Ландшафт актуальных угроз безопасности информации и тенденции их развития

Докладчик:
начальник отдела,
к.т.н. Сердечный Алексей Леонидович
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Источники исходных данных об угрозах безопасности информации

Граф связей источников

Мониторинг

более **1 тыс.** *сайтов*

более **4 тыс.** *каналов и чатов*

около **2 тыс.** *блогов и гильдий*

более **5 тыс.** *репозиториев*

В основе графа более **380 тыс.** *источников*

Информационная карта

Информационные технологии

Информационная безопасность

Россия-Украина (топит.)

Darknet

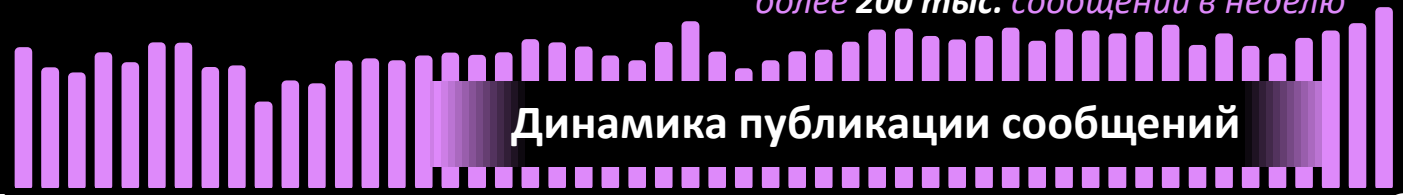
Азия и Ближний В...

Источники исходных данных об угрозах безопасности информации

Виды источников

- базы данных (угроз, уязвимостей, эксплойтов, инцидентов);
- новостные источники;
- отчёты, статьи и заметки исследователей;
- TI-платформы;
- теневой интернет (Darknet)

*более **200 тыс.** сообщений в неделю*

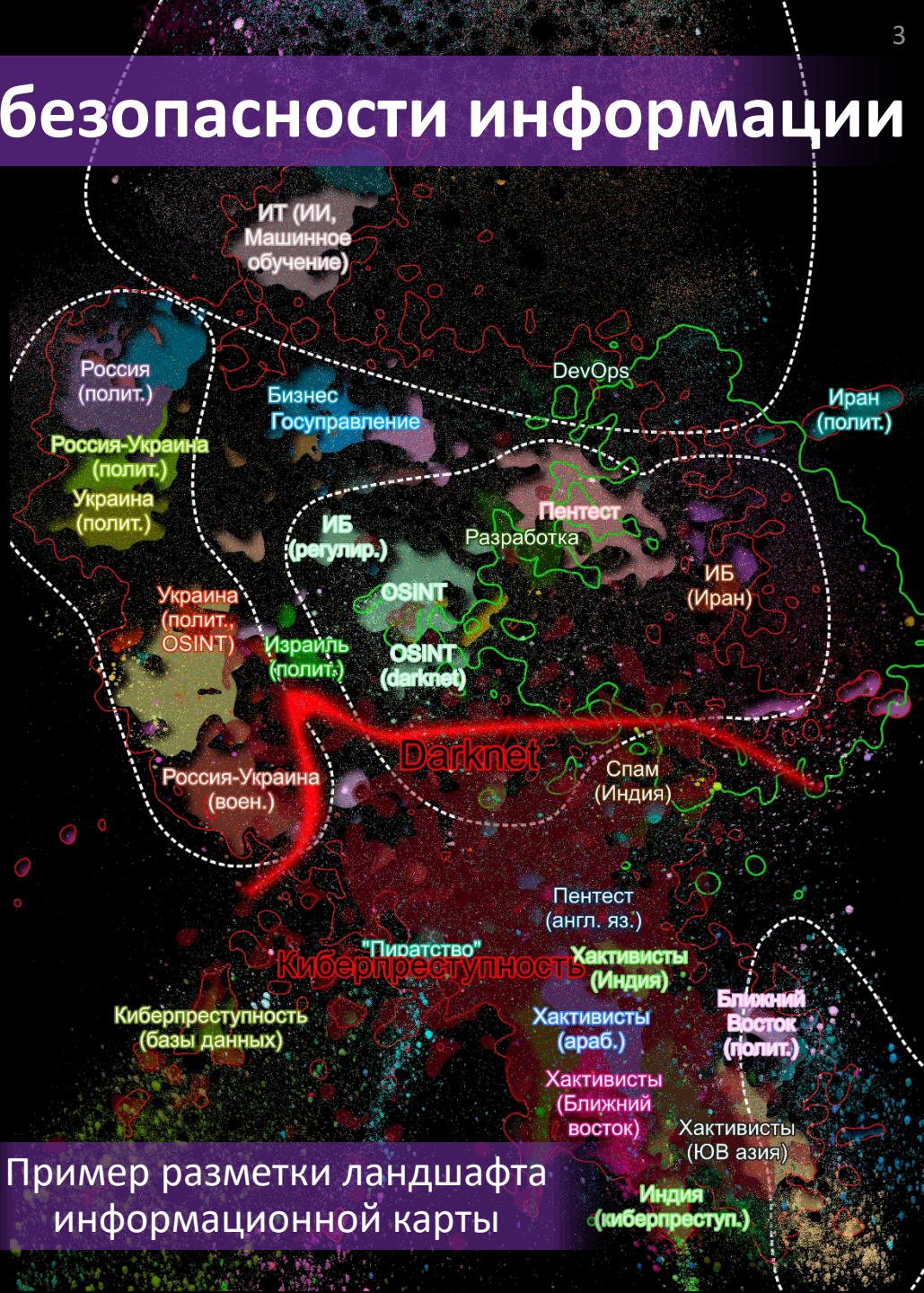


Потенциал

- высокий
- средний
- базовый повышенный
- базовый

Виды нарушителей

- APT-группировки
- Финансово-мотивированные группировки
- Хактивисты
- Низкоквалифицированные киберпреступники

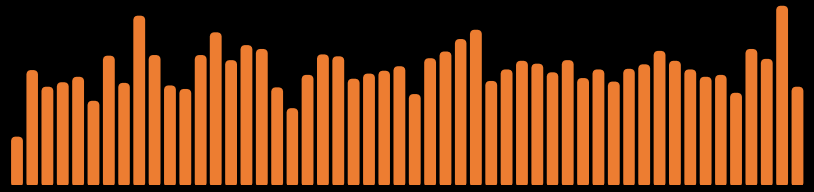


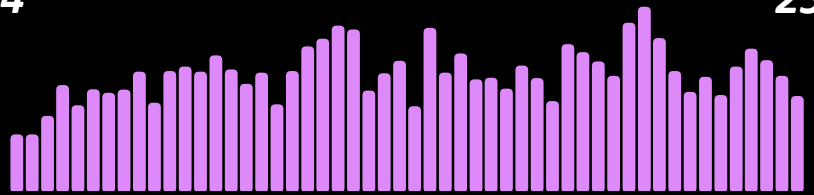
Пример разметки ландшафта информационной карты

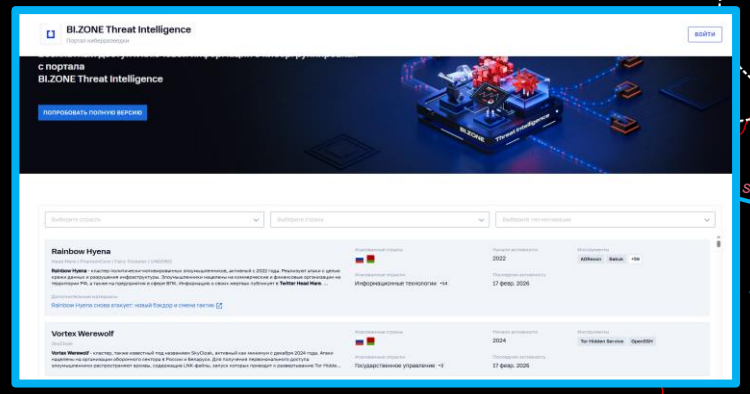
Источники исходных данных о хакерских группировках

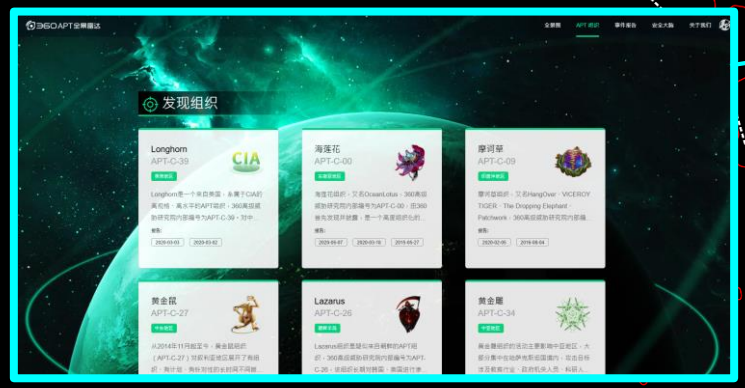
	2024	2025
Сообщений:	8 729	13 043
Отчётов:	2 789	3 295
Источников (TG/сайты):	544 / 398	596 / 304

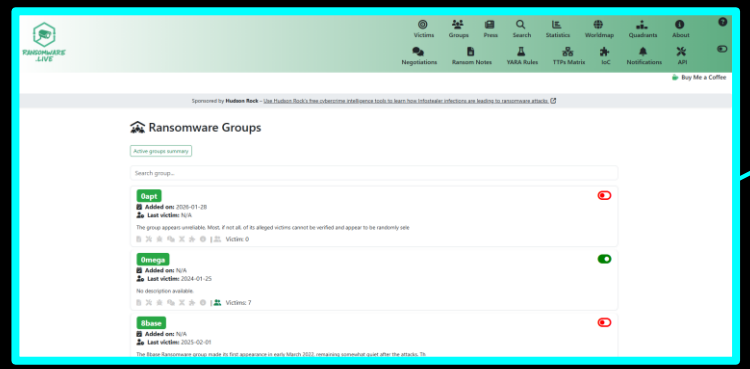
Динамика публикации отчётов

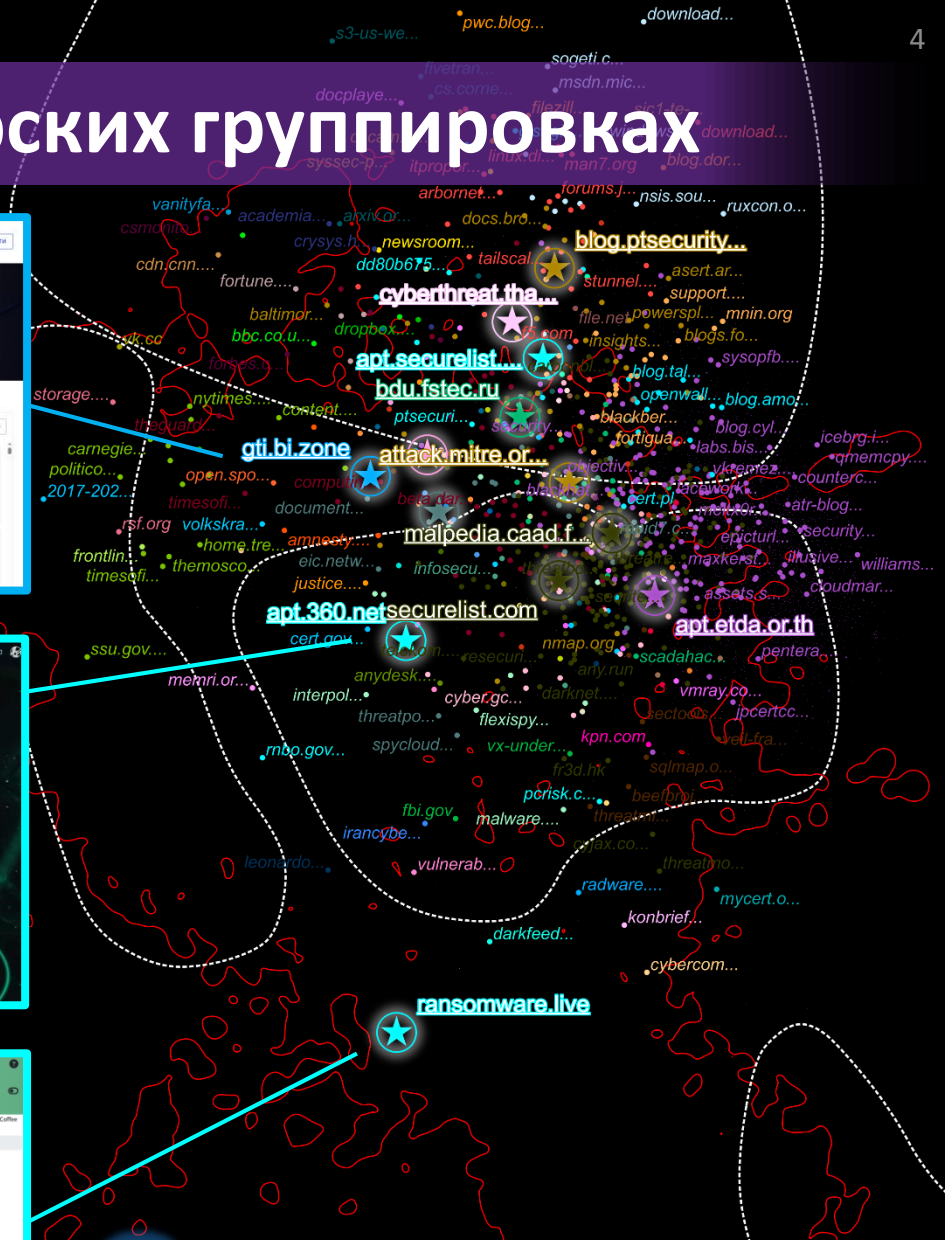












база сведений о хакерских группировках

исследователь (первоисточник публикации)

