ЗАДАЧИ И ФУНКЦИИ НКЦКИ В КОНТЕКТСТЕ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ, СВЯЗАННЫМ С РАСПРОСТРАНЕНИЕМ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ФИШИНГОМ

Воронкин А.Н., van@cert.gov.ru

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Задачи и функции НКЦКИ

- Координация деятельности по реагированию и выявлению инцидентов внутри страны – ГосСОПКА (ФЗ-187)

ГОССОПКА

- Компетентная организация – организация, уполномоченная определять нарушения в сети «Интернет»

РФ RU RIPN РОСНИИРОС .SU MSK IX FAITID Фонд содействия развитию технологий и инфраструктуры интернет Доменный патруль рф

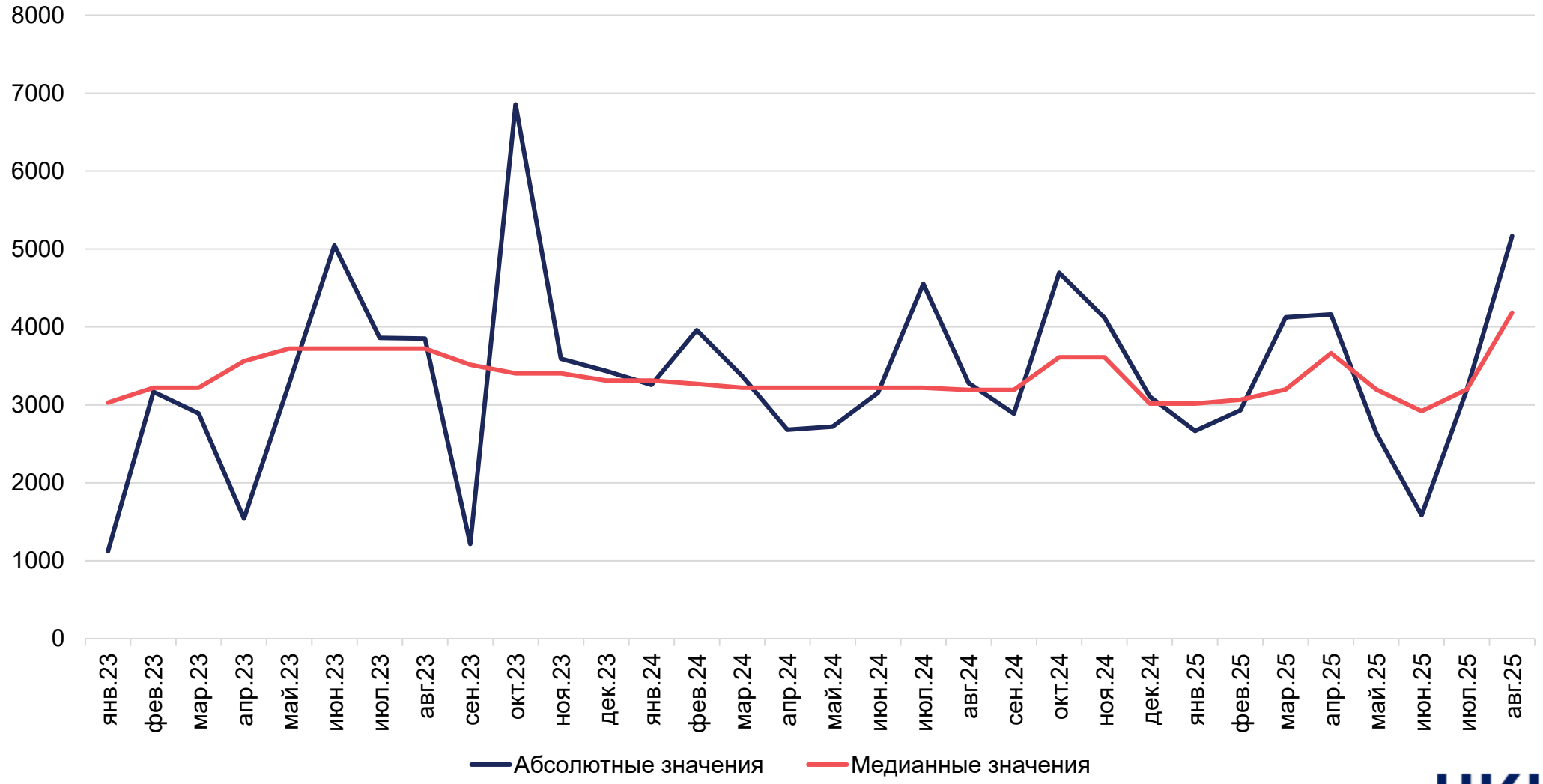
- Национальный CERT Российской Федерации –
National Computer Incident Response & Coordination Center (CERT.GOV.RU)

