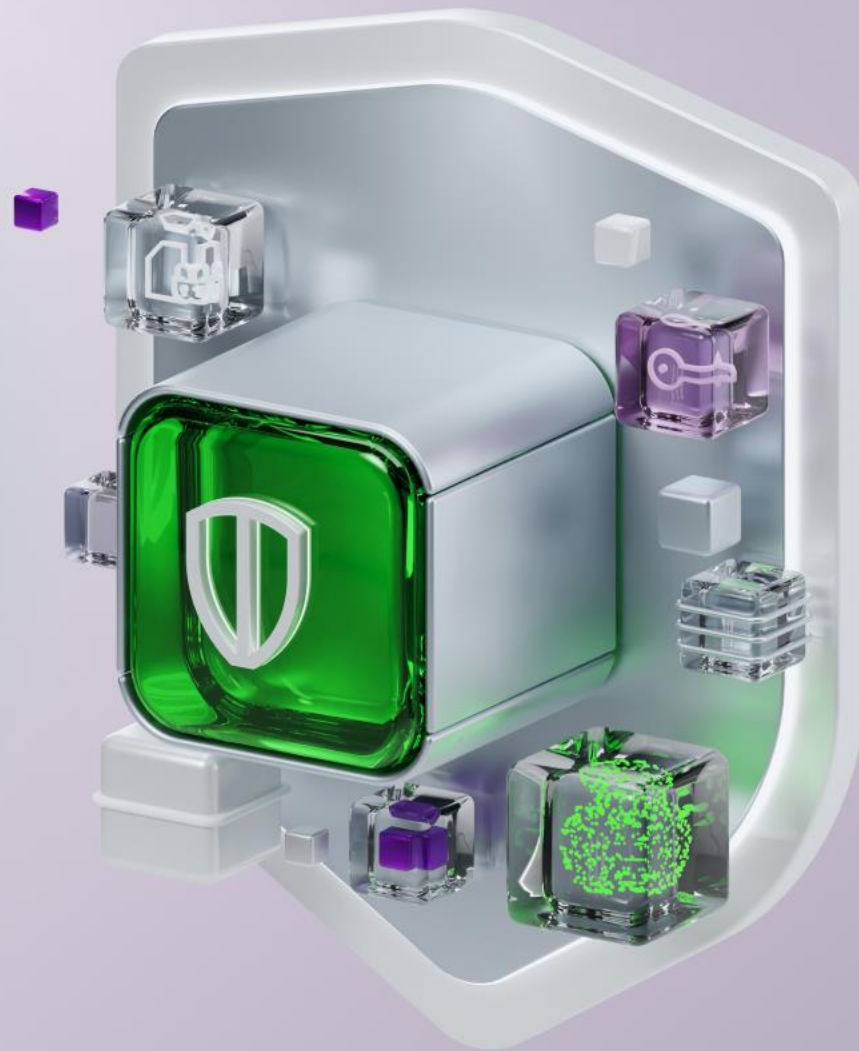


Индекс кибербезопасности

Аналитический отчёт об использовании
сервисов кибербезопасности в России



Введение

Кибербезопасность остается критической необходимостью для любого бизнеса. Высокая доля проникновения цифровых технологий в бизнес-процессы, от управления финансами до взаимодействия с клиентами, делает компании уязвимыми перед киберпреступниками. Хакеры разрабатывают все более изощренные методы взлома, используя искусственный интеллект и машинное обучение. Это требует от бизнеса постоянного обновления своих защитных механизмов и адаптации к новым угрозам.

Законодательство в сфере защиты данных продолжает ужесточаться: каждая компания должна соответствовать требованиям регуляторов. Компании, столкнувшиеся с крупными утечками данных, часто проходят через длительный период восстановления репутации, а также теряют лояльность своих клиентов.

Комплексный подход, включающий защиту сети, обучение сотрудников, внедрение систем обнаружения и реагирования на инциденты, является ключом к обеспечению надежной защиты от киберугроз. Обеспечение эффективной киберзащиты — стратегическое решение, определяющее конкурентоспособность и устойчивость компании в цифровой среде.

В обновленном исследовании мы вновь рассмотрели актуальные аспекты кибербезопасности, выяснили, изменилась ли роль ИБ-сервисов в бизнесе, визуализировали опыт и практику использования таких сервисов в динамике — с момента нашего последнего замера в 2022 году. Предлагаем вашему вниманию результаты исследования.

