

ук по сайту:



АВТОРСЬКІ НОВИНИ КОМЕНТАРІ СПОРТ КРИМІНАЛ ДУМКА КУЛЬТУРА КОРУПЦІЯ КОНФЛІКТИ

# Держспецзв'язку фіксує зміну тактики хакерів: від стілерів до довгострокової компрометації

07 квітня 2026 р.,  
19:16

Олена Юрченко 525 0



Держспецзв'язку фіксує зміну тактики хакерів: від стілерів до довгострокової компрометації

**Є в Україні один документ, який виходить двічі на рік, якого ніхто не чекає з нетерпінням, але який варто читати уважніше за гороскоп. Це аналітичний звіт CERT-UA — Національної команди реагування на кіберінциденти при Державній службі спеціального зв'язку та захисту інформації.**

Свіжий випуск за друге півріччя 2025 року написаний мовою, якою зазвичай пишуть інструкції до пральних машин — сухо, точно, без емоцій. Але якщо перевести його з бюрократичної на людську, виходить доволі моторошна історія про те, як ціла країна щодня живе під цифровим обстрілом, і чому навіть зменшення кількості «прильотів» — не привід розслабитися.

Розбір звіту CERT-UA за друге півріччя 2025 року для тих, хто не читає PDF-ки від Держспецзв'язку, але, мабуть, мав би.

**Менше інцидентів, більше тривоги**

Головна новина звіту звучить майже оптимістично: вперше з початку повномасштабного вторгнення кількість кіберінцидентів у півріччі зменшилась. Було 3 018 — стало 2 909, мінус чотири відсотки. Жодного критичного інциденту. Інцидентів високого рівня — п'ять замість шести. Здавалось би, відкривай шампанське.

**Читайте по темі:** [Розкрито аферу BitCapital на 5,3 мільйона гривень: позики в крипті оберталися жорстким тиском та погрозами](#)

Але CERT-UA — люди, які шампанське відкривають рідко і з підозрою дивляться на будь-яку пляшку, що шипить. Тому вони одразу пояснюють: зменшення кількості не означає зменшення загрози. Противник не став добрішим і не пішов у відпустку. Він змінив тактику. І ця нова тактика — значно неприємніша за стару.

У першому півріччі 2025-го серед хакерських угруповань була популярна модель, яку аналітики охрестили «Steal & Go» — вкради й тікай. Зловмисник закидав жертві стілер (програму для крадіжки даних), вичавлював з комп'ютера все цінне за кілька хвилин і зникав, не залишаючи слідів. Швидко, ефективно, мінімальний ризик виявлення. Щось на кшталт кишенькової крадіжки в метро: поки ви помітили — злодій уже на іншій станції.

У другому півріччі модель змінилась. Тепер хакери не тікають. Вони заходять, озирються, знаходять зручне місце і залишаються. CERT-UA фіксує зміщення акценту з одноразового викрадення інформації на отримання стійкого несанкціонованого доступу. Іншими словами, замість «вкради й тікай» — «зайди й живи». Компрометація перестала бути подією і стала початком тривалих стосунків. Без згоди другої сторони, зрозуміло.

### **Вони повертаються**

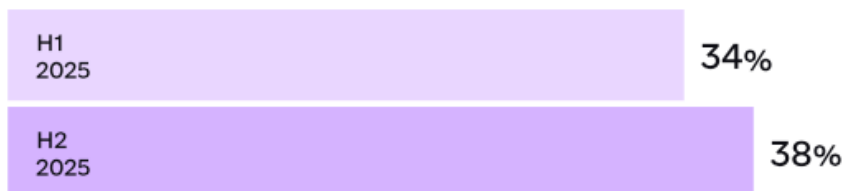
Окремий розділ звіту присвячений явищу, яке будь-який IT-фахівець зустрине з нервовим посмикуванням ока. Зловмисники повертаються до раніше скомпрометованих систем. Не тому, що забули щось вкрати. А тому, що хочуть перевірити: чи ви усунули причину зламу, чи просто перезавантажили сервер і помолились?

