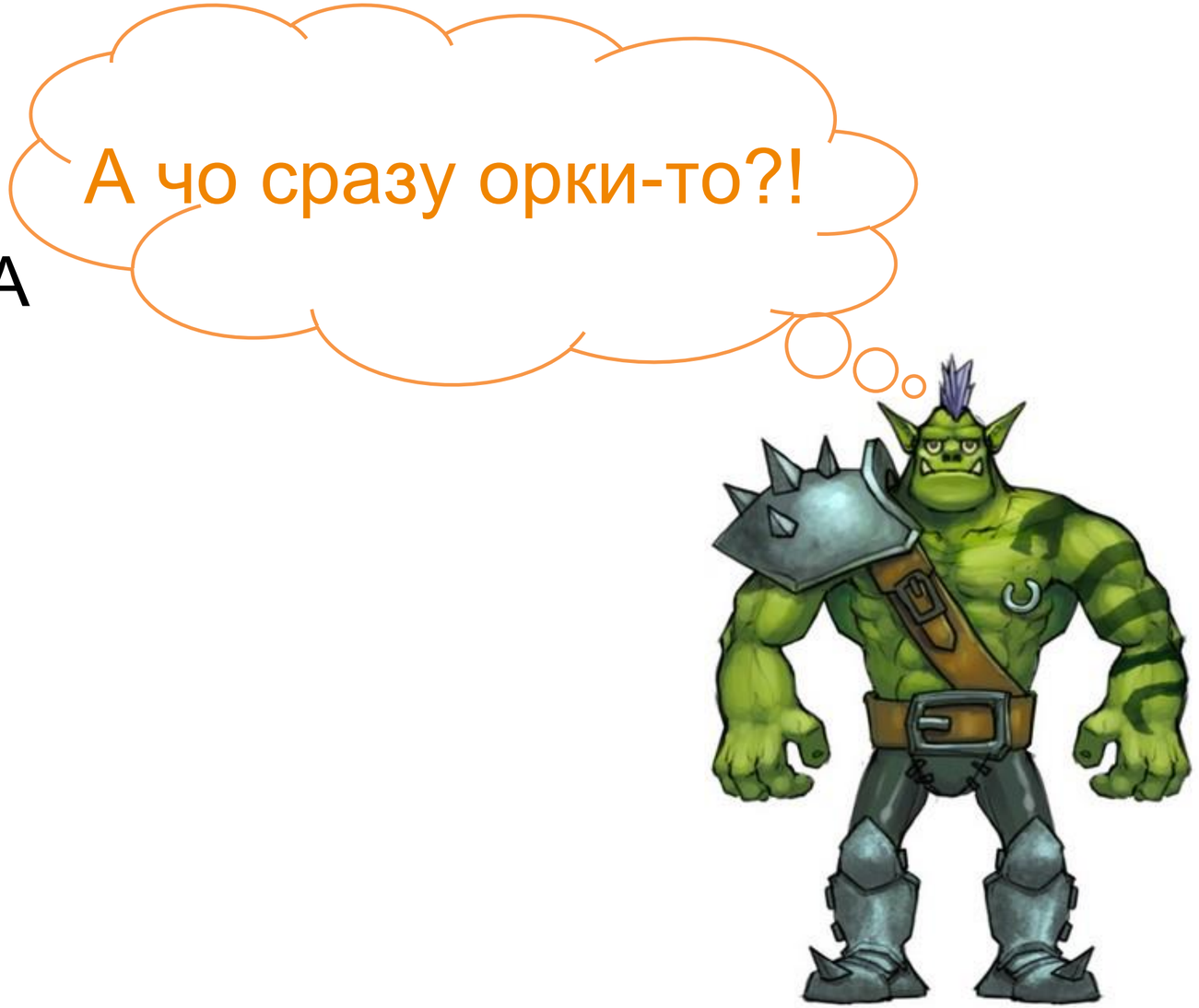
# Вкатываемся в 2025 по ландшафту угроз

Сергей Нейгер
Директор по развитию бизнеса ПМ

# Как хакеры, только добрые

# Четыре отдела

- Корпцентр ГосСОПКА
- ОИК
- НИИП
- ОРКИ



# Уже сделали отчёты:

- Исследование китайской APT-группировки Space Pirates
- Исследование индийской APT-группировки APPIN
- Исследование APT-группировки, про которое нельзя рассказывать