Вместе с аналитическим агентством ORO, мы изучили опыт **более 400** компаний разных сегментов и отраслей, использующих сервисы для обеспечения кибербезопасности.



Основные выводы

У бизнеса растет запрос на усиление защиты ИТ-инфраструктуры

62% компаний планируют рост бюджета на ИБ в следующем году. В 2022 году этот показатель находился на уровне 50%.

Помимо внешних угроз, основными драйверами называют необходимость защиты персональных данных, КИИ и противодействие социальной инженерии. Причем, планы по бюджетированию не зависят от того, столкнулась ли компания с инцидентом.

33% компаний, понесших ущерб, задумались о необходимости подключения услуг ИБ только после кибератаки. У компаний, не получивших ущерб, защищено на 15% больше ИТ-ресурсов.



Решения ИБ помогают минимизировать риски убытков и усилить конкурентоспособность

Главными целями внедрения ИБ-решений называют минимизацию убытков и повышение устойчивости ИТ-систем (36% и 34%, соответственно).

Помимо этого, использование ИБ-сервисов способствует укреплению доверия клиентов и партнеров, а также росту конкурентоспособности компаний. 48% компаний, которым удалось достичь лучшей конкурентоспособности, полностью удовлетворены результатами внедрения ИБ-сервисов.



Основные выводы

Помимо защиты от вредоносных программ и атак, есть потребность в анализе защищенности, управлении событиями и доступами

Защита от вредоносных программ и спама остаётся распространённой практикой (используют более 60% компаний). В 2024 году приоритет смещается к анализу защищенности (22%), управлению событиями и информацией о безопасности (19%, рост vs 2022), системам управления учетными записями и доступом (18%, рост vs 2022).

Хотя финансовые и кадровые ограничения остаются актуальными, их значимость снижается: компании реже говорят о том, что затраты на внедрение могут не окупиться или что трудно найти квалифицированных специалистов.



Потенциал использования сервисной модели растет

Уже 32% компаний (по сравнению с 22% в 2022 году) используют сервисную модель ИБ, еще 49% рассматривают ее внедрение. 64% компаний (на 10 п.п. больше, чем в 2022 году) планируют рост бюджета на сервисную модель.

Основными преимуществами сервисной модели остаются готовые процессы обеспечения ИБ, высокий уровень компетенций аутсорсинговой команды и быстрая адаптация защиты под новые угрозы.



Бизнес открыт к привлечению аутсорсинга ИБ-решений, но также сам активно вовлекается в обеспечение ИБ

43% компаний не имеют выделенных специалистов ИБ. Но половина из них собираются создавать ИБ-отдел, а другая половина — лояльны к использованию сервисной модели. У компаний со сформированным ИБ-отделом служба ИБ активно участвует в бизнесе компании.

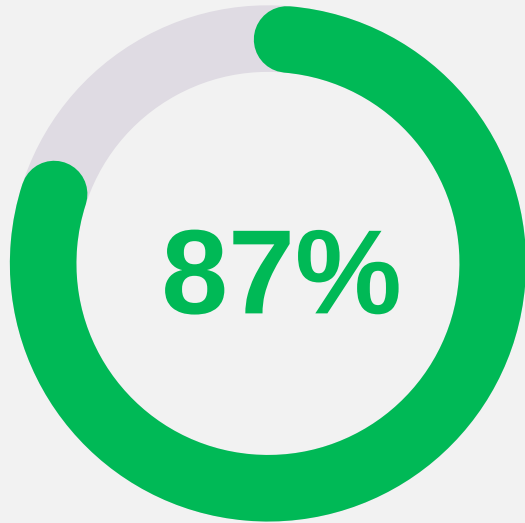
В 2024 году более 20% компаний частично или полностью передали ИТ-системы на аутсорс (больше, чем в 2022 году), и еще больше 50% готовы это сделать. Основные задачи аутсорсинговых команд — сканирование на уязвимости, мониторинг и анализ инцидентов, аудиты безопасности и обновление политик. При выборе аутсорсингового партнера ключевой фактор — оперативность реагирования.



