

PHDays 2025: ИЦ

Алексей Синадский

30.05.2025, митап ИЦ

Лужники



CYBERARENA

КИБЕРАРЕНА

Бизнес-доклады, партнерские зоны
Business talks and partner zones

- | | |
|-----------------------------------------------------------|------------------------------------------------|
| R Регистрация
Registration | 16 Зал 16 «Эдисон»
Edison Hall 16 |
| 11 Зал 11 «Братья Райт»
Wright Brothers Hall 11 | 17 Зал 17 «Якоби»
Jacobi Hall 17 |
| 12 Зал 12 «Тьюринг»
Turing Hall 12 | 18 Зал 18 «Королев»
Korolev Hall 18 |
| 13 Зал 13 «Гальвани»
Galvani Hall 13 | 19 Выставка партнеров
Cyber expo |
| 14 Зал 14 «Маркони»
Marconi Hall 14 | 20 Арена «Ломоносов»
Lomonosov Arena |
| 15 Зал 15 «Морзе»
Morse Hall 15 | |

CYBERHUB

КИБЕРХАБ

Технические доклады, воркшопы, Standoff
Technical talks, workshops, and Standoff

- | | |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R Регистрация
Registration | 26 Зал 26 «Бэббидж»
Babbage Hall 26 |
| 21 Зал 21 «Лавлейс»
Lovelace Hall 21 | 27 Positive Labs |
| 22 Зал 22 «Горохов»
Gorokhov Hall 22 | 28 Конкурсы PHDays
PHDays competition |
| 23 Зал 23 «Да Винчи»
Da Vinci Hall 23 | 29 Positive Talent Spot
Место для общения с экспертами в IT и ИБ
и обсуждения карьерных перспектив
The place to network with IT and information security
experts and discuss career prospects |
| 24 Зал 24 «Шеннон»
Shannon Hall 24 | |
| 25 Зал 25 «Попов»
Popov Hall 25 | Standoff |

Присмотрел доклад?

- 3 дня, параллельно 20+ залов

Зал 21 «Лавлейс»	Зал 22 «Горохов»	Зал 23 «Да Винчи»	Зал 24 «Шеннон»
------------------	------------------	-------------------	-----------------

Зал 25 «Попов»	Зал 26 «Бэббидж»	Лекторий Positive Labs	Standoff
----------------	------------------	------------------------	----------

Научпоп-сцена «KULIBIN»	Education Hub
-------------------------	---------------

Арена «Ломоносов»	Пресс-центр	Зал 11 «Братья Райт»	Зал 12 «Тьюринг»	Зал 13 «Гальвани»
-------------------	-------------	----------------------	------------------	-------------------

Зал 14 «Маркони»	Зал 15 «Морзе»	Зал 16 «Эдисон»	Зал 17 «Якоби»	Зал 18 «Королев»	Пространство киберустойчивости Innostage
------------------	----------------	-----------------	----------------	------------------	------------------------------------------