Статистика выявленных и заблокированных вредоносных доменных имен

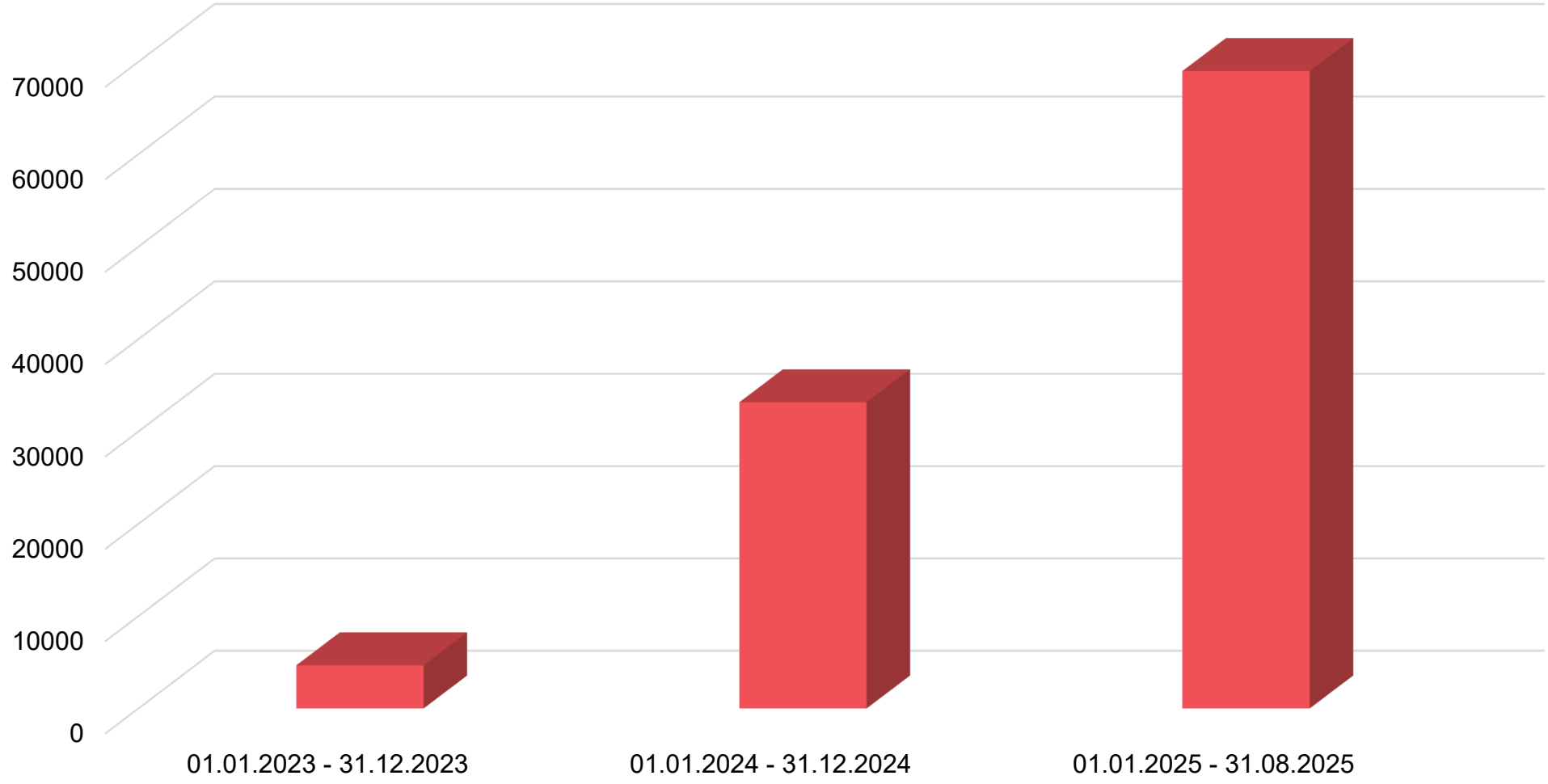
- **Стабильно высокие показатели** выявляемых и блокируемых вредоносных доменов в российских доменных зонах (**39 951** домен в 2023 году, **41 794** в 2024 году, **26 473** за период с 1 января по 31 августа 2025 года). Снижение по сравнению с аналогичным периодом прошлого года составило менее 1%, поэтому к концу года ожидаются показатели, аналогичные показателям предыдущего года.

- **Кратный рост** выявляемых и блокируемых вредоносных доменов преимущественно иностранных доменных зон (**4 673** домена в 2023 году, **33 163** в 2024 году, **68 990** за период с 1 января по 31 августа 2025 года). Рост по сравнению с аналогичным периодом прошлого года составил 369%.

Статистика снятия с делегирования доменов в российских доменных зонах за 2023 - 2025 годы



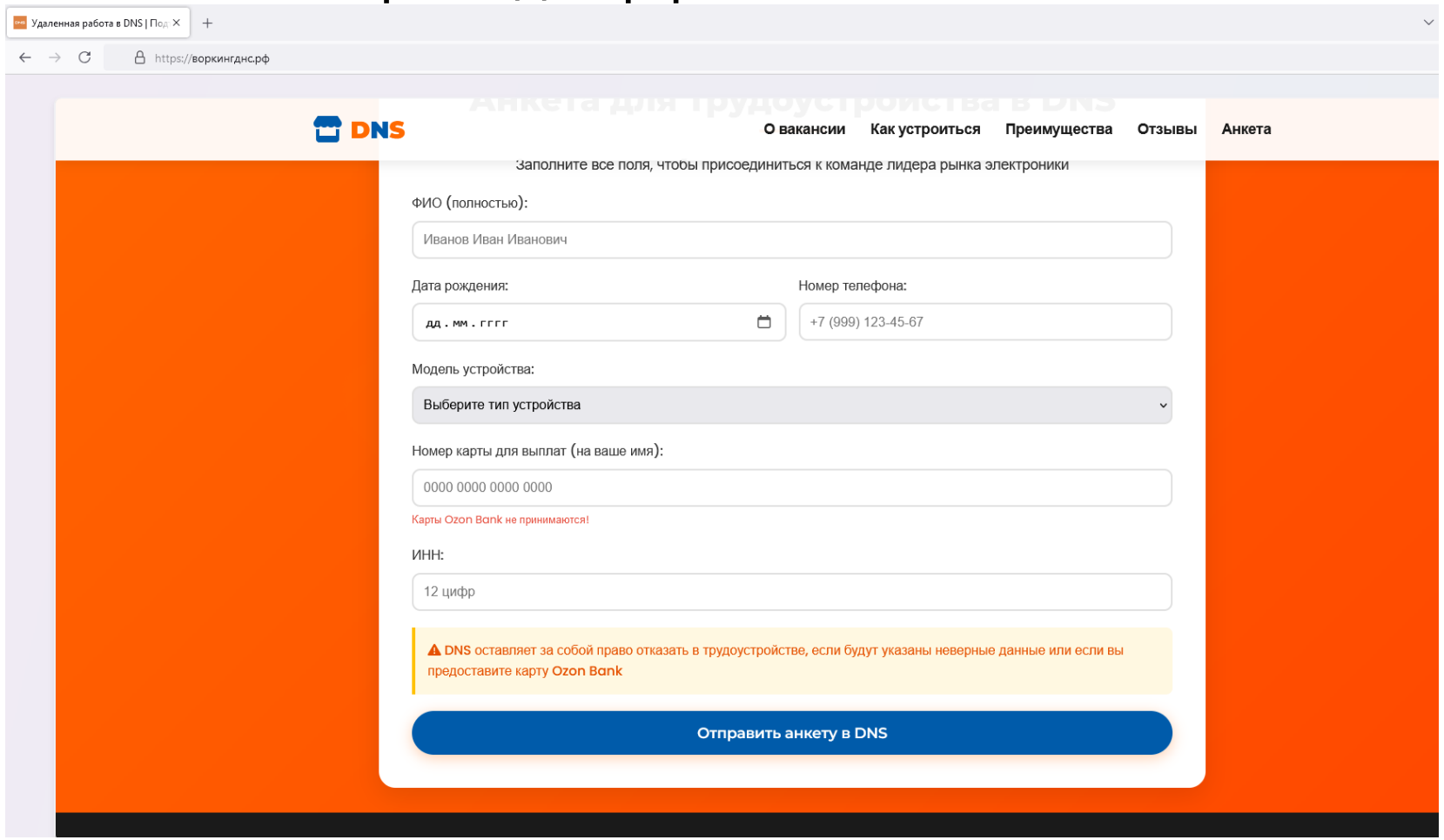
Статистика блокирования средствами ЦМУ ССОП ФГУП «ГРЧЦ»