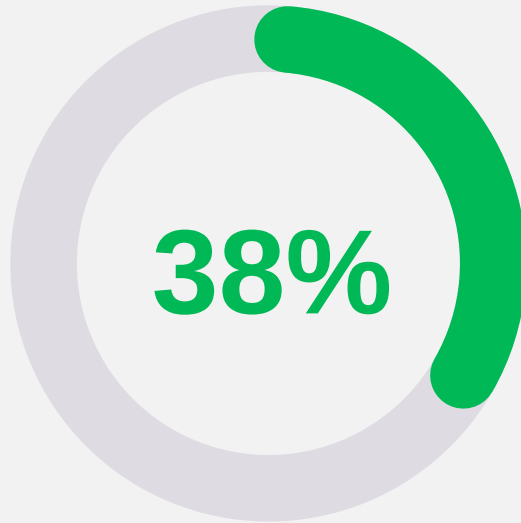
Риски и киберугрозы



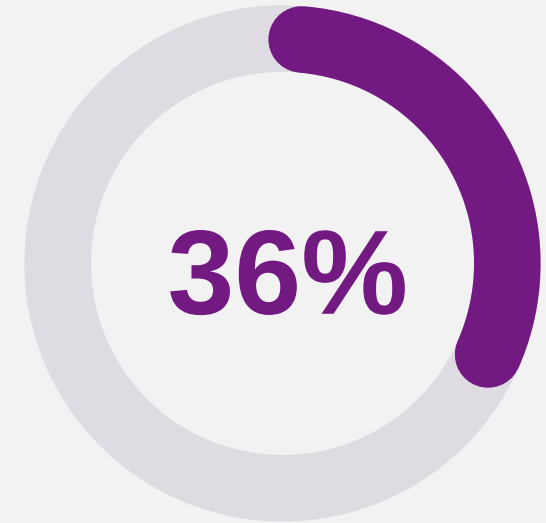
Почти все компании подверглись атакам в 2024 году, 38% из них понесли ущерб, в том числе финансовый



