Азиз Мирбакиев
Пресейл-архитектор (СНГ)

Как противостоять APT-атакам

Или почему одних только
антивирусов не достаточно

Обеспечиваем практическую кибербезопасность

20 лет

опыта исследований и разработок

1,5+ тыс.

сотрудников: инженеров по ИБ, разработчиков, аналитиков и других специалистов

250+

экспертов в нашем исследовательском центре безопасности

200+

обнаруженных уязвимостей нулевого дня в год

250+

аудитов безопасности корпоративных систем делаем ежегодно

50%

всех уязвимостей в промышленности и телекомах обнаружили наши эксперты

- Создаем продукты и решения
- Проводим аудиты безопасности
- Расследуем инциденты
- Исследуем угрозы

Выпускаем более 20 исследований в год

- Ежеквартальные отчеты

об актуальных киберугрозах и трендах, прогнозы, расследования активности хакерских группировок, отраслевые исследования.

Наши проекты

STANDOFF

САМЫЕ КРУПНЫЕ В МИРЕ ОТКРЫТЫЕ КИБЕРУЧЕНИЯ

Команды этичных хакеров атакуют виртуальный город, находят уязвимости в корпоративных и промышленных IT-инфраструктурах, а специалисты по киберзащите выявляют и расследуют атаки. Участники киберучений SOC на базе наших продуктов мониторят инфраструктуру и выявляют угрозы.

standoff365.com

phd 12

ЕЖЕГОДНЫЙ МЕЖДУНАРОДНЫЙ ФОРУМ ПО ПРАКТИЧЕСКОЙ БЕЗОПАСНОСТИ

Выступления отечественных и зарубежных специалистов в области информационной безопасности, закрытые и открытые круглые столы с участием лидеров мнений, мастер-классы и лабораторные практикумы от известных экспертов.

phdays.com

BUG BOUNTY

BUG BOUNTY ОТ POSITIVE TECHNOLOGIES

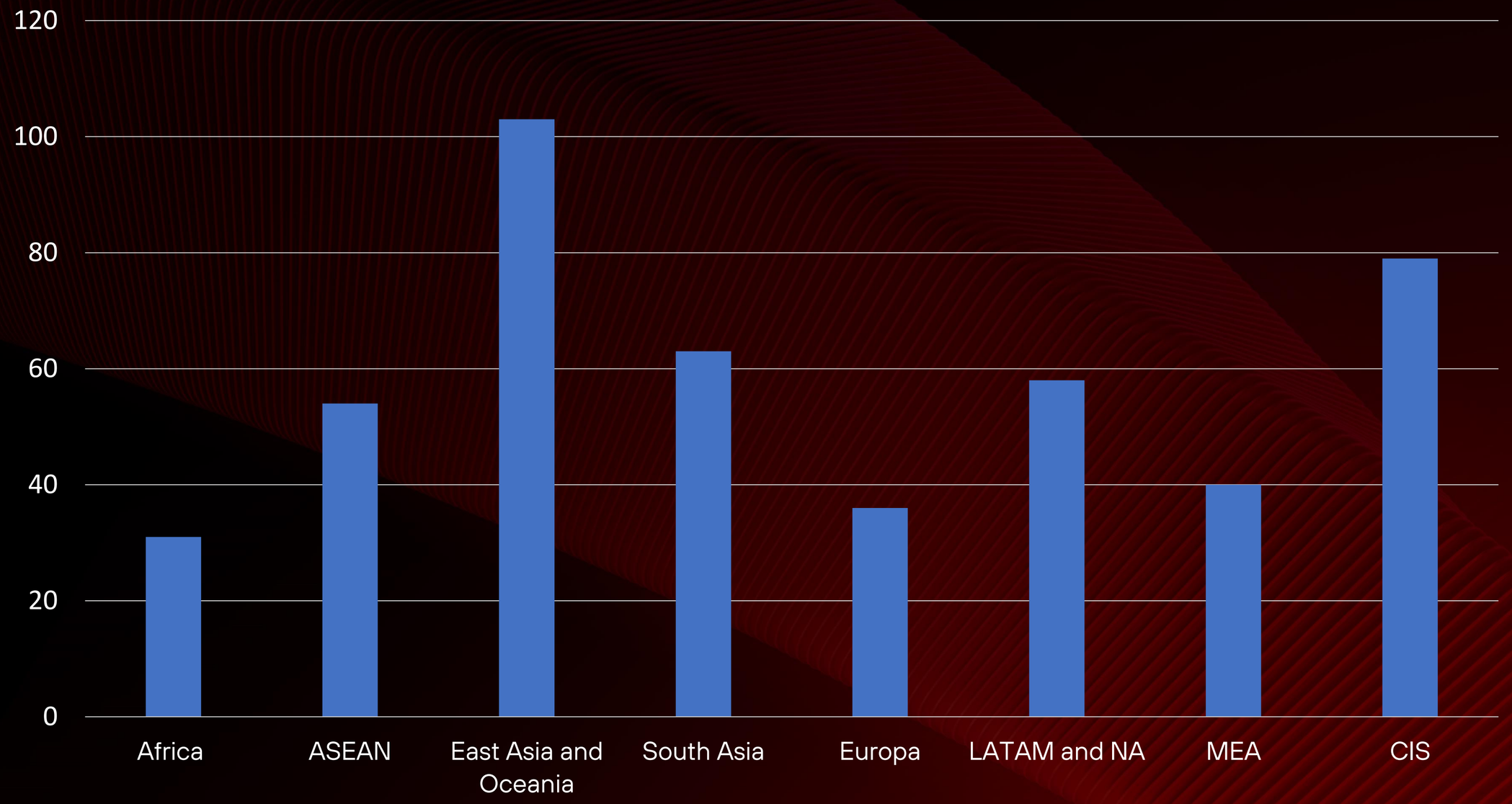
Bug bounty — это программа, в рамках которой компании привлекают сторонних специалистов по безопасности для тестирования своего программного обеспечения на уязвимости за финансовое вознаграждение.

