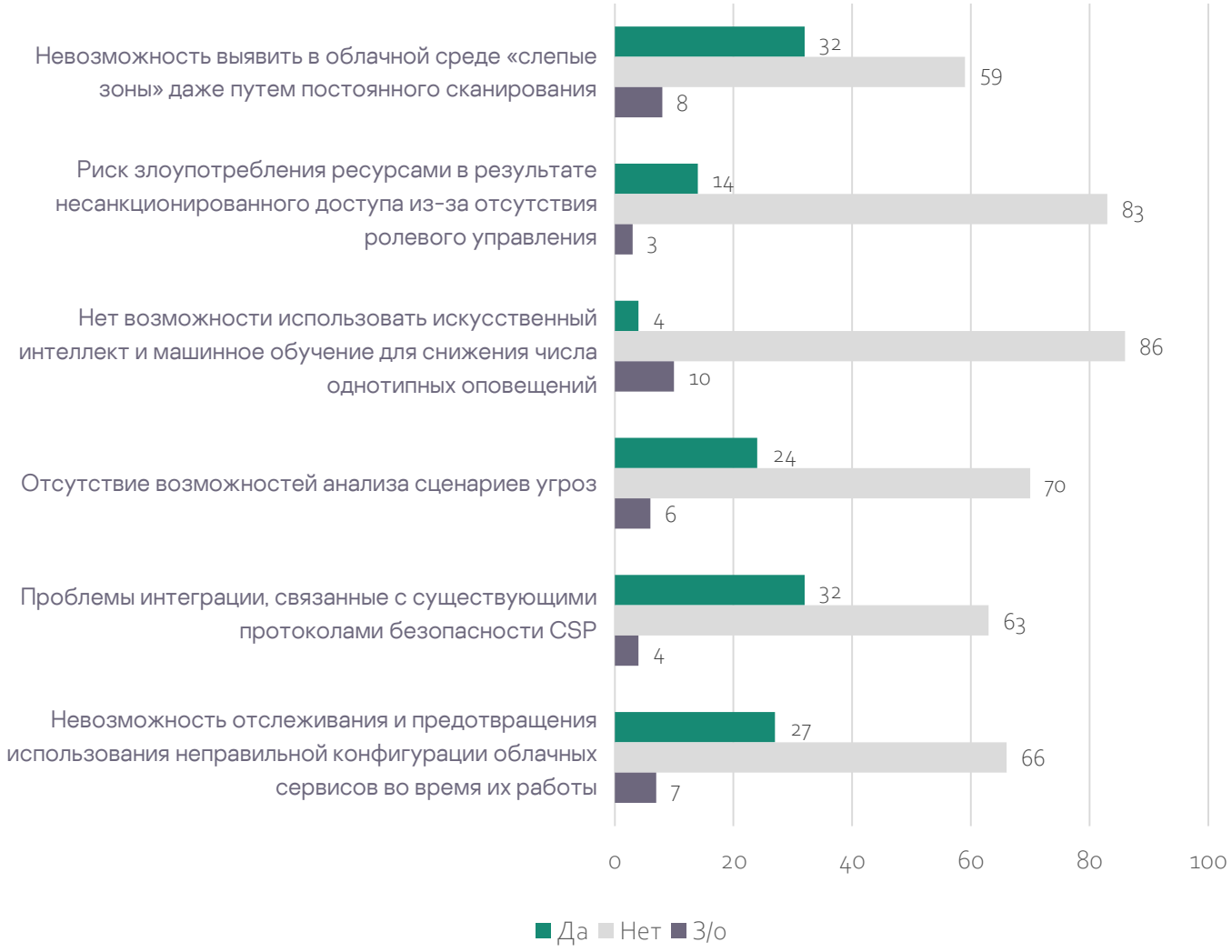
Соотношение размера компаний-респондентов и поставщиков, с которыми сотрудничают при переносе текущей рабочей нагрузки в публичное облако (%)



Подавляющее большинство использующих “облака” компаний (64%) не сталкиваются с проблемами в обеспечении информационной безопасности. Однако ряд проблем все же присутствует:

- Невозможность выявить в облачной среде «слепые зоны» даже путем постоянного сканирования (32%);
- Проблемы интеграции, связанные с существующими протоколами безопасности CSP (32%);
- Невозможность отслеживания и предотвращения использования неправильной конфигурации облачных сервисов во время их работы (27%);
- Отсутствие возможностей анализа сценариев угроз (24%).

