КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИТОГИ

КОД ИБ ИТОГИ | 08 ДЕКАБРЯ 2022

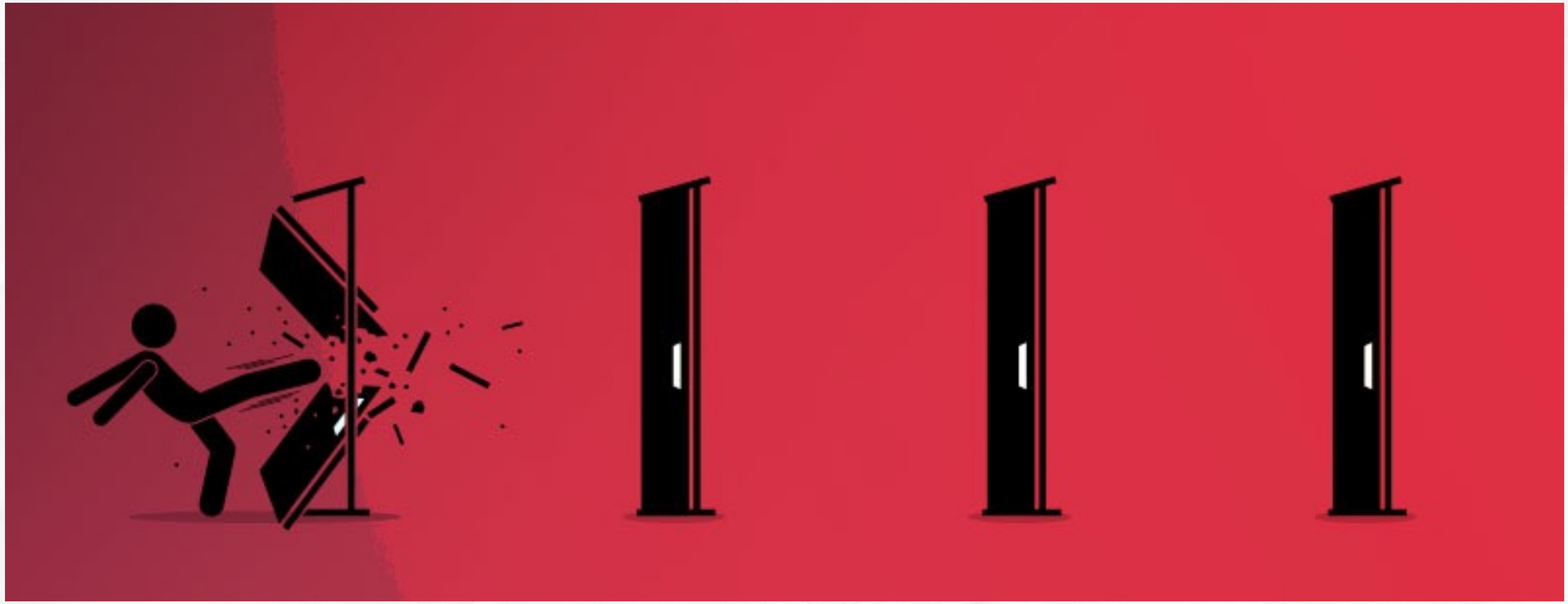
ИЗМЕНЕНИЯ ЛАНДШАФТА УГРОЗ: РОССИЯ В РЕЖИМЕ RED TEAM

ЛУКА САФОНОВ, КИБЕРПОЛИГОН

МОСКВА

Red Team тестирование более радикально, чем обычный пентест. В этом и состоит его ключевая особенность.Широкий набор методов воздействия на систему включает:

- Компрометацию внешнего периметра
- Приемы социальной инженерии
- Атаки на беспроводные сети
- Физический доступ к объектам инфраструктуры
- Закрепление в скомпрометированных системах




Zerg Rush!

DDoS: panic

Мінцифра

💥**Цифровий наступ від ІТ-армії: понад 900 паралізованих онлайн-ресурсів протягом листопада**

Наші воїни продовжують звільняти Україну від окупантів, а ІТ-армія — розхитувати економіку ворога та деморалізувати росіян на цифровому фронті.

