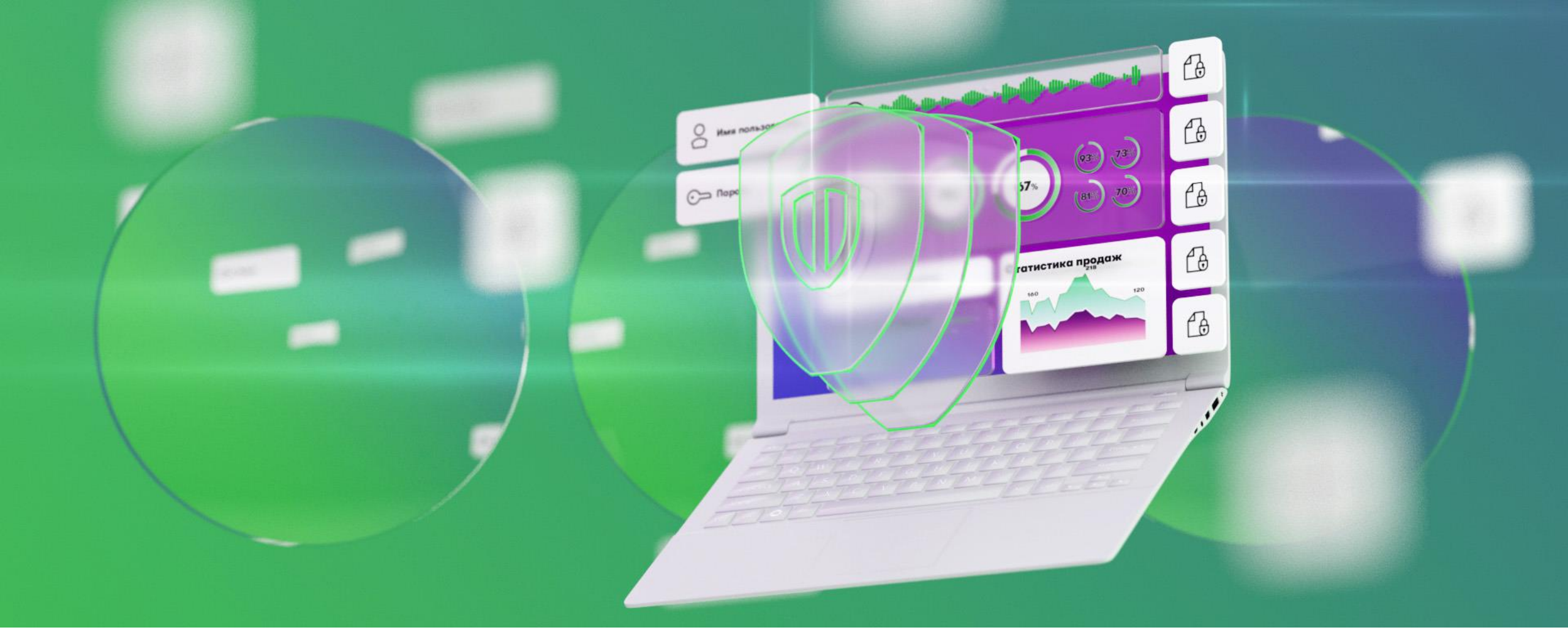
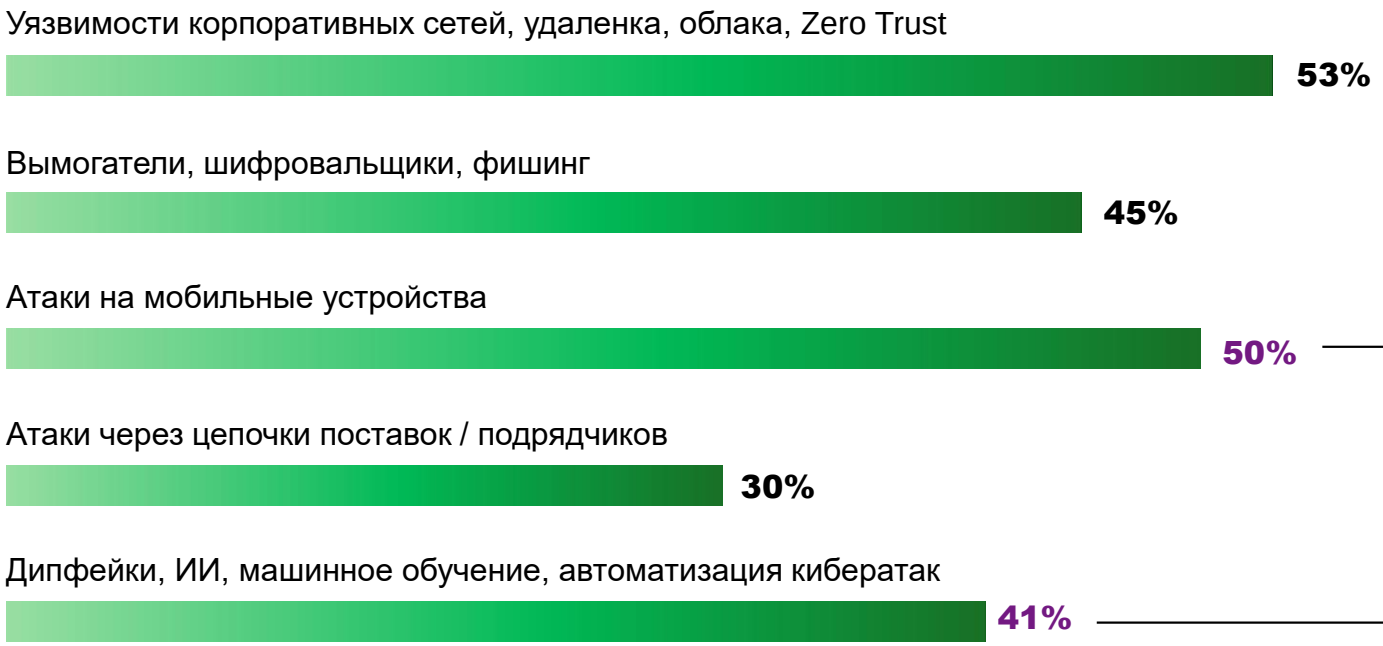


