Сложность ИТ и атаки вирусов шифровальщиков

Количественный отчет по результатам всемирного опроса руководителей в сфере ИТ

VERITAS

Оглавление

VERITAS

Методология исследования

Организация **Wakefield Research** провела **в конце сентября 2020 г.** количественное исследование среди 2690 ИТ-руководителей высшего звена в компаниях с более чем 1000 сотрудников, расположенных в 21 стране мира. Опрос проводился в формате онлайн после приглашения по электронной почте.

Северная Америка

150 участников

– США

Европа, Ближний Восток и Африка

1,640 участников

– Бенилюкс
– Великобритания
– Венгрия
– Германия
– Испания
– Италия
– ОАЭ
– Польша
– Россия
– Саудовская Аравия
– Турция
– Франция
– Швеция
– ЮАР

Азиатско-Тихоокеанский регион

900 участников

– Австралия
– Индия
– Китай
– Сингапур
– Южная Корея
– Япония

Основные выводы

Миграция в облака повышает сложность ИТ-инфраструктур

Российские компании активно переходят в облачную среду, что усложняет ИТ-инфраструктуры

63% российских компаний хранят в облаке все данные и приложения или их часть

35% компаний выбрали стратегию гибридного мультиоблака

11 **облачных сервисов** использует средняя российская компания, что немного меньше общемирового показателя

Недостаточная отказоустойчивость дорого обходится российским компаниям

62% высокопоставленных представителей ИТ-отрасли отметили, что средства безопасности не поспевают за темпами развития облаков

43% компаний сталкивались с атаками шифровальщиков, в среднем на компанию приходится 5 атак

35% российских компаний признались, что заплатили вымогателям выкуп, целиком или частично

Только 15% компаний используют стратегию 3-2-1 для резервного копирования и восстановления

71% компаний будут вынуждены потратить **более 5 дней** на восстановление после атаки

17% данных, потерянных компанией, не удастся восстановить

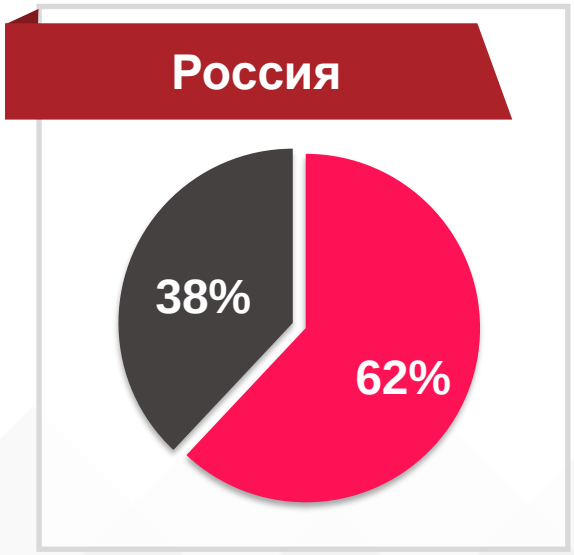
VERITAS

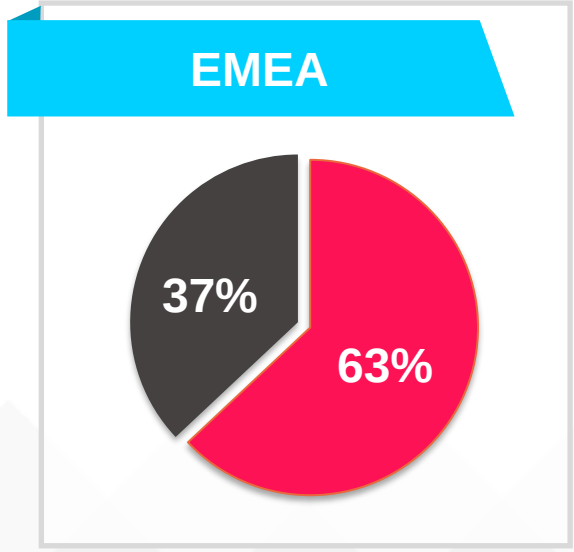
Подробные результаты исследования

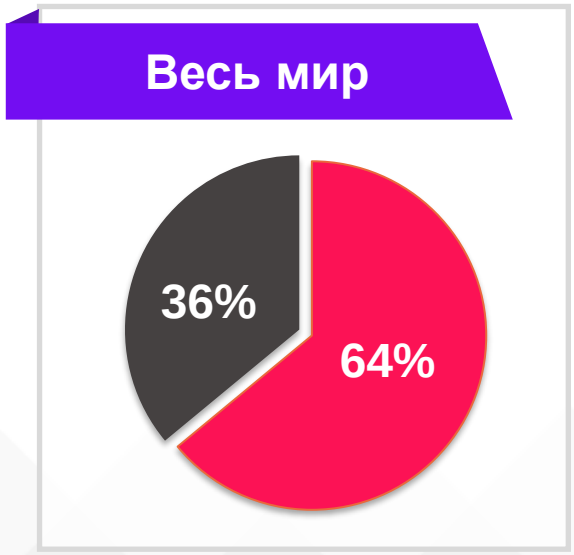
VERITAS

Высокая степень уязвимости: безопасность «отстает» от инфраструктуры

Большинство российских ИТ-руководителей высшего звена (62%) **отмечают, что применяемые ими средства информационной безопасности не успевают за развитием ИТ-инфраструктуры**, оставляя компанию без адекватной защиты от угроз.







