

**Владимир Клявин**

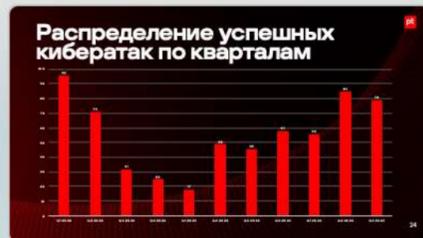
Коммерческий директор



**ИБ — Вызов 2030**



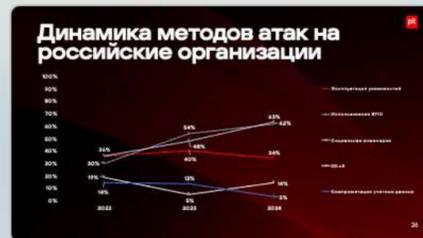
23



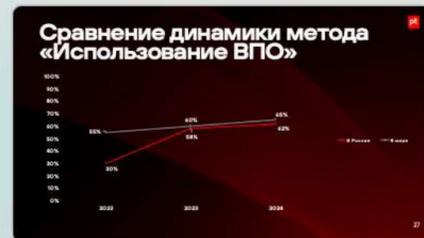
24



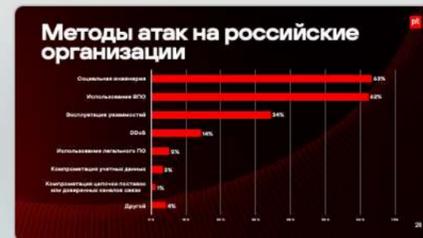
25



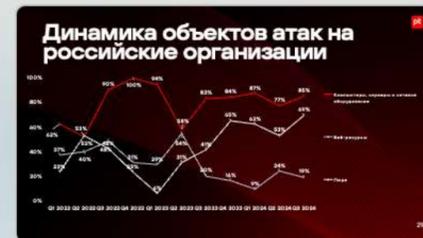
26



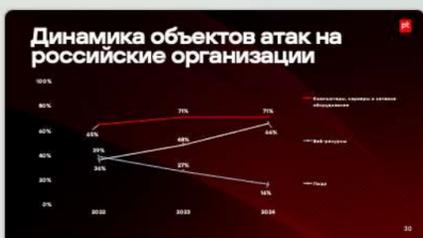
27



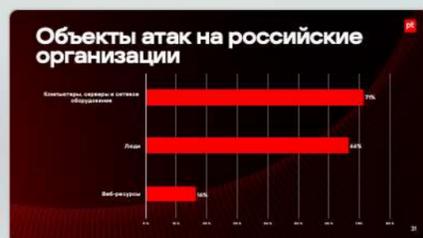
28



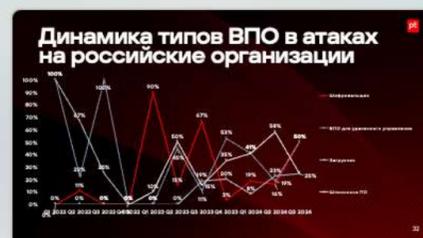
29



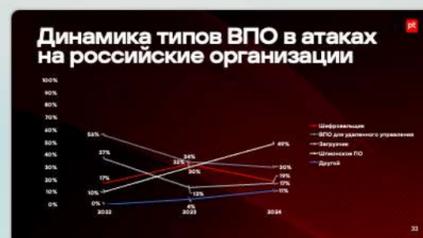
30



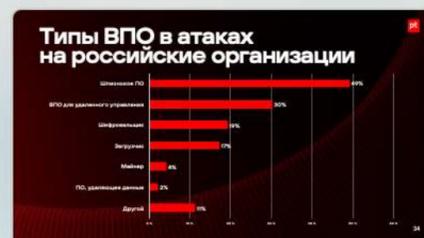
31



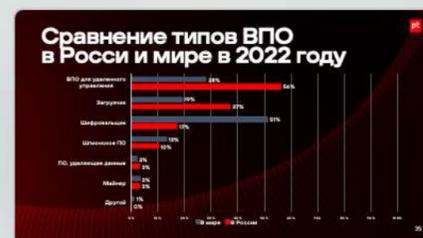
32



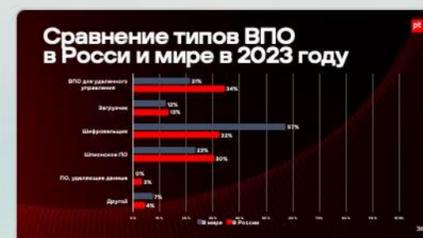
33



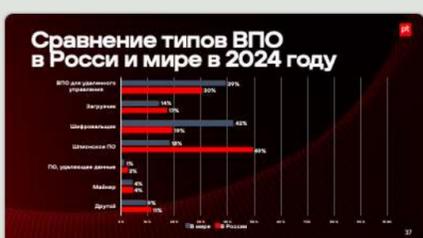
34



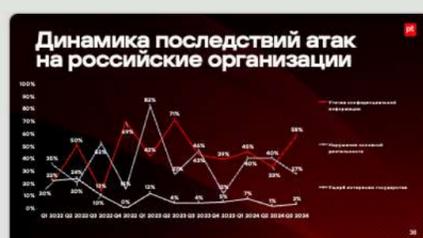
35



