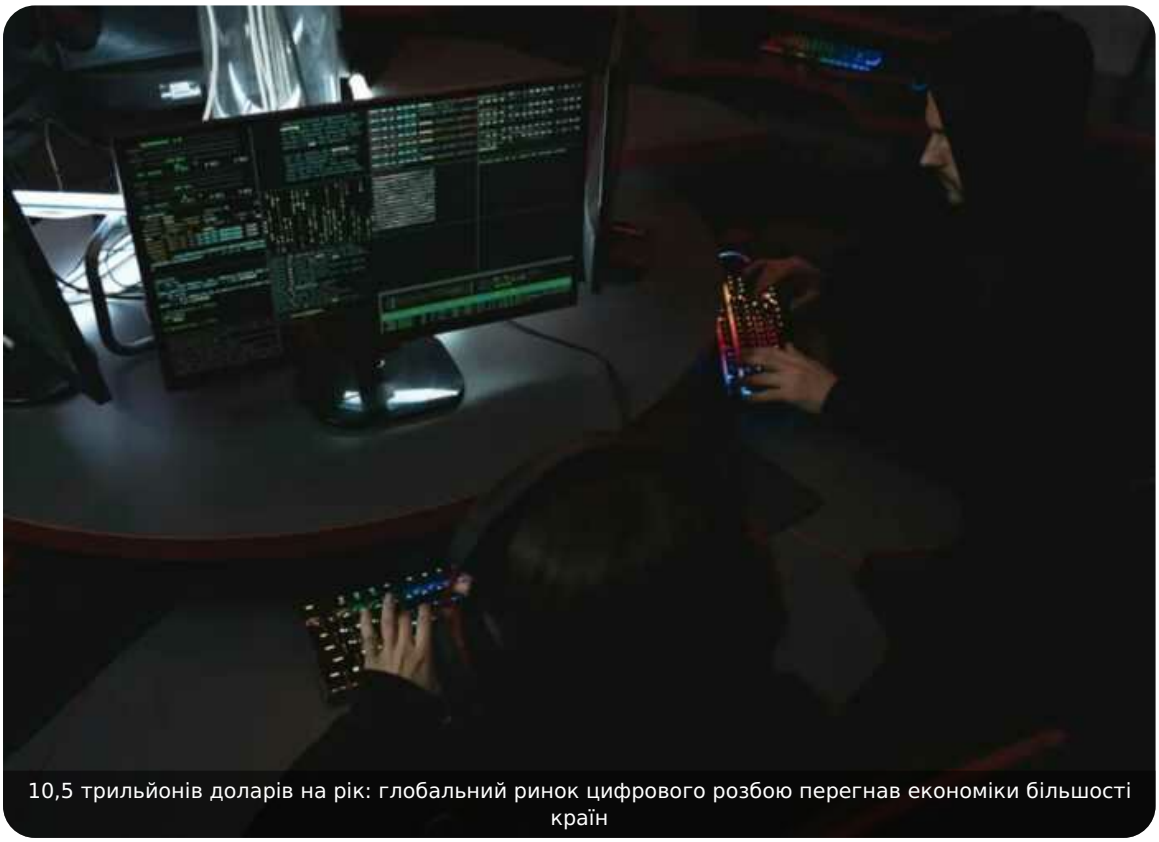
10,5 трильйонів доларів на рік: глобальний ринок цифрового розбою перегнав економіки більшості країн

04 травня 2026 р., 20:45



10,5 трильйонів доларів на рік: глобальний ринок цифрового розбою перегнав економіки більшості країн

Забудьте про самотніх геніїв у каптурах — сучасна кіберзлочинність виглядає як кремнієва долина, де замість смузі п'ють сльози системних адміністраторів.

