МегаФон | ПроБизнес

Риски применения инструментов ИБ без учёта современных угроз

МегаФон | ПроБизнес

МЕГАФОН | ПроБизнес

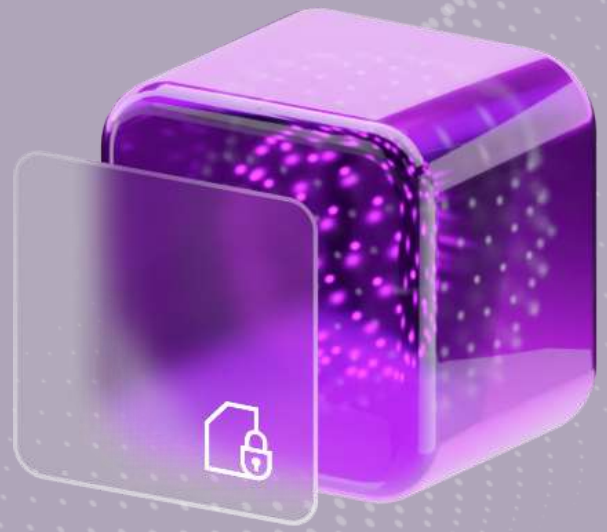
Станислав Погоржельский

Специалист по технологической поддержке облачных и инфраструктурных решений

МЕГАФОН | ПроБизнес

Инструменты

МегаФон | ПроБизнес



— Межсетевые экраны (firewalls)
— Системы предотвращения вторжений (Intrusion Prevention Systems, IPS)
— Системы обнаружения вторжений (Intrusion Detection Systems, IDS)
— Виртуальные частные сети (Virtual Private Networks, VPN)
— DDOS-защита (Distributed Denial of Service protection)
— Системы авторизации и аутентификации
— Системы мониторинга безопасности
— SOC/SIEM

Инструменты ИБ

- Защита внешнего периметра
- Повышение осведомлённости Сотрудников
- SOC
- Аудит ИБ