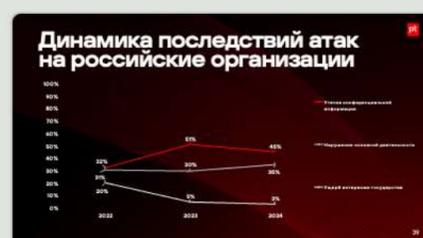
36



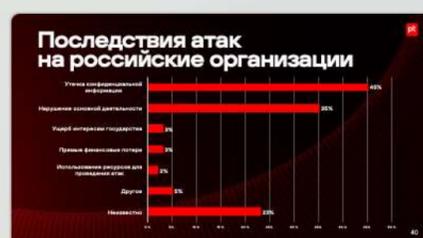
37



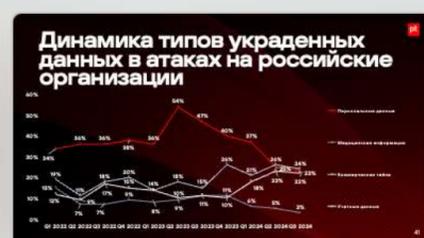
38



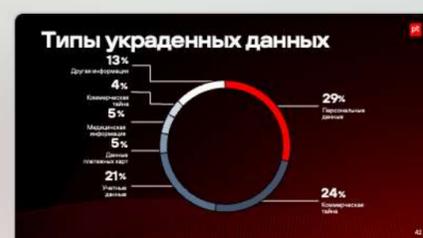
39



40



41



42



43



44



45



46



47



48



49

### PHDAYS FEST

## Как будут атаковать Россию в 2030 году

1 ★

### phdX pt

2 ★

### Количество успешных атак на Россию

3 ★

### С места в карьер

4 ★

### Что в общем и целом

5 ★

### Почему атаки будут более разрушительными?

6 ★

### Атака по одному клику

7 ★

### Все-as-a-service

8 ★

### Одно событие

9 ★

### Что будет с АРТ?

10 ★

### Информационная война?

11 ★

### Дипфейки в режиме реального времени

12 ★

### Какой будет информационная война в 2030?

13 ★