Глобальний ринок цифрового розбою розрісся до масштабів, що перевищують економіки більшості країн світу, а сервісна модель "Злам як послуга" дозволяє будь-якому дилетанту влаштувати колапс корпорації за ціною підписки на Netflix. У цьому світі Telegram замінив Даркнет, а штучний інтелект пише фішингові листи краще за професійних копірайтерів. Поки ми вибудовуємо стіни, хакери просто купують ключі від наших дверей у "брокерів доступу", перетворюючи кібервійну на найприбутковіший бізнес XXI століття.

У звітах з кібербезпеки прийнято описувати хакерські атаки як окремі події — але насправді за кожним успішним зламом стоїть ціла мережа взаємозалежних постачальників послуг, посередників і виконавців.

Кіберзлочинність давно перестала бути справою самітників і перетворилася на повноцінну підпільну індустрію з власним ринком праці, ланцюгами постачання та навіть конкуренцією між «вендорами».

За оцінками дослідників, у 2025 році глобальні збитки від кіберзлочинності сягнули $10,5 трлн на рік — більше, ніж ВВП будь-якої країни світу, крім США та Китаю, зазначає видання Cybercalm. Для порівняння: це вдвічі перевищує ВВП України за всю її незалежну історію, разом узяту. Кіберзлочинність як сервісна модель зробила атаки доступними навіть для людей без технічних знань: купити готовий інструмент для злому можна так само легко, як замовити доставку їжі.

Компанія з кібербезпеки CrowdStrike ще в 2021 році систематизувала цю екосистему, розділивши її на три великі категорії: послуги, дистрибуція та монетизація. Сьогодні ця структура залишається актуальною, але кожна з категорій суттєво еволюціонувала — і доповнилася двома новими вимірами, яких п’ять років тому просто не існувало: штучним інтелектом та Telegram як основним майданчиком підпільної торгівлі.

Рівень перший: послуги та постачальники

Базова інфраструктура кіберзлочинності — це набір спеціалізованих сервісів, які злочинні угруповання «орендують» або купують замість того, щоб розробляти самостійно. Принцип той самий, що й у легальному технологічному бізнесі: навіщо будувати власний дата-центр, якщо можна орендувати хмару?

Брокери початкового доступу (Initial Access Brokers)

Це, мабуть, найпомітніша категорія підпільного ринку останніх років. Брокери доступу — зловмисники, які спеціалізуються на зламі корпоративних мереж і наступному продажі цього доступу іншим групам. Вони не проводять атаки самостійно — вони постачають «відчинені двері».

За даними Group-IB, у 2024 році зафіксовано понад 3 000 пропозицій продажу доступу до корпоративних мереж — на 15% більше порівняно з 2023 роком. Регіон Північної Америки показав найбільший приріст — 43%. Ціни варіюються від кількох сотень до десятків тисяч доларів залежно від розміру організації та рівня привілеїв.

Ransomware-as-a-Service та Crime-as-a-Service

Модель «вимагачі як сервіс» (RaaS) фактично демократизувала один із найприбутковіших видів кіберзлочинності. Розробники програм-вимагачів більше не проводять атаки самостійно — вони створюють платформу й продають або здають в оренду доступ до неї афіліатам, отримуючи від 10 до 30% від кожного виплаченого викупу.

У 2024 році Group-IB ідентифікувала 39 нових RaaS-оголошень і зафіксувала 44-відсоткове зростання кількості афіліатів. Кількість атак через спеціалізовані сайти витоків збільшилась на 10% — до понад 5 000 задокументованих випадків. У 2024 році одна компанія зі списку Fortune 50 виплатила рекордний викуп у $75 млн.

Послуги анонімізації та «куленепробивний» хостинг

Інфраструктура анонімності — ще один ключовий елемент підпільного ринку. Сюди входять резидентні проксі-мережі (трафік маршрутизується через пристрої реальних користувачів, що робить його майже невиявним), приватні VPN-сервіси без журналів активності, а також «куленепробивні» хостинг-провайдери — компанії, що надають серверну інфраструктуру і свідомо ігнорують скарги на зловживання.

