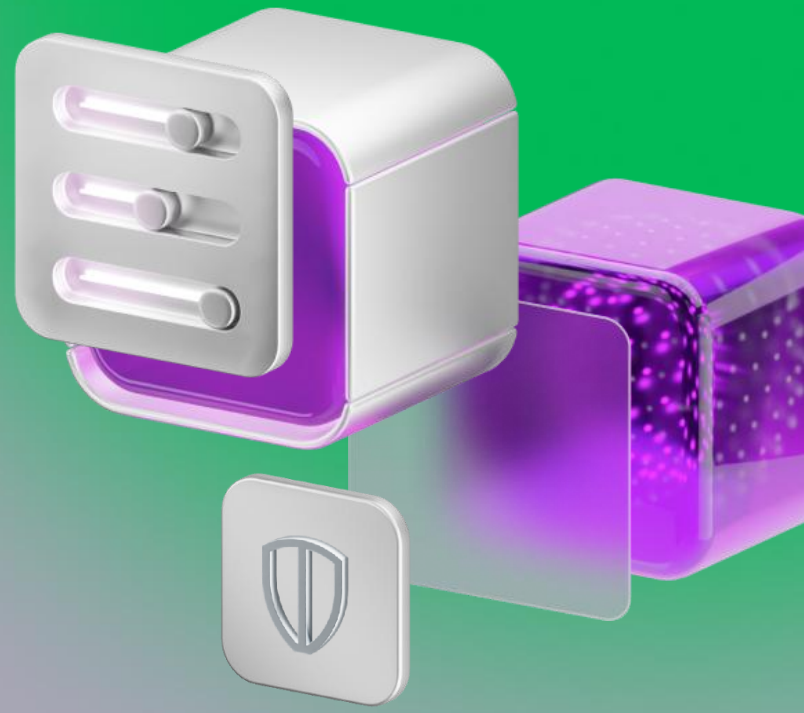
МегаФон | ПроБизнес
ТЕХНОЛОГИИ ЛИДЕРСТВА

От вызовов к итогам: МегаФон SOC



Роман Соловьев
Эксперт по продуктам
направления кибербезопасности

8 (936) 192-30-33
Roman.V.Solovyev@megafon.ru

Количество кибератак продолжает расти

В рамках исследования «Индекс Кибербезопасности в России»[1] было опрошено 400 представителей компаний разных отраслей, которые используют сервисы по обеспечению кибербезопасности. Из них

87%

компаний подвергались кибератакам в 2024 году.

40% - 765 тыс.

Зарегистрированных преступлений в России в 2024 г – преступления с использованием ИТ [2]

33%

Опрошенных компаний[1] понесли финансовые потери свыше 1 млн рублей

25 млн. ₽

средний ущерб от атаки

МегаФон | ПроБизнес

[1] Исследование компании «МегаФон» и аналитического агентства ORO 2025 г..
[2] По данным ТАСС

Угроза становится серьезнее с каждый годом

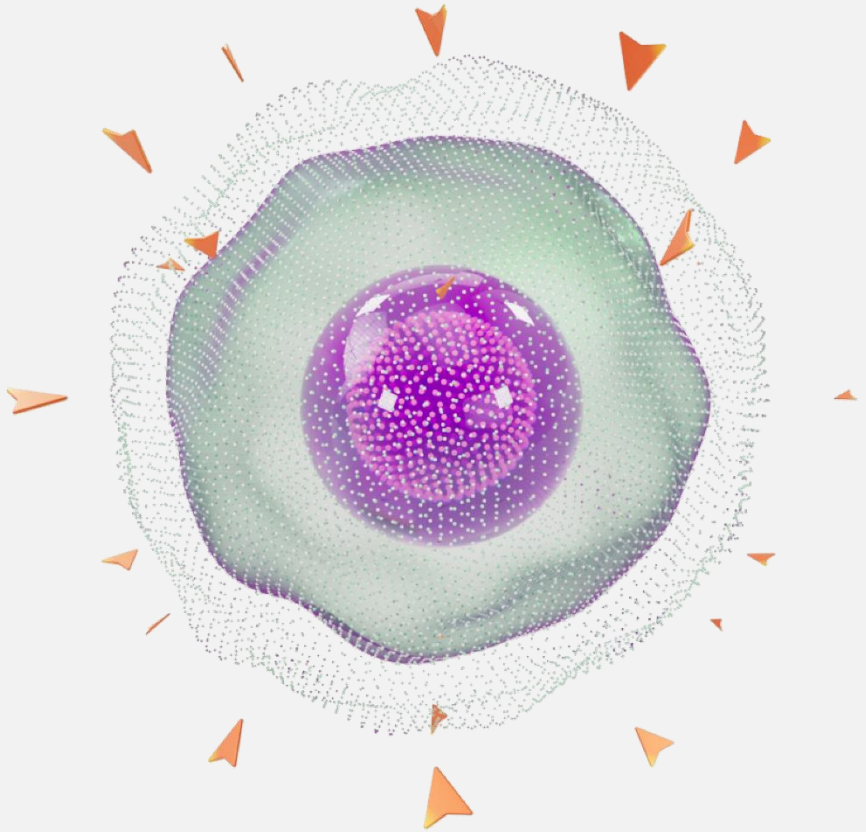
Наблюдается кратный рост кибератак на российские организации

×9,6

увеличилось количество атак на инфраструктуру клиентов

×5

увеличился спрос на сервисы кибербезопасности

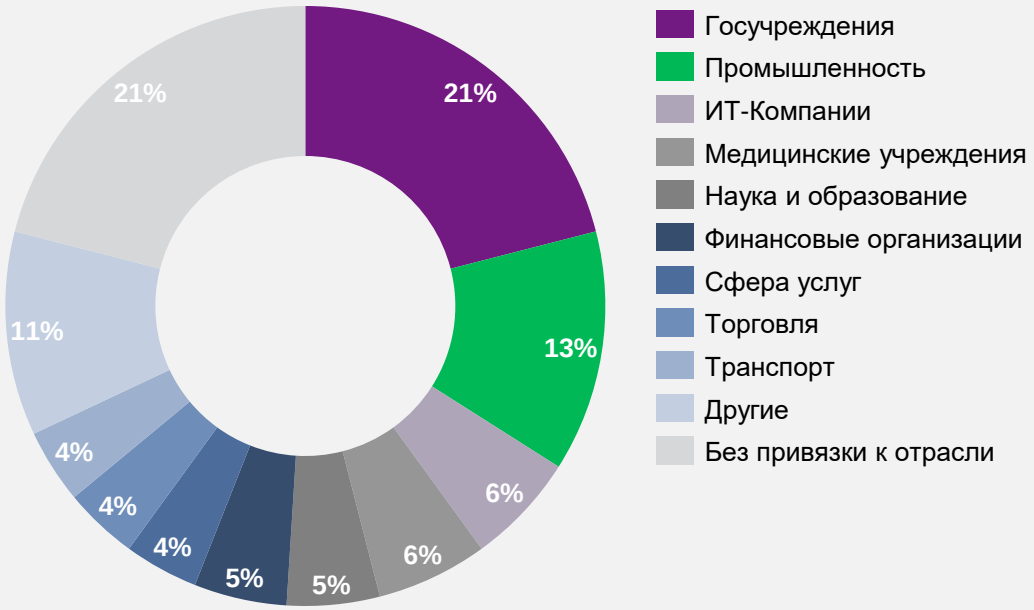


МегаФон | ПроБизнес

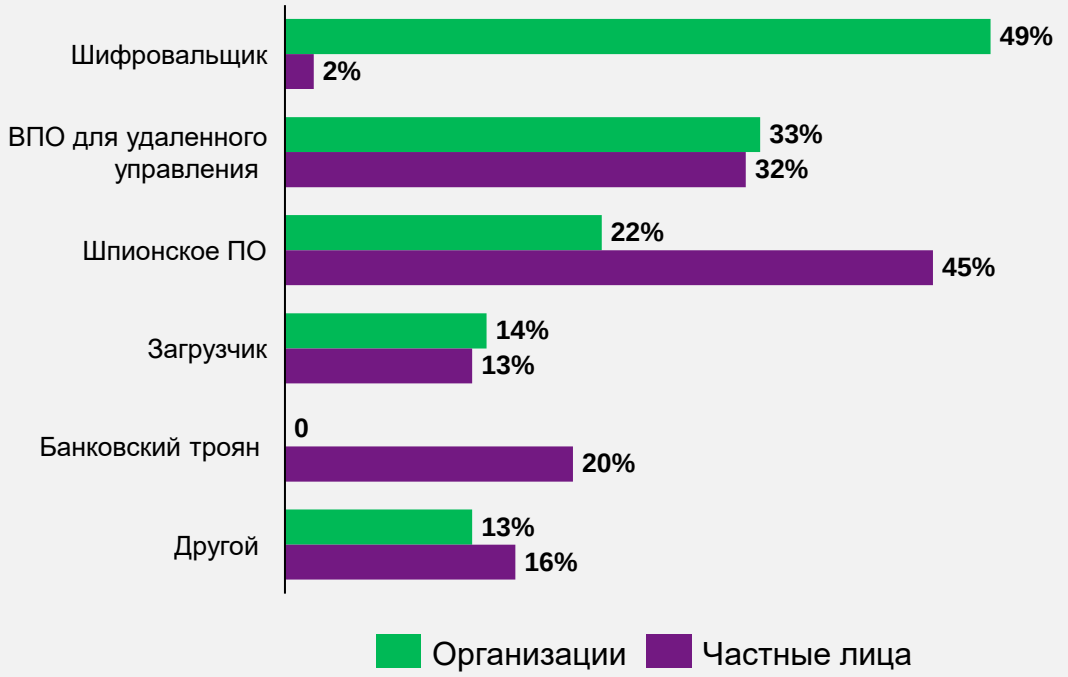
По данным исследования компании «МегаФон» «Индекс Кибербезопасности в России» в 2024 г. Опрошено 400 представителей компаний разных отраслей, которые используют сервисы по обеспечению кибербезопасности (опрос 2023 г.).

ВПО на сферы деятельности

Доля успешных атак на организации, H1 2025



Доля успешных атак с использованием вредоносного ПО, H1 2025



По данным исследования Positive Technologies «Актуальные киберугрозы: I–II кварталы 2025 года»

Кибератаки стали и сложнее, и «дешевле»

Согласно данным Positive Technologies Expert Security Center за четвертый квартал 2024 года и первый квартал 2025 года, основным инструментом злоумышленников остается вредоносное ПО

В 2 раза выросло количество инцидентов, вызванных атаками путем компрометации поставщиков ПО или оборудования, а также путем компрометации доверенной третьей стороны (атака через подрядчика)

Рост искусственного интеллекта, включая генеративные системы, и увеличивает сложность кибератак и позволяет сделать атаки «дешевыми» для злоумышленников, что позволит выгодно атаковать и сегмент малого и среднего бизнеса

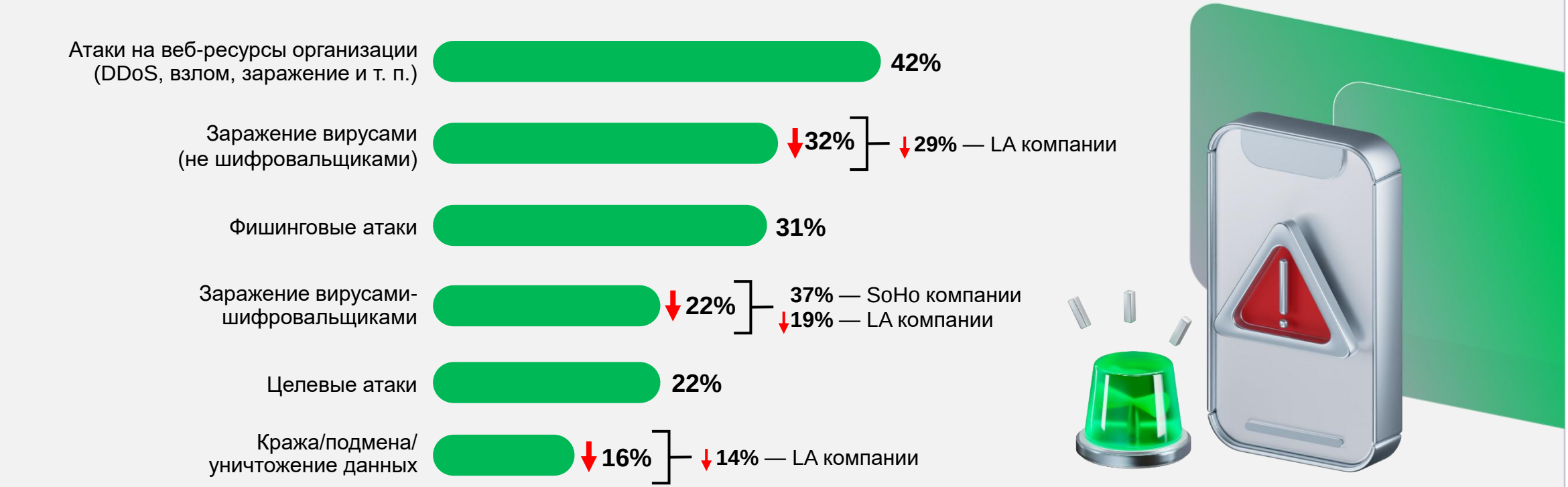
В качестве исходного вектора проникновения злоумышленники чаще всего эксплуатировали уязвимости ИТ-систем и методы социальной инженерии

МегаФон | ПроБизнес

[1] На основе данных отчета Kaspersky и К2: «Барьеры и драйверы российского бизнеса при организации процессами управления киберинцидентами и использовании SOC»

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.

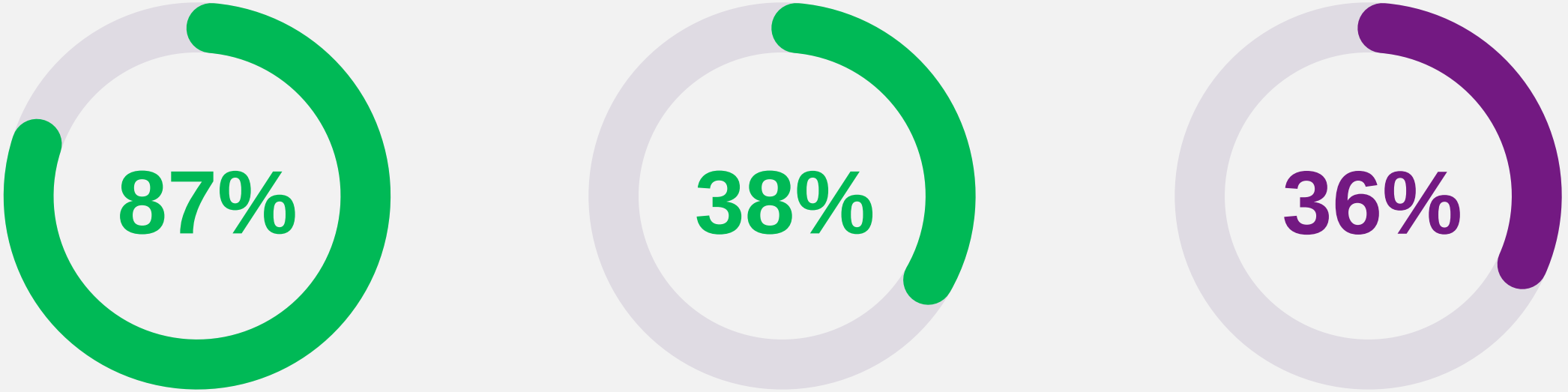
Типы угроз по размеру финансового ущерба среди компаний, столкнувшихся с кибератаками

	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 свыше1 млн ₽, в среднем ущерб составил 20–30 млн ₽.

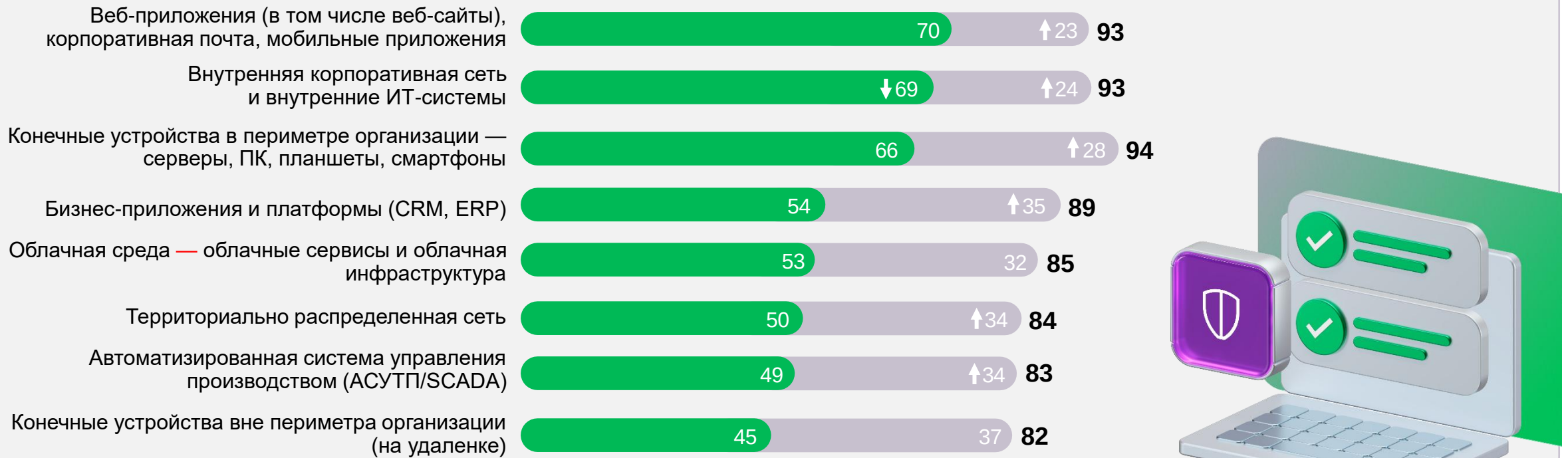
Почти все компании подверглись атакам в 2024 году, 38% из них понесли ущерб, в том числе финансовый



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, %



МегаФон | ПроБизнес

— Уже защищено, %

— Планируется защищать, %

↑↓ Значимо выше / ниже, чем 2022 году

Индекс кибербезопасности

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

МегаФон | ПроБизнес

— Уровень достигнутой цели, %

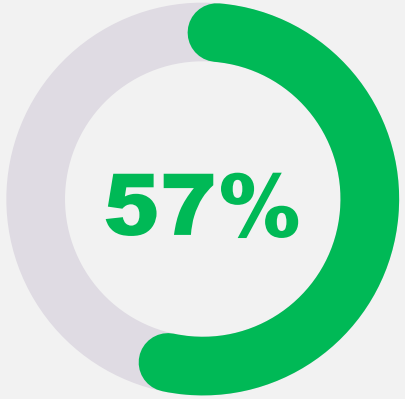
— Уровень поставленной цели, %

Значимо выше / ниже, чем 2022 году

Индекс кибербезопасности

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

МегаФон успешно помогает защищать бизнес и государство от современных киберугроз

2547+

клиентов

Уже активно пользуются услугами и сервисами кибербезопасности от МегаФон

>22

продуктов кибербезопасности

- МегаФон SOC
- Защита от DDoS
- Услуги Антифрода
- Security awareness
- Платформа киберразведки
- Управление уязвимостями
- Безопасность сетей и приложений (WAF, NGFW, IDPS)
- Анализ защищённости ИТ-инфраструктуры
- Криптозащита и.т.д

>11

лет на рынке

Соответствие мировым стандартам

PCI DSS, ISO 27001, ISO 27017, ISO 27018, ISO 9001, ISO 20000

Полностью российские решения

Решения добавлены в реестр российского программного обеспечения

Высший уровень защищенности

УЗ-1, К1, 1Г. Решения сертифицированы ФСТЭК и ФСБ России, соответствуют требованиям № 152-ФЗ

МегаФон | ПроБизнес

МегаФон SOC

МегаФон Security Operation Center – коммерческий центр мониторинга и реагирования на инциденты информационной безопасности, обеспечивающий защиту в режиме 24/7 для эффективного противодействия кибератакам любого уровня сложности

Анализируемых событий ИБ в сутки

20 млрд

Активов на мониторинге от самого крупного клиента

4000+

Пиковая нагрузка по EPS

>540 000

Гибкие сценарии оповещения сотрудников заказчиков

8+ ИТ отделов

Собственные правила корреляции и сценарии реагирования

600+

МегаФон является аккредитованным Центром ГосСОПКА, Класса А

МЕГАФОН | ПроБизнес

МегаФон помогает организациям на всех этапах защиты

Консалтинг

Помощь в проведении аудитов и прохождении категорирования ИТ-инфраструктуры Заказчиков

Выявление

Круглосуточный мониторинг и анализ событий информационной безопасности, раннее детектирование типовых и сложных атак

Реагирование

Оперативное реагирование на инциденты информационной безопасности, своевременное уведомление клиента

Устранение и расследование

Консультационная помощь в ликвидация последствий инцидента, разработка подробных рекомендаций по устранению причин возникновения

Прогнозирование

Проактивный поиск и обнаружение угроз с использованием собственной системы киберразведки, обогащенной данными лидеров рынка и собственными аналитиками

Профилактика

Регулярный анализ ИТ-инфраструктуры и процессов на предмет выявления уязвимостей и определения возможных рисков для компании

Преимущества работы с МегаФон SOC

- Уникальные компетенции собственной смены и аналитиков SOC
- Круглосуточная поддержка: три линии поддержки по уровню экспертизы для оперативного реагирования на атаки любой сложности
- Полный спектр услуг у одного поставщика
  Предоставление дополнительных СЗИ по подписке
- Сертифицированные решения от ведущих вендоров
  SLA 99,7% режим работы 24/7
- Гибкое ценообразование за счет работы с решениями разных вендоров и использования собственных облачных ресурсов
- Собственные каналы связи с высокой надежностью
  И уникальные данные с мобильной сети
- Защищенное облако соответствующее всем стандартам безопасности
- Своевременное отслеживание изменений в технологиях и законодательстве

МЕГАФОН | ПроБизнес
ТЕХНОЛОГИИ ЛИДЕРСТВА

Роман Соловьев
Эксперт по продуктам
направления кибербезопасности
8 (936) 192-30-33
Roman.V.Solovyev@megafon.ru

Оставить заявку