Время	Зал	Доклад					
22.05							
12:00-13:00	Лавлейс	Как ломают DeepSeek и как ИИ ломает нас					
13:00-13:50	Горохов	Apache Arrow: быстрее, ниже, сложнее					
14:00-14:50	Горохов	Как мы приучали утку: работа с данными в X раз быстрее без магии и шаманства					
15:00-16:00	Шеннон	Знай свой IoT: как ML-профилирование раскрывает атаки					
15:00-16:00	Лекторий PT	(нет) Не стой под стрелой: безопасность систем промышленного дистанционного управления					
15:30-15:45	Тьюринг	(нет) Что важно для защиты умных многоквартирных домов					
16:00-16:50	Горохов	Как заставить тормозить ClickHouse					
Куда-то пропал из программы		(мб) Как мы поймали актуальную угрозу после 1000 и 1 фолза на мемах «это база» и «слома					
19:00-19:15	Шеннон	Применение легковесных LLM в аналитических задачах ИБ					
23.05							
10:35-11:05	Королёв	LLM и агенты: разгоняем SOC					
10:55-11:35	Тьюринг	Современные реалии проектирования и построения сетевой инфраструктуры					
11:05-11:35	Королёв	AutoML threat detection: повышаем уровень автономности SOC					
11:35-12:05	Королёв	Как мы делаем near-real-time защиту в Яндекс Облако: AI в процессах и технологиях					
13:00-13:50	Да Винчи	Усиление облачной безопасности. Используем CSPM для нужд SOC					
13:00-14:00	Лавлейс	Токены доступа и API gateway: как обеспечить безопасность запросов					
13:45-14:00	Королёв	Детектирование SSH-туннелей на основе системных вызовов от процесса демона SSH (sshd)					
14:00-14:50	Горохов	Централизованное управление распределенным файрволом					
14:00-15:00	Кибергород	(мб, скорее нет) Кто такой этот ваш Искусственный Интеллект? Воркшоп					
14:30-14:45	Эдисон	Как с помощью LLM выявлять реальные уязвимости LLM-приложений					
15:00-16:00	Лавлейс	Источники данных для фаззинга API веб-приложений					
15:00-16:00	Бэббидж	Развитие трейсинга в hh.ru . От Cassandra и OpenTelemetry до Vector и ClickHouse					
15:00-15:50	Горохов	Что вы делаете не так с Elasticsearch с инженерной стороны					
15:00-15:15	Эдисон	Как поймать атакующих на их ошибках					
15:30-16:00	Королёв	IDFW: как заблокировать атаку везде и сразу					
15:30-19:30	Гальвани	(мб) LLM в повседневной деятельности специалиста по ИБ; воркшоп					
16:00-16:50	Да Винчи	Легитимные C2: как популярные сервисы работают на хакеров					
16:40-17:20	Тьюринг	Харденинг сетевой инфраструктуры					
17:30-18:15	Эдисон	Бизнес-разведка методами OSINT					
18:00-18:40	Тьюринг	Контроль конфигурации сетевого оборудования. Как обеспечить?					
24.05		Как мы изменения в сети валидировали					
12:30-13:20	Горохов	VS Code: выжимаем все из нашей IDE — и даже больше					
14:00-15:00	Да Винчи	Обеспечение конфиденциальности данных при разработке ML-моделей с использованием те					
14:30-14:45	Тьюринг	Инвентаризация Windows посредством SSH					
15:00-15:50	Горохов	Поиск аномалий с использованием Python: от теории к практике					
16:00-17:00	Да Винчи	SDRcraft: искусство радиоэлектронной борьбы					
	Kulibin (научпоп)	(скорее, нет) Моделируя будущее: цифровые двойники					
17:00-18:00	Шеннон	От яхт до рутинга: эксплуатация уязвимостей IoT для полной компрометации устройств					

Доклады

Программа: <https://phdays.com/forum/program/>
Записи: <https://phdays.com/forum/broadcast/>

Как ломают DeepSeek и как ИИ ломает нас

- Масалович ☹️
- Сохранять, пока есть
- Применение – быстрый анализ решений конкурентов
- Сеть Колмогорова-Арнольда. Подбор $f(x)$
- Роевой ИИ. Социальные функции
- Модель Барабаши-Альберт, безмасштабные сети

Похоже, для ИИ работает модель Барабаши-Альберт

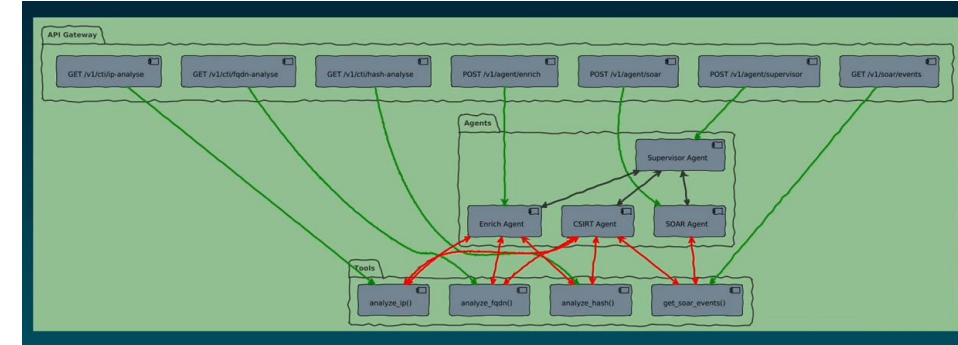
phd X pt

- Безмасштабная сеть (scale-free network –степенное распределение по степени узла)
- Рост сети
- Принцип предпочтительного присоединения