Фішинг-набори та Webinject

Фішинг-набори — готові веб-інструменти для автоматизації фішингових атак — доступні на підпільних ринках за суми від кількох десятків доларів. Більш

складні інструменти типу Webinject дозволяють вбудовувати шкідливий код безпосередньо в браузер жертви під час відвідування банківських сайтів — жертва бачить звичний інтерфейс, але насправді взаємодіє зі шкідливим шаром.

Послуги з вербування та «грошові мули»

Вербування звичайних людей для участі у злочинних схемах — окрема спеціалізація. Так звані «грошові мули» фізично знімають готівку із зламаних рахунків або отримують переказ на власний рахунок, а потім пересилають кошти далі по ланцюжку відмивання. Частину цих людей свідомо вербують на підпільних форумах; інші стають жертвами шахраїв, які пропонують «легкий заробіток».

Рівень другий: дистрибуція та доставка атак

Навіть найдосконаліше шкідливе програмне забезпечення марне без механізму доставки. Саме тому дистрибуція — окремий сегмент підпільного ринку з власними спеціалістами та сервісами.

Спам- та фішингові кампанії залишаються найпоширенішим інструментом початкового проникнення. За даними ENISA, фішинг є домінуючим вектором злому в 60% задокументованих інцидентів у Євросоюзі. Окремі групи спеціалізуються виключно на масових розсилках — вони не розробляють шкідливе ПЗ і не монетизують дані, їхній «продукт» — це охоплення аудиторії.

Ще одна ключова категорія — завантажувачі або «лоадери» (loaders). Це угруповання, які вже контролюють заражені пристрої і пропонують «встановити» шкідливе ПЗ іншої групи у вже скомпрометованій мережі. Фактично це послуга субпідряду: одна група будує плацдарм, інша — його використовує для власних цілей.

Exploit-кити — набори для автоматичної експлуатації вразливостей у браузерах та плагінах — дозволяють заражати пристрої жертв без будь-якої взаємодії з їхнього боку: достатньо просто відвідати скомпрометований сайт. Трафік на такі сайти перенаправляється через зламані легітимні веб-ресурси, що ускладнює виявлення.

Рівень третій: монетизація — перетворення злому на гроші

Зламати мережу — лише половина справи. Наступна задача — конвертувати здобуті дані чи доступ у реальні кошти, залишаючись при цьому невиявленим. Монетизація — найрізноманітніший сегмент кіберзлочинної екосистеми.

Кардингові форуми залишаються основним ринком збуту викрадених платіжних даних. Ціна залежить від типу картки, країни та наявності повного «дампу» з CVV-кодом. Окремі сервіси перевірки карток дозволяють автоматично верифікувати дійсність тисяч номерів за лічені хвилини.

Відмивання грошей еволюціонувало разом із криптовалютою. «Міксери» та «тумблери» — сервіси, що перемішують криптотранзакції для приховування їхнього походження, — стали стандартним інструментом. За даними Chainalysis, загальний обсяг криптозлочинності у 2024 році перевищив $51 млрд. Паралельно існують мережі підставних компаній для відмивання коштів через легальні банківські канали.

«Шахрайський перепродаж» — схема, за якої викрадені кошти конвертуються в реальні товари (зазвичай електроніка, ювелірні вироби або автомобілі), які потім перепродаються за готівку. Це ускладнює відстеження: гроші «очищаються» через легальний товарний ринок.

Вимагання — ще одна форма монетизації, що вийшла далеко за межі класичного ransomware. Сьогодні поширена «подвійна атака»: зашифрувати дані і водночас погрожувати їх публікацією. Деякі угруповання повністю

відмовились від шифрування й займаються виключно крадіжкою та шантажем — це простіше й так само прибутково.

Новий вимір: штучний інтелект як підсилювач злочинності

П’ять років тому ШІ у кіберзлочинності був екзотикою. Сьогодні він вбудований у підпільну екосистему як стандартний інструмент. Дослідники Trend Micro зафіксували принципову зміну: злочинці більше не будують ШІ-інструменти самостійно — вони купують готові сервіси або зламують легальні платформи.

