# Экспертные данные. Новый источник сведений о киберугрозах


Артём Савчук
Технический директор

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

# Экспертные данные

## Новый источник сведений о киберугрозах

# Направления деятельности

**Исследование защищённости**

- Пентест
- Аудит ИБ
- Оценка соответствия требованиям Банка России
- Категорирование объектов КИИ

**SOC**

- Коммерческий SOC
- Подключение к ГосСОПКА
- Расследование инцидентов ИБ
- Группа быстрого реагирования

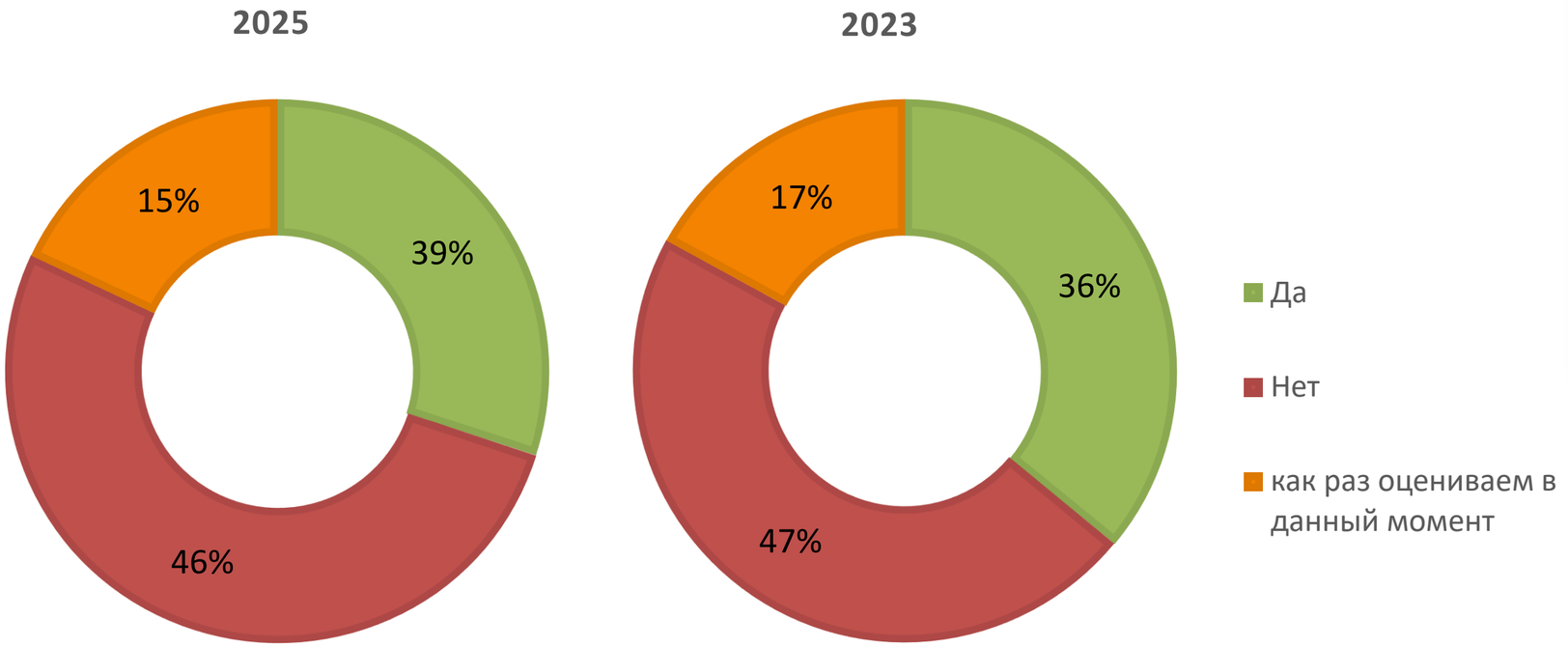
**Продукты**

- AM Rules (БРП)
- **AM TI Portal**
- Киберполигон Ampire
- AM Incident Management System

**Сквозная экспертиза** по всем направлениям деятельности

# Вы используете TI?

«Вы используете сервисы Threat Intelligence в данный момент ?»*




## Бизнес пошел в контрразведку

### Спрос на услуги предотвращения киберинцидентов растет

Рост числа киберинцидентов подтолкнул организации чаще обращаться за услугами специалистов по расследованию и предотвращению таких событий: мониторингу теневых форумов, анализу объявлений о продаже данных организации и составах группировок. Участники рынка наблюдают увеличение спроса на подобные услуги на 20–40% год к году. Сейчас их объем оценивается на уровне 15 млрд руб.— около 8% от всего рынка информбезопасности. Интерес к сегменту начали проявлять и госзаказчики, но серьезного роста такие клиенты не обеспечат из-за регуляторных барьеров, полагают эксперты.

