Индекс Кибербезопасности в России

Отчет по результатам исследования

МегаФон

Введение

Кибербезопасность перестала быть вопросом только лишь соответствия требованиям регуляторов. Теперь информационная безопасность — одно из основных средств достижения бизнес-целей.

Под влиянием пандемии многие компании были вынуждены перенести бизнес в онлайн, перевести работников на удаленную работу — и таким образом стали более уязвимы перед киберпреступниками.

Компании всё больше осознают, что риски киберугроз растут, растет и потенциальный ущерб от кибератак. Однако многие инциденты можно предотвратить, если в организации внедрена надлежащая практика обеспечения кибербезопасности.

Вместе с аналитическим агентством АО «ТНС МИЦ» мы опросили 400 представителей компаний разных отраслей, которые используют сервисы по обеспечению кибербезопасности.

Цель опроса — изучить и описать роль таких сервисов в компаниях, оценить механизмы их внедрения, эффект от их использования, а также выявить потенциал дальнейшего развития этого направления.

Мы сравнили опыт использования сервисов кибербезопасности в компаниях с разным уровнем цифровой зрелости. Так, бизнес с высоким уровнем цифровизации обладает более сложной ИТ-инфраструктурой, которая требует дополнительных мер и процессов по обеспечению информационной безопасности (ИБ).

Предлагаем вашему вниманию результат этого исследования.

Основные выводы

1 В ближайшие годы кибербезопасность будет играть ключевую роль в росте экономики

Информационная безопасность необходима для цифровизации бизнеса и роста экономики организации — с этим согласны почти 90% опрошенных. При этом 80% говорят, что бизнес не уделяет должного внимания управлению киберрисками.

Так, даже среди компаний, которые уже используют сервисы ИБ, 38% компаний понесли ущерб от недостаточной защищенности своих ИТ-систем.

2 Новая реальность: беспрецедентный рост атак требует от компаний комплексной киберзащиты

Число кибератак на российские компании в первые месяцы 2022 года по сравнению с аналогичным периодом 2021 года выросло в четыре раза.

В прошлом году почти все компании, участвующие в исследовании, подвергались атакам, каждая пятая компания понесла финансовый ущерб.

Компании, которые не понесли ущерб, имели более комплексную защиту — в среднем, у них защищено на 25% больше ИТ-систем.

3 Наиболее распространенные киберугрозы связаны с уязвимостью корпоративных сетей, удаленной работой, облачными сервисами

Массовый и быстрый переход компаний на удаленный режим работы привел к новой проблеме ИБ — угрозе несанкционированного доступа к корпоративным данным.

Около 90% опрошенных компаний настроили удаленную работу сотрудников, при этом только у половины эти ресурсы защищены.

Защита удаленных рабочих мест остается в приоритете, 37% компаний планируют инвестировать в обеспечение безопасности конечных устройств вне периметра организации.

ⓘ Здесь и далее выводы построены на данных компаний, использующих и планирующих использовать сервисы кибербезопасности

Основные выводы

4 Киберзащита необходима подавляющему большинству компаний, поскольку бизнес массово мигрировал в онлайн

Почти все компании (91%) согласны с тем, что онлайн-бизнес более чувствителен к киберугрозам.

С переходом в онлайн, особенно под влиянием стремительно меняющихся внешних обстоятельств, повышается уязвимость ИТ-систем, возрастает важность обеспечения информационной безопасности.

5 Компании продолжают инвестировать в укрепление кибербезопасности бизнеса

Около половины компаний планируют увеличивать бюджет на ИБ в 2022 году.

При этом компании, которые понесли финансовый или имиджевый ущерб, в 1,5 раза чаще остальных готовы вкладываться в повышение кибербезопасности компании.

6 Надежность и опыт поставщика наряду с качеством самого ИБ-решения определяют выбор компании-партнера

Вместе с качеством решения компании оценивают экспертизу и надежность поставщика, который осуществляет интеграцию и техническую поддержку.

Эффект от самого качественного решения может быть сведен на нет без поддержки опытного и надежного партнера с высоким уровнем экспертизы в обеспечении кибербезопасности.

Основные выводы

7 Чем крупнее компания, тем сложнее ее ИТ-система и тем больше внимания надо уделять вопросам кибербезопасности

Половина крупных компаний имеет выделенный ИБ-отдел и использует ИБ-решения более 5 лет.

Крупные компании часто используют широкий спектр решений по обеспечению кибербезопасности, такие как:

- защита от DDoS-атак (54%);
- системы управления ИБ (53%);
- системы корпоративного обучения ИБ (51%);
- средства анализа защищенности (42%);
- системы управления событиями и информацией о безопасности SIEM/SOC (31%);
- решения по управлению инцидентами IRP — 31%.

8 Малый и средний бизнес испытывают нехватку специалистов по ИБ, что делает их особенно уязвимыми перед киберугрозами

С этим утверждением согласны 85% опрошенных.

Около 60% компаний малого и среднего бизнеса, которые уже сейчас используют сервисы ИБ, не имеют выделенных ИБ-специалистов, из них 26% планируют привлекать внешних партнеров.

41% компаний малого бизнеса уже используют ИБ-ресурсы по сервисной модели — когда услуги по обеспечению кибербезопасности предоставляют компании-партнеры.

9 Сервисная модель использования услуг ИБ — надежная альтернатива или способ укрепить существующую модель обеспечения кибербезопасности

ИБ — сфера, где необходимо соблюдение требований различных регуляторов. Надежный партнер должен обладать необходимыми лицензиями, глубоким пониманием специфики отрасли клиента, иметь опыт реализации подобных проектов.

Аутсорсинг ИБ дает доступ к высоко-квалифицированным специалистам и повышает уровень кибербезопасности в компании.

Основные выводы

10 Вовлеченность топ-менеджмента в управление кибербезопасностью повышает эффективность внедрения и использования сервисов ИБ

Только в 28% компаний топ-менеджмент и руководство участвуют в управлении операционной отказоустойчивостью бизнеса.

Таким компаниям в среднем на 30% чаще удается достигать поставленных целей:

- повышать продуктивность пользователей;
- сокращать эксплуатационные издержки за счет новых ИБ-решений или автоматизации процессов по обеспечению кибербезопасности;
- обеспечивать безопасность инструментов при цифровой трансформации;
- повышать устойчивость ИТ-системы в целом.

11 Информационная безопасность — это конкурентное преимущество

92% удовлетворены результатами внедрения решений по обеспечению кибербезопасности бизнеса.

80% согласны, что компании, внедряющие усиленные меры ИБ, получают преимущества перед конкурентами.

МегаФон

Индекс цифровизации

Индекс цифровизации учитывает уровень проникновения технологий в управленческую и операционную деятельность компаний, а также степень интеграции во внутренние и внешние коммуникации.

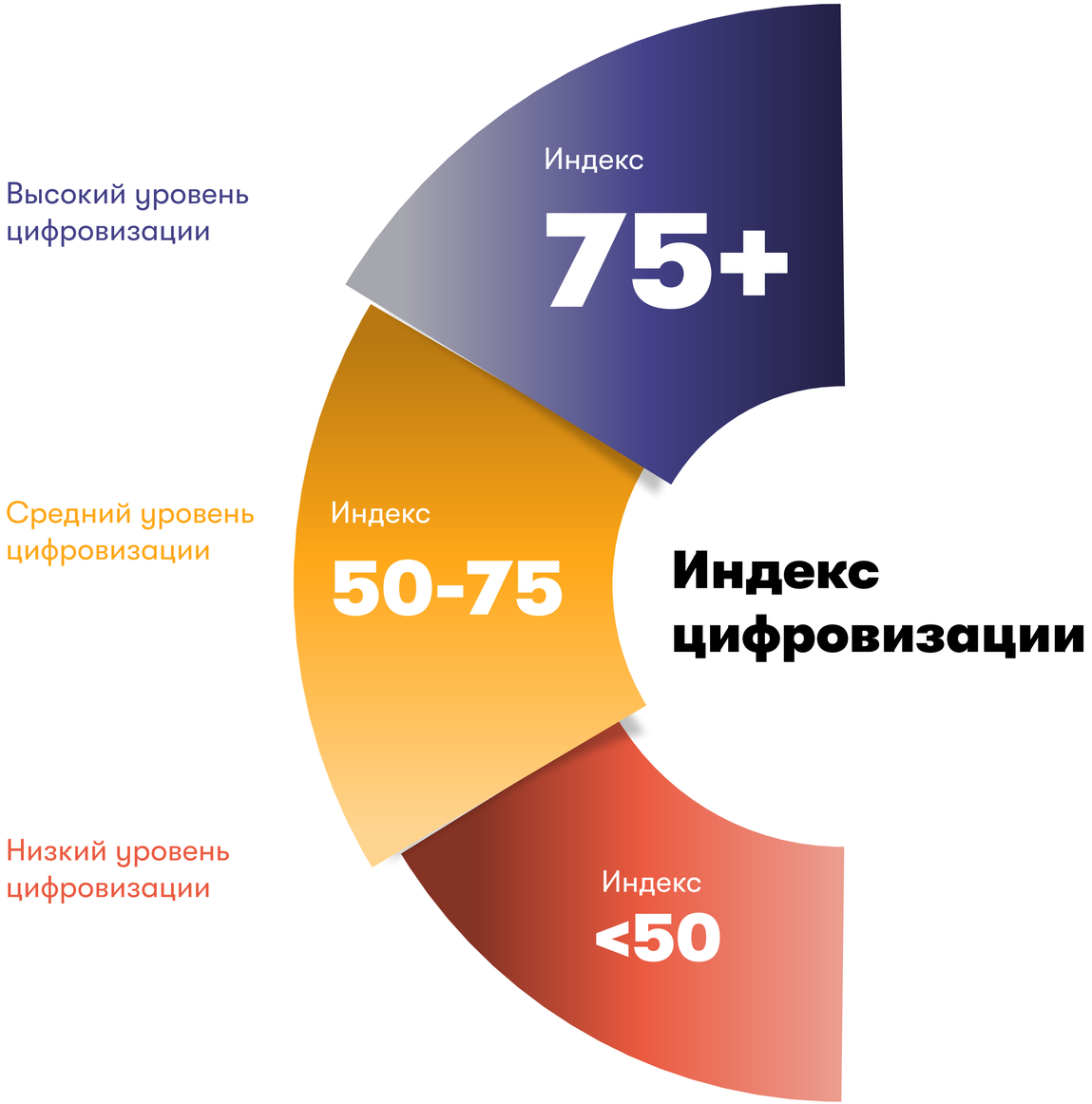
Индекс цифровизации имеет диапазон от 0 до 100,
где 100 — наивысший уровень цифровизации, 0 — ее отсутствие.