Jailbreak-as-a-Service — окремий сегмент ринку: постачальники продають методи обходу захисту комерційних мовних моделей (ChatGPT, Claude, Gemini) для генерації фішингових листів, сценаріїв соціальної інженерії та шкідливого коду. На підпільних маркетплейсах також продають скомпрометовані акаунти ChatGPT і Claude — для масової автоматизації або обходу санкційних обмежень (актуально для росії, Ірану та Північної Кореї, де доступ до цих сервісів заблоковано).

Дипфейк-технології перетворились із курйозу на інструмент корпоративного шахрайства. Зафіксовані випадки, коли зловмисники підробляли відео- та аудіозвернення керівників компаній, щоб змусити фінансових співробітників здійснити великі перекази. Оцінка загроз Europol за 2025 рік прямо попереджає: злочинні угруповання дедалі активніше використовують генеративний ШІ для масштабування фішингу та шахрайських операцій.

Паралельно з’являються перші зразки шкідливого ПЗ, що динамічно генерують власний код за допомогою вбудованих мовних моделей — адаптуючись до конкретного середовища та ускладнюючи виявлення. Поки що ці техніки залишаються нішевими через нестабільність і залежність від зовнішніх API, але тенденція зафіксована.

Нова інфраструктура: Telegram замінив даркнет

Якщо п’ять років тому основним майданчиком підпільної торгівлі були анонімні форуми в мережі Tor та даркнет-маркетплейси, то сьогодні центр ваги змістився в бік Telegram. Дослідження компанії Cyfirma підтверджує: Telegram став основною платформою для хакерів.

Масштаби вражають. Лише через одну групу в Telegram — Huione Guarantee — з 2021 по 2025 рік пройшло $27 млрд транзакцій, пов’язаних із незаконною діяльністю. Це перевищує обіг найвідоміших даркнет-маркетплейсів за всю їхню історію. Коли в травні 2025 року Telegram заблокував цей канал, його місце миттєво зайняли клони — і за лічені місяці новий канал досяг обігу в $1,1 млрд.

Telegram приваблює злочинців з кількох причин: відносна анонімність, можливість створювати великі закриті групи, зручна інтеграція з криптовалютними ботами та значно нижча технічна складність порівняно з Tor. Продаж зламаних баз даних, кредитних карток, інструментів для кіберзлочинності, вербування «грошових мулів» — все це відбувається у відкритих і закритих каналах із мінімальною модерацією.

Після арешту Павла Дурова у Франції в серпні 2024 року Telegram оголосив про передачу правоохоронним органам даних користувачів, які займаються незаконною діяльністю. У 2024 році платформа заблокувала понад 15,3 млн каналів і груп. Попри це, за спостереженнями дослідників, кіберзлочинна активність у Telegram продовжує зростати.

Чому таргетування постачальників ефективніше, ніж переслідування виконавців

Відстежити всі зв’язки між угрупованнями та їхніми постачальниками — завдання надскладне через широке використання зашифрованих каналів зв’язку та криптовалюти. Однак аналітична компанія Chainalysis ще в 2021 році сформулювала принцип, який залишається актуальним: правоохоронні

органи досягають кращих результатів, якщо атакують спільну інфраструктуру, а не кінцевих виконавців.

Логіка проста: знищити один RaaS-сервіс означає одночасно вивести з ладу десятки угруповань, які ним користувались. Зламати мережу «куленепробивного» хостингу — позбавити інфраструктури цілий кластер злочинних операцій. Цей підхід показав реальні результати: операції проти інфраструктури Emotet (2021), LockBit (2024) та ALPHV/BlackCat (2024) завдали значно більших збитків кіберзлочинній екосистемі, ніж точкові арешти окремих хакерів.

Є й інша перевага: постачальники підпільних послуг зазвичай мають слабшу операційну безпеку, ніж найбільші злочинні угруповання. Їхні «сліди» залишаються в даних, які потім допомагають ідентифікувати клієнтів вищого рівня.