# Сегодня — инфа из новых отчётов

Лайк, подписка, колокольчик ☺

Перспективный мониторинг


**Исследование: ландшафт киберугроз за 2024 год**

Сотрудники «Перспективного мониторинга» провели глубокое исследование тенденций и угроз в области кибербезопасности за 2024 год.

**Что вошло в отчёт:**

- типы кибератак;
- наиболее часто используемые тактики, техники и процедуры (ТТП);
- эксплуатируемые уязвимости.

Цель документа — повышение осведомлённости и подготовленности безопасности инфраструктуры с целью выработки компаниями эффективных стратегий защиты.

ℹ️ Скачать документ и ознакомиться с ним вы сможете через бота ПМ. В стартовом меню выберите кнопку «Исследования» и следуйте инструкции. Если вы уже пользовались ботом, сначала перейдите в стартовое меню при помощи команды /start.

Скачать Ландшафт киберугроз за 2024 год

🔥 5 👏 2 🤔 1 483 edited 17:00

@PM_PUBLIC

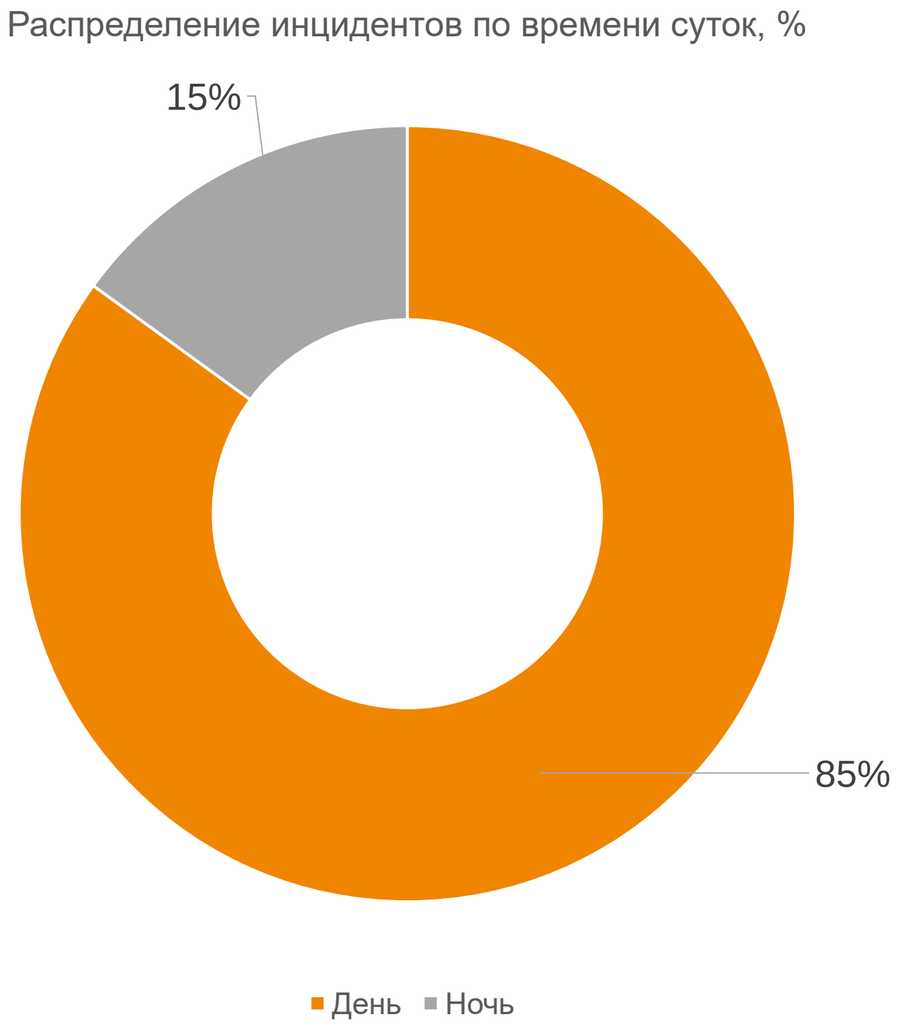
# Мониторинг за 2024 год

**4117**
компьютерных
инцидентов

# Мониторинг за 2024 год

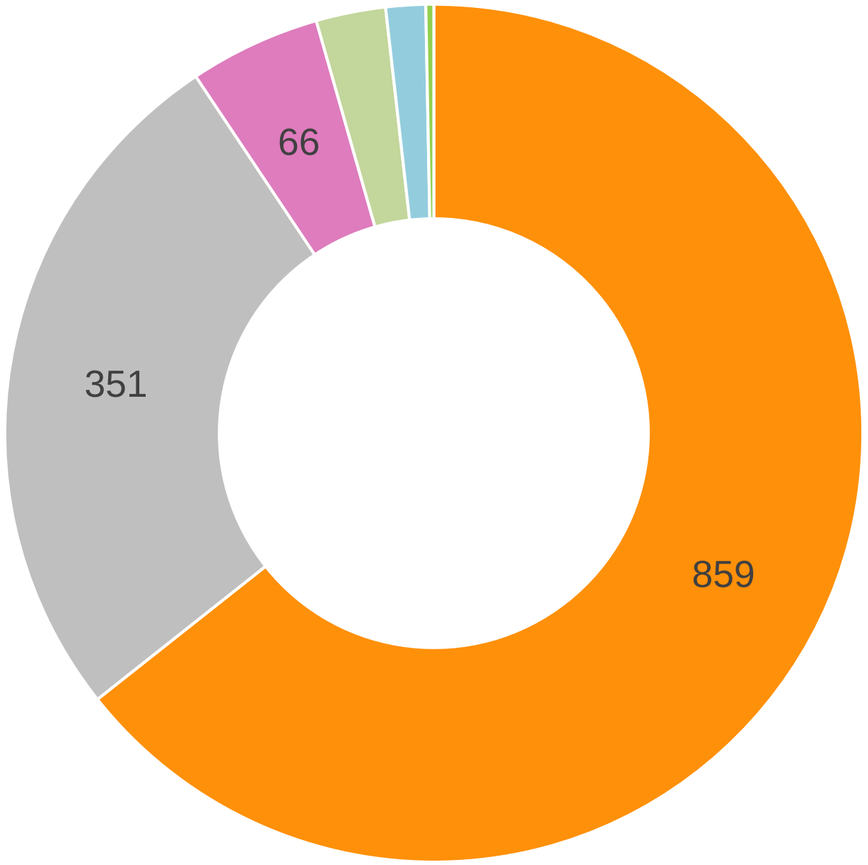
1. Ночью чуть больше доля инцидентов высокой и максимальной критичности

2. Поэтому мониторинг 24/7 всё-таки нужен. Желательно, конечно, и реагирование тоже



# Мониторинг за 2024 год

**1335**
компьютерных атак




- Сетевое сканирование
- Попытки эксплуатации уязвимости
- Неудачные попытки авторизации
- DDoS-атака
- Попытки внедрения ВПО
- Социальная инженерия

