

ЗАДАЧИ И ФУНКЦИИ НКЦКИ В КОНТЕКСТЕ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ, СВЯЗАННЫМ С РАСПРОСТРАНЕНИЕМ ВРЕДНОСНОГО 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»



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



ГОССОПКА

НКЦКИ

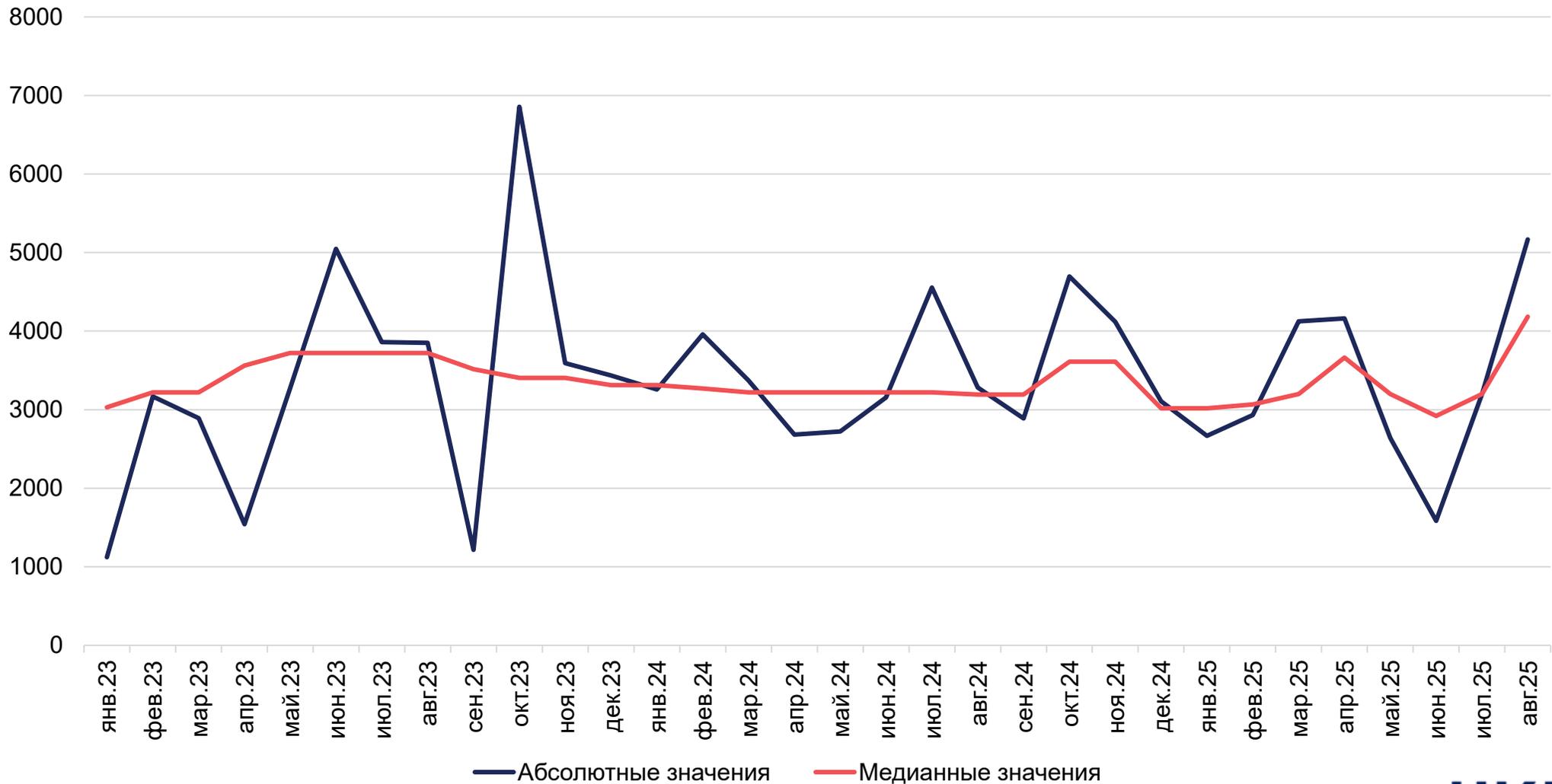
Статистика выявленных и заблокированных вредоносных доменных имен



