



ИТОГИ 2023 ГОДА
ЗАЩИТА ДАННЫХ
С АЛЕКСЕЕМ ПЛЕШКОВЫМ



КОТ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ



Самые часто случающиеся инциденты информационной безопасности в 2023 году (RU)



58%

Утечки данных

40%

Программы вымогатели

47%

ПО для удаленного доступа

32%

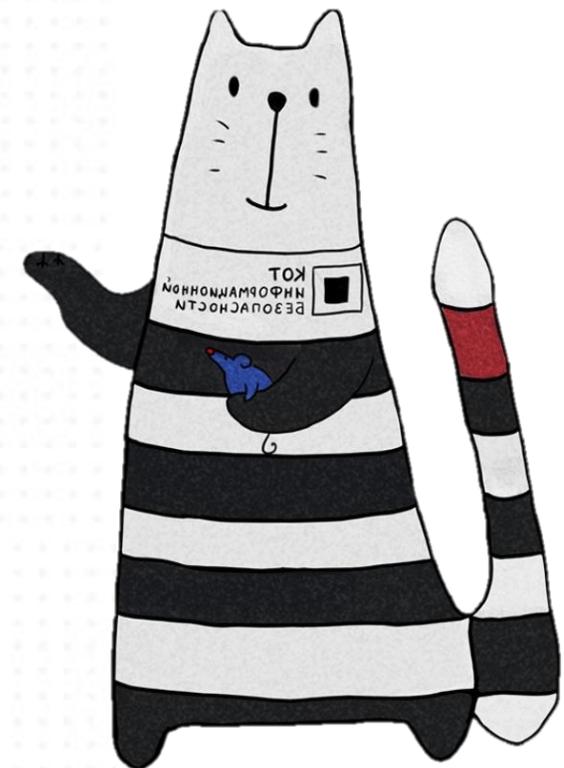
Электронный шпионаж

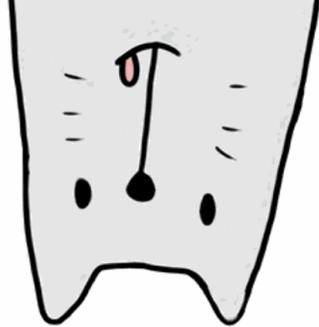
41%

Кража данных

11%

Атаки изнутри





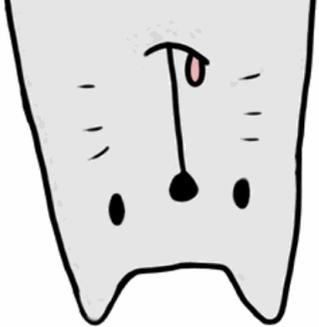
Утечки информации ограниченного доступа в Мире, 2023

Утекло данных: Σ 364 M+

UK: 40M+ избирателей

USA: 37M+ клиентов T-Mobile





Утечки информации ограниченного доступа в России, H1.2023

ВНУТРЕННИЙ НАРУШИТЕЛЬ+

...

сторонние исполнители работ по
заказу организации, партнеры и
внештатные сотрудники

...



732

pwned websites

12,847,430,579

pwned accounts

115,765

pastes

228,881,530

paste accounts

Largest breaches



772,904,991 [Collection #1 accounts](#)



verifications.io

763,117,241 [Verifications.io accounts](#)



711,477,622 [Onliner Spambot accounts](#)



622,161,052 [Data Enrichment Exposure From PDL Customer accounts](#)



593,427,119 [Exploit.In accounts](#)



509,458,528 [Facebook accounts](#)



457,962,538 [Anti Public Combo List accounts](#)



393,430,309 [River City Media Spam List accounts](#)

myspace

359,420,698 [MySpace accounts](#)



268,765,495 [Wattpad accounts](#)

Recently added breaches



23,209,732 [RailYatri accounts](#)



4,774,445 [SoarGames accounts](#)



4,999,001 [Go Ninja accounts](#)



5,412,603 [Estante Virtual accounts](#)



143,711 [Bleach Anime Forum accounts](#)



12,629,245 [IndiHome accounts](#)



434,784 [Jam Tangan accounts](#)



98,726 [KitchenPal accounts](#)



7,071,293 [OMGPOP accounts](#)



14,055,729 [Acuity accounts](#)

;-hibp?