І часто з'ясовується, що помолились. CERT-UA делікатно формулює це як «неповне усунення причин попереднього інциденту». Менш делікатно це звучить так: організація пережила кібератаку, відновила працездатність системи, видихнула і вирішила, що все минулося. А через місяць ті самі хакери зайшли через ту саму діру, яку ніхто не залатав. Це не гіпотетичний сценарій — це реальні випадки з українського кіберпростору другого півріччя 2025 року.

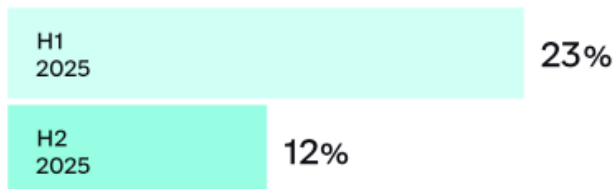
### **Хто по кого приходять**

Четвірка головних мішеней залишається незмінною і виглядає саме так, як ви очікуєте від країни, що перебуває у стані війни. Урядові організації — 38 відсотків усіх інцидентів (було 34). Місцеві органи влади — 23 відсотки (було 20). Сектор безпеки та оборони — 6 відсотків у статистиці CERT-UA, але ця цифра — лукава, бо значна частина атак на військових опрацьовується кіберпідрозділами ЗСУ і в цю статистику просто не потрапляє. Енергетичний сектор тримається на четвертому місці з 4 відсотками.

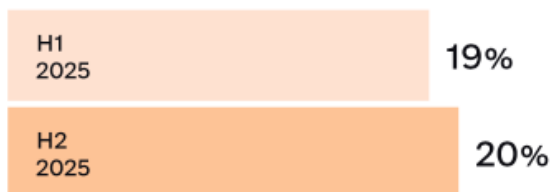
### Місцеві органи влади



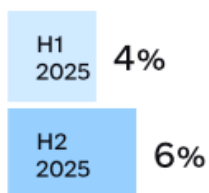
### Сектор безпеки та оборони



### Урядові організації



### Енергетичний сектор



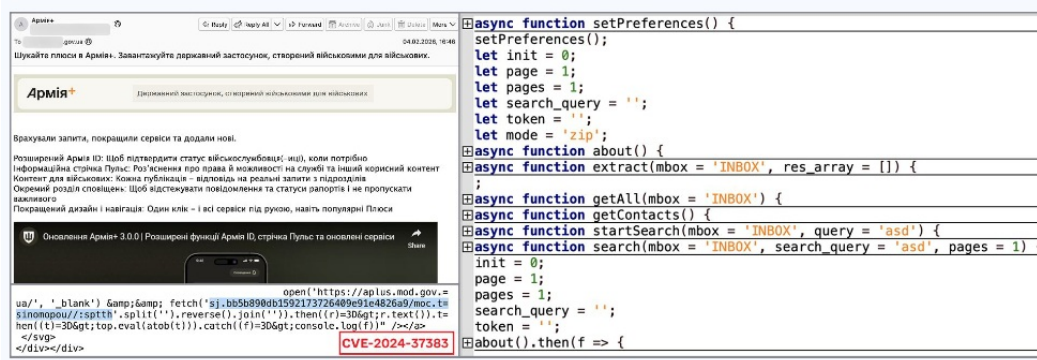
Цікаво інше: попри те, що розсилки шкідливого програмного забезпечення стало більше, кількість реальних заражень зменшилась. Люди, виявляється, поступово вчаться не клікати на все, що блимає. Три з половиною роки війни — непоганий курс цифрової грамотності, хоча й дещо дорогий.

**Читайте по темі:** [Прокуратура викрила продаж майна «Київського радіозаводу» за ціною, в 20 разів нижчою за ринкову](#)

### Нові обличчя, старі наміри

Звіт фіксує появу нових кластерів кіберзагроз — у класифікації CERT-UA кожне хакерське угруповання отримує код UAC з порядковим номером. У другому півріччі з'явилися кілька «новачків», хоча слово «новачок» тут звучить так само недоречно, як «початківець» стосовно кишенькового злодія з двадцятирічним стажем.