Обратите внимание на «светофор» справа:
в дальнейшем мы будем использовать индекс цифровизации и эту цветовую кодировку, чтобы показать различия между компаниями в отношении использования сервисов кибербезопасности.

Пример использования

50% опрошенных компаний имеют высокий уровень цифровизации

23% опрошенных компаний имеют низкий уровень цифровизации

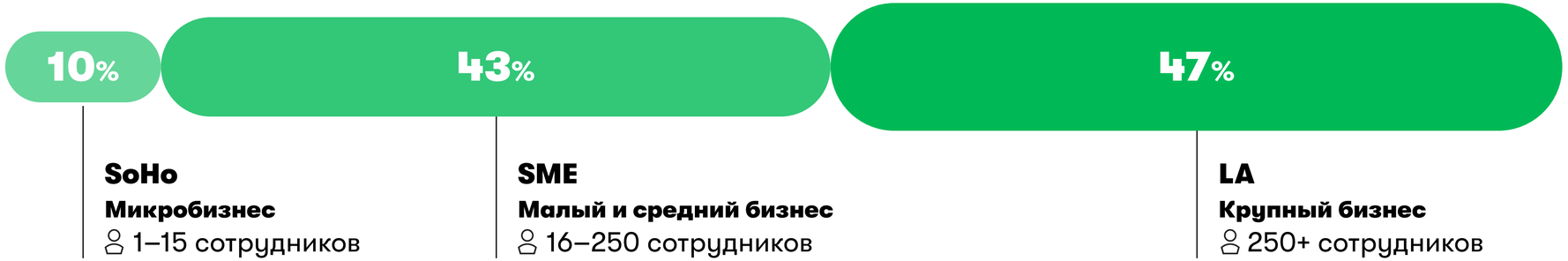


МегаФон

Профиль компаний

Большинство компаний, которые используют сервисы ИБ, — крупные, с развитой ИТ-инфраструктурой. Уровень цифровизации таких компаний выше остальных. Они активно используют новые технологии для различных бизнес-процессов и глубоко интегрируют их в ИТ-инфраструктуру компании. При этом есть и небольшая доля прогрессивных представителей малого бизнеса, понимающих важность обеспечения кибербезопасности и активно использующих эти сервисы.

Размер компаний, участвовавших в опросе



SoHo
Микробизнес
1–15 сотрудников

SME
Малый и средний бизнес
16–250 сотрудников

LA
Крупный бизнес
250+ сотрудников

Индекс цифровизации компаний, участвовавших в опросе

62 **64** **70**

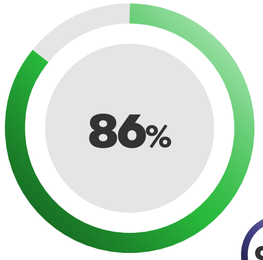
Среднее значение

67

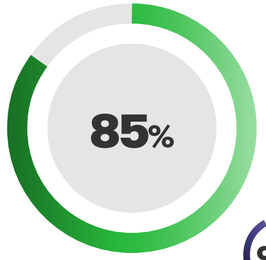
МегаФон

Роль сервисов кибербезопасности

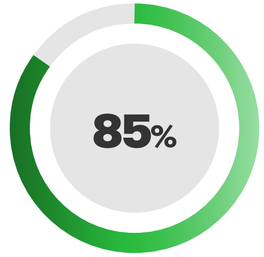
Число кибератак на российские компании выросло в четыре раза в первые месяцы 2022 года по сравнению с аналогичным периодом 2021 года. В связи с этим задача обеспечения киберзащиты компаний вышла на первый план.



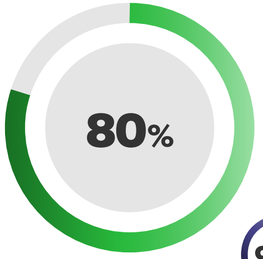
Считают, что за время пандемии выросла важность защиты конфиденциальной информации в компаниях



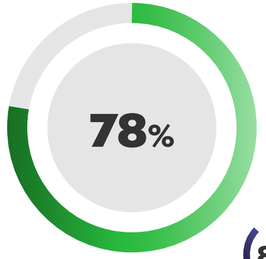
Согласны, что ИБ стала обязательным требованием при цифровизации бизнеса



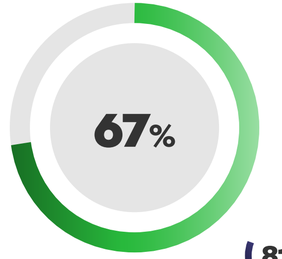
Уверены, что в ближайшие годы кибербезопасность будет играть ключевую роль в росте экономики



Считают, что большинство компаний не уделяют должного внимания управлению киберрисками



Уверены, что ИБ перестала быть вопросом соответствия требованиям регуляторов, но стала одним из основных средств достижения бизнес-целей



Получают существенную экономическую выгоду от инвестиций в ИБ

МегаФон

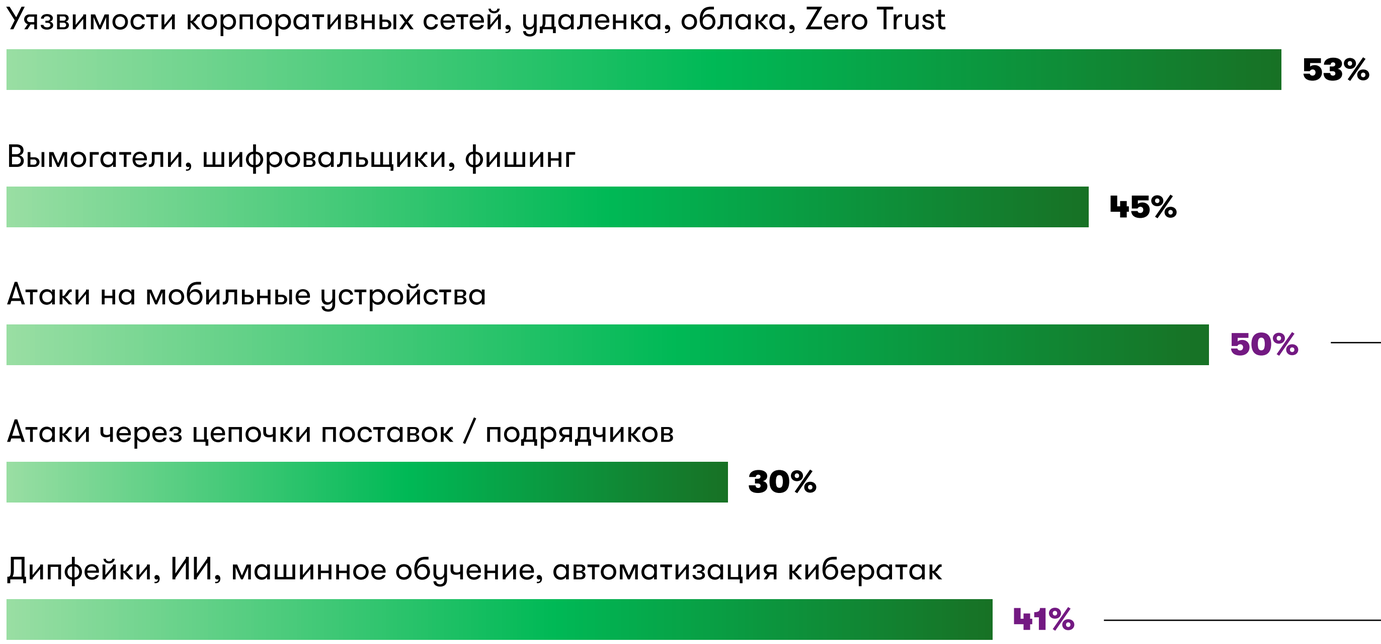
Высокий уровень цифровизации

Низкий уровень цифровизации

Быстрорастущие угрозы 2022 года

Ожидается существенный рост атак на мобильные устройства и развитие автоматизации кибератак, по сравнению с 2021 годом. Киберугрозы в корпоративных сетях, облаках и на удаленке по-прежнему лидируют.