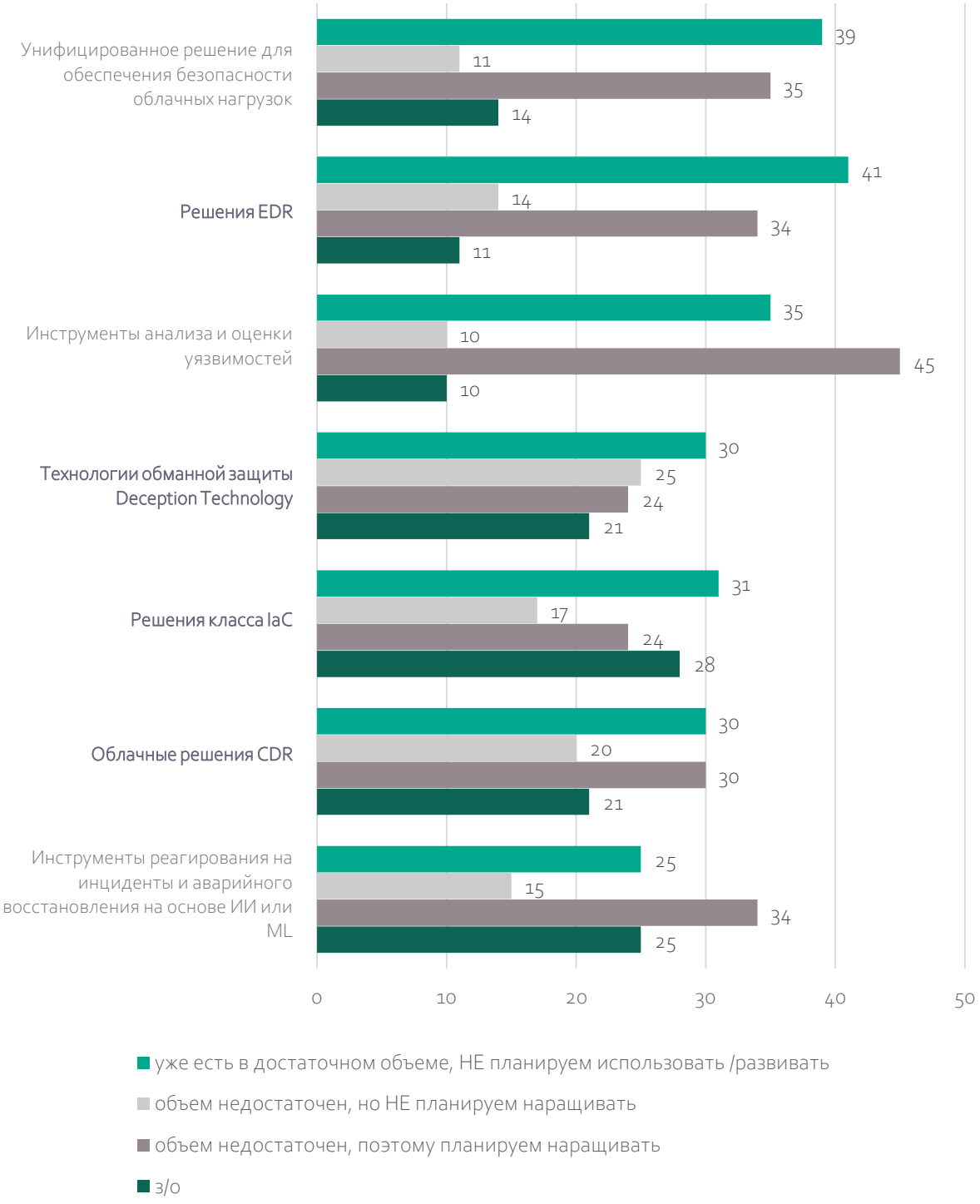
При использовании существующих решений по обеспечению безопасности на облачной платформе сталкиваетесь ли со следующими проблемами? (%)



Говоря о планах по внедрению и использованию решений в области облачной безопасности, те, кто уже использует облачную ИТ-инфраструктуру (64%), отметили недостаточный объем следующих решений:

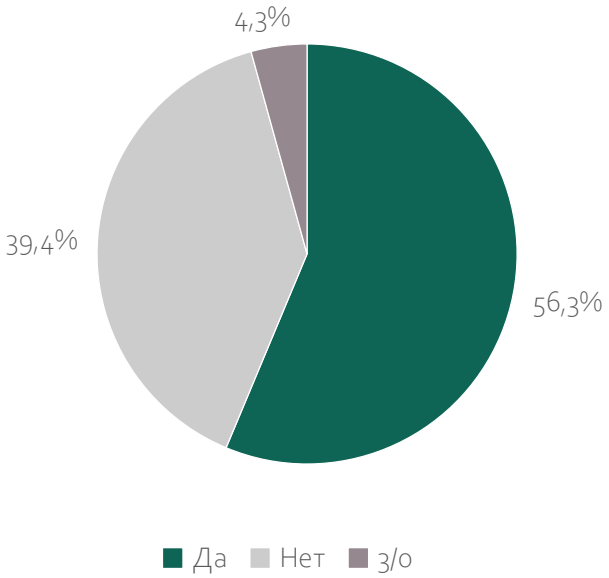
- Инструменты анализа и оценки уязвимостей (55%);
- Облачные решения CDR (50%);
- Технологии обманной защиты Deception Technology (49%);
- Инструменты реагирования на инциденты и аварийного восстановления на основе ИИ или ML (49%);
- Решения EDR (48%);
- Унифицированное решение для обеспечения безопасности облачных нагрузок (46%);
- Решения класса IaC (41%).

Планируете ли использовать или развивать следующие решения в области облачной безопасности в ближайшие 3 года? (%)

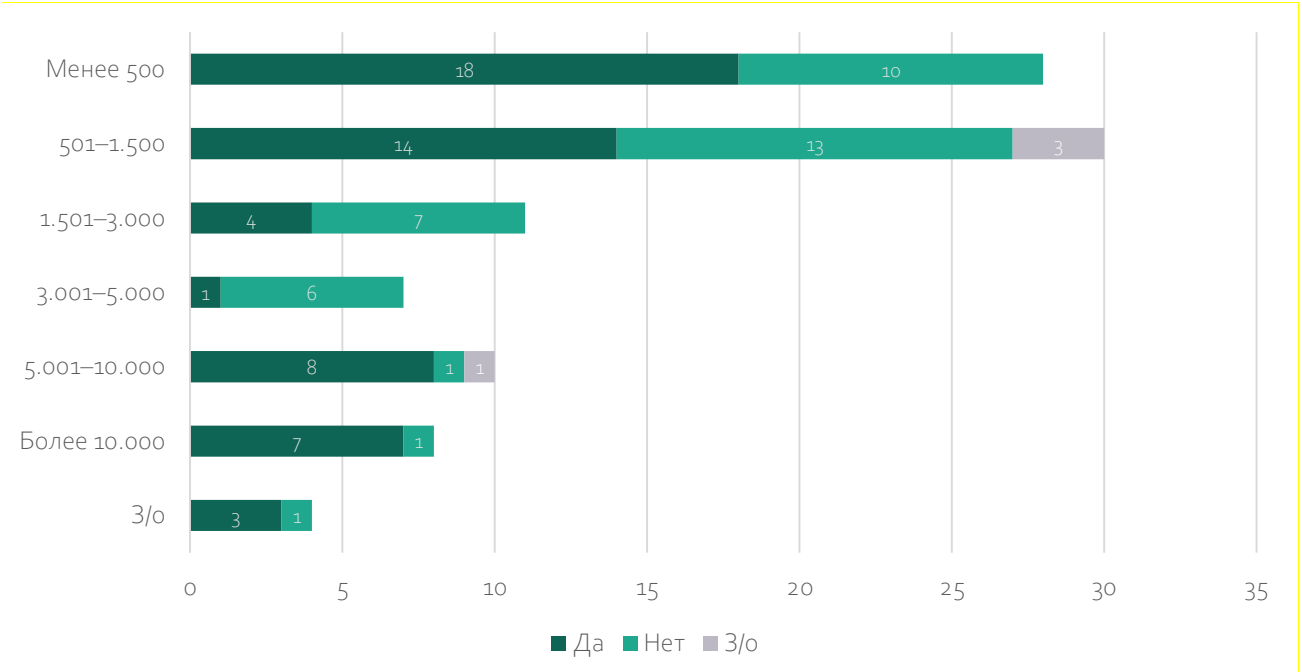


Более половины (56,3%) компаний используют облачную ИТ-инфраструктуру или облачные технологии для создания и развертывания приложений в облаке. 39,4% обходятся в разработке без "облаков", остальные 4,2% затруднились ответить. Компании среднего размера в основном не используют облачные технологии для разработки и развертывания приложений.