*Опрос зрителей эфира AM Live от 26 февраля 2025 года

# Экспертные данные
# АО «ПМ»

1. «Базы решающих правил» (БРП, включают наборы snort, yara, ossec, suricata правил)
2. TI feeds (IoC в STIX или любом другом пользовательском формате)
3. AM Rules (Свидетельство Роспатента №2016620316 от 03.03.2016 г.)
4. Категорированные веб-ресурсы
5. Бюллетени ИБ

# База решающих правил AM Rules

— собственная база правил обнаружения атак для решений классов IDS/IPS/NGFW/EDR. Мы разрабатываем правила, которые выявляют атаки и сопутствующие события ИБ на любом этапе


**>50 000**

актуальных сигнатур AM Rules

**60%**

собственных уникальных правил

**40%**

правил из ET Open, которые дополнительно валидируются и обогащаются аналитиками ПМ

# Преимущества БРП AM Rules

**35 000** индикаторов компрометации и образцов вредоносного кода анализируются **ежедневно**

**1000** новых сигнатур AM Rules ежемесячно

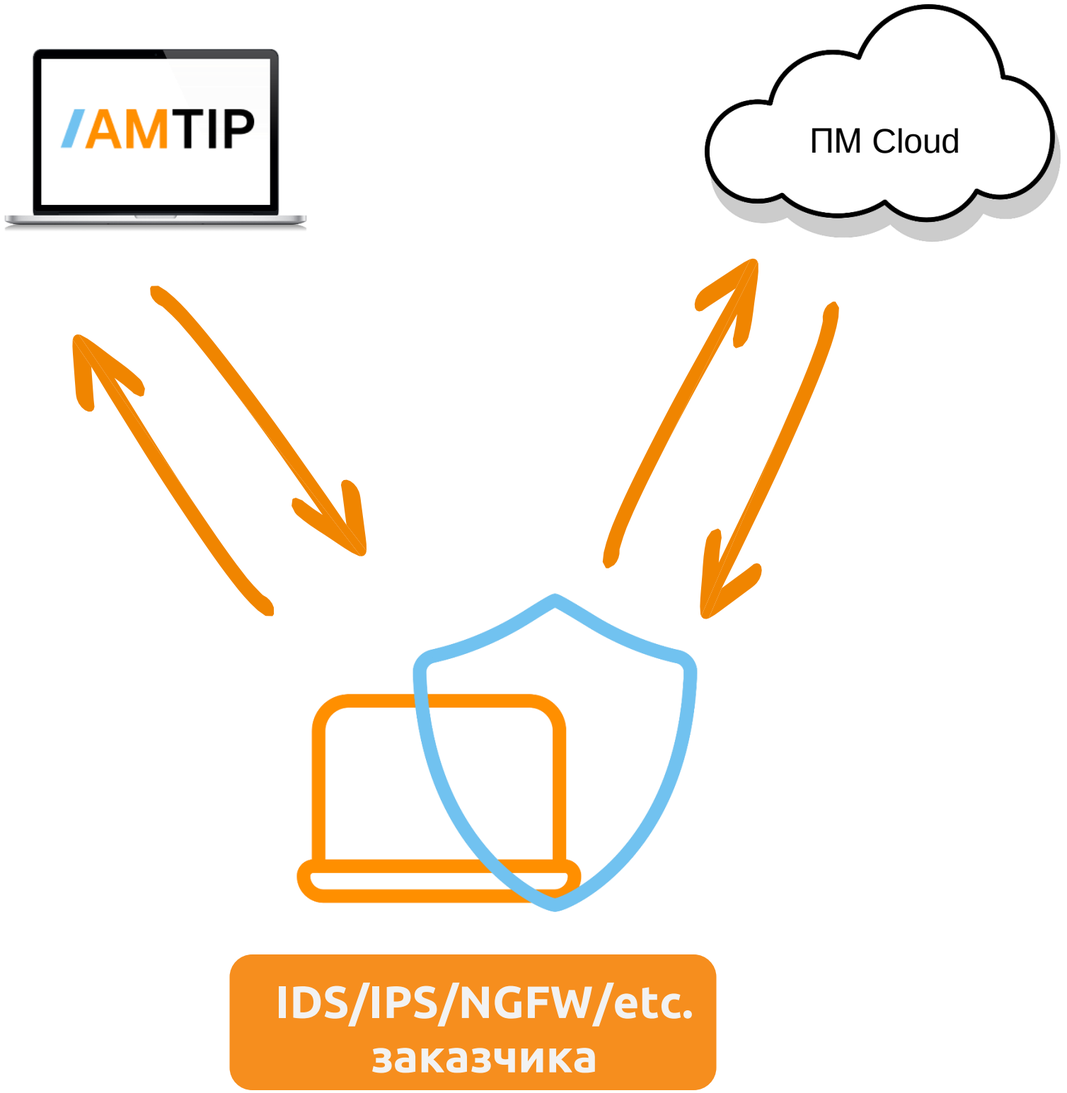
**№1** первые на российском рынке, кто начал выпускать собственные сигнатуры с 2016 года