Какие угрозы приобретут наибольшее распространение в 2022 году



Упоминаются
×1,5 раза чаще
в сравнении с 2021

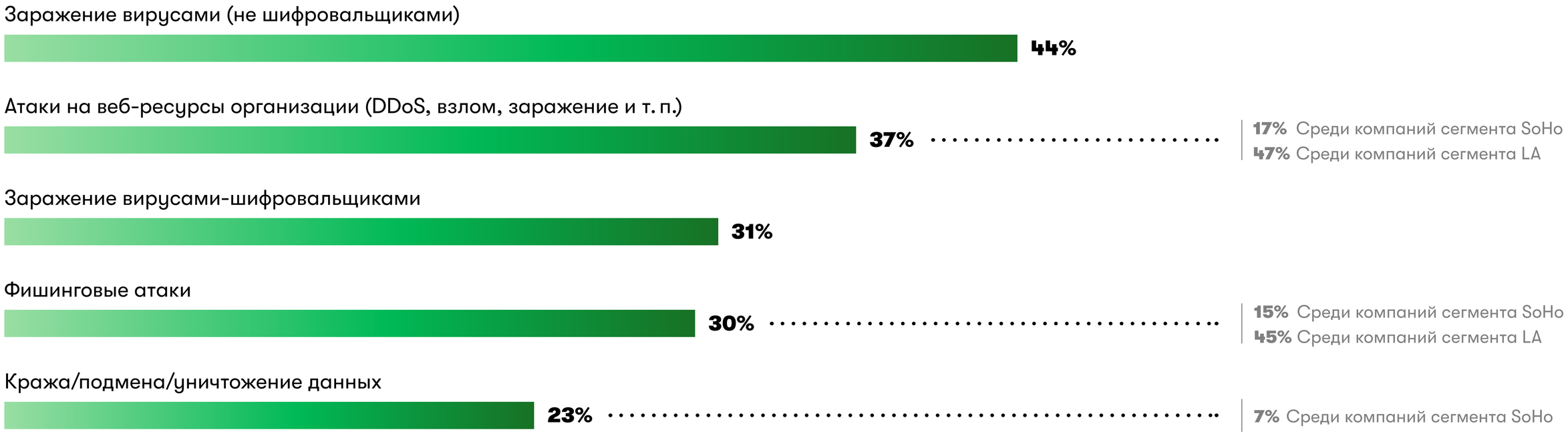
МегаФон

Респондентам был доступен множественный ответ, поэтому общая сумма не равна 100%

Киберугрозы, с которыми столкнулись компании за год

Чаще всего угрозы выражены в заражениях вирусами. В более крупных компаниях с большим количеством инфраструктуры угрозы в целом возникают чаще, особенно часто встречаются атаки на веб-ресурсы (DDoS, взлом, заражение и т. д.).

Угрозы/атаки, с которыми столкнулись за год



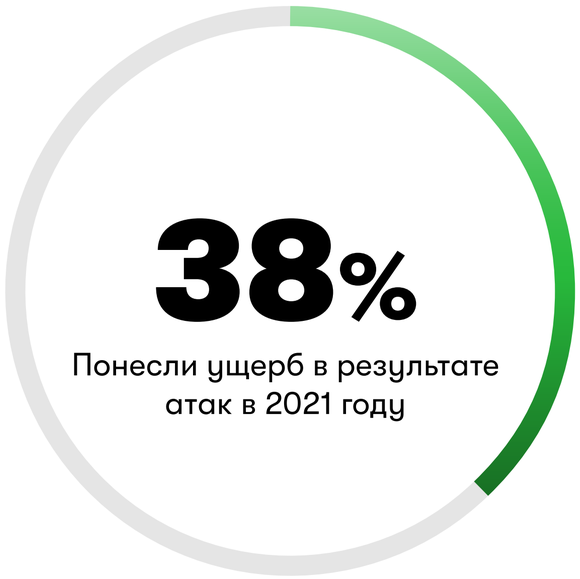
МегаФон

Кибератаки и ущерб от них

Почти все компании подвергались атакам в прошлом году, 38% из них понесли ущерб, в том числе финансовый.

90%

Подвергались кибератакам в 2021 году



38%

Понесли ущерб в результате атак в 2021 году

20%

Понесли финансовый ущерб

Из них каждая пятая компания оценила свой ущерб более чем

в 5 млн ₽

МегаФон

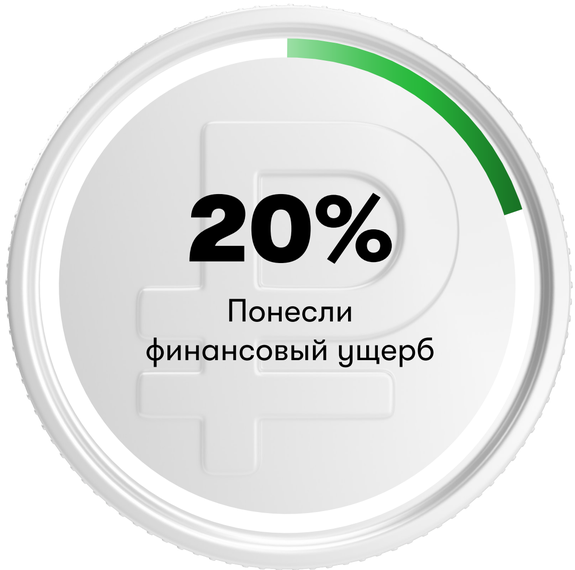
Какие решения МегаФона помогут предотвратить кибератаки и минимизировать риски финансового и репутационного ущерба

Узнать больше

Связь ущерба с типами кибератак

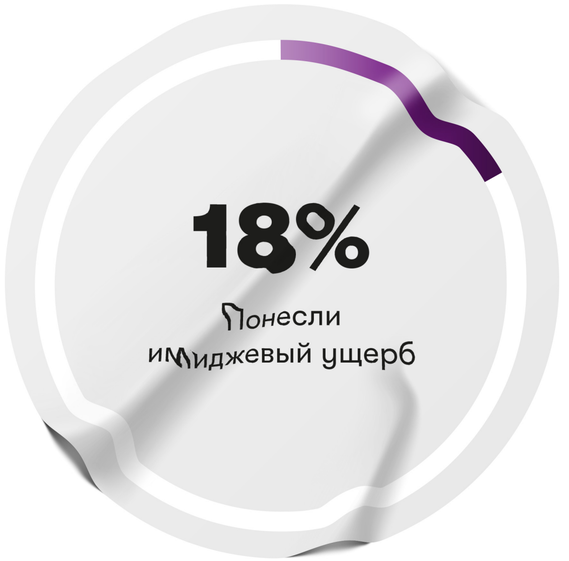
Хакерские атаки с целью получения прямой финансовой выгоды стали, к сожалению, обыденным явлением. Ущерб от атак может быть в равной степени имиджевый и финансовый.

Финансовый ущерб чаще возникает при заражениях вирусами и подмене/уничтожении данных.
На имидж в большей степени влияют фишинговые атаки, которые нацелены, как правило,
на получение реквизитов доступа для последующей кражи данных.



Атаки, с которыми сталкивались

42%	Заражение вирусами (не шифровальщиками)	58%
49%	Фишинговые атаки	38%
36%	Кража/подмена/уничтожение данных	49%

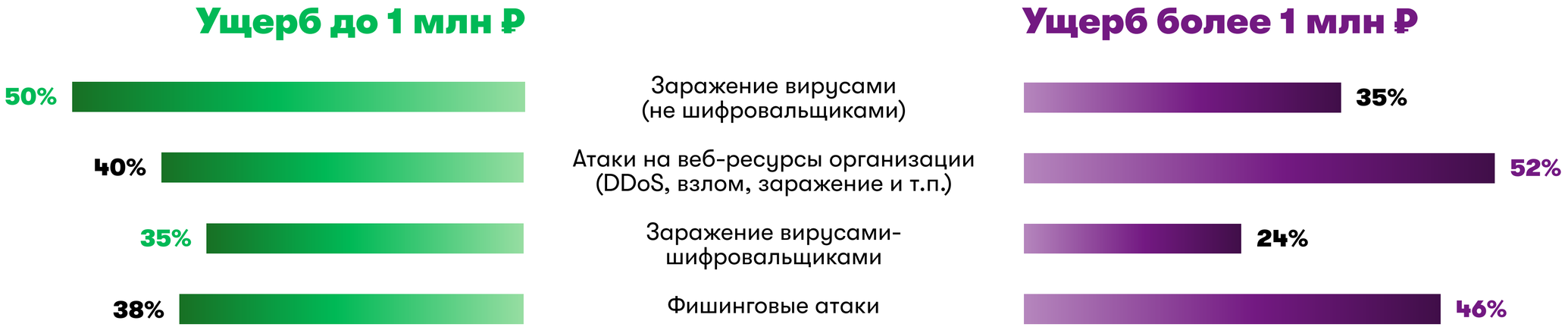


МегаФон

Размер ущерба и типы кибератак

Наибольший урон компаниям за последний год нанесли атаки на веб-ресурсы (в том числе DDoS) и фишинговые атаки. Это происходит потому, что компании зачастую недооценивают риски информационной безопасности – например, связанные с осведомленностью сотрудников в области кибербезопасности, патч-менеджментом и безопасной разработкой.