Cyber Security

Key Trends

- Attacks Against Cloud Services
- Rise in IoT Devices
- Integration of AI and Machine Learning
- Zero Trust Cyber Security
- Multi-factor Authentication
- Continuously Evolving Ransomware
- Rise in Insider Threats
- Explosion of BYOD and Mobile Devices
- Growing IT Skills Gap
- Increasing Threat of Deepfakes
- International State-sponsored Warfare
- Organizational Behavior
- Connected Cars
- User Awareness
- Attacks on the Health Care Sector

The number of IoT devices is estimated to increase by 18% in 2023 and reach 27 million by 2025.

Source: IoT Analytics

The multi-factor authentication market is expected to reach \$26.7 billion by 2025 with a CAGR of 15%.

Source: MarketsandMarkets

The number of unfilled cybersecurity job openings is expected to be at 3.5 million in 2025.

Source: Cybersecurity Ventures

The global connected cars market size is estimated to reach \$191.83 billion by 2028.

Source: Fortune Business Insights

The post-pandemic cybersecurity market is expected to reach \$51.6 billion by 2026.



Source: MarketsandMarkets

The cost of a data breach, the cost of implementation of insider threat programs, had increased 38% since 2016.

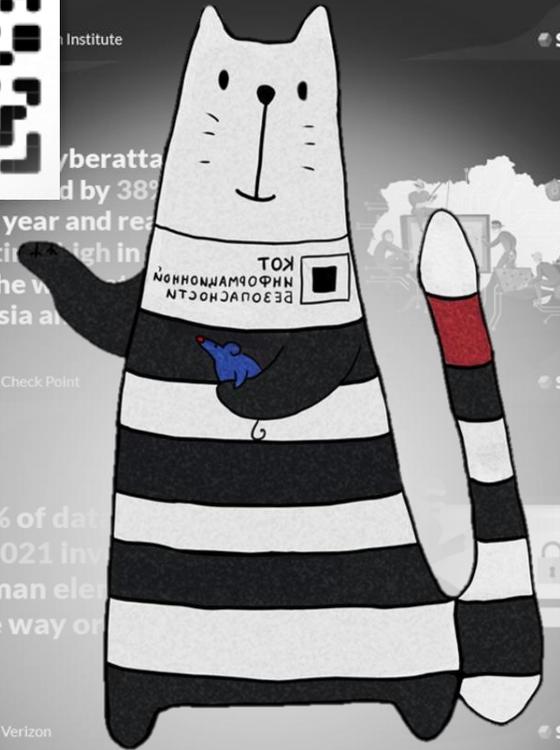
Source: Ponemon Institute

The number of cyberattacks in Russia last year and reached an all-time high in 2022, to the value of \$1.2 billion.

Source: Check Point

82% of data breaches in 2021 involved human element, one way or another.