[доклад](#)

LLM и агенты: разгоняем SOC



- В целом, работает, если не плоские чаты. Определить роль, инструменты, задачу
- Результат – Few-Shot для исследования экономит до 25% времени аналитика
- Рекомендации
 - Температура в 0, чтобы стабильно отвечать на одни и те же вопросы
 - Выбор модели: смотреть разные, не обязательно самые крутые
 - Промпт. Подавать корректные вопросы, формализовать ответы (что хочется получить)
 - Делать тесты с вопросами. Валидация входа/выхода - как минимум, на уровне http.
 - Мониторинг. LangSmith, Grafana
 - При внедрении явно отключать дебаг
 - Сбор диалогов и оценок
 - Использовать чистые данные, не обучать на синтетике, иначе через поколения будет хуже.

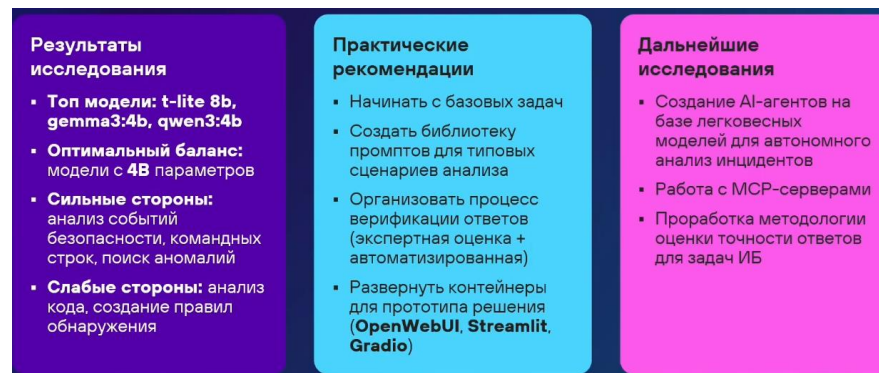
[Доклад](#)

Легковесные LLM для аналитики [доклад](#)

Голос куратора: создаем плагин для Burp Suite без клавиатуры [доклад](#)

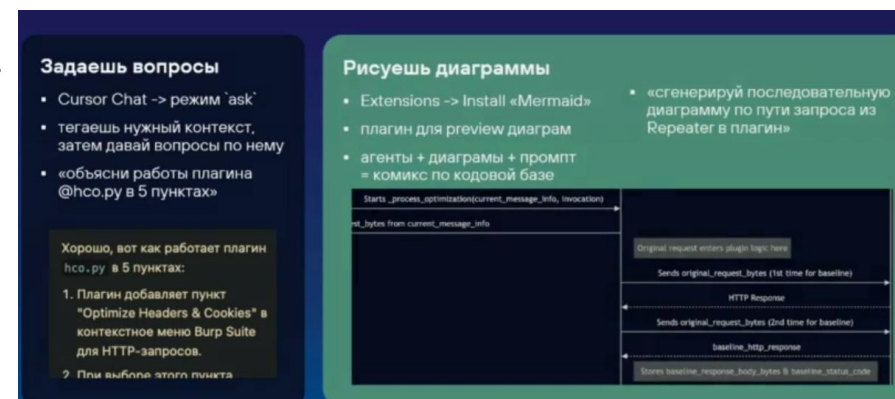
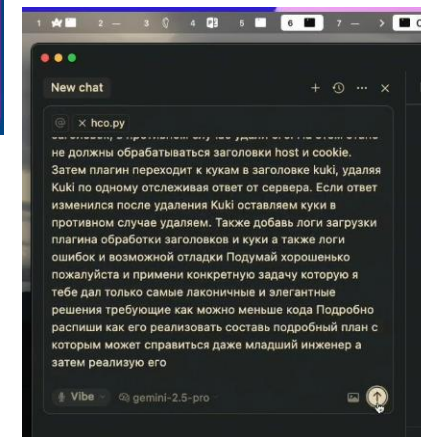
• Легковесные LLM для аналитики