Контекст для України

Україна перебуває в специфічному положенні: вона є одночасно і мішенню найактивніших у світі державних хакерів, і країною, де кіберзахист перетворився на питання національної безпеки. Важливо розуміти: між «комерційною» кіберзлочинністю та державними кібератаками — насамперед з боку росії — межа часто розмита.

Дослідження Trend Micro характеризує російськомовну кіберзлочинну екосистему як «найсофістикованішу та найстійкішу у світі». Частина угруповань, що формально є «комерційними», фактично діє в інтересах або за замовленням спецслужб — особливо в контексті повномасштабного вторгнення в Україну. CERT-UA регулярно фіксує атаки з використанням тих самих інструментів і інфраструктури, що їх продають на підпільних маркетплейсах.

Джерело: Cybercalm

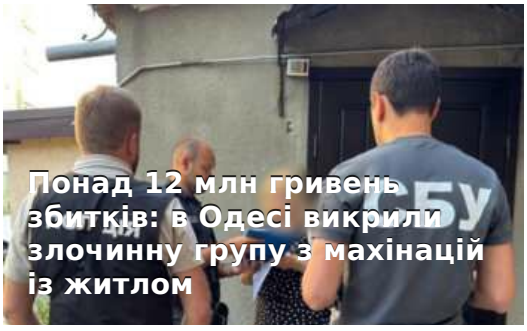
Антон Бабич
РЕДАКТОР

Координує роботу редакції та відповідає за оперативність публікацій. Раніше працював у провідних українських виданнях та на телеканалах.

Теги: Кібершахрайство | Події | Штучний інтелект (ШІ) | месенджер | Даркнет | Telegram | ВВП | хакери

Читайте по темі:

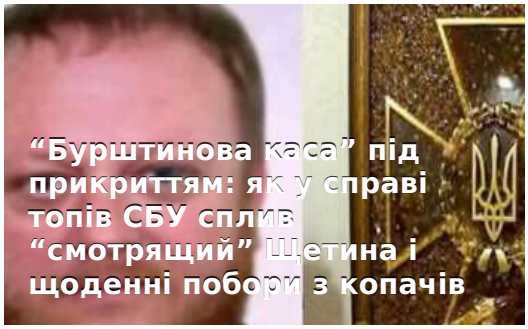
Схема «швидкою до кордону»: на Закарпатті викрили незаконний виїзд ухилянтів



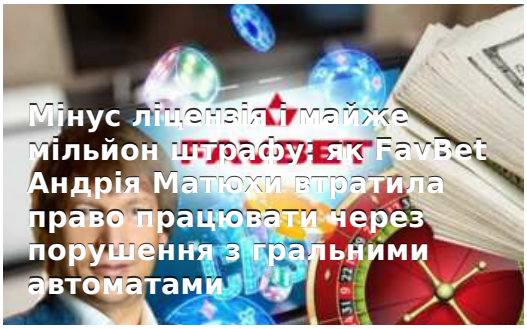
Понад 12 млн гривень збитків: в Одесі викрили злочинну групу з махінацій із житлом

Напад на підлітка та бійка з охороною: у Святопетрівському затримали трьох чоловіків за побиття 14-річного хлопця

У столиці Ford Explorer протаранив антипаркувальний обмежувач і почав «дрифтувати» біля житлового комплексу

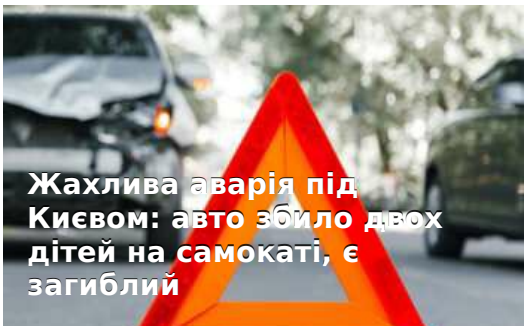


“Бурштинова каса” під прикриттям: як у справі топів СБУ сплив “смотрящий” Шетина і щоденні побори з копачів



