

# Конвеєр фейків та спаму: як білоруська платформа ProхуSmart допомагає шахраям орендувати тисячі «українських» номерів

[Читати на руском](#)


Конвеєр фейків та спаму: як білоруська платформа ProхуSmart допомагає шахраям орендувати тисячі «українських» номерів

**Ваша «сестра» у відчай просить терміново переказати гроші — ось тільки сестри у вас немає. Докучливі «страхові агенти», фальшиві дзвінки від імені оператора зв'язку, тривожні SMS із вимогою негайно перейти за посиланням — усе це давно стало частиною повсякденного життя. А за переважною більшістю таких атак стоять SIM-ферми: стелажі з мобільними телефонами та модемами, здані в оренду шахраям для автоматизованих кампаній у глобальному масштабі.**

Те, що SMS-повідомлення надійшло з місцевого номера, зовсім не означає, що його надіслав хтось із вашої країни. Саме доступ до місцевої телеком-інфраструктури ініціатори загроз і використовують, аби вселити довіру до підроблених звернень, зазначає видання [Cybercalm](#). У квітні 2026 року компанія [Infrawatch](#) оприлюднила результати масштабного розслідування, що показує, як ціла індустрія «SIM-ферм як послуги» живить шахрайство по всьому світу — зокрема й в Україні.

## Що таке SIM-ферма і чому вона небезпечна

SIM-ферма — це мережа з сотень, а іноді й тисяч SIM-карток, підключених до модемів та смартфонів, які одночасно виконують обчислювальні й комунікаційні завдання. За логікою вона нагадує криптоферму: велика кількість уніфікованого обладнання, орієнтованого на автоматизацію. Проте замість видобутку криптовалюти SIM-ферма продукує телефонні номери та мобільні IP-адреси «на вимогу».

## Важливі новини

07.05.2026



**Підсанкційна та оголошена в розшук банкірша Альона Шевцова витрачає сотні тисяч доларів в Дубаї та п...**

#Ibox #Розыск #розшук

03.05.2026



**Родина Злочевського з кіпрськими паспортами продовжує обкрадати Україну та відкривати нові бізнеси**

#САП #Инфокс #Инфокс



**ЯК ОБИЙТИ БЛОКУВАННЯ І ЧИТАТИ НАШ САЙТ**

## Останні новини

[По даті](#) [По переглядам](#) [По коментарям](#)

00:03 Тайвань, Іран та РФ на порядку денному: Трамп летить до Китаю для складних переговорів із Сі Цзіньпіном

10 травня 2026 г.

23:56 Повторення «югославського сценарію»: У Євросоюзі готуються до сплеску нелегального обігу зброї

23:49 «Мені це не подобається!»: Трамп різко відреагував на пропозиції Тегерана 📸

23:43 **Російські війська просунулися західніше Гришиного на Покровському напрямку, — DeepState** 📸

23:36 30 днів на переговори: Тегеран пропонує США припинити вогонь та частково вивезти уран в обмін на зняття санкцій 📸

Сам собою такий пристрій не є злочинним інструментом. Бізнес використовує SIM-ферми для тестування та масштабування телеком-сервісів, розробники — для перевірки мобільних застосунків, компанії — для легальних масових розсилок. Але коли керування цією інфраструктурою переходить до зловмисників, вона перетворюється на потужний конвеєр спаму, смішингу (фішингу через SMS), шахрайських дзвінків та автоматизованих атак на онлайн-сервіси.

Кожна SIM-картка у фермі фактично є окремим «пристроєм», з якого можна реєструвати нові облікові записи, обходити SMS-верифікацію, керувати бот-мережами в соцмережах і на форумах, поширювати дезінформацію та пропаганду, а також маскувати справжнє походження трафіку. Саме тому SIM-ферми стали улюбленим інструментом організованої кіберзлочинності: вони дають злочинцям «місцеве обличчя» у будь-якій країні — американський номер для атак на мешканців США, німецький — на користувачів у Німеччині, український — для атак на українців.