- Легковесные - до 8B
- Отдельные задачи решают
- С техническими задачами сложности
- Выбор: T-lite, Gemma3, Qwen



• LLM в IDE

- Лайв-кодинг в прямом эфире
- Идея: не давать LLM свободы в фантазии, только реализация
- LLM – «терпеливый джун»
- CursorIDE + Gemini2.5Pro + WhisperFlow
- Основной совет: менять чаты, хранить контекст
- uithub.com – генератор исходников для LLM
 - (описание файлов из репозитория)



Как мы делаем near-real-time защиту в Яндекс Облако: AI в процессах и технологиях

- Начинать с инвентаризации (расширенная категоризация UDV NTA?)
- Хранить базу данных об активах с хронологией
- Полезно описывать изменения (+функция DATAPK Version Control?)



Активы

- Инвентаризация — основание, на котором строится безопасность. Это первый пункт всех стандартов, рекомендаций и книг
- Актив — любая интересная сущность в Yandex Cloud и за его пределами
- Обычно для сбора активов доступны только события, в которых они участвуют (например, из аудитных логов), но не состояние актива целиком



The diagram illustrates the lifecycle of a Virtual Machine (VM) within an Organization's Cloud environment. It shows the flow from Organization to Cloud, then to Network, and back to Cloud. A timeline at the bottom marks key events: Created, Add VM to Cloud, Started, VM IP, Stopped, Delete, and Delete from Cloud, plotted against time (t).

Хронология данных

- Физическому времени источника нельзя доверять
- Небольшие изменения в прошлом могут приводить к существенным изменениям всей хронологии актива



The slide presents three scenarios for data chronology using a Virtual Machine lifecycle as an example:

- Атрибуты активов меняются во времени:** A standard timeline showing Created, Started, Stopped, and Deleted states.
- Физическое время может не соответствовать логическому:** A timeline where the physical order of events (Created, Deleted) differs from the logical state transitions (Stopped, Started).
- Физическое время может не соответствовать логическому:** A timeline where the physical creation time is later than other events, requiring a reordering of transactions in the source database.

Additional notes for the third scenario: "Сообщение о создании пришло позже всех остальных из-за действий в сервисе при его разработке и починке в дальнейшем" and "Атрибуты, назначенные активу в момент создания, должны появиться во всех остальных точках во времени вплоть до Deleted".

AutoML threat detection: повышаем уровень автономности SOC

- Правила - ML - LLM
- Со структурированными данными ML пока помогает
 - Weak learning: взять правила, разметить большой датасет, использовать
- MLOps -> AutoML -> AI ассистент
- ML-инженеры нужны, в основном, доменные
- Подробнее в рассказе Николая