bugbounty.standoff365.com

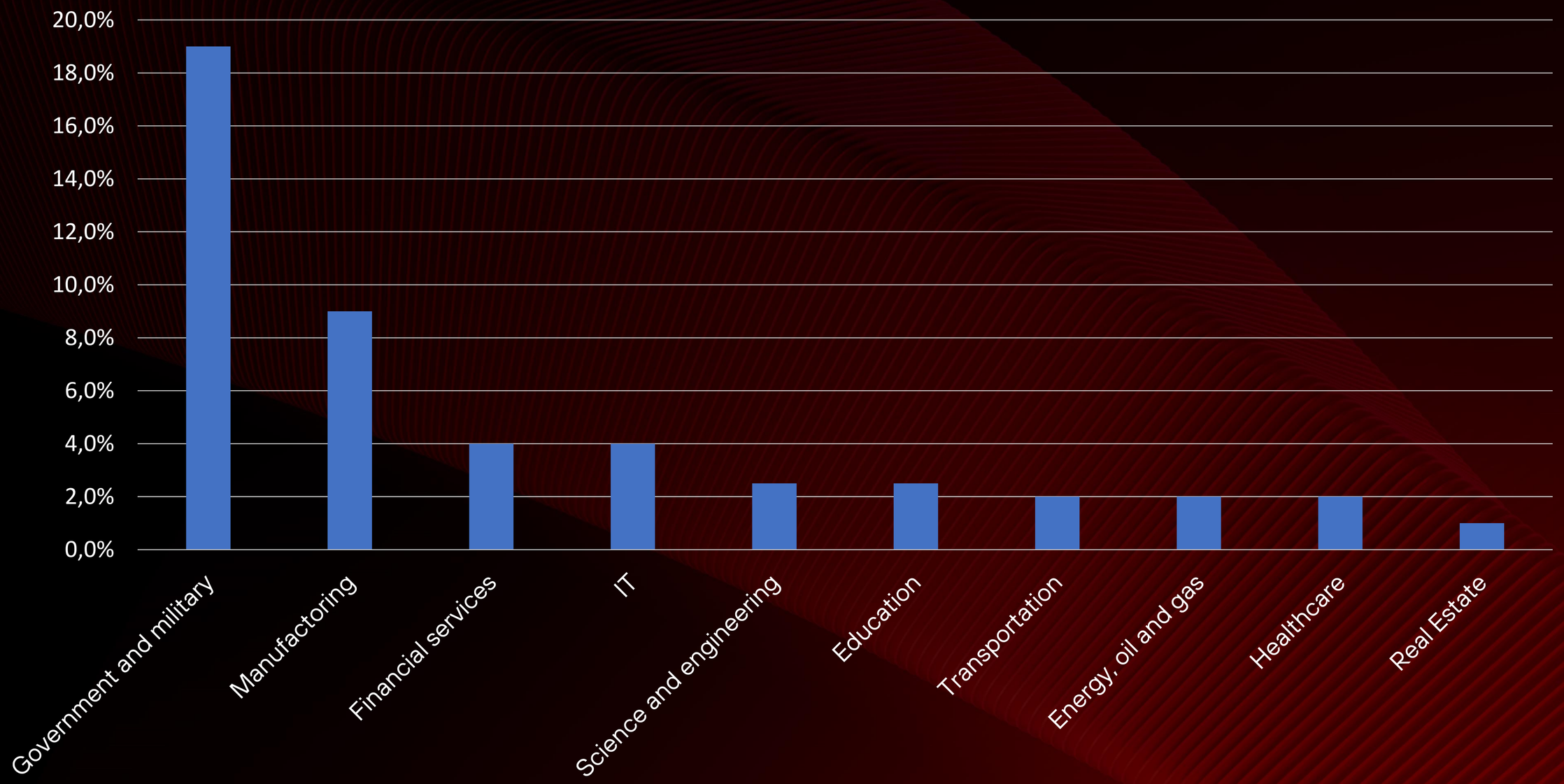
01

Статистика

Количество APT-групп, атаковавших регионы за 2024 год



Самые атакуемые отрасли APT-группами за 2024 год



Резюме

Количество атак

Во II квартале 2024 зафиксированно в 2,6 раз атак больше, чем во II квартале 2023

Кого атакуют

73% - Россия
8% - Казахстан
7% - Беларусь
18% - Госучреждения
11% - Промышленность
10% - Телекоммуникации

Интерес на теневых рынках

Во II квартале 2024 опубликовано на 35% больше объявлений, чем во II квартале 2023
40% объявлений связаны с базами данных, 70% из них раздают бесплатно

Как атакуют

Больше всего: использование ВПО и социальная инженерия

DDoS в СНГ – 18%
DDoS в мире – 8%

22% от атак ВПО - шифровальщики, из них 88% финансово мотивированы.
21% от атак шифровальщиков - промышленность

Кто атакует

18% - кибершпионские группировки, цель - госучреждения, промышленность, сферу науки и образования

26% - хактивисты, цель – кража данных и DDoS

Последствия атак

Для организаций:
41% - утечка конфиденциальных данных, основные: персональных данных (30%) и коммерческая тайна (29%)
37% - нарушение основной деятельности

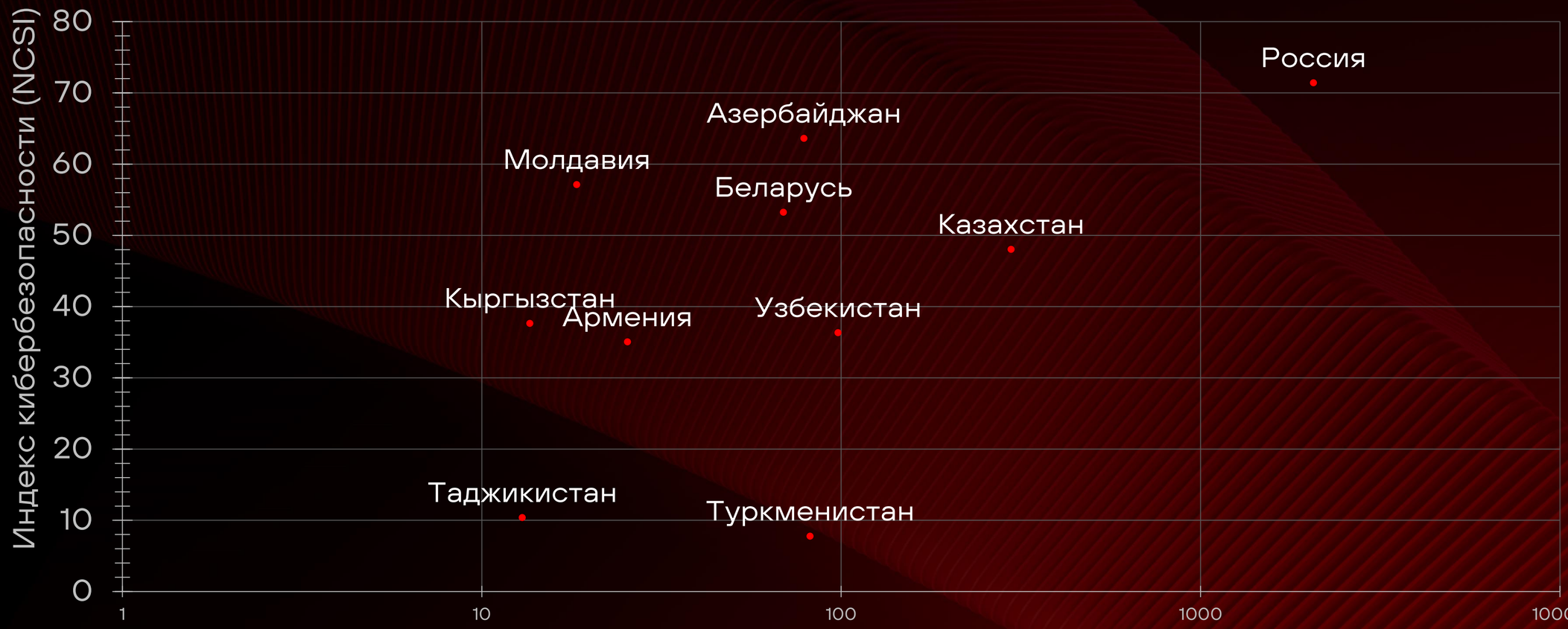
Для частных лиц:
69% - утечка конфиденциальных данных
32% - прямые финансовые потери

