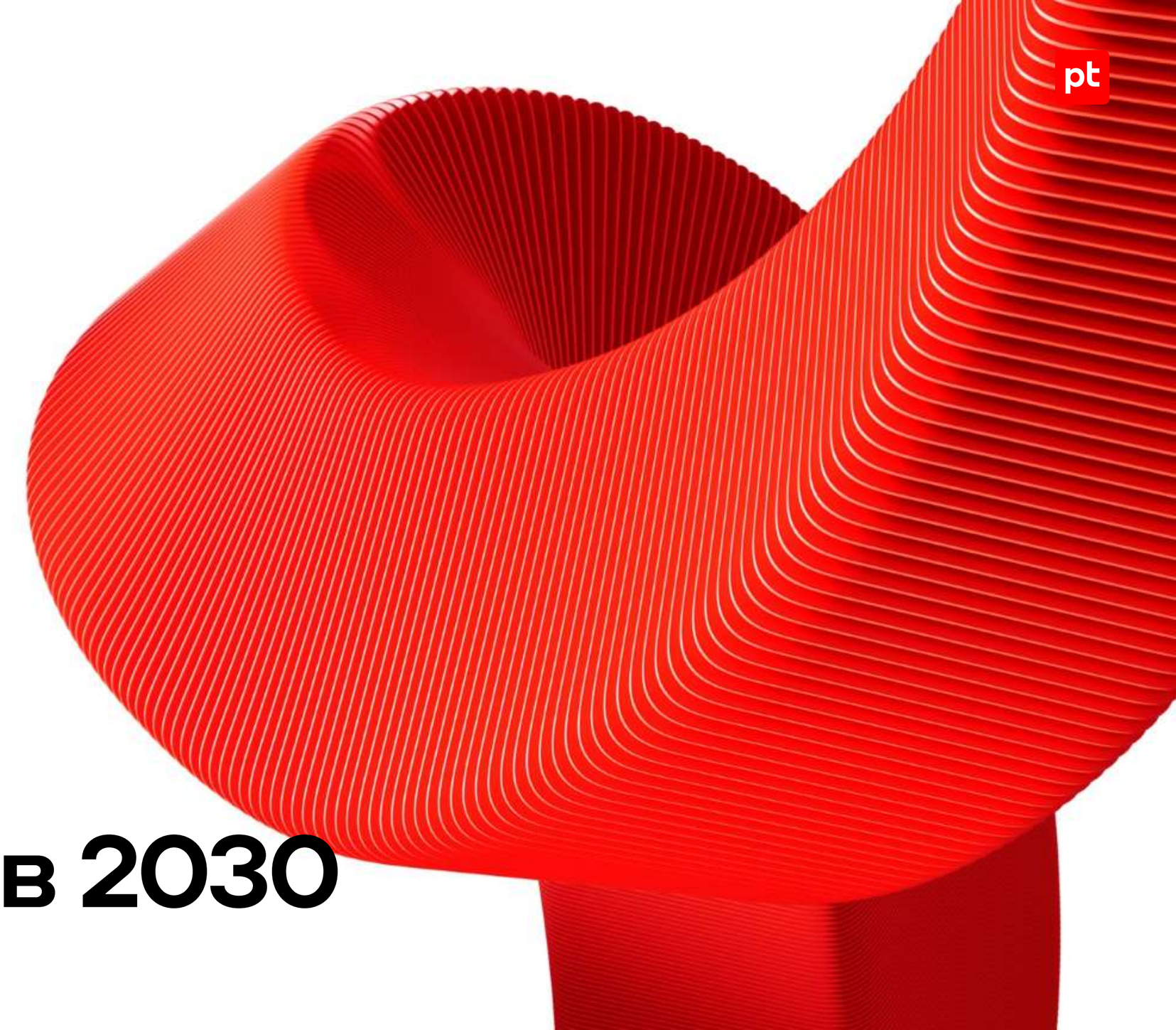
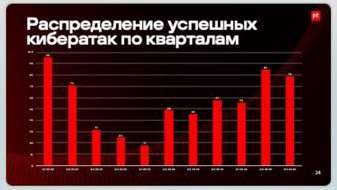
Владимир Клявин
Коммерческий директор