Безопасность отстает

Безопасность развивается в том же темпе

Основные проблемы, сопутствующие чрезмерной сложности ИТ-инфраструктуры

Россия

Доступ сотрудников к файлам
42%

Внешние атаки
38%

Утечка данных
36%

EMEA

Внешние атаки
37%

Внутренние атаки
36%

Утечка данных
35%

Весь мир

Внешние атаки
37%

Внутренние атаки
35%

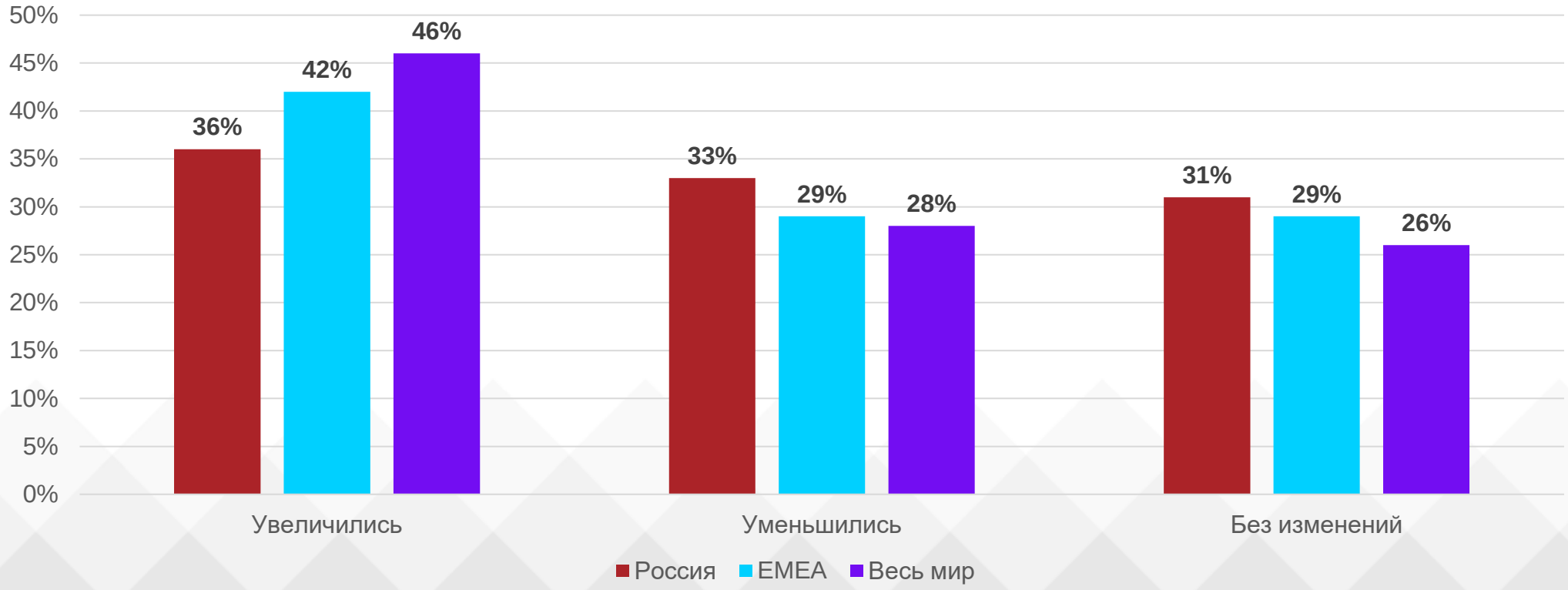
Утечка данных
32%

VERITAS

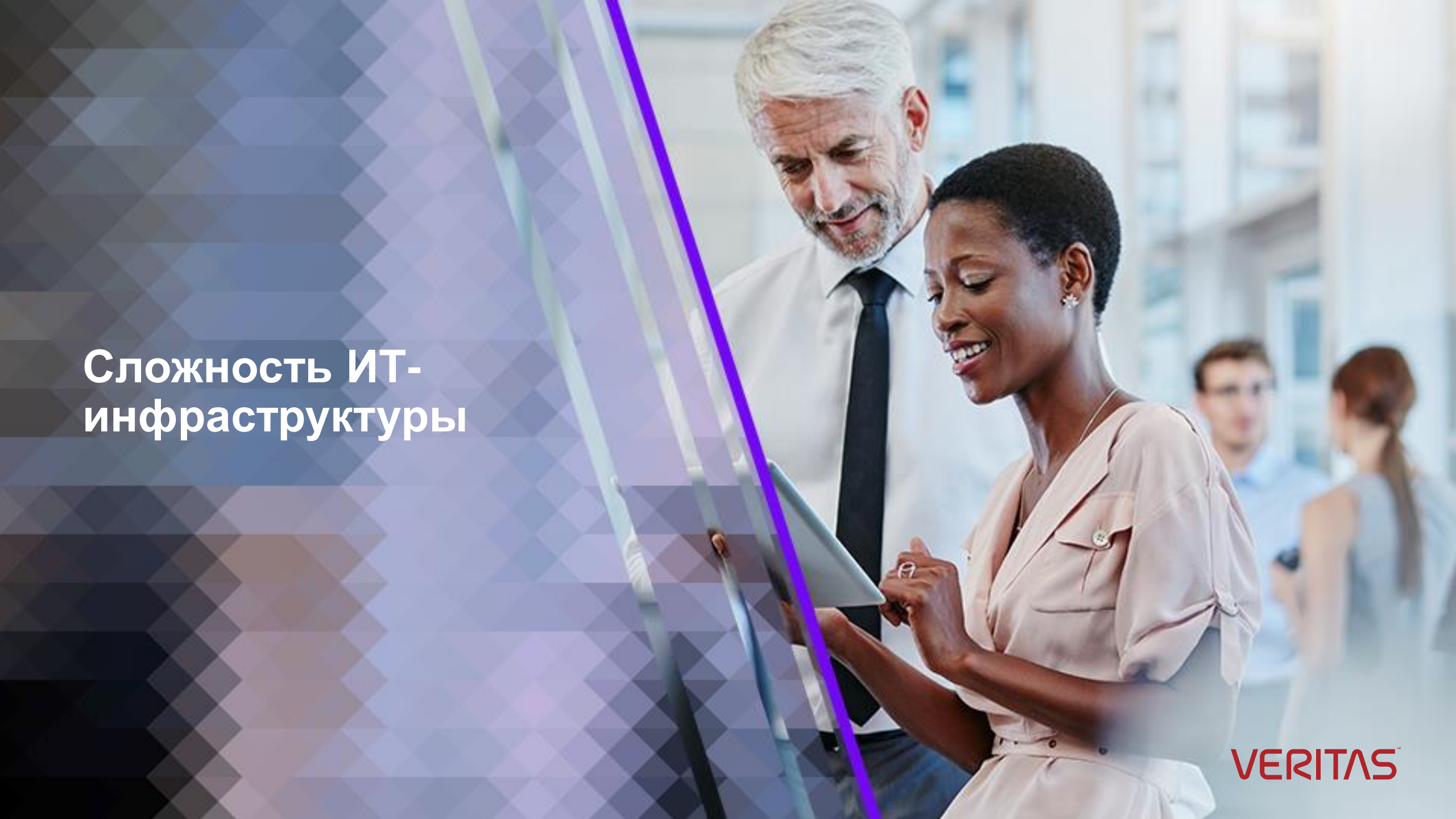
Бюджеты на ИТ и COVID-19

Большинство **(67%) российских ИТ-руководителей** заявили, что на фоне пандемии бюджеты на информационную безопасность в их компаниях не изменились или увеличились