Подверглись
атакам



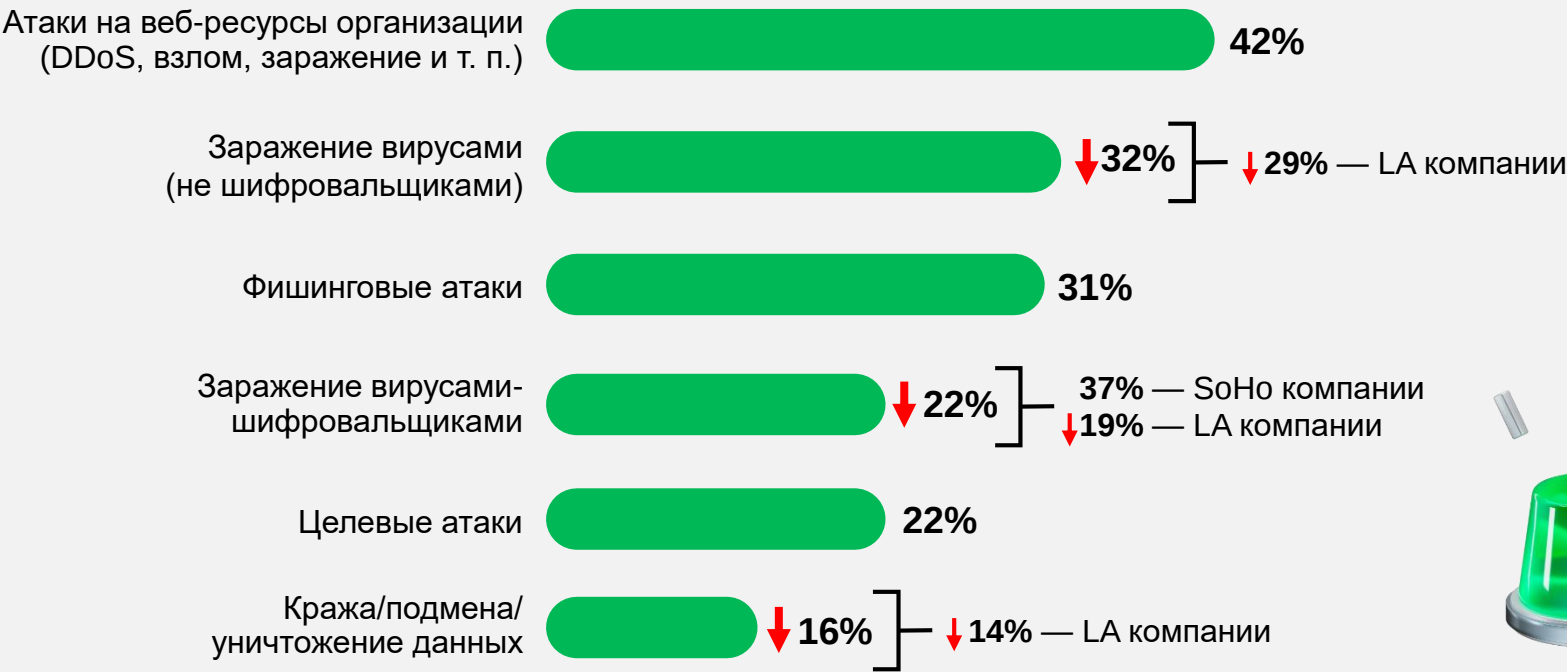
Понесли
ущерб



Понесли
финансовый
ущерб

42% компаний подверглись атакам на веб-ресурсы. Малый бизнес чаще сталкивался с заражением вирусами-шифровальщиками

Угрозы/атаки, с которыми столкнулись за год



Размер ущерба и типы кибератак

Наибольший урон компаниям продолжают нести атаки на веб-ресурсы (в том числе DDoS). Также более трети инцидентов связаны с целями кражи, подмены или уничтожения данных.

Типы угроз по размеру финансового ущерба среди компаний, столкнувшихся с кибератаками

	до 1 млн ₽	более 1 млн ₽
Атаки на веб-ресурсы организации (DDoS, взлом, заражение и т.п.)	42%	58%
Заражение вирусами (не шифровальщиками)	41%	35%
Фишинговые атаки	33%	35%
Заражение вирусами-шифровальщиками	29%	24%
Целевые атаки	28%	21%
Кража/подмена/уничтожение данных	24%	36%

33%

компаний понесли финансовые убытки свыше 1 млн ₽, в среднем ущерб составил 20–30 млн ₽.



47% компаний понимают важность обеспечения информационной безопасности и внедряют сервисы ИБ превентивно

Почему компании внедряли решения по кибербезопасности:

47%

Превентивно, из-за роста киберугроз

23%

По требованию регулятора



9%

После киберинцидента
(с ущербом)

31%

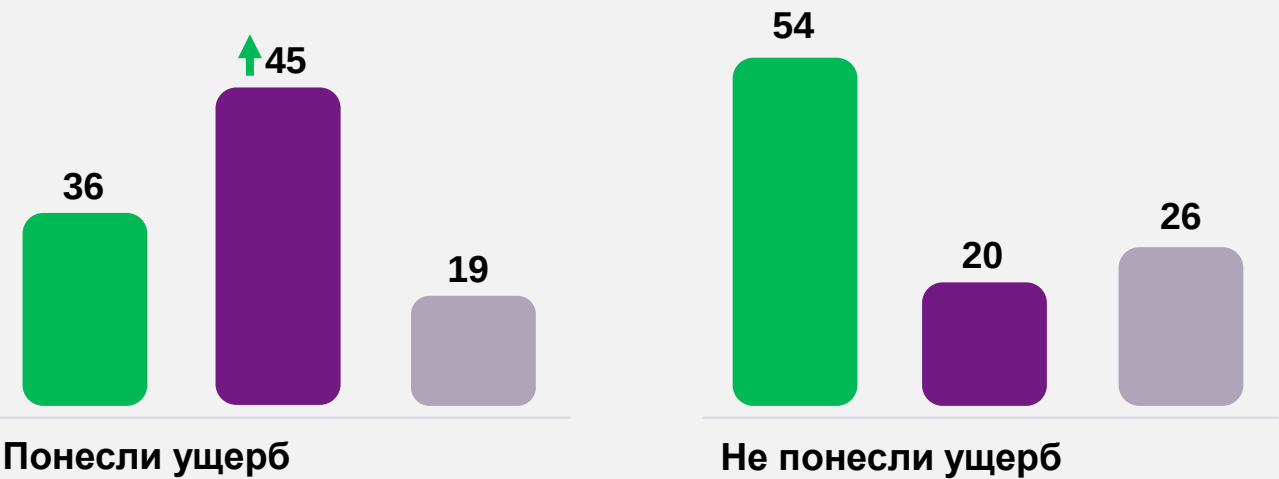
Из них относится
к отрасли «финансы
и страхование»

20%

После киберинцидента
(без ущерба)

Компании, понесшие ущерб, чаще остальных стали использовать сервисы ИБ после инцидента

Предпосылки к использованию сервисов ИБ, %



- Превентивно, из-за роста киберугроз
- После киберинцидента
- По требованию регулятора

В киберзащите по-прежнему важен комплексный подход

Компании, которые не понесли ущерб в 2024 году, имели под защитой ИБ больше ИТ ресурсов организации.