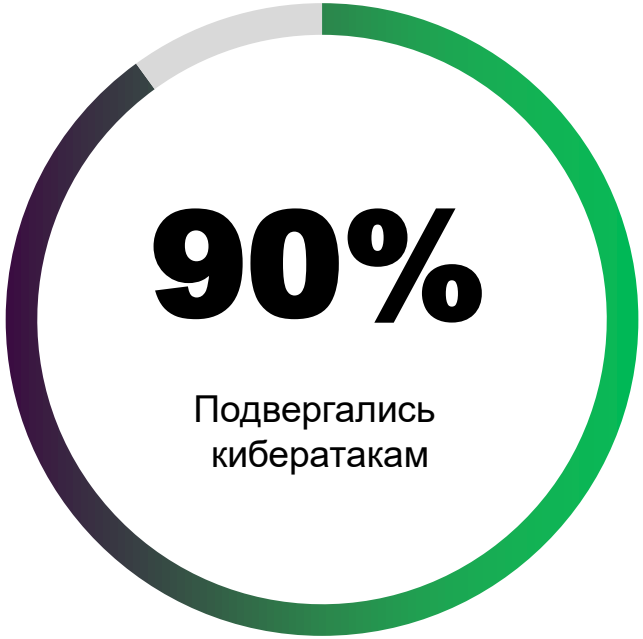
МегаФон | ПроБизнес

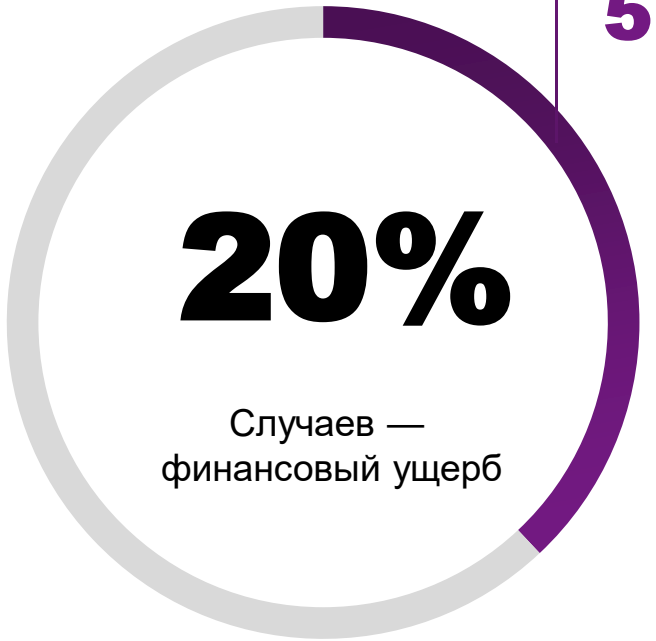
Современные угрозы

МегаФон | ПроБизнес

Кибератаки-2021-2023

Статистика российского рынка





Из них каждая пятая компания оценила свой ущерб в более чем

5 млн ₽

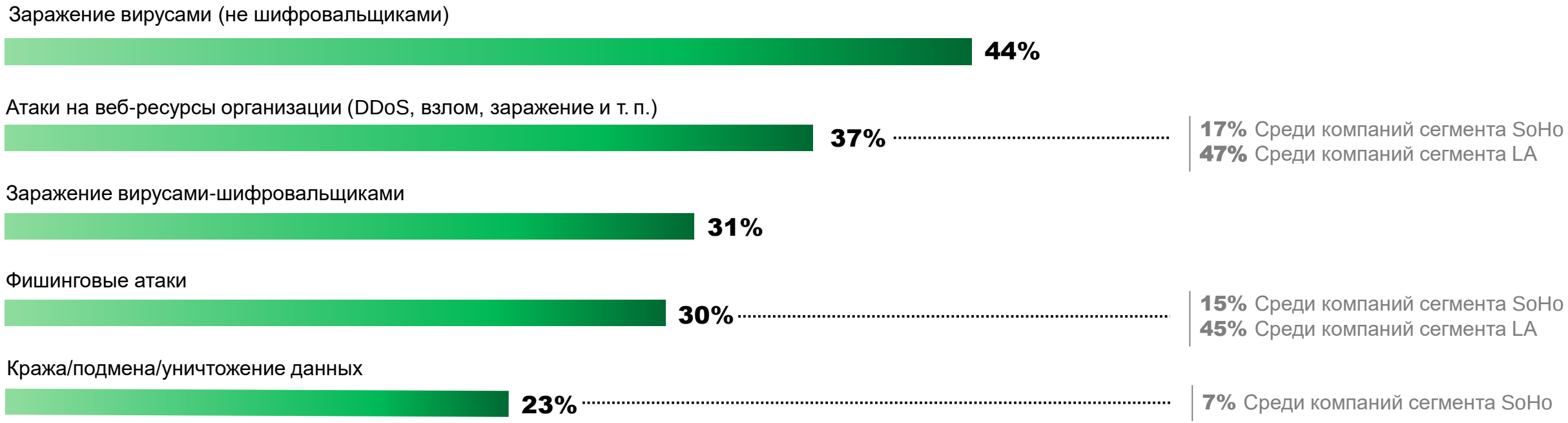
МегаФон | ПроБизнес

*По данным исследования МегаФона «Индекс Кибербезопасности»

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 | ПроБизнес

*По данным исследования МегаФона «Индекс Кибербезопасности»

Причины утечки данных

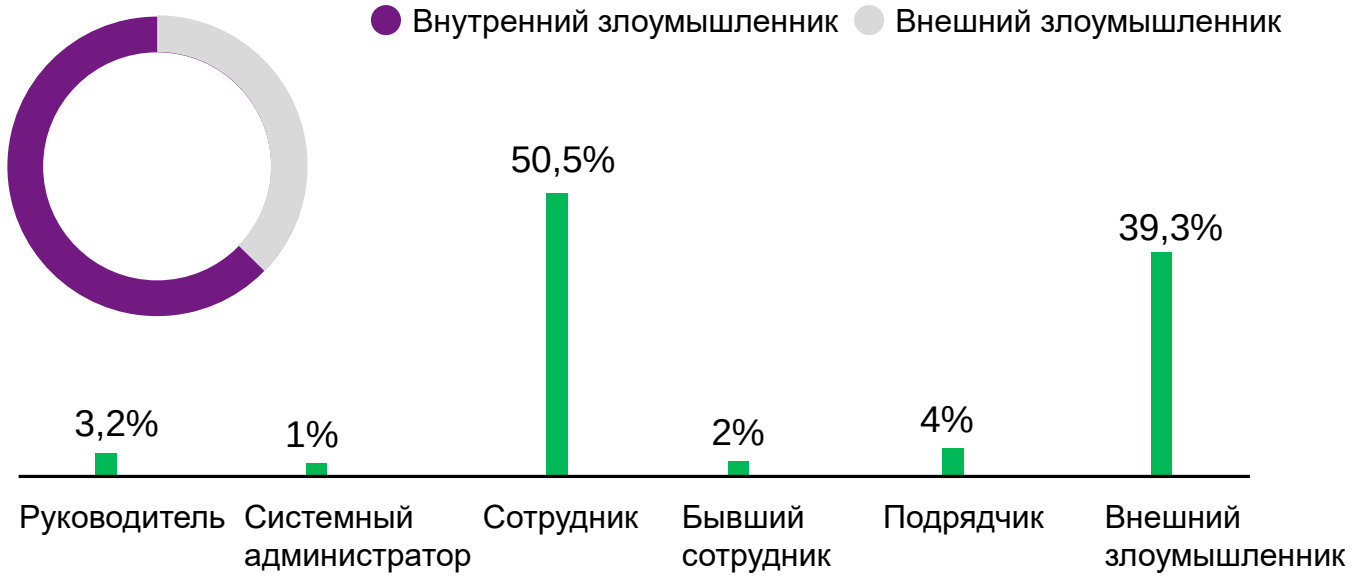
- Данные
- Приложения
- Базы данных
- Операционная система