Цифровой статус СНГ

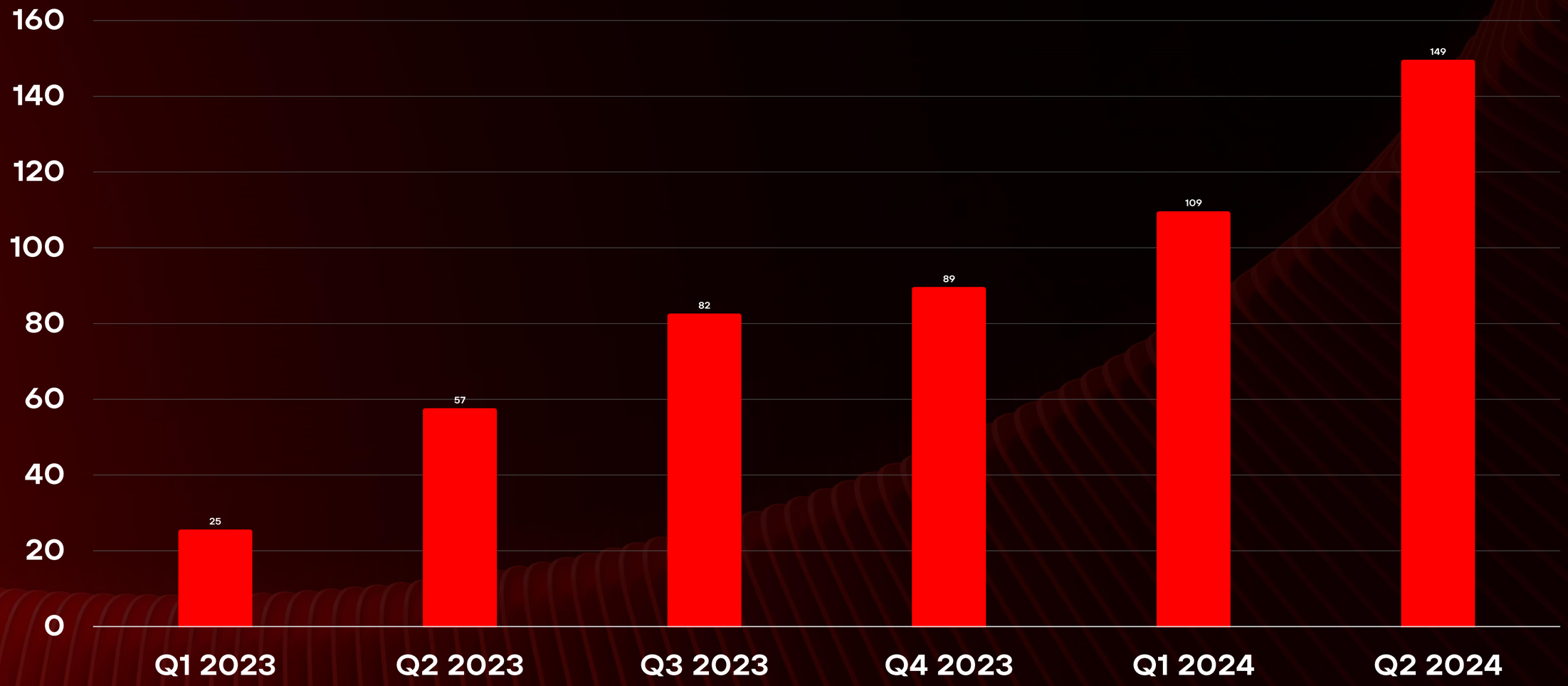
Соотношение численности населения и уровня проникновения интернета

Цифровой статус СНГ

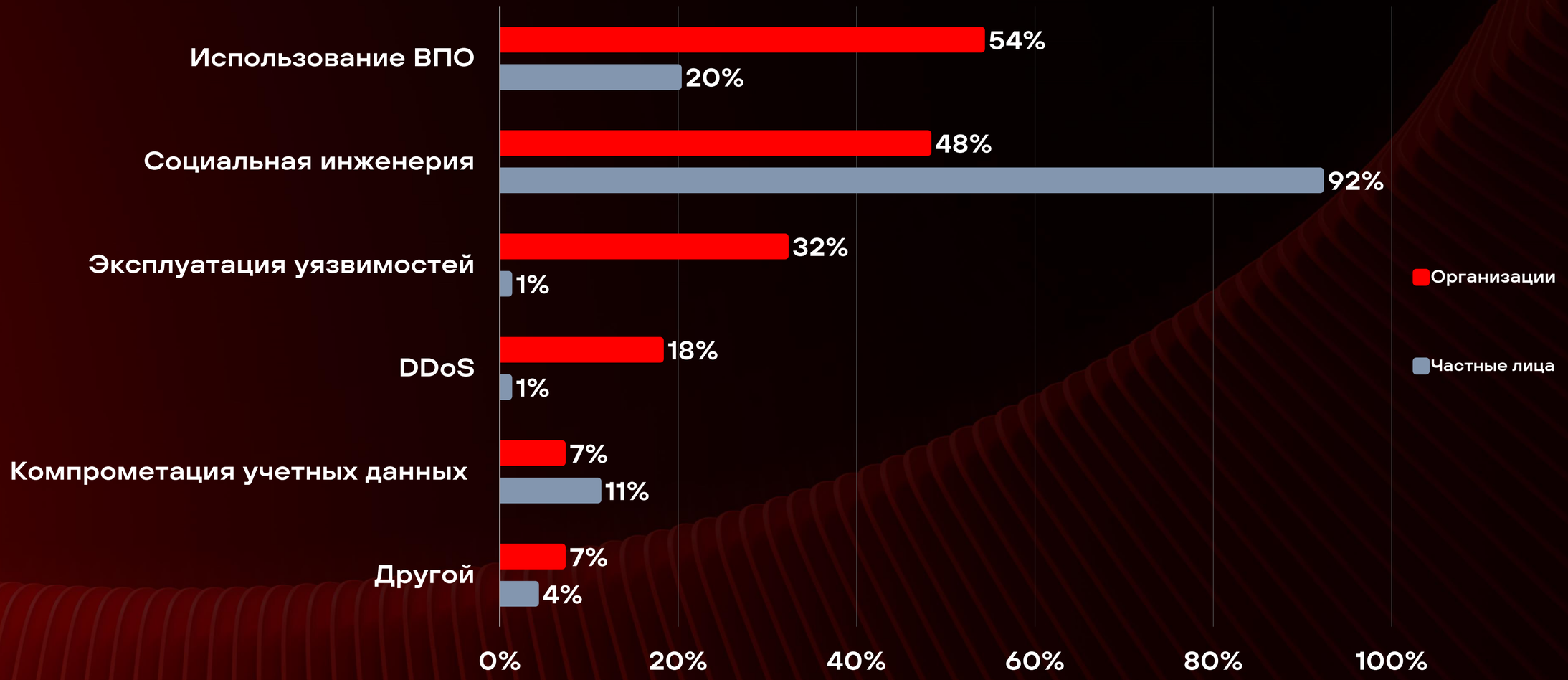
Соотношение индекса кибербезопасности (NCSI) и ВВП страны