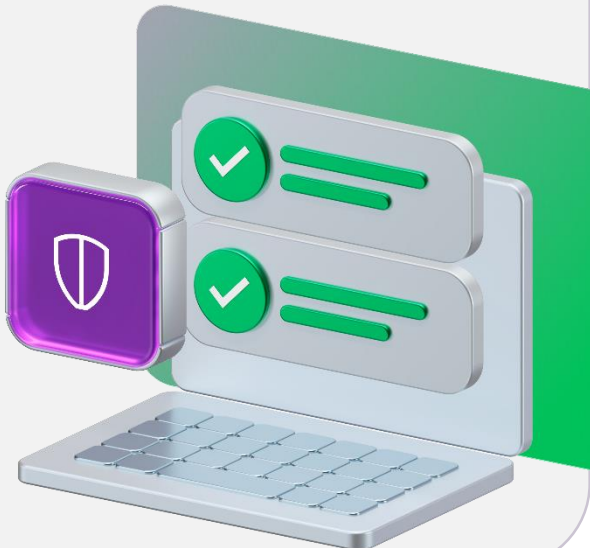
Какие системы защищены у компаний, которые не понесли ущерб при киберинцидентах, %



Компании стремятся защитить основные ИТ-системы

В 2025 году больше трети компаний крупного и среднего бизнеса планируют начать защищать бизнес-приложения и облачные платформы.

Для каких ресурсов компании используют средства киберзащиты, %



Роль сервисов кибербезопасности и их применение



Главными целями внедрения услуг кибербезопасности остаются минимизация рисков финансовых потерь и повышение устойчивости ИТ-систем



Использование сервисов ИБ

К базовым средствам защиты компании планируют подключать средства анализа защищенности, управления событиями и информацией о безопасности.



Экспертиза и опыт разработчика, а также скорость работы решения остаются ключевыми факторами при выборе ИБ-сервисов

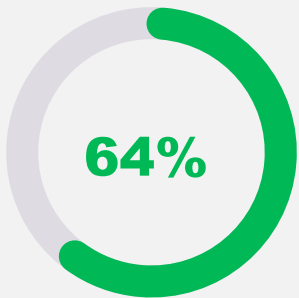
Параметры при выборе ИБ-решений, %



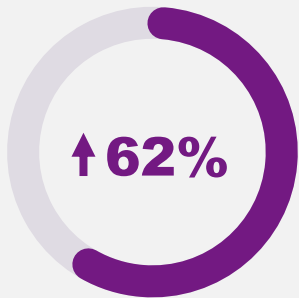
Бюджетирование ИБ



Компании планируют больше инвестировать в развитие ИТ- и ИБ-систем в 2025 году, в том числе и те, кто не понес ущерба от кибератак



Увеличивают бюджет на ИТ в 2025 году



Увеличивают бюджет на ИБ в 2025 году



↑ 59% Планируют увеличить бюджет на ИБ в 2025 году, но ущерба не понесли

68% Понесли имиджевый или финансовый ущерб и планируют увеличить бюджет на ИБ в 2025 году