Source: Verizon



Select-Hub

Select-Hub

Select-Hub

Select-Hub

Software Supply Chain Attacks

Data Breaches

IOT

Advanced Persistent Threats



Cloud Security & Privacy

Emotet

Password Attacks

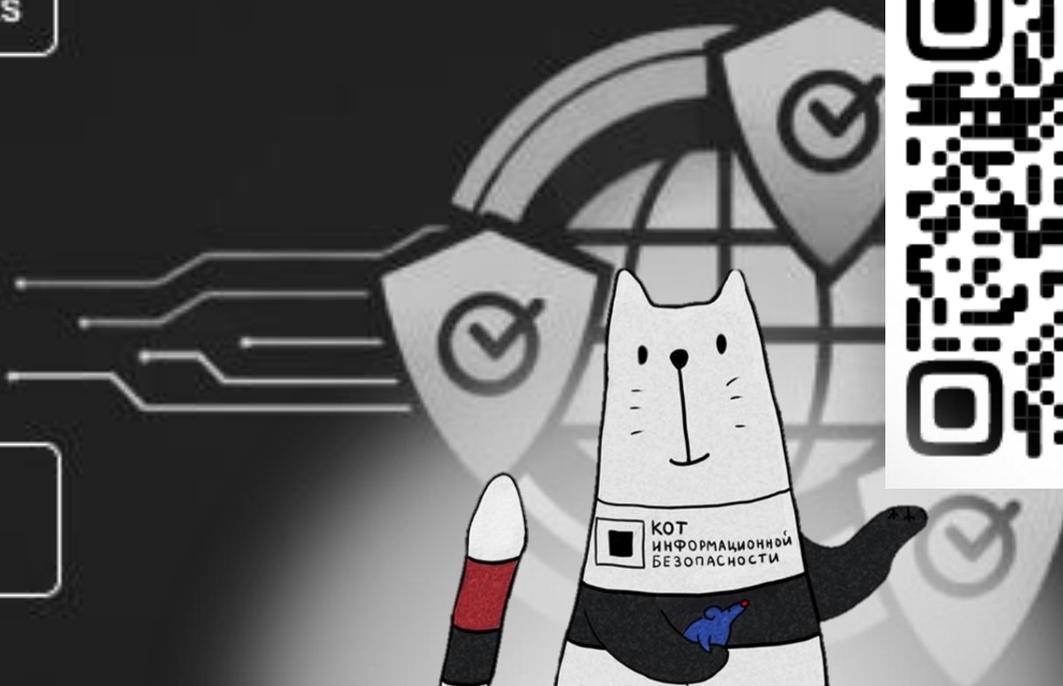
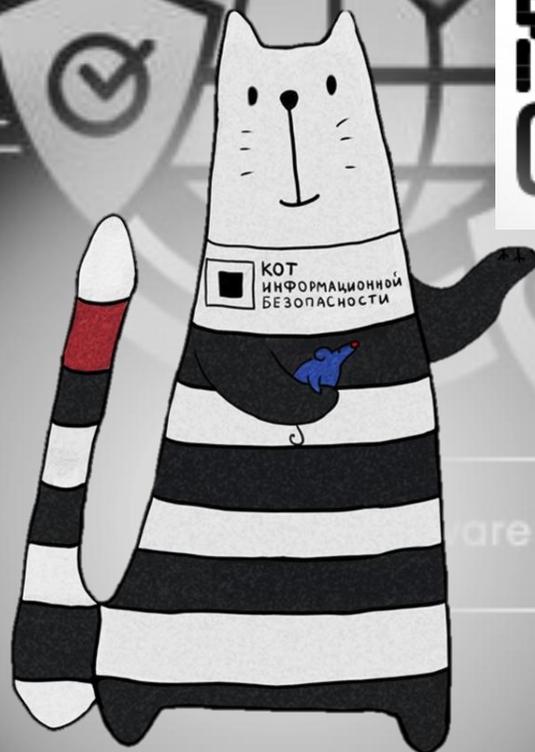
Multi-Layer Security

Cloud Security Threats

Phishing

ware

Malware



Какие три угрозы безопасности данных в Вашей организации/отрасли Вы считаете наиболее актуальными и критичными, почему?