95%

- Виртуализация
- Физический сервер
- Сети, хранилища
- Дата-центр

5%

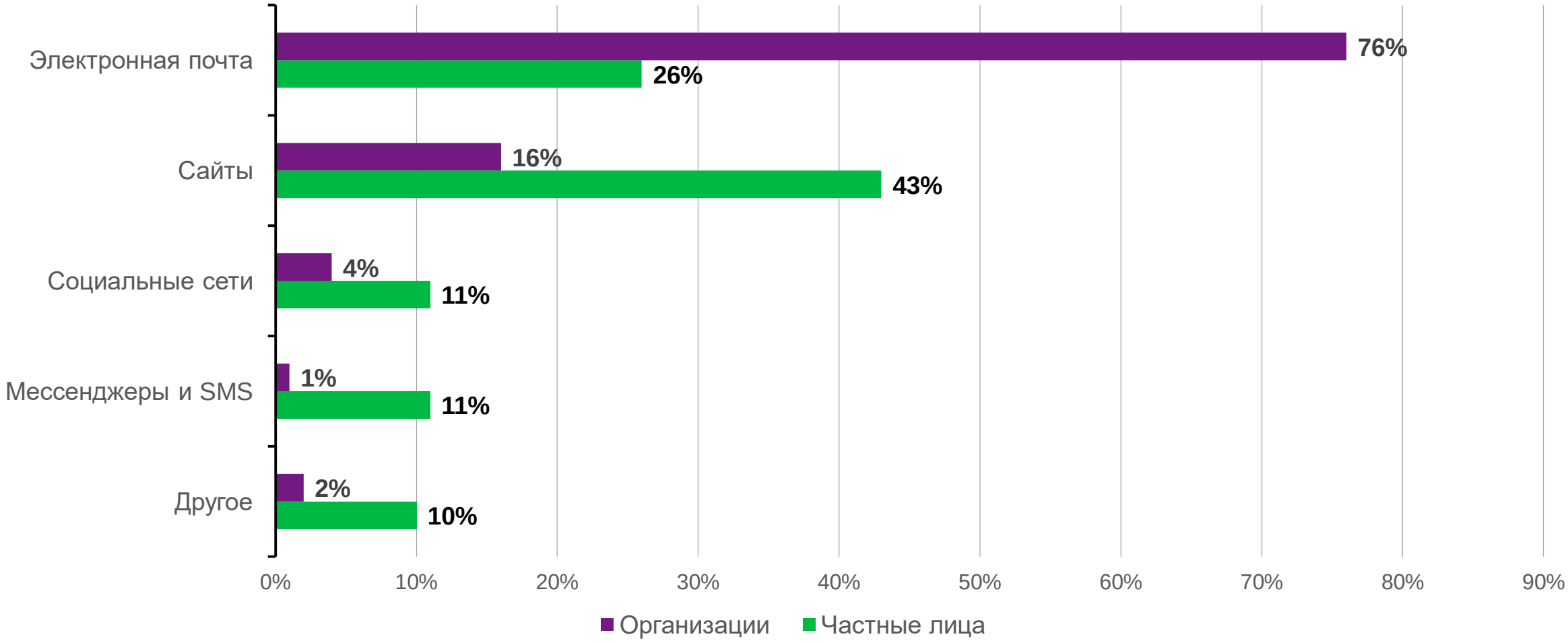
Виновники утечек



МегаФон | ПроБизнес

Источник Аналитический центр компании InfoWatch

Точки входа malware

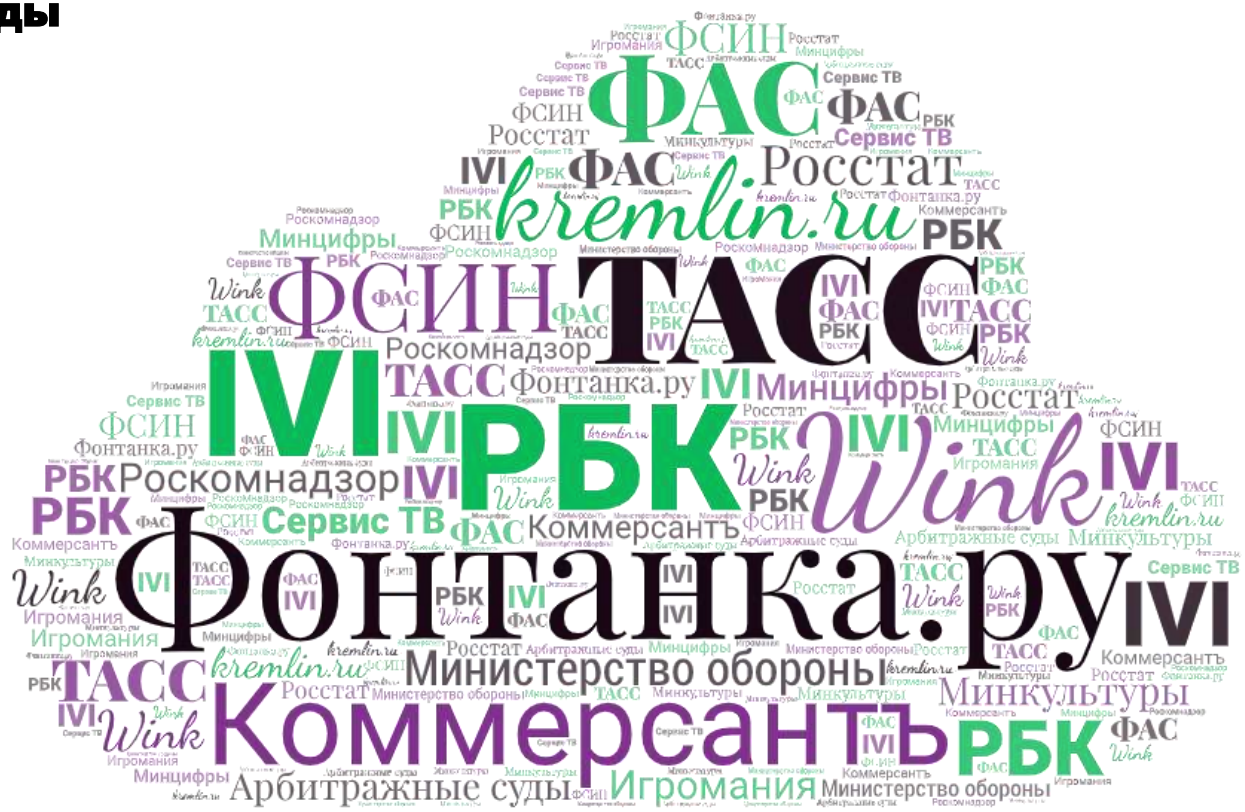


МегаФон | ПроБизнес

Взлом веб-ресурсов также стали чаще выбирать при организации целевых атак

Атаки на веб-ресурсы стали основной причиной критических ИБ-инцидентов в последние годы

Решение WAF (Web Application Firewall) становится must have даже для тех компаний, для которых веб-сайт — не главный канал продаж