За останній місяць ІТ-армія призупинила роботу купи російських сайтів та онлайн-ресурсів. Серед них:

1️⃣ **Воєнторги та магазини дронів і радіоприладів**
ІТ-армія зробила серію DDoS-атак на профільні магазини, щоб свіжомобілізовані росіяни через керівництво чи волонтерів не могли придбати якісне спорядження.

2️⃣ **Центральний банк рф**
Зробили відомими персонал банку, спеціалізовані системи та вихідні файли. Наші кібербійці опублікували також інформацію про банківські операції мо рф, персональні дані військовослужбовців рф, номери телефонів, рахунків і банківських карток.

3️⃣ **Платформа пропутінських волонтерів Добро**
Зламано та опубліковано дані 650 тисяч учасників платформи Добро, де під гаслом #МыВместе збирали мітинги на підтримку війни.

4️⃣ **Альфа Банк**
Серія DDoS-атак призвела до сотень обурених відгуків клієнтів банку та більшої недовіри до російської банківської системи загалом. А що трапилось, росіяни? 🙃

5️⃣ **Ozon**
У День шопінгу айтівці створили штучний попит на товари, що призвело до помилок у покупців на платформі. Менше покупок — менше податків в економіку рф.

6️⃣ **Термінове оновлення 1С**
1С випустило термінове оновлення, де виправлялася помилка із закладкою проти піратства. росіяни активно намагалися його завантажити, але все без шансів. Система була перевантажена, а підприємства не могли повернутися до роботи. Ось такі позаплановані вихідні і ризик втратити дані.

7️⃣ **День Гідності та Свободи**
ІТ-армія оригінально привітала українців на 60 російських ресурсах, серед яких сайти міністерств, служб та управлінь.