### Дорогу ВПО!

14 ★

### Доля успешных атак при помощи ВПО

15 ★

### Типы ВПО в атаках на Россию

16 ★

### Что повлияет на ВПО?

17 ★

### Матрица

18 ★

### И что дальше?

19 ★

### Supply Chain

20 ★

### Основные тенденции

21 ★

### Открытый, но небезопасный API

22 ★

### Какие тенденции?

23 ★

### Не баг, а закладка

24 ★

### IoT = Internet of Tragedies?

25 ★

### Устройства IoT

26 ★

### Edge

27 ★

### IoT в различных сферах

28 ★

### Угрозы для IoT

29 ★

### Атаки на энергетику и ICS/SCADA

30 ★

### Цифровые двойники

31 ★

### Цифровые двойники – как будут развиваться?

32 ★

### Атаки на цифровые двойники

33 ★

### Примеры атак

34 ★

### Еще

35 ★

### BCI

36 ★

### Пункт назначения

37 ★

### Куда едем

38 ★

### Куда приедем

39 ★

### «Пункт назначения»

40 ★

### Атаки на геолокацию

41 ★

### Медицине потребуется лечение

42 ★

### Развитие медицины

43 ★

### Атаки на медицинский IoT

44 ★

### BCI

45 ★

### BCI

### Где будет применяться к 2030?

### Как будут атаковать?

### Эволюция сценария применения биометрии

### Как будут атаковать биометрию?

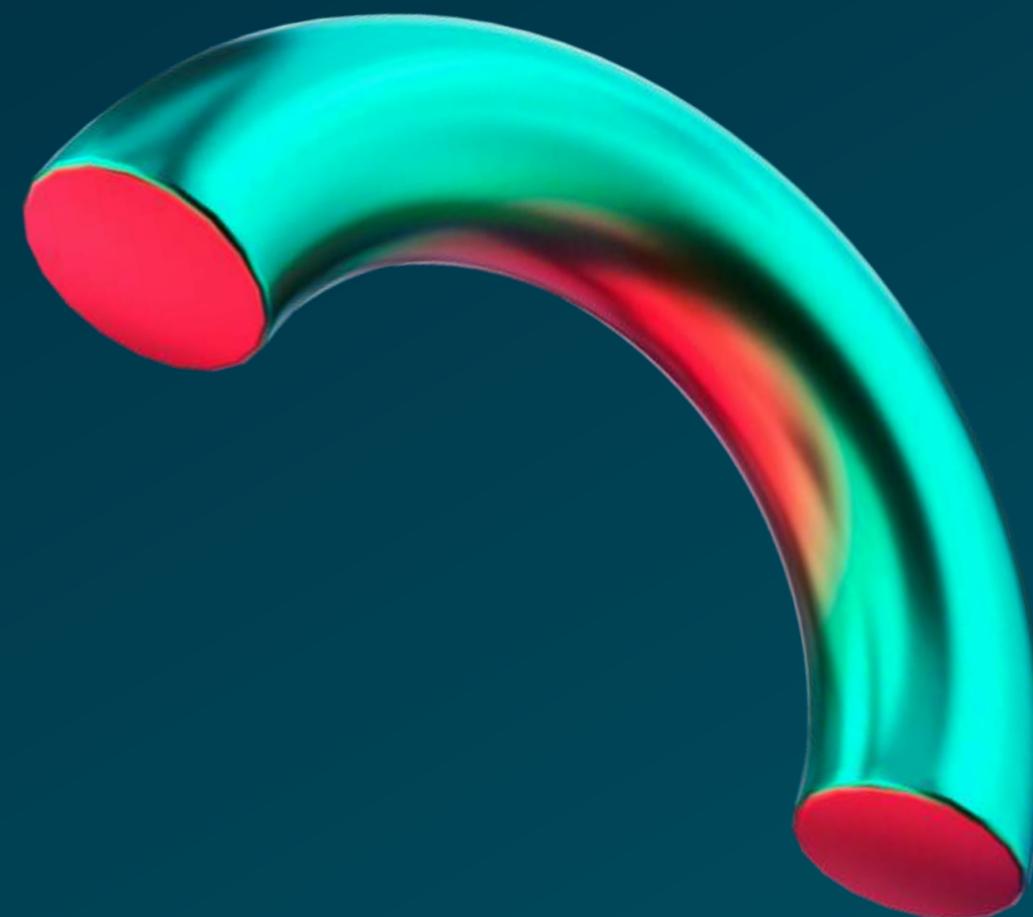
### Атаки на цифровые активы

### Блокчейн

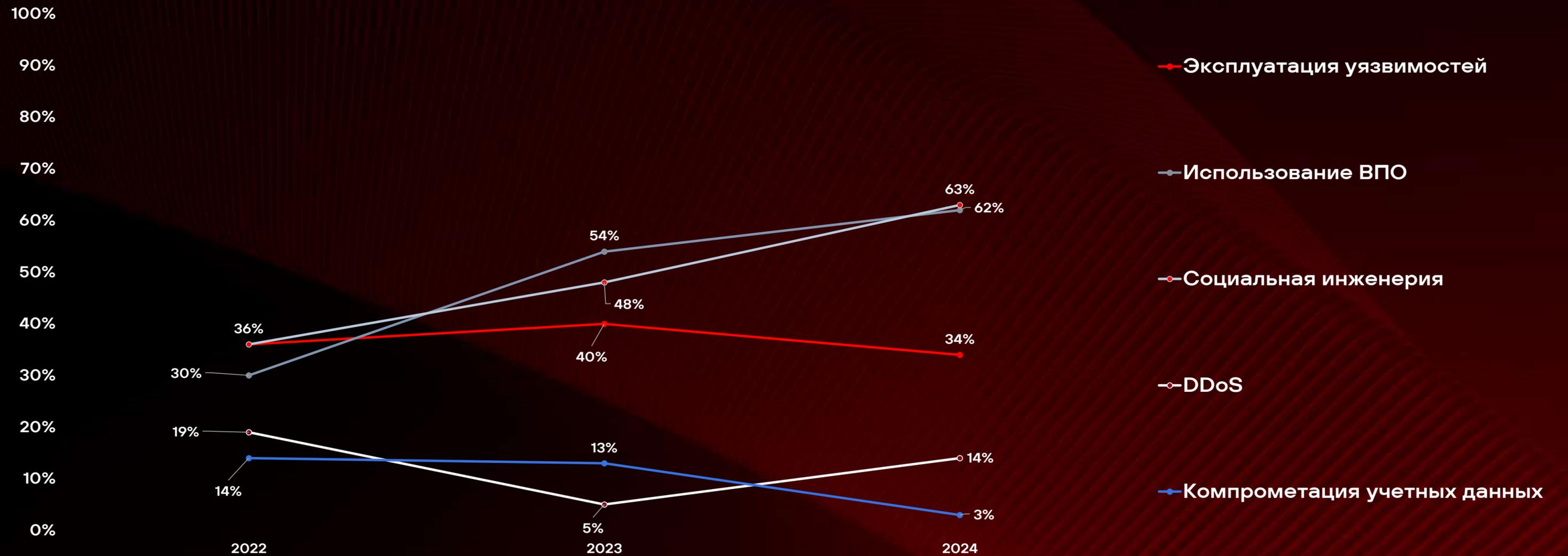
### Блокчейн

### Блокчейн

# Наши исследования



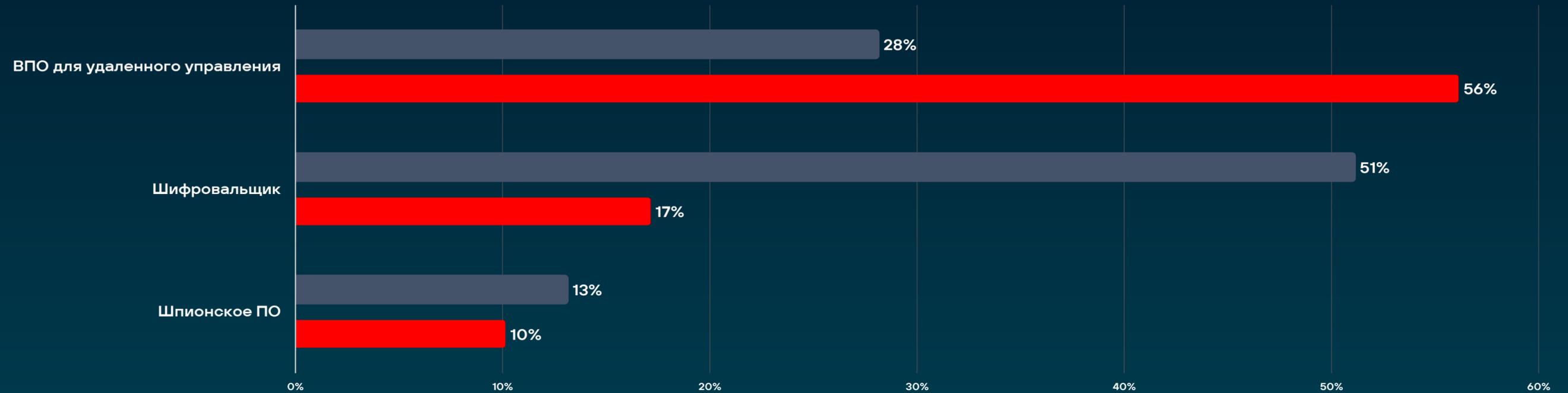
# Динамика методов атак на российские организации



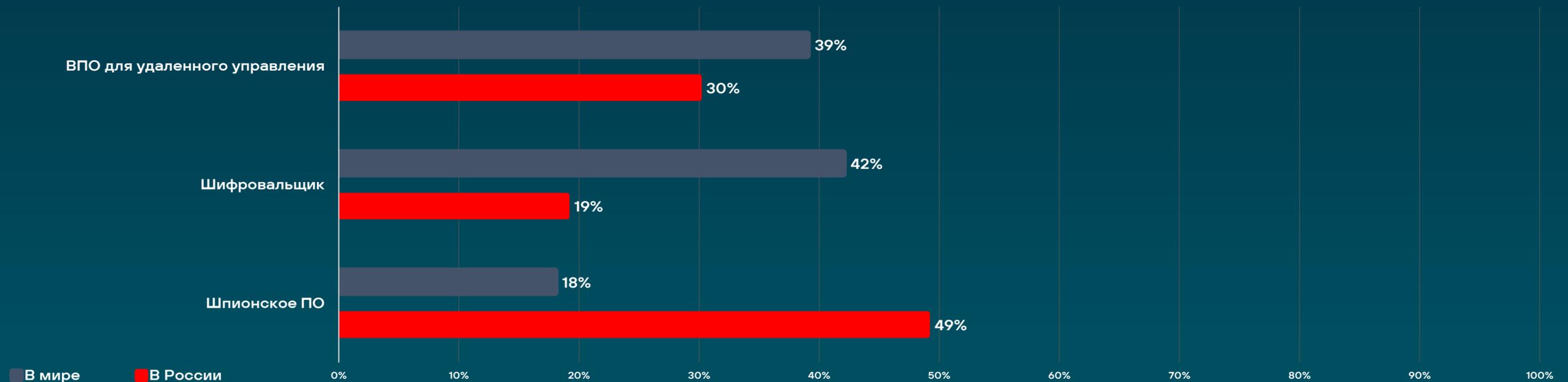
# Типы ВПО в атаках на Россию



2022



2024



# Что повлияет на ВПО?



## 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
<b>Архитектура C2</b>	Централизованные сервера, простые HTTP/IRC	Децентрализованные P2P, блокчейн-маршрутизация
<b>Модели оплаты</b>	Покупка «китов» (каждый модуль отдельно)	Подписка, почасовая оплата, pay-per-victim
<b>Уровень автоматизации</b>	Ручная настройка, шаблонные пакеты	AI/ML-движок для подбора эксплойтов и оптимизации кода
<b>Обновления и поддержка</b>	Ручные апгрейды, простые патчи	CI/CD-конвейеры, Git-style versioning, canary release
<b>Скрытность</b>	Статический шифратор/обфускатор	Полиморфные и метаморфные движки, fileless-модули
<b>Интеграция с дарквеб-маркетами</b>	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