# Топ-10 CVE

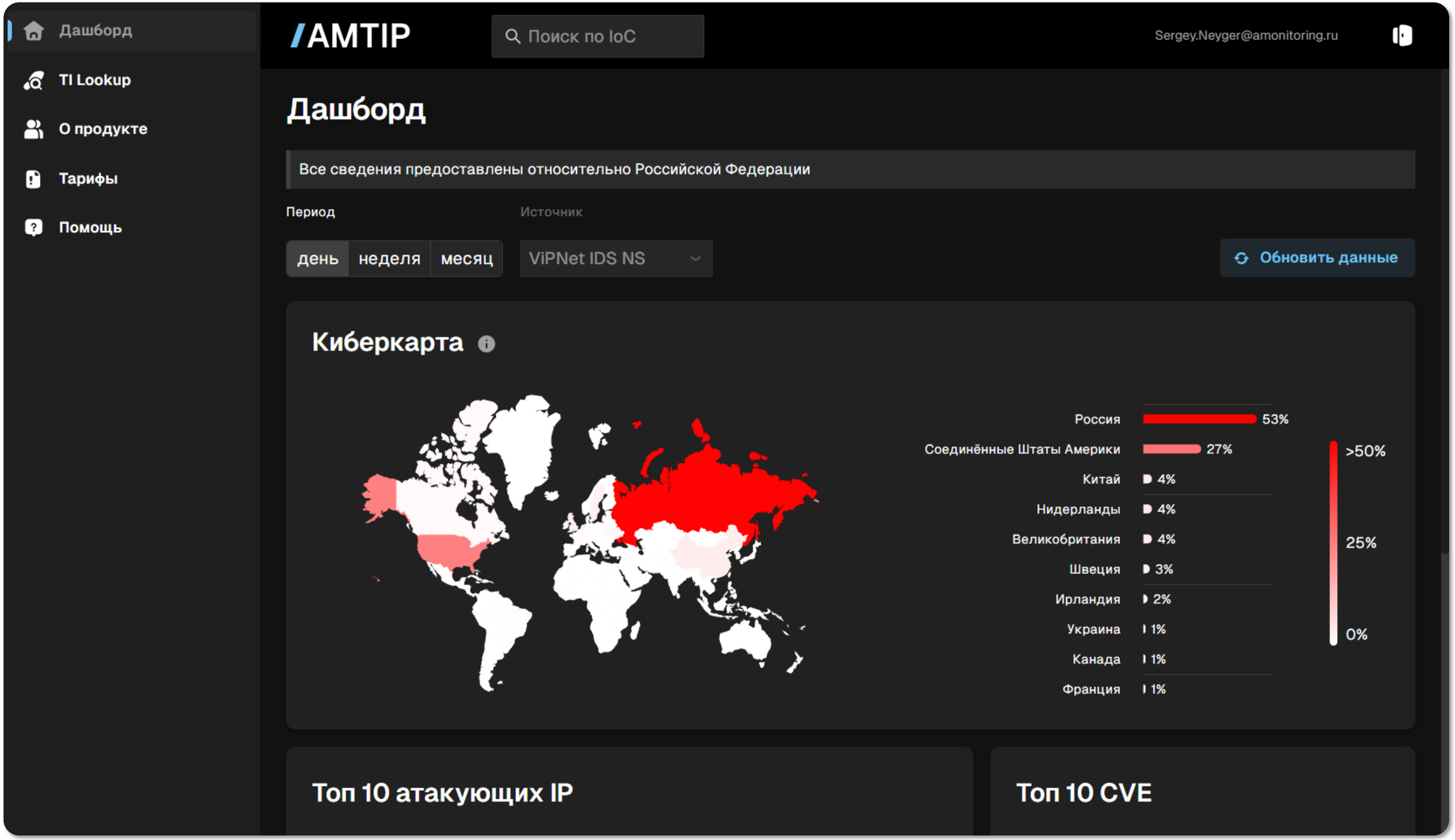
| | |
|---|---|
| 2020-5761 | Grandstream HT800 series firmware version 1.0.17.5 and below |
| 2022-0289 | Use after free in Safe browsing in Google Chrome prior to 97.0.4692.99 |
| 2018-6892 | CloudMe before 1.11.0 |
| 2009-1016 | WebLogic Server component in BEA Product Suite |
| 2021-34527 | Windows Print Spooler Remote Code Execution Vulnerability |
| 2021-28165 | Eclipse Jetty |
| 2019-11707 | Firefox < 67.0.3, and Thunderbird < 60.7.2 |
| 2002-0012 | Vulnerabilities in a large number of SNMP implementations |
| 2019-8506 | Multiple Apple Inc software |
| 2024-6409 | A race condition vulnerability was discovered in how signals are handled by OpenSSH's server (sshd) |