Машинно-сгенерированные (DGA) домены

Вредоносные домены, схожие с наименованиями легитимных организаций

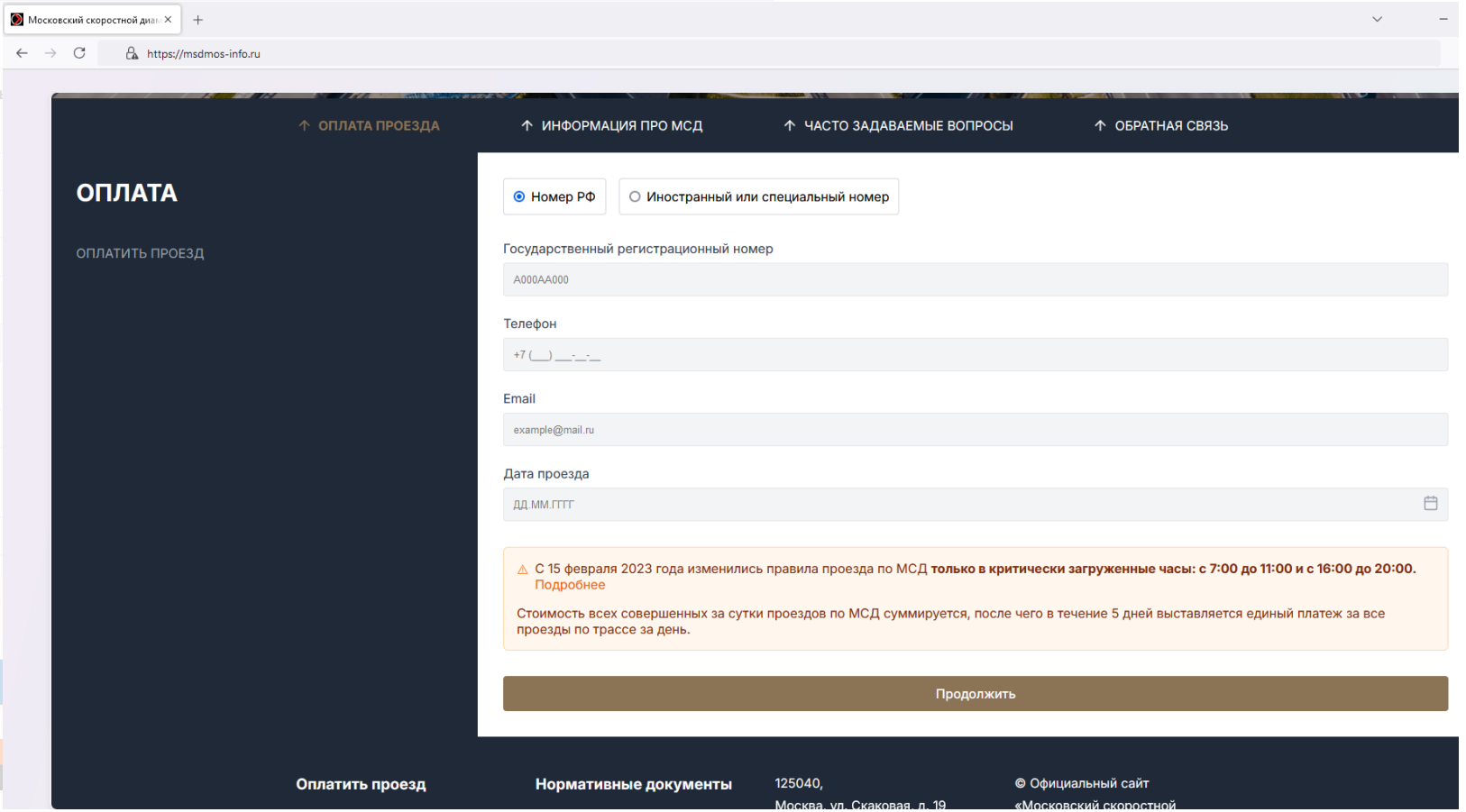
воркингднс.рф



Вредоносные домены, схожие с наименованиями легитимных организаций

воркингднс.рф

msdmos-info.ru, msdmog.ru



ГОССОПКА

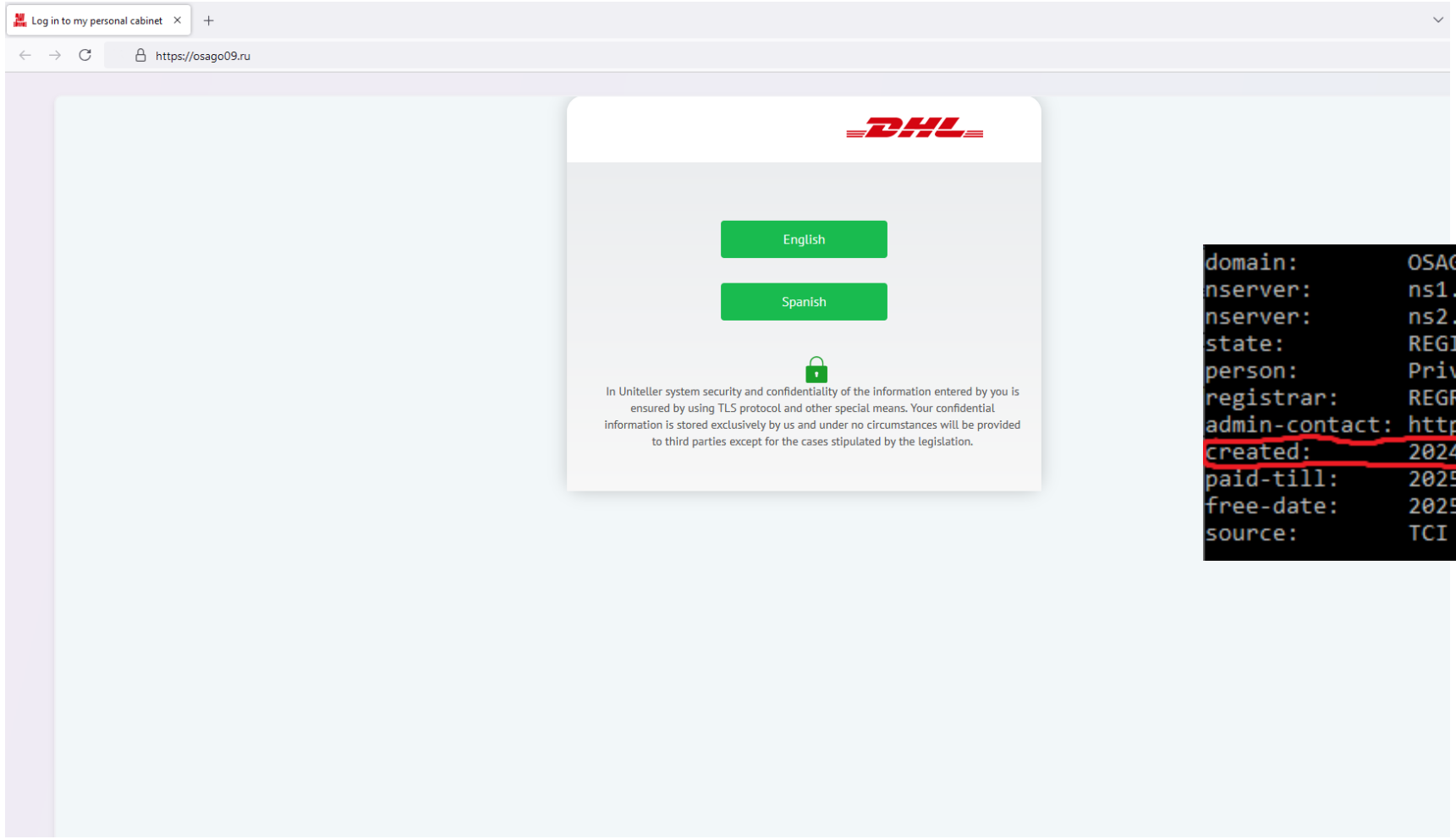
НКЦКИ

DGA из слов естественного языка (сложные DGA-домены)

items-5295.ru
items-2948.ru
items-6295.ru
items-3857.ru
items-5798.ru
objects-190438.ru
arenda-174769.ru