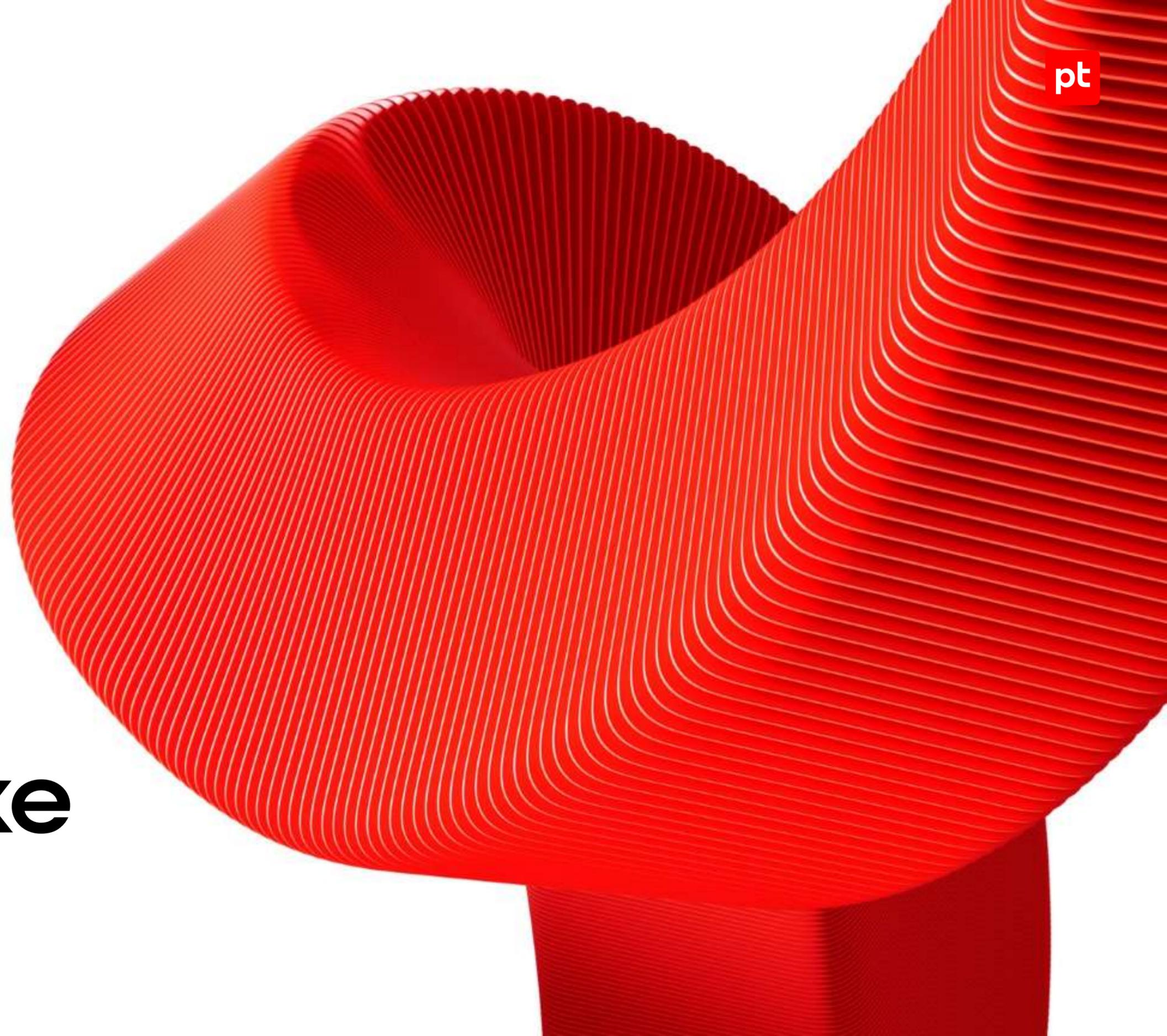
Внедрение вредоносных слоёв в образы Docker и OCI  
Саботаж через уязвимости в функциях Function-as-a-Service