Используете ли технологии для создания и развертывания приложений в облаке? (%)

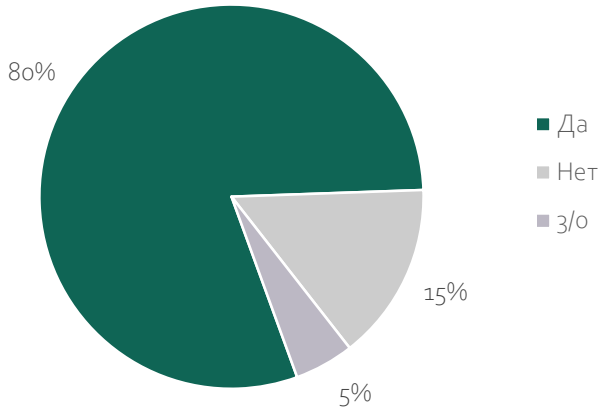


Соотношение размера компании и данных об использовании технологий для создания и развертывания приложений в облаке (%)



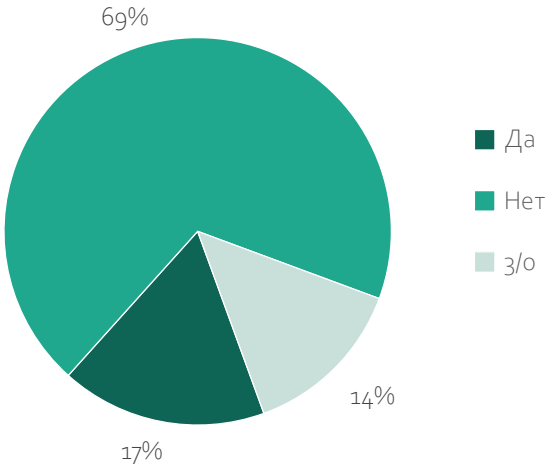
80% планируют расширять применение облачных технологий для создания и развертывания приложений в облаке в перспективе ближайших трех лет.

Планируете ли расширять использование технологий для создания и развертывания приложений в облаке в ближайшие 3 года? (%)



39,4% отметили, что не используют технологии для создания и развертывания приложений в облаке, из них у 69% нет этого в планах на ближайшие три года. Лишь 17,2% планирует использовать облачные технологии для создания приложений, еще 13,8% затруднились ответить.

Планируете ли в ближайшие 3 года применять технологии для создания и развертывания приложений в облаке? (%)



В ближайшие три года большинство из тех, кто планирует расширять (80%) и применять (17,2%) технологии для создания и развертывания приложений в облаке, для укрепления облачной среды планирует внедрять все перечисленные ниже решения.

Для укрепления защиты облачной среды планируете ли в ближайшие три года использовать/ расширять решения? (%)