Угрозы по размеру финансового ущерба среди компаний, которые сталкивались с кибератаками

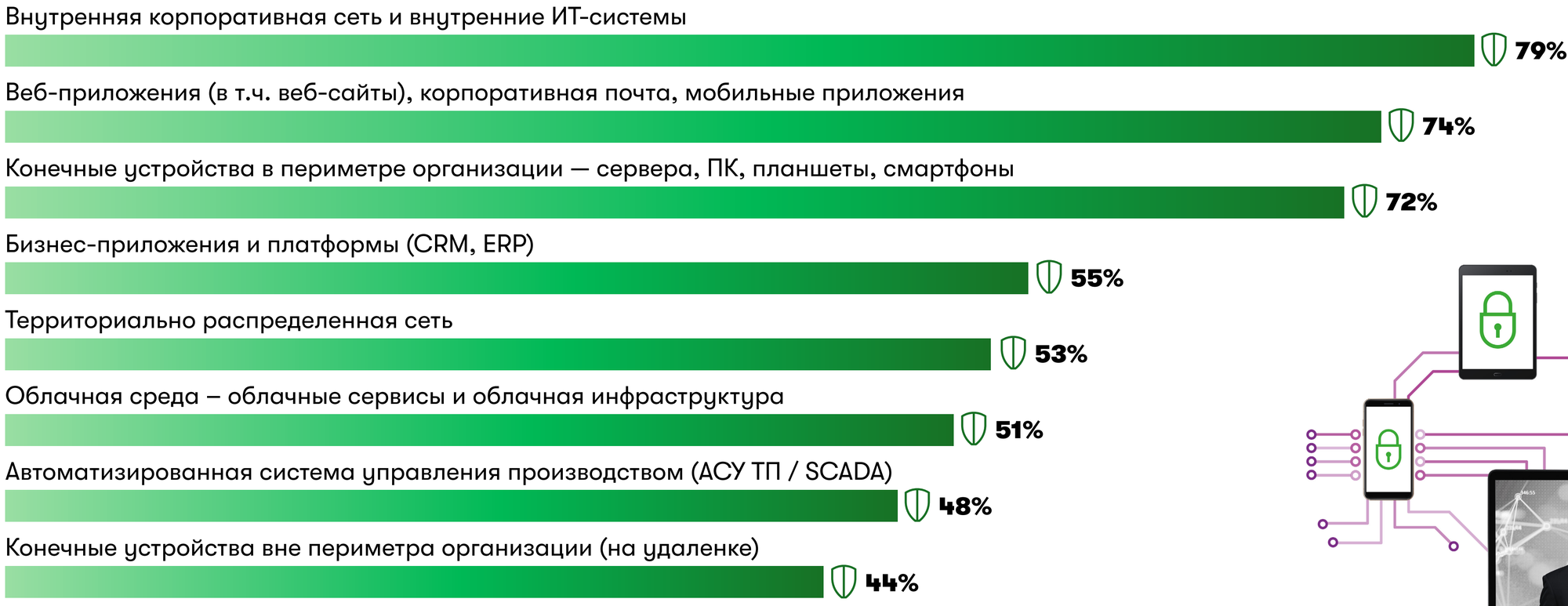


МегаФон

В киберзащите важен комплексный подход

Несмотря на то, что уровень защиты отдельных ИТ-систем довольно высокий, компании нуждаются в комплексной защите: чем больше инструментов используется, тем больше уязвимостей они «закрывают» и тем ниже вероятность возникновения ущерба.

Какие системы защищены

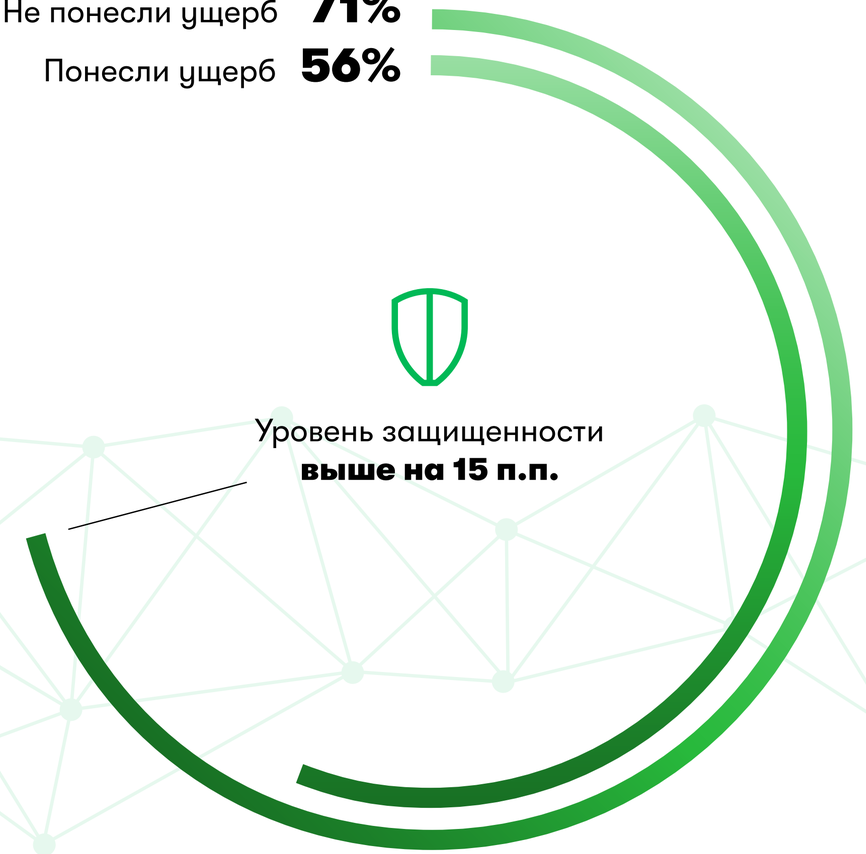


МегаФон

Взаимосвязь уровня защиты и ущерба

Кибератаки в последние годы приобрели мультивекторный характер, поэтому уровень защищенности IT-систем напрямую зависит от того, как реализована ИБ-защита. Это подтверждается мнением компаний: те, кто не понесли ущерб в 2021 году, имели более комплексную защиту.

Уровень защищенности ИТ-систем



МегаФон

* Уровень защищенности – отношение защищенных систем к имеющимся

Предпосылки к использованию сервисов ИБ

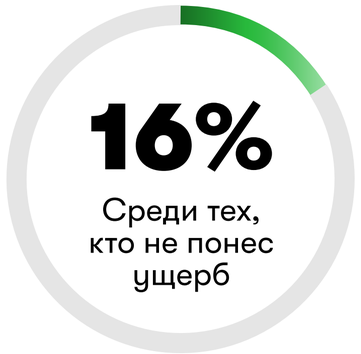
Почти половина компаний внедряла ИБ-решения превентивно, из-за общего роста киберугроз.

Почему компании внедряли решения по кибербезопасности:

29%
По требованию регулятора

48%
Превентивно, из-за роста киберугроз

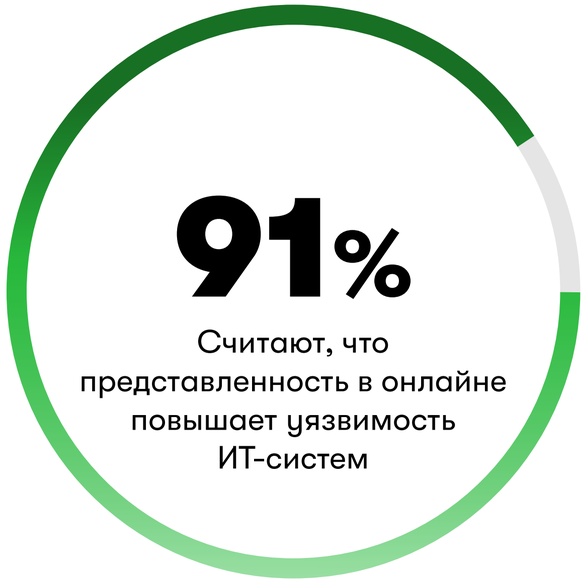
23%
После киберинцидента

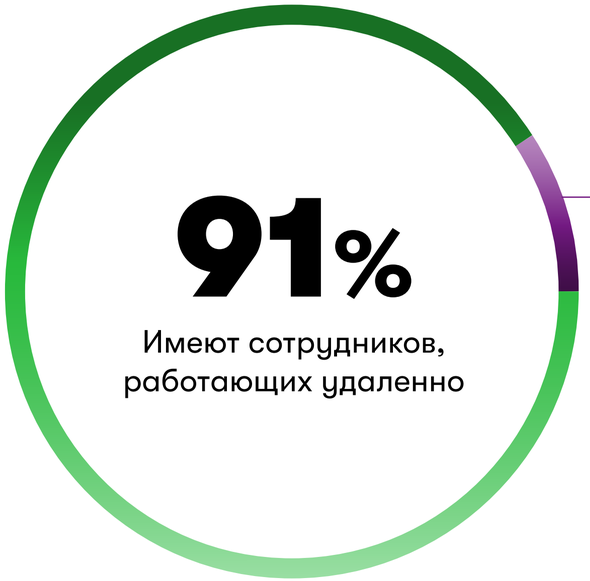


МегаФон

Переход в онлайн и кибербезопасность

Вынужденная переориентация офлайн-бизнеса в онлайн, а также массовый и быстрый переход компаний на удаленный режим работы вскрыли новую проблему кибербезопасности — угрозу несанкционированного доступа к корпоративным данным.





Здравоохранение, медицина
23%

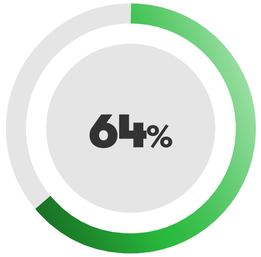
20%
Администрация, госуправление

Только
44%
компаний защищают конечные устройства вне периметра организации (на удаленке)

МегаФон

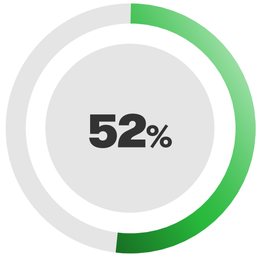
Что критично важно для обеспечения безопасности удаленной работы

В первую очередь — защита систем удаленного доступа и серверного оборудования. Для небольших компаний в меньшей степени важны ИТ- и ИБ-специалисты, зачастую эти компании не имеют в штате такие ресурсы. Для них такую поддержку оказывают аутсорс-партнеры.