Информационная карта хакерских группировок

Источники исходных данных

kaspersky · SOLAR · pt · BI.ZONE Cybersecurity · F6 · MITRE ATT&CK · malpedia · THALES · ETDA · MISP Threat Sharing · RANSOMWARE .LIVE

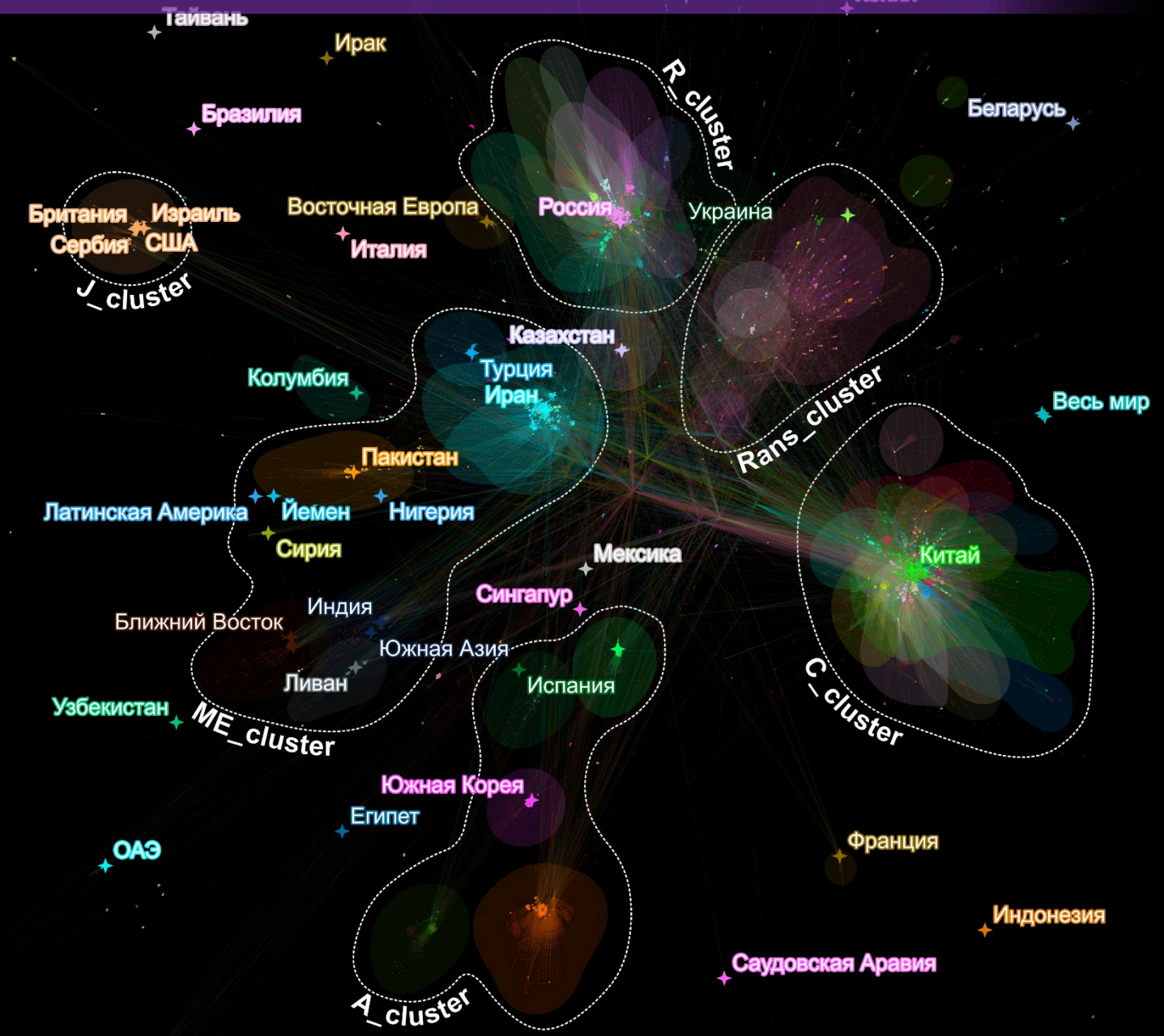
3 513 наименований хакерских группировок

5 830 наименований вредоносного ПО

Более **10 000** отчетов и публикаций

Более **1 000** экспертных организаций

918 способов реализации угроз БИ



Инструмент ← Название группировки → Страна

Группировки, атаковавшие Россию в 2025 году

Источники исходных данных

kaspersky · SOLAR · pt · BI.ZONE Cybersecurity · F6 · MITRE ATT&CK · malpedia · THALES · ETDA · MISP Threat Sharing · RANSOMWARE.LIVE

3 513 наименований хакерских группировок

5 830 наименований вредоносного ПО

Более **10 000** отчетов и публикаций

Более **1 000** экспертных организаций

918 способов реализации угроз БИ

Инструмент ← Название группировки → Страна

Группировки, атаковавшие Россию в 2025 году

Источники исходных данных

kaspersky · SOLAR · pt · BI.ZONE Cybersecurity · F6 · MITRE ATT&CK · malpedia · THALES · ETDA · MISP Threat Sharing · RANSOMWARE .LIVE

3 513 наименований хакерских группировок

5 830 наименований вредоносного ПО

Более **10 000** отчетов и публикаций

Более **1 000** экспертных организаций

918 способов реализации угроз БИ

Инструмент ← Название группировки → Страна

Группировки, атаковавшие Россию в 2025 году

Источники исходных данных

kaspersky · SOLAR · pt · BI.ZONE Cybersecurity · F6 · MITRE ATT&CK · malpedia · THALES · ETDA · MISP Threat Sharing · RANSOMWARE.LIVE

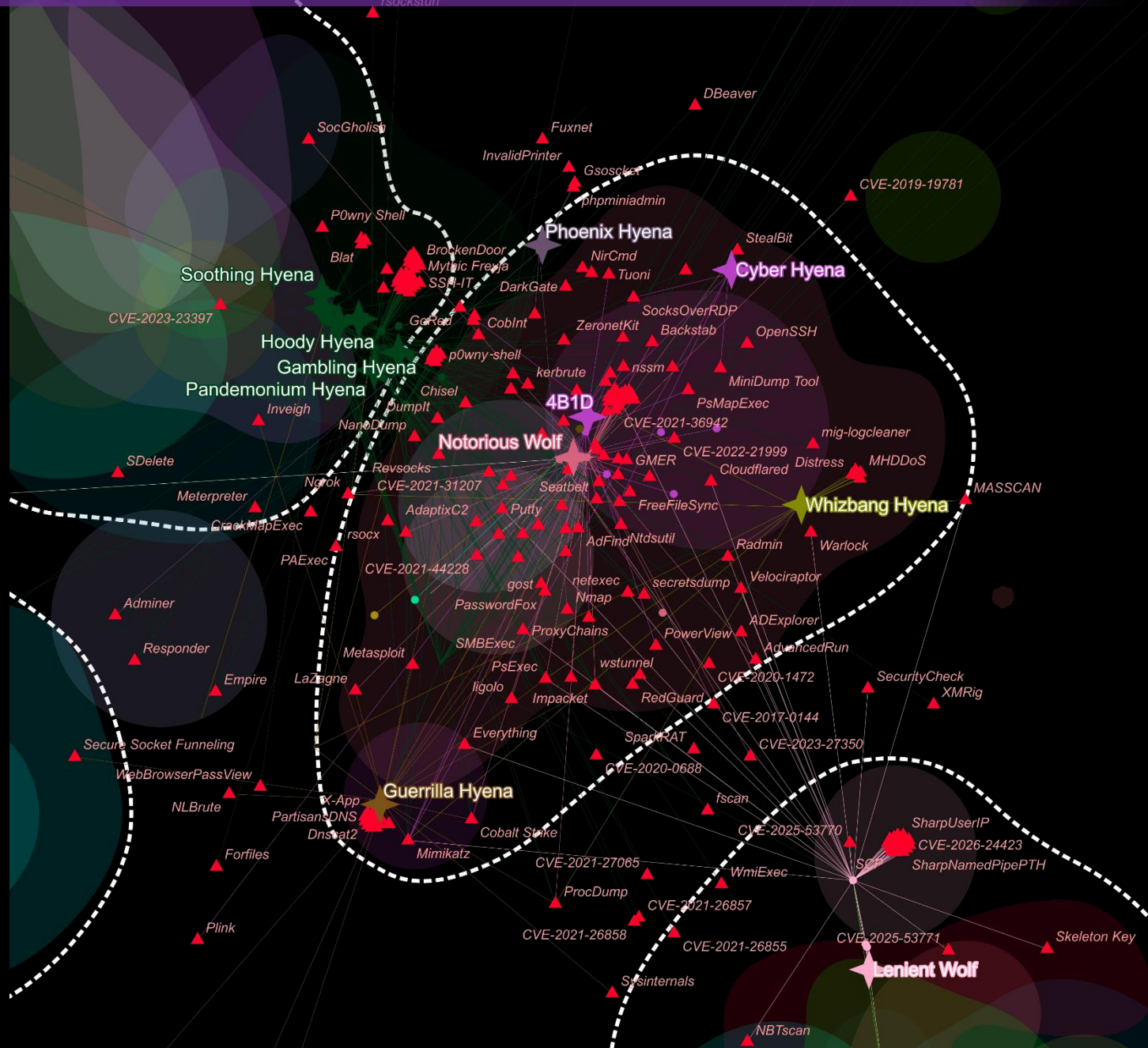
3 513 наименований хакерских группировок

5 830 наименований вредоносного ПО

Более **10 000** отчетов и публикаций

Более **1 000** экспертных организаций

918 способов реализации угроз БИ

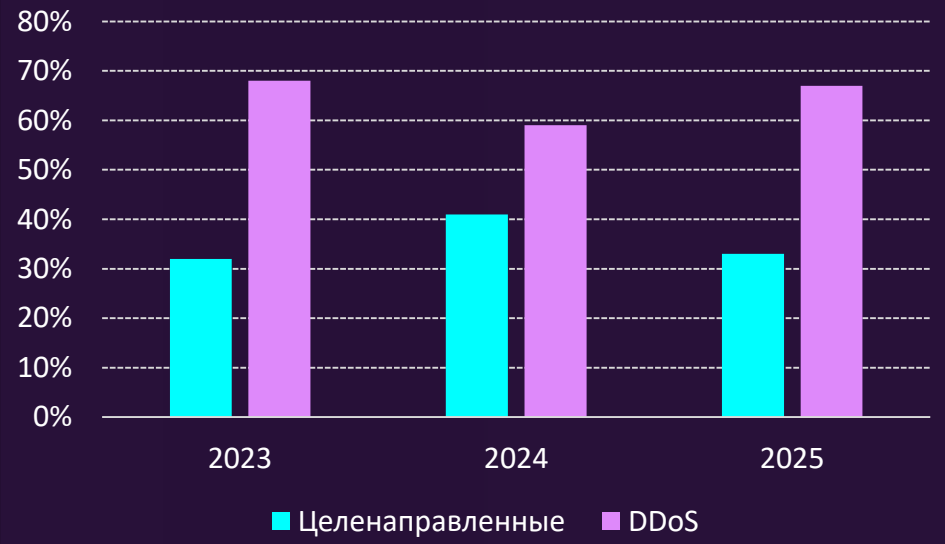


Инструмент ← Название группировки → Страна

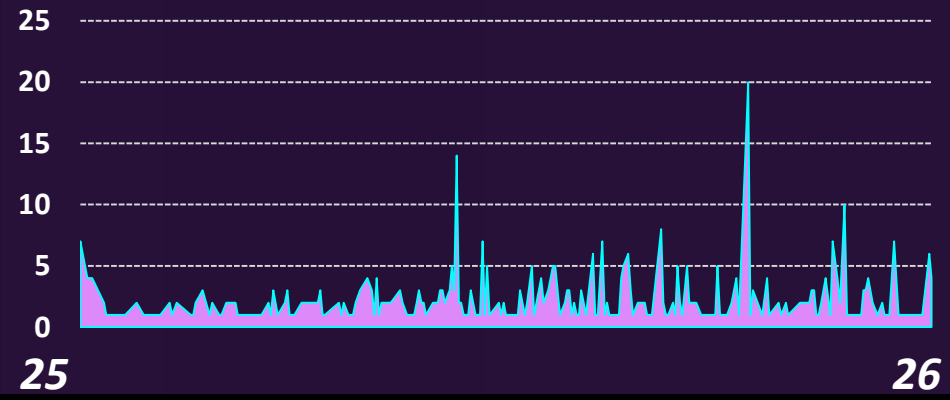
Статистика инцидентов, упоминаемых в открытых источниках