Распределение успешных кибератак по кварталам

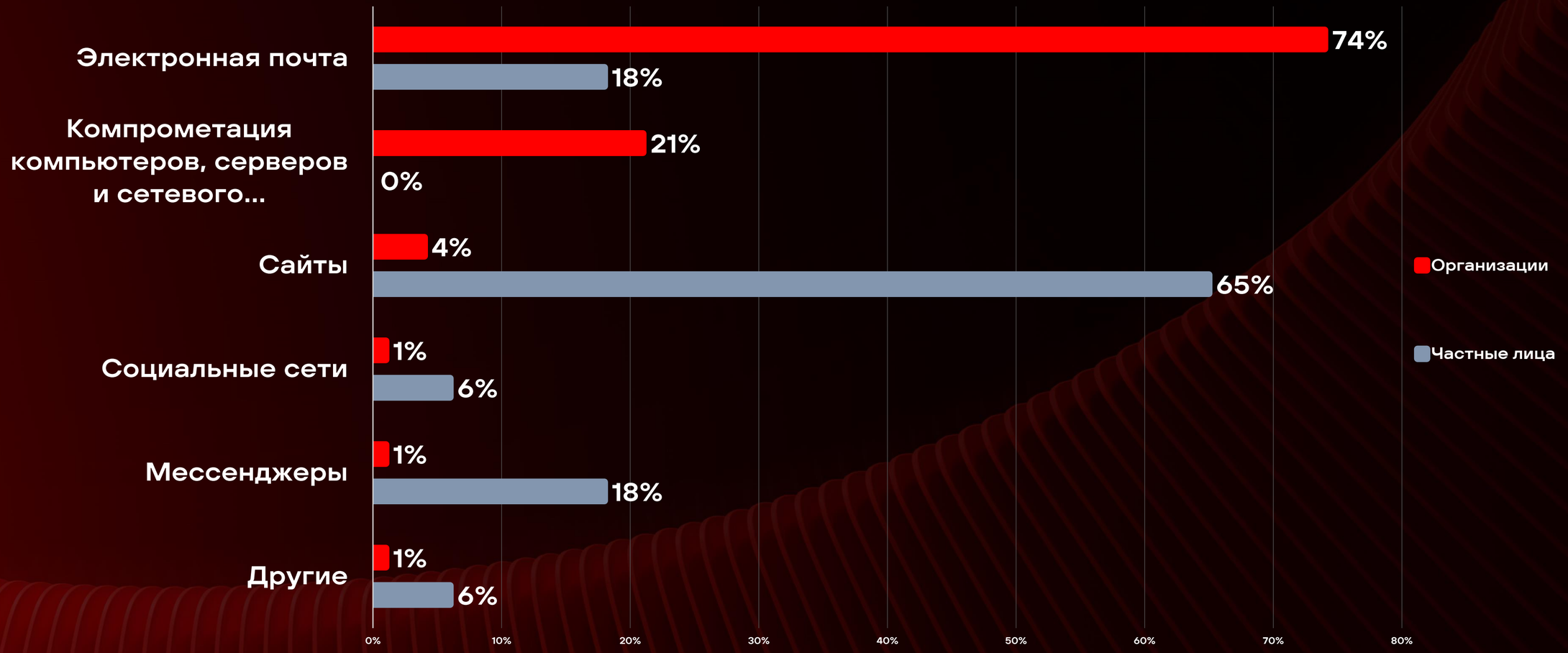


Методы атак на страны СНГ



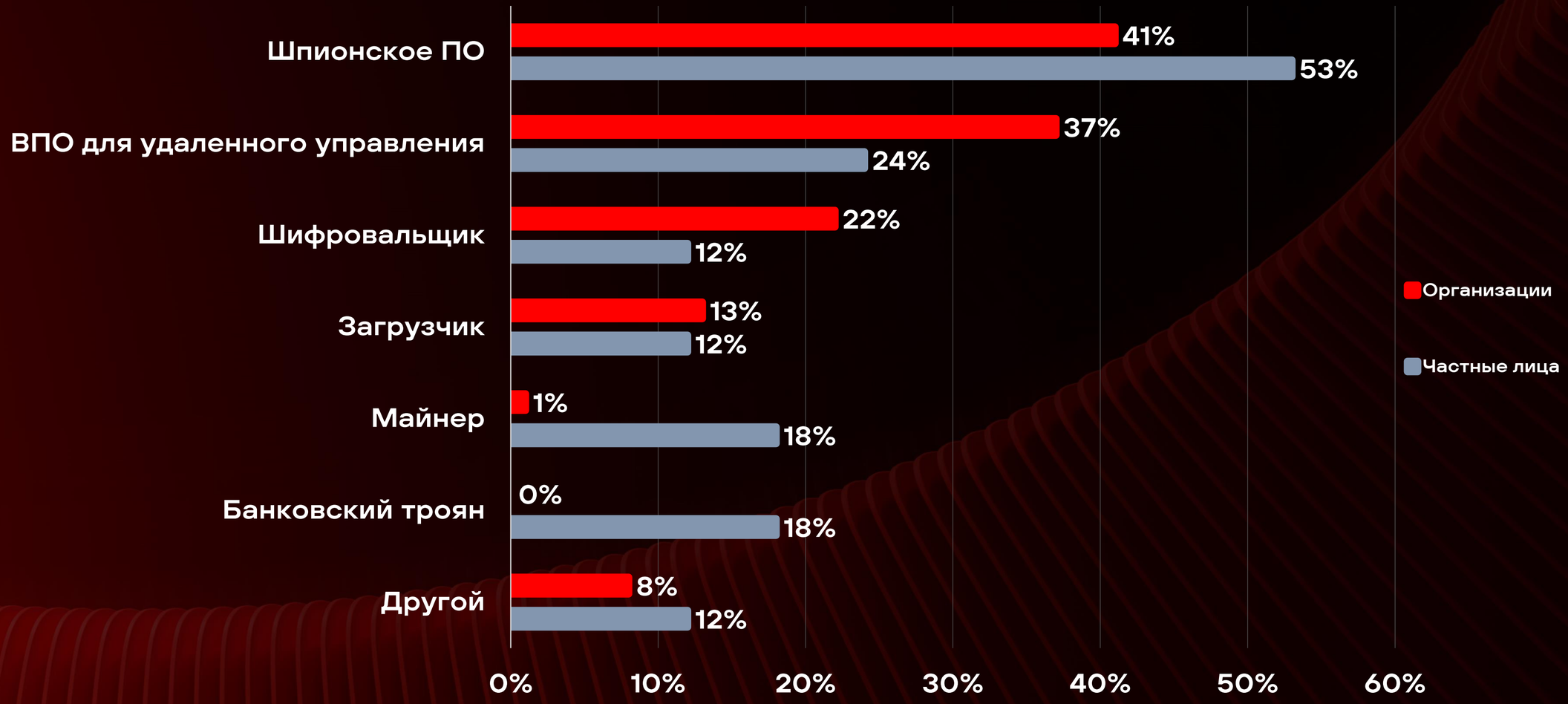
Способы распространения ВПО

(доля успешных атак с использованием ВПО)