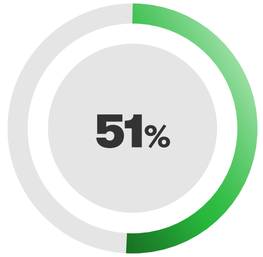
Защита систем удаленного доступа, серверного оборудования

79%



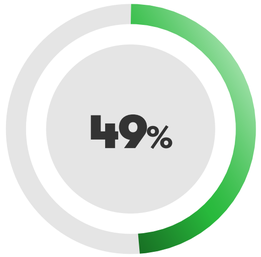
Защищенное (лицензионное) программное обеспечение

72% 40%



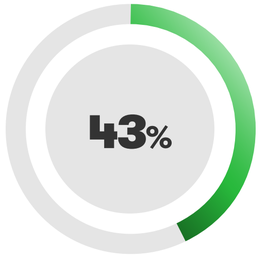
Защита клиентского оборудования

66% 40%



Четкие правила организации удаленной работы

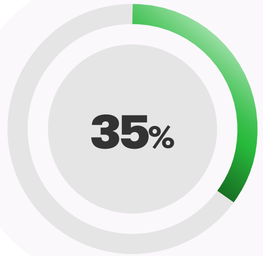
70%



Контроль пользователей, работающих удаленно

61%

26% Среди компаний сегмента SoHo



Штат ИТ- / ИБ-специалистов

50% 23%

15% Среди компаний сегмента SoHo

43% Среди компаний сегмента LA

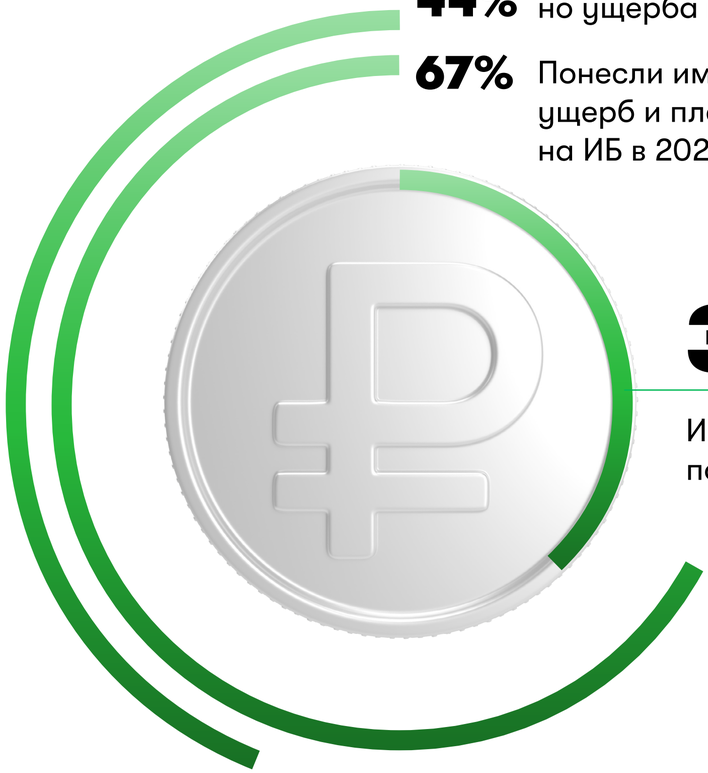
МегаФон

Высокий уровень цифровизации

Низкий уровень цифровизации

Подходы к бюджетированию

Компании реже планируют вкладываться в развитие ИБ, в сравнении с общим развитием ИТ-систем. При этом те, кто уже столкнулись с атаками и понесли ущерб, — в 1,5 раза чаще готовы инвестировать в укрепление кибербезопасности компании.



44% Готовы увеличить бюджет на ИБ в 2022 году, но ущерба не понесли

67% Понесли имиджевый или финансовый ущерб и планируют увеличить бюджет на ИБ в 2022 году

38%

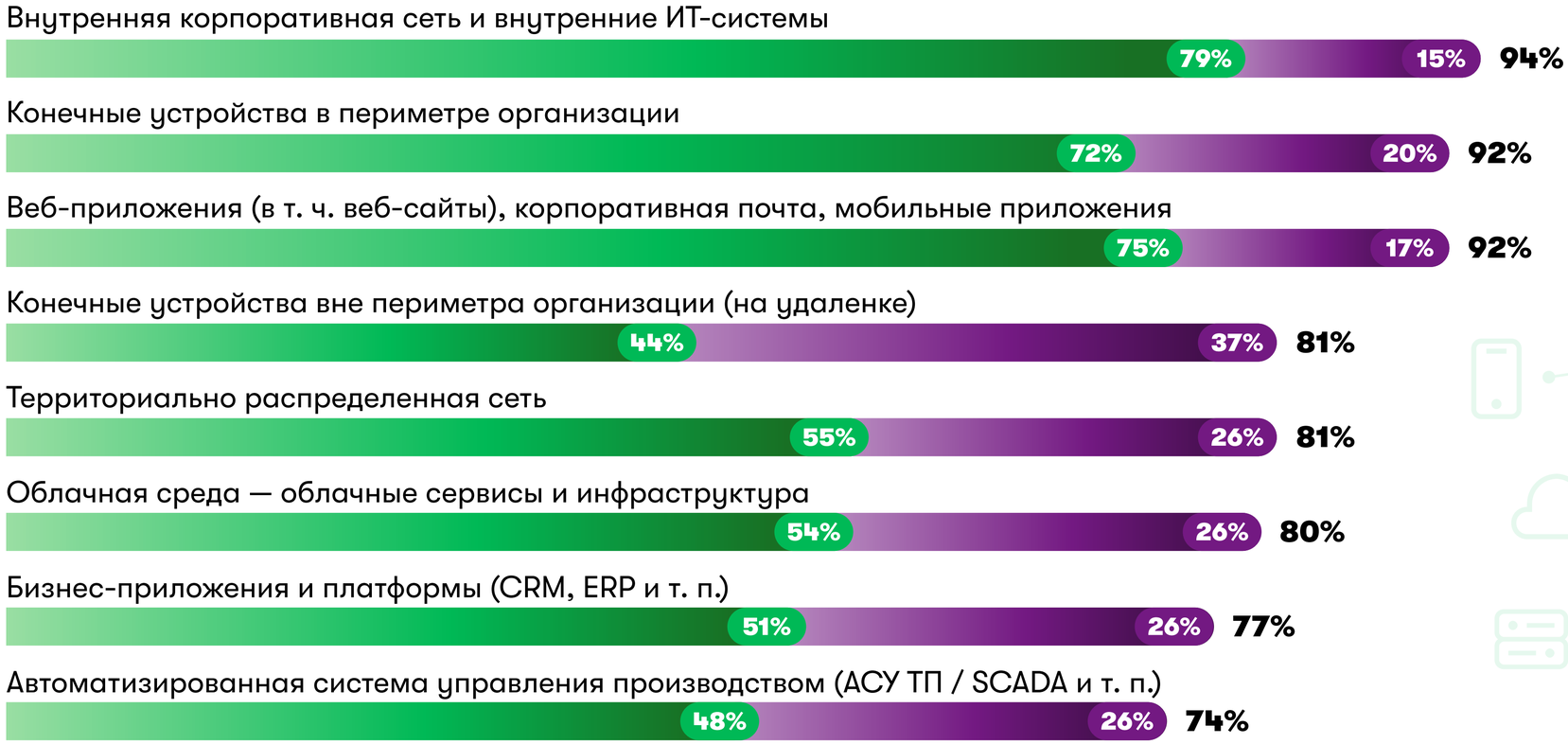
Из всех опрошенных компаний понесли ущерб в 2021 году

МегаФон

Какие ИТ-ресурсы защищают чаще всего

Конечные устройства в периметре организаций, а также корпоративная почта и корпоративная сеть, как правило, уже защищены. Конечные устройства на удаленке — приоритетные сервисы для защиты.

Для каких ресурсов компании используют средства киберзащиты



МегаФон

Уже используется

Планируется

Доля ИБ в структуре постоянных затрат компаний

Компании с высоким уровнем цифровизации инвестируют в сервисы кибербезопасности в 3 раза больше.

Средние затраты на ИБ

Высокий уровень цифровизации **17%**

Все компании **12%**

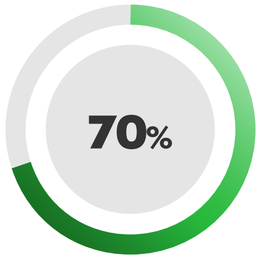
Низкий уровень цифровизации **5%**

МегаФон

Направления инвестиций в ИБ

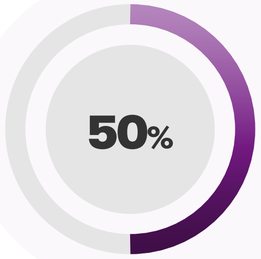
Половина компаний планирует инвестировать в новые решения по обеспечению кибербезопасности. 2/3 компаний получают существенную экономическую выгоду от инвестиций в ИБ.