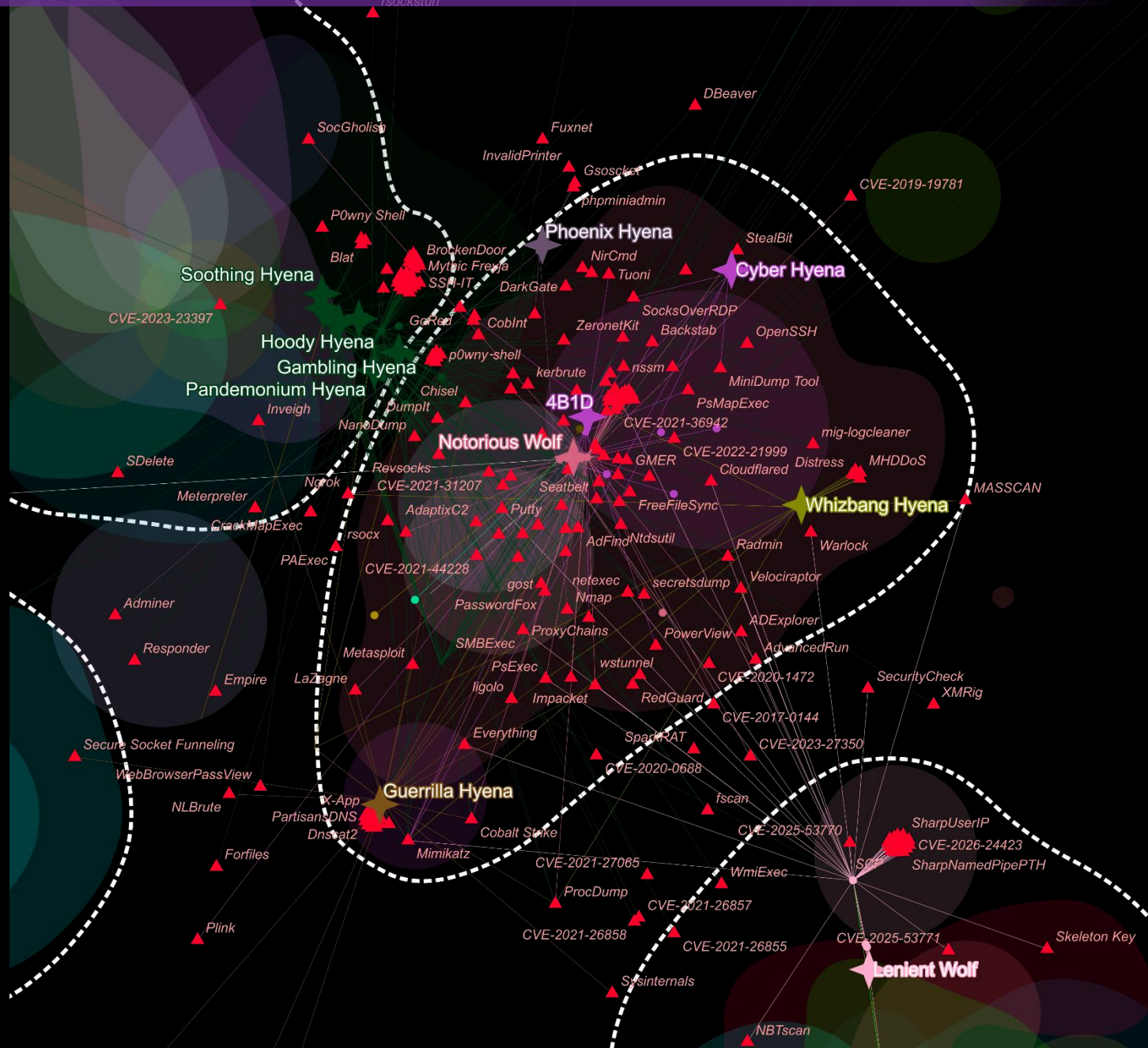
Зафиксировано упоминаний инцидентов:	2023	2024	2025
	389	405	479