**ViPNet** БРП AM Rules работают во всей линейки продуктов ViPNet АО «ИнфоТеКС» с 2018 года

**Ежедневно** производится обновление базы правил

# Форматы поставки БРП AM Rules

Поставляем AM Rules через AM Threat Intelligence Portal или облачное хранилище АО «ПМ»




## Форматы поставки

Сетевые правила

SURICATA

SNORT

Хостовые правила

OSSEC

YARA

# AM URL фильтрация

— категорирование веб-ресурсов в зависимости от контента и связанных атрибутов на основе собственного алгоритма


**5 000 000**

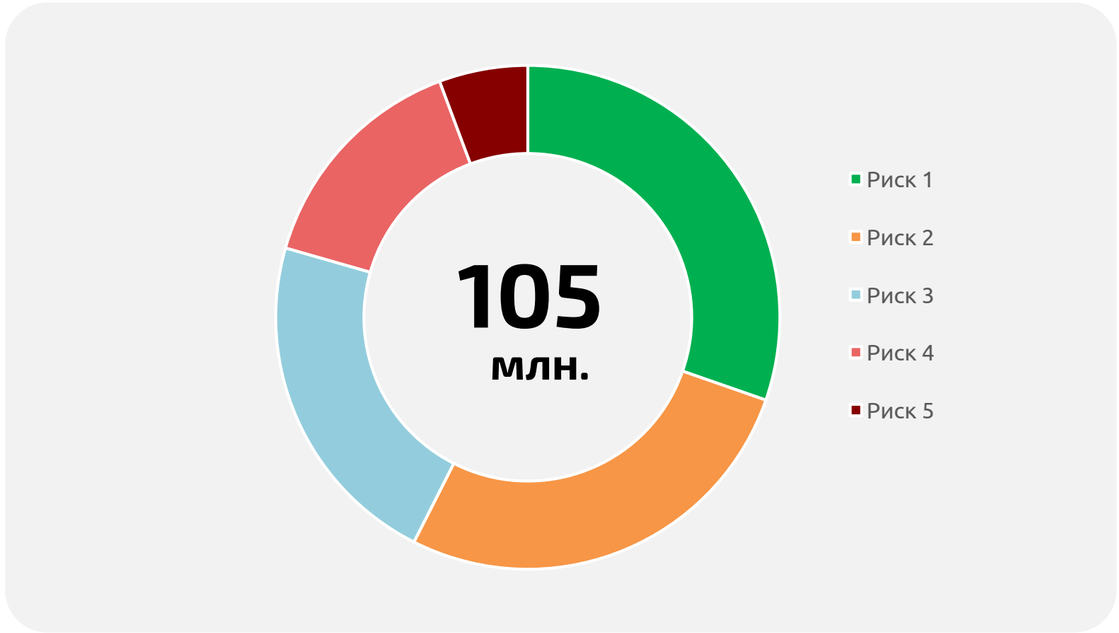
**Категорированных ресурсов в 2021 году**