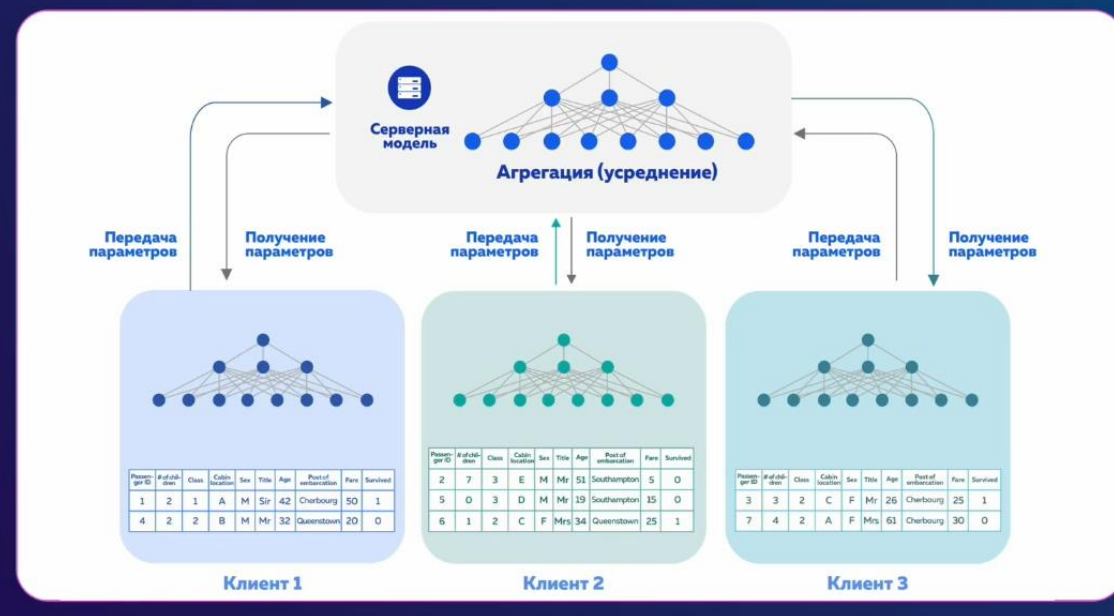


FedML (aka Обеспечение конфиденциальности данных при разработке ML-моделей с использованием технологии федеративного обучения и криптографических методов)

[доклад](#)

- Как установить, кто самый богатый в комнате человек, не раскрывая состояние.
 - Горизонтальный FedML (HFL). Разные сущности, одинаковые признаки. Разные больницы.
 - Вертикальный FedML (VFL). Разные признаки, но пересекающиеся признаки.
- Чтобы нельзя было восстановить сущности из градиентов, используется гомоморфное шифрование. Пока могут только линейные преобразования. Полиномы не могут.
- Защиты от Poison-атак (отравления данных) пока нет.
- Идея применения в UDV: FedML для дообучения на отдельных производствах. Отдавать с логами эмбединги или градиенты. Снижение эффекта дрейфа данных.

Горизонтальный FedML (HFL) PhD



Знай свой IoT: как ML-профилирование раскрывает атаки

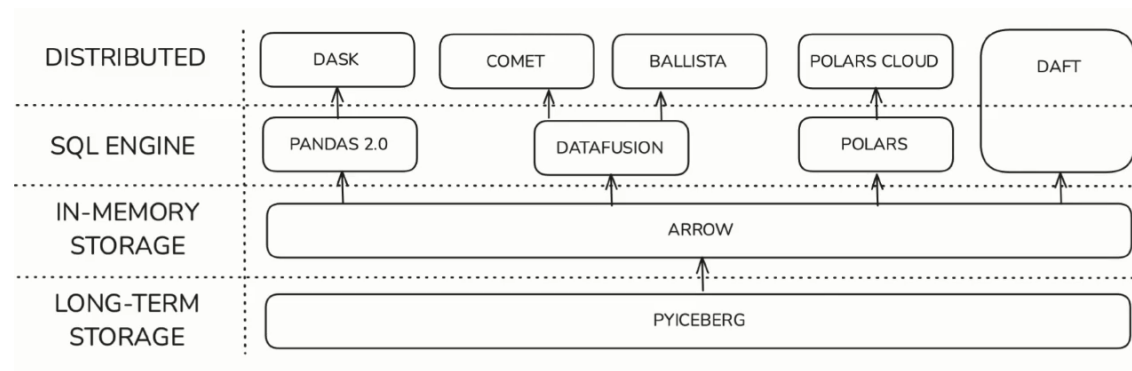
- Выучивают IoT-устройства 26 фиксированных типов
 - Определять тип устройств ещё не умеют
- Выявление атак – но все связаны с ростом трафика
 - мб есть простые методы?
- Датает - CIS IoT 2022 (Канадский университет)
- Список признаков опубликован: [GitHub](#)
- Отдельные модели для выявления и классификации атак
- Лаборатория И.В. Котенко
<https://github.com/levshun>
- Дмитрий Левшун



Про хранение данных:

Как мы приручали утку: работа с данными в X раз быстрее без магии и шаманства [доклад](#)