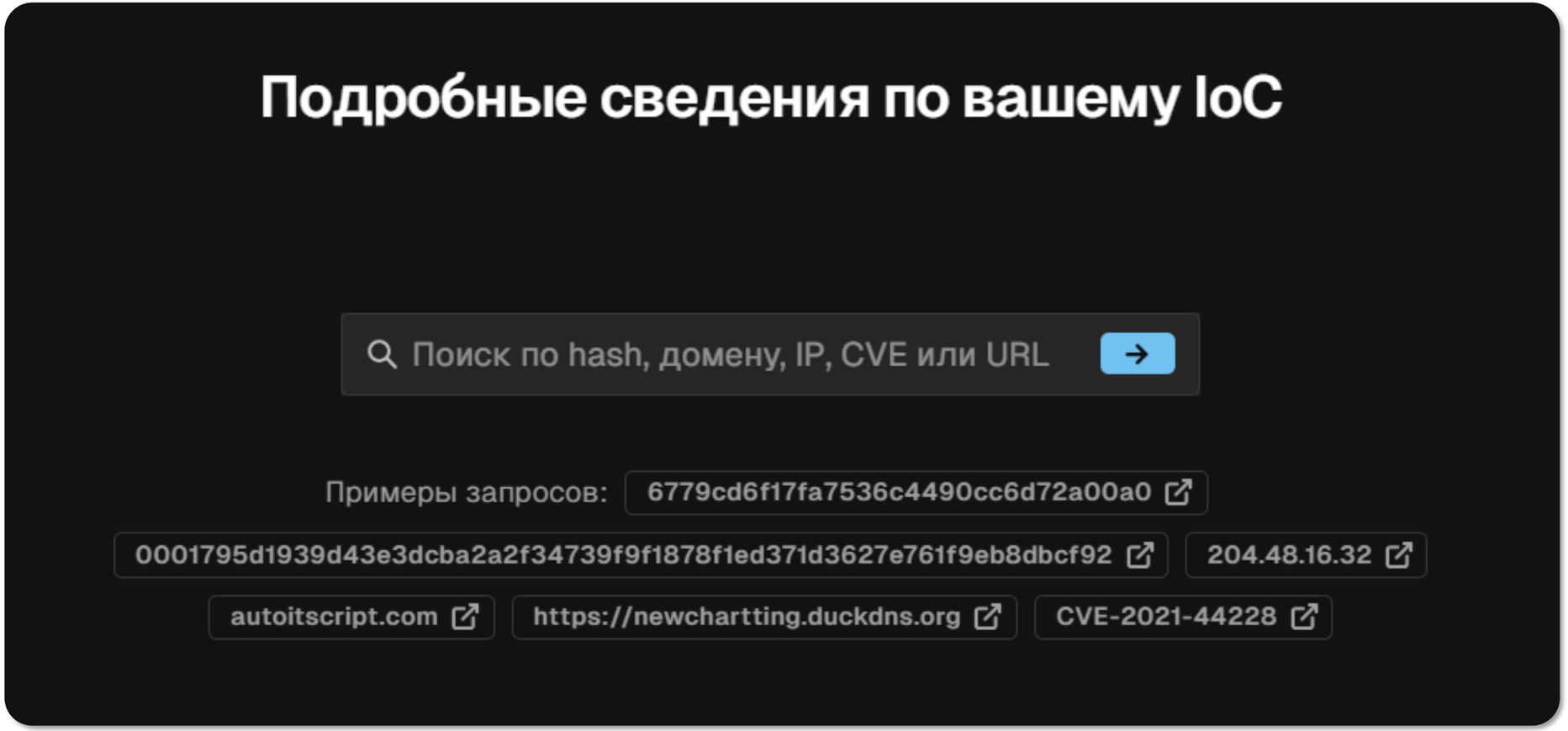
# Топ-10 атакующих IP

?