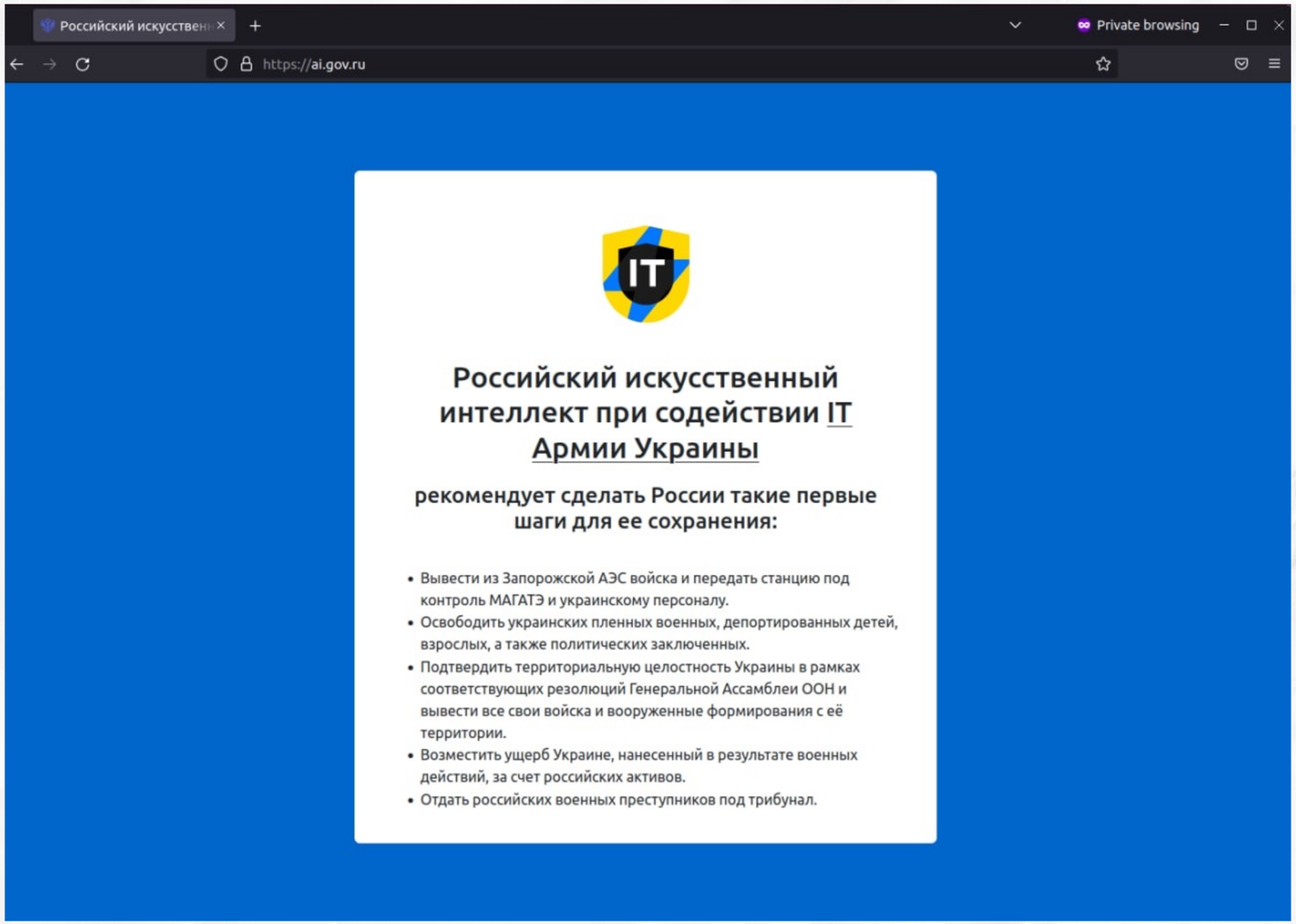
IT ARMY of Ukraine

Ви попрацювали на славу!💪
Росіяни відчули сьогодні регулярні перебої в роботі сервісів онлайн телебачення. Продовжуємо тематику вихідного дня, наступна ціль — сервіси замовлення їжі онлайн.
Дякуємо всім за крутий результат!