Apache Arrow: быстрее, ниже, сложнее [доклад](#)



- **Хранение**

- Для хранения (120ГБ/час с одного) используют S3
- S3 - проблемы от 100млн файлов; решения:
 - делать Parquet с одной тяжёлой колонкой (оверхед 1 байт на строку, в Pandas 57 при объекте)
 - Долговременное хранение: Pyiceberg
- DuckDB - аналог SQLite для аналитических данных. In-process, не имеет зависимостей (всё в одной репе); так работает PT

- **Чтение: Arrow**

- Недостатки: нет SQL-оптимизатора, только обработка примитивов. Поэтому Arrow встраивается в качестве compute.
- DataFusion - SQL-движок для Arrow
- Apache Arrow - произвольный доступ и прочее (не читать тяжёлую колонку, пока не прочитали остальное);
- Arrow Scanner - экономия ОЗУ

- **Обработка:**

- DataFusion Ballista - распределённые вычисления для DataFusion
- Polaris - самый быстрый вариант обработки данных на одном узле.
 - Два режима выполнения: сразу как в Pandas и lazy как в Spark
 - Оконные функции в Polars работают неправильно. Пока довели до ума только примитивы.
- 2022: появился DAFT. Как Polars, только умеет в распределённость. Создавался под ML. Появились оконные функции

Мониторинг безопасности OSS

- Воронка уязвимостей: обновления, патчи, достижимые методы
- 83% уязвимости в транзитивных зависимостях

26% фиксов
НЕ чистые обновления безопасности



Исправление приходит с новой функциональностью или фикс ненастоящий / слабый. Можно поймать проблему с совместимостью.



Руководство Бравого Докер Секурити Мастера: latest

- [Слайды квиза](#)

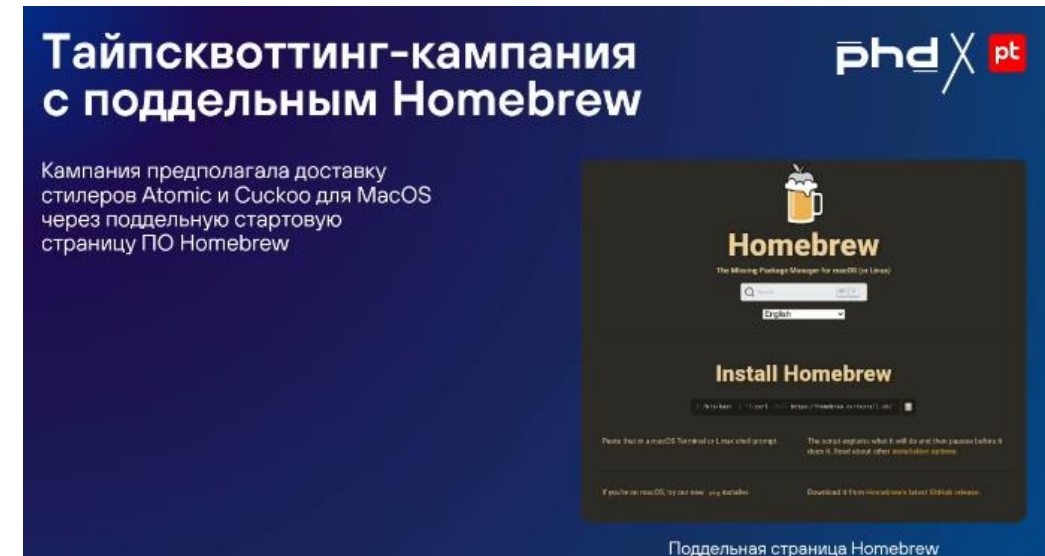
> Пример: форк-бомба

```
admin@sabbath-dev:~$ docker run -d --pids-limit 100 forkbomb
92dcc959603e2293f53ef19044da5684d6664b854c3896ee049e1b1339f06e7b
admin@sabbath-dev:~$
```