Изменение бюджетов на информационную безопасность с начала пандемии COVID-19



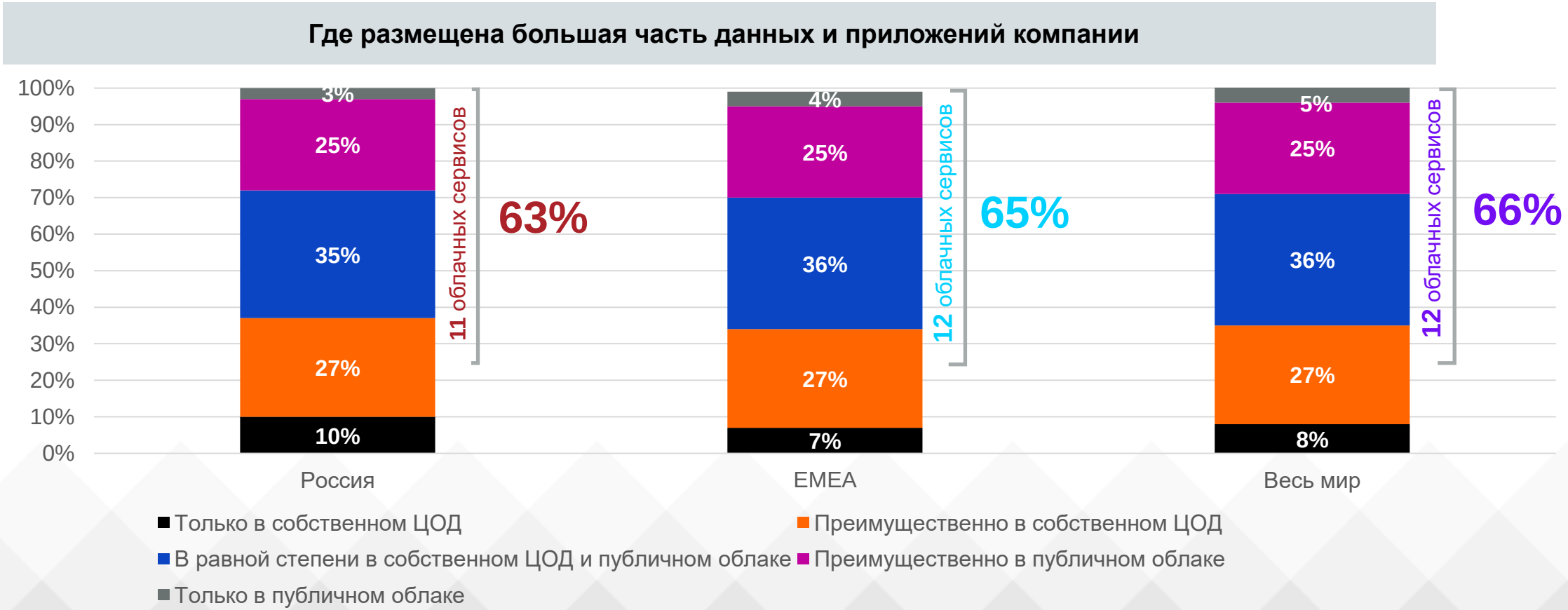
Сложность ИТ-инфраструктуры



VERITAS

Компании полагаются на гибридные облака

35% российских компаний применяют гибридную мульти-облачную стратегию, и **63%** компаний хранят в облаке все данные или их часть



Защищены ли ваши резервные копии?

Только 15% российских компаний следуют рекомендации хранить три копии данных, одна из которых находится за пределами офиса и не имеет доступа по электронным каналам связи. Это немного больше, чем среднее значение в регионе EMEA (14%).

Схема резервного копирования	Весь мир	Россия	EMEA	Информационная безопасность развивается в том же темпе (Россия)	Информационная безопасность отстает (Россия)
3 и более копий	36%	**37%**	34%	42%	34%
2 копии *(1 за пределами офиса)*	49%	**43%**	50%	32%	49%
2 копии *(0 за пределами офиса)*	14%	**20%**	16%	26%	16%

Рост числа облачных сервисов

В среднем российская компания использует 11 облачных сервисов (IaaS, PaaS и SaaS).