**100 000 000**

**Категорированных ресурсов в 2024 году**

# Категорирование ресурсов

Каждой категории присвоен риск от 1 до 5




**81**
категория

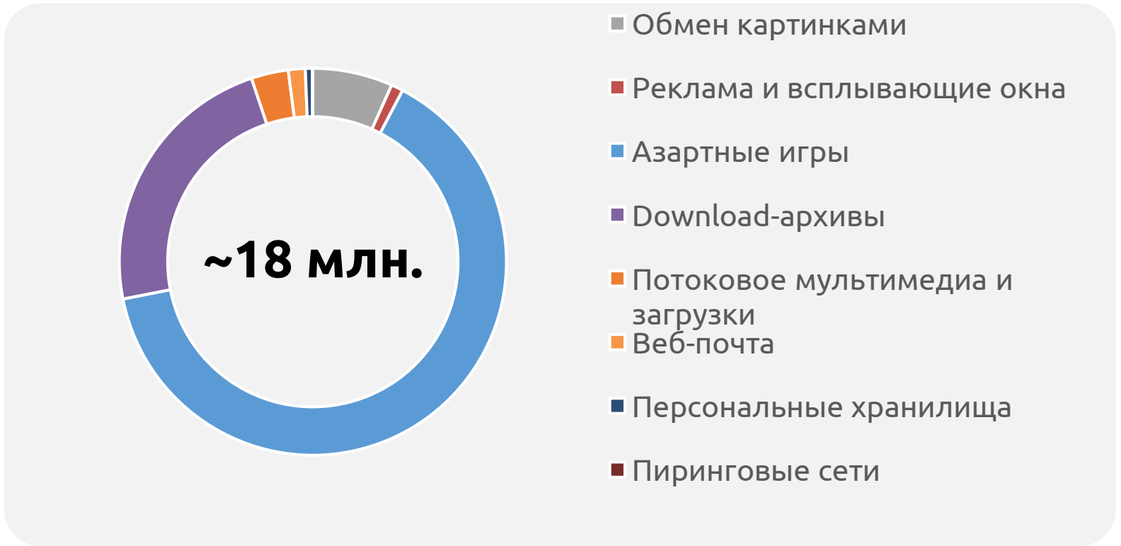
**100+ млн.**
категорированных ресурсов

**15%**
ежемесячный
при рост

**24/7/365**
обновление категоризатора

# Категорирование ресурсов

## Категорированных ресурсов с риском 4




## Категорированных ресурсов с риском 5

# Применимость


Управление сетевой безопасностью

Разграничение политики доступа в сеть Интернет

# AM Threat Intelligence Feeds

– комплексные сведения об индикаторах компрометации (Indicator of Compromise, IoC), которые помогают своевременно выявить угрозы и инциденты ИБ

- Собственная платформа **AM TI Pipeline** для сбора сведений из публичных «песочниц» и антивирусов
- Система киберразведки **AM Pellonia** для сбора сведений из текстовых источников
- **Специалисты Компании** ежедневно верифицируют и обогащают базу новыми сведениями вручную

**51 000 000**

**индикаторов компрометации**

**4%**

**ежемесячный прирост базы**

# Ключевые преимущества AM TI Feeds

01

## Уникальность

Сведения об индикаторах компрометации из SOC’а ПМ

02

## «Низкий порог входа»

Низкая стоимость относительно аналогов

03

## Мы гибкие

Интегрируемая с продуктами разных вендоров

04

## Комплексные сведения об индикаторе

Помимо оценки вредоносности и категории мы предоставляем обширную сведения об индикаторах компрометации: применяемые техники и тактики, взаимосвязи, метки образцов

05

## ViPNet

Сведения об угрозах используются во всей линейке продуктов ViPNet АО «ИнфоТеКС»

# Поставка AM TI Feeds

Поставляем в формате STIX 2.1 {:} JSON через AM Threat Intelligence Portal


SIEM

IDS/IPS/NGFW

TI-платформы

# Бюллетени ИБ

Информационный бюллетень Центра мониторинга АО «ПМ»

| | |
|---|---|
| Название документа | **Уязвимость “MonikerLink” в Microsoft Outlook** |
| Разослан | 2024-03-05 |
| Идентификатор | AM-2024-ALE-0305-01 |
| Описание угрозы | **CVE-2024-21413** |

**CVSSv3.1:** 9.8, AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Объект уязвимости:** Компонент библиотеки ole32.dll в Microsoft Outlook

**Требования к атакующему:** Удаленный неаутентифицированный

**Максимальный результат атаки**: Удаленное исполнение кода

# Бюллетени ИБ

Меры противодействия

Использовать правило ViPNet IDS NS:

- sid 3285268 "AM EXPLOIT Microsoft Windows Outlook NTLM Credentials Leak aka 'MonikerLink' (CVE-2024-21413)"

Использовать правило ViPNet IDS HS / ViPNet EPP:

- 902486 "Подозрение на эксплуатацию MonikerLink в Microsoft Outlook"

Использовать метаправило ViPNet TIAS:

- Раскрытие NTLM-хэша аутентификации в Microsoft Outlook (CVE-2024-21413)

Ссылки на источники

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413
- https://research.checkpoint.com/2024/the-risks-of-the-monikerlink-bug-in-microsoft-outlook-and-the-big-picture

# Угрозы vs Риски

**Угрозовый рассвет: почему растут киберриски и как устроено их страхование**

Forbes 07 ноября 2023

РБК+ Все выпуски Истории Экспертиза Презентации Решение Новс

Тенденции, Весь мир, 27 окт 2022, 09:55

**Бизнес начал вкладывать в страхование киберрисков**

интерфакс

ЭКОНОМИКА 12:23, 15 июня 2023

**ЦБ планирует сформировать условия для создания института страхования киберрисков**

Москва. 15 июня. INTERFAX.RU - Банк России планирует сформировать условия для создания института страхования киберрисков и предоставить расширенный перечень данных внешним пользователям для формирования моделей страхования, говорится в материале ЦБ "Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023-2025 годов", опубликованном на сайте регулятора.