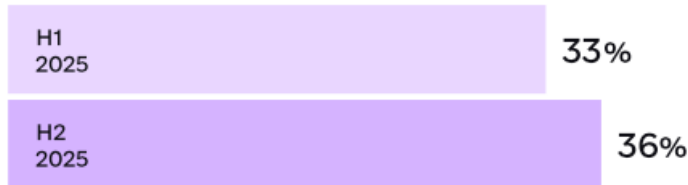
Особливу тривогу викликають так звані zero-click атаки — ті, де жертві навіть не треба нічого натискати. Достатньо просто отримати листа. Угрупування UAC-0233 та UAC-0250 експлуатували вразливості поштових серверів Roundcube та Zimbra, які дозволяли виконувати шкідливий код без будь-якої взаємодії з боку користувача.



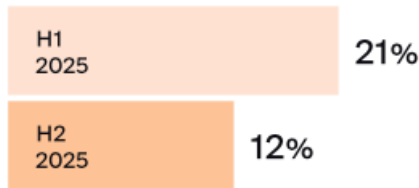
## Приклад активності UAC-0233

Лист приходиться, код виконується, поштова скринька — включно з листуванням, резервними кодами двофакторної автентифікації та пароллями застосунків — пакується в архів і відправляється зловмисникам. Жертва при цьому навіть не підозрює, що щось відбулося. Це як обікрасти квартиру, поки господар сидить у вітальні і дивиться серіал.

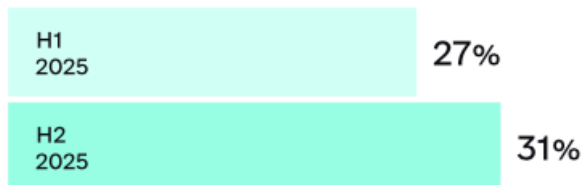
### 02.02 Розповсюдження ШПЗ (Malware distribution)



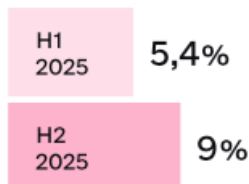
### 02.01 Зараження ШПЗ (Malware infection)



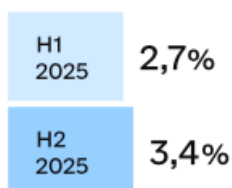
### 03.03 Фішинг (Phishing)



### 05.01 Компрометація облікового запису (Account Compromise)



### 05.02 Компрометація системи (System Compromise)



Повернулись і кібервимагачі — ті, хто шифрує ваші файли і вимагає гроші за розшифрування. UAC-0238 з липня 2025 року атакував органи місцевого

самоврядування за допомогою програм-вимагачів сімейства Proton. Точкою входу слугував старий добрий RDP, виставлений в інтернет — те, про що кібербезпековці кричать останні десять років, але що й досі стирчить назовні в половині українських держустанов, як незачинені двері підвалу.

Друге угруповання вимагачів, UAC-0243, використовувало варіацію сумнозвісного LockBit 3.0 під назвою X2anylock (або Warlock). Заходили через вразливі сервери Microsoft SharePoint, а для горизонтального переміщення мережею використовували абсолютно легітимні інструменти — Cloudflare Tunnel, Velociraptor та RClone. Тобто зламували вас за допомогою тих самих програм, якими ви, можливо, й самі користуєтесь. Аналогічні атаки CERT-UA фіксує проти держорганів Португалії, Хорватії та Туреччини — Україна в цьому клубі потрапила не за власним бажанням, а за географічним принципом: якщо ви в зоні інтересів російських спецслужб, вам рано чи пізно придуть.

### **WinRAR, яким б'ють двічі в одну воронку**

Є в цьому звіті деталь, від якої хочеться одночасно сміятись і плакати. Одна з найпоширеніших технік другого півріччя — експлуатація вразливості WinRAR з кодом CVE-2025-8088. Для тих, хто не стежить за кібербезпекою щоденно: WinRAR — це програма для розпакування архівів, якою в Україні користуються приблизно всі, і яка вже котрий рік є улюбленою «дверима» для хакерів.