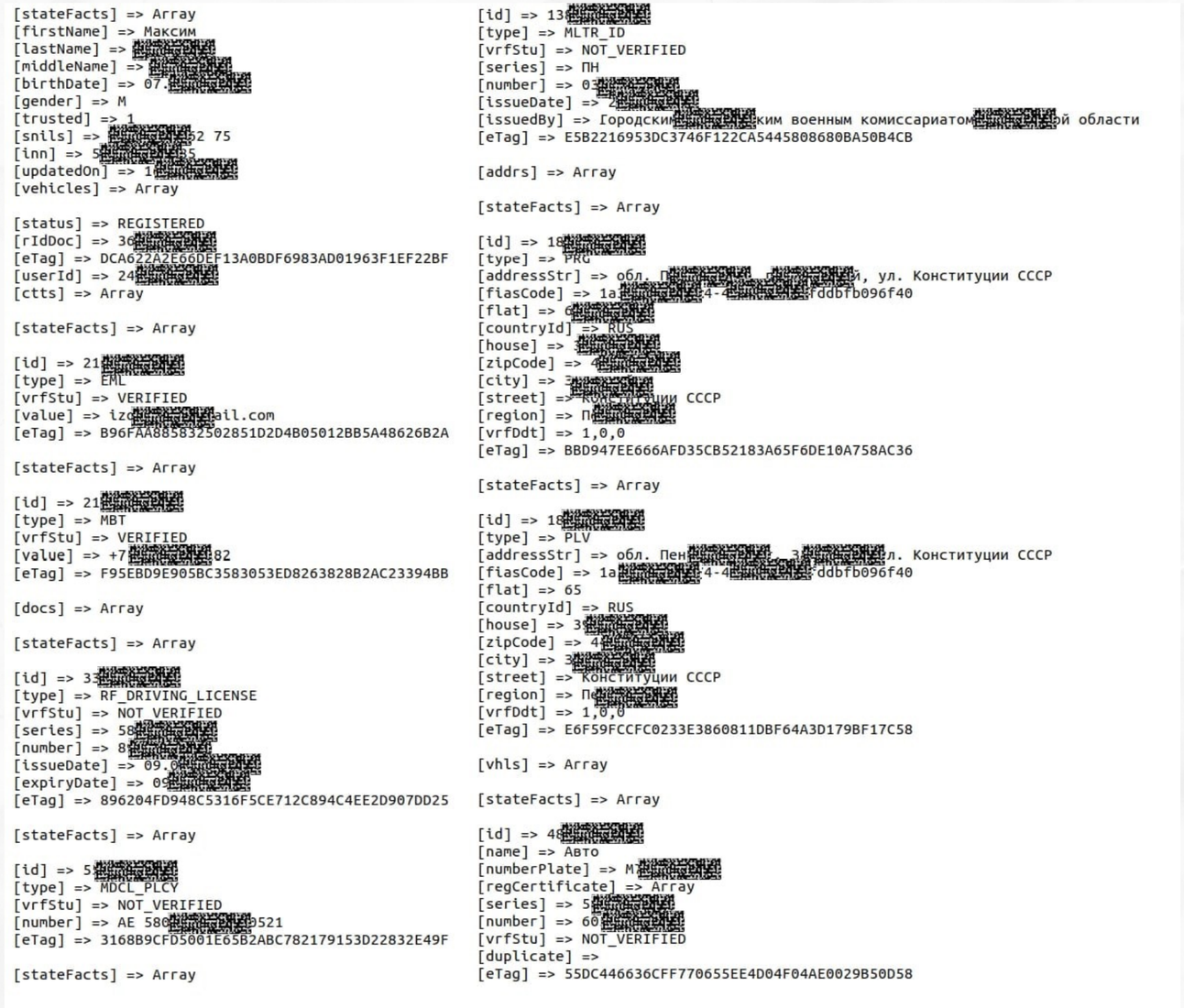
Great job today!💪
Russians have noticed regular hitches in the work of TV streaming services today. We'll stick to our 'weekend theme'. Our next target is online food delivery services.
Thanks again for the stellar results!