"Задача страхования киберрисков состоит в покрытии убытков, возникших в результате успешно реализованных кибератак", - отмечает ЦБ.

Также Банк России отмечает, что рынок страхования киберрисков развивается от года к году. "По данным международных экспертов, по состоянию на 2022 год глобальный рынок страхования киберрисков достигнет $14 млрд, а к 2025 году он будет составлять уже $20 млрд", - говорится в материале.

ВЕДОМОСТИ

Финансы Инвестиции Технологии Медиа Политика Общество Менеджмент ...

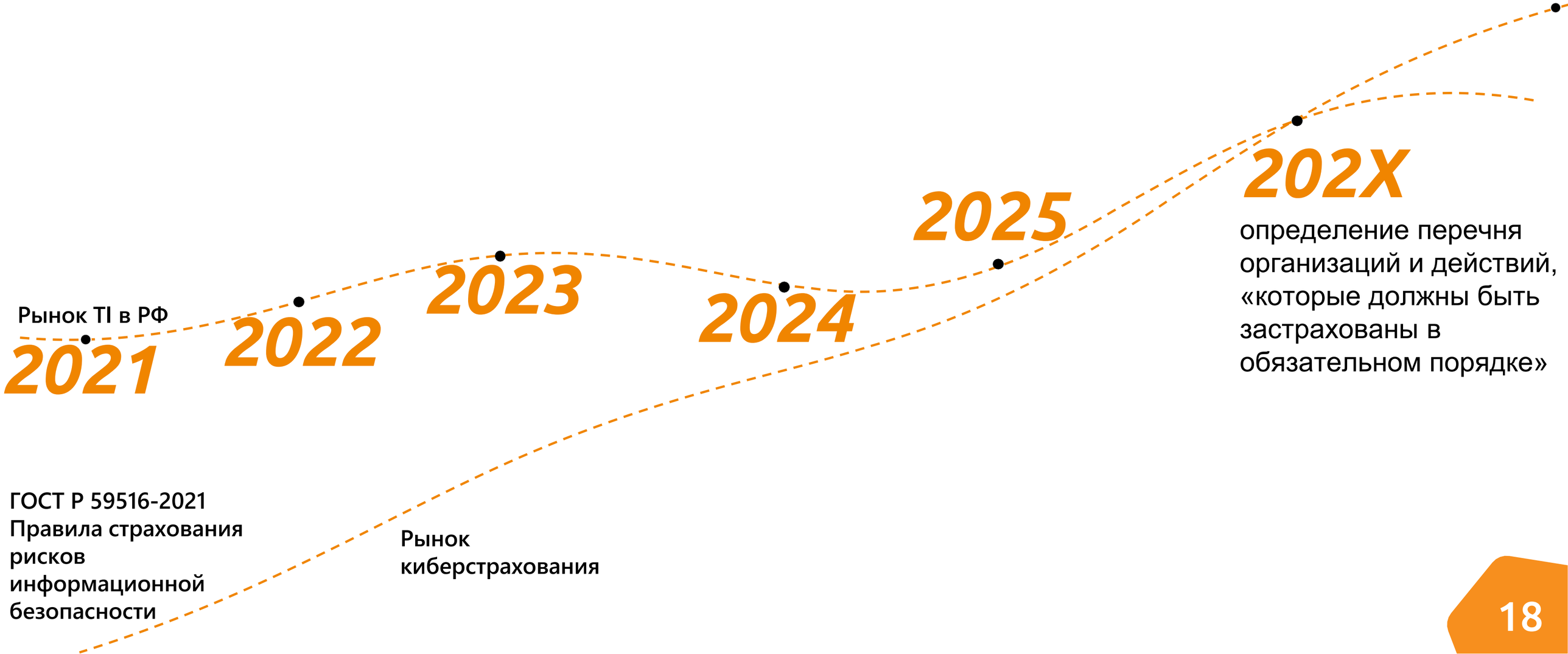
Ведомости& Спорт Право Страна Технологии и инновации Капитал Промышленность