Snatch: как стилеры помогают совершать целевые атаки

- Сценарий: долго незаметно пишут, потом сливают
- Доставка
 - Фишинг, GitHub, поддельные сайты, слитые программы
 - Малвертайзинг - рекомендации стилера вместо Zoom, ссылки на YouTube
 - ClickFix - инструкция от капчи: нажмите Win, CtrlV, Enter,....
- Выявление
 - Мониторить слитные учётки
 - Трафик от стилеров похож на нормальный
 - Способ выявления – тайпсквоттинг.
 - PoC есть в ИЦ, добавим?
- Как защищаться?
 - Смотреть, что запускаешь
 - Разрывать сессии (Google, например, долго хранит)



Со стенда РТ NAD (офлайн)

- Метаданные
 - Хранят на SSD в Elastic 5.1, по сравнению с 5 уже сжали в 3 раза.
 - Планируют к концу года S3, ожидают сжатие ещё (?) в 8 раз.
- Трафик
 - Хранят в PCAPах без сжатия на HDD, менять не планируют.
 - Каждая сессия в отдельном PCAP, большие пилят на части по гигабайту.

Ещё интересные доклады

[доклад](#) • Токены доступа и API gateway: как обеспечить безопасность запросов

- opaque / self-contained токены
- Точки инспекции, риски (безопасность / задержка)

[доклад](#) • Легитимные C2: как популярные сервисы работают на хакеров

- Telegram, WA, Discord для передачи отступков
- Детекция – по периодичности, иногда по содержимому, по контексту
 - трафик Discord без установленного приложения – но FP
 - Запросы к YouTube без браузерного приложения, частые обращения к API субтитров

[доклад](#) • От яхтинга до рутинга: эксплуатация уязвимостей IoT для полной компрометации устройств

- Реальная ситуация на моторных судах, устройство, возможности

[доклад](#) • SDRcraft: искусство радиоэлектронной борьбы

- Актуальные устройства для анализа радиосигнала

[доклад](#) • Предсказуемывай это! Анализируем интернет быстро, качественно, дешево

- Адаптивный скан, оптимизация сканирований (уход от прямоугольников в Masscan)

[доклад](#) • Сколько стоит SOC на open source

- Идеи хранилок

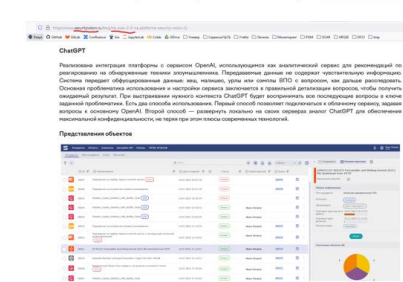
[доклад](#) • Асинхронность vs. потоки: кто выживет в эпоху NoGIL?

- Асинхронность даёт экономию ресурсов. Поток - 4МБ. Сокет - 4КБ. И при параллелизме на 10 тысяч потоков уже не хватает. И планировщик задач чуть тратит время на выбор
- NoGIL: многопоточный код стал быстрее, а однопоточный - медленнее
- В Python с GIL на 1 поток тратится 1 поток ОС, в Python nogil тоже можно использовать виртуальные потоки.



- Слайд из презентации про PHD 2024:

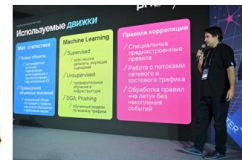
ML, AI, LLM, ChatGPT (?)... Правила!