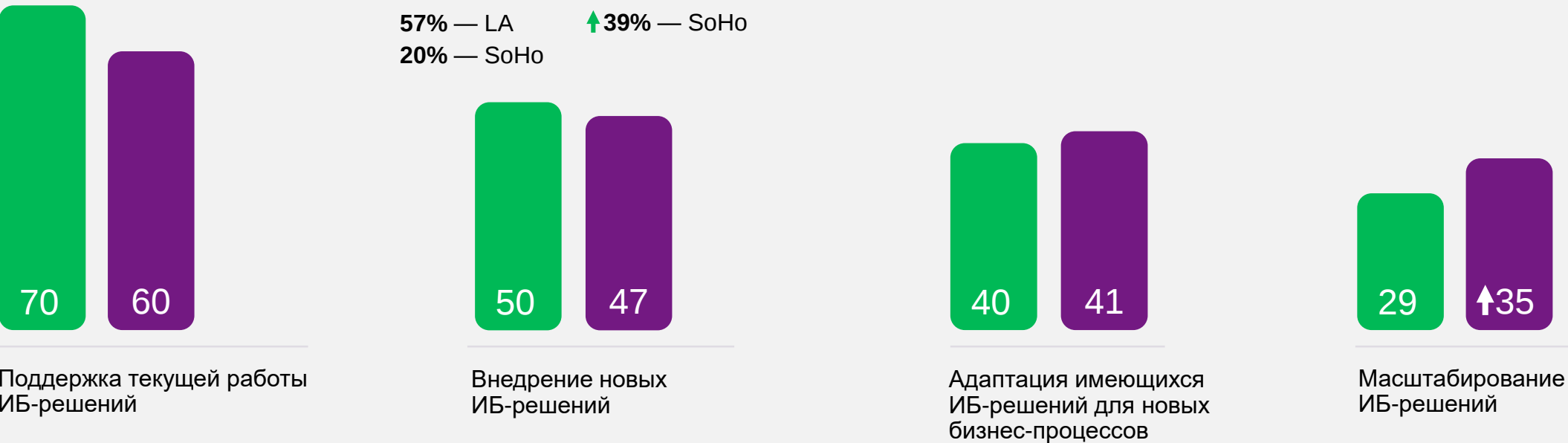
В 2025 году компании планируют выделять на ИБ большую долю средств, чем сейчас — до 15% от бюджета в среднем

13%
тратили в среднем бюджета на ИБ

15%
планируют потратить на ИБ в 2025

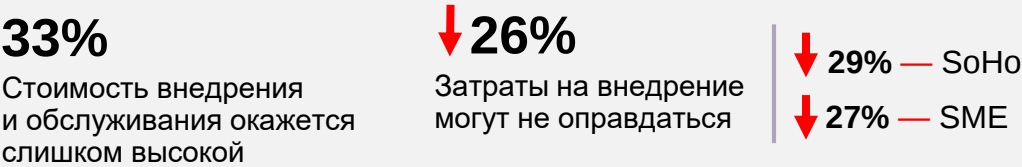
Увеличение доли бюджета на ИБ связано с тем, что на текущий момент все больше компаний планируют масштабировать свои ИБ-решения

Текущие затраты на сервисы ИБ включают, %



Ключевыми рисками при внедрении ИБ остаются стоимость и нехватка квалифицированных кадров

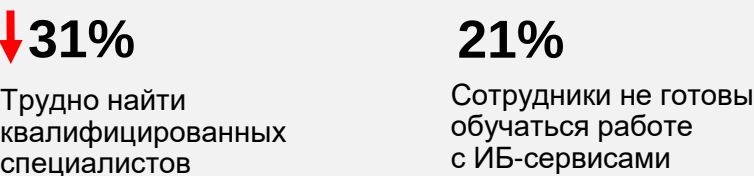
Финансовые



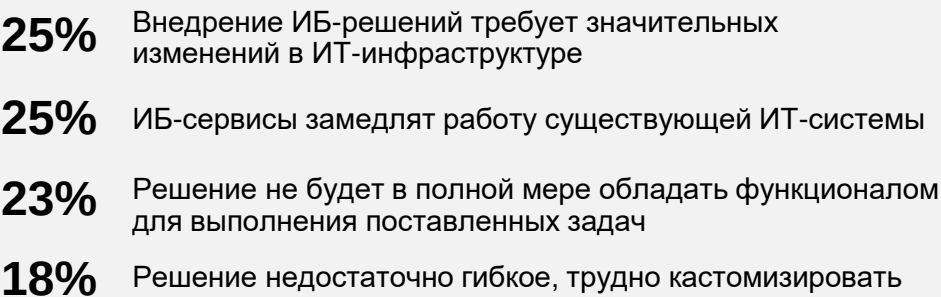
Проблемы с поддержкой



Проблемы, связанные с персоналом



Проблемы с функционалом



Аутсорсинг сервисов ИБ



В 2024 году растет популярность сервисной модели: треть компаний уже использует ее, еще половина — планируют начать

