ЗВІТ
Національної поліції України
про стан виконання заходів з питань забезпечення кібербезпеки держави у 2025 році

З метою виконання вимог Закону України «Про основні засади забезпечення кібербезпеки України» (далі – Закон) та Стратегії кібербезпеки України, Національна поліція України як один із основних суб'єктів національної системи кібербезпеки звітує про стан виконання заходів з питань забезпечення кібербезпеки держави, віднесених до її компетенції.

Так, Національна поліція України (далі – Національна поліція) відповідно до Закону в установленому порядку виконує такі основні завдання: забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі, здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі.

Суспільно-політична ситуація, зокрема повномасштабна збройна агресія рф, зумовила суттєве зростання попиту на соціальну допомогу, гуманітарні та військові товари. Указані обставини стали сприятливим підґрунтям для активізації кіберзлочинності. Інформаційні технології є невід'ємною складовою функціонування економічних, соціальних, управлінських та комунікаційних процесів у державі та суспільстві. Водночас стрімкий розвиток цифрового середовища несе не лише позитивні можливості, а й створює умови для вчинення протиправних дій.

У таких умовах особливої актуальності набуває питання протидії злочинам, пов'язаним з віртуальними активами, які формують один із найдинамічніших та найскладніших сегментів сучасної кіберзлочинності. Цей вид протиправної діяльності розвивається пропорційно до зростання цифрової економіки та популярності криптовалютних технологій.

Віртуальні активи (зокрема Bitcoin, Ethereum, Tether, а також нові токени, DeFi-протоколи, NFT та стейблкоїни) дедалі частіше використовуються не лише як інструмент інвестування чи розрахунків, а й як засіб легалізації незаконних доходів, фінансування злочинної діяльності та ухилення від фінансового контролю.

Основна складність полягає в децентралізованій природі блокчейн-технологій. Відсутність центрального адміністратора або регулятора унеможливлює повноцінний контроль за транзакціями та ідентифікацію їхніх учасників. У більшості публічних блокчейнів відображаються лише адреси гаманців, які не мають прямого зв'язку з особою користувача. Це створює передумови для анонімності або псевдоанонімності фінансових операцій.

Крім того, глобальний характер цифрових мереж дозволяє злочинцям здійснювати транзакції через юрисдикції з різними правовими режимами регулювання криптоактивів. Це ускладнює розслідування, оскільки відстеження коштів потребує міжнародної співпраці, судових запитів і доступу до даних

провайдерів, які часто розташовані в інших державах або діють поза правовим полем.

Кіберзлочинність завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до технологій та призводить до значних репутаційних та матеріальних втрат. Набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки. Агресія з боку рф відбувається не тільки у вигляді військових дій, але й у вигляді кібервійни.

24 лютого 2022 року радикально змінився ландшафт загроз, з якими стикається Україна. Агресія відбувається на всіх фронтах, зокрема й кіберсфері. Ворог не відмовився від ідеї паралізувати ІТ-системи державного та приватного сектору, проводити акції саботажу та диверсій проти об'єктів критичної інфраструктури, ускладнювати функціонування ІТ-складових системи оборони країни.

Активними залишаються фінансово мотивовані угрупування які здійснюють масовані розсилки електронних листів, що містять шкідливе програмне забезпечення, що використовується для завантаження і запуску на комп'ютерах інших програм та модулів, що забезпечують можливість подальшого дослідження інфікованих пристроїв зловмисниками для визначення жертв і прийняття рішення щодо можливості викрадення коштів.

Упродовж 2025 року практична діяльність Національної поліції щодо протидії кіберзлочинності характеризувалася активністю та всебічним підходом, що вплинуло на досягнуті результати.

Так, у 2025 році підрозділами Національної поліції зареєстровано **26,9 тис.** кіберзлочинів, повідомлено про підозру **3,5 тис.** особам у вчиненні **9 тис.** кримінальних правопорушень, до суду з обвинувальним актом скеровано майже **9,1 тис.** кримінальних правопорушень.

Потерпілим забезпечено відшкодування (з урахуванням накладеного арешту та вилученого майна) понад **784,8 млн грн**, що становить **102,39%** від завданих кримінальними правопорушеннями збитків.

Із **583** скерованих до суду обвинувальних актів у кримінальних провадженнях відносно організованих груп та злочинних організацій, виявлених працівниками підрозділів Національної поліції, **72** пов