https://vkusvill.ru/
178.248.232.221 (80/tcp, 443/tcp)
https://av.ru/
46.235.185.176 (80/tcp, 443/tcp)
212.193.157.110 (80/tcp, 443/tcp)
46.235.189.110 (80/tcp, 443/tcp)
37.220.163.2 (80/tcp, 443/tcp)
https://www.okeydostavka.ru/msk
178.248.237.112 (80/tcp, 443/tcp)
https://www.delivery-club.ru/moscow
5.61.236.234 (80/tcp, 443/tcp)
https://samokat.ru/
46.235.188.221 (80/tcp, 443/tcp)
46.235.186.103 (80/tcp, 443/tcp)
212.193.155.174 (80/tcp, 443/tcp)
46.235.191.53 (80/tcp, 443/tcp)
37.220.160.159 (80/tcp, 443/tcp)
93.93.88.47 (80/tcp, 443/tcp)
78.41.111.106 (80/tcp, 443/tcp)
37.220.162.180 (80/tcp, 443/tcp)
212.193.152.42 (80/tcp, 443/tcp)
https://www.utkonos.ru/
178.248.234.39 (80/tcp, 443/tcp)

Deface: propaganda

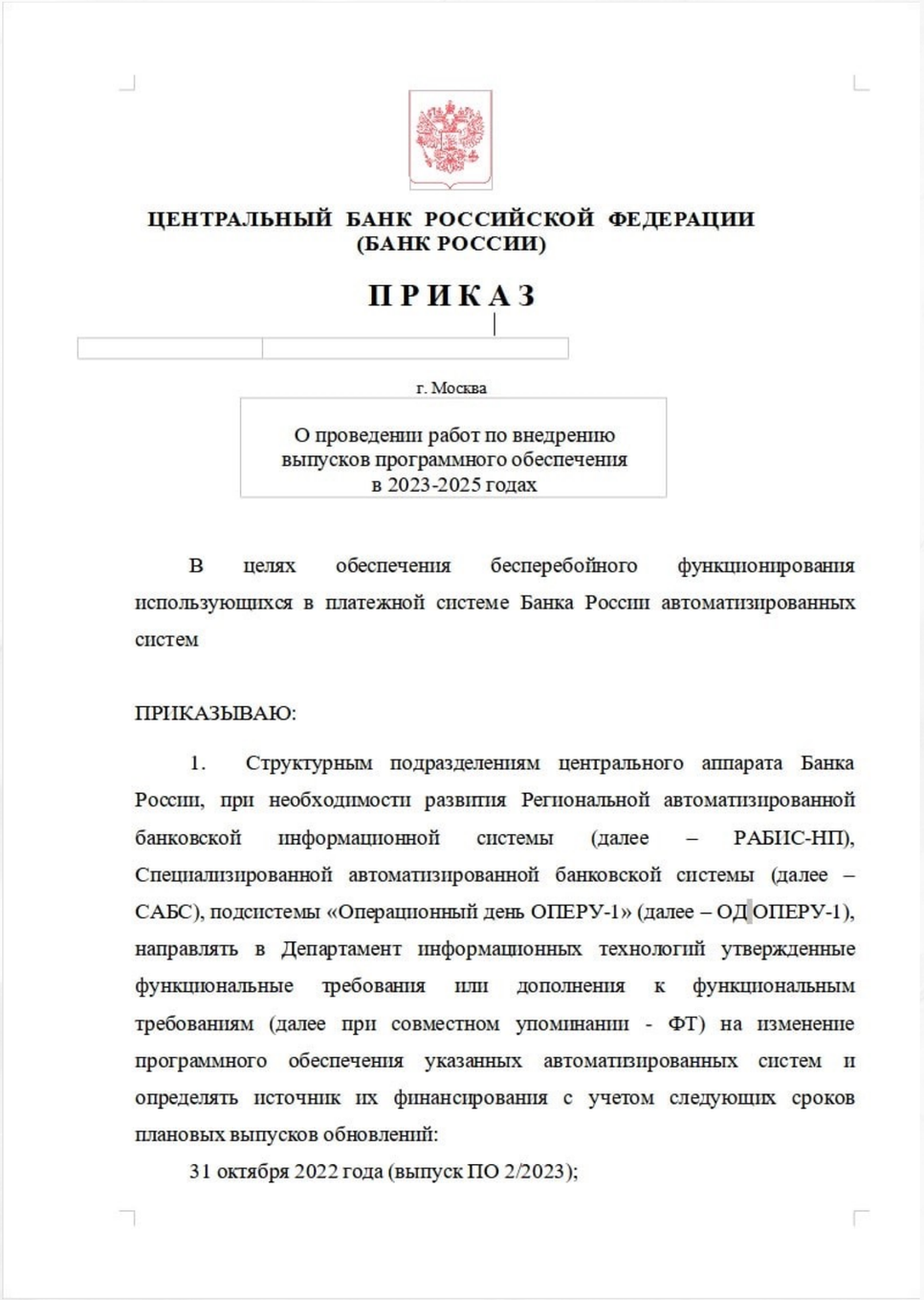


Credential stuffing: chaos



```
[stateFacts] => Array
[firstName] => Максим
[lastName] => [redacted]
[middleName] => [redacted]
[birthDate] => 07.[redacted]
[gender] => M
[trusted] => 1
[snils] => [redacted]52 75
[inn] => 5[redacted]5
[updatedOn] => 1[redacted]
[vehicles] => Array

[status] => REGISTERED
[rIdDoc] => 36[redacted]
[eTag] => DCA622A2E66DEF13A0BDF6983AD01963F1EF22BF
[userId] => 24[redacted]
[ctts] => Array

[stateFacts] => Array

[id] => 21[redacted]
[type] => EML
[vrfStu] => VERIFIED
[value] => izo[redacted]ail.com
[eTag] => B96FAA885832502851D2D4B05012BB5A48626B2A

[stateFacts] => Array

[id] => 21[redacted]
[type] => MBT
[vrfStu] => VERIFIED
[value] => +7[redacted]82
[eTag] => F95EBD9E905BC3583053ED8263828B2AC23394BB

[docs] => Array

[stateFacts] => Array

[id] => 33[redacted]
[type] => RF_DRIVING_LICENSE
[vrfStu] => NOT_VERIFIED
[series] => 58[redacted]
[number] => 8[redacted]
[issueDate] => 09.0[redacted]
[expiryDate] => 05[redacted]
[eTag] => 896204FD948C5316F5CE712C894C4EE2D907DD25

[stateFacts] => Array

[id] => 5[redacted]
[type] => MDCL_PLCY
[vrfStu] => NOT_VERIFIED
[number] => AE 580[redacted]0521
[eTag] => 3168B9CFD5001E65B2ABC782179153D22832E49F

[stateFacts] => Array

[id] => 13[redacted]
[type] => MLTR_ID
[vrfStu] => NOT_VERIFIED
[series] => ПН
[number] => 03[redacted]
[issueDate] => 2[redacted]
[issuedBy] => Городским[redacted]ким военным комиссариатом[redacted]ой области