29 сентября, 00:21 / Технологии

**Для страхования киберрисков может быть создан отдельный фонд**

*Он может стать частью новой нацпрограммы «Экономика данных»*

# Предотвратить или компенсировать



/AMTIP

# AM Threat Intelligence Portal

Включен в реестр отечественного ПО,
реестровая запись №22808 от 06.06.2024

# Составляющие AM TIP

**Для людей**

**Для машин**

**TI Lookup**

WEB

API

**AM TI Feeds**

**БРП AM Rules**

- Аналитики SOC
- Исследователи
- Администраторы ИБ

- Аналитические СЗИ
- СЗИ уровня сети
- СЗИ уровня узла

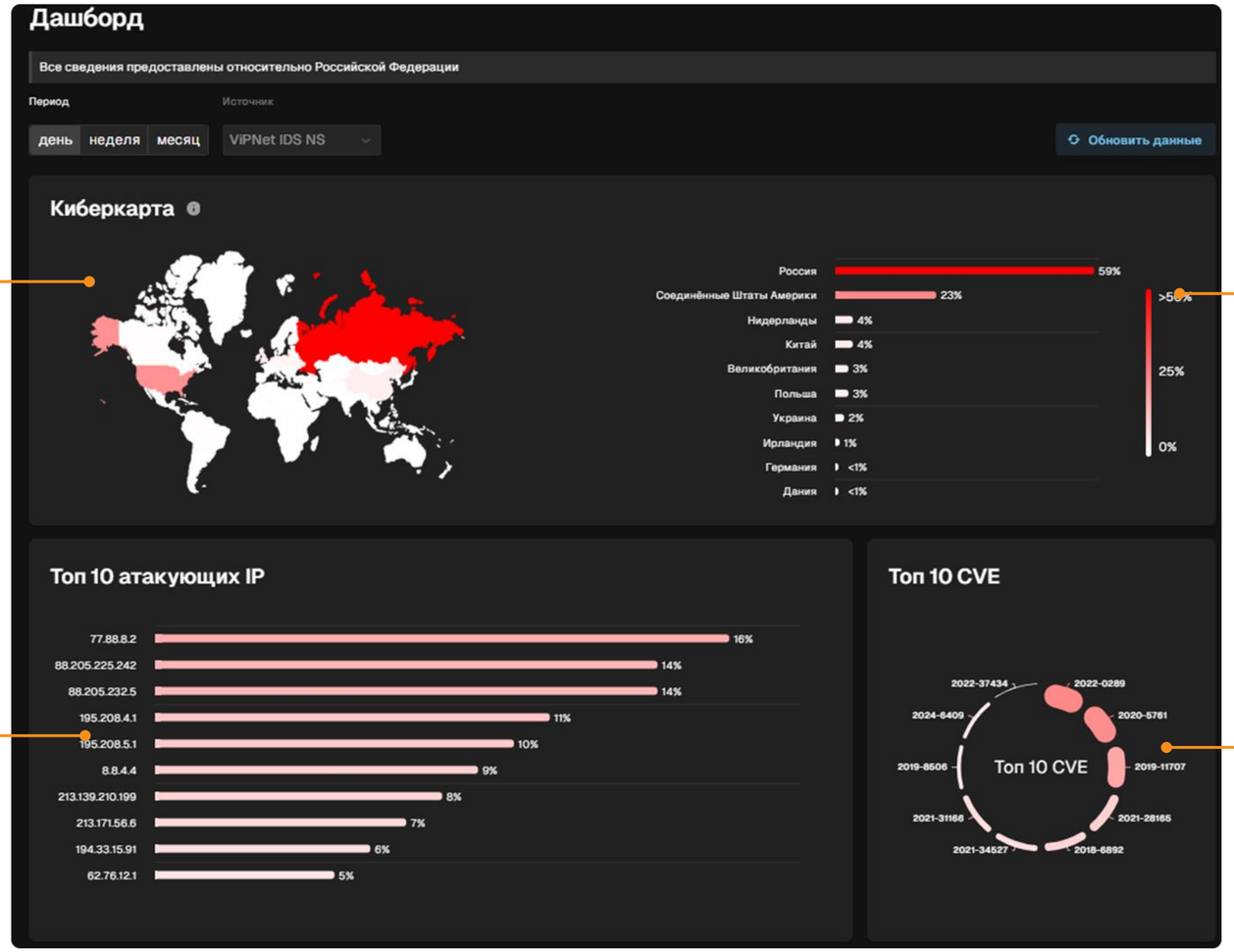
# Дашборд

## Киберкарта

На Киберкарте в режиме реального времени отображается цветовая индикация стран, из которых фиксируются угрозы по отношению к РФ за выбранный период

## ТОП 10 атакующих IP

Рейтинг атакующих IP из выбранной на карте страны по отношению к РФ с выбранным периодом и источниками в процентах по убыванию




## ТОП атакующих стран

Рейтинг стран, из которых зафиксированы угрозы по отношению к РФ с выбранным периодом и источниками в процентах по убыванию

## ТОП 10 CVE

Рейтинг эксплуатируемых CVE из выбранной на карте страны по отношению к РФ с выбранным периодом и источниками, которые чаще всего фиксируются в событиях безопасности продуктов ИнфоТеКС и ПМ