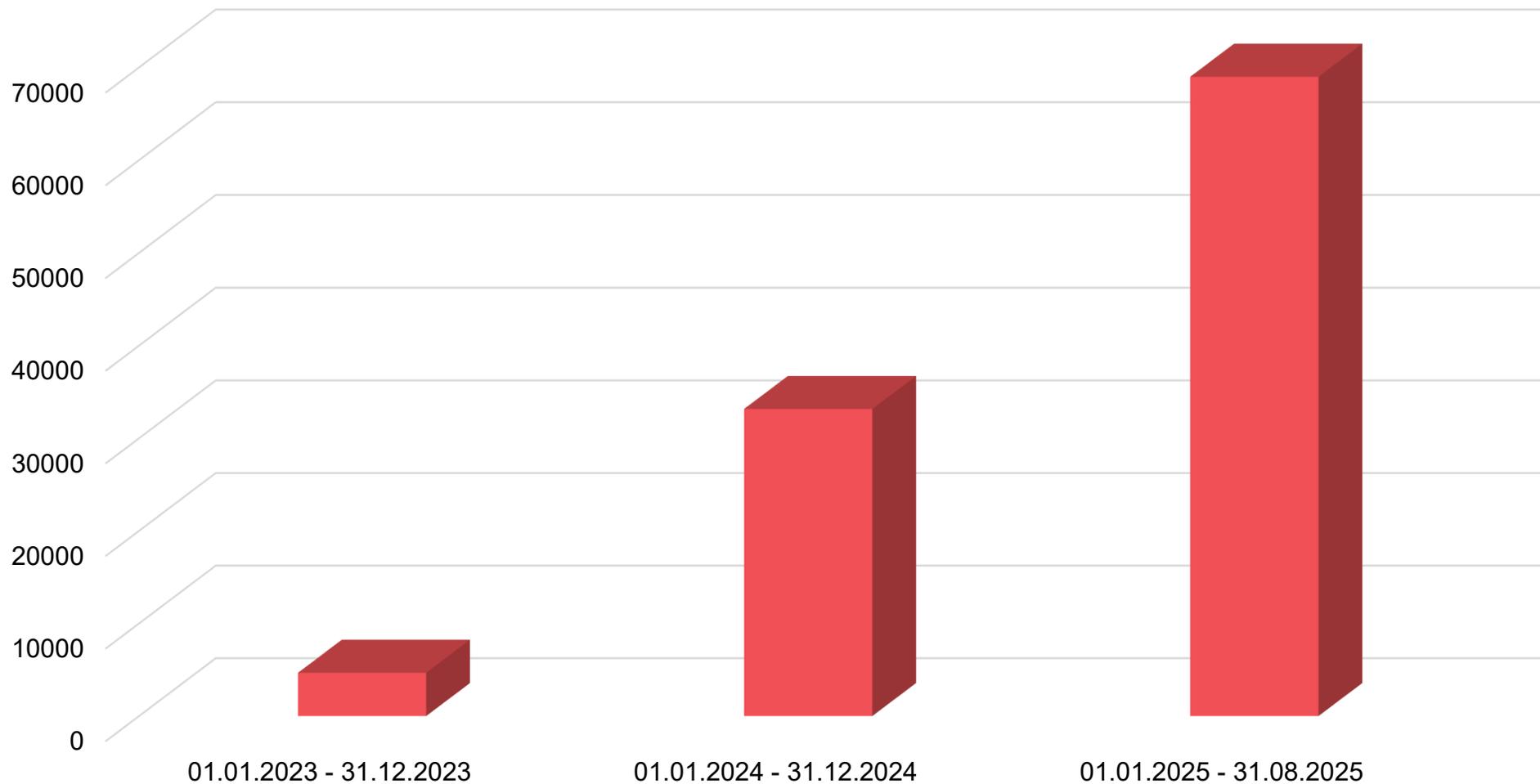
▶ **Стабильно высокие показатели** выявляемых и блокируемых вредоносных доменов в российских доменных зонах (**39 951** домен в 2023 году, **41 794** в 2024 году, **26 473** за период с 1 января по 31 августа 2025 года). Снижение по сравнению с аналогичным периодом прошлого года составило **менее 1%**,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

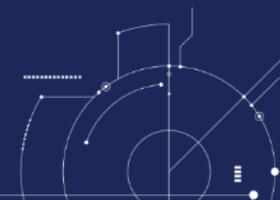
Статистика снятия с делегирования доменов в российских доменных зонах за 2023 - 2025 годы



Статистика блокирования средствами ЦМУ ССОП ФГУП «ГРЧЦ»



Машинно-генерированные (DGA) домены



sklad-0662.shop iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
ru-oplat035295.ru help-1955.info zakaz-01586.ru help-9711.info zakaz-01579.ru nycaciu8.pro
fiqoxai0.pro zakaz-01574.ru af885857.top safe-0703.info help-0027.info megyduo5.pro
rent-id6198.info rorygea0.pro af885853.top cdek-5512.info lycehui7.pro ginytee9.pro
confirmation-id1616.com rn512353.icu safe-4378.info bonus-ec.cyou lk442.ru secure-i.cfd
rn3265152.icu hiriwoa7.pro paryju9.pro safe-4341.info ord09.click af885856.top af885854.top ru-oplat01848472.ru
xisidoy7.pro sale4267.ru ru-oplat060503.ru zakaz-01582.ru sale4274.ru af885855.top ru-527.pro
help-0483.info safe-4181.info help-0041.info sale4263.ru bonus-qb.cyou lk468.ru qogyhaa4.pro ord74811.info
af885851.top ru-991.pro zakaz-8311.shop foniqau2.pro sale4276.ru lk199.ru lk675.ru
cdek-2982.info narynya7.pro hyqagy06.pro ord-5136.shop lk125.ru sale4280.ru
rn315152.icu ru-oplat7675353.ru lk152.ru zakaz-01585.ru canuvay6.pro safe-1965.info
lk119.ru zakaz-01577.ru zakaz-01581.ru zakaz-1125.info safe-1407.info
confirmation-id67528.com lk417.ru bonus-wc.cyou lk648.ru bonus-gr.cyou
zakaz-01583.ru ru-oplat095636.ru ru-oplat0536902.ru zakaz-01587.ru

Вредоносные домены, схожие с наименованиями легитимных организаций

воркингднс.рф

Удаленная работа в DNS | Под: × +

← → ↻ https://воркингднс.рф

DNS [О вакансии](#) [Как устроиться](#) [Преимущества](#) [Отзывы](#) [Анкета](#)

Заполните все поля, чтобы присоединиться к команде лидера рынка электроники

ФИО (полностью):
Иванов Иван Иванович

Дата рождения: Номер телефона:

Модель устройства:
Выберите тип устройства

Номер карты для выплат (на ваше имя):

Карты Ozon Bank не принимаются!

ИНН:

⚠ DNS оставляет за собой право отказать в трудоустройстве, если будут указаны неверные данные или если вы предоставите карту Ozon Bank

[Отправить анкету в DNS](#)

Вредоносные домены, схожие с наименованиями легитимных организаций

воркингднс.рф

Удаленная работа в DNS | Плоский экран

← → ↻ 🔒 https://воркингднс.рф

DNS

Заполните все поля, чтобы...