objects-329043.ru
arenda-189347.ru
arenda-374690.ru
arenda-894384.ru
objects-284790.ru
item83444.ru
item43843.ru
item43473.ru
item23844.ru
item38443.ru
objects-36984.ru

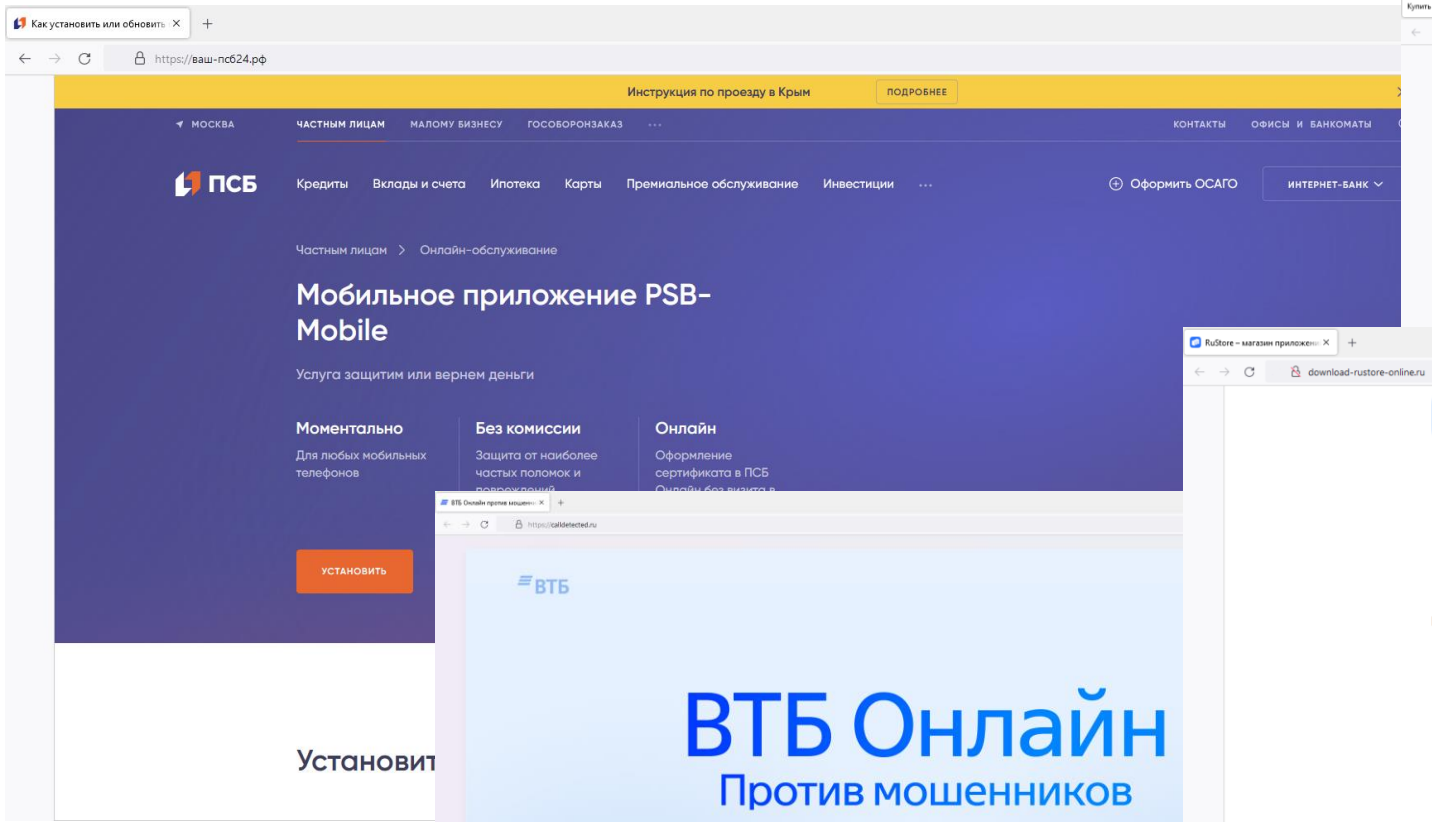
force-poll.ru
personality-force.ru
rating-force.ru
force-action.ru
leader-force.ru
uniting-force.ru
force-leader.ru
force-uniting.ru
smarts-paying.ru
smarts-payments.ru
smartspayment.ru
smarts-payer.ru
restfulpays.ru
performance-stage.ru
restfulpayings.ru
restful-paying.ru
org-verif.ru
orgverif.ru