Вразливість дозволяє при розпакуванні архіву непомітно створити додатковий файл у директорії автозавантаження Windows. Тобто ви розпаковуєте нібито нешкідливий архів з документом, а десь у надрах системи тихенько з'являється файл, який запуститься при наступному включенні комп'ютера. Інформацію про вразливість оприлюднили в серпні, а вже з вересня почались масові розсилки з експлойтами. Першим цю діру використало угруповання UAC-0010 (воно ж Gamaredon, воно ж — структурний підрозділ ФСБ Росії, розташований у тимчасово окупованому Криму). Потім підтягнулись UAC-0002, UAC-0226 та інші. Ефективна вразливість в екосистемі російських хакерських груп поширюється зі швидкістю вірусного відео — хтось знайшов, усі скопіювали.

Той самий UAC-0010, відомий своєю параноїдальною наполегливістю — на одному зараженому комп'ютері він створює більше сотні шкідливих файлів у різних директоріях — у 2025 році освоїв ще й альтернативні потоки даних (Alternate Data Streams, ADS). Це штатна функція файлової системи NTFS, яка дозволяє зберігати додаткові дані, прив'язані до файлу. Фішка в тому, що ці потоки не видно у звичайному провіднику Windows. Файл може мати розмір 0 байт і виглядати абсолютно порожнім, але в його альтернативному потоці буде сидіти повноцінний шкідливий код. Це як подвійне дно у валізі, тільки цифрове.

### **Коли хакер дзвонить по телефону**

Але найелегантнішою — і найнебезпечнішою — зміною другого півріччя стала еволюція соціальної інженерії. Тут варто процитувати звіт дослівно в одному реченні, бо воно заслуговує на те, щоб його повісити на стіну кожного кібербезпековця: «Первинна взаємодія з об'єктами атак дедалі частіше здійснюється з використанням телефонних номерів українських мобільних операторів і легітимних облікових записів».

Розшифровую. Російські хакери — зокрема APT28 (вони ж UAC-0001, вони ж підрозділ ГУ Генштабу ЗС РФ, тобто військова розвідка) та Void Blizzard (UAC-0190) — тепер не просто надсилають фішинговий лист з вкладенням. Вони спершу дзвонять. З українського номера. Розмовляють українською. Використовують аудіо- та відеозв'язок. Демонструють знання про конкретну людину та організацію. Встановлюють довіру. І лише потім, після живого спілкування, надсилають у месенджер «службовий документ» — XLS-файл

із макросом, який відкриває двері у вашу систему.

APT28 провело таким чином масштабну кібероперацію проти українських військовослужбовців та працівників підприємств оборонно-промислового комплексу. Файл був замаскований під службову документацію. Жертва отримувала його не від невідомого відправника, а від «колеги», з яким щойно розмовляла по телефону. Рівень довіри — максимальний. Рівень підозри — нульовий.

Це якісний стрибок. Від масових фішингових розсилок, де один лист з тисячі «вистрілить», — до точкових операцій, де кожна атака підготовлена індивідуально, з розвідкою, легендою та акторською грою.

Кіберспецоперації дедалі більше нагадують класичну розвідку: вербувальний підхід, встановлення контакту, формування довіри, отримання доступу.

### **Скомпрометовані роутери як зброя**

Ще один тривожний тренд — використання скомпрометованих українських пристроїв як проміжних вузлів для атак. Угруповання UAC-0002 (Sandworm, він же підрозділ ГРУ, відповідальний за найбільш деструктивні кібератаки в історії України) після компрометації об'єкта критичної інфраструктури було виявлено завдяки моніторингу спроб повторної автентифікації у вже змінені облікові дані. Спроби підключення йшли з українських IP-адрес, і всі ці адреси мали спільну рису — публічно доступну панель адміністрування мережевого пристрою.

Тобто ваш роутер з паролем admin/admin або з незакритою адмін-панеллю може прямо зараз працювати як проміжний вузол у ланцюзі атаки російської військової розвідки на українську критичну інфраструктуру. Хакери вмикали на таких пристроях SOCKS-проксі та SSH-тунелювання, перетворюючи побутовий роутер на елемент наступальної кіберінфраструктури. Щоб ускладнити відстеження, використовувались ланцюги з кількох таких пристроїв — щось на кшталт цифрової версії «естафети», де кожен вузол знає лише попередній і наступний.