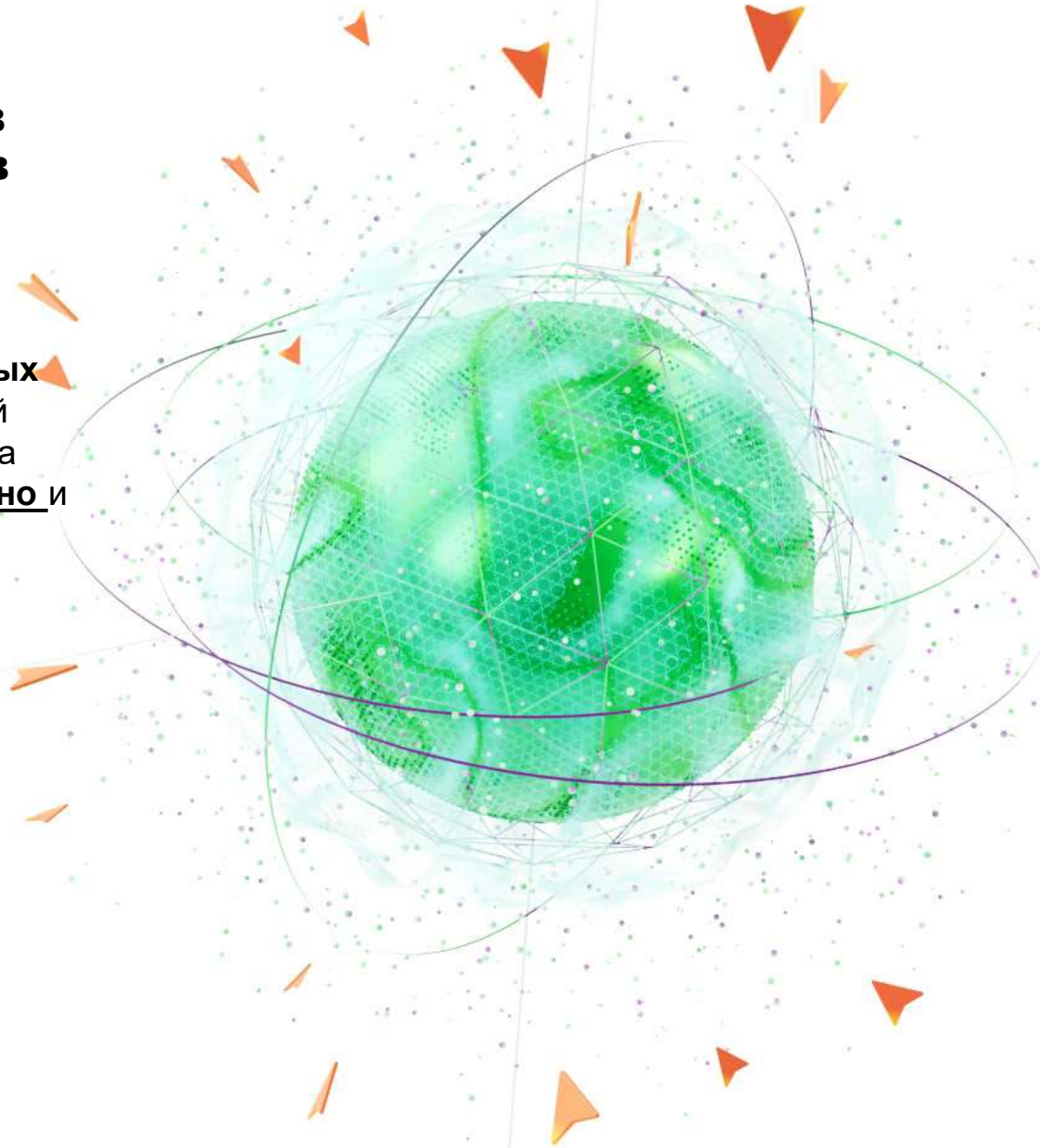
* Из открытых источников

Киберриски

Компании часто сталкиваются со сложностями в области кибербезопасности. Но дело не только в росте количества и сложности кибератак

На организацию, которую атакуют, повлияет **отсутствие квалифицированных кадров в штате**, недостаток ресурсов на анализ всех происходящих событий информационной безопасности, а также нехватка времени. А как известно, на инциденты информационной безопасности (ИБ) надо **реагировать мгновенно** и правильным способом, пока они не причинили значительный ущерб.

Усилить защиту от кибератак и компенсировать нехватку ресурсов поможет **Security Operation Center** — выделенный центр мониторинга и реагирования на инциденты ИБ, который работает в режиме **24/7** и объединяет в себе опыт тысяч компаний.



МегаФон

Указ Президента РФ от 01.05.2022 № 250

«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Персональная ответственность!

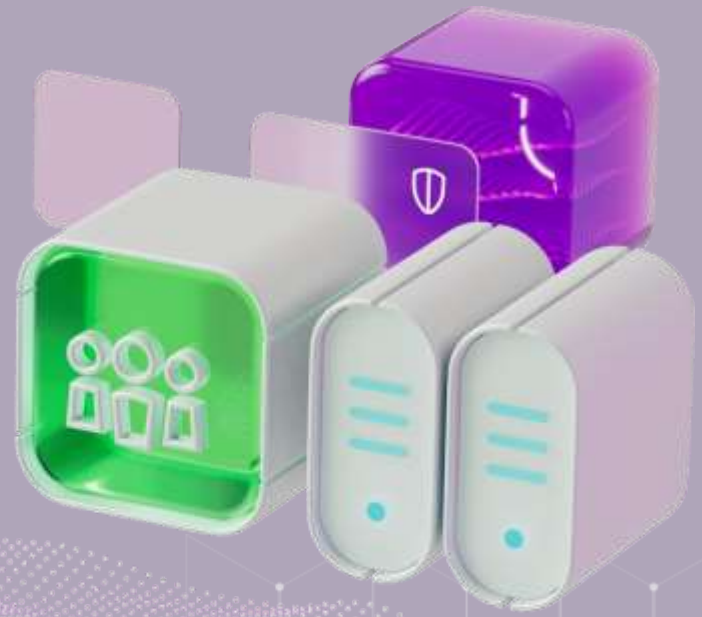
«2. Возложить на руководителей органов (организаций) персональную ответственность за обеспечение информационной безопасности соответствующих органов (организаций).»
П. 2 Указа

Возложить данные функции на существующее структурное подразделение

а) возложить на заместителя руководителя полномочия по обеспечению ИБ, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты; б) создать структурное подразделение, осуществляющее функции по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение;
Пп.а) б) п.1 Указа