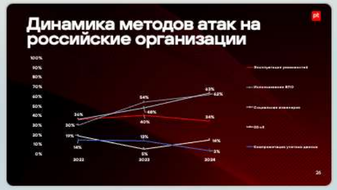
ИБ — Вызов 2030

23

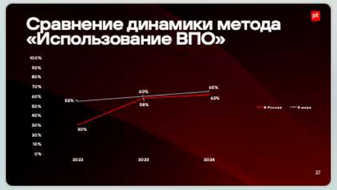


24

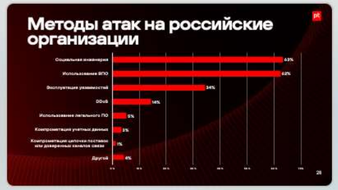
25



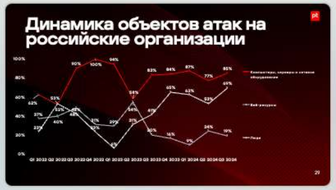
26



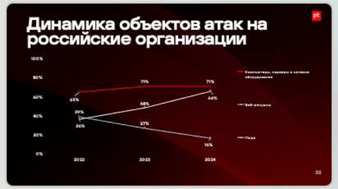
27



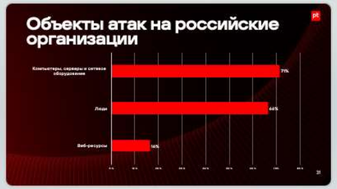
28



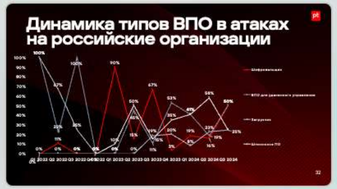
29



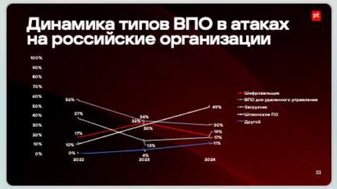
30



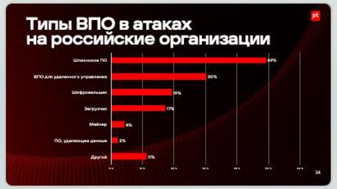
31



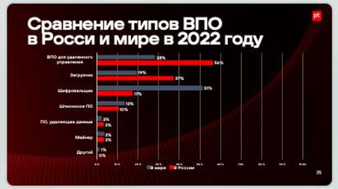
32



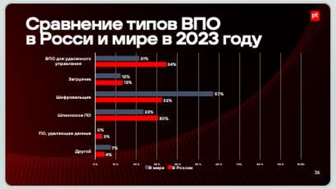
33



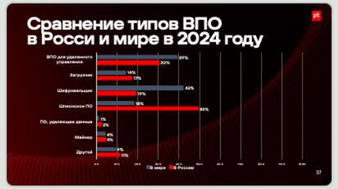
34



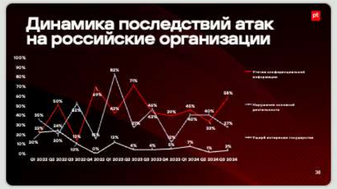
35



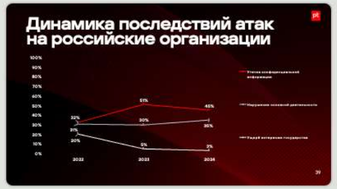
36



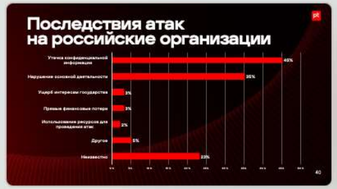
37



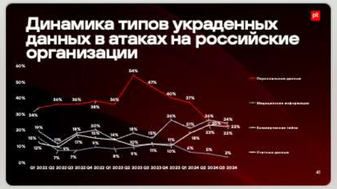
38



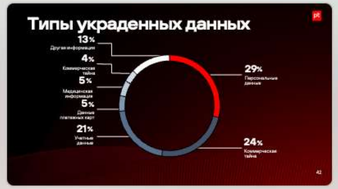
39



40



41



42

43

44

45

46

47

48

49

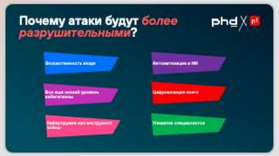