MSSP – как рецепт успешной смены парадигмы

МегаФон | ПроБизнес

Быстрорастущие угрозы

Какие угрозы приобретают наибольшее распространение:



Упоминаются

×1,5 раза чаще

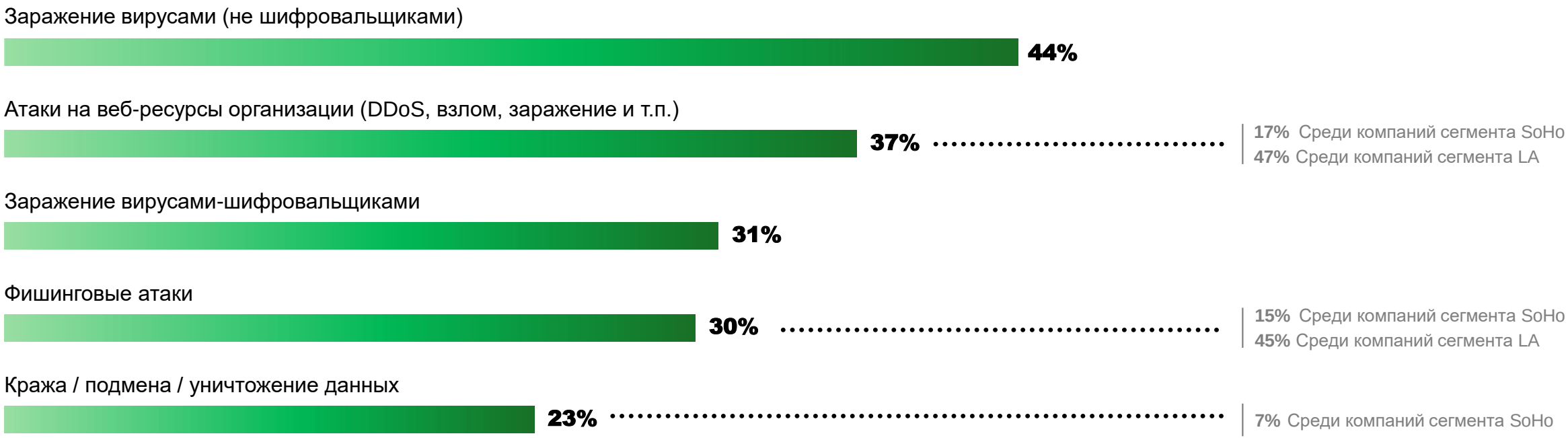
В 2022 году в сравнении с 2021 годом

ПроБизнес

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

Киберугрозы, с которыми столкнулись компании за год

Угрозы / атаки, с которыми столкнулись за год:



ПроБизнес

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

К чему все приводит?

rbc.ru
https://www.rbc.ru › ✅Общество

[СК возбудил уголовное дело после утечки данных ... - РБК]

6 авг. 2022 г. — Из-за **утечки** Роскомнадзор составил на «**Яндекс.Еду**» протокол за нарушение российского законодательства в сфере **персональных дан**

Стало известно о рекордной утечке данных клиентов СДЭК

РБК: данные 25 миллионов клиентов СДЭК попали в сеть

Стало известно о новой утечке данных клиентов компании СДЭК, которая могла коснуться 25 миллионов пользователей и

bfm.ru
https://www.bfm.ru › news

«Гемотест» подтвердил утечку данных 30 млн клиентов

18 мая 2022 г. — «**Гемотест**» обратился в правоохранительные органы. В начале м анонимных телеграм-каналах появились сведения об **утечке** данных 30 млн кл

ria.ru
https://ria.ru › Новости

Данные о заказах клиентов Delivery Club вновь утекли в Сеть

10 июн. 2022 г. — Второй файл с 1,2 миллиона строк данных о заказах клиентов **Delivery Club** был опубликован в интернете, сообщается в Telegram-канале "**Утечки** ...

ФТС сообщила о DDoS-атаках. Сервисы отключены

28 февраля 2023 года Федеральная таможенная служба (ФТС) технологическую инфраструктуру, в результате возникли проблемы в

ВТБ переживает крупнейшую DDoS-атаку в своей истории

6 декабря 2022 года представители ВТБ сообщили TAdviser о том, что технологическая инфраструктура банка находится под «беспрецедентной кибератакой из-за рубежа». По их словам, она стала крупнейшей не только в 2022 году, но и за все время работы банка. Подробнее здесь.

Зафиксирована мощнейшая в истори
DDoS-атака на российских брокеров

Крупные инциденты

В марте 2022 г. CNews писал о том, что в работе популярного в России интернет-магазина Wildberries произошел крупномасштабный сбой. Клиенты долгое время не могли сделать новый заказ, применить скидку и авторизоваться в профиле. Во время неполадок служба информационной безопасности сервиса доставки СДЭК разослала своим сотрудникам предупреждение о кибератаке на Wildberries с советом вывести деньги, заблокировать и перевыпустить карту, привязанную к маркетплейсу. Эксперты заявляли, что Wildberries стал жертвой масштабной атаки вируса-шифровальщика.

ПроБизнес

Вызовы

Указ Президента РФ №250
от 01.05.2022

Указ Президента РФ №166 от
30.03.2022

Введение оборотных штрафов за утечки
персональных данных

Уход поставщиков оборудования

Уход поставщиков ПО

Изменение цепочки поставок

Рассчитываете на свои силы?

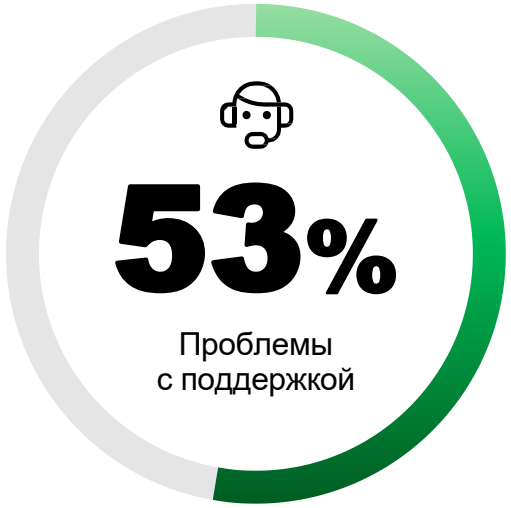
Ключевые риски внедрения ИБ on-prem

46% Стоимость внедрения и обслуживания окажется слишком высокой

36% Затраты на внедрение могут не оправдаться

40% Трудно найти квалифицированных специалистов для обслуживания ИБ-решений

19% Сотрудники не готовы обучаться работе с ИБ-сервисами



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

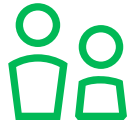
15% Решение недостаточно гибкое, трудно кастомизировать