Россия

11 облачных сервисов

EMEA

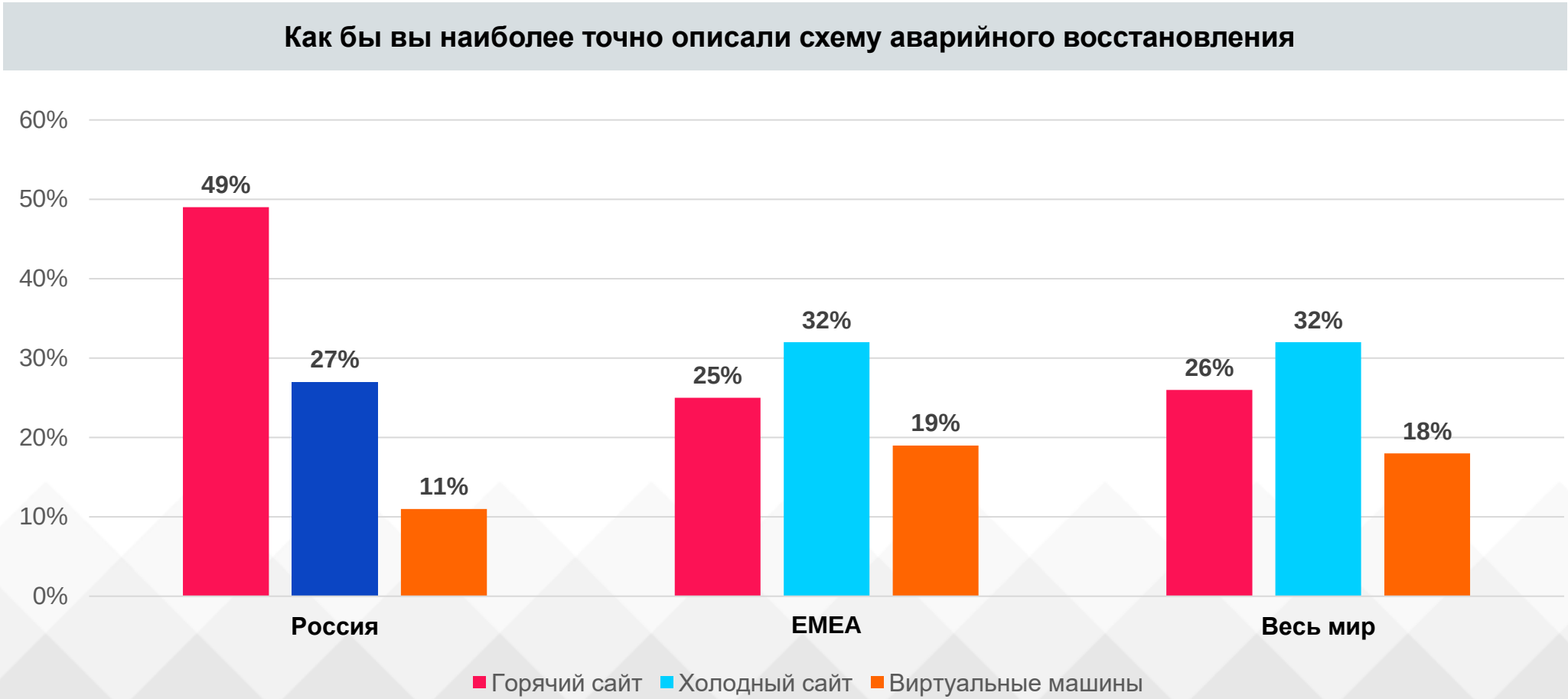
12 облачных сервисов

Весь мир

11.7 облачных сервисов

Восстановление данных не оптимизировано

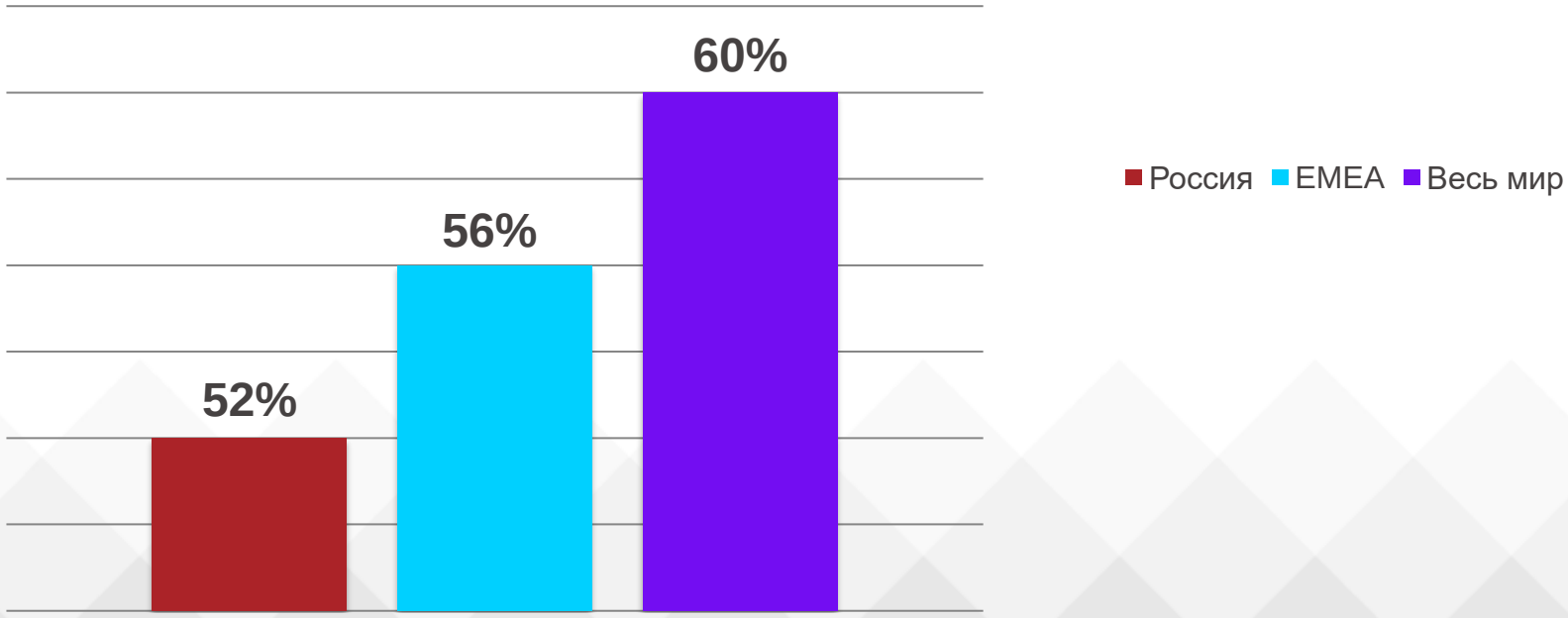
В России компании чаще используют для аварийного восстановления резервный «горячий» сайт, чем «холодный» или виртуальные машины.