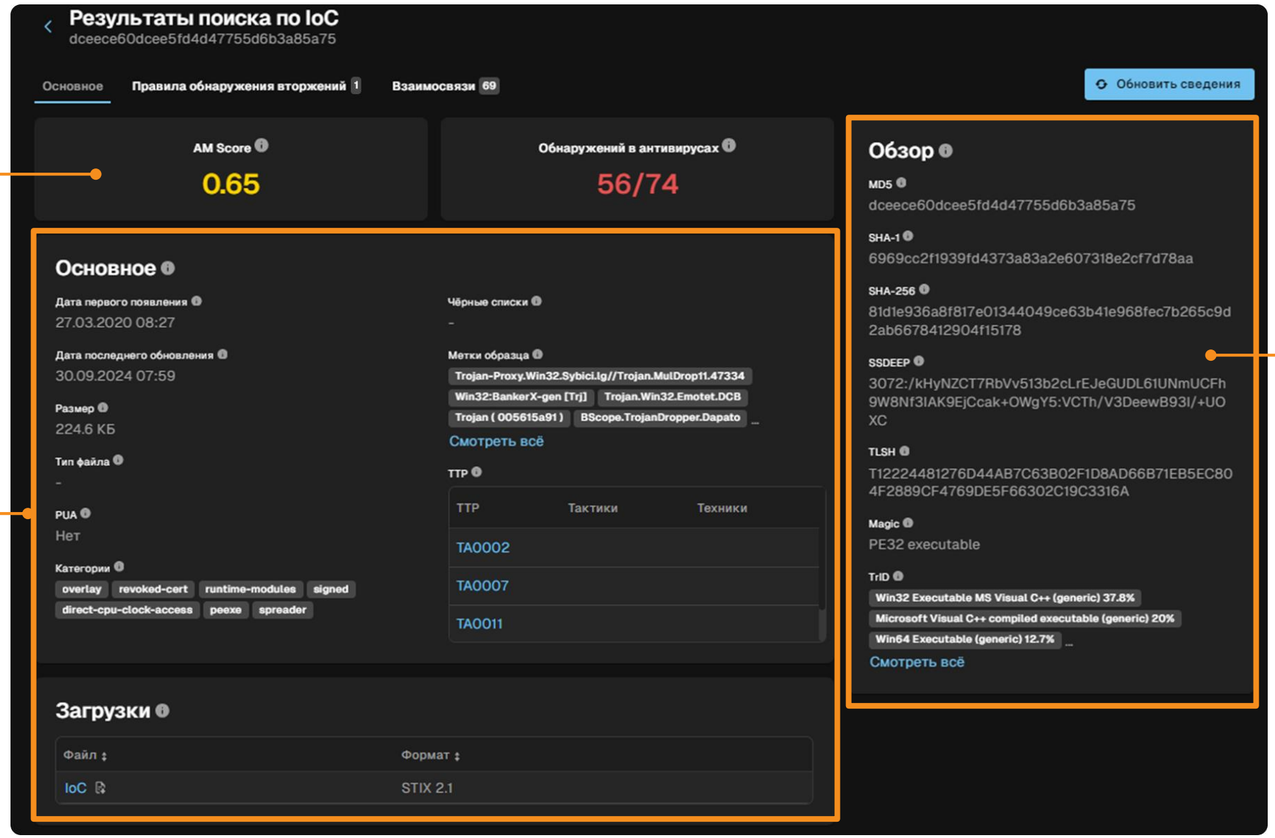
# Функциональность TI LOOKUP

### AM Score

Оценка вредоносности ресурса на основе методики ПМ. Цветовая индикация результата позволяет ускорить реакцию на угрозу

### IoC

Комплексные сведения об индикаторе компрометации с возможностью выгрузки IoC в формате STIX 2.1