Виды инцидентов

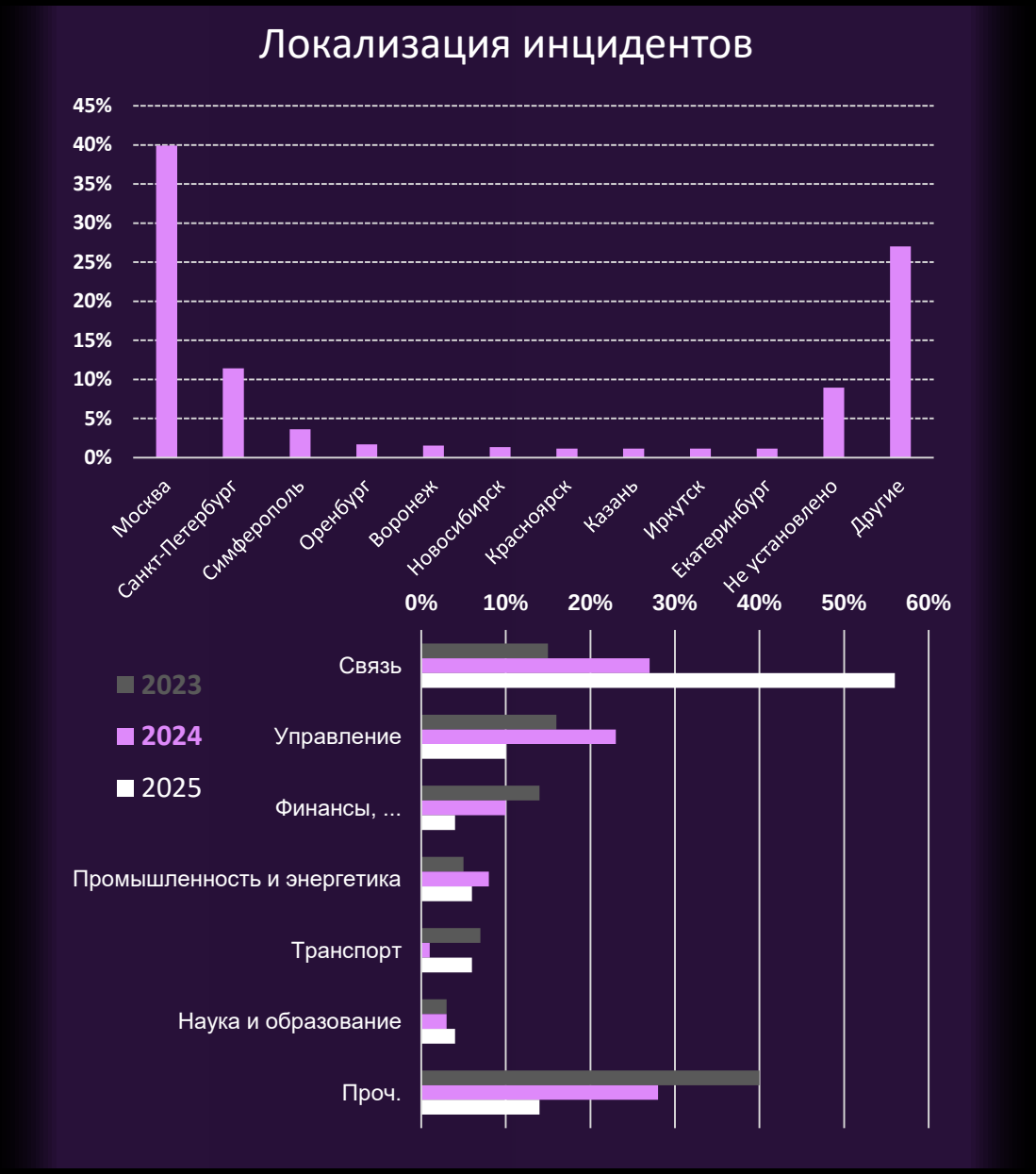


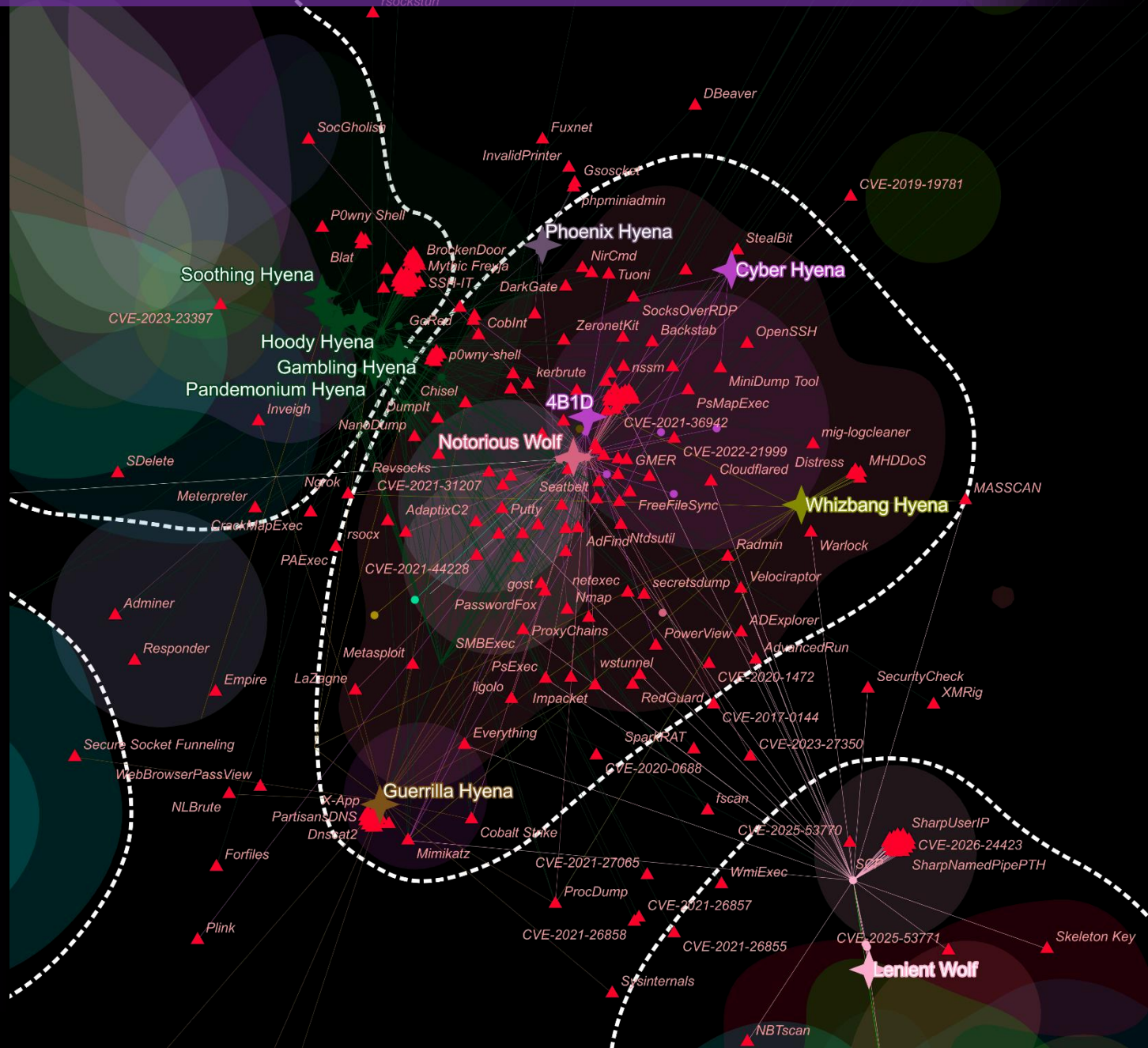
Динамика инцидентов



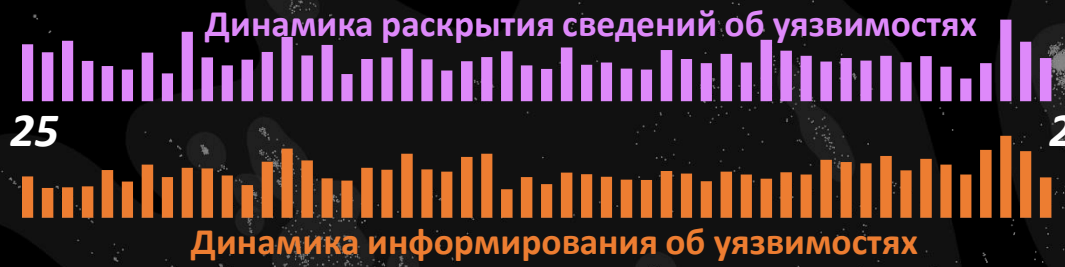


Статистика инцидентов, упоминаемых в открытых источниках





Информационная карта уязвимостей за 2025 год



Windows

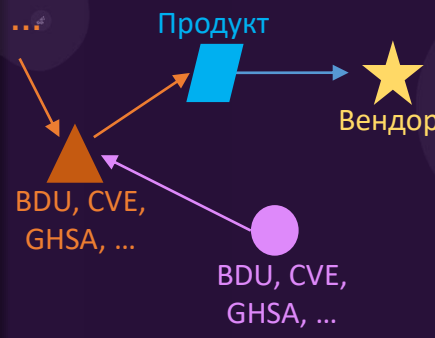
Облачное ПО

Аппаратное обеспечение

Веб

Linux/Unix

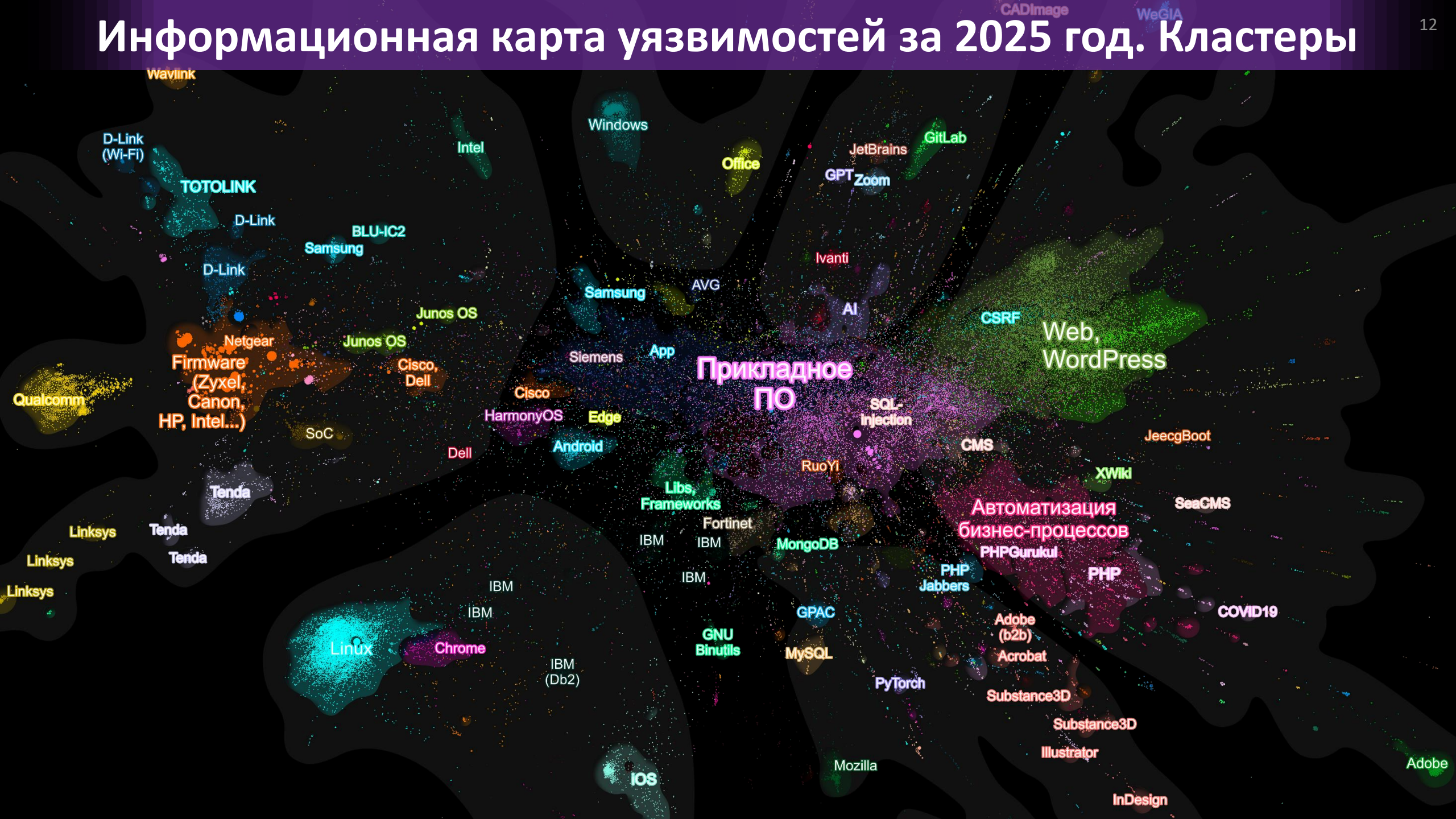
Прикладное ПО



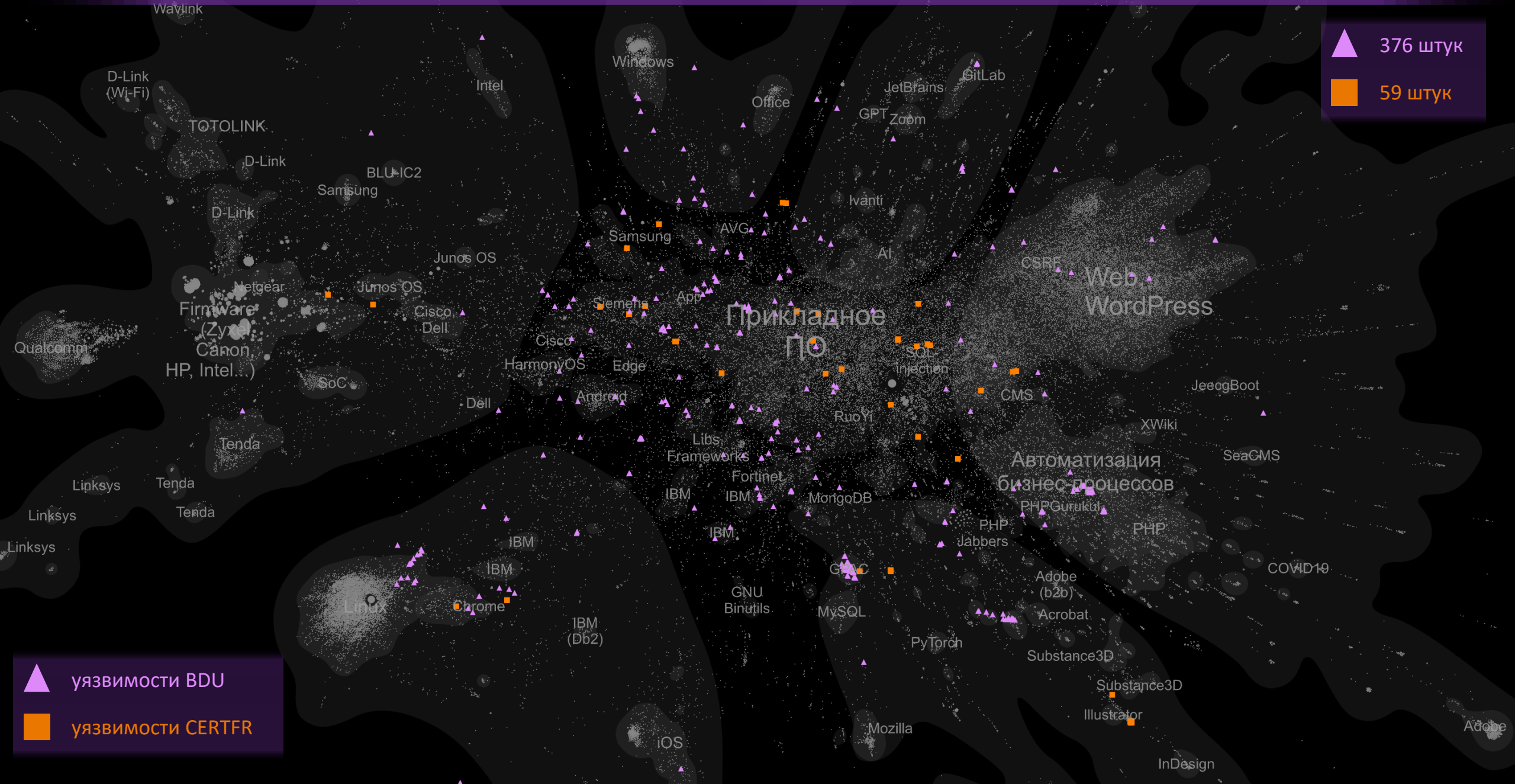
зона с отозванными идентификаторами уязвимостей

	BDU	CVE
Опубликовано:	16 230	49 972
Отозвано:	33	1 799
Вендоры:	810	3 757

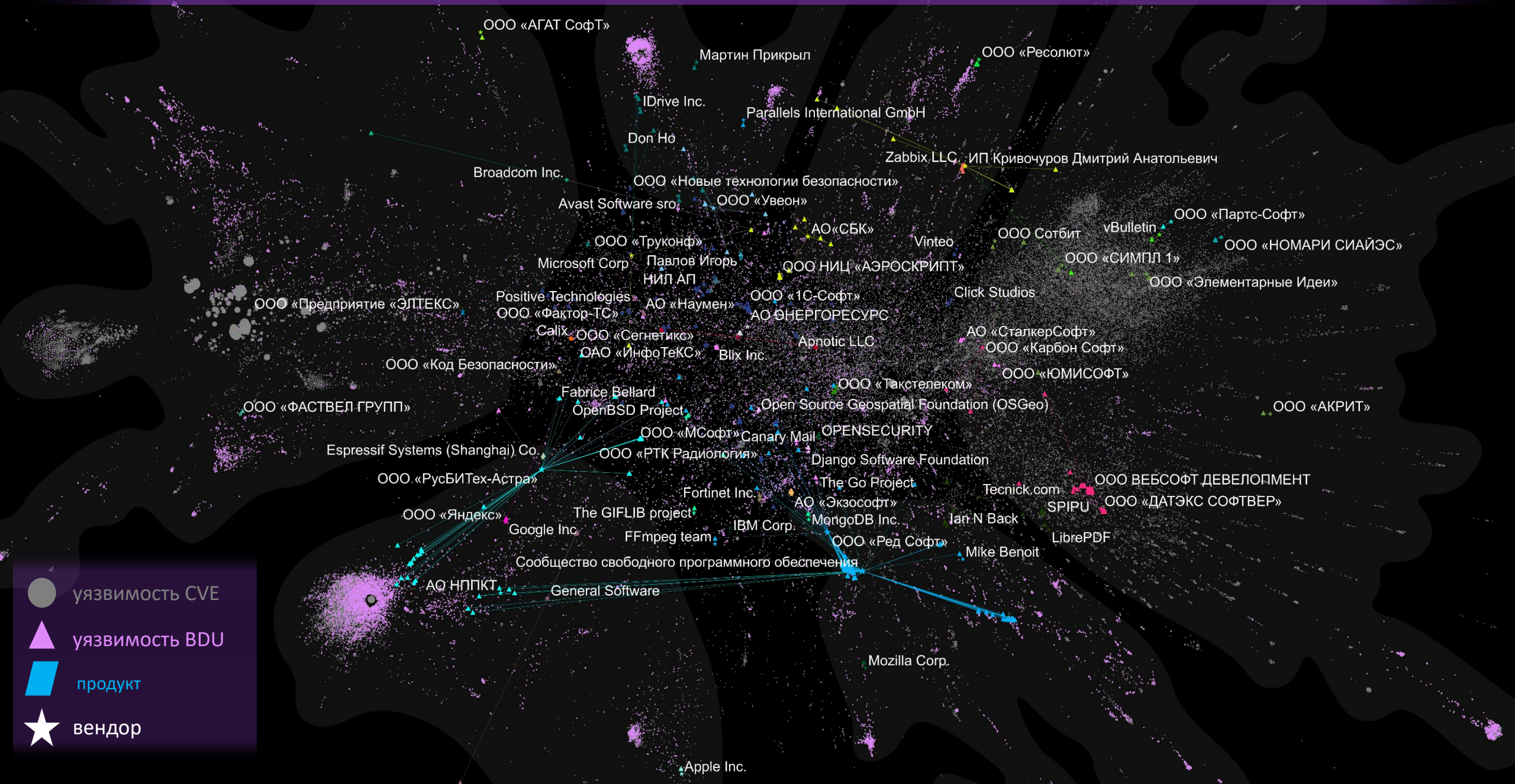
Информационная карта уязвимостей за 2025 год. Кластеры