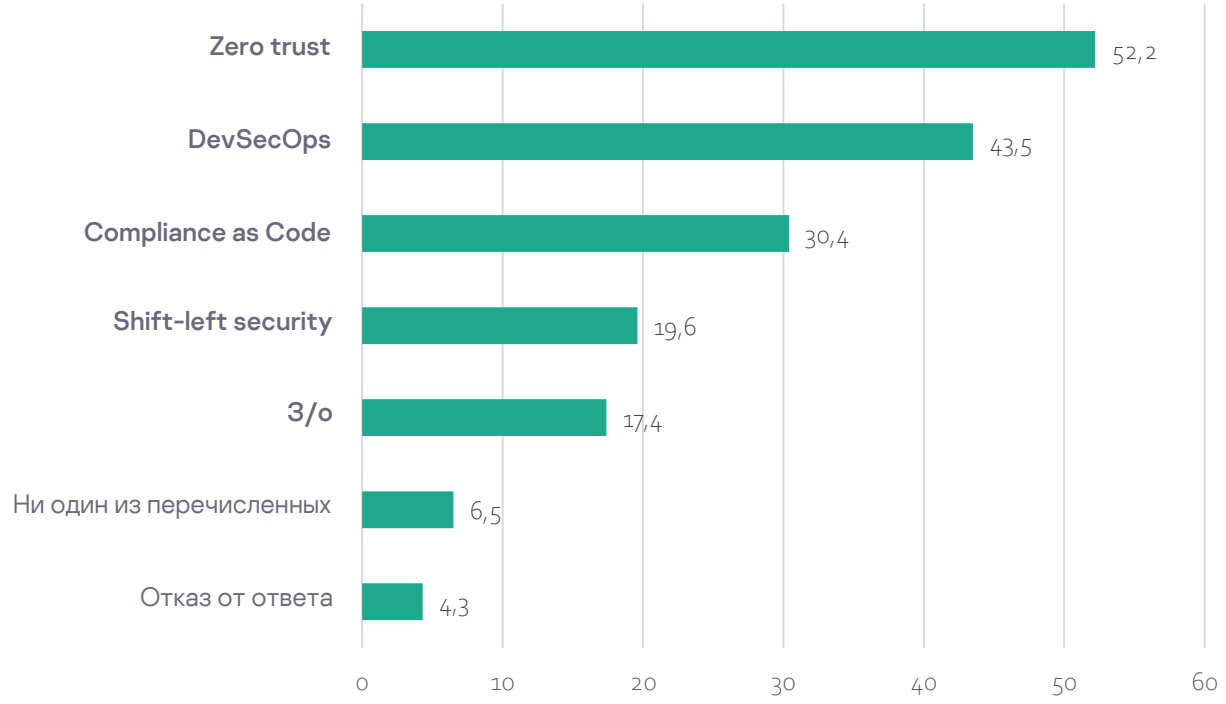
Среди подходов, которые применяются в ИБ-стратегии приложений в организации, чаще всего упоминали Zero trust (52,2%) и 43,5% - DevSecOps. Для создания качественного программного обеспечения важно продумывать безопасность, начиная с самых ранних стадий. От этого зависит стабильность его работы в будущем и доверие потребителей.

Использование методологий безопасной разработки, таких как DevSecOps, уже стало стандартом. Они помогают сделать процесс разработки более эффективным, сократить время вывода новых приложений и функций на рынок, несмотря на усложнение этих

приложений для имплементации в облако, что повышает требования к масштабированию и более высоким нагрузкам. Поэтому этим нельзя пренебрегать. Обеспечить защиту помогают специализированные решения для сред разработки.

Современные инструменты позволяют бесшовно встроить безопасность в процесс разработки, например, как это реализовано в решении Kaspersky Cloud Workload Security. Благодаря удобному интерфейсу, а также синхронизации, автоматизации, возможности проверок в рантайме разработчики могут комфортно работать в любых средах и обеспечивать безопасность своего приложения, не тратя на это лишнее время и ресурсы. Также мы рекомендуем внедрять концептуальные подходы к обеспечению безопасности, такие как Zero Trust ("нулевое доверие"). Его суть в том, что ни одному пользователю или устройству по умолчанию нельзя доверять. При таком подходе компании должны строго ограничивать и контролировать права доступа, использовать надёжные механизмы аутентификации, а также сегментировать сеть, чтобы снизить риски», — комментирует Дмитрий Шмойлов, руководитель отдела безопасности программного обеспечения "Лаборатории Касперского".

Какие подходы применяются в ИБ-стратегии приложений в организации? (%)



Для защиты облачной инфраструктуры чаще всего используется встроенная защита провайдера облака (73,9%), защита виртуализации (63%), решение для защиты конечных устройств или EPP-платформа (54,3%). Только половина респондентов использует технологию EDR и защиту контейнеров (50%). Реже упоминались сервисы MDR (37%), защита, предоставляемая MSSP (34,8%), защита бессерверных вычислений (26,1%).