1

2

3

4

5



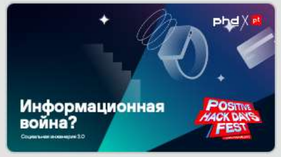
6

7

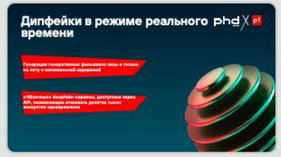
8


9

10



11



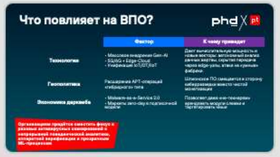
12

13

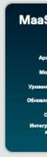
14

15

16



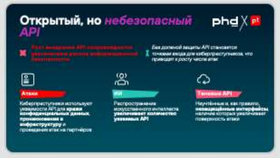
17


18

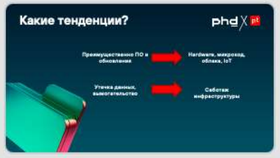
19

20

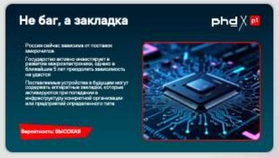
21



22

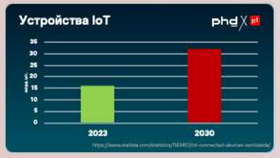


23



24

25



26

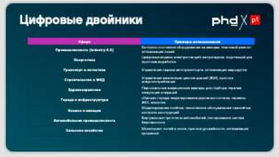

27

28

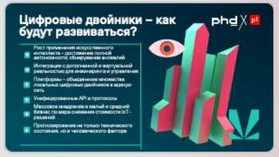
29

30

31



32

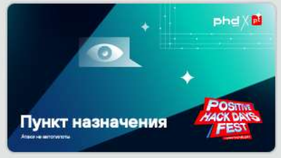


33

34

35


36



37

38

39

40

41

42

43

44

45

46

47

48

49

50

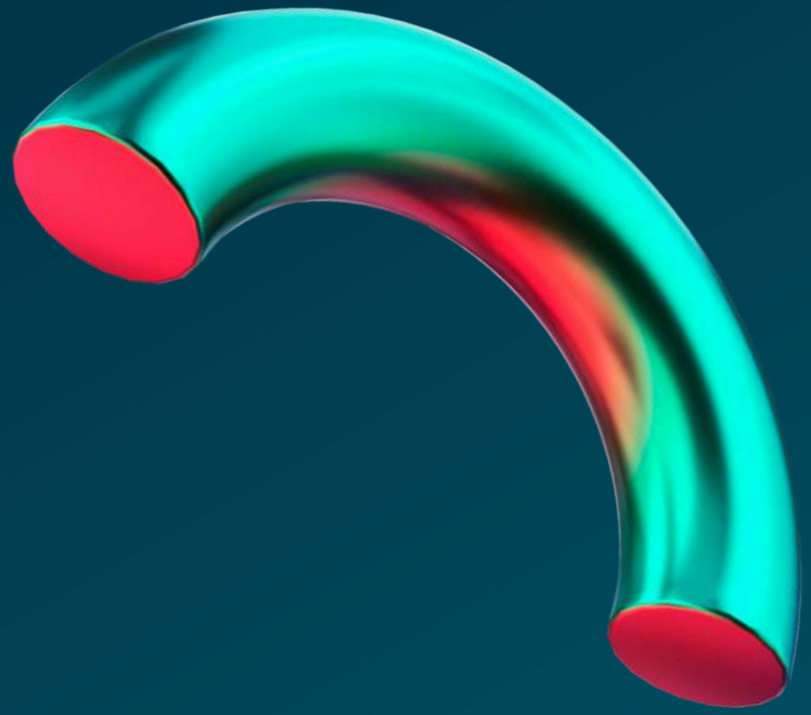
51

52

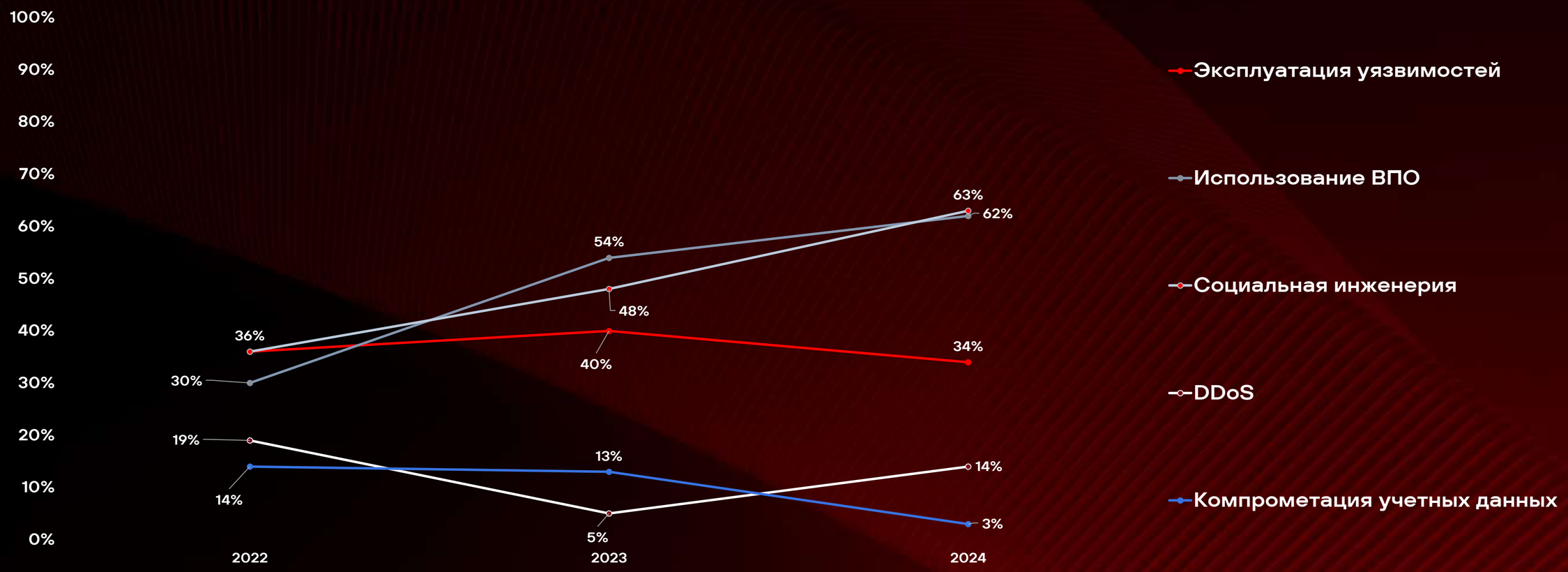
53

54

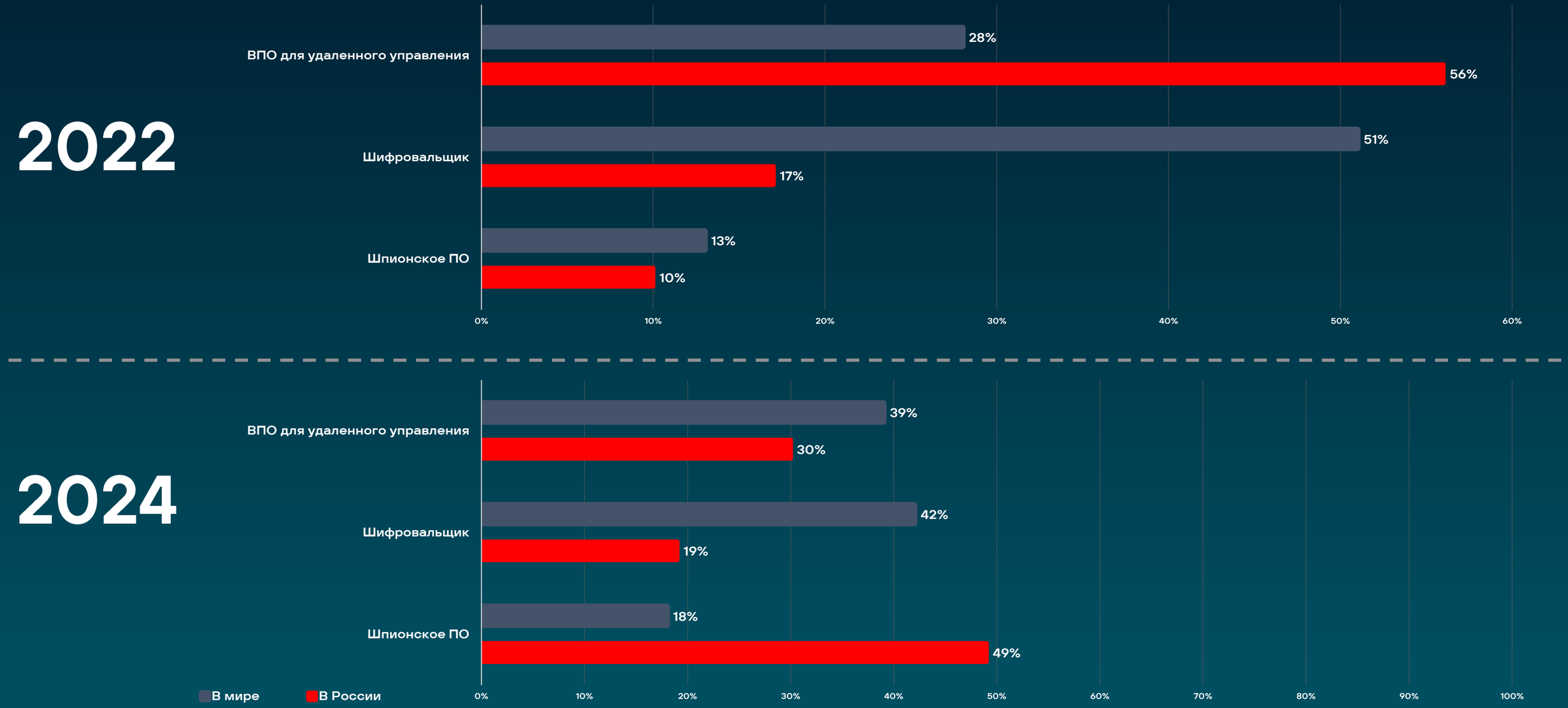
Наши исследования



Динамика методов атак на российские организации