ФИО (полностью):
Иванов Иван Иванович

Дата рождения:
дд . мм . гггг

Модель устройства:
Выберите тип устройства

Номер карты для выплат (на ваше имя):
0000 0000 0000 0000
Карты Ozon Bank не принимаются!

ИНН:
12 цифр

⚠️ DNS оставляет за собой право отказать в предоставлении карты Ozon Bank

Продолжить

msdmos-info.ru, msdmog.ru

Московский скоростной диалог

← → ↻ 🔒 https://msdmos-info.ru

↑ ОПЛАТА ПРОЕЗДА ↑ ИНФОРМАЦИЯ ПРО МСД ↑ ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ ↑ ОБРАТНАЯ СВЯЗЬ

ОПЛАТА

ОПЛАТИТЬ ПРОЕЗД

Номер РФ Иностраннй или специальный номер

Государственный регистрационный номер
A000AA000

Телефон
+7 () _ _ _ _

Email
example@mail.ru

Дата проезда
дд.мм.гггг

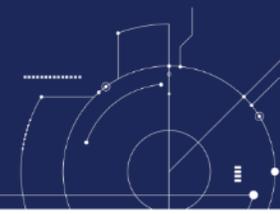
⚠️ С 15 февраля 2023 года изменились правила проезда по МСД только в критически загруженные часы: с 7:00 до 11:00 и с 16:00 до 20:00. Подробнее

Стоимость всех совершенных за сутки проездов по МСД суммируется, после чего в течение 5 дней выставляется единый платеж за все проезды по трассе за день.

Продолжить

Оплатить проезд Нормативные документы 125040, Москва, ул. Скаковая, д. 19 © Официальный сайт «Московский скоростной

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



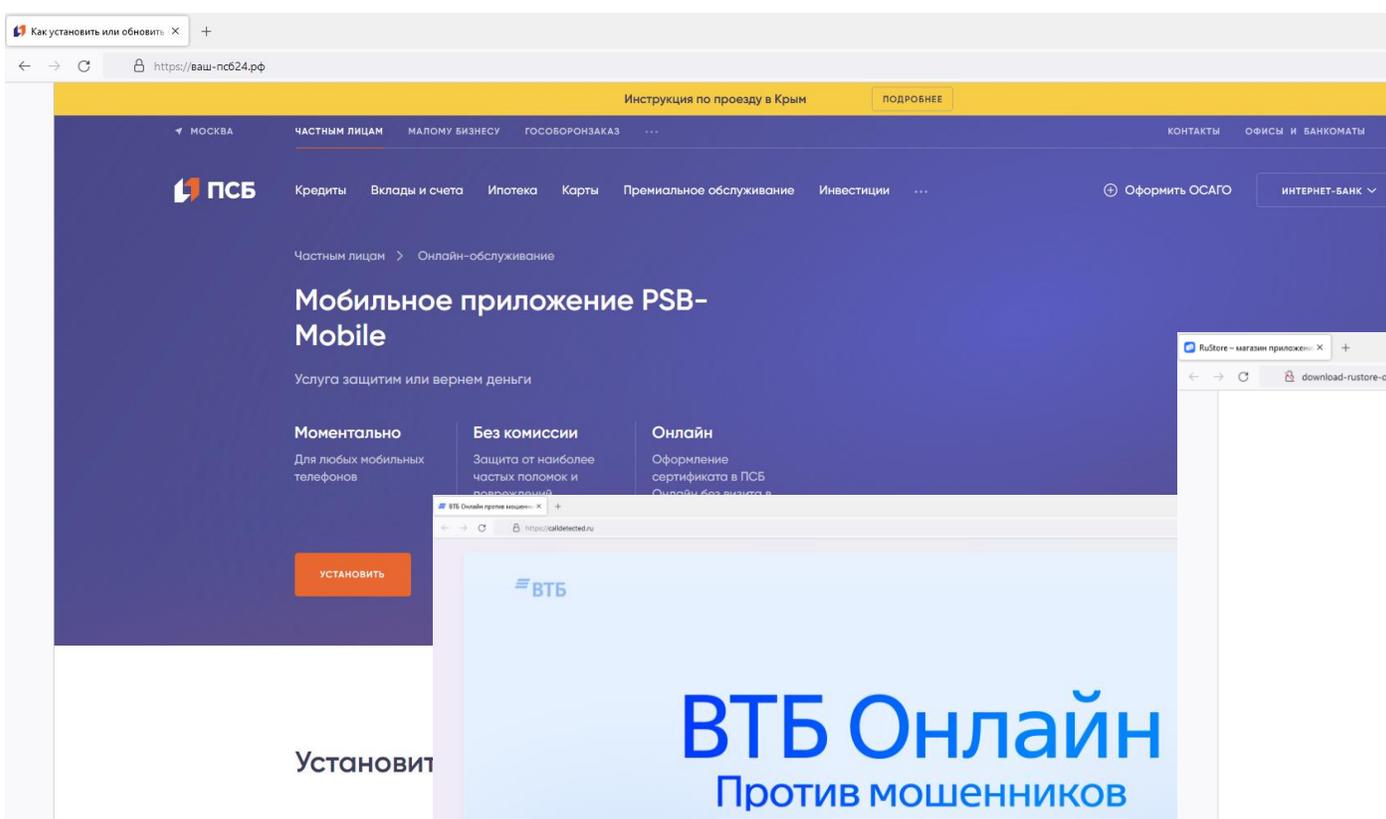
force-poll.ru
personality-force.ru
rating-force.ru
force-action.ru
leader-force.ru
uniting-force.ru
force-leader.ru
force-uniting.ru
smarts-paying.ru
smarts-payments.ru
smartspayment.ru
smarts-payer.ru
restfulpays.ru
performance-stage.ru
restfulpayings.ru
restful-paying.ru
org-verif.ru
orgverif.ru