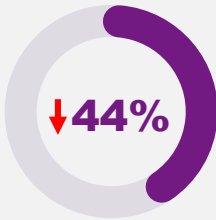


Готовых процессы и компетенции для обеспечения ИБ, а также быстрая адаптация — основные преимущества сервисной модели

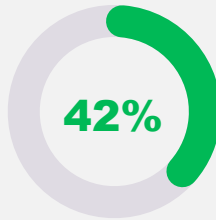
Преимущества сервисной модели ИБ по сравнению с традиционной



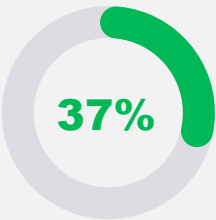
Готовые процессы обеспечения ИБ



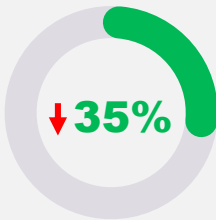
Более высокий уровень компетенций по сравнению со штатными ИБ-специалистами
↓41% — LA



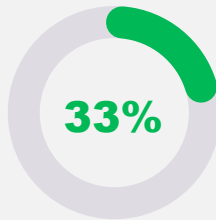
Более быстрая адаптация защиты под новые и развивающиеся угрозы



Сокращение расходов на оплату ИБ-специалистов



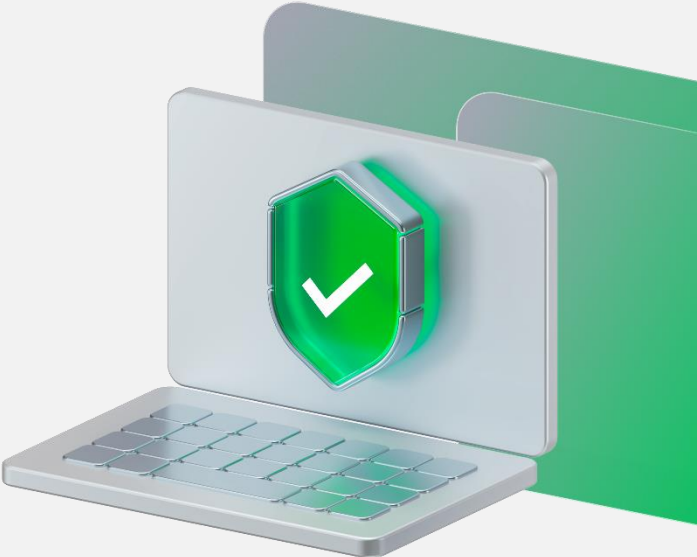
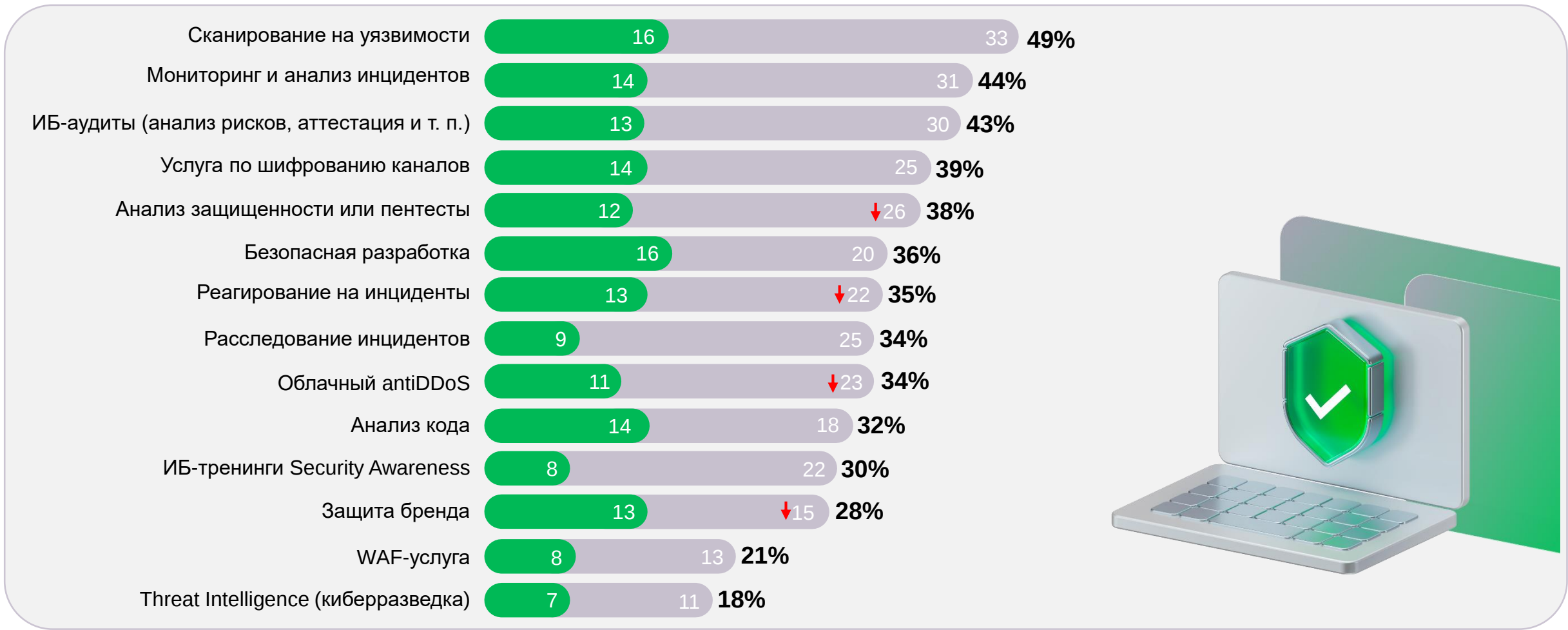
Сокращение времени на внедрение/запуск ИБ-решения
↓36% — LA
↓31% — SME