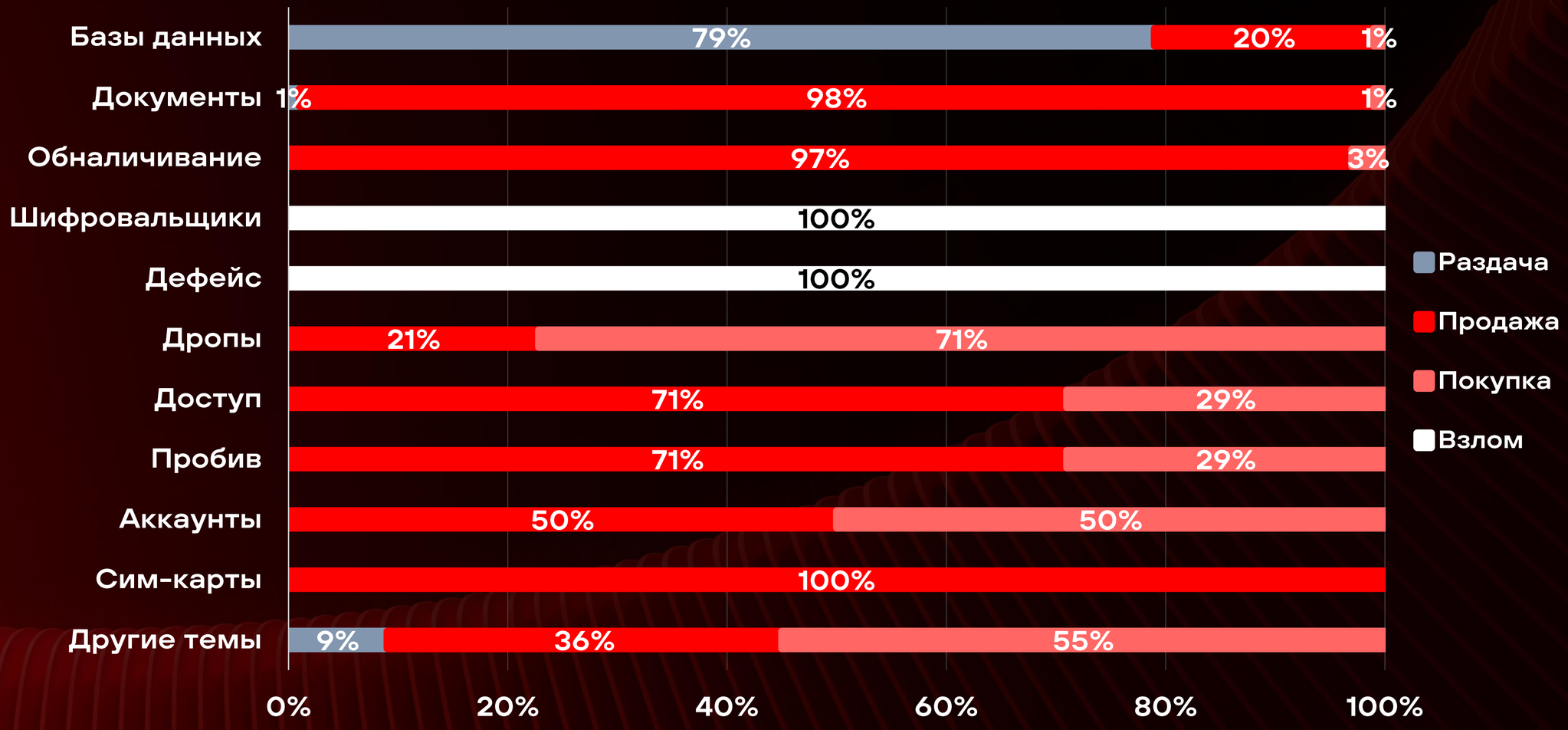
Типы ВПО

(доля успешных атак с использованием ВПО)