<https://www.securityvision.ru/blog/irp-soar-2-0-na-platfome-security-vision-5/>



<https://www.securityvision.ru/news/security-vision-na-phdays-13-kak-eto-bylo/>



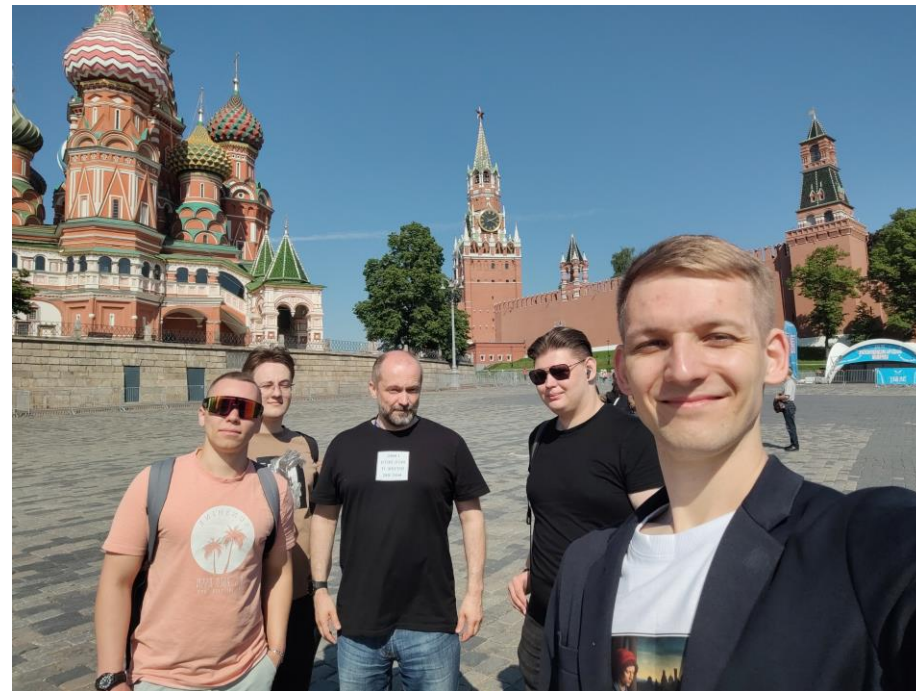
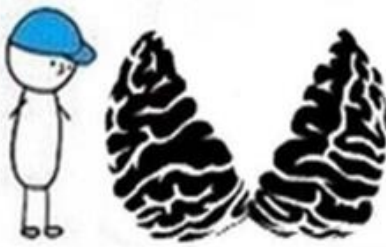
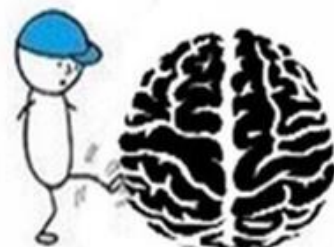
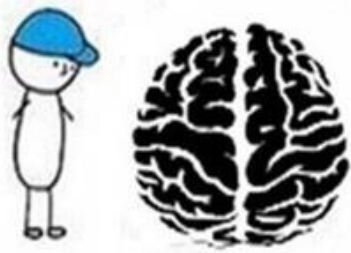
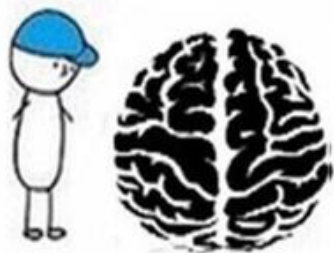
- Идея из 2025: большие модели шагнули вперёд, кто не использует сейчас – может не догнать потом

Послушать ещё? <https://phdays.com/>

The screenshot shows the 'Программа' (Program) page for PHDays 2024. It features a grid of sessions categorized by time slots (e.g., 10:00-10:30, 10:30-11:00) and topics (e.g., Python, Platform Engineering, School CISO). Each session entry includes a title, speaker names, and a 'Watch' button. The interface is dark-themed with green accents.

The screenshot shows the 'Трансляция' (Live Stream) page for PHDays 2024. The main content area displays a video player with a live stream of a speaker. The video title is 'А кто-то по прежнему уверен в своей незаменимости' (And who still believes in their own indispensability). The video player includes a progress bar and a volume icon. The sidebar on the right lists recommended sessions with their titles and 'Watch' buttons. The top navigation bar includes links to 'ПОЗИТИВ МЕРЧ' (Positive Merch) and 'ПРОГРАММА' (Program).

Вне конфы



Полезные контакты

- Дмитрий Левшун – к.т.н. в ИТМО, занимается ML в ИБ (с И.В. Котенко)
- Абдулхамид Бучаев – аспирант ИТМО, диссер про анализ событий ИБ
- Михаил Васильев (Гарда, делает DСАР) – занимается аномалиями (<https://onixlas.github.io/>), решает задачи, применимые в NTA