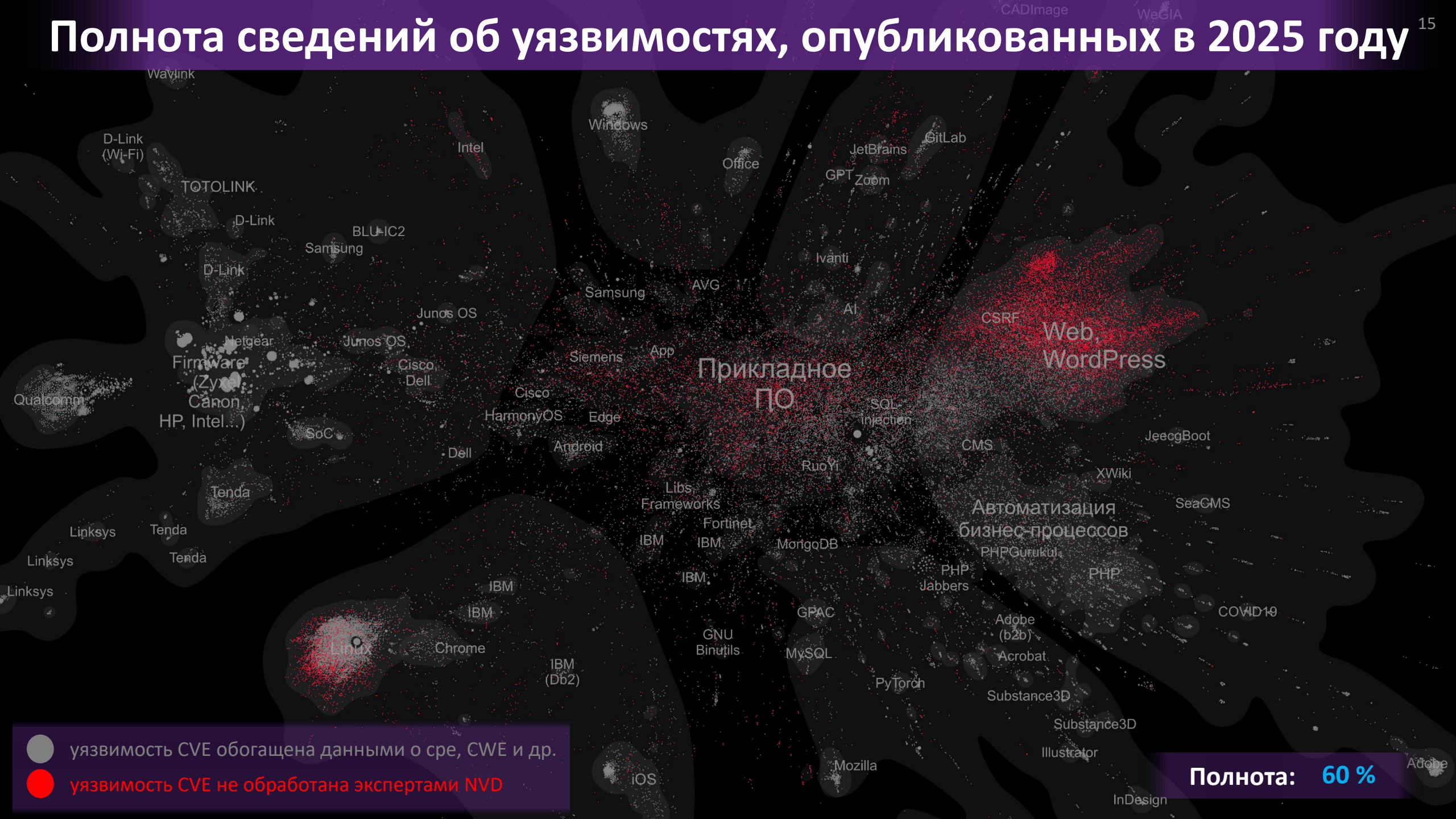
Уязвимости BDU и CERTFR без CVE



Уникальные уязвимости в bdu.fstec.ru (2025 год)



Полнота сведений об уязвимостях, опубликованных в 2025 году

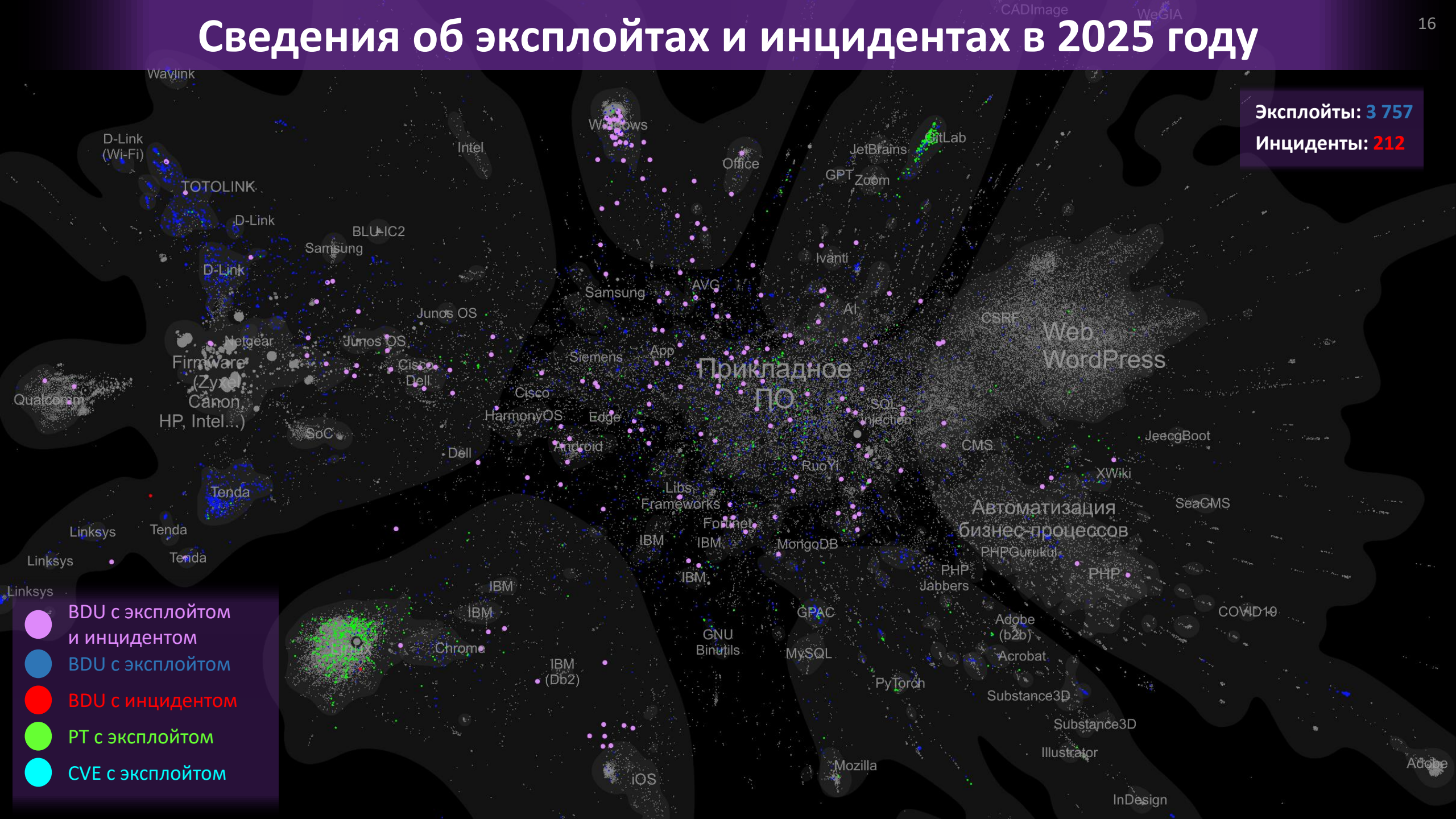


уязвимость CVE обогащена данными о cpe, CWE и др.

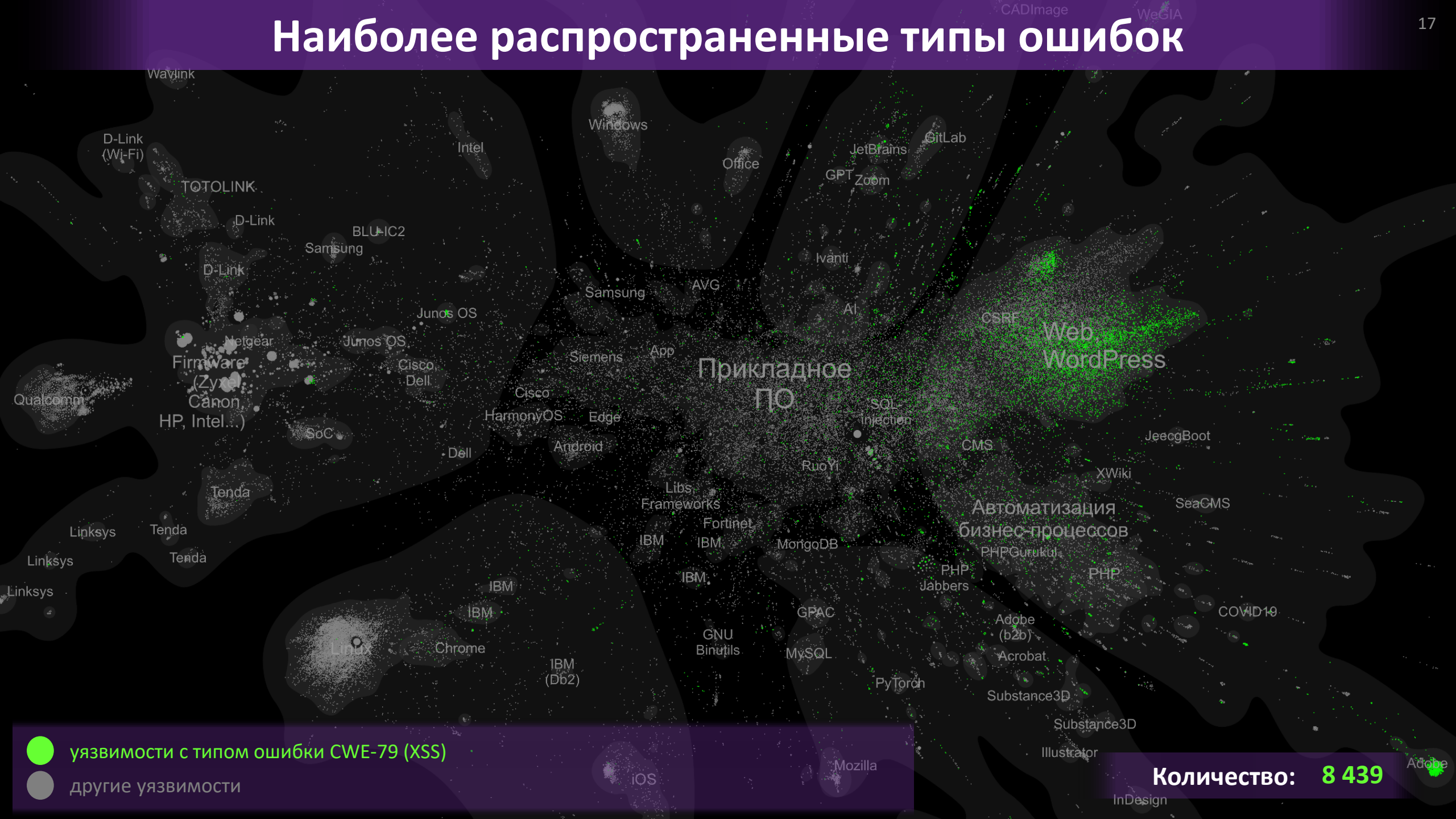
уязвимость CVE не обработана экспертами NVD