Ключевые векторы инвестиций в информационную безопасность

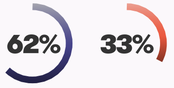


Поддержка текущей работы ИБ-решений

82% Среди производственных компаний

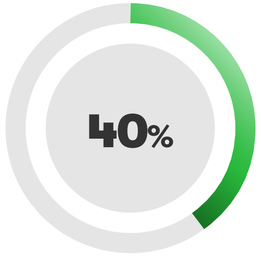


Внедрение новых ИБ-решений

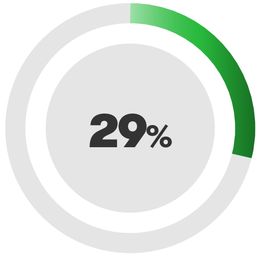


63% Среди финансовых и страховых компаний

30% Среди компаний торговли и ретейла



Адаптация имеющихся ИБ-решений для новых бизнес-процессов



Масштабирование ИБ-решений

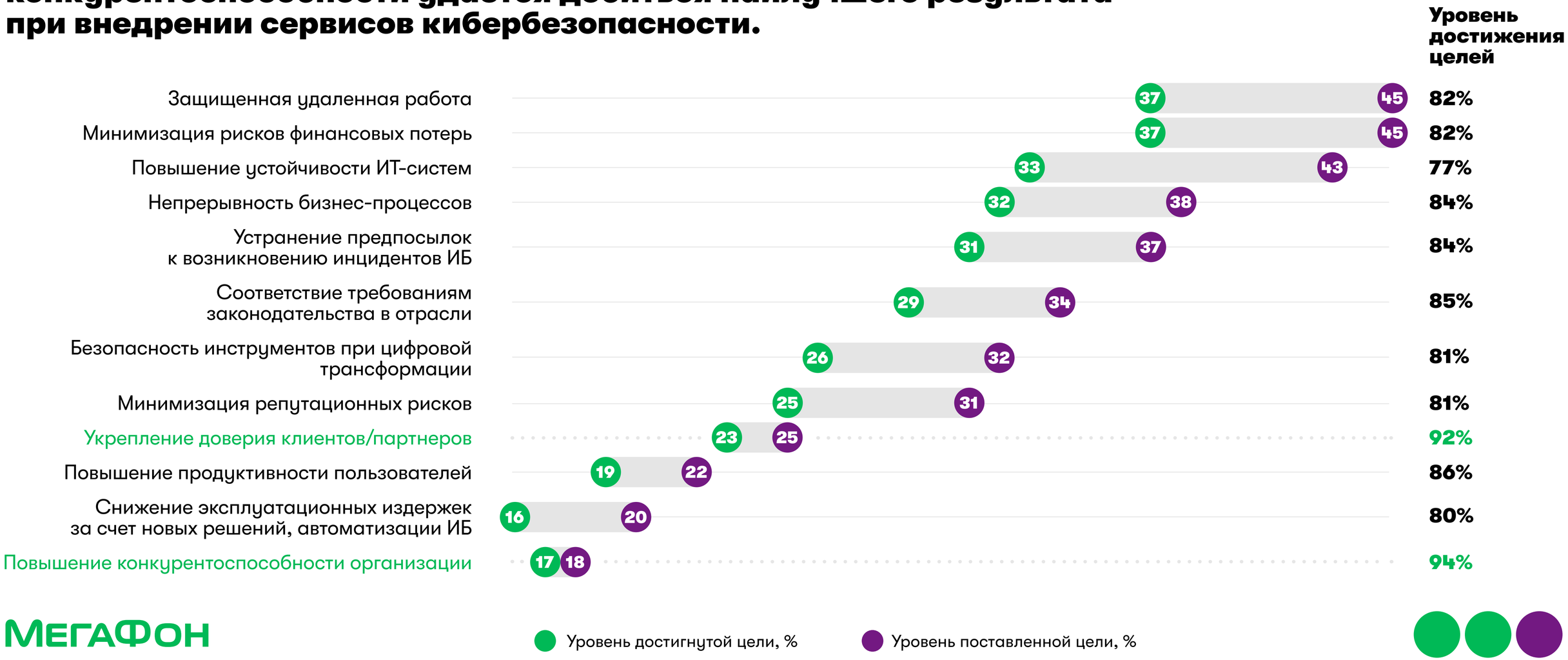
МегаФон

Высокий уровень цифровизации

Низкий уровень цифровизации

Цели внедрения сервисов ИБ

Цель обеспечения конкурентоспособности не первоочередна, но именно в укреплении доверия клиентов/партнеров и повышении конкурентоспособности удается добиться наилучшего результата при внедрении сервисов кибербезопасности.



МегаФон

Риски внедрения сервисов ИБ

Ключевыми рисками внедрения ИБ считаются затраты и их окупаемость, сложность поиска квалифицированных специалистов. Отдельные риски, связанные с функционалом, также беспокоят компании. Нивелирование рисков возможно при выборе проверенных партнеров по внедрению средств ИБ.

46% Стоимость внедрения и обслуживания окажется слишком высокой

36% Затраты на внедрение могут не оправдаться

56% Среди компаний сегмента SoHo

40% Трудно найти квалифицированных специалистов для обслуживания ИБ-решений

19% Сотрудники не готовы обучаться работе с ИБ-сервисами

32% Среди компаний сегмента здравоохранения

33% Сложнее решать технические проблемы, необходимо обращаться к разработчику

31% Большие операционные риски для бизнеса, если ИБ-решение перестанет поддерживаться

30% Внедрение ИБ-решений требует значительных изменений в ИТ-инфраструктуре

27% ИБ-сервисы замедлят (ухудшат) работу существующей ИТ-системы

24% Решение не будет в полной мере обладать функционалом для выполнения поставленных задач

15% Решение недостаточно гибкое, трудно кастомизировать

МегаФон

Информационная безопасность — это конкурентное преимущество

Большинство компаний, использующих решения ИБ, удовлетворены результатами внедрения и считают, что усиленные меры ИБ позволяют получить преимущества перед конкурентами и экономическую выгоду.

Удовлетворенность результатами внедрения решений ИБ

27%
Полностью удовлетворен

65%
Скорее удовлетворен

8%
Скорее не удовлетворен

80%
Согласны, что компании, внедряющие усиленные меры ИБ, получают преимущества перед конкурентами

МегаФон

Высокий уровень цифровизации

Низкий уровень цифровизации

Использование сервисной модели

Российский рынок кибербезопасности достаточно зрелый и готов получать услуги по сервисной модели, доверие его к поставщикам услуг неуклонно растет. Однако для консервативного государственного сектора такой формат обеспечения ИБ пока менее перспективен.

22% компаний используют сервисную модель ИБ, и потенциал у аутсорсинга велик — еще 49% рассматривают такую модель как рабочую.

49%

Рассматривают сервисную модель

29%

Не используют и не планируют использование сервисной модели

49% В секторе гос-управления, ЖКХ

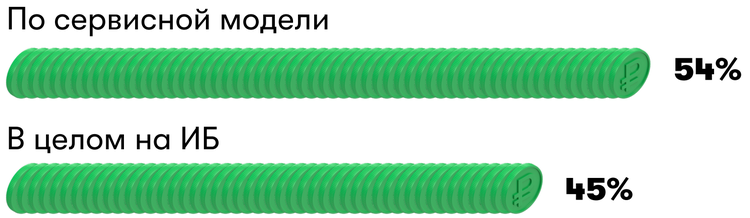
22%

Используют сервисную модель

41% Среди компаний сегмента SoHo

Компании ожидают, что их инвестиции в сервисную модель будут расти более динамично, чем на ИБ в целом.

Рост бюджета на ИБ



МегаФон

Высокий уровень цифровизации

Низкий уровень цифровизации

Востребованность услуг аутсорсинга ИБ

Зачастую ИБ-аутсорсинг — это способ снизить капитальные затраты за счет использования сервисной модели. Самые распространенные сервисы — защита от DDoS-атак и внешнее сканирование на уязвимости. Последний — уже востребован или планируется к использованию у 57% компаний.

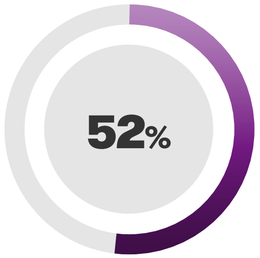
Какие услуги ИБ по сервисной модели наиболее востребованы

МегаФон

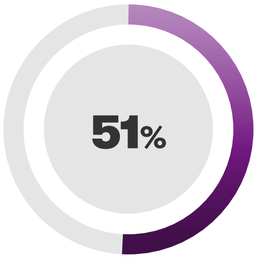
Преимущества сервисной модели ИБ

Многие организации работают в условиях отсутствия выделенных специалистов по кибербезопасности. В таких случаях аутсорсинг помогает решить кадровую проблему и повысить уровень зрелости ИБ.

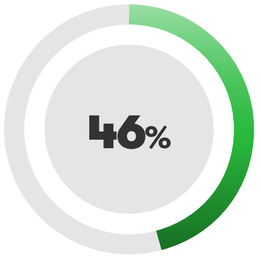
Преимущества сервисной модели ИБ по сравнению с традиционной



Более высокий уровень компетенций аутсорсинговой команды по сравнению со штатными ИБ-специалистами