Серйозну загрозу бачать і державні органи. Секретна служба США попередила, що масштабні SIM-ферми здатні не лише розсилати шахрайські повідомлення, а й переважувати мобільні мережі, створювати перешкоди у роботі служб екстреного виклику та слугувати каналом для зашифрованих комунікацій організованих злочинних угруповань.

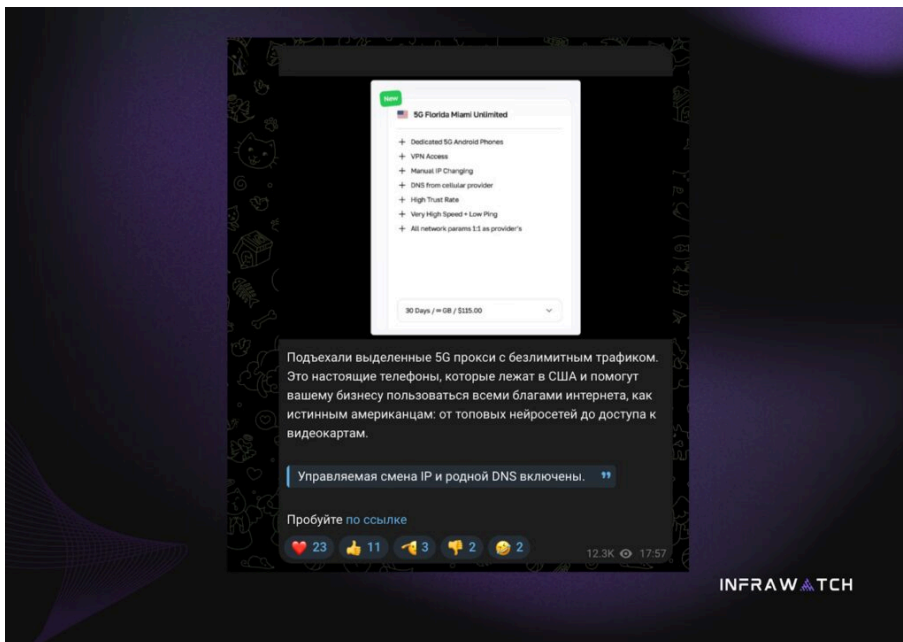
#### 94 локації у 17 країнах: як виглядає «SIM-ферма як послуга»

Розслідування Infracore, оприлюднене у квітні 2026 року, відкрило цілу екосистему комерційних SIM-ферм, об'єднаних спільною платформою керування Proxymart. За даними компанії, йдеться про 87 активних панелей керування у 17 країнах та щонайменше 94 фізичні локації зі стелажми телефонів і 4G/5G-модемів, підключених до мереж місцевих операторів. Найбільша концентрація обладнання — у США, де ферми виявлено у 19 штатах; окремі майданчики зафіксовано у Європі, Південній Америці та Австралії.

Країнами, де знайдено фізичну інфраструктуру, стали США, Канада, Велика Британія, Німеччина, Іспанія, Португалія, Україна, Латвія, Франція, Румунія, Бразилія, Ірландія, Нідерланди, Австралія, Італія, Польща та Грузія. Ферми підключені щонайменше до 35 мобільних операторів, серед яких AT&T, Verizon, T-Mobile, Vodafone, EE, O2, Three, Deutsche Telekom, Orange, Rogers, Telstra, а також українські Kyivstar і lifecell. Доступом до цієї інфраструктури торгують щонайменше 24 комерційних провайдерів проксі-сервісів.