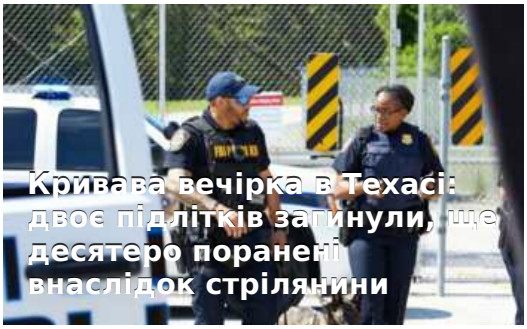
Мінус ліцензія і майже мільйон штрафу: як FavBet Андрія Матюхи втратила право працювати через порушення з гральними автоматами

FoxCloud, ein in Transnistrien betriebenes Hostingnetzwerk mit UK-Fassade, ermöglicht Piraterie, Proxy-Dienste und mutmaßliche Cyberangriffe in Europa



Жахлива аварія під Києвом: авто збило двох дітей на самокаті, є загиблий

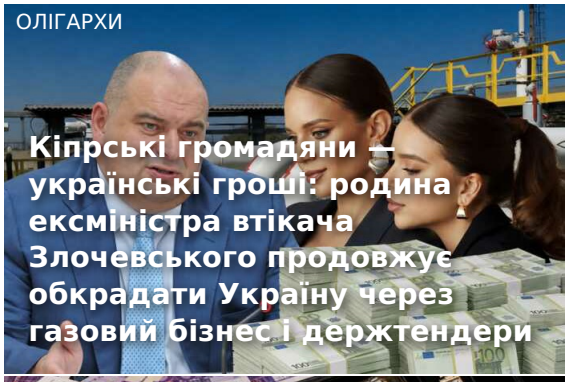
У Харкові судитимуть 17-річного юнака за серію підпалів військових авто



Кривава вечірка в Техасі: двоє підлітків загинули, ще десятеро поранені внаслідок стрілянини

Коментарі:

comments powered by Disqus

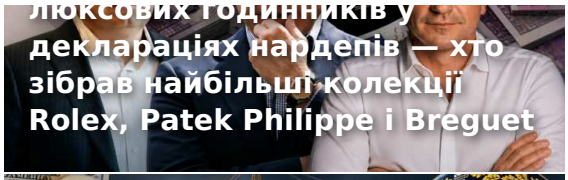


ОЛІГАРХИ

Кіпрські громадяни — українські гроші: родина ексміністра втікача Злочевського продовжує обкрадати Україну через газовий бізнес і держтендери

ДЕПУТАТИ

Від Григорія Суркіса до Миколи Тищенка: сотні



Люксових годинників у деклараціях нардепів — хто зібрав найбільші колекції Rolex, Patek Philippe і Breguet

ПРОКУРОРИ

Porsche, новобудова і “подарунки”: як родина прокурорів Коркунів накопичує елітні активи під час війни

04.05.2026, 20:45 •
Події

10,5 трильйонів доларів на рік: глобальний ринок цифрового розбою перегнав економіки більшості країн

04.05.2026, 20:30 •
Війна

«Це нечесно»: Зеленський відповів на пропозиції РФ про припинення вогню на один день

04.05.2026, 20:27 •
Силовики

Суд заарештував трьох бійців батальйону "Вовки Да Вінчі" у справі про викрадення чоловіка

04.05.2026, 20:18 •
Корупція

«Проєкт 23» і «Манхеттен»: як Цукерман і Мужель через «плівки Міндича» засвітили мережу смотрящих у енергетиці, зерні та оборонці

04.05.2026, 20:15 •
Події

From an international scam to “reputation laundering”: former Rocket investor Timur Rokhlin suppresses investigations and expands a shadow empire