[eTag] => E5B2216953DC3746F122CA5445808680BA50B4CB

[addrs] => Array

[stateFacts] => Array

[id] => 18[redacted]
[type] => PRG
[addressStr] => обл. П[redacted], ул. Конституции СССР
[fiasCode] => 1a[redacted]4-4[redacted]ddbfb096f40
[flat] => 6[redacted]
[countryId] => RUS
[house] => [redacted]
[zipCode] => 4[redacted]
[city] => 3[redacted]
[street] => Конституции СССР
[region] => П[redacted]
[vrfDdt] => 1,0,0
[eTag] => BBD947EE666AFD35CB52183A65F6DE10A758AC36

[stateFacts] => Array

[id] => 18[redacted]
[type] => PLV
[addressStr] => обл. Пен[redacted], ул. Конституции СССР
[fiasCode] => 1a[redacted]4-4[redacted]ddbfb096f40
[flat] => 65
[countryId] => RUS
[house] => 3[redacted]
[zipCode] => 4[redacted]
[city] => 3[redacted]
[street] => Конституции СССР
[region] => П[redacted]
[vrfDdt] => 1,0,0
[eTag] => E6F59FCCFC0233E3860811DBF64A3D179BF17C58

[vhls] => Array

[stateFacts] => Array

[id] => 48[redacted]
[name] => Авто
[numberPlate] => М[redacted]
[regCertificate] => Array
[series] => 58[redacted]
[number] => 60[redacted]
[vrfStu] => NOT_VERIFIED
[duplicate] =>
[eTag] => 55DC446636CFF770655EE4D04F04AE0029B50D58
```

Leak: fear



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П Р И К А З

г. Москва

О проведении работ по внедрению выпусков программного обеспечения в 2023-2025 годах

В целях обеспечения бесперебойного функционирования использующихся в платежной системе Банка России автоматизированных систем

ПРИКАЗЫВАЮ:

1. Структурным подразделениям центрального аппарата Банка России, при необходимости развития Региональной автоматизированной банковской информационной системы (далее – РАБИС-НП), Специализированной автоматизированной банковской системы (далее – САБС), подсистемы «Операционный день ОПЕРУ-1» (далее – ОД ОПЕРУ-1), направлять в Департамент информационных технологий утвержденные функциональные требования или дополнения к функциональным требованиям (далее при совместном упоминании - ФТ) на изменение программного обеспечения указанных автоматизированных систем и определять источник их финансирования с учетом следующих сроков плановых выпусков обновлений:

31 октября 2022 года (выпуск ПО 2/2023);

Кого ломали?