### **Що з усього цього впливає**

Звіт CERT-UA — це не паніка і не алармізм. Це холодна фіксація реальності, в якій Україна живе вже четвертий рік. Кіберпростір залишається повноцінним театром воєнних дій, де щодня відбуваються тисячі зіткнень, про які не пишуть у зведеннях Генштабу, але які можуть мати наслідки не менш серйозні, ніж ракетний удар по енергоінфраструктурі.

Позитив є: кількість інцидентів вперше знизилась, заражень стало менше при більшій кількості розсилок, критичних інцидентів не було. Українські організації поступово адаптуються — десь краще налаштували захист, десь працівники нарешті навчилися не відкривати підозрілі файли.

Але негатив переважає. Противник стає розумнішим, терплячішим і винахідливішим. Він більше не б'є наманя — він цілиться. Він більше не тікає після крадіжки — він оселяється. Він більше не пише корявих фішингових листів з помилками — він телефонує вам особисто, називає по імені і знає, в якому підрозділі ви служите.

І поки WinRAR залишається на кожному другому комп'ютері держслужбовця, поки RDP стирчить в інтернет з паролем «qwerty123», поки після кіберінциденту обмежуються перезавантаженням замість повноцінного розслідування — ці 2 909 інцидентів за півріччя будуть не зменшуватись, а зростати. Бо противник вчиться швидше, ніж ми латаємо діри.

А якщо вам здається, що все це вас не стосується, бо ви не працюєте ні в уряді, ні в армії, — перечитайте абзац про роутери. Той сірий прямокутник з антеною, що стоїть у вас під телевізором, прямо зараз може працювати на

ворога. І він, на відміну від WinRAR, навіть ліцензії не потребує.

Автор: **Олексій Федоров** для УК

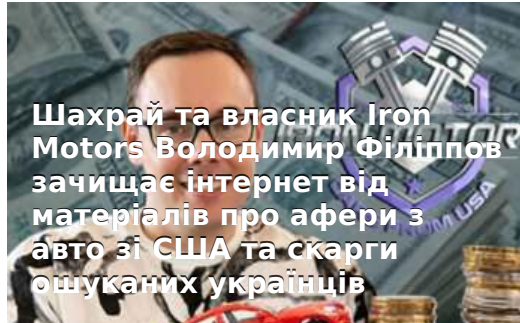
Теги: [CERT-UA](#) [Держспецзв'язку](#) [рос](#) [Кібершахрайство](#) [Шахрайство](#)  
[кібератаки](#) [Російські хакери](#) [хакери](#)

[< Попередня новина](#) [Наступна новина >](#)

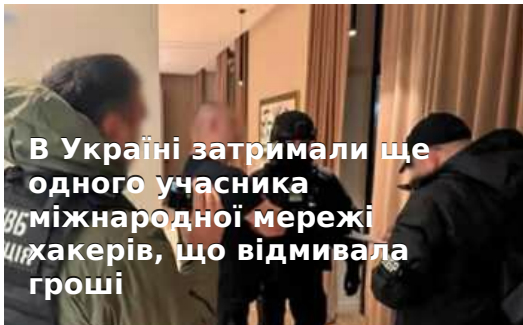
## Читайте по темі:



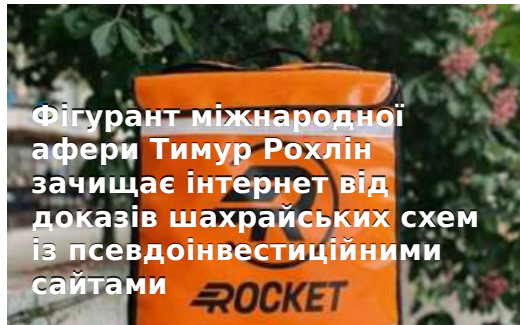
**В Україні викрили масштабну схему привласнення та продажу квартир померлих і самотніх людей**



**Шахрай та власник Iron Motors Володимир Філіппов зачищає інтернет від матеріалів про афери з авто зі США та скарги ошуканих українців**