Полнота: 60 %

Сведения об эксплойтах и инцидентах в 2025 году



Наиболее распространенные типы ошибок

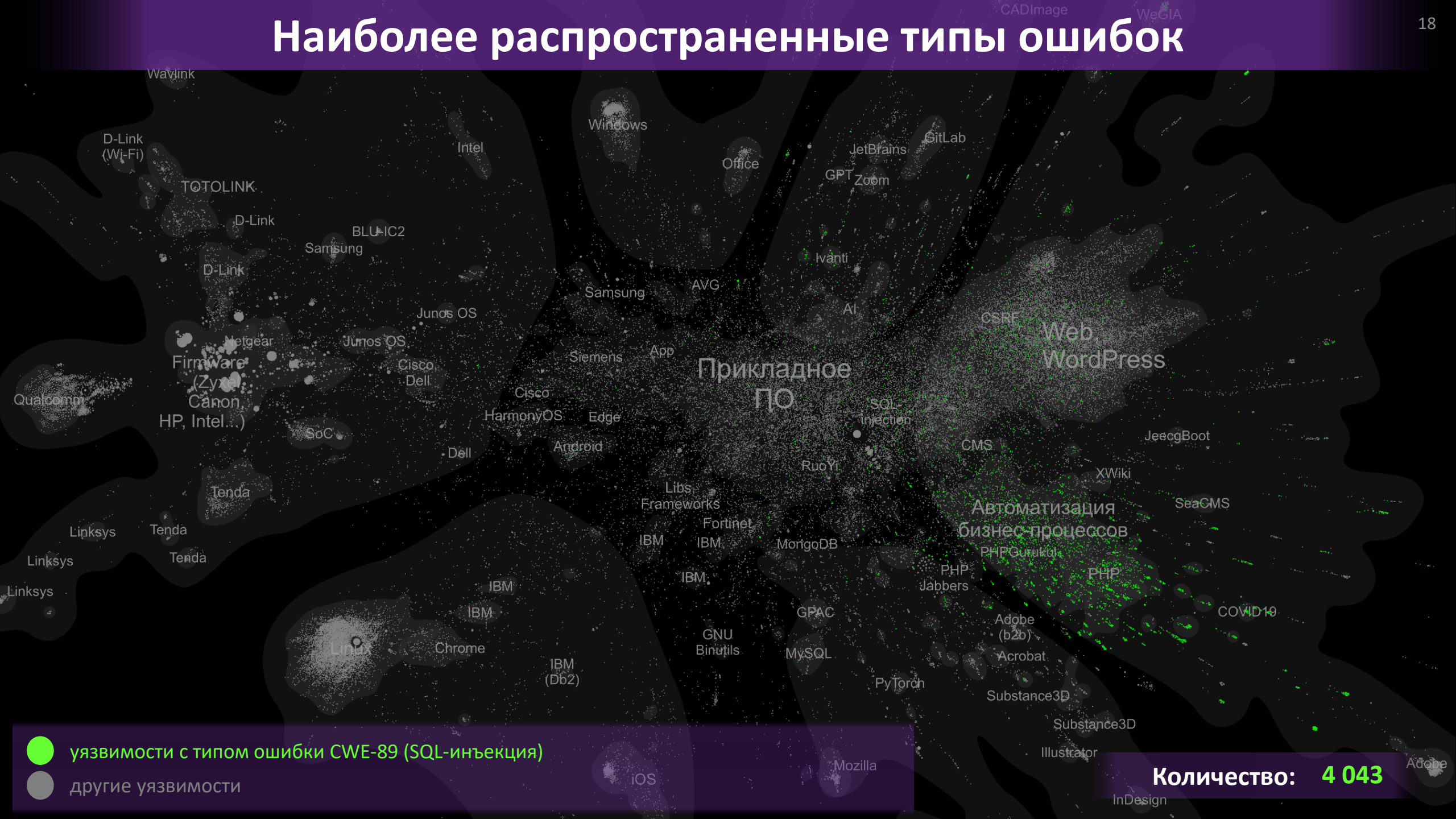


уязвимости с типом ошибки CWE-79 (XSS)

другие уязвимости

Количество: 8 439

Наиболее распространенные типы ошибок

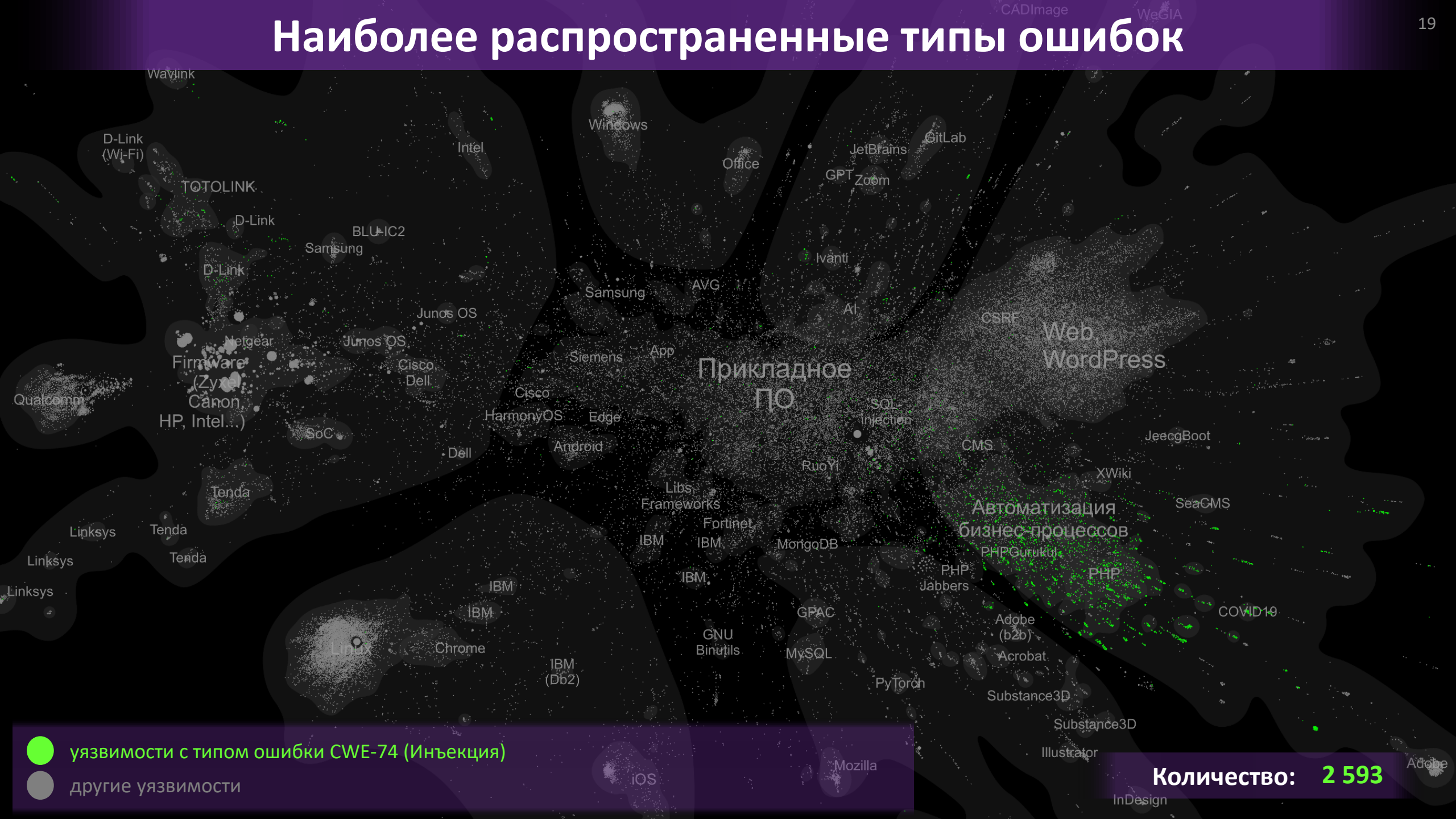


уязвимости с типом ошибки CWE-89 (SQL-инъекция)

другие уязвимости

Количество: 4 043

Наиболее распространенные типы ошибок

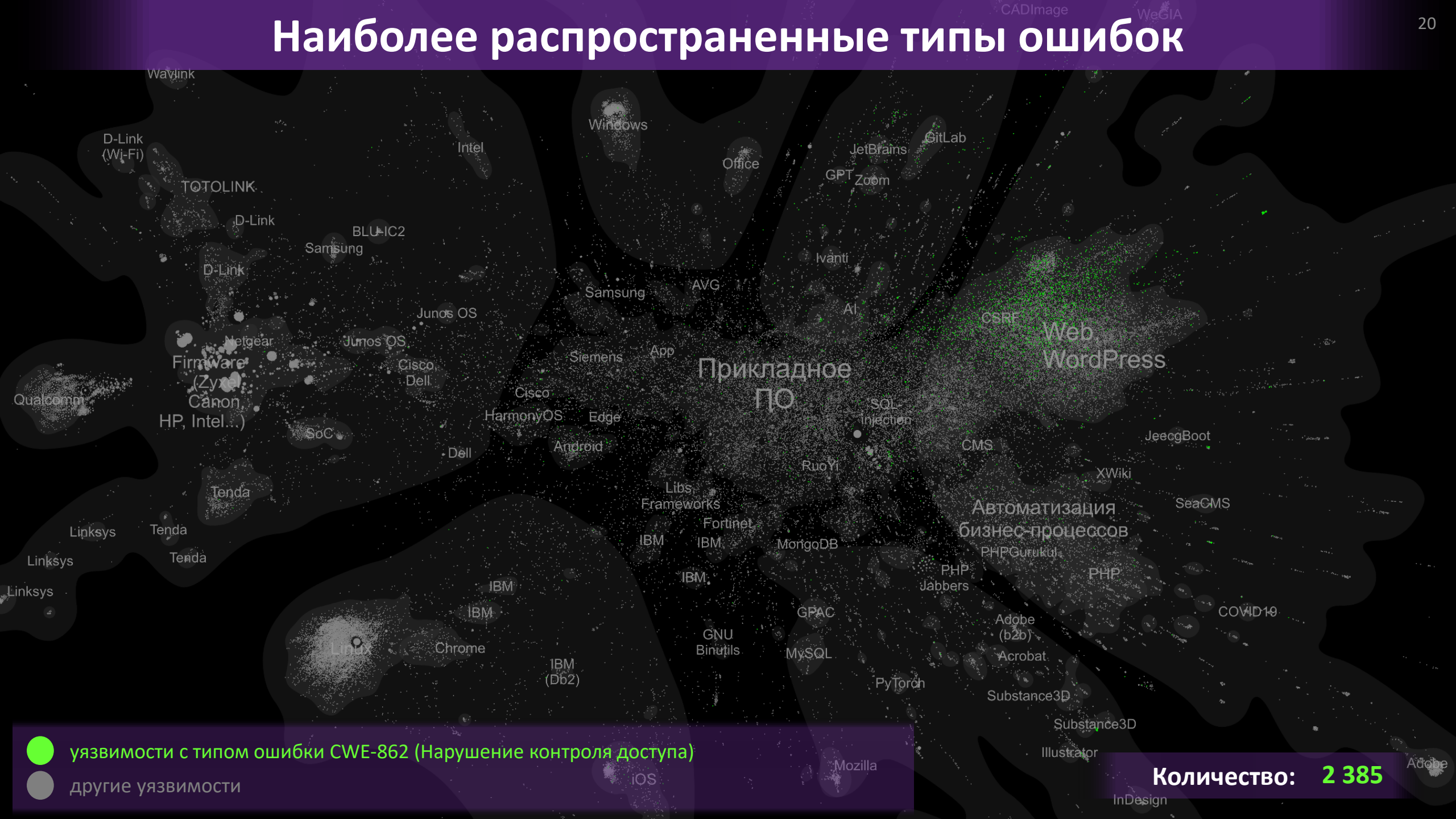


уязвимости с типом ошибки CWE-74 (Инъекция)