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



Как установить или обновить

Инструкция по проезду в Крым

МОСКВА ЧАСТНЫМ ЛИЦАМ МАЛОМУ БИЗНЕСУ ГОСБОРОНЗАКАЗ

Кредиты Вклады и счета Ипотека Карты Премияльное обслуживание Инвестиции

Оформить ОСАГО ИНТЕРНЕТ-БАНК

Частным лицам > Онлайн-обслуживание

Мобильное приложение PSB-Mobile

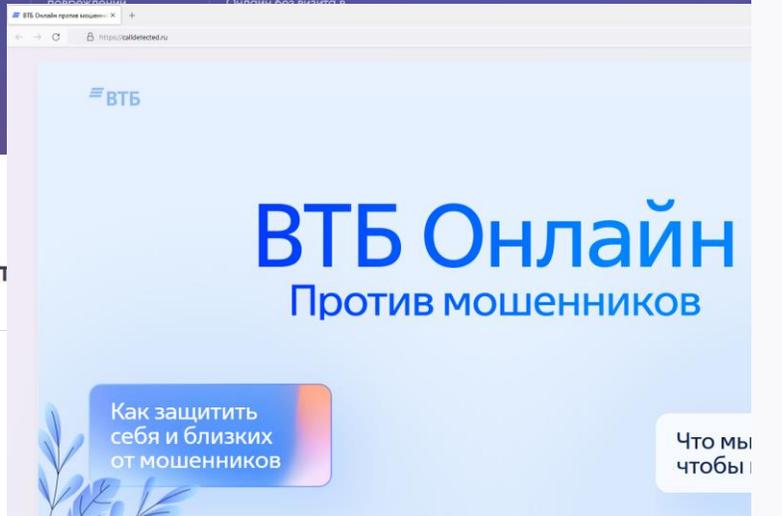
Услуга защитим или вернем деньги

Моментально
Для любых мобильных телефонов

Без комиссии
Защита от наиболее частых поломок и повреждений

Онлайн
Оформление сертификата в ПСБ Онлайн без визита в отделение

Установить



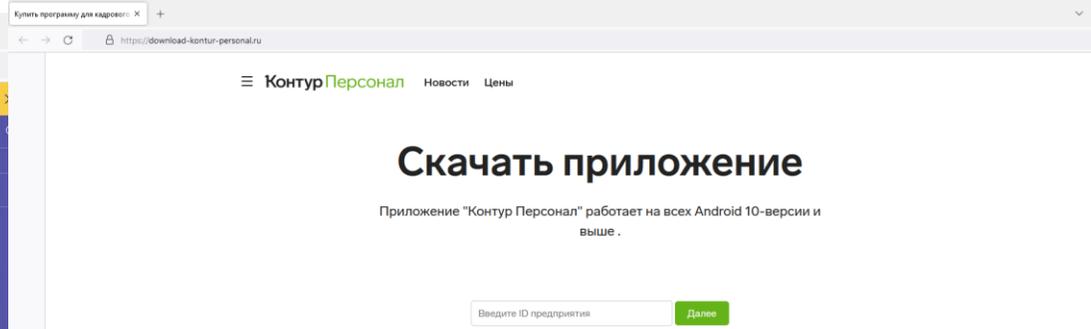
ВТБ

ВТБ Онлайн

Против мошенников

Как защитить себя и близких от мошенников

Что мы чтобы!



Купить программу для кадров

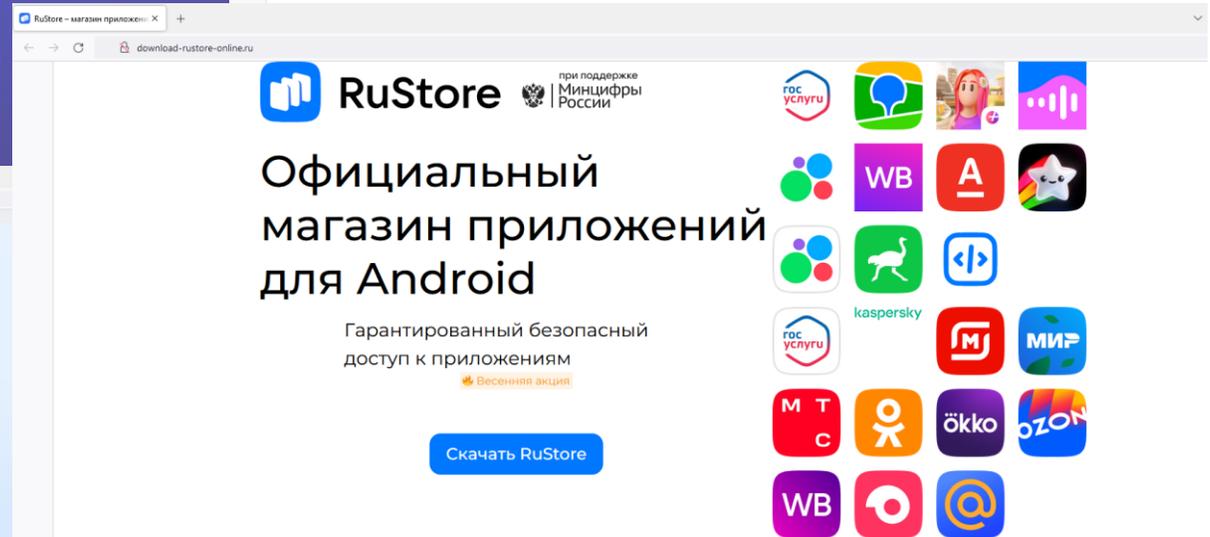
КонтурПерсонал Новости Цены

Скачать приложение

Приложение "Контур Персонал" работает на всех Android 10-версии и выше.