Саму платформу Proxymart дослідники пов'язують із розробниками з Мінська (Білорусь). Вона продається як «коробкове рішення»: власнику ферми пропонують вебінтерфейс, API, автоматичну ротацію IP-адрес (зокрема шляхом вмикання-вимикання «режиму польоту» на кожному телефоні), підтримку протоколів OpenVPN, SOCKS5, VLESS та HTTP-проксі, а також функцію підміни відбитків операційної системи — пристрій може видавати себе за macOS, iOS, Windows чи Android. Сервіси, що працюють на базі Proxymart, активно рекламуються на Telegram-каналах, орієнтованих на російськомовну аудиторію, — зокрема як спосіб обійти геоблокування та отримати доступ до «західних» AI-сервісів і платформ для роботи з GPU.

	 Підпишіться на наш канал в Telegram. Оперативно про головне
23:30	«Викинули з машини та поїхали»: у Києві жінка намагалася відбити чоловіка у поліцейських під час мобілізації 📺
23:22	«Росія не стане союзником США»: Бен Годжес назвав ідею Трампа «відтягнути» Москву від Китаю нереалістичною
23:15	«Це не розкіш, а прозорі статки»: голова Херсонської ОВА Прокудін відповів на скандал довкола Audi Q7 і квартири в Києві 📺
23:09	Шахрайство в Москві, борги на мільярди та партнери під санкціями: розкрито невідомі факти про власника постачальника ЗСУ Fire Point Дениса Штілермана 📺
23:03	Суд у Харкові виніс вирок жінці за проросійські дописи в Telegram і виправдовування агресії РФ
22:56	BMW X5 і будинок під Києвом: активи родини керівника Держжосмосу Міхеєва визнали необґрунтованими
22:52	Фармацевтичний план «Б»: як Тимур Міндіч та Ігор Червоненко побудували аптечну імперію на податкових схемах
22:46	Суд на Закарпатті засудив мешканця Рахівщини за проросійські дописи в Telegram
22:40	Замість купальників — патріотизм: у РФ пропонують штрафувати жінок на мільйони за фото в бікіні 📺
22:34	Трагедія перед Ель-Класіко: Гансі Флік втратив батька за кілька годин до матчу з «Реалом» 📺
22:28	Конвеєр фейків та спаму: як білоруська платформа Proxymart допомагає шахраям орендувати тисячі «українських» номерів 📺
22:22	Кіпрські чиновники на святі у токсичного бізнесмена: Дмитро Пунін презентував виноробний проєкт попри кримінальні справи 📺
22:16	Бренди замість батарей: голова Голосіївської РДА Дунаєвська шокує розкішшю на тлі комунальних проблем району
22:10	П'ять років за коментарі в Telegram: суд виніс вирок мешканцю Кам'янського за виправдовування агресії РФ
22:04	РФ готує штурми на Майське та Віролюбівку: росіяни посилюють сили на Краматорському напрямку
21:57	Мільйон з бюджету за помилку ДФС: суд зобов'язав виплатити компенсацію ексмитнику Олегу Кондратюку
21:50	Уперше на напрямку: важкий БПЛА «Баба Яга» змусив окупантів кинути полонених і втекти



Показово, що жодних реальних перевірок клієнтів (KYC) більшість провайдерів не проводить, а оплату часто приймають у криптовалюти. Це означає, що фактично будь-який покупець — включно з професійними шахраями та операторами бот-мереж — може орендувати готову інфраструктуру для атак.

### Реакція правоохоронців: від Нью-Йорка до операції SIMCARTEL

У вересні 2025 року Секретна служба США демонтувала у Нью-Йорку мережу з понад 300 SIM-серверів і близько 100 000 SIM-карток, що працювала поблизу штаб-квартири ООН. За оцінкою правоохоронців, потужності цієї ферми вистачило б, аби вивести з ладу мобільний зв'язок у масштабах усього Нью-Йорка. Місяцем пізніше, у жовтні 2025 року, Європол підтримав міжнародну операцію SIMCARTEL в Австрії та Латвії: сім затриманих, 1200 вилучених SIM-боксів і 40 000 активних SIM-карток, які фігурують щонайменше у 1700 кримінальних провадженнях про кібершахрайство.