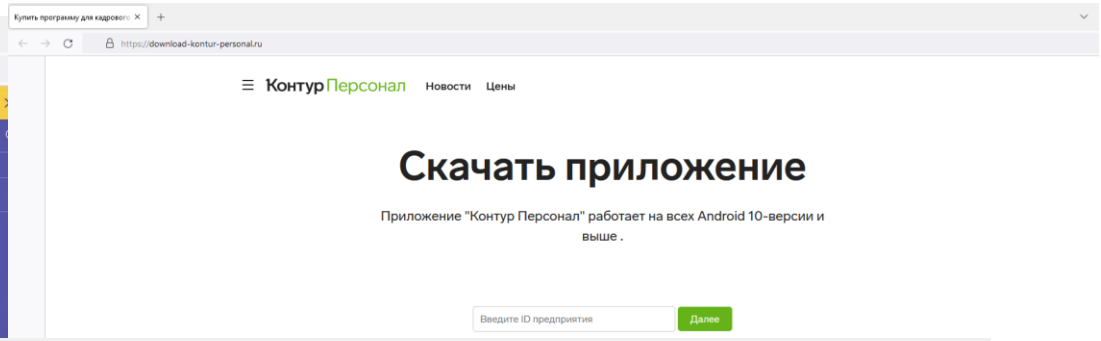
Использование злоумышленниками «старых» доменов

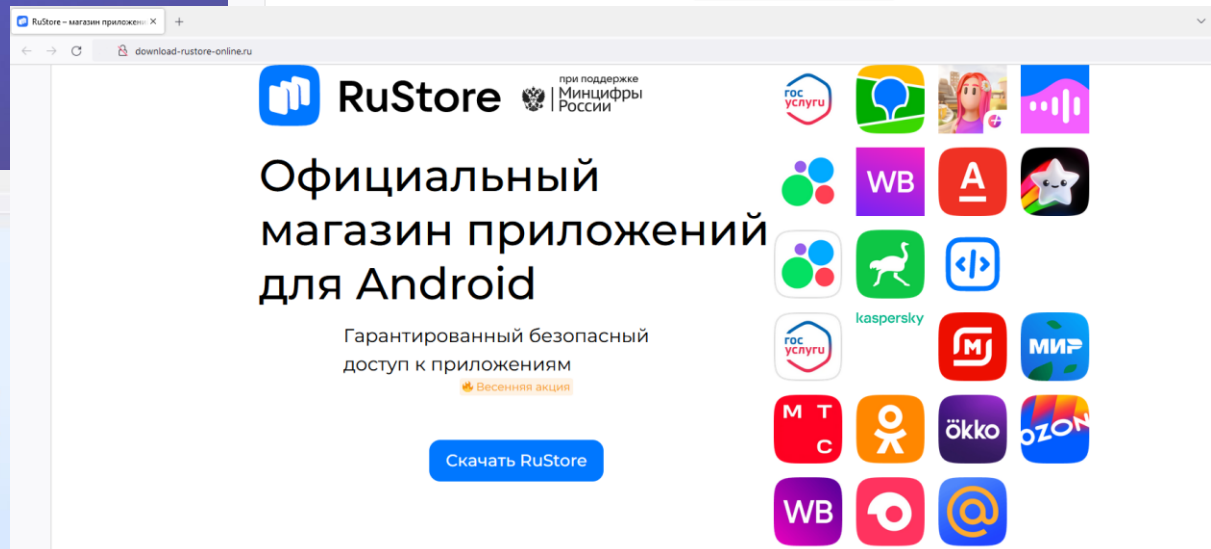



```
domain:         OSAGO09.RU
nserver:        ns1.hosting.reg.ru.
nserver:        ns2.hosting.reg.ru.
state:          REGISTERED, NOT DELEGATED, UNVERIFIED
person:         Private Person
registrar:      REGRU-RU
admin-contact:  http://www.reg.ru/whois/admin_contact
created:        2024-09-17T16:55:11Z
paid-till:      2025-09-17T16:55:11Z
free-date:      2025-10-18
source:         TCI
```