ПроБизнес

Нивелирование рисков с помощью MSSP

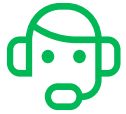
MSSP (Managed Security Service Provider) — это информационная безопасность по подписке. Компании выбирают функционал и каждый месяц оплачивают счет с фиксированной суммой. Взамен провайдер настраивает и поддерживает защиту информационных систем под ключ

Прозрачность расходов, PAYG, возможность быстро масштабироваться в обе стороны



Квалифицированный персонал

Гибкие возможности пилотирования и оценки функционала, высокая адаптивность к меняющимся условиям



Единое окно технической поддержки и консультационного обслуживания

Гарантии SLA

ПроБизнес

Популярность MSSP

49%

Рассматривают сервисную модель

29%

Не используют и не планируют использование сервисной модели

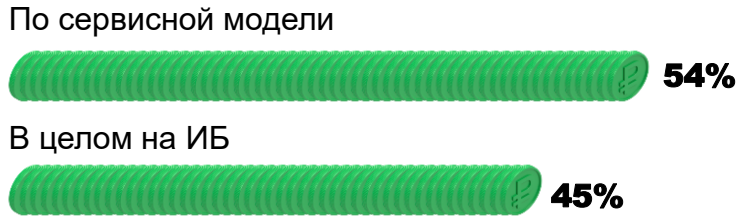
49% В секторе гос-управления, ЖКХ

22%

Используют сервисную модель

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

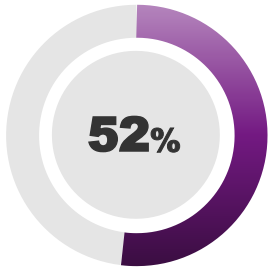
Рост бюджета на ИБ



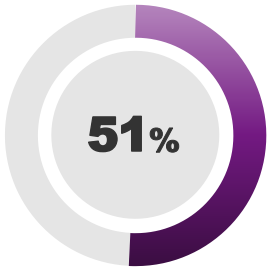
ПроБизнес

Преимущества MSSP

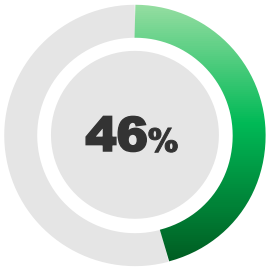
Преимущества сервисной модели ИБ по сравнению с традиционной



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

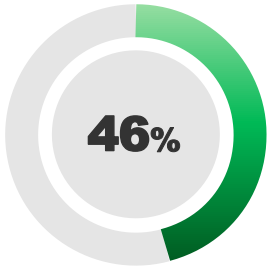


Готовые процессы обеспечения ИБ

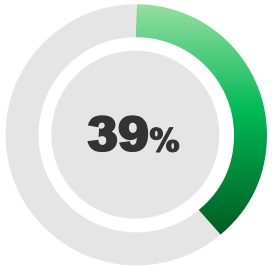


Более быстрая адаптация защиты под новые и развивающиеся угрозы

66% Среди компаний торговли и ретейла

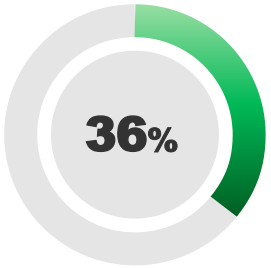


Сокращение времени на внедрение/запуск ИБ-решения



Сокращение расходов на оплату ИБ-специалистов

58% Среди компаний сегмента здравоохранения



Сокращение затрат на приобретение ИБ-решений

18% Среди компаний сегмента SoHo

ПроБизнес

Услуги MSSP «МегаФона»