Попри гучні ліквідації, SIM-ферми залишаються у так званій «сірій зоні» законодавства більшості країн. Саме обладнання не є забороненим, а регулятори зазвичай не мають інструментів, щоб оперативно реагувати на зміну власника чи «орендаря» інфраструктури. Наразі єдиною державою, яка на рівні закону заборонила володіння та постачання SIM-ферм, залишається Велика Британія — там нова норма покликана позбавити шахраїв готового інструменту для масових атак. Проте поза межами юрисдикції Лондона ця заборона не діє.

### Що це означає для українців

Україна є однією з 17 країн, де Infracatch зафіксувала фізичні SIM-ферми, а також однією з юрисдикцій, до яких активно маршрутизується шахрайський трафік. За даними Департаменту кіберполіції Національної поліції України, смішинг і фішингові SMS стабільно входять до топу онлайн-загроз: користувачі отримують повідомлення про «заблоковану картку», «недоставлену посилку», «державну субсидію», «виграш» або нібито від знайомого з проханням позичити гроші. Лише у 2024 році середня сума шахрайської транзакції з платіжними картками в Україні зросла на 40% і сягнула понад 4200 гривень, а сумарні збитки перевищили мільярд гривень.

Додатковий ризик створює російсько-українська війна. Росія та її проксі-структури мають очевидний інтерес до інфраструктури, яка дозволяє розсилати SMS і здійснювати дзвінки з «українських» номерів — для поширення паніки, дезінформації, фейкових звернень від імені військових, волонтерів чи держорганів. Той факт, що платформа Proxymart розроблена у Мінську та активно просувається у російськомовному сегменті, не додає оптимізму.

### Як розпізнати атаку через SIM-ферму і не стати жертвою

Жоден технічний захід не скасовує основного правила: дзвінки та SMS варто сприймати критично незалежно від того, з якого номера вони надійшли. Місцевий код країни чи оператора більше не є гарантією, що повідомлення справжнє.

## Теги новин

COVID-19 агресия России Атака

# Війна Война ВСУ

Вторжение Дональд Трамп Донбасс ДТП  
Зеленский ЗСУ Киев Київ

коронавирус Коррупция **Напад**

# Росії на

# Україну Нападение

России на Украину оккупанты  
оккупанти Порошенко Путин Росія

# Россия СБУ США Украина

Україна ЧП Эпидемия коронавируса

## Наші опитування

**Чи вірите ви, що Дональд Трамп зможе зупинити війну між Росією та Україною?**

- Так, повністю зможе
- Частково зможе, але не відразу
- Ні, не зможе
- Це залежить від дій інших сторін
- Важко відповісти

[Голосувати](#)

[Показати результати опитування](#)  
[Показати всі опитування на сайті](#)

- Не довіряйте знайомому вигляду номера. SIM-ферми дають шахраям саме локальну «прописку». Повідомлення з українського номера цілком може бути частиною автоматизованої кампанії, розгорнутої за кордоном.
- Слідкуйте за новими схемами. Сьогодні шахраї рідко обіцяють «виграш у лотерею». Значно частіше вони маскуються під банки, «Нову пошту», «Укрпошту», Кіберполіцію, державні сервіси (включно з «Дією»), операторів зв'язку, роботодавців, родичів і колег.
- Звертайте увагу на сигнали підробки. Знеособлене звертання, граматичні помилки, скорочені посилання (bit.ly, cutt.ly тощо), дивні символи в адресі (наприклад, «roz3tka.ua» замість «rozetka.ua»), невідповідність відправника тексту повідомлення — усе це маркери фішингу. Ніколи не переходьте за посиланнями з SMS або месенджера: якщо сумнівається, відкрийте офіційний застосунок банку чи сервісу самостійно або зателефонуйте на номер зі зворотного боку картки.
- «Терміново» — майже завжди підозріло. Шахраї свідомо створюють паніку: «картку заблоковано», «посилку повернуть», «рідний у лікарні та потрібні гроші». Саме цей емоційний тиск штовхає жертву до необдуманих дій. Зупиніться, передзвоніть родичу за відомим вам номером, зв'яжіться з банком через офіційний канал.
- Увімкніть двофакторну автентифікацію — але не через SMS. [SMS-коди залишаються одним із найслабших способів підтвердження](#), особливо з огляду на [SIM-свопінг](#). Де можливо, використовуйте застосунки-автентифікатори або ключі доступу ([passkeys](#)).
- Фіксуйте інциденти. Про підозрілі повідомлення варто повідомляти Кіберполіцію через [cyberpolice.gov.ua](#) або за номером 102. Це допомагає відстежувати схеми та блокувати інфраструктуру.