Введите ID предприятия

Далее



RuStore при поддержке Минцифры России

Официальный магазин приложений для Android

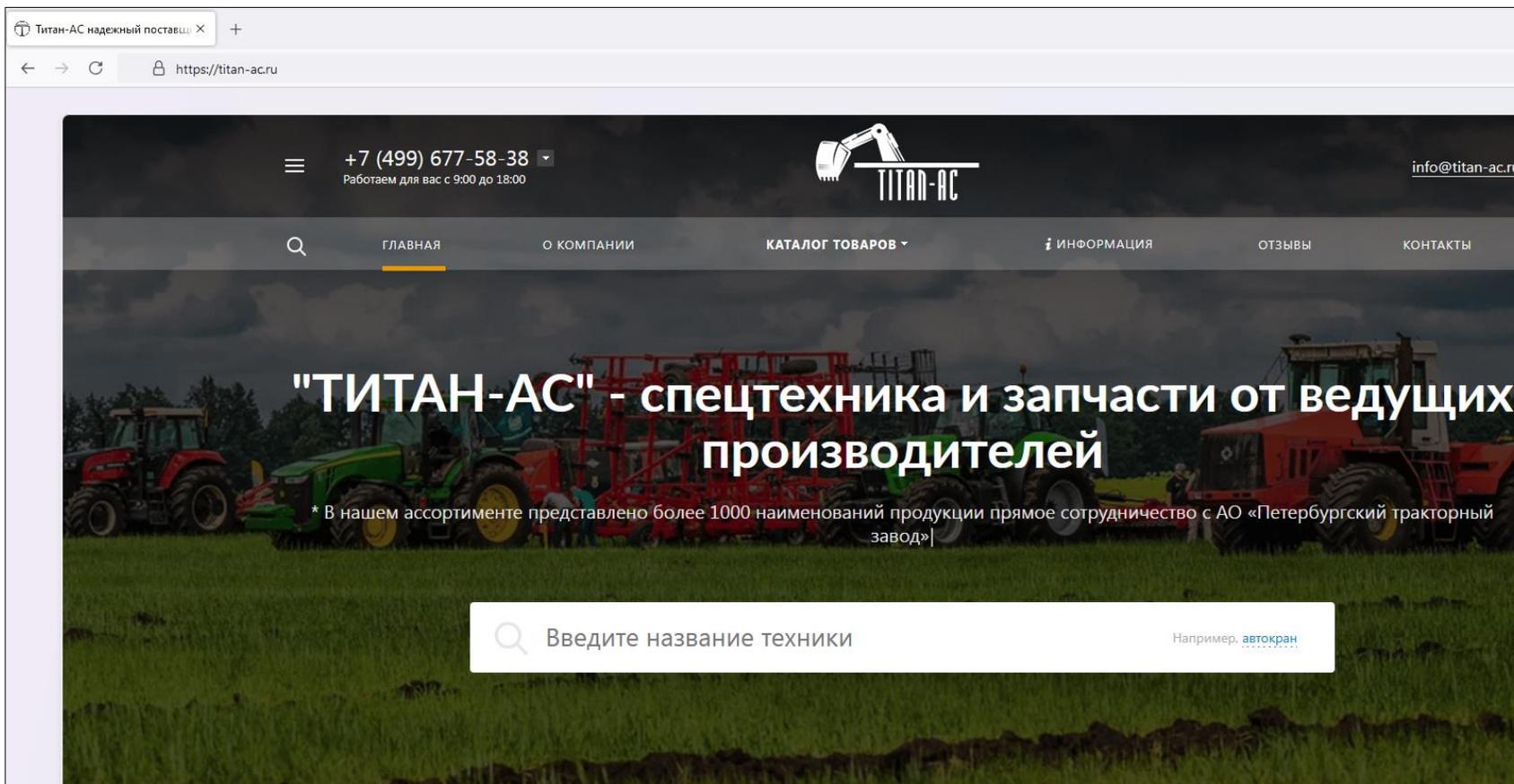
Гарантированный безопасный доступ к приложениям