Типы ВПО в атаках на Россию



Что повлияет на ВПО?

	Фактор	К чему приведет
Технологии	• Массовое внедрение Gen-AI • 5G/6G + Edge-Cloud • Унификация IoT/OT/IIoT	Дают вычислительную мощность и новые векторы: автономный анализ данных жертвы, скрытая передача через edge-узлы, атаки на «умные» фабрики
Геополитика	Расширение APT-операций «гибридного» типа	Шпионское ПО смещается в сторону киберразведки вместо чистой монетизации
Экономика дарквеба	• Malware-as-a-Service 2.0 • Маркеты zero-day в подписочной модели	Позволяет даже «не-технарям» арендовать модули слежки и таргетировать ниши

Организациям придётся сместить фокус с разовых антивирусных сканирований к непрерывной поведенческой аналитике, аппаратной верификации и прозрачным ML-процессам

MaaS 1.0 vs MaaS 2.0

	MaaS 1.0	MaaS 2.0
Архитектура C2	Централизованные сервера, простые HTTP/IRC	Децентрализованные P2P, блокчейн-маршрутизация
Модели оплаты	Покупка «китов» (каждый модуль отдельно)	Подписка, почасовая оплата, pay-per-victim
Уровень автоматизации	Ручная настройка, шаблонные пакеты	AI/ML-движок для подбора эксплойтов и оптимизации кода
Обновления и поддержка	Ручные апгрейды, простые патчи	CI/CD-конвейеры, Git-style versioning, canary release
Скрытность	Статический шифратор/обфускатор	Полиморфные и метаморфные движки, fileless-модули
Интеграция с даркнет-маркетами	Ручное размещение на форумах и хостингах	Автоматическая публикация на DNM-маркетах через API

Основные тенденции

Искусственный интеллект

Автоматизированный подбор уязвимостей в коде и конфигурациях CI/CD
Генерация «глубоких фейков» (deepfake-контента и поддельных цифровых сертификатов)

Рост атак на аппаратном уровне

Внедрение микро-чипов с бэкдорами на стадии производства.
Манипуляции прошивкой (firmware) IoT- и edge-устройств.