Сокращение затрат на приобретение ИБ-решений

Востребованность услуг аутсорсинга ИБ

Наибольшей востребованностью среди аутсорсинговых ИБ-услуг продолжает пользоваться сканирование уязвимостей: сервис уже используется или планируется к внедрению в 49% компаний.



Критерии выбора аутсорсингового партнера

При выборе аутсорсинговой компании бизнес ориентируется на наличие сертификатов, оперативность поддержки и скорость внедрения. С 2024 года возросла роль рекомендаций поставщиков со стороны регулятора.

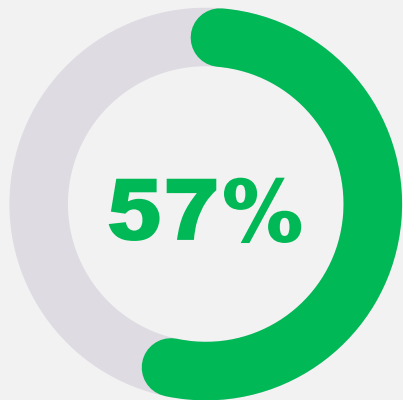


Организация ИБ в компаниях



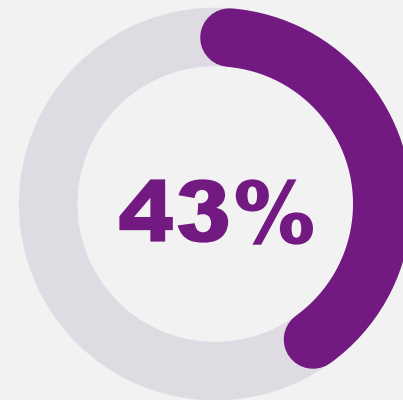
Организация ИБ-процессов в компаниях

У 43% компаний нет выделенного ИБ-отдела или специалистов, но половина из них планирует его создать. Те же, кто продолжит обходиться без ИБ-отдела, уже пользуются услугами ИБ по сервисной модели или рассматривают такой вариант.



компаний имеют выделенных
ИБ-специалистов или ИБ-отдел

17% — среди компаний сегмента SoHo
28% — среди компаний сегмента SME
39% — среди компаний сегмента LA



компаний не имеют выделенных
ИБ-специалистов или ИБ-отдела

50% — Планируют создать ИБ-отдел
50% — Не планируют создавать ИБ-отдел
42% — Рассматривают использование сервисной модели
32% — Не используют и не рассматривают
25% — Используют сервисную модель

Почти все компании удовлетворены результатами внедрения ИБ-решений: треть из них — полностью удовлетворены



31%

Полностью
удовлетворены



63%

Скорее
удовлетворены



6%

Скорее
не удовлетворены



МЕГАФОН

ПроБизнес
ТЕХНОЛОГИИ ЛИДЕРСТВА



**Узнайте больше
о решениях
кибербезопасности**