Типы объявлений

На теневых площадках



Цены на виды информации

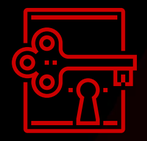
Продающейся на теневых площадках

Базы данных

100 – 50 000 долл. США

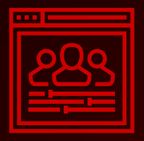
Документы

7 – 2 700 долл. США



Доступ

75 – 2 000 долл. США

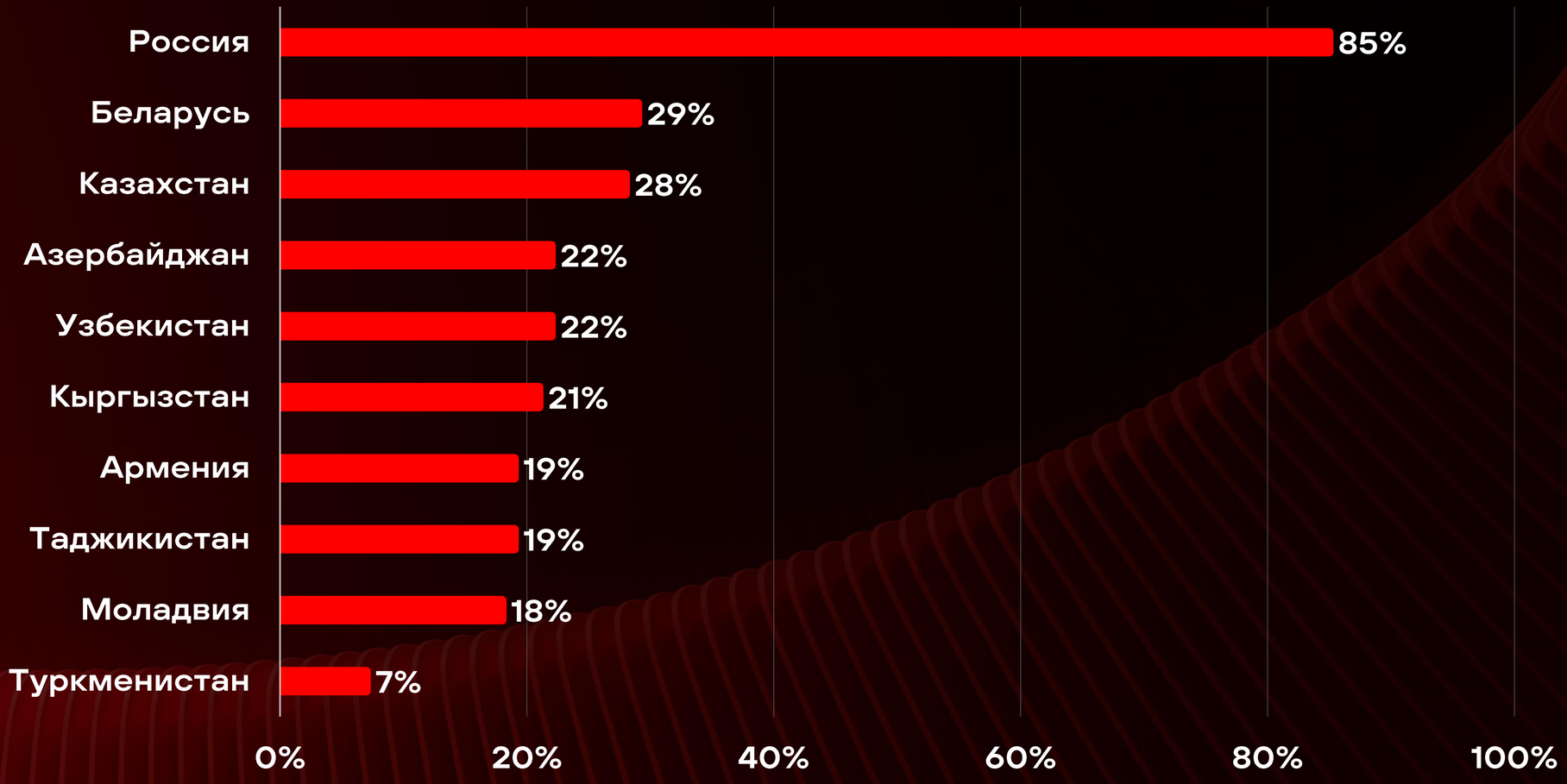


Аккаунты

50 – 170 долл. США

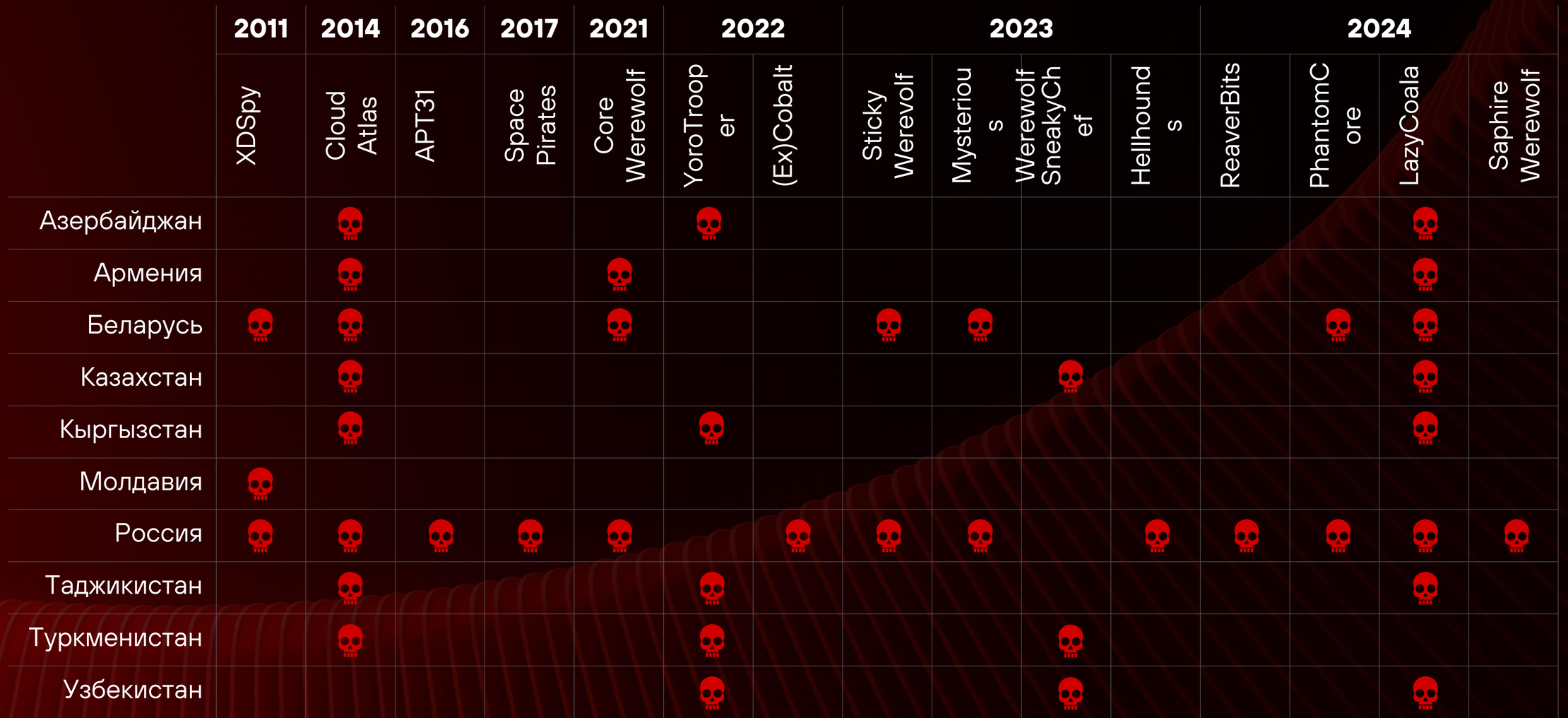
Распределение объявлений по странам

На теневых площадках



Самые активные группировки

(в странах СНГ в 2023 и 2024 годах)



02

Problemática

Антивирусные решения

- Нет полного покрытия конечных станций
- Нет защиты контейнеров
- Требуют много вычислительных и аппаратных ресурсов
- Нет защиты систем виртуализации и гипервизоров
- Не эффективны против угроз «нулевого дня»
- Неконтролируемая реакция на гипотетические угрозы
- Реагируют только на объекты (файлы, ссылки и т.д.)
- Учитывают «аномалию» только на уровне одного хоста
- Слаборазвитая защита сетевых соединений

Системы мониторинга сетевого трафика

Не собирают аналитику и не хранят исторические данные, включая сырой трафик

Плохо понимают техники и тактики злоумышленников

Профилируют трафик по типу, а не по угрозам и риску

Работают только с NetFlow и прочими *Flow потоками

Не имеют возможности проверить сомнительные объекты

Нет полноценного анализа трафика

Не умеют извлекать из трафика объекты для пост-анализа

Не работают с шифрованным трафиком

Могут видеть только уязвимости, а не сами угрозы и возможный инцидент

Файрволлы и межсетевые экраны

Не защищают от атак на cookies, токены, формы запросов (HTTP)

Не предназначены для точечной работы с протоколами (в частности HTTP / HTTPS)