Михаил Тутаев, директор по продуктам МТС Web Services:

«*Облако позволяет компаниям сэкономить время на размещении заказов на оборудование, его логистику и монтаж, а значит ускорить запуск новых проектов. Виртуальная инфраструктура поднимается за минуты, есть возможность увеличивать или уменьшать ее объем в зависимости от потребности и более гибко управлять своими тратами в целом. Это означает, что если предприятие использует меньше вычислительных мощностей, чем рассчитывало, то его серверы не простаивают, а если — больше, нет необходимости ждать новых поставок.*

Информационную безопасность в облаке можно условно разделить на две большие составляющие: безопасность облачной инфраструктуры и безопасность клиентских информационных систем. За первую всегда отвечает провайдер, за вторую – клиенты. <…>

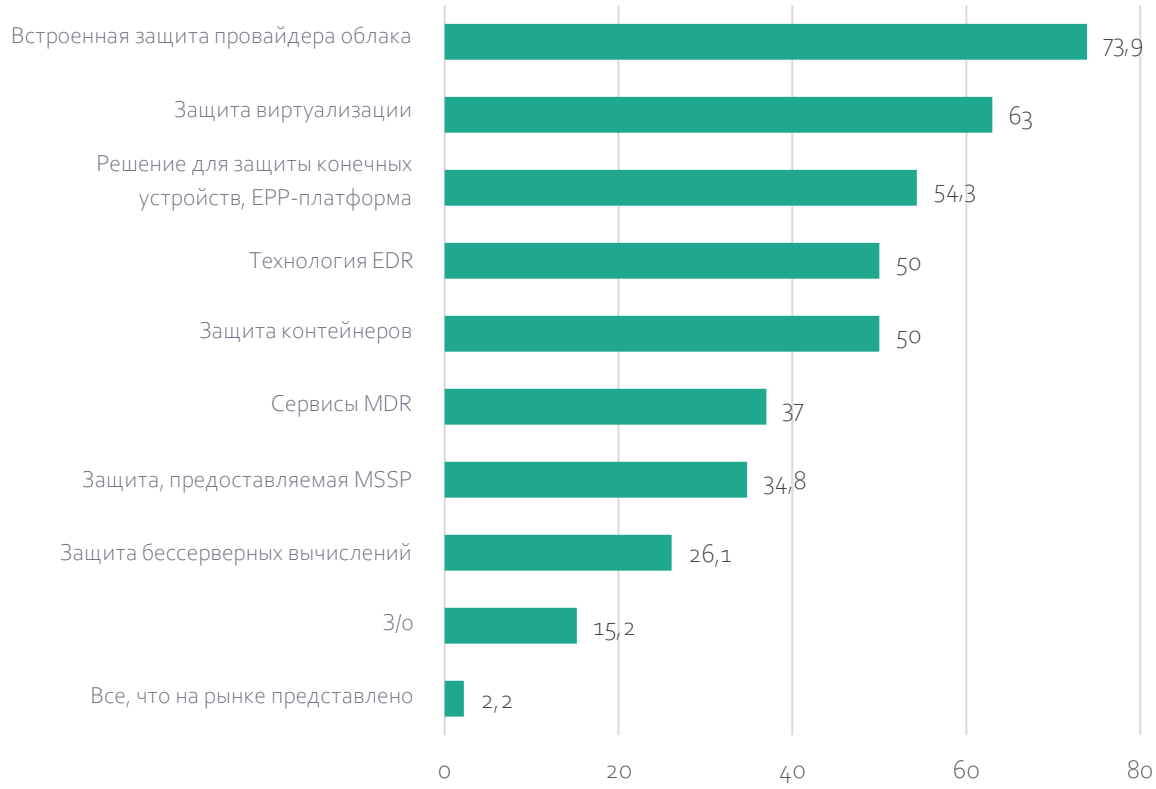
Что касается безопасности клиентских информационных систем, мы осознаем дефицит специалистов по информационной безопасности на рынке, поэтому предлагаем клиентам забрать на себя часть задач по обеспечению ИБ.

В среднем рынок облаков в России (IaaS, PaaS и SaaS) растёт более чем на 20% в год. В 2023 году он превысил 200 млрд рублей.

Мы прогнозируем еще больший рост рынка облаков в России за счет увеличения спроса на обучение искусственного интеллекта в виртуальной инфраструктуре и граничные вычисления (EDGE-ЦОДы), а также за счет увеличения доли затрат на облака в ИТ-бюджетах российский компаний.