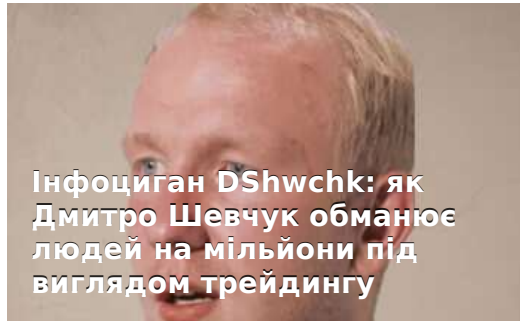
**В Україні затримали ще одного учасника міжнародної мережі хакерів, що відмивала гроші**



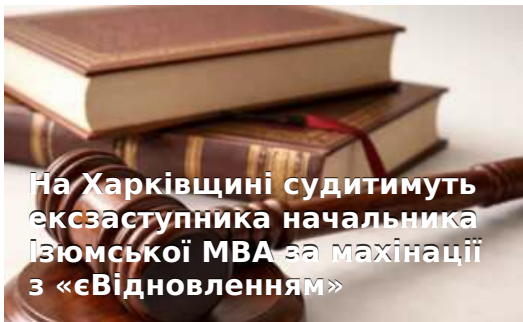
**Фігурант міжнародної афери Тимур Рохлін зачищає інтернет від доказів шахрайських схем із псевдоінвестиційними сайтами**



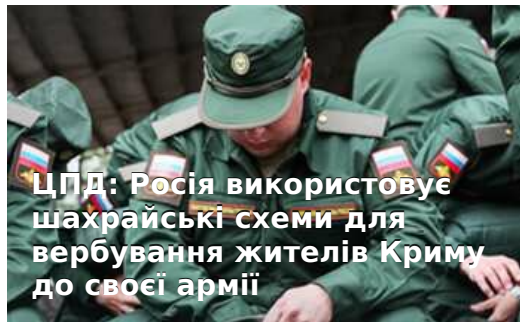
**Масштабні махінації в освіті: керівницю ліцею в Києві обвинувачують у незаконних виплатах на 8 мільйонів**



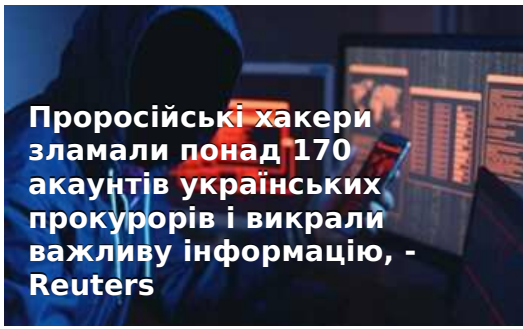
**Інфоциган DShwchk: як Дмитро Шевчук обманює людей на мільйони під виглядом трейдингу**



**На Харківщині судитимуть ексзаступника начальника Ізюмської МВА за махінації з «Відродженням»**



**ЦПД: Росія використовує шахрайські схеми для вербування жителів Криму до своєї армії**



## Коментарі:

comments powered by [Disqus](#)

## ОСТАННІ НОВИНИ



17.04.2026, 13:56 •  
Новини

**Мільйони в кеші при скромних доходах: родина чиновника Держпраці Віктора Шайтана задекларувала 305 тисяч доларів і десятки об'єктів нерухомості**



17.04.2026, 13:52 •  
Корупція

До 30% «відкатів» на дронах і РЕБ: НАБУ завершило справу проти Гайдая, Кузнецова та командування Нацгвардії



17.04.2026, 13:51 •  
Кримінал

Розкрито аферу BitCapital на 5,3 мільйона гривень: позики в крипті оберталися жорстким тиском та погрозами



17.04.2026, 13:39 •  
Новини

Шахрайство на 10 мільйонів євро і розкішне життя: як експіввласник Rocket Тимур Рохлін виманював гроші інвесторів і скуповував VIP-активи