Сетевая безопасность

- Защита от DDoS
- WAF
- Криптозащита (ГОСТ VPN)
- NGFW

Консалтинговые услуги

- Аудит ИБ
- Анализ защищенности (Pentest)
- SOC

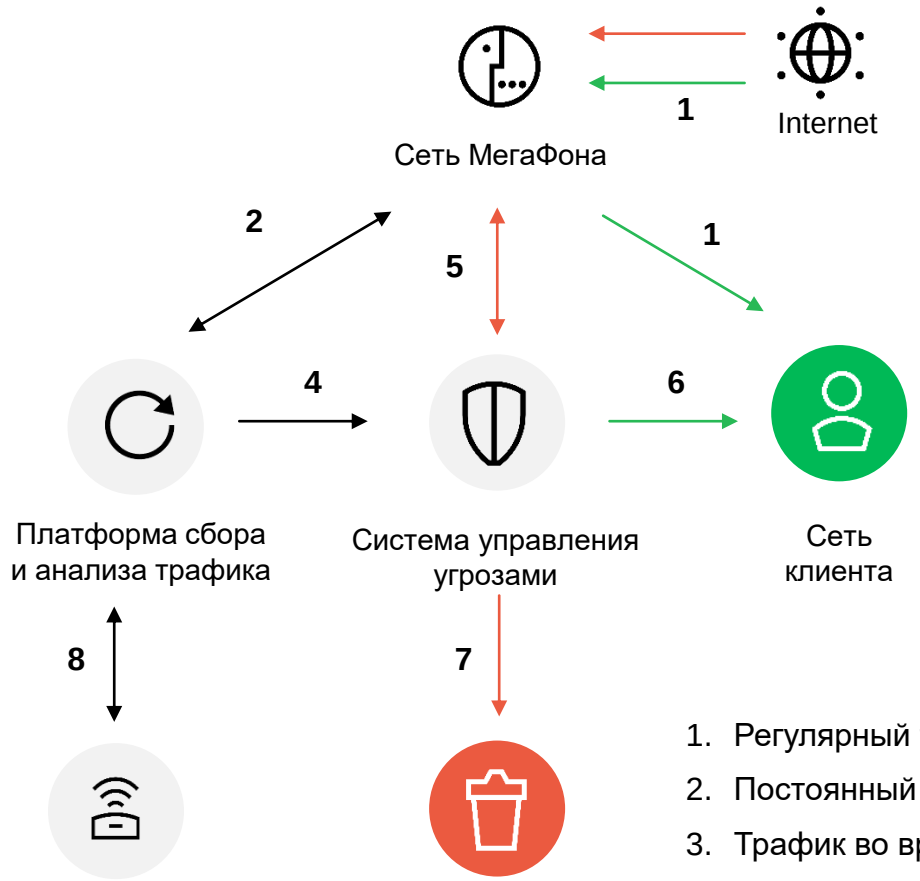
Защита данных

- Защита корпоративной почты

ПроБизнес

Защита от DDoS-атак

Технологии от отечественного вендора (соответствует требованиям для государственных и оборонных заказчиков)



- Противодействие атакам ёмкостью до 300 Гбит/с, не требует дополнительных настроек и установки дорогого оборудования
- Автоматическая фильтрация зловредного трафика в течение 5-15 секунд после начала атаки
- Защита от всех современных типов атак на сетевом уровне
- Выделенная служба мониторинга и реагирования 24/7/365

1. Регулярный трафик
2. Постоянный анализ трафика
3. Трафик во время DDoS-атаки
4. Указание на фильтрацию трафика
5. Направление трафика на фильтрацию
6. Отфильтрованный трафик
7. Аннулирование вредоносного трафика
8. Обновление базы сигнатур