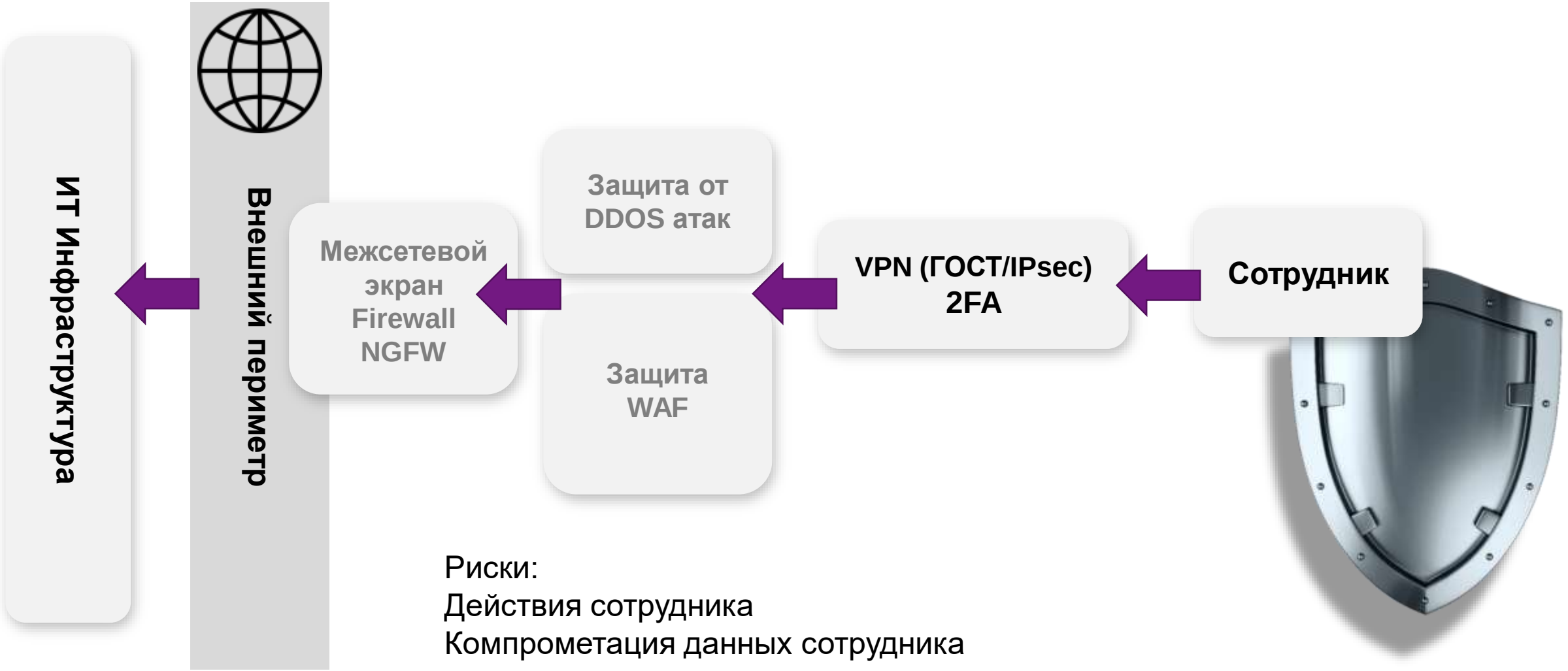
МегаФон | ПроБизнес

Защита внешнего периметра организации от киберугроз



МегаФон | ПроБизнес

Внешний периметр



Риски:
Действия сотрудника
Компрометация данных сотрудника

ЧТО ТАКОЕ NGFW

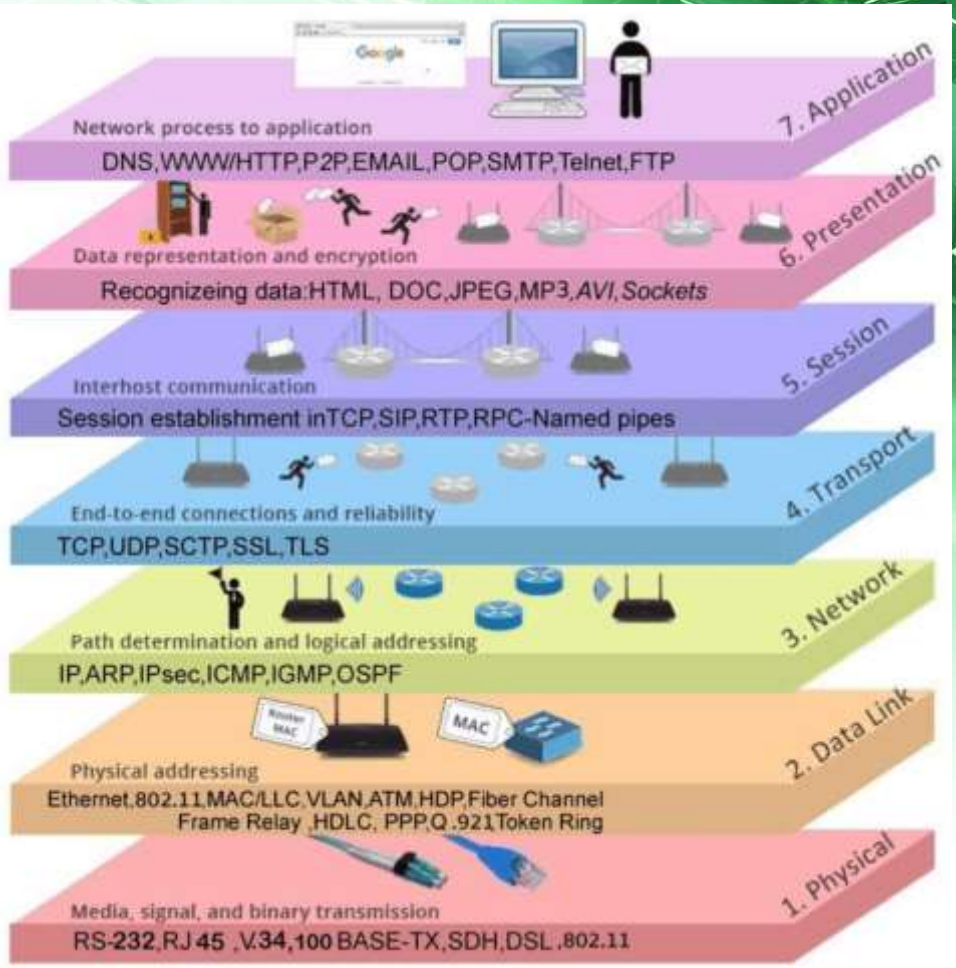
Функции NGFW:

- Межсетевое экранирование;
- Обнаружение и предотвращение атак (в т.ч. атаки на веб-приложения);
- Антиспам;
- Потоковый антивирус;
- Контроль приложений;
- Фильтрация интернет-запросов пользователей;
- VPN;
- Анализ событий/формирование отчетов.