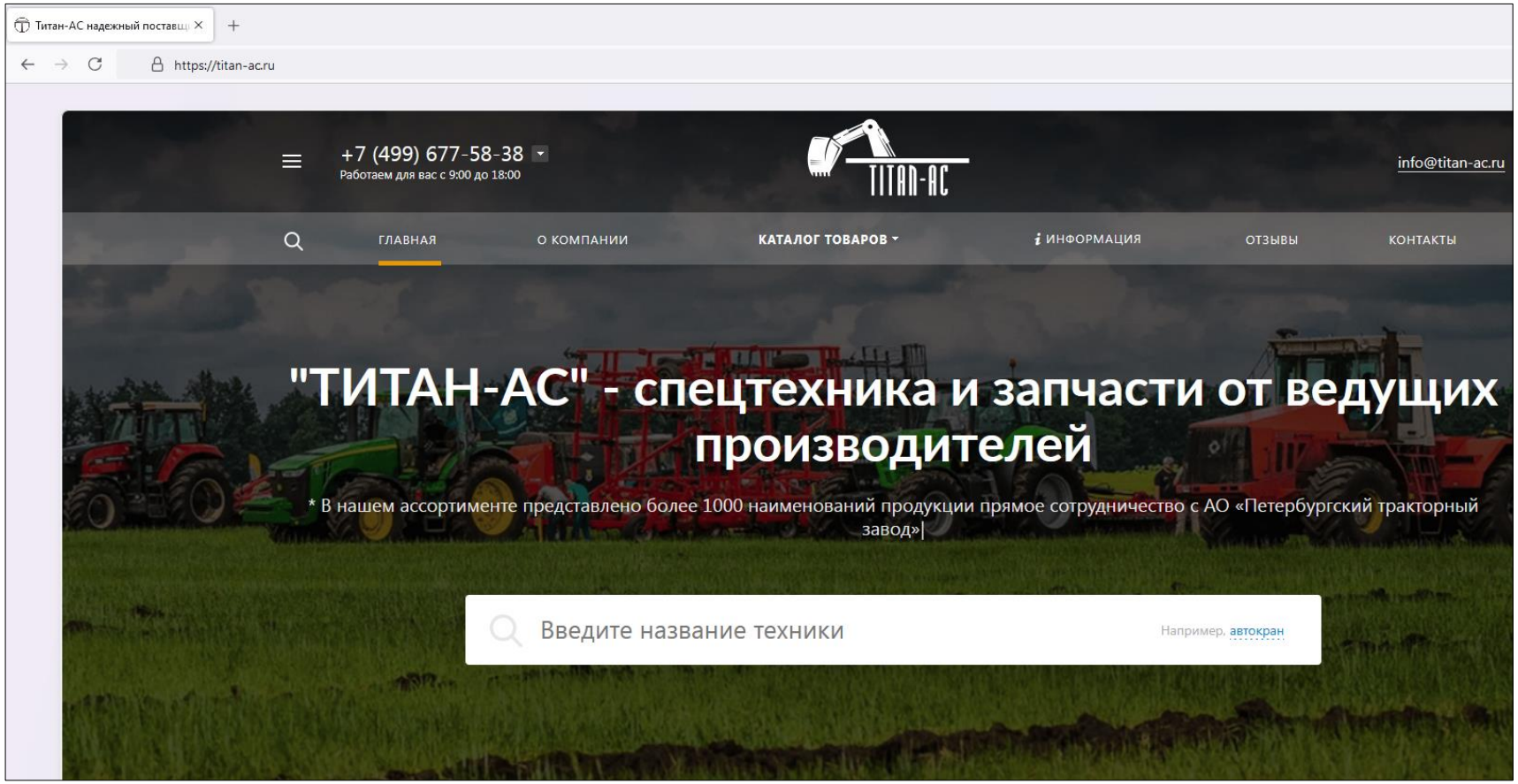
Доставка ВПО с использованием фишинговых сайтов