ТОП-3 внутренних угроз ИБ Q4.2023

1

ПРЕВЫШЕНИЕ
ПОЛНОМОЧИЙ

2

СГОВОР С
ИНСАЙДЕРОМ

3

«СЛУЧАЙНЫЕ»
УТЕЧКИ

Изменения в законодательстве

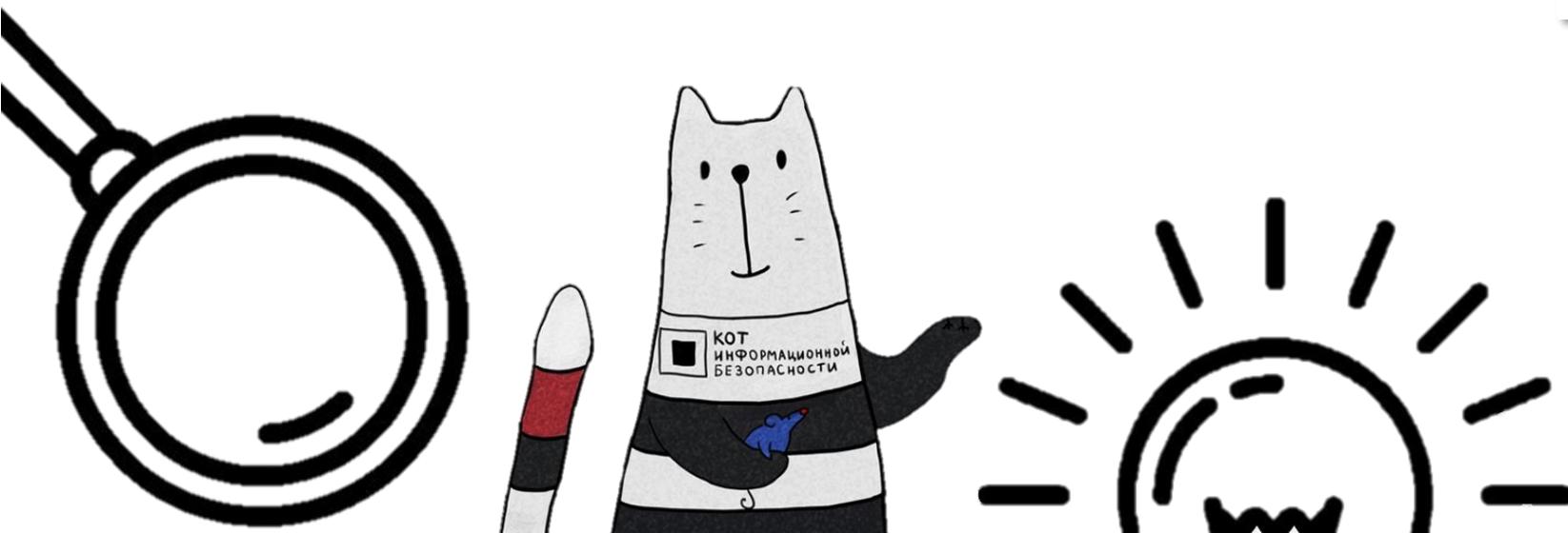


Изменения с 1 января 2023 года

- изменения правил категорирования объектов КИИ (127-П)
- планы по импотозамещению СЗИ у субъектов КИИ (Указ № 250)
- ...