NGFW – многофункциональный продукт

Модель OSI для облачного NGFW

Уровень	Функции	PDU	Примеры
7. Прикладной	Некоторое высокоуровневое API	Данные	HTTP, FTP
6. Представительский	Представление данных между сетевым сервисом и приложением	Данные	ASCII, EBCDIC, JPEG
5. Сеансовый	Управление сеансами: продолжительный обмен информацией в виде множества передач между нодами	Данные	RPC, PAP
4. Транспортный	Надёжная передача сегментов между двумя нодами в сети	Сегменты/Дейтаграммы	TCP, UDP
3. Сетевой	Структуризация и управление множеством нод в сети	Пакеты	IPv4, IPv6
2. Канальный	Надёжная передача датафреймов между двумя нодами соединённых физическим уровнем	Фреймы	PPP, IEEE 802.2, Ethernet
1. Физический	Передача и приём потока байтов через физическое устройство	Биты	USB, витая пара

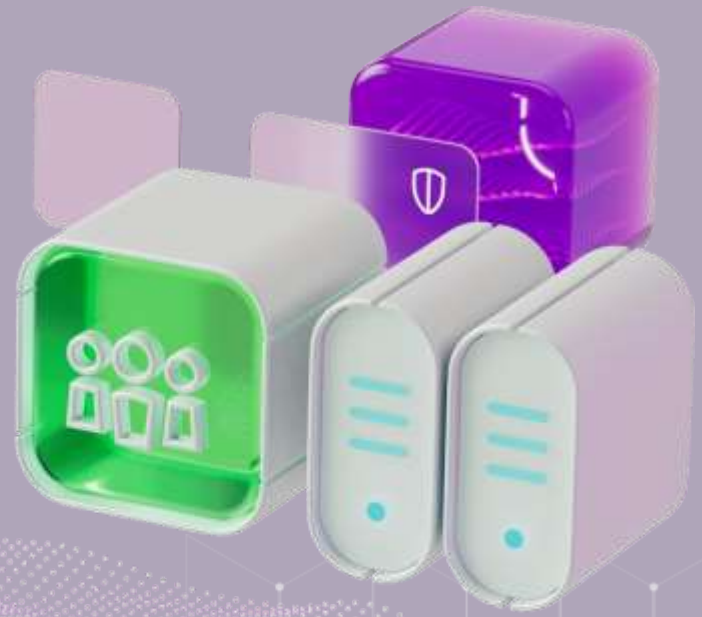


*Сетевая модель OSI (англ. open systems interconnection basic reference model)

МегаФон | ПроБизнес

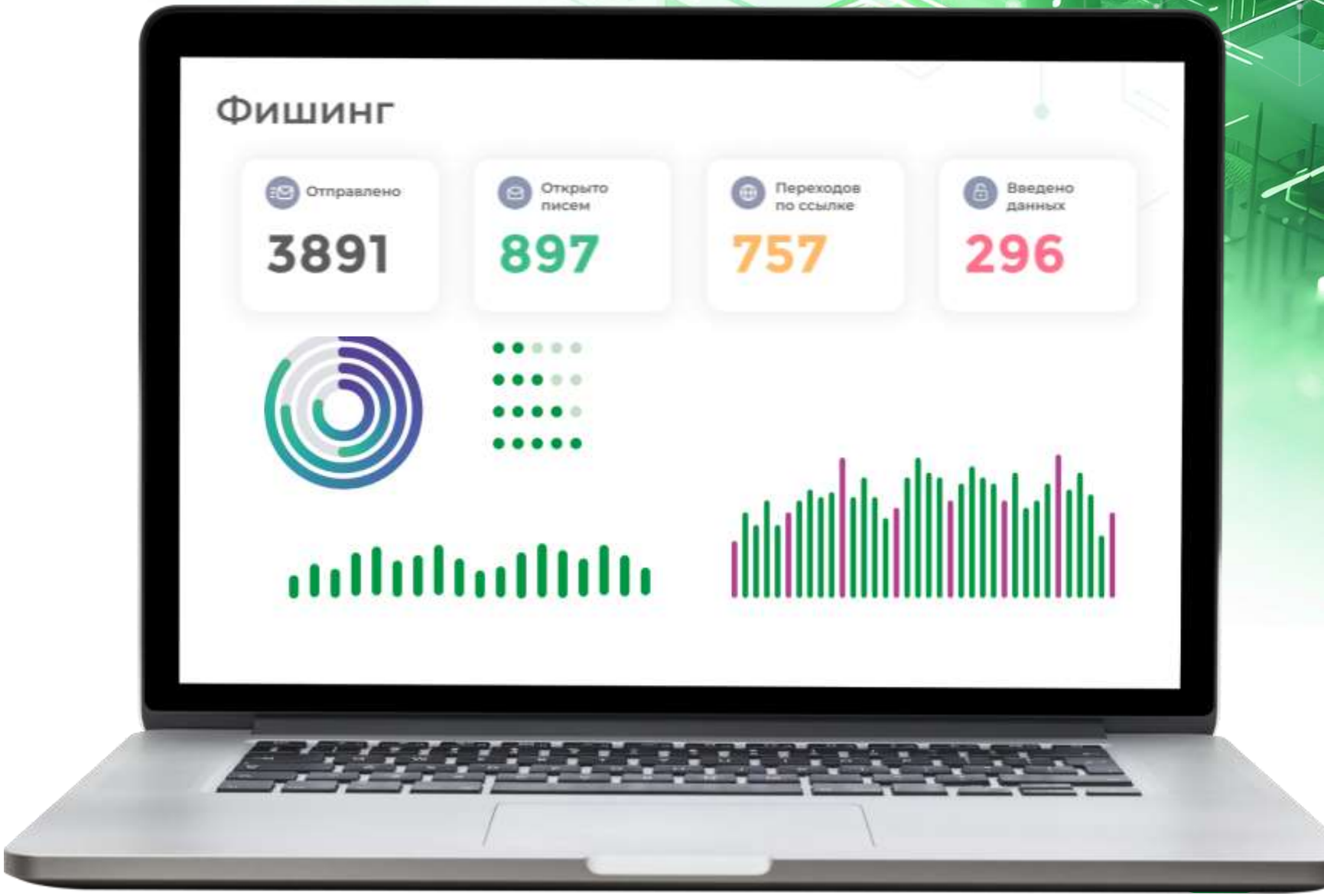
МегаФон | ПроБизнес

Как быть с сотрудниками?