Чаще всего среди облачных сервисов российские компании пользуются виртуальной инфраструктурой, резервным копированием, объектным хранилищем для размещения данных в облаке и виртуальными рабочими местами». <…>

Какие решения используете для защиты облачной инфраструктуры? (%)



Ожидания клиентов от поставщиков услуг облачных технологий

Принятие облачных технологий как безопасной среды

Потребность в расширении сервисной модели и увеличении числа предоставляемых SaaS-услуг говорит о том, что организации хотят сосредоточиться на бизнес-процессах и снизить операционные затраты. Однако для более широкого принятия облачных технологий поставщикам облачных услуг необходимо совершенствовать свои предложения – как в плане ценовой политики, так и функциональных возможностей, поддержки.

Провайдерам необходимо учитывать различные аспекты для более широкого принятия облачных технологий. Сбор мнений пользователей об облачных ИТ-услугах показывает, что облачные провайдеры должны учитывать множественные аспекты, такие как доступность сервисов, стоимость, безопасность и качество поддержки. Улучшение этих областей может значительно повысить удовлетворенность клиентов и привести к более широкому внедрению облачных решений. Учитывая текущие тенденции и потребности компаний, облачные провайдеры должны расширять свои предложения, оптимизировать процессы и разрабатывать стратегии, ориентированные на конкретные сегменты рынка.

Провайдерам следует бороться с предубеждениями, касающимися облачных технологий. Мнения респондентов, не использующих облачную ИТ-инфраструктуру, подчеркивают необходимость более активной работы облачных провайдеров в области информирования и обучения потенциальных пользователей, а также в создании более гибких, безопасных и адаптируемых решений.

Качество документации

Респонденты, использующие облачную ИТ-инфраструктуру, подчеркивают важность более тщательного документирования архитектуры облачных решений и процессов взаимодействия с ними. Прозрачность и понимание архитектуры облака помогают пользователям более эффективно управлять своими ресурсами, а также минимизировать риски, связанные с ошибками в настройках и неэффективными процессами.

Требования к функциональным возможностям и интеграциям

Нужны более совершенные системы управления идентификацией и доступом (IAM). Эффективность систем управления идентификацией и доступом выходят на первый план в свете возрастания угроз безопасности и необходимости соблюдения нормативных требований. Надежные механизмы IAM помогают компаниям лучше контролировать доступ к ресурсам и снижать риски, связанные с утечкой данных.

Необходим более совершенный механизм перемещения виртуальных серверов. В последние годы большое количество компаний сталкивается с проблемами при перемещении своих виртуальных серверов между облачными провайдерами. Запрос на возможность экспорта виртуальных машин в другие системы виртуализации подчеркивает необходимость в более открытых и интегрируемых облачных решениях.

Ориентация на отечественного клиента. Поддержка отечественных облачных решений, которые могут использоваться для импортозамещения, находят отклик у респондентов. Сейчас как никогда высока потребность в решениях, адаптированных для специфических рыночных условий России.

Решение для защиты облачной ИТ-инфраструктуры

На сегодняшний день возникла необходимость в решении, которое оптимально подходит не только для компаний с разнородной и сложной ИТ-инфраструктурой, но и любому бизнесу, которому нужно улучшить защиту гибридного облака и обеспечить безопасность разработки.

В ответ на стремительное распространение облачных и контейнерных технологий в компаниях разного уровня в России и в мире «Лаборатория Касперского» представила решение Kaspersky Cloud Workload Security (CWS). Используя глобальные данные анализа угроз в реальном времени и алгоритмы ML, Kaspersky CWS защищает рабочие нагрузки на хостах, виртуальных машинах и контейнерах, независимо от того, какая облачная инфраструктура используется – частная, публичная или гибридная. Kaspersky CWS снижает риски, сопутствующие переходу в облака, и высвобождает ресурсы службы информационной безопасности.

Решение Kaspersky Cloud Workload Security состоит из Kaspersky Security для виртуальных и облачных сред (для защиты гибридной инфраструктуры) и Kaspersky Container Security (для защиты контейнерных сред). За счет этого оно позволяет защитить инфраструктуру от самого широкого спектра кибератак: вредоносного ПО, фишинга, контейнеров с наличием уязвимостей в среде исполнения и других, а также сокращает затраты на эксплуатацию и управление инфраструктурой и упрощает ее развертывание.