### Окрема загроза: SIM-свопінг

Разом із SIM-фермами варто тримати у полі зору й іншу атаку на мобільний зв'язок — так званий SIM-свопінг, або підміну SIM-картки. У цій схемі шахрай не орендує номери, а переводить ваш номер під свій контроль: видає себе за абонента перед оператором і добивається переоформлення SIM-картки на нову «болванку». Отримавши контроль над номером, він має коротке вікно, аби перехопити SMS із кодами двофакторної автентифікації й зайти у ваш банк, месенджер чи поштову скриньку.

Перший сигнал такої атаки — раптове зникнення мобільного зв'язку: дзвінки й SMS перестають надходити без очевидних причин. У такій ситуації діяти потрібно негайно: зв'язатися з оператором з іншого номера, заблокувати SIM-картку, повідомити банк і змінити паролі до критичних сервісів. Для захисту від SIM-свопінгу варто встановити у свого оператора додаткове кодове слово для операцій із номером, увімкнути послугу заборони дистанційної заміни SIM-картки (де вона доступна), а також переходити з SMS-автентифікації на застосунки-автентифікатори та ключі доступу ([passkeys](#)).

### Підсумок

SIM-ферми перетворили шахрайські SMS і дзвінки з разових махінацій на промисловість з готовими «коробковими» рішеннями для зловмисників. Окремі національні заборони та ліквідації мереж допомагають знижувати тиск, але не усувають загрозу повністю — тим паче поки значна частина інфраструктури розміщена у юрисдикціях, які не співпрацюють із західними правоохоронцями, і просувається серед російськомовної аудиторії. У цих умовах головним рубежем оборони залишається сам користувач: здорова недовіра до будь-якого «терміново», звичка перевіряти інформацію офіційними каналами та коректне налаштування автентифікації роблять атаки через SIM-ферми економічно не вигідними для шахраїв.

Теги: [США](#) [SIM-ферма](#) [криптоферма](#) [Криптовалюта](#) [Infrawatch](#) [Беларусь](#) [Білорусь](#) [ProxySmart](#)  
[Мошенництво](#) [Шахрайство](#) [кол-центр](#)



**Марія Войтенко**

ОГЛЯДАЧ НОВИН

Роздрукувати

Надіслати товаришу

## Коментарі:

comments powered by Disqus

### Головна

Про нас  
Статті  
Архів  
Закони  
Контакти

### Новини

Рейдерство  
Корупція  
Економіка  
Новини світу

### Конфлікти

Політика  
Корпоративні  
конфлікти  
Кримінал

### Позиція

Коментарі  
Різне

### Думка

Політика  
Економіка

### Події

### Відео

### Війна

### Блоги

2013-2026 © АНТИКОР — національний антикорупційний портал


Реклама на сайті • Наші партнери

Політика конфіденційності


Використання матеріалів сайту дозволено лише за наявності активного гіперпосилання на джерело. Усі права на тексти, зображення, фотографії та відеоматеріали належать їх авторам.


 Facebook

 Twitter

 YouTube

 RSS-підписка

 Email-розсилка

 Мобільна версія