IoT/IIoT

Массовые векторы через «умную» промышленность (Smart Manufacturing).
Целевая компрометация оборудования «умных городов» и инфраструктуры энергетики

Атаки на контейнеры

Внедрение вредоносных слоёв в образы Docker и OCI
Саботаж через уязвимости в функциях Function-as-a-Service

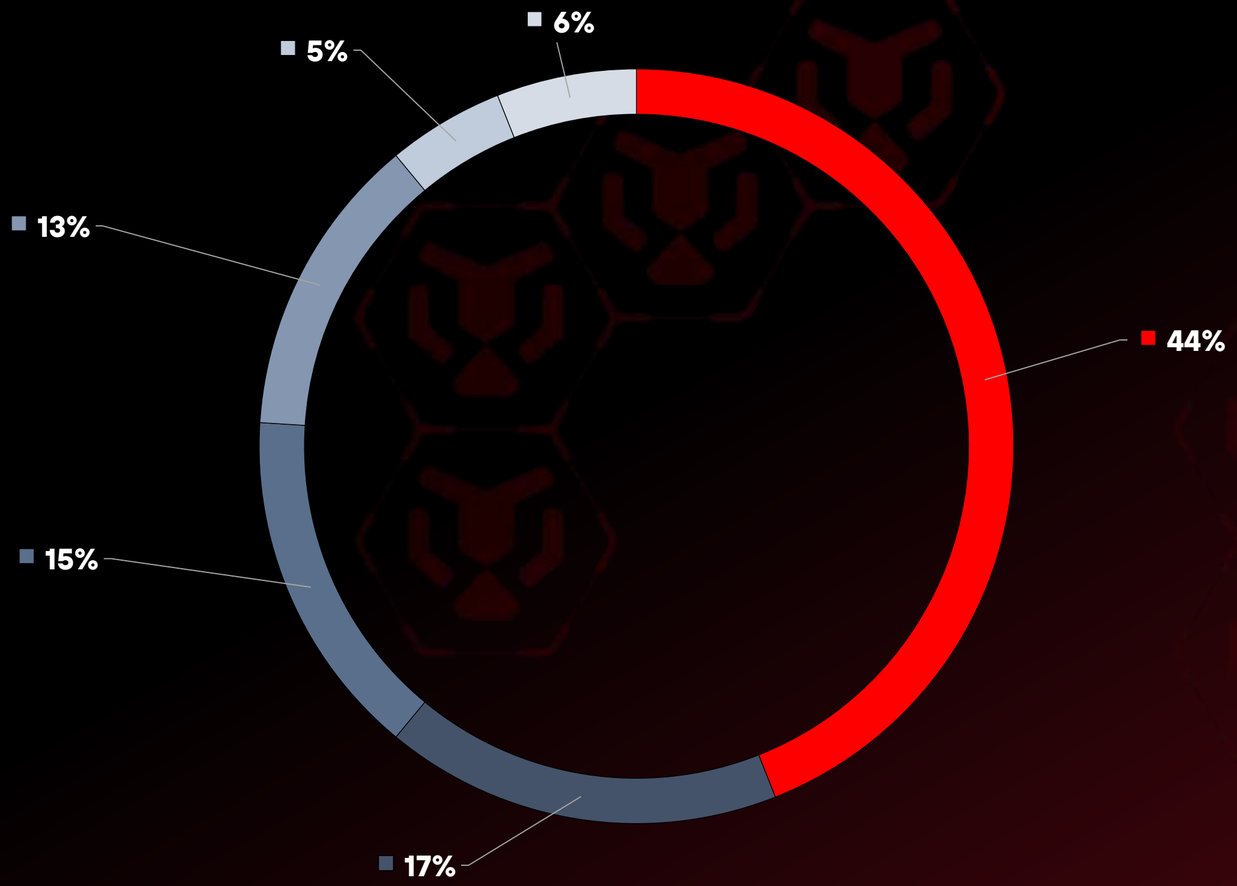
Квантовая угроза

Развитие квантовых компьютеров подрывает стойкость нынешних алгоритмов шифрования и ЭЦП

Что можно сделать уже сейчас?