МегаФон | ПроБизнес

Провели тестовую фишинговую рассылку



МегаФон | ПроБизнес

Security Awareness от МегаФона: платформа для повышения осведомленности сотрудников

Платформа в лёгкой и понятной форме повышает осведомлённость сотрудников в сфере информационной безопасности и цифровой гигиены.

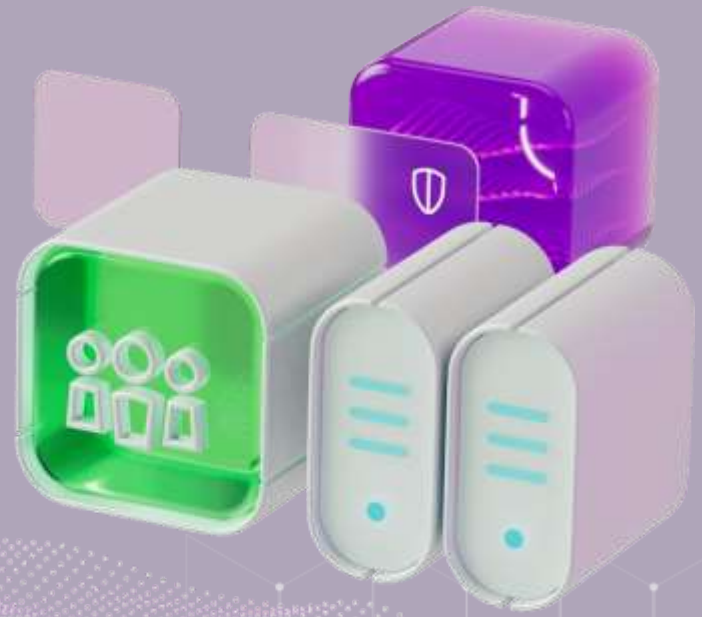
При помощи имитации фишинговых рассылок у компании есть возможность проверить степень уязвимости сотрудников к действиям злоумышленника.

Теория	Практика
Обучающие курсы	Тестовые задания
Имитация фишинга	Вирусные вложения
Подробная аналитика	Выявление уязвимых сотрудников

МегаФон | ПроБизнес

МегаФон | ПроБизнес

SOC



МегаФон | ПроБизнес

Из чего состоит SOC

Команда экспертов ИБ

SIEM

Security Information and Event Management

Платформа для сбора и анализа информации о событиях ИБ

IRP

Incident Response Platform

Платформа для автоматизации реагирования на киберинциденты

МегаФон

SIEM

Security Information and Event Management

– **система, которая используется для сбора, анализа и управления событиями безопасности. Она позволяет собирать данные из различных источников, включая системы брандмауэров, системы обнаружения вторжений и системы управления угрозами.**

- **Сбор и агрегация данных:** SIEM получает данные из различных источников, включая логи, события, потоки данных, устройства и приложения.
- **Анализ и корреляция:** SIEM анализирует данные, используя различные методы, такие как машинное обучение, статистические анализы и правила, чтобы выявлять угрозы и аномалии.
- **Реагирование и уведомление:** SIEM может отправлять уведомления о событиях безопасности, генерировать предупреждения и автоматически принимать меры по блокированию или заблокированию угроз.
- **Хранение и архивирование:** SIEM сохраняет данные о событиях безопасности и может предоставлять возможность поиска и доступа к этим данным для анализа и расследования происшествий.
- **Управление рисками:** SIEM помогает оценить риски и улучшить безопасность за счет выявления и устранения уязвимостей в системе.
- **Соответствие нормативным требованиям:** SIEM помогает организациям следить за соблюдением нормативных требований в области безопасности.