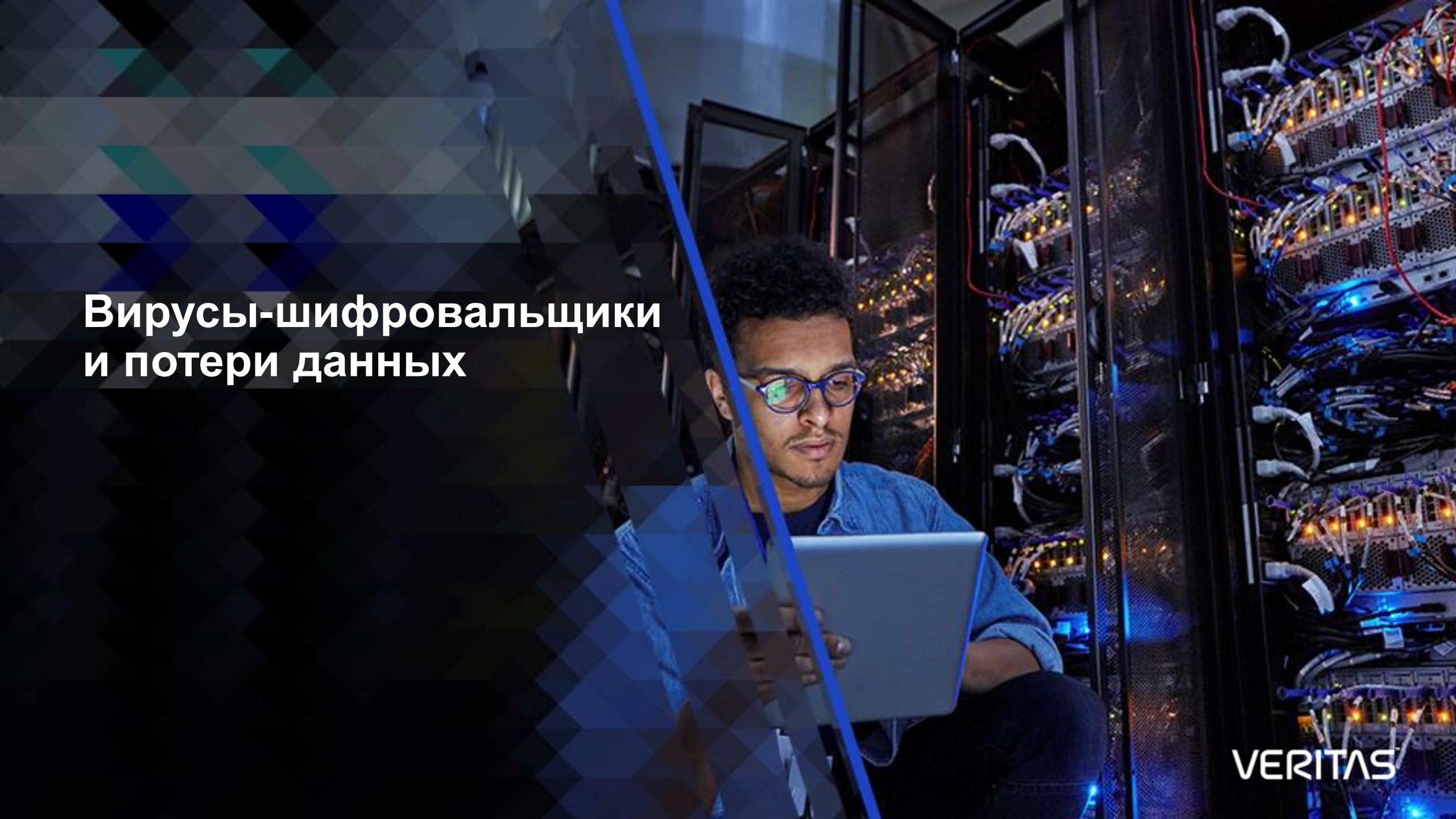
Тестирование аварийного восстановления

Российские компании тестируют процедуры аварийного восстановления (DR) реже, чем их коллеги в регионе EMEA: **лишь 52% проводили тестирование в течение последних трех месяцев. Для региона EMEA этот показатель составляет 56%, а в среднем по миру — 60%.**

% компаний, тестировавших аварийное восстановление в последние три месяца



Вирусы-шифровальщики и потери данных



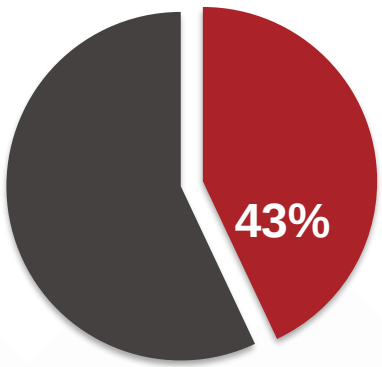
VERITAS

Вирусы-шифровальщики: растущая угроза

В России ситуация с вирусами-шифровальщиками несколько хуже, чем в среднем по региону EMEA**. 43% российских респондентов признали, что испытали как минимум одну атаку. В регионе EMEA этот показатель составляет 38%.**

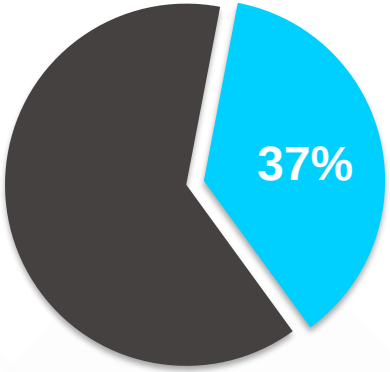
% компаний, когда-либо сталкивавшихся с атакой вирусов-шифровальщиков