# Топ-10 атакующих IP

| IP-адрес | | AM Score |
|---|---|---|
| 99.234.92.103 | 30628370 | 0,47 |
| 67.67.67.67 | 15893626 | 0,47 |
| 118.184.169.48 | 14399630 | 0,77 |
| 149.154.167.220 | 13178828 | 0,72 |
| 8.8.4.4 | 7701877 | 0,75 |
| 209.250.254.15 | 4926360 | 0,35 |
| 114.114.114.114 | 4128206 | 0,62 |
| 185.45.82.72 | 3878593 | |
| 37.143.10.32 | 3817808 | |
| 185.45.83.25 | 3808114 | |


Дашборд
TI Lookup
О продукте
Тарифы
Помощь
/AMTIP
Поиск по IoC
Sergey.Neyger@amonitoring.ru
Дашборд
Все сведения предоставлены относительно Российской Федерации
Период
Источник
день
неделя
месяц
ViPNet IDS NS
Обновить данные
Киберкарта
Россия 53%
Соединённые Штаты Америки 27%
Китай 4%
Нидерланды 4%
Великобритания 4%
Швеция 3%
Ирландия 2%
Украина 1%
Канада 1%
Франция 1%
>50%
25%
0%
Топ 10 атакующих IP
Топ 10 CVE




# amtip.ru — доклад через 2 часа

# Кажись, всё...

В ноябре 2024 года глава «Ростелекома» Михаил Осеевский заявил, что персональные данные всех россиян утекли в сеть.

Заместитель председателя правления Сбербанка Станислав Кузнецов отметил, что в сети оказались данные около 90% россиян.

# Тренды на 2025

- Искусственный интеллект продолжит оставаться мощным инструментом для киберпреступников, и в 2025 году тренд укрепится. Злоумышленники активно используют эти технологии для проведения мошеннических атак. Генерация фальшивых писем, синтез голосов и Deepfake-видео делают атаки максимально убедительными.
- Атаки на цепочки поставок останутся одной из основных стратегий для злоумышленников. Вредоносные обновления и компрометация сторонних сервисов станут частыми способами проникновения в системы крупных организаций.
- Программное обеспечение продолжает оставаться привлекательной мишенью. Популярные системы и сервисы могут стать объектом новых атак, направленных на эксплуатацию известных уязвимостей, а ИИ поможет злоумышленникам автоматизировать этот процесс.
- ИИ также будет анализировать поведение, сообщения, интересы жертв для создания персонализированных атак и обхода систем безопасности. Атакующие смогут с лёгкостью подделать голос или внешний вид доверенного лица. В 2025 году ожидаем усиления тенденции использования злоумышленниками мессенджеров для проведения атак.
- С ростом популярности облачных сервисов, злоумышленники будут всё активнее искать уязвимости в облачных платформах. Цель — не только крупные компании, но и малый бизнес, который часто не уделяет должного внимания безопасности в облаке.
- Проблемы с конфигурациями и слабой настройкой безопасности останутся основными точками входа для атак. Например, незащищённые API или неверно настроенные права доступа могут стать причиной серьёзных утечек данных.

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

# Спасибо
# за внимание!


Сергей Нейгер

Директор по развитию бизнеса,
«Перспективный мониторинг»

Sergey.Neyger@amonitoring.ru


t.me/pm_public amonitoring.ru amtip.ru