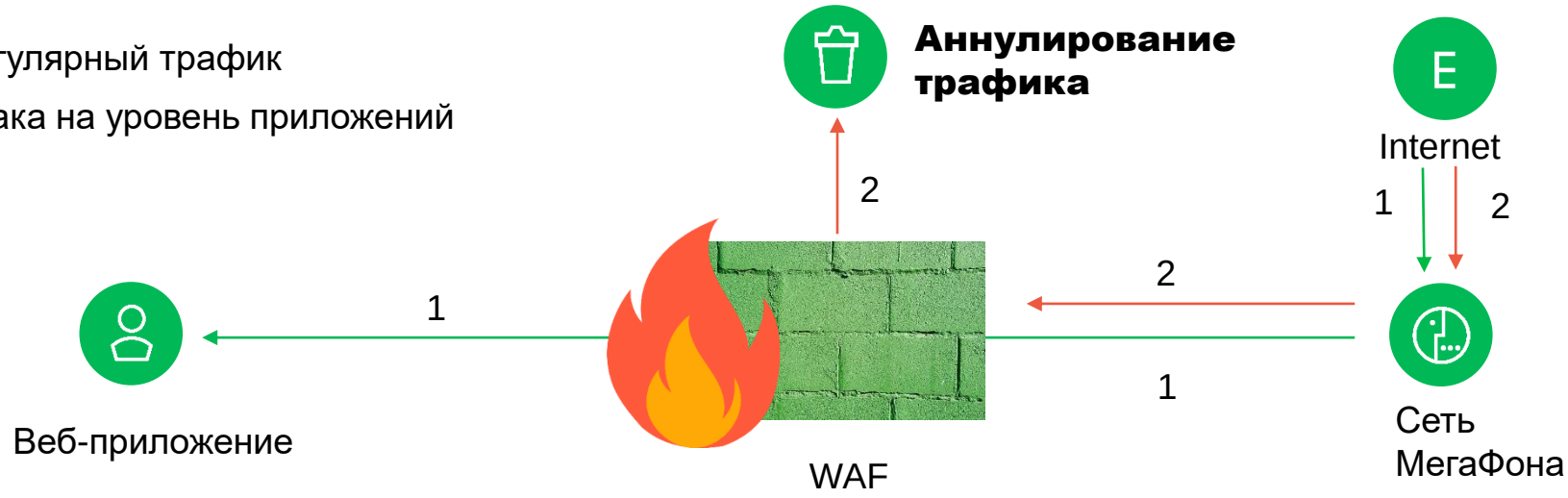
ПроБизнес

МегаФон WAF

Надежная защита веб-приложений от взломов, утечек данных и сбоев в работе

- Реализован на базе отечественного программного обеспечения
- Работает в автоматическом режиме
- Обнаруживает и блокирует атаки нулевого дня и атаки, использующие известные уязвимости веб-приложений
- Устойчив к распространенным методикам обхода механизмов защиты WAF

1. Регулярный трафик
2. Атака на уровень приложений



ПроБизнес

Криптозащита

Услуга гарантированно защищает вашу информацию при её передаче по открытым каналам связи. Ни оператор связи, ни производитель оборудования, ни злоумышленники — никто не имеет доступа к защищаемым данным

Услуга «Криптозащита» построена на базе решений российских производителей криптооборудования

Криптошлюзы используют только российские криптоалгоритмы (ГОСТ 28147-89, ГОСТ 34.10/34.11-2012, ГОСТ 34.12/34.13-2015)

Можно создать VPN «с нуля» либо организовать систему шифрования в уже существующей VPN

Экономия на капитальных затратах на закупку оборудования и персонале для обслуживания

Возможности решения:

- Выбор вендора из топ-3 российских лидеров криптооборудования
- Платформа сертифицирована ФСБ России
- Снижение капитальных затрат при выборе сервисной модели
- Возможность создания отказоустойчивого кластера

ПроБизнес

Подробности на сайте

МегаФон NGFW

Комплексная защита информационных ресурсов клиента от сетевых атак и вирусов, фильтрация доступа сотрудников в Интернет

1. Безопасная публикация ресурсов и сервисов
2. Межсетевое экранирование
3. Система обнаружения и предотвращения вторжений
4. Анализ и предотвращение новых угроз
5. Интернет фильтрация