Россия



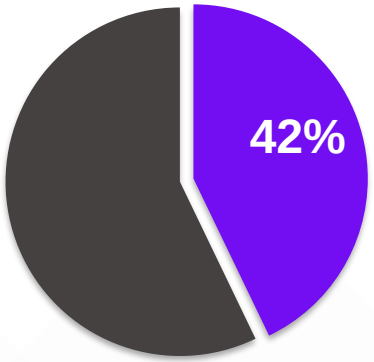
5 атак в среднем

EMEA



4,4 атаки в среднем

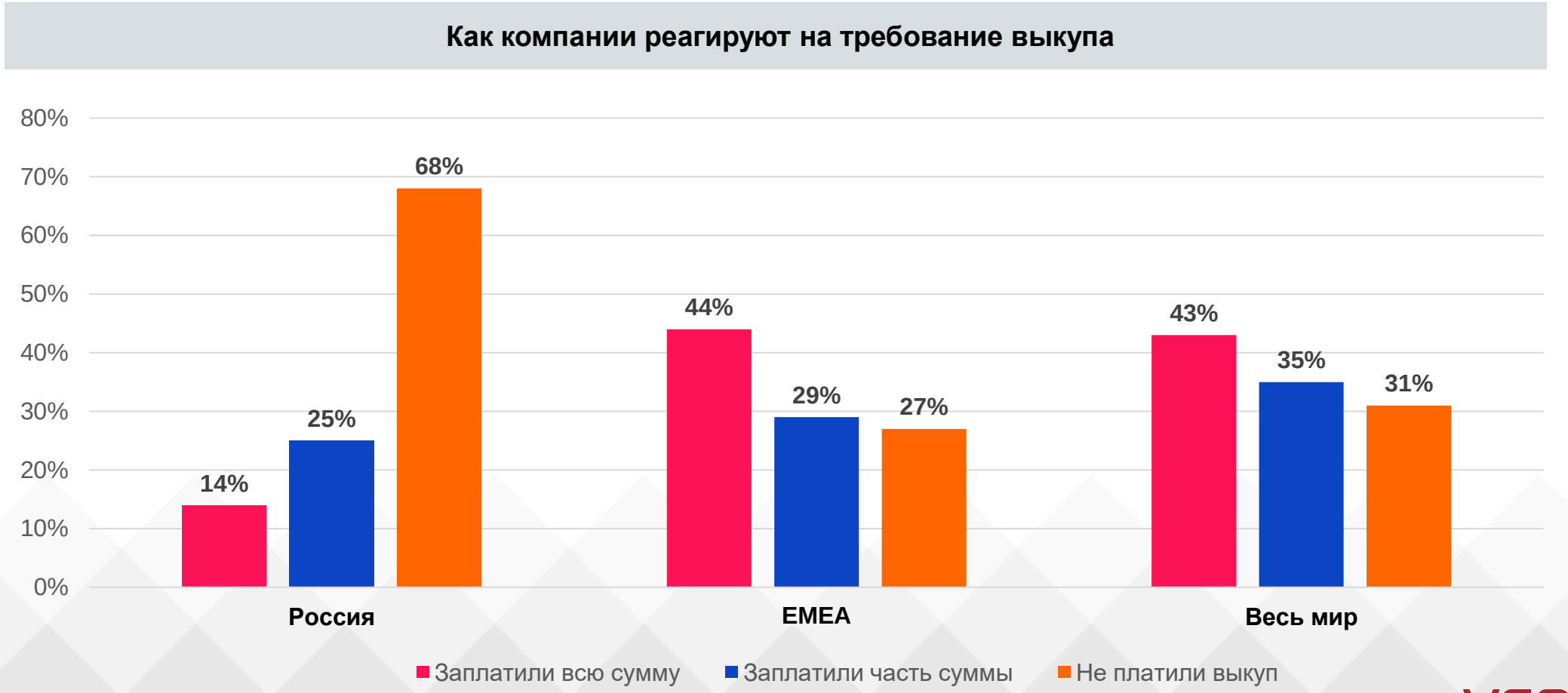
Весь мир



4,5 атаки в среднем

Компании платят выкуп — полностью или частично

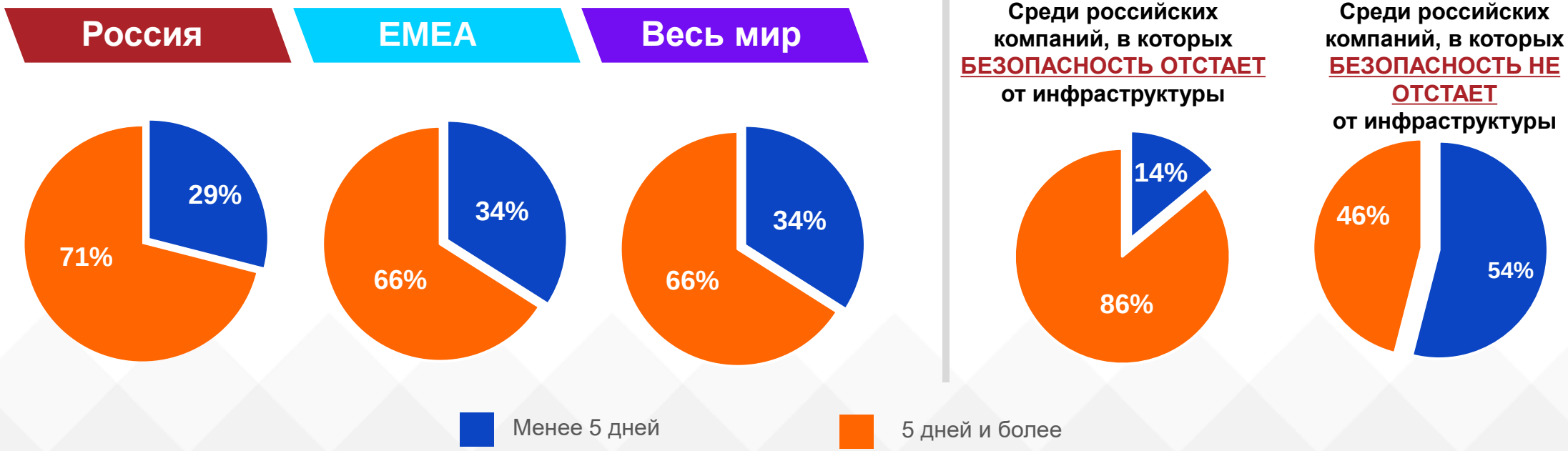
Российские компании чаще решают не платить выкуп.