### IoC

Дополниетльные атрибуты индикатора компрометации

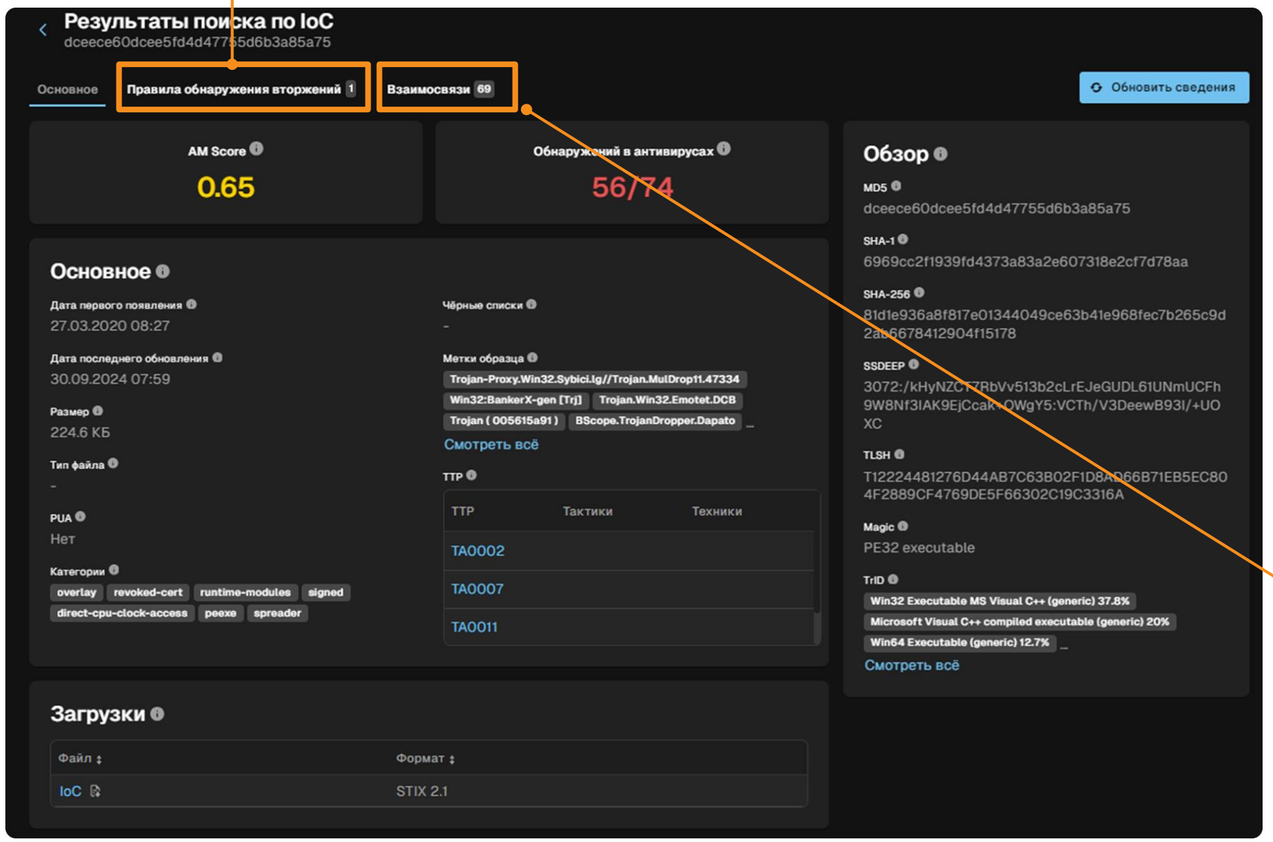
**Типы исследуемых объектов:**

Hash, IP, CVE, Domain, URL

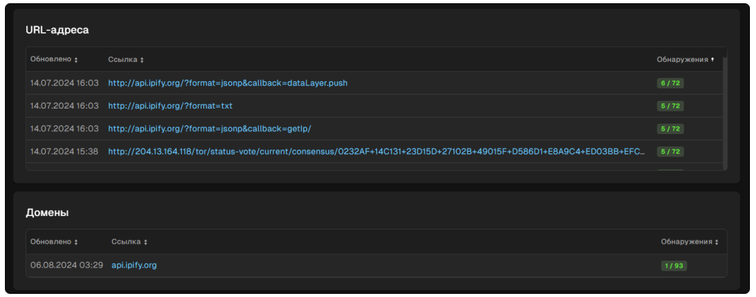
# Функциональность TI LOOKUP

## БРП AM Rules

Описание сигнатур по исследуемому объекту с возможностью просмотра и выгрузки правила в форматах Snort, Suricata, YARA, OSSEC

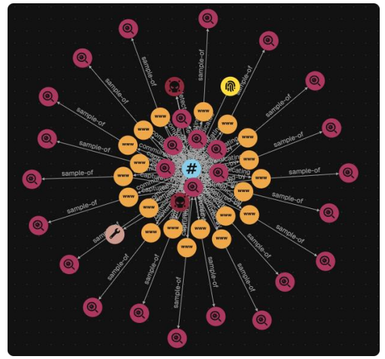







## Взаимосвязи

Информация о связанных индикаторах компрометации и адаптивный граф со связями и комплексными сведениями об индикаторе компрометации



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

# Спасибо
# за внимание!

t.me/pm_public

@AMonitoring

amtip.ru

**Артём Савчук**

Технический директор

+7 (495) 737-61-97

info@amonitoring.ru