## 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



# Уязвимости в российском ПО

## 33%

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

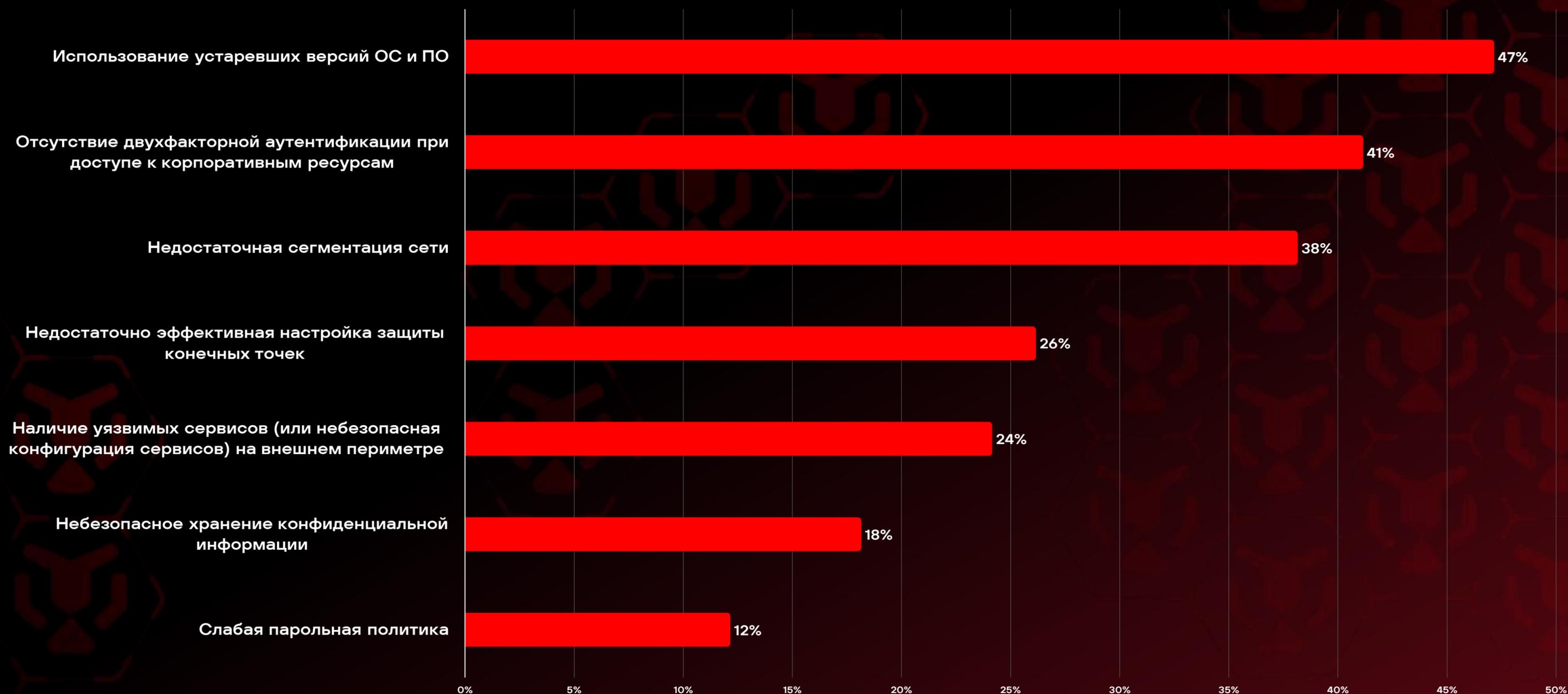
в **3 раза**

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!