другие уязвимости

Количество: 2 593

Наиболее распространенные типы ошибок

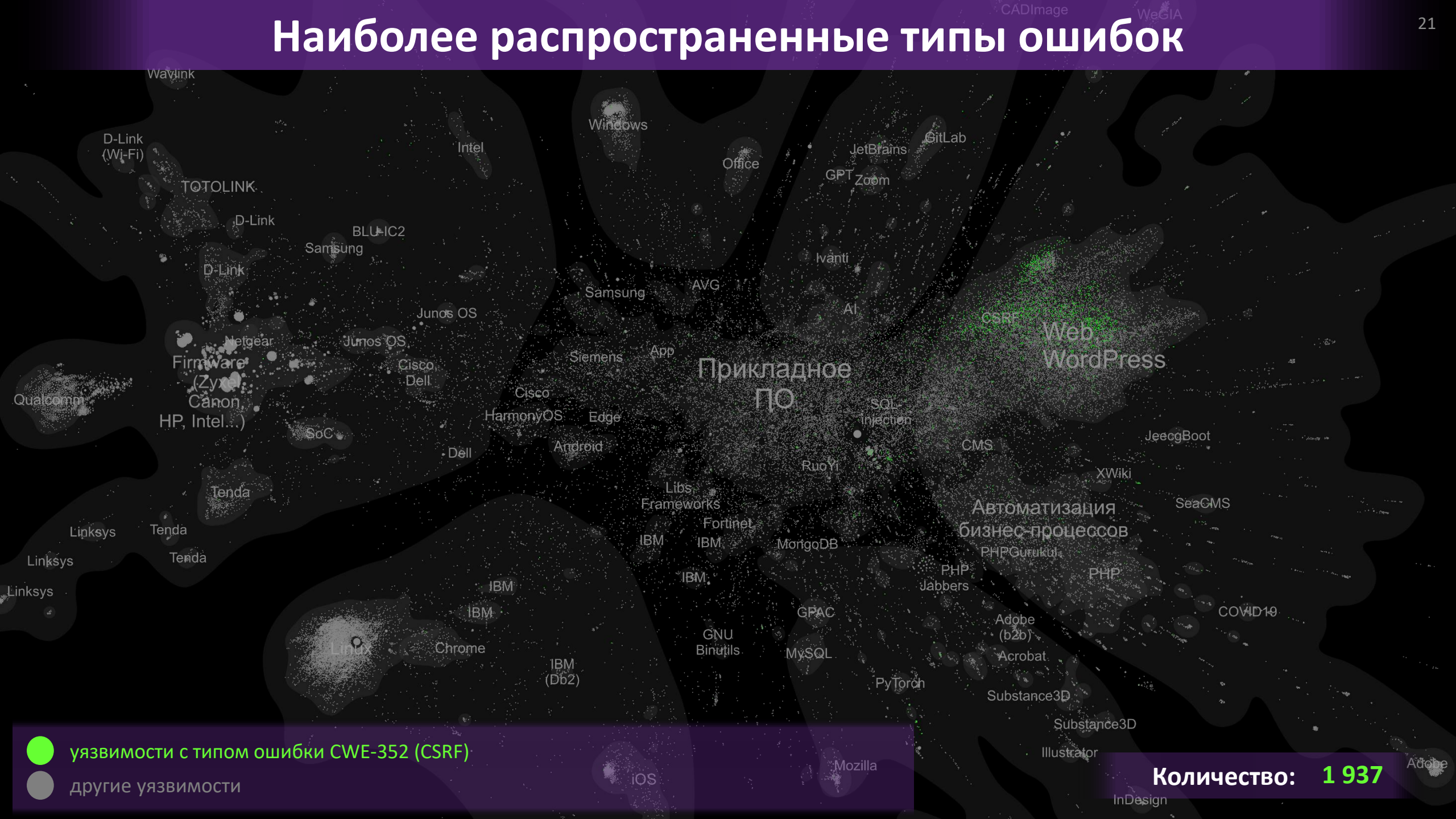


уязвимости с типом ошибки CWE-862 (Нарушение контроля доступа)

другие уязвимости

Количество: 2 385

Наиболее распространенные типы ошибок

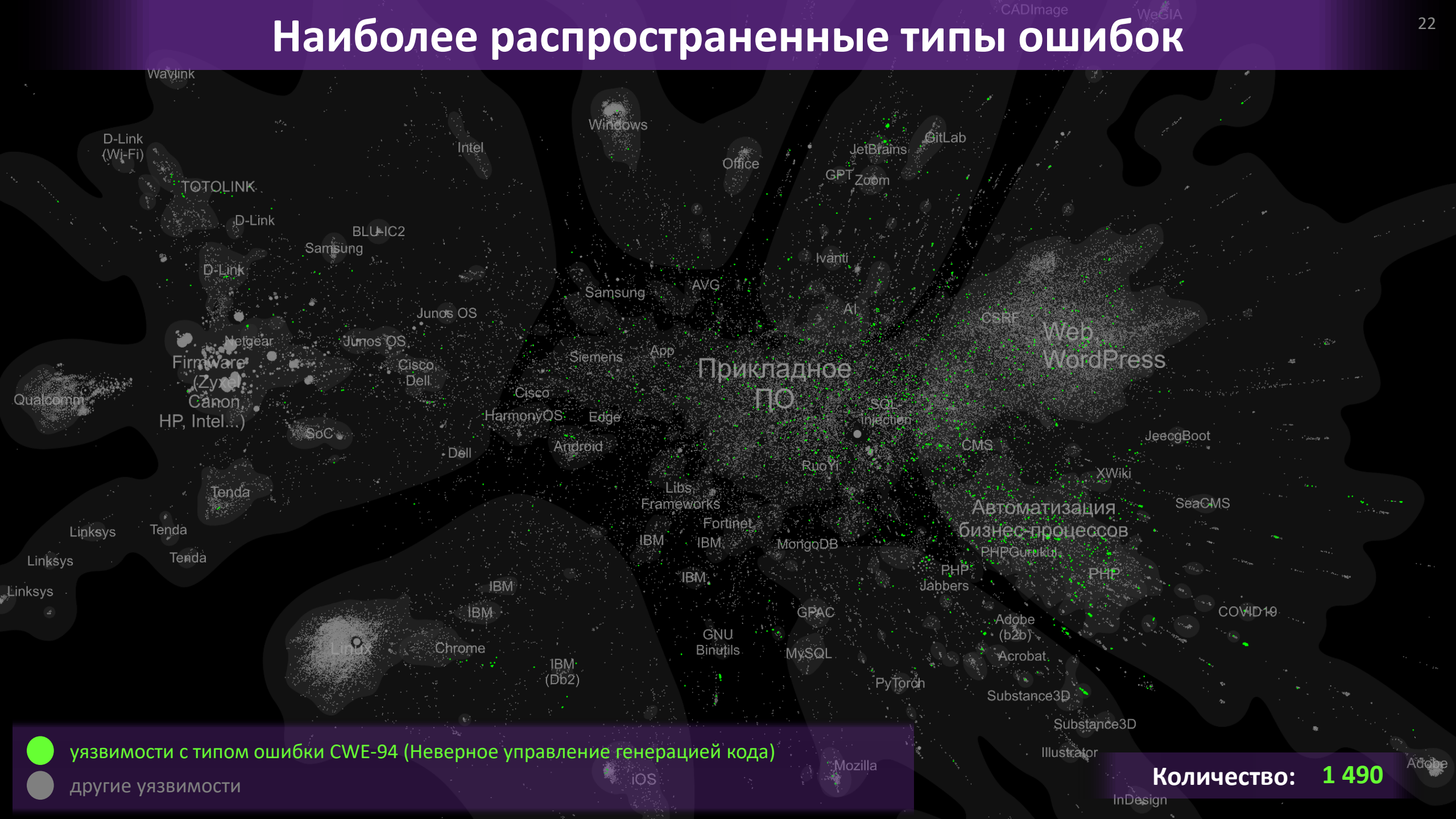


уязвимости с типом ошибки CWE-352 (CSRF)

другие уязвимости

Количество: 1 937

Наиболее распространенные типы ошибок

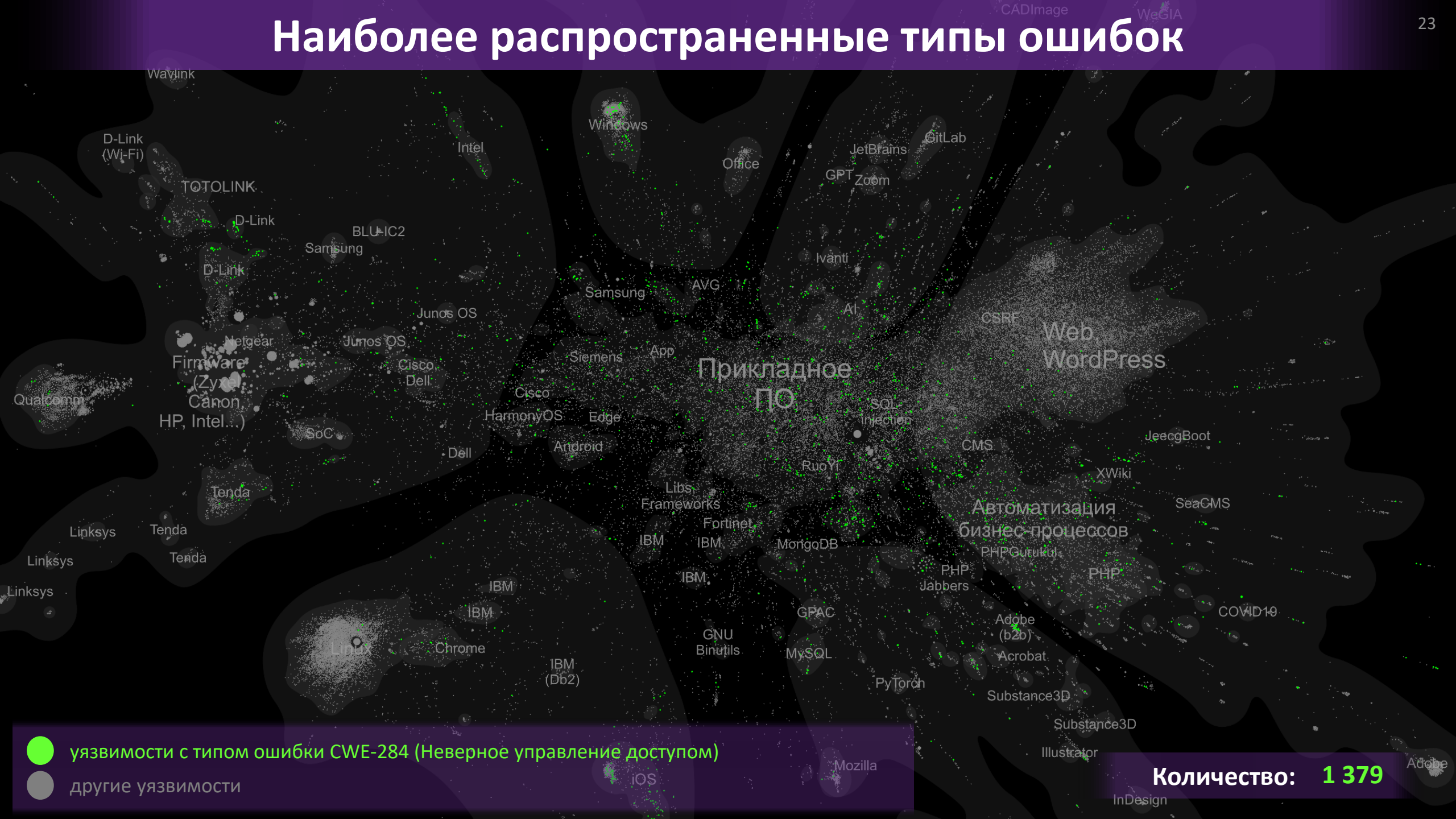


уязвимости с типом ошибки CWE-94 (Неверное управление генерацией кода)