НАПРИМЕР

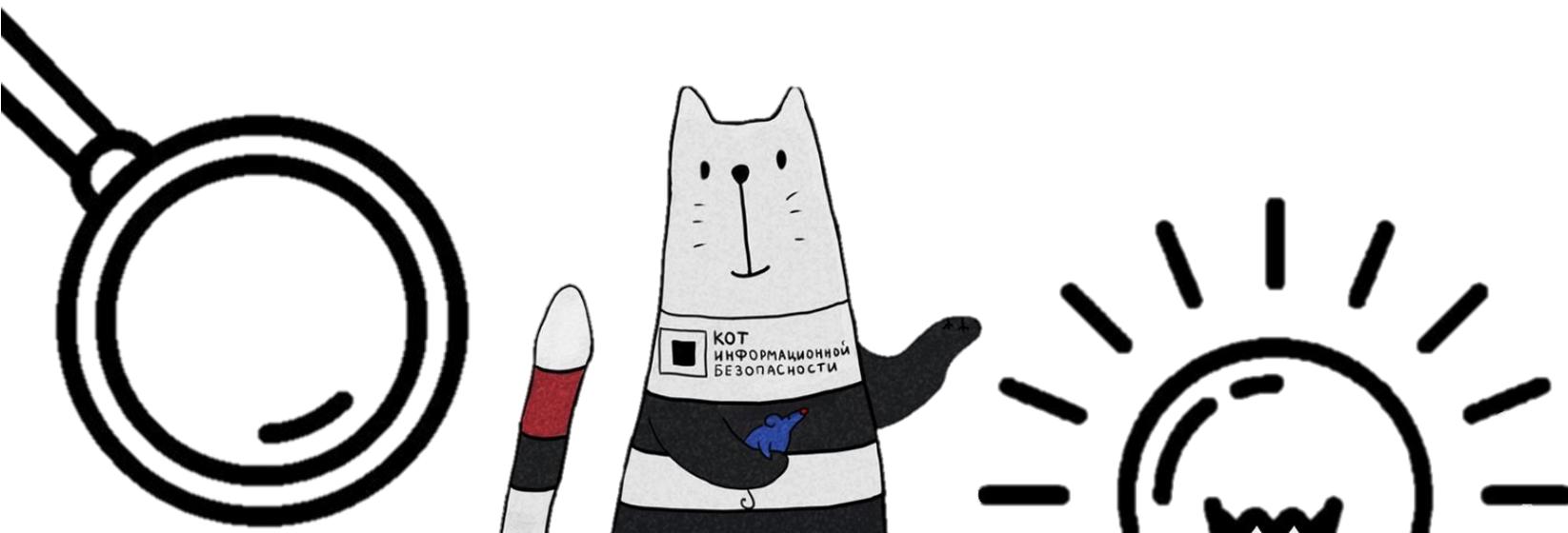


Изменения с 1 марта 2023 года

- оценка степени вреда: новый порядок
- четкие правила уничтожения ПДн
- трансграничная передача ПДн
- новые правила проверок РКН
- ...



ИЛИ



Как изменения в законодательстве РФ 2022-2023 годов в области защиты данных повлияли на планы развития Вашей компании/направления?



На работе запретили нейросети: Chat GPT, YandexGPT и другие

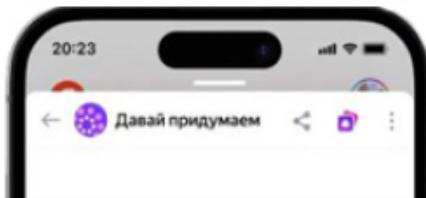
Повеселю вас новостями с моей бюджетной конторки, которая всё больше напоминает театр абсурдов. Дело в том, что на днях вышли два экстренных приказа.

★ Первый приказ цитирую: «о запрете использования на рабочих местах устройств фирмы Apple». Имеется ввиду запрет абсолютно всех устройств бренда Apple. Запрещён даже пронос на территорию организации подобных устройств. [За первое же нарушение могут сходу уволить]. Но этот запрет назревал, и мы понимаем откуда «ноги растут».

★ Второй приказ ещё интереснее: «на рабочих местах исключить технически доступ ко всем нейросетям, и ресурсам, ассоциированным с ними». Это очень интересный приказ) Безопасникам пока пришлось попросту отключить интернет в организации, чтобы его выполнить.

Потому что во-первых GPT — ресурсов, а так же «ассоциированных с ними» в интернете миллионы, и как их запретить все и сразу — вопрос. А что касается таких как «Алиса — GPT», ну, т.е. YandexGPT, то пока у безопасников нет понимания как его запретить, не порезав сам yandex.ru

YandexGPT IS CENSORED !



**Практика
защиты данных**



ЦБ с 25 декабря запретит сотрудникам пользоваться Apple на работе

Центробанк с 25 декабря запретит использование техники Apple в служебных целях



**Практика
защиты данных**



В Госдуму внесли законопроект об ужесточении наказания за утечки данных

В Госдуму внесли поправки о штрафах до ₽500 млн и сроках за утечки данных

В Госдуму внесли пакет поправок, предусматривающих ужесточение ответственности за утечки персональных данных. В финальную версию не вошел «смягчающий» механизм компенсационных выплат пострадавшим, на котором настаивало Минцифры



Практика
защиты данных

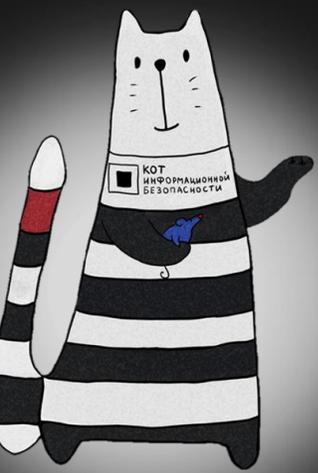


На какие три инновационных подхода или метода по защите данных Вы рекомендуете обратить внимание коллегам в 2024 году?



ПЛЕШКОВ АЛЕКСЕЙ КОНСТАНТИНОВИЧ

НЕЗАВИСИМЫЙ ЭКСПЕРТ ПО
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



“

БЕЗОПАСНОСТИ МНОГО НЕ БЫВАЕТ