Первоначальный доступ

По результатам проектов по расследованию инцидентов и ретроспективному анализу — 2023–2024



- Веб-приложения на сетевом периметре
- Фишинговые электронные письма, открытые сотрудниками
- Доверительные отношения (trusted relationship)
- Доступные извне сервисы, не относящиеся к веб-сервисам
- Уязвимости нулевого дня
- Другие

Уязвимости в российском ПО

33%

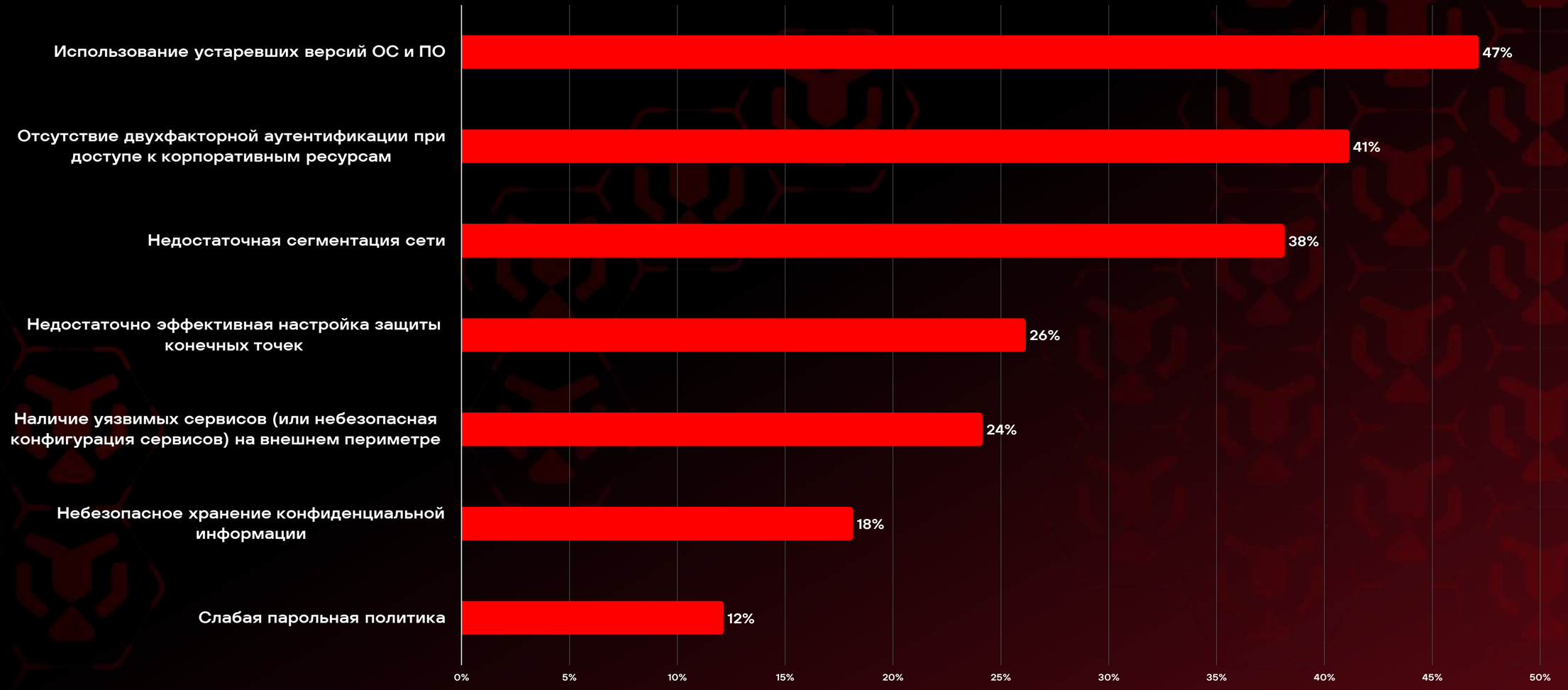
атак на сайты под управлением CMS «1С-Битрикс» (в прошлом году 13%). **ТОП 1 по количеству**

в **3 раза**

больше уязвимостей в российском ПО специалисты PT SWARM нашли в 2024 году (по сравнению с 2023)

Почему хакеры достигают цели

По результатам проектов по расследованию инцидентов и ретроспективному анализу — 2023–2024



Спасибо!