ОСНОВНЫЕ ВЫВОДЫ

Принятие облачных технологий

Облачные технологии вызывают все больше доверия и становятся все более популярными в бизнес-среде: в той или иной степени их используют уже 64% компаний. Ключевыми преимуществами облачной инфраструктуры её пользователи называют:

- Более эффективное использование вычислительных ресурсов.
- Более низкие расходы на средства мониторинга и контроля.
- Простоту приведения в соответствие с законами и нормативами.
- Гибкость кастомизации под требования пользователей.

Среди компаний, не мигрировавших в облака, популярно мнение, что важнейшим преимуществом локальной инфраструктуры является более высокий уровень кибербезопасности — так считают в 85% компаний. Такое мнение участников исследования может говорить о предубеждениях, связанных с облачной безопасностью, но облака могут быть безопасными при правильной системе защиты.

Сценарии использования облачных технологий

Наиболее активно в облака переносятся следующие системы и бизнес-процессы:

- ИТ-системы (72% компаний),
- Базы данных (69%),
- Клиентские сервисы (65%),
- Электронная почта и коммуникационные платформы (61%).

Разрабатывают и развертывают приложения в облачной среде уже более 56% компаний, причем 80% из них планируют расширять применение облачных технологий в разработке ПО в течение ближайших трех лет.

Обеспечение безопасности облачных нагрузок

Наиболее популярные подходы к обеспечению безопасности облачной инфраструктуры:

- Zero Trust (52% компаний),
- DevSecOps (43,5%).

Наиболее популярные инструменты киберзащиты облачных нагрузок:

- Встроенные средства защиты провайдеров облачных решений (74%),
- Защита виртуализации (63%),
- EPP-платформы — решения для защиты конечных устройств (54,3%).

Тренды и перспективы рынка облачных технологий

- Несмотря на очевидные преимущества облачных решений, такие как эффективность использования ресурсов и минимизация инвестиций, потребность в безопасности и контроле остается высоким приоритетом для организаций. Значительная часть компаний по-прежнему убеждена, что локальная инфраструктура выигрывает у облачной в безопасности. Поэтому в условиях растущей конкуренции ключевым преимуществом облачных провайдеров станет способность предлагать не только эффективные и надежные, но и безопасные решения, — а также способность донести до клиента, что "облака" не уступают традиционной инфраструктуре в плане защищенности от киберугроз.
- Среди пользователей облачных платформ высок запрос на автоматизацию и внедрение новейших технологий кибербезопасности на основе ИИ и ML, а также инструменты анализа уязвимостей и реакции на инциденты. В них чаще всего готовы инвестировать компании: в решения на основе ИИ планируют вкладываться 34% респондентов, в инструменты анализа и оценки уязвимостей — 45%.
- Облачные технологии для разработки и развертывания приложений будут расти в популярности. ИБ-стратегии компании, касающиеся разработки приложений, показывают, что компании хорошо осведомлены об интегрированном подходе к безопасности в разработке и управлении облачными ресурсами и ожидают реализации этого подхода в новых ИБ-продуктах.

Kaspersky Cloud Workload Security

Узнать больше

Возьмите курс на облачную безопасность

Специализированная защита облачных инфраструктур для устойчивого полета вашего бизнеса

CNews Analytics

CNews Analytics (CNA) — аналитическое агентство, специализирующееся на исследованиях в области информационных технологий и телекоммуникаций.

Деятельность агентства сосредоточена на следующих направлениях:

- Проведение заказных исследований рынков ИТ и телекоммуникаций, включающих анализ первичной и вторичной информации, интервью с представителями отрасли ИКТ, массовые опросы потребителей и иные процедуры, необходимые для получения исчерпывающей информации о рынке;
- Предоставление консалтинговых услуг в области маркетингового стратегического планирования в сфере ИКТ;
- Проведение инициативных исследований рынков ИТ и телекоммуникаций;
- Подготовка рейтингов компаний, работающих на рынках ИТ и телекоммуникаций;
- Подготовка открытых обзоров рынков ИТ и телекоммуникаций, включающих статистическую и аналитическую информацию, мнения экспертов и комментарии ведущих игроков рынка ИКТ. Обзоры публикуются в открытом доступе на сайте CNews. Аудитория обзоров CNews Analytics превышает 100 тыс. уникальных читателей.