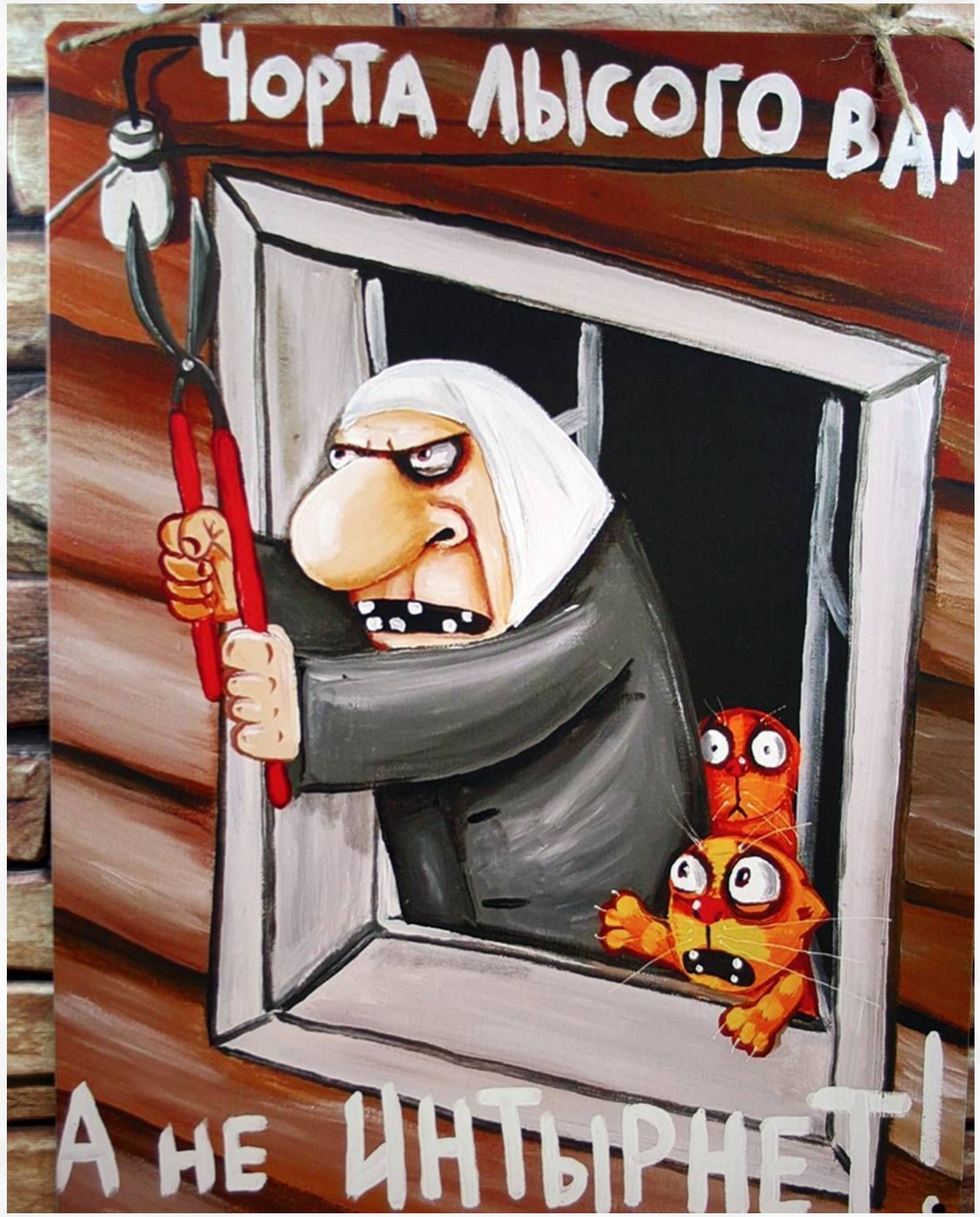
Что делать?

Что делать? Импортозамещение.

Что делать? Old but Gold: fail2ban/nftbables

Что делать? Geo IP block

```
geo $country {
default no;
include /etc/nginx/geo.conf;
127.0.0.0/24 ru;
}

if ($country ~* UA )
{
rewrite ^(.*)$ https://xn--80askzj.com.ua/;
}
```



Готов ответить
на ваши вопросы

@LukaSafonov


ХОРОШИЙ ВОПРОС
ОТВЕЧАТЬ Я НА НЕГО КОНЕЧНО ЖЕ НЕ БУДУ