Весенняя акция

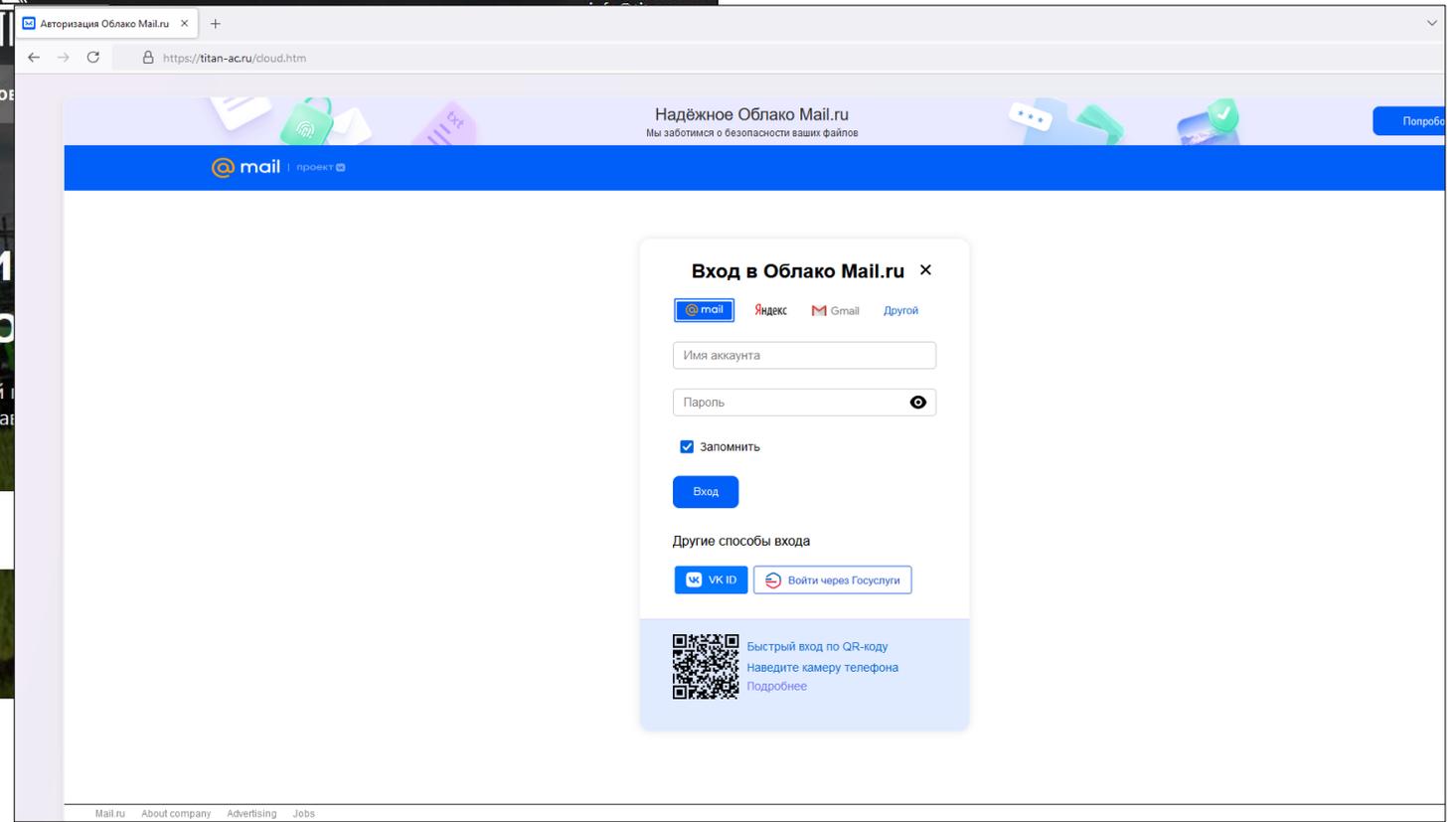
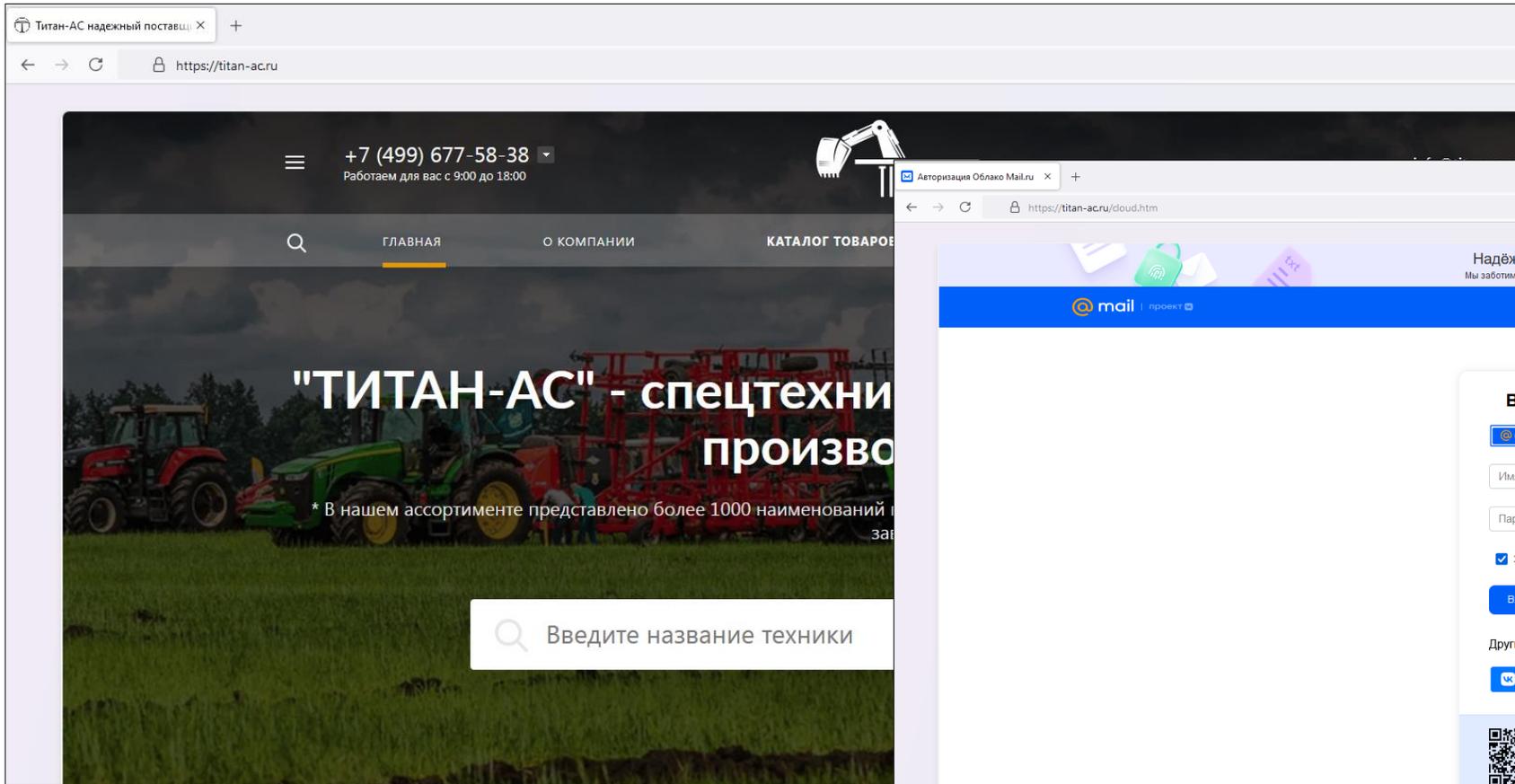
Скачать RuStore