04.05.2026, 20:09 •
Корупція

“Режим стерти все”: як Павло Щербань і Ростислав Шурма зачищають інтернет від інформації про корупційні схеми банку “Альянс”

04.05.2026, 19:42 •
Чиновники

АРМА під керівництвом Ярослави Максименко: питання до управління активами, затримок із поверненням коштів і прозорості фінансових операцій

04.05.2026, 19:39 •
Бізнесмени

Міскодинг, криптовалюта і офшори: як власник FavBet Андрій Матюха побудував схему відмивання сотень мільйонів гривень

04.05.2026, 19:30 •
Силовики

Напад на військових у Соборному районі: у Дніпрі під час заходів оповіщення розстріляли представників ТЦК

04.05.2026, 19:27 •
Корупція

«Алхімія» на митниці: як тонни отруйного метанолу заїжджають в Україну під виглядом розчинників

04.05.2026, 19:27 •
Депутати

В Ізмаїлі вже 6 років судять ексдепутата Якова Воробйова за крадіжку плит на 1 мільйон гривень

04.05.2026, 19:24 •
Олігархи

“London curator” of shadow oil: how Azim Novruzov used Alkagesta and Sumato Energy to move sanctioned Russian crude through Malta

04.05.2026, 19:15 •
Війна

Іран атакував ОАЕ ракетами та дронами, у Фуджейрі палає нафтовий об’єкт

04.05.2026, 19:15 •
Події

Розкрадання на 63 мільйони: у Вінниці викрили схему відчуження майна профспілок

04.05.2026, 17:15 •
Війна

У Запоріжжі СБУ затримала російського агента, який під виглядом пенсіонера

шпигував за позиціями ЗСУ

04.05.2026, 17:12 •
Війна

📷 Удар по святині та ринку: росіяни атакували Вільнянськ дронами, вбивши подружжя

04.05.2026, 17:06 •
Судді

📷 Люксовий автопарк та болгарські апартаменти: що задекларував суддя Олег Непорада

04.05.2026, 17:00 •
Корупція

📷 Нацполіція викрила посадовців ТЦК на незаконному збагаченні на 92 мільйони гривень

04.05.2026, 16:12 •
Події

📷 Схема «швидкою до кордону»: на Закарпатті викрили незаконний виїзд ухилянтів

04.05.2026, 16:03 •
Події

📷 На борту круїзного лайнера в Атлантиці спалахнув хантавірус: щонайменше троє загиблих

04.05.2026, 15:54 •
Події

Понад 12 млн гривень збитків: в Одесі викрили злочинну групу з махінацій із житлом

04.05.2026, 15:54 •
Війна

Цифровий блекаут до «побєди»: у Москві перед парадом вимикають мобільний інтернет і SMS

04.05.2026, 15:45 •
Війна

Путін призначив командувачем ПКС РФ генерала Чайку, обвинуваченого у злочинах у Бучі

04.05.2026, 15:42 •
Силовики

Вирок за «допомогу» з контрактом: у Львові засудили прикордонника, який вимагав 2000 доларів за працевлаштування

04.05.2026, 15:36 •
Події

Нерухомість на 3 мільйони: харківська поліцейська Євгенія Іващенко отримала в подарунок квартиру від батька

04.05.2026, 15:27 •
Події

Відень висилає трьох росіян через шпигунське обладнання на дахах дипустанов

04.05.2026, 15:15 •
Корупція

Дніпро економить на очищенні води: ціна реагентів для «Дніпроводоканалу» впала ще на 21%

04.05.2026, 15:12 •
Бізнесмени

📷 Казино під наглядом «смотрящого»: Андрій Довбенко виявився реальним власником Beton та Slot City

04.05.2026, 15:09 •
Силовики

📷 Ошукали на 275 000 доларів: у Києві викрили криптоаферистів, які обіцяли «безпечні інвестиції»

04.05.2026, 13:39 •
Чиновники

📷 Скромні декларації — мільйонні активи: як Олег Семків і його родина “освоюють” будівельний ринок Франківська