ПроБизнес

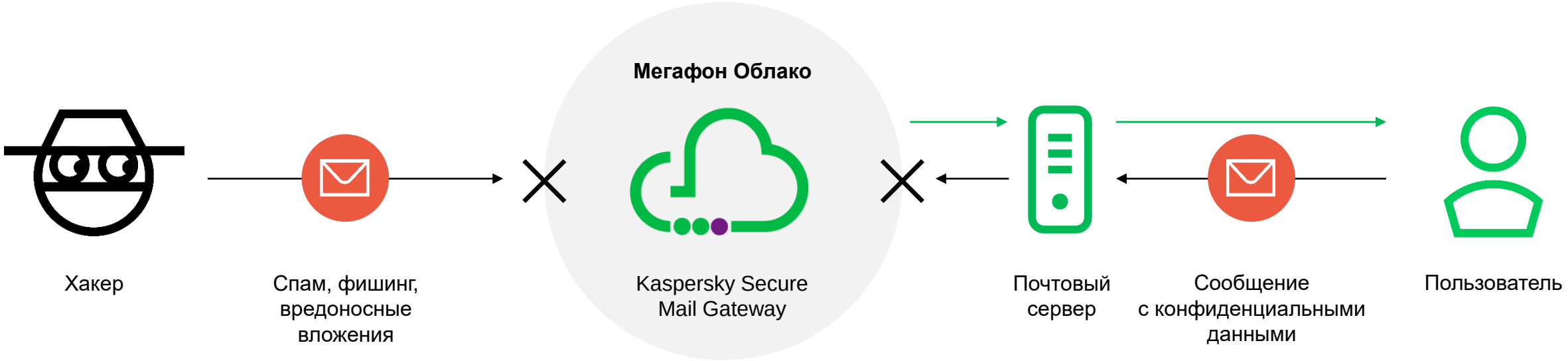
Защита корпоративной почты

От фишинговых писем, спама и зараженных вирусами почтовых вложений

1 **Блокировка нежелательных рассылок** (включая социальную инженерию), фишинга, сообщений с зараженными вложениями

2 **Борьба с угрозами** на уровне периметра

3 **Оперативное обнаружение** признаков целевой атаки и блокировка ее составляющих



ПроБизнес

МегаФон SOC

Security Operation Center – коммерческий центр мониторинга и реагирования на инциденты ИБ в режиме 24/7

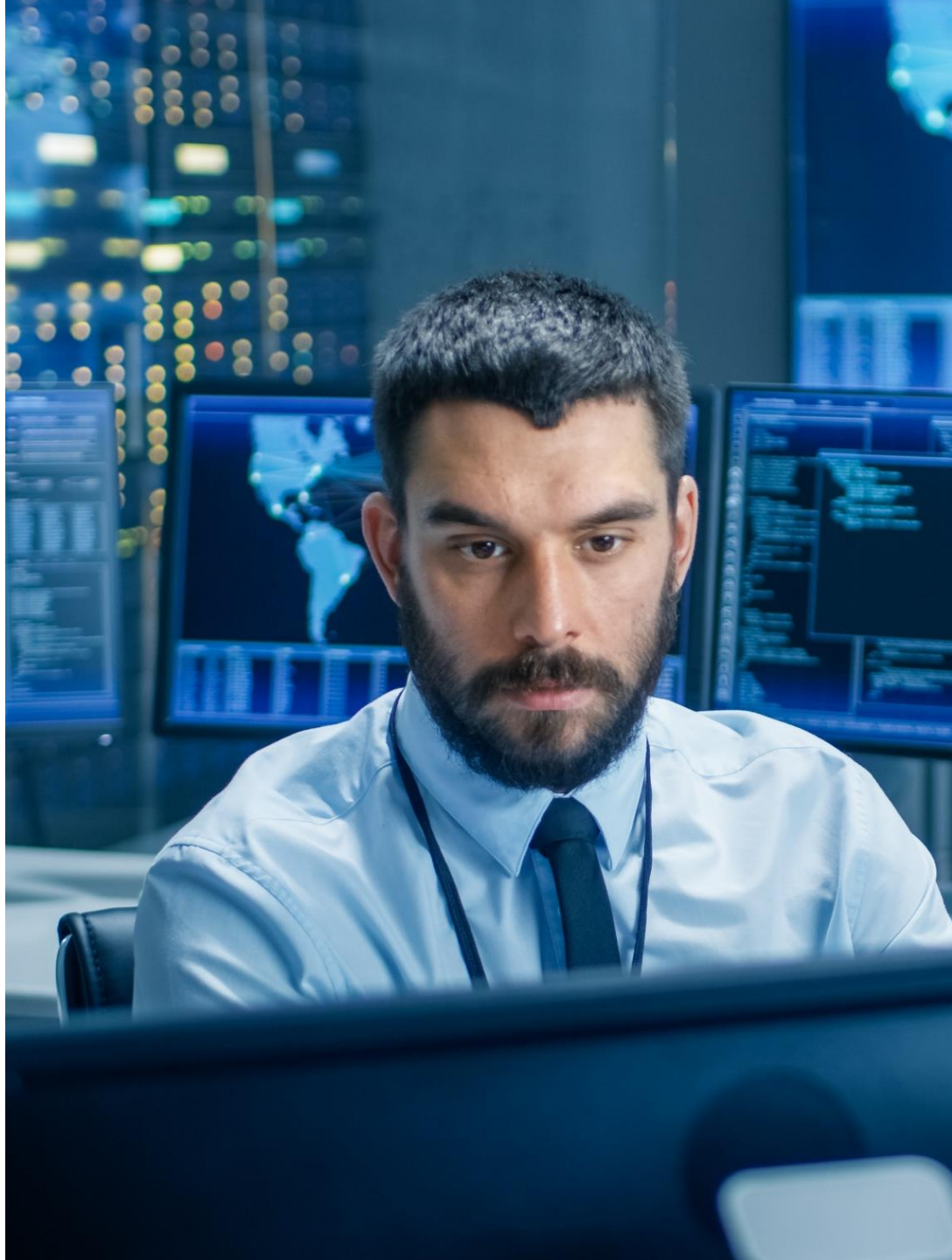
Агрегация событий ИБ
из разных источников