Сложности, связанные с восстановлением после атак вирусов-шифровальщиков

В большинстве российских компаний – 71% – полное восстановление после атаки шифровальщика займет 5 дней и более.

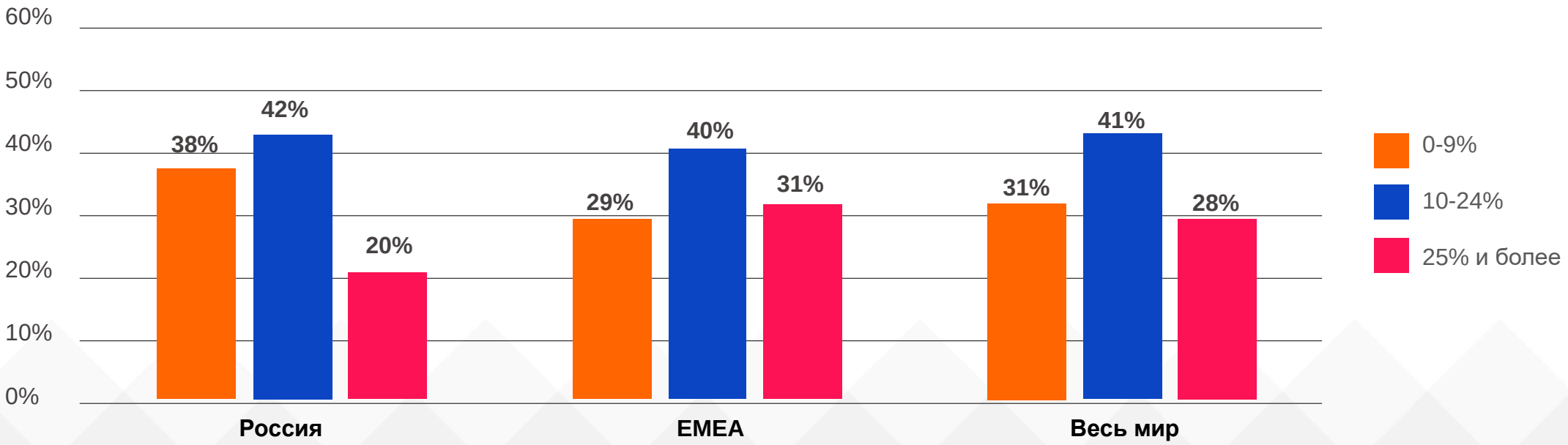
Как организации оценивают время восстановления после атаки шифровальщика



Данные и файлы, пострадавшие от атак вирусов-шифровальщиков

Ущерб для файлов и данных в российских организациях, испытавших атаку, был существенным.

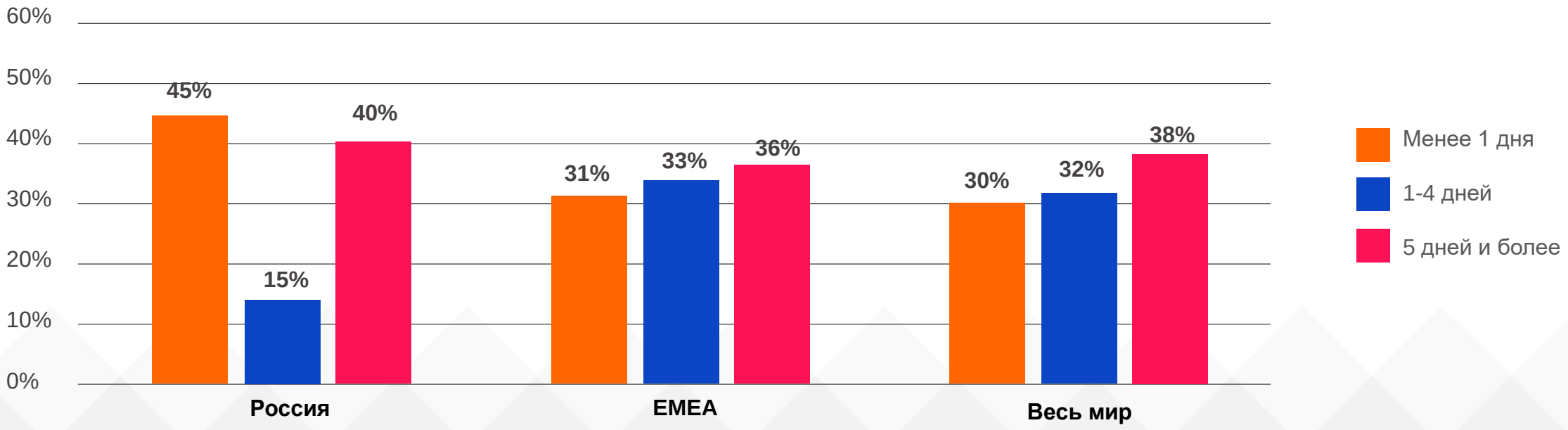
Процент файлов и данных, пострадавших или утраченных в результате атаки шифровальщика



Влияние атак вирусов-шифровальщиков на бизнес

Атаки шифровальщиков оказали существенное влияние на бизнес российских компаний.

Сколько дней, в среднем, бизнес испытывал негативные последствия атаки




VERITAS