гос услуги, WB, A, kaspersky, гос услуги, М Т С, ökko, MIPI, WB, @

Использование уязвимостей CMS для компрометации ресурса



Использование уязвимостей CMS для компрометации ресурса

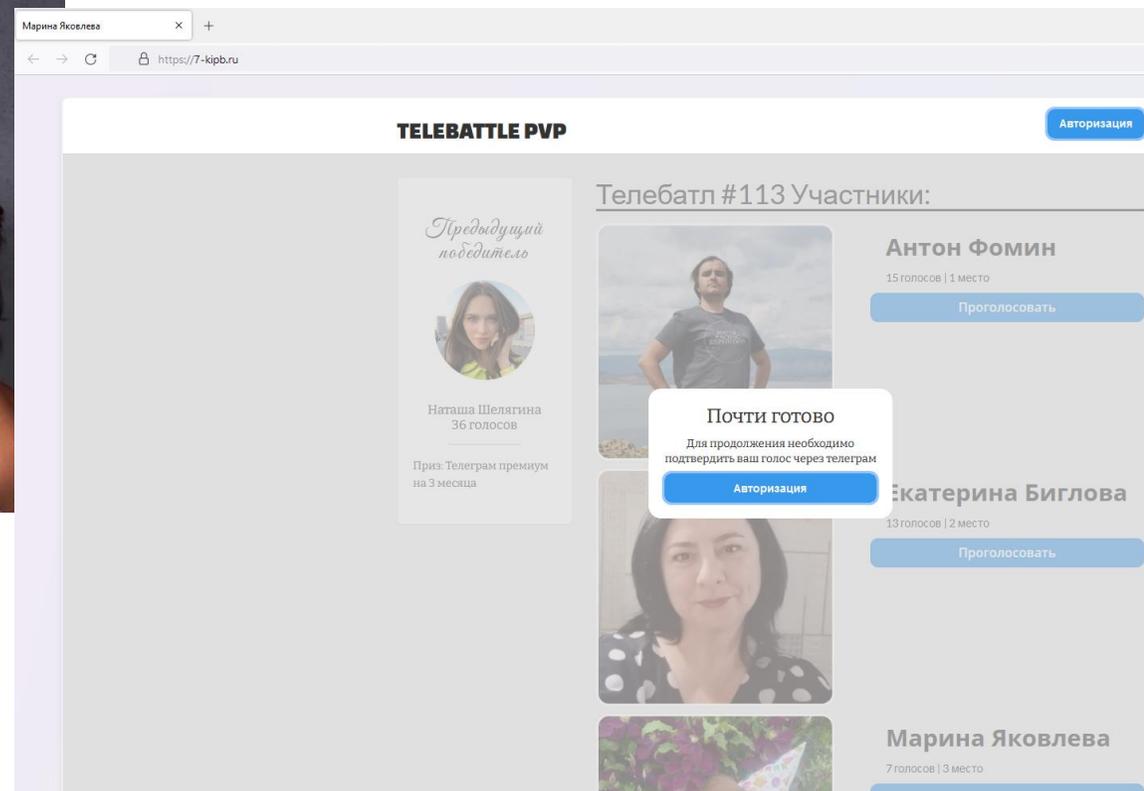
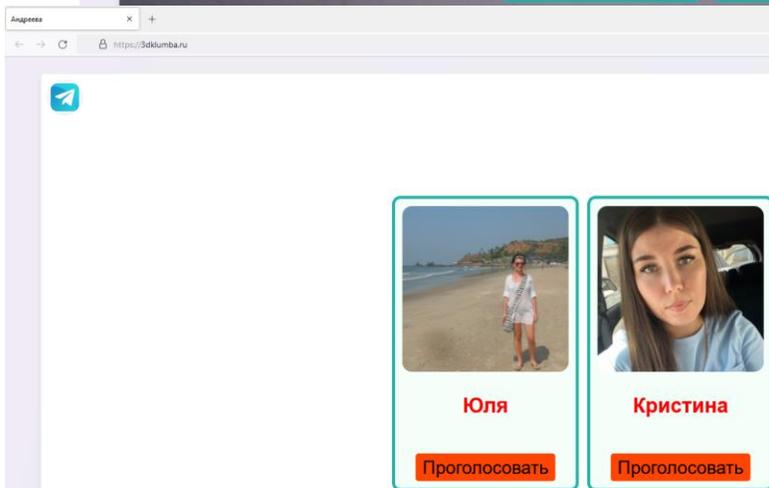
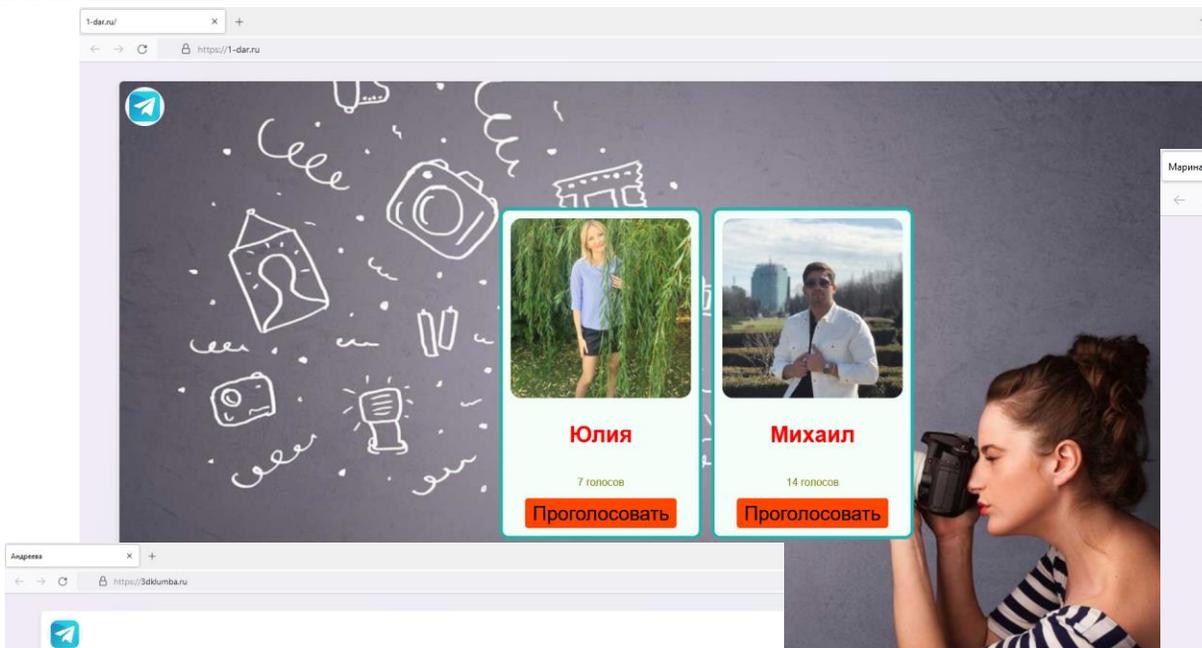