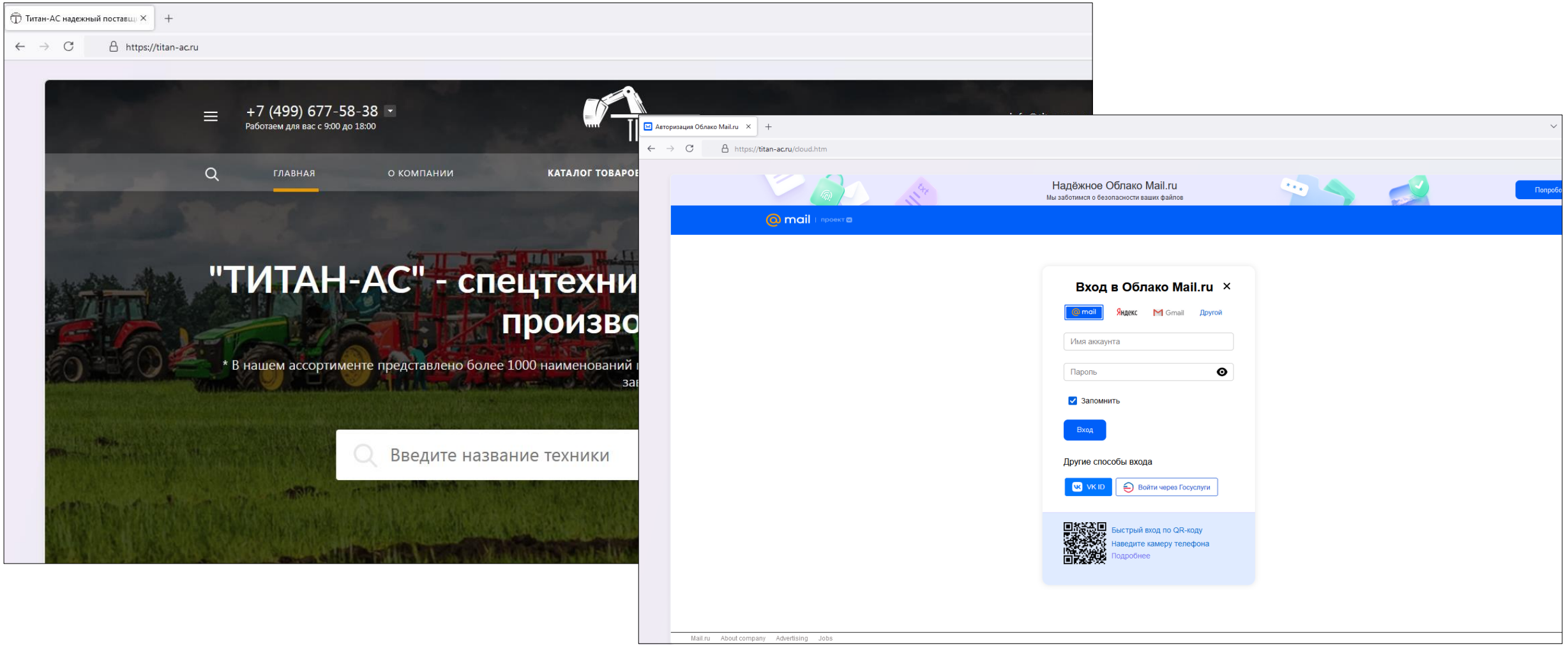




Использование уязвимостей CMS для компрометации ресурса



Использование уязвимостей CMS для компрометации ресурса



ГОССОПКА

НКЦКИ

Некорректная настройка DNS-зоны домена

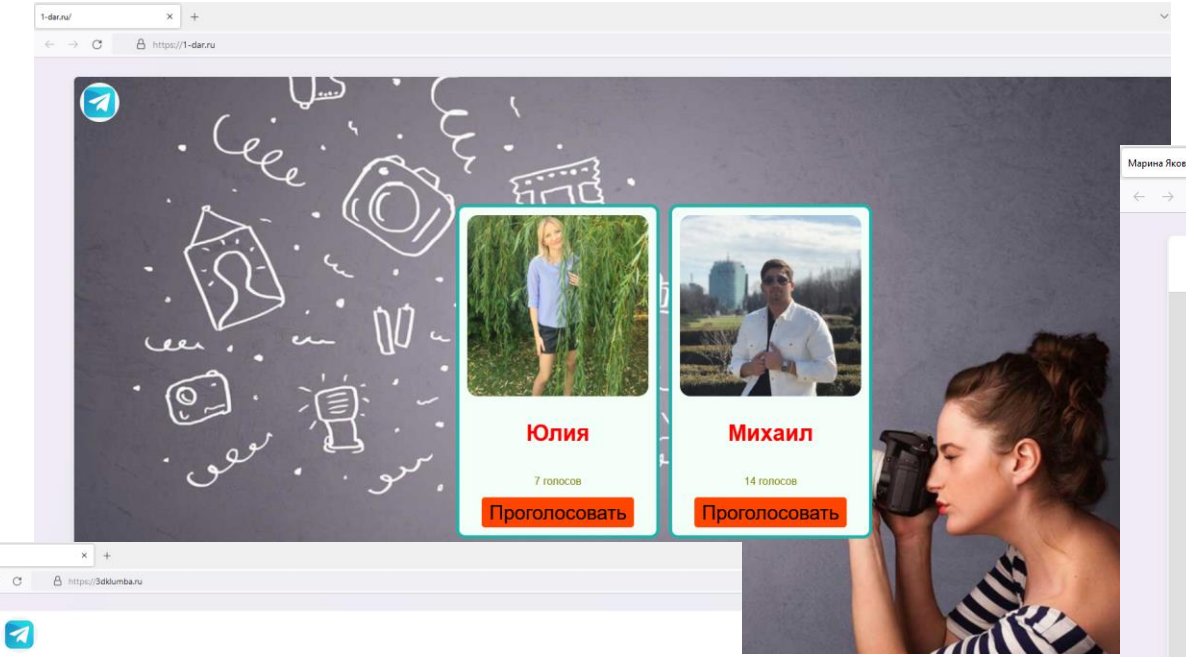
1) Регистрация «легитимного» домена.

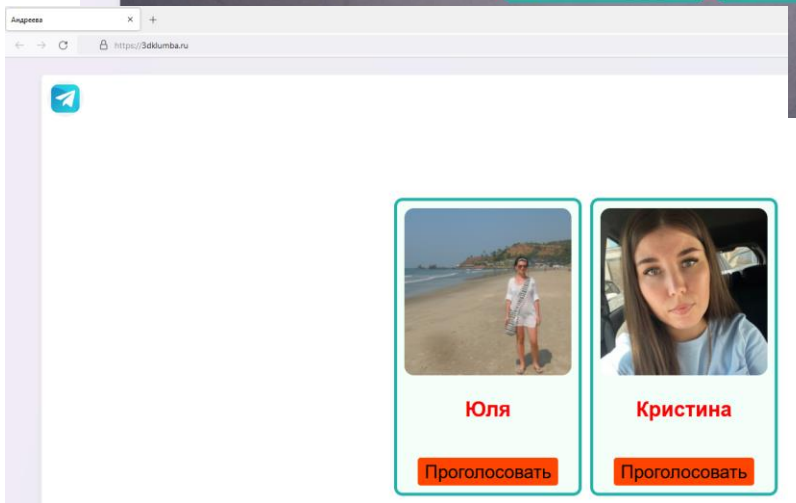
2) Делегирование домена на сторонние name-сервера провайдера хостинга.