Не позволяют применять «виртуальный patching» к защищаемой системе

Нет автоматического обучения и поведенческого анализа

Не позволяют терминировать трафик на себе и проксировать дальше

Не контролирует и не реагирует на ответы защищаемого ресурса

Не защищают от нелегитимных запросов к защищаемой системе

Не работают со сквозным шифрованным трафиком

Не коррелирует не связанные события между собой для вынесения вердикта

03

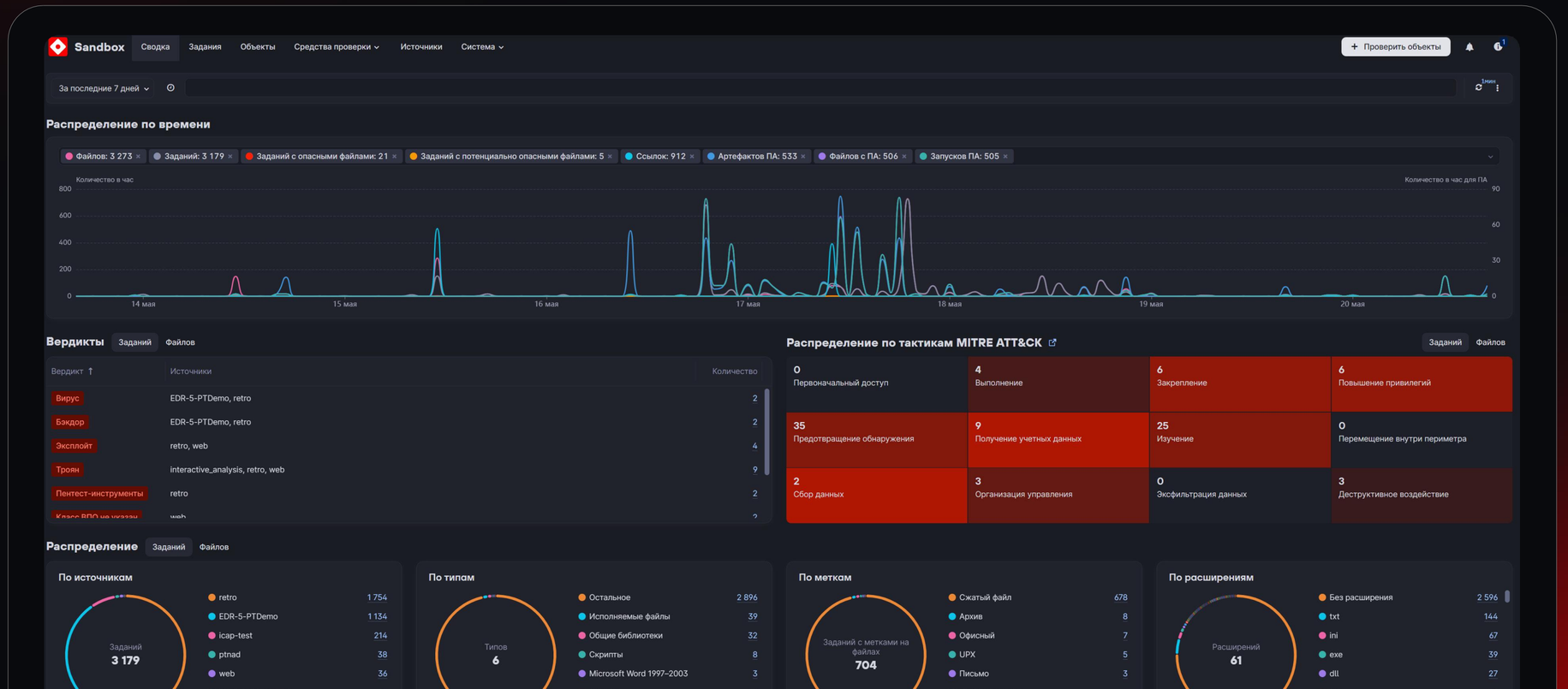
Решение задач

Песочница PT Sandbox

Обнаруживает вредоносное ПО на уровне гипервизора, операционной системы и виртуальной машины

Легко встраивается в инфраструктуру и контролирует основные каналы передачи файлов и ссылок

Адаптируется к особенностям бизнеса, обеспечивая защиту от целенаправленных атак



Как работает PT Sandbox

Песочница получает объекты из различных типов источников, обрабатывает файлы и ссылки и определяет в них вредоносное содержимое

PT Network Attack Discovery

Система поведенческого анализа сетевого трафика для обнаружения скрытых кибератак
Точно обнаруживает действия злоумышленников в сети, упрощает расследование инцидентов и помогает в проактивном поиске угроз