Некорректная настройка DNS-зоны домена



- 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



Некорректная настройка DNS-зоны домена

The image shows a Telegram login page with a browser window overlay. The browser window displays a Telegram channel page with a drawing of a house and a camera. The Telegram login page has the following elements:

- Telegram logo
- Text: "Sign in to Telegram"
- Text: "Please confirm your country code and enter your phone number."
- Country dropdown menu: "Russian Federation"
- Phone Number input field: "+7 -----"
- Checkbox: "Keep me signed in" (checked)
- Next button: "NEXT"
- Link: "LOG IN BY QR CODE"

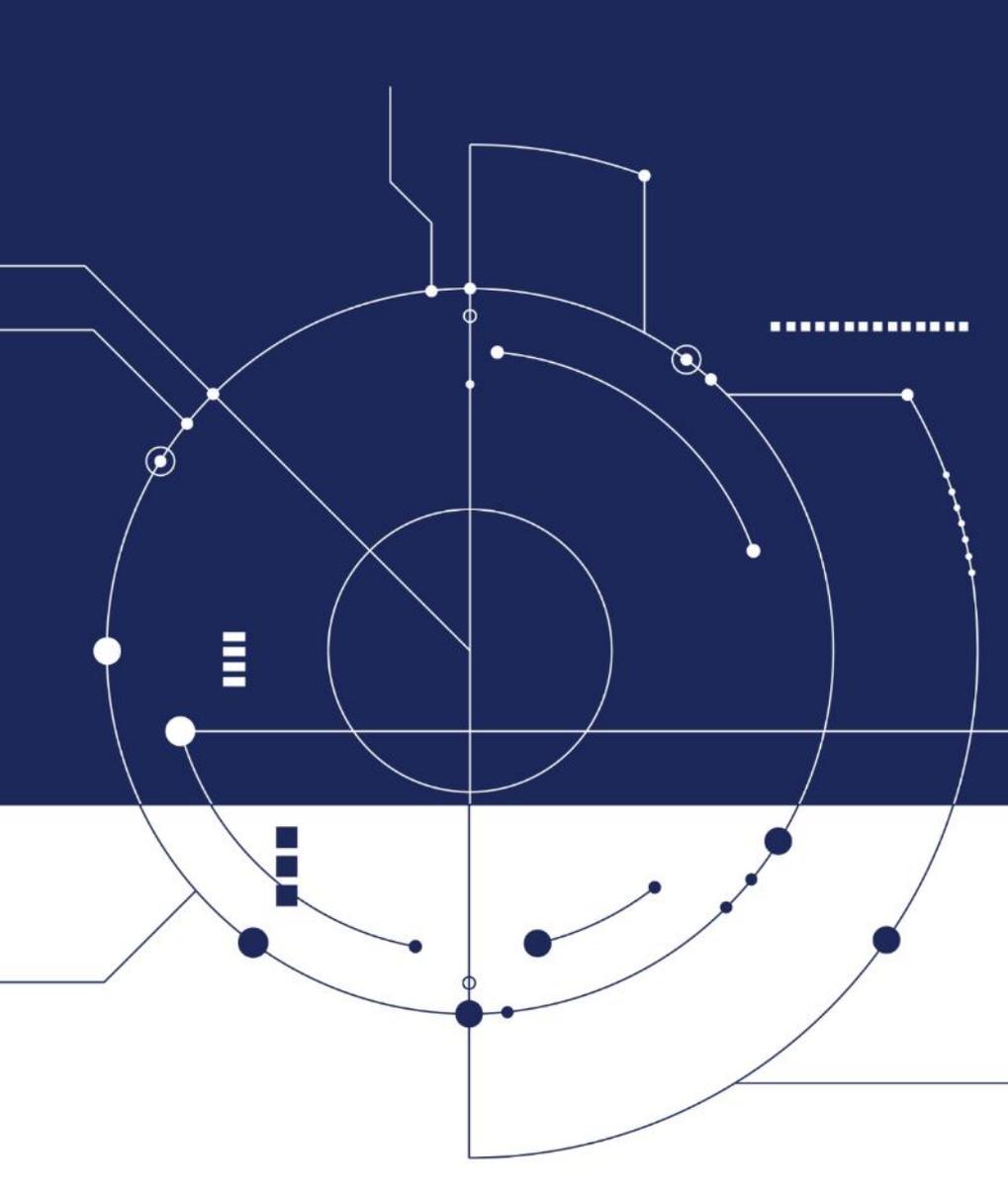
On the right side, there is a list of users with a "Проголосовать" button for each:

- Антон Фомин (1 место)
- Катерина Биглова (2 место)
- Марина Яковлева (3 место)

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