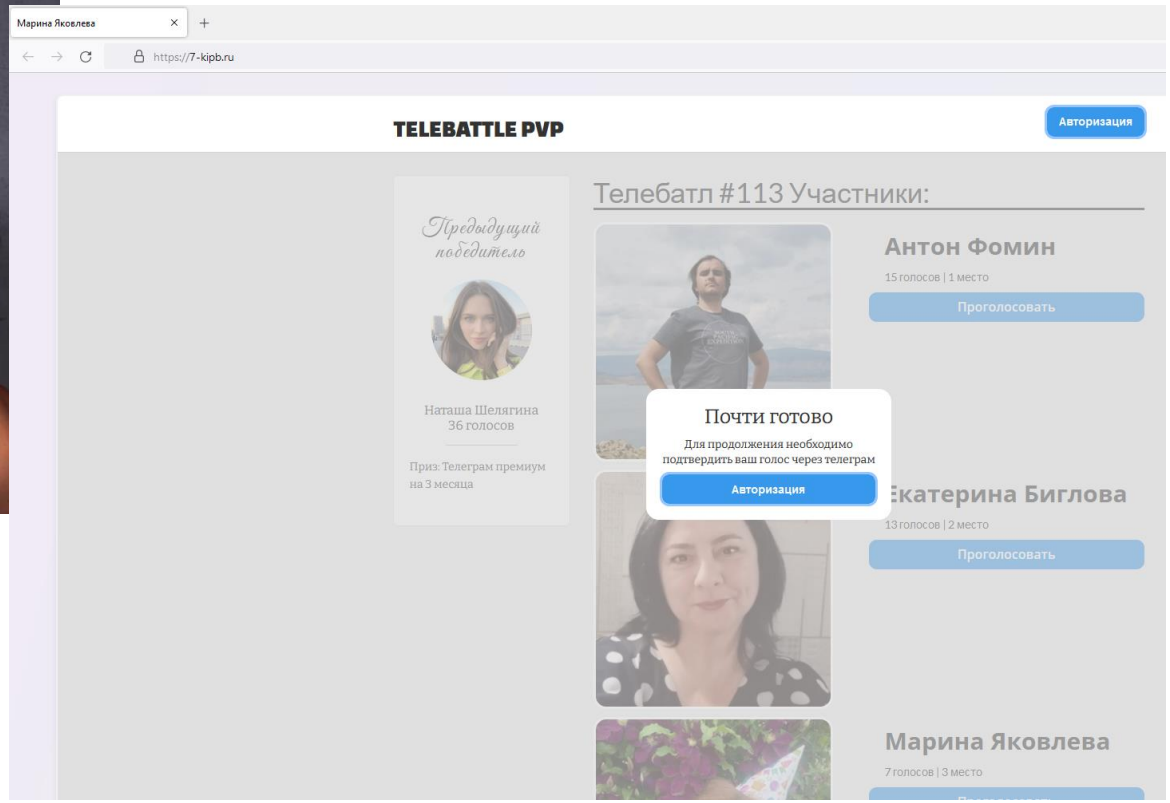
3) Отсутствие настроек DNS на стороне провайдера хостинга (отсутствие A, MX и других типов записей).

4) Действия злоумышленника по выявлению доменов с отсутствующей DNS-зоной у name-сервера и его делегирование на вредоносный ресурс (например, прописать A-запись).

Некорректная настройка DNS-зоны домена



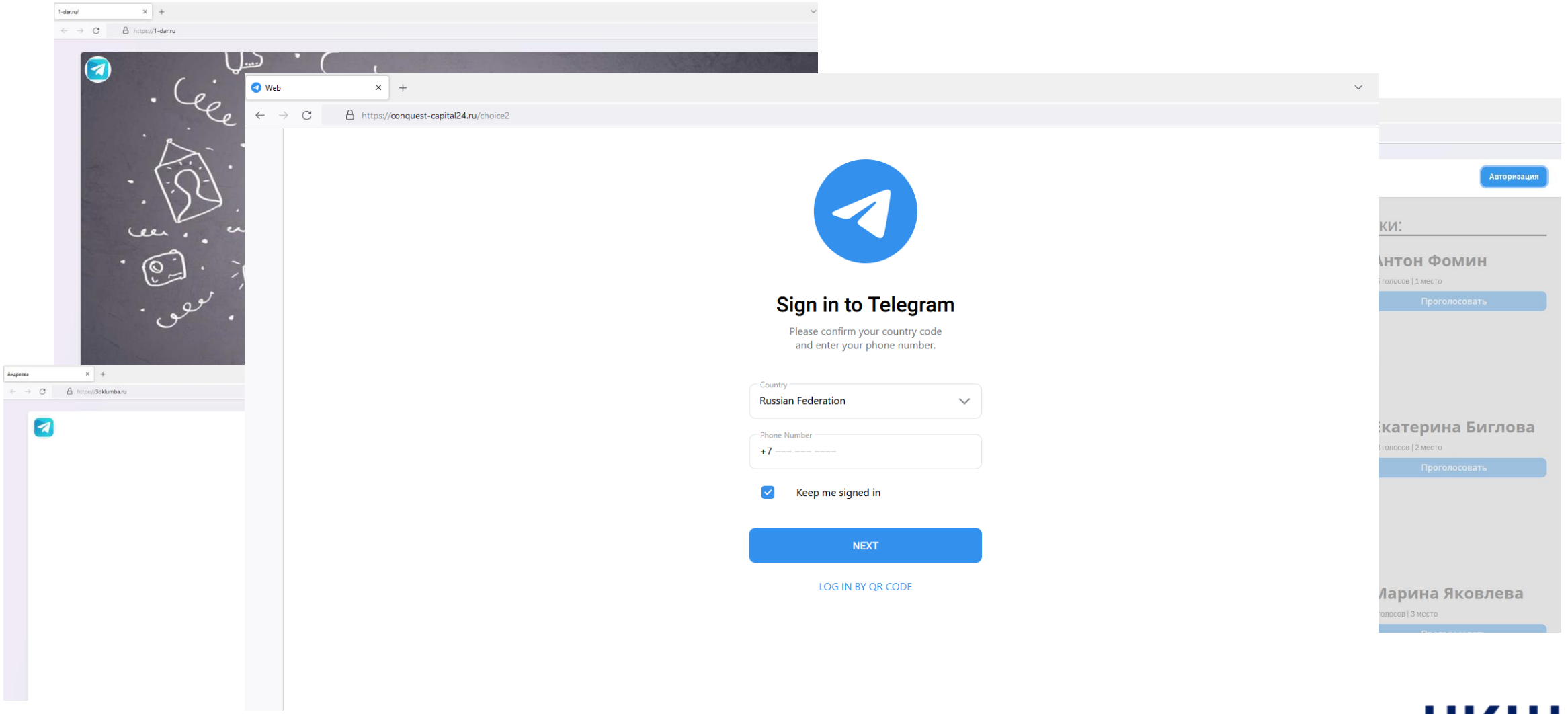




ГОССОПКА

НКЦКИ

Некорректная настройка DNS-зоны домена



Методы по защите от взлома ресурса и «угона» домена

1) Использование актуальной версии CMS и налаженный процесс ее обновления (бюллетени НКЦКИ).

2) Использование двухфакторной аутентификации для доступа в личный кабинет на сайте регистратора.

3) Корректная настройка DNS-зоны для домена (всегда прописывать DNS-зону на стороне провайдера хостинга).

4) Вовлечение большего числа участников как среди регистраторов и компетентных организаций, так и среди владельцев информационных ресурсов в ГосСОПКА.

Спасибо за внимание!

van@cert.gov.ru

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