МегаФон

Kill Chain

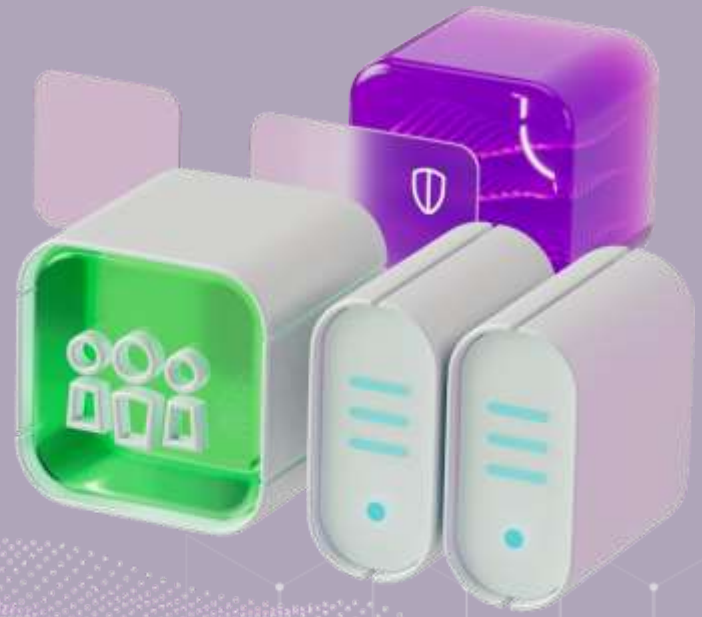
МегаФон | ПроБизнес

Kill Chain – варианты защиты

МегаФон | ПроБизнес

МегаФон | ПроБизнес

Прочие тренды

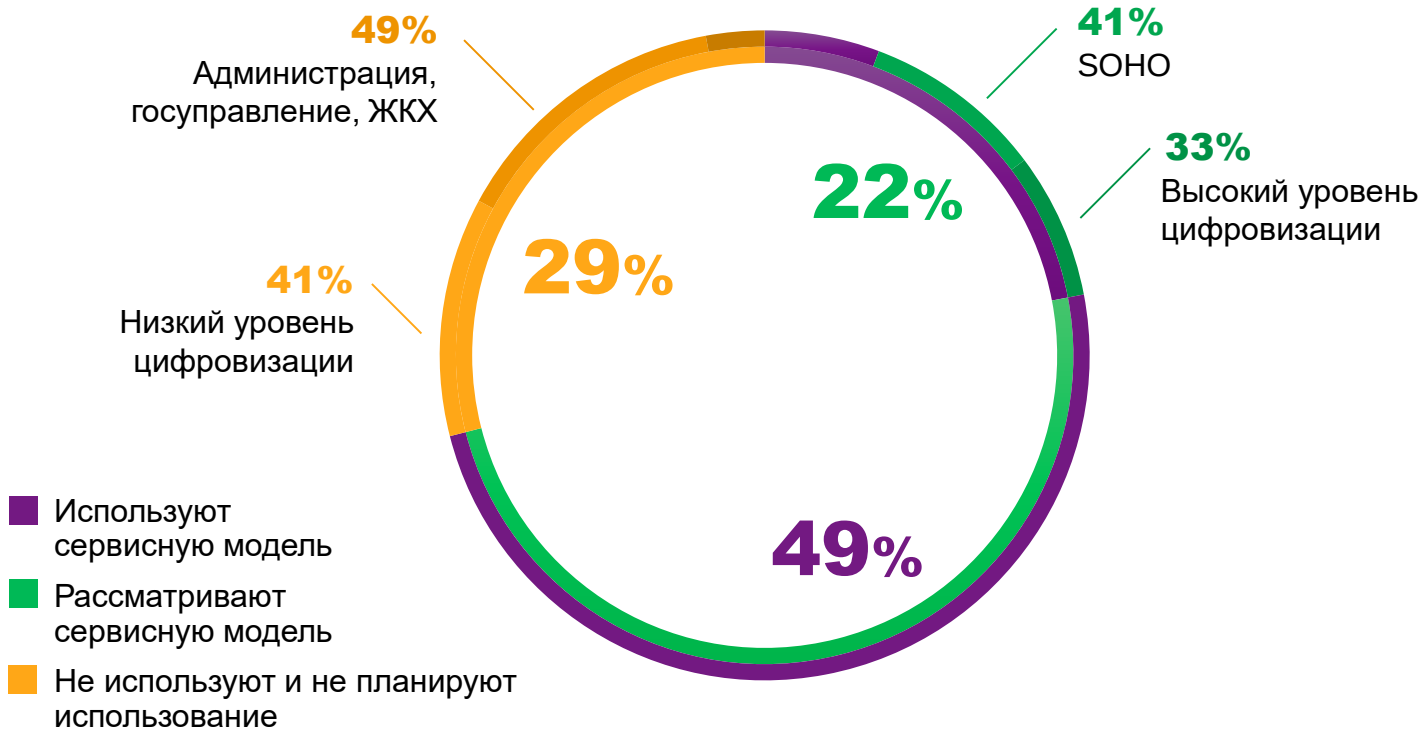


МегаФон | ПроБизнес

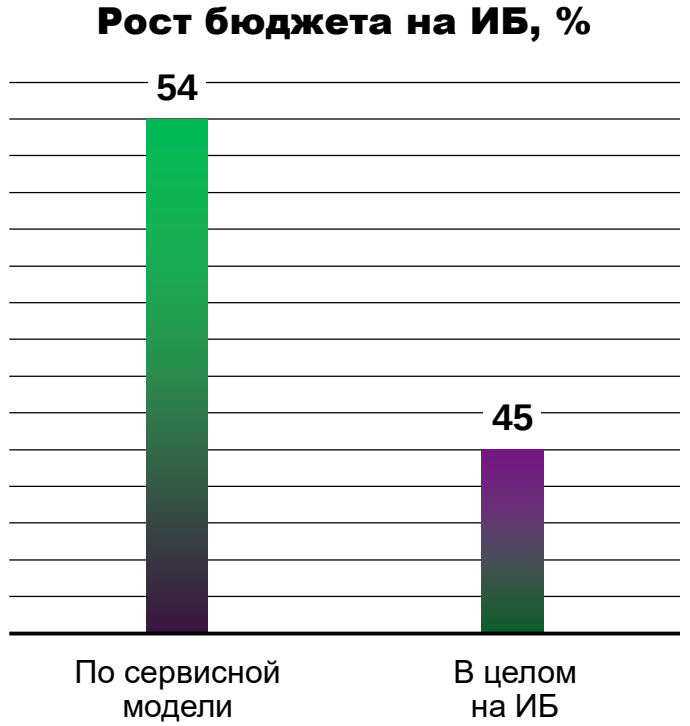
Рост доверия к сервисной модели

В условиях постоянной нехватки ИБ-специалистов

22% компаний используют сервисную модель ИБ, потенциал у аутсорсинга велик — еще 45% рассматривают такую модель как рабочую. Впрочем для госсектора такой формат обеспечения ИБ менее перспективен.



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



МегаФон | ПроБизнес

Значение в группе значимо выше/ниже всей выборки (95% доверительный интервал)

Анализ защищенности IT-инфраструктуры

Оценим текущий уровень защищенности вашей инфраструктуры найдем уязвимости и проверим, насколько она соответствует требованиям регуляторов

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.)

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

Характеристика 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

МегаФон | ПроБизнес

Подробности на сайте

Выводы

1. Постепенно компании выбирают требуемый набору инструментов ИБ
2. Растёт осознанность в принятии решений по защите
3. Квалификация (и ЗП) специалистов ИБ растёт
4. Компании вынуждены привлекать аутсорс по ИБ, т.к. это сложно

МегаФон | ПроБизнес

Технологии включают бизнес

Станислав Погоржельский

Специалист по технологической поддержке облачных и инфраструктурных решений

stanislav.pogorzhels@Megafon.ru