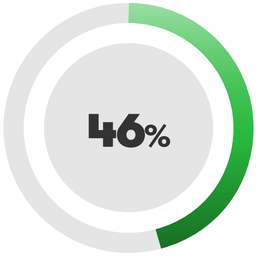


Готовые процессы обеспечения ИБ

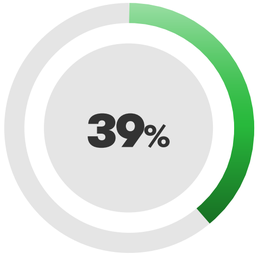


Более быстрая адаптация защиты под новые и развивающиеся угрозы

66% Среди компаний торговли и ретейла

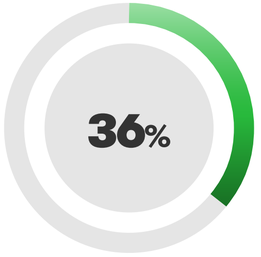


Сокращение времени на внедрение/запуск ИБ-решения



Сокращение расходов на оплату ИБ-специалистов

58% Среди компаний сегмента здравоохранения



Сокращение затрат на приобретение ИБ-решений

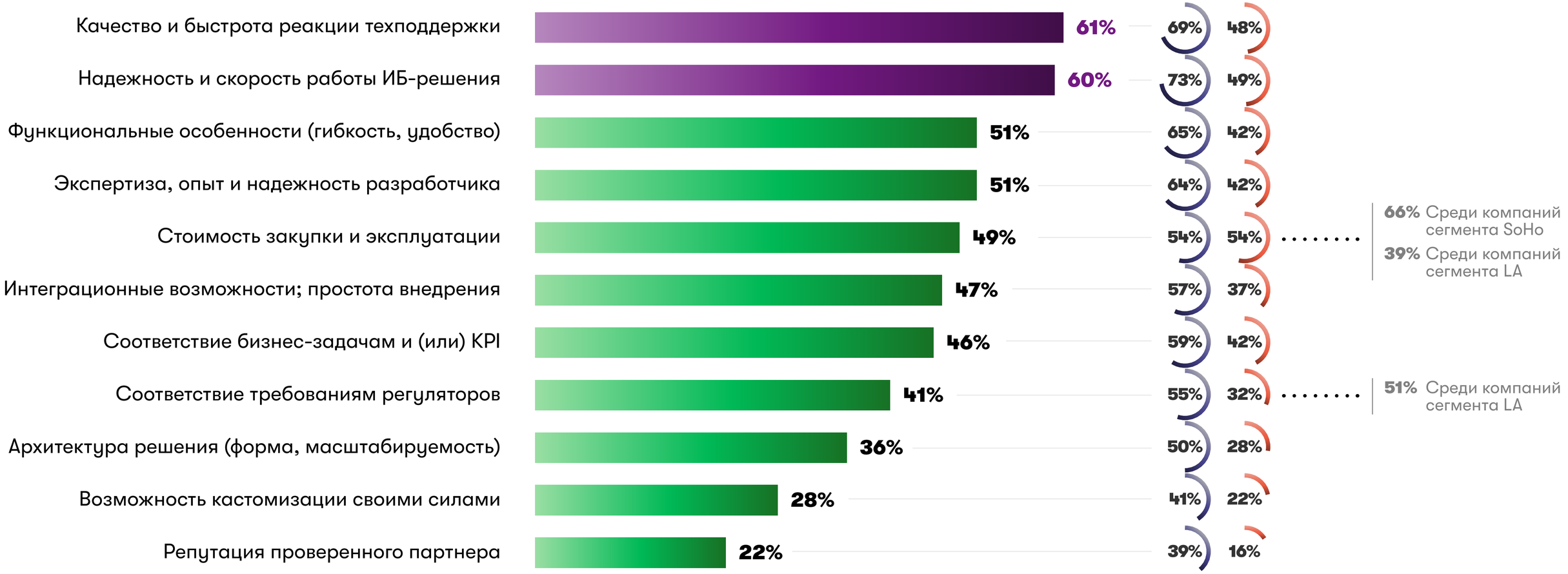
18% Среди компаний сегмента SoHo

МегаФон

Критерии выбора ИБ-сервисов

Качество, надежность и скорость являются более важными параметрами при выборе ИБ-решений, чем стоимость. Однако стоимость играет ключевую роль при выборе для SoHo.

Наиболее важные параметры при выборе поставщика ИБ-решений

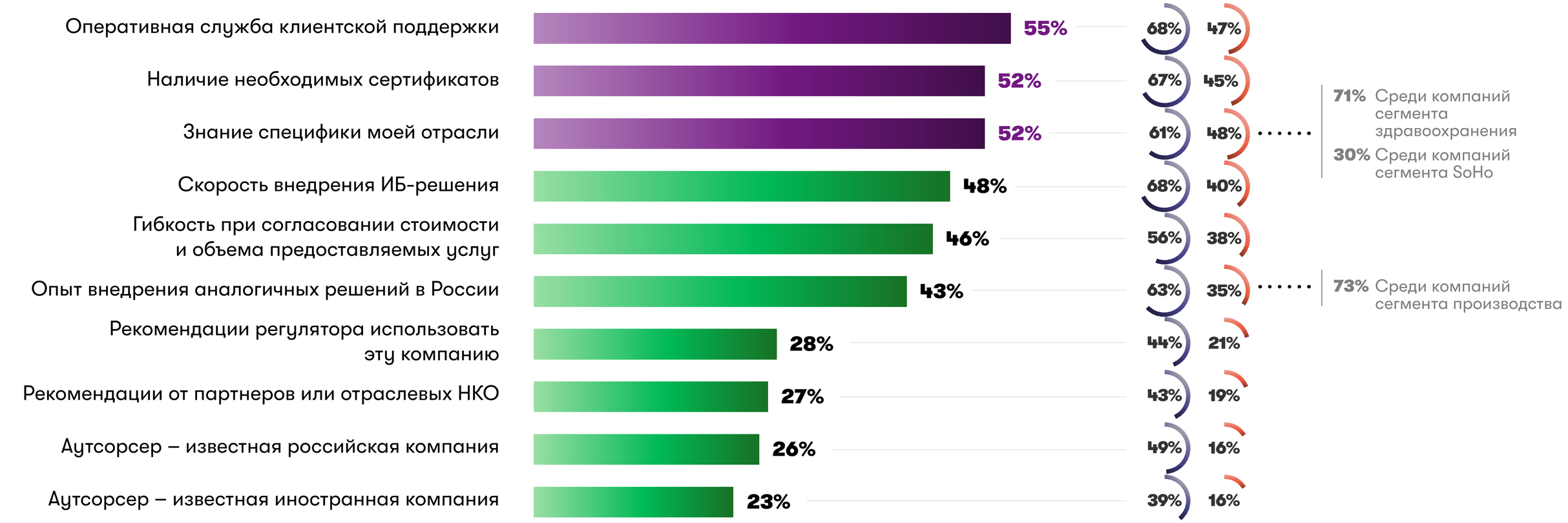


МегаФон

Критерии выбора аутсорсингового партнера

Техподдержка, наличие лицензий регуляторов, а также знание отрасли — наиболее важные параметры при выборе аутсорсинг-партнера. Для многих заказчиков также важно получать оперативное реагирование на свои запросы от сертифицированных ИБ-экспертов.

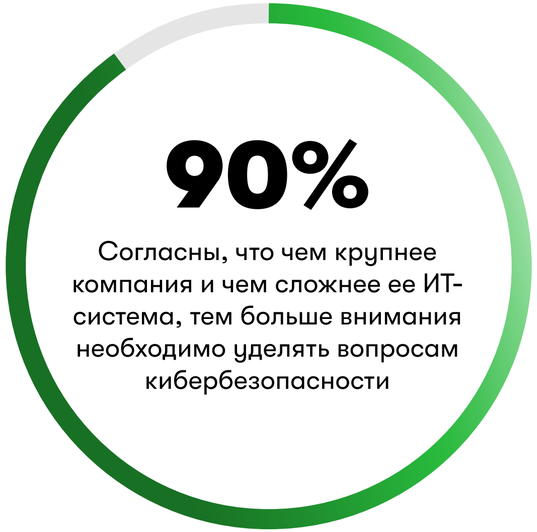
Наиболее важные параметры при выборе аутсорсинг-партнера

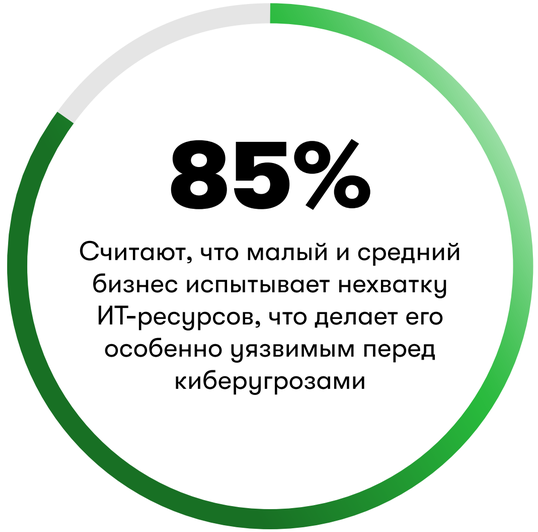


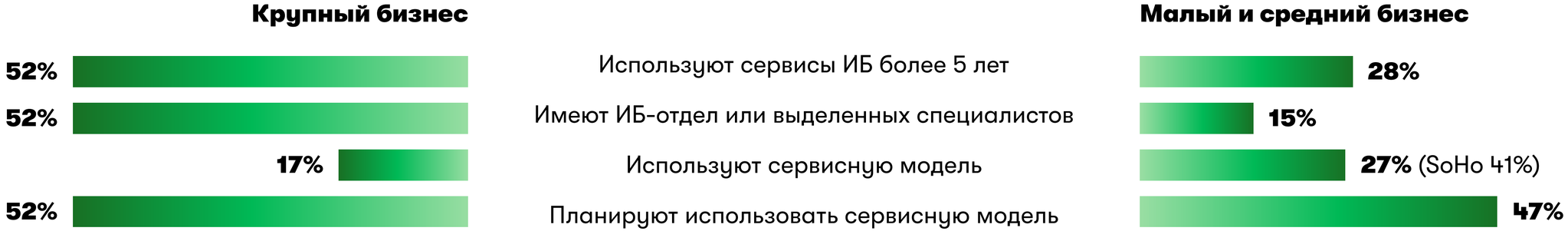
МегаФон

Особенности использования сервисов ИБ

Вопросы кибербезопасности актуальны как для крупных компаний с масштабной ИТ-инфраструктурой, так и для среднего и малого бизнеса, где трудно организовать работу по предотвращению киберугроз скромными ресурсами.