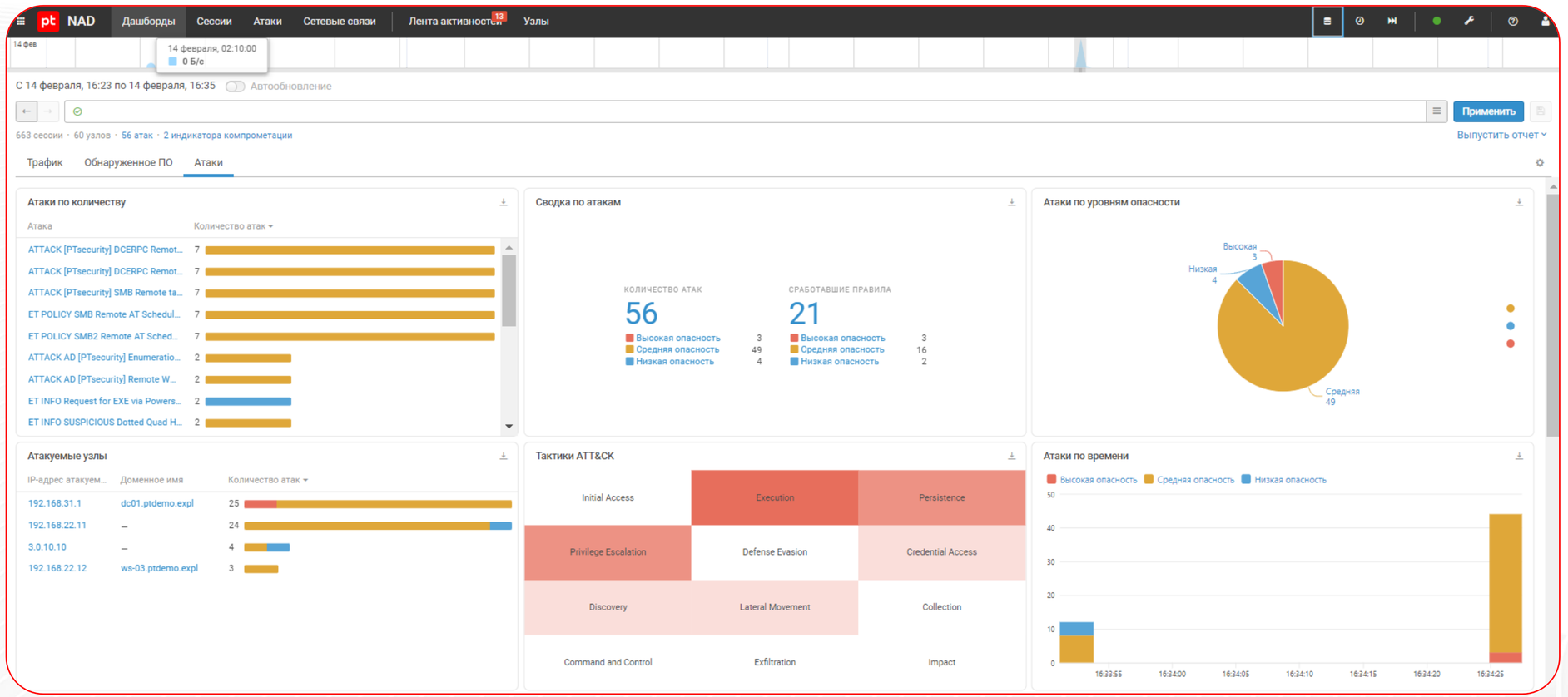


Рисунок 1. Дашборд PT NAD

PT NAD

Точно выявляет сложные сетевые атаки и сокращает время обнаружения хакеров до одного часа

Упрощает расследование инцидентов и показывает слабые точки в сети

Сокращает время реагирования на приоритетные угрозы

РЕЗУЛЬТАТ

Сокращает время присутствия злоумышленника в сети до считаных минут

Как работает PT NAD

Захватывает, разбирает сетевой трафик на периметре и в инфраструктуре с помощью технологии DPI

Исходная копия сетевого трафика

Видимость сети

Обнаружение хакера в сети

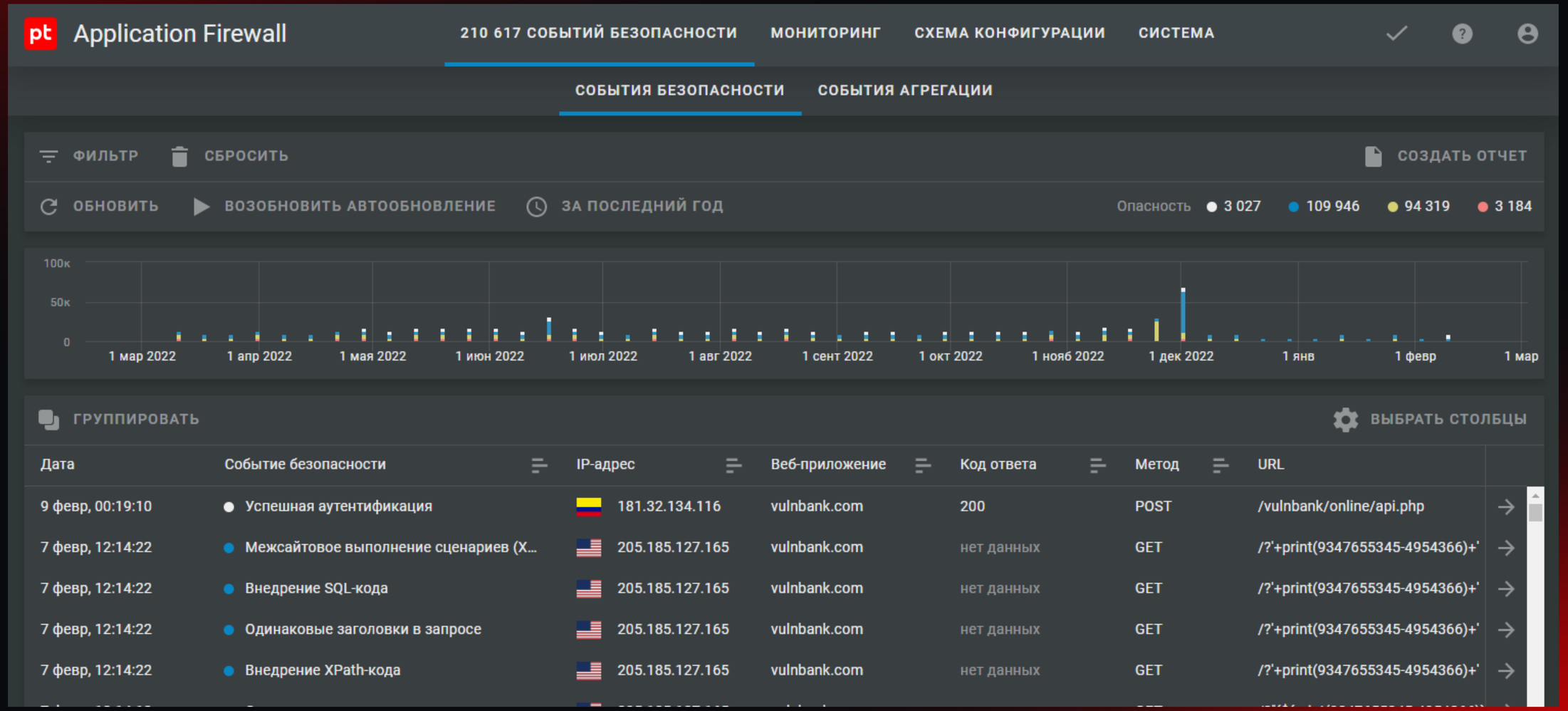
Аномалии

Контроль регламентов ИБ

SOC

С помощью статистических и поведенческих модулей обнаруживает активность злоумышленника на самых ранних этапах проникновения в сеть, а также во время попыток закрепиться в ней и развить атаку

PT Application Firewall PRO



PT Application Firewall PRO

- Анализирует прикладной трафик, специализируется на анализе HTTP/HTTPS
- Учитывает бизнес-логику работы приложений
- Детектирует и предотвращает распределенные по времени атаки
- Защищает API веб-приложения

Возможности PT Application Firewall

БЛОКИРУЕТ МАССОВЫЕ И ЦЕЛЕВЫЕ АТАКИ

Благодаря комбинации защитных механизмов и экспертизе Positive Technologies, PT Application Firewall обеспечивает комплексную защиту от известных угроз и атак нулевого дня.

БЫСТРО ВСТРАИВАЕТСЯ В ИНФРАСТРУКТУРУ

PT Application Firewall имеет встроенный мастер настройки и предустановленные шаблоны политик безопасности, благодаря которым его легко установить и использовать.

АДАПТИРУЕТСЯ ПОД ЗАЩИЩАЕМЫЕ ПРИЛОЖЕНИЯ

PT Application Firewall сочетает в себе «коробочность» и возможности тонкой настройки, что позволяет ему работать одновременно с большим числом приложений разной степени сложности и значимости.

Следите за нами

habrahabr.ru/
company/pt

t.me/
positive_technologies

vk.com/
ptsecurity

t.me/
positive_investing

Артём Нюхалов

Территориальный
менеджер по продажам,
Центральная Азия

Спасибо!