другие уязвимости

Количество: 1 490

Наиболее распространенные типы ошибок

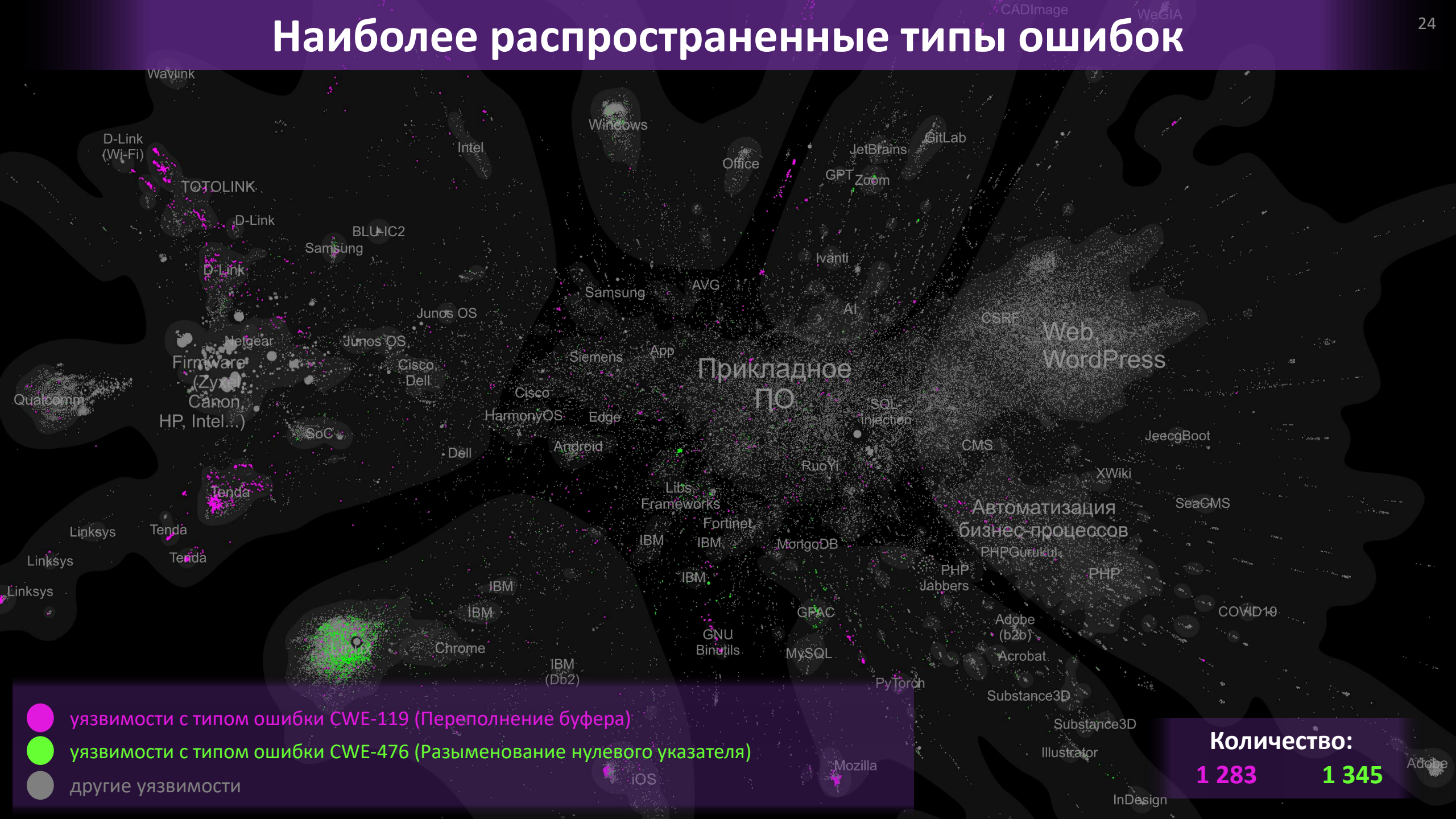


уязвимости с типом ошибки CWE-284 (Неверное управление доступом)

другие уязвимости

Количество: 1 379

Наиболее распространенные типы ошибок



уязвимости с типом ошибки CWE-119 (Переполнение буфера)

уязвимости с типом ошибки CWE-476 (Разыменование нулевого указателя)

другие уязвимости

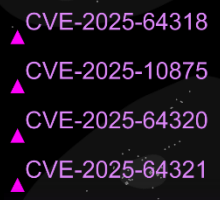
Количество:

1 283 **1 345**

Уязвимости и ИИ

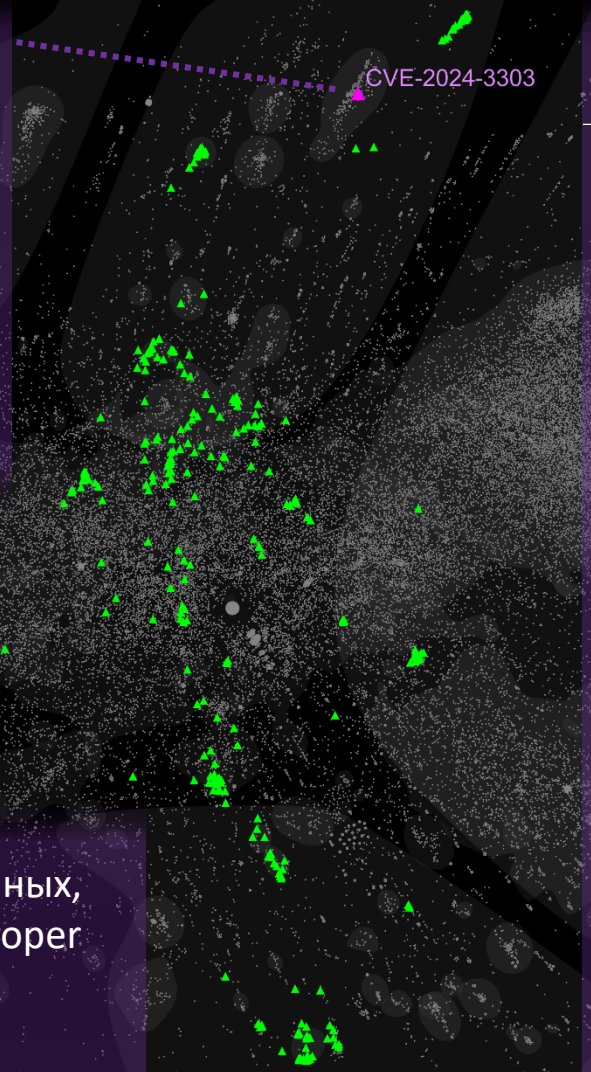
BDU:2025-05388: GitLab, CWE-74 («Инъекция»), CWE-116 (Некорректное кодирование или сокрытие выходных данных)

Уязвимость программной платформы на базе git для совместной работы над кодом GitLab Enterprise Edition связана с неверной нейтрализацией особых элементов в выходных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти существующие ограничения безопасности и получить несанкционированный доступ к защищаемой информации



CWE-1427: Ненадлежащая нейтрализация входных данных, используемых для формирования промптов LLM (Improper Neutralization of Input Used for LLM Prompting)

Проблема возникает из-за того, что LLM воспринимает и системные инструкции разработчика, и входные данные пользователя как единый поток текста на естественном языке. Модель не может на уровне архитектуры надежно отличить «команды» от «данных»



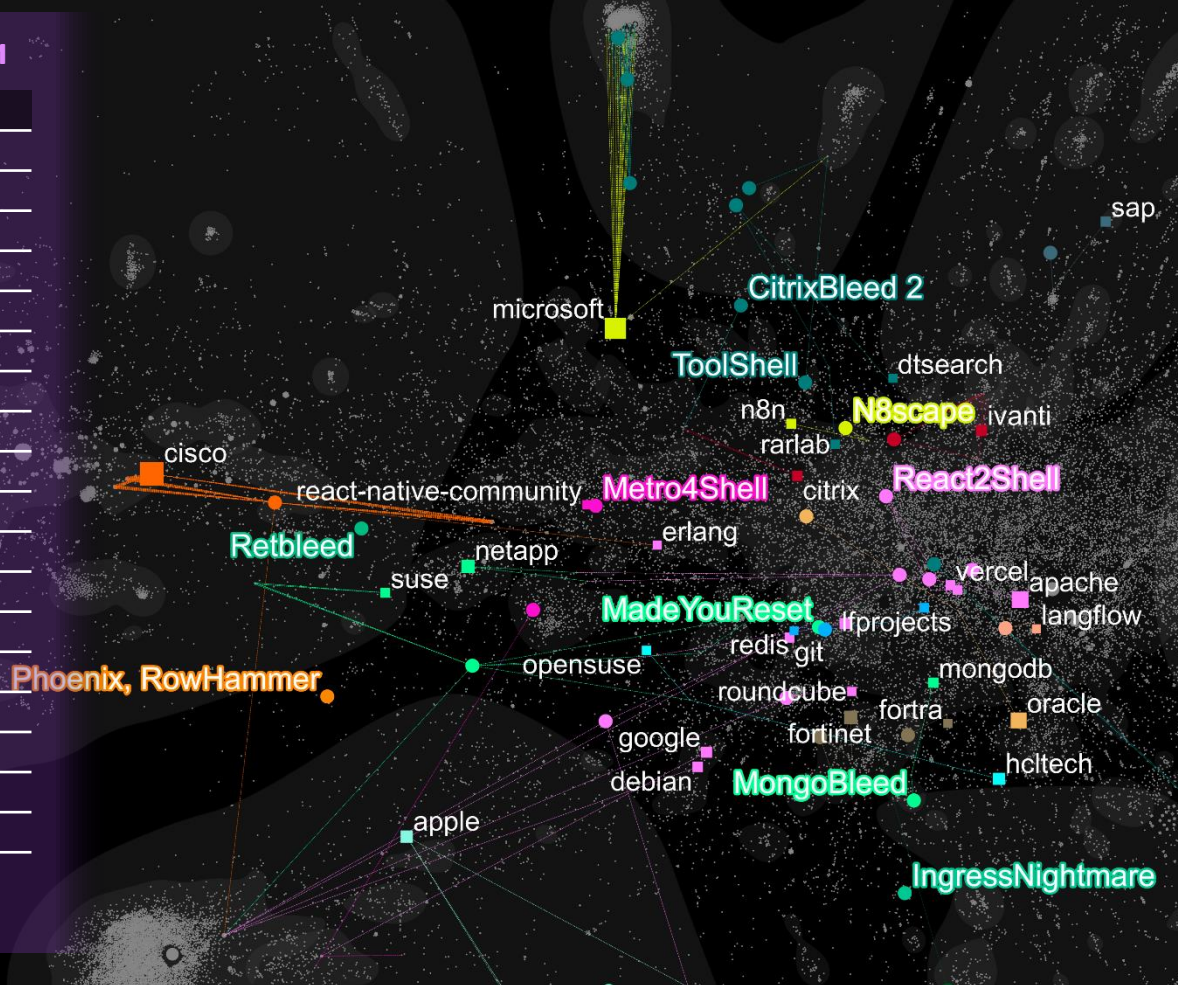
▲ уязвимость в продуктах ИИ

	k
nvidia:triton_inference_server	24
vllm:vllm	20
llamaindex:llamaindex	13
huggingface:transformers	11
librechat:librechat	6
flowiseai:flowise	6
ollama:ollama	6
langgenius:dify	5
applio:applio	4
agpt:autogpt_platform	4
keras:keras	4
bentoml:bentoml	3
apache:airflow	3
lfprojects:mlflow	3
chatchat-space:langchain-chatchat	3
humansignal:label_studio	3
aimstack:aim	2
artificial_intelligence_project:artificial_intelligence	2
gaizhenbiao:chuanhuchatgpt	2
lfprojects:valkey	2
huggingface:smolagents	2
drupal:artificial_intelligence	2
nvidia:nvidia_resiliency_extension	2
pytorch:pytorch	2
dbgpt:db-gpt	2
...	...

Именные и цитируемые уязвимости 2025 года

Именные уязвимости

№	Имя
1	React2Shell
…	
5	ToolShell
…	
11	CitrixBleed 2
…	
13	MongoBleed
…	
33	IngressNightmare
…	
59	EBS-Exploit
…	
106	Metro4Shell
…	
165	MadeYouReset
…	
252	N8scape
…	
377	Phoenix, RowHammer
…	…



10 самых популярных уязвимостей

№	BDU	Э	И	Вендор	k
1	BDU:2025-15156	✓	✓	facebook, vercel	2491
2	BDU:2025-11053	✓	✓	microsoft	799
3	BDU:2025-12468	✓	✓	oracle	796
4	BDU:2025-08691	✓	✓	git-scm, debian, apple	750
5	BDU:2025-08714	✓	✓	microsoft	689
6	BDU:2025-03185	✓	✓	vercel	543
7	BDU:2025-09597	✓	✓	dtsearch, rarlab, microsoft	466
8	BDU:2025-07765	✓	✓	debian, redhat, suse, opensuse, sudo_project, canonical	422
9	BDU:2025-12999	✓	✓	microsoft	421
10	BDU:2025-02511	✓	✓	debian, netapp, apache	419

Меры защиты

Базовые меры

- идентификация и аутентификация
- управление доступом
- защита периметра и конечных точек
- устранение уязвимостей
- регистрация и учет
- повышение осведомленности сотрудников
- резервирование данных

Меры для защиты от нарушителей высокого уровня опасности

- разведка угроз
- инвентаризация инфраструктуры и управление уязвимостями
- SIEM
- ложные информационные системы
- другие усиливающие меры