17.04.2026, 12:57 •  
Війна

Росіяни завдали удару по Харкову, є постраждалих



17.04.2026, 12:55 •  
Новини

Молдова оголосила персонами нон грата керівництво армії РФ у Придністров'ї



17.04.2026, 12:11 •  
Війна

**Чернігівська ТЕЦ призупинила роботу після нічної атаки РФ: у місті немає гарячої води**



17.04.2026, 12:03 •  
Війна

**ISW: Росія використала «великоднє перемир'я» для накопичення ракет для масованих ударів**



17.04.2026, 11:46 •  
Корупція

Пільгові тарифи в портах і кримінальні справи: як бізнесмен Дмитро Коваленко через «Гранову» захоплює аграрний ринок після заробітків на російському вугіллі



17.04.2026, 11:43 •  
Корупція

**7 років тюрми за «золоті» овочерізки: керівницю Київської РДА Ольгу Дроздову засудили за розкрадання на укриттях**



17.04.2026, 11:19 •  
Новини

**США повністю вивели війська із Сирії: контроль над територіями передано новому уряду**



17.04.2026, 09:50 •  
Корупція

**📷 Мільйонна зарплата — нуль заощаджень: як прокурор Сергій Дейнека приховує витрати на житло і живе «в борг» у колег**



17.04.2026, 09:47 •  
Війна

**Нічна атака на Чернігів: ворог поцілів по критичній інфраструктурі, виникли пожежі**



17.04.2026, 09:46 •  
Корупція

**Тисячі фейкових КЕП для окупованих територій: у Києві засудили податківцю, яка зливала дані пенсіонерів і відкривала доступ до їхніх рахунків**



17.04.2026, 09:43 •  
Новини

**Паливна криза: у Європі запасів авіаційного палива вистачить лише на шість тижнів**



17.04.2026, 09:35 •  
Корупція

**📷 Хабар у 4 тисячі доларів, схеми на вирубці лісосмуг і п'яне ДТП: як прокурор Офісу Генпрокурора Максим Олефір роками рятував брата від кримінальної відповідальності**



17.04.2026, 09:29 •  
Війна

**📷 Армія РФ вчора втратила 1000 солдатів та понад 110 артсистем**



17.04.2026, 09:14 •  
Війна

**📷 ППО знешкодила 147 «шахедів», проте частина балістики та дронів досягла цілей на 8 локаціях**



17.04.2026, 09:12 •  
Новини

**Велика Британія може долучитися до участі в кредиті від ЄС для України на 90 мільярдів євро, — ЗМІ**



17.04.2026, 09:10 •  
Війна

**📷 Унаслідок російських обстрілів загорівся Дунайський біосферний заповідник**



17.04.2026, 09:02 •  
Війна

**📷 Росіяни атакували Дніпропетровщину: пошкоджено гімназію, підприємства та будинки, є поранені**



17.04.2026, 08:46 •  
Новини

**Дефіцит арсеналів: США відкладають постачання зброї до Європи та України**



16.04.2026, 23:53 •  
Коментарі

**📷 Зеленський: Нідерланди в червні передадуть Україні протимінний корабель класу Alkmaar**



16.04.2026, 23:50 •  
Війна

**Три сценарії Кремля: у ЦПД розповіли про плани РФ щодо війни в Україні та конфлікту з НАТО**



16.04.2026, 23:47 •  
Новини

**📷 Особистий духівник зрадника Медведчука досі живе у Києво-Печерській Лаврі та хрестив доньку Чернишова**



16.04.2026, 23:45 •  
Війна

**Окупаційний «суд ЛНР» засудив громадянина Польщі до 13 років колонії за службу в ЗСУ**



16.04.2026, 23:22 •  
Авторські

**📷 📺 Нардеп від забороненої ОПЗЖ Віталій Борт під час війни провів майже 3 місяці у Маямі під виглядом відряджень, а пов'язаний із ним бізнес в окупації платить податки до бюджету РФ**



16.04.2026, 23:18 •  
Новини

**Вибори в Болгарії можуть привести до влади проросійські сили, — Reuters**



16.04.2026, 23:16 •  
Новини

**📷 Ізраїль відпустив російське судно з викраденим українським зерном**



16.04.2026, 23:15 •  
Корупція

**Прокуратура викрила продаж майна «Київського радіозаводу» за ціною, в 20 разів нижчою за ринкову**

ХАБ