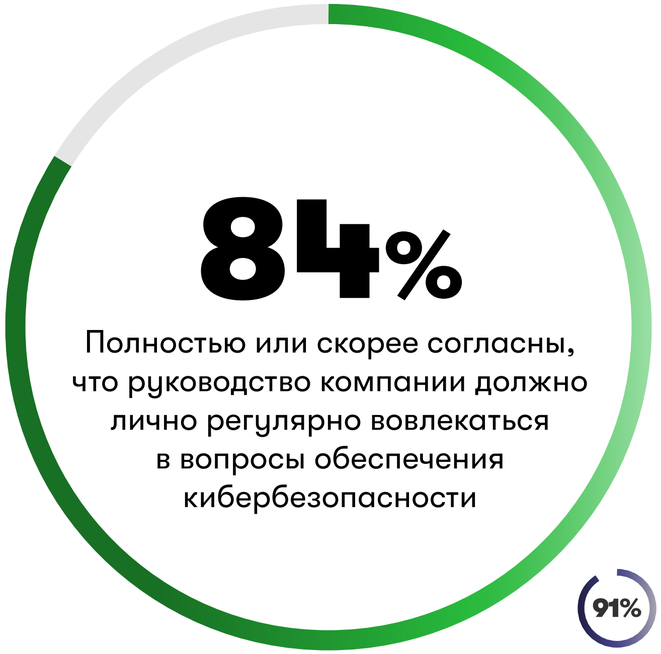




МегаФон

Роль руководства и сотрудников в кибербезопасности компании

В большинстве компаний согласны, что вовлекаться в обеспечение кибербезопасности должны не только ИТ- / ИБ-служба, но и все остальные сотрудники компании, включая руководство.



МегаФон

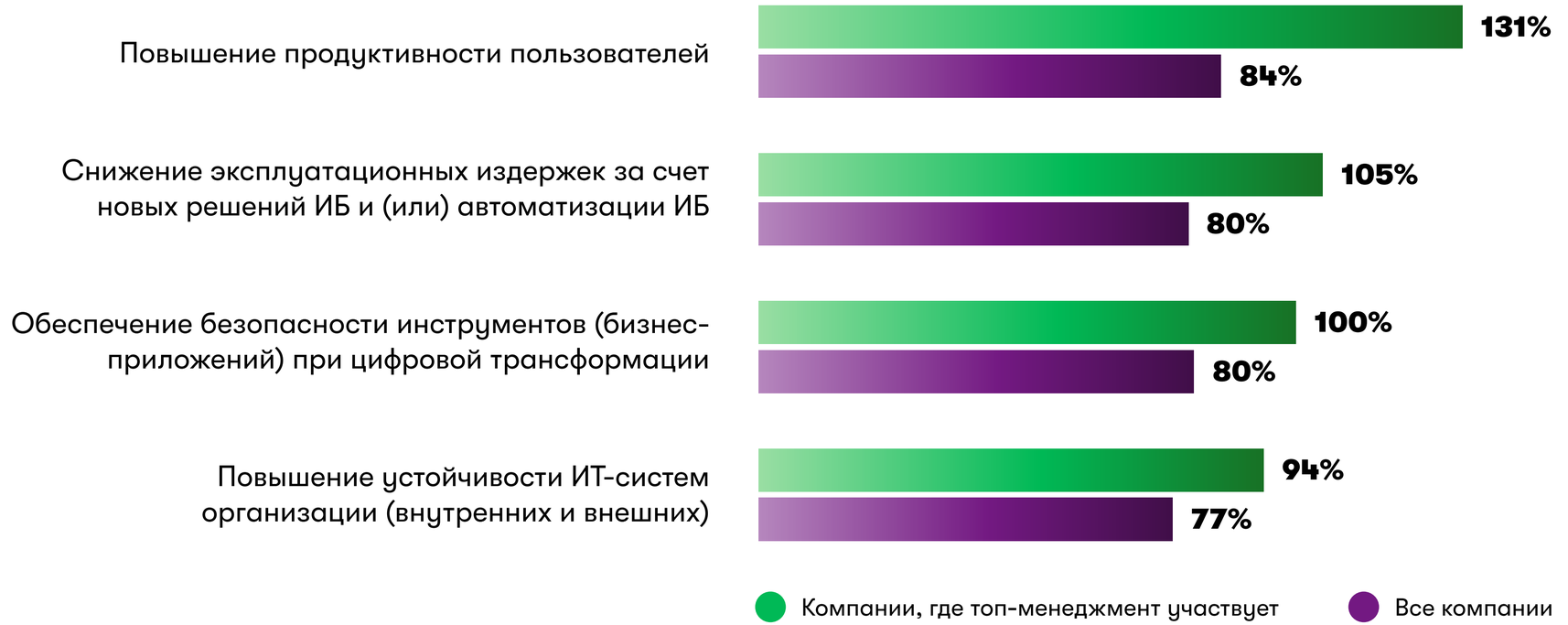
Высокий уровень цифровизации

Низкий уровень цифровизации

Влияние топ-менеджмента на выполнение целей по кибербезопасности

Вовлеченность топ-менеджмента в управление кибербезопасностью в компании повышает эффективность внедрения и использования сервисов ИБ в среднем на 30%.

Уровень выполнения целей (отношение поставленных целей к достигнутым)*

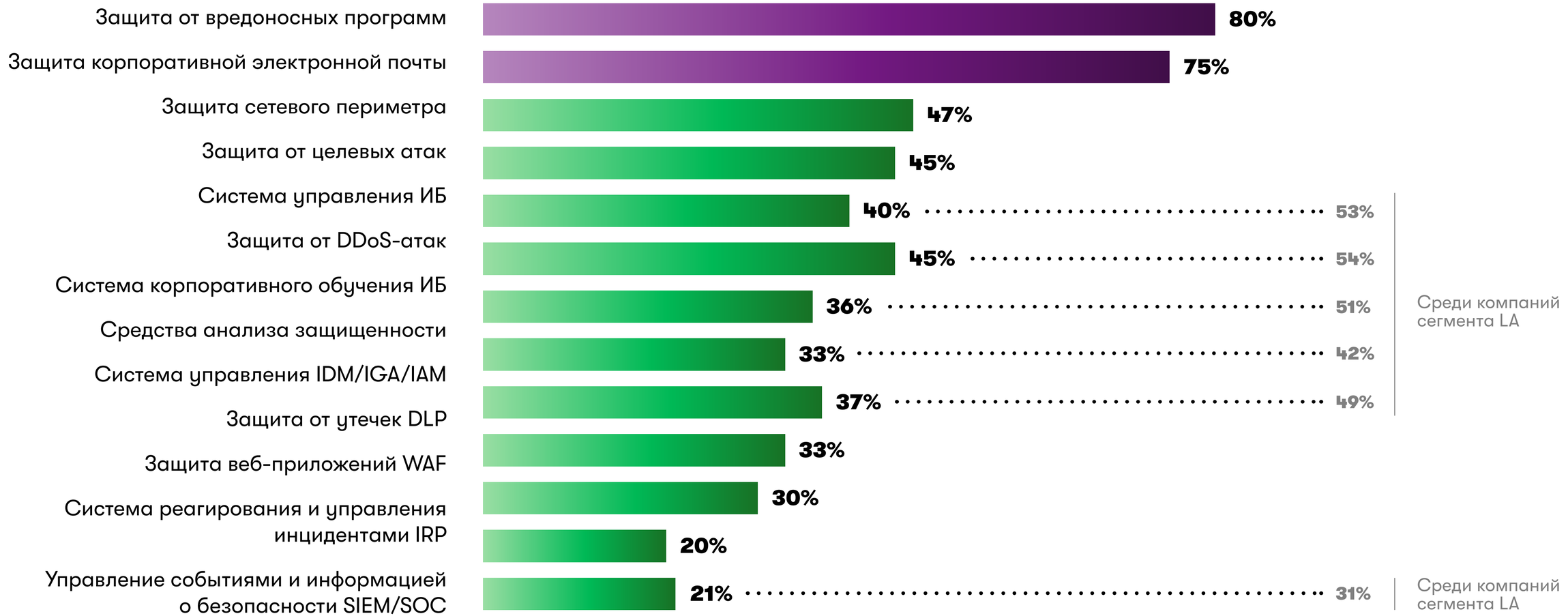


* Там, где значение превышает 100%, — цели не ставились, но достигнуты

МегаФон

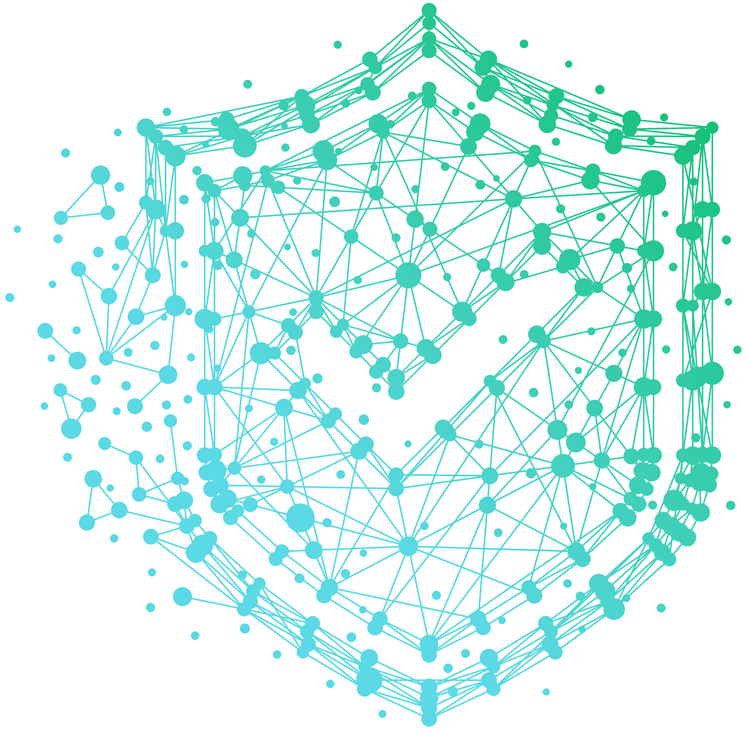
Использование сервисов ИБ

Крупные компании часто используют более широкий спектр решений по обеспечению кибербезопасности.



МегаФон

С МегаФоном твой бизнес сильнее



Узнай больше о сервисах кибербезопасности и используй актуальные технологии для защиты своего бизнеса

security.megafon.ru

МегаФон