Анализ событий
и инцидентов ИБ

Реагирование
на инциденты

Отчетность
и визуализация данных

ПроБизнес



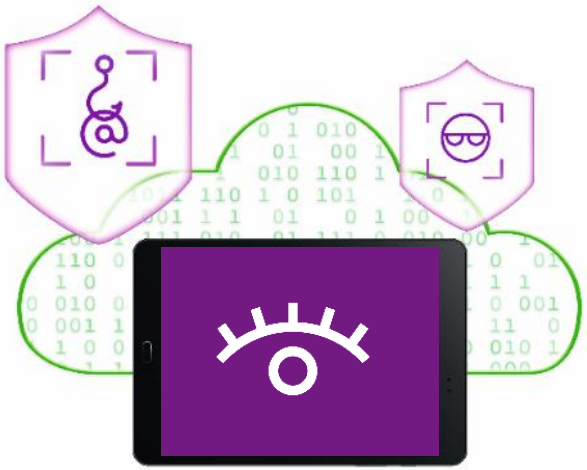
Анализ защищенности IT-инфраструктуры

Услуги

- Тестирование на проникновение
- Анализ защищенности
- Аудит соответствия требованиям регуляторов и различных международных стандартов
- Расследование инцидентов
- Red teaming
- Тестирование на устойчивость к Dos/DDoS атакам
- Удаленный офис (VPN, ВКС и т.д.)
- КИИ «под ключ»: категорирование, проектирование/внедрение СУИБ/СЗИ

Объекты тестирования

• Сети Wi-Fi • Веб-приложения • Мобильные приложения • ДБО • Бизнес приложения (ERP, CRM и т.д.) • АБС • Алгоритмы машинного обучения • Блокчейн проекты • Внешний периметр • Внутренний периметр • Социальная инженерия



Итоги работ

Оценка влияния обнаруженных уязвимостей на бизнес-процессы компании, наихудшие последствия возможной атаки

Описание обнаруженных уязвимостей: эксплуатация, критичность, рекомендации по устранению

Общий вывод о безопасности инфраструктуры: оценка рисков и рекомендации по улучшению

ПроБизнес

Технологии включают бизнес

Антон Бельгисов
Менеджер по развитию облачных
и инфраструктурных решений МегаФона

anton.belgisov@Megafon.ru

+7 937 90 400 90

8 800 550 05 55
b2b.megafon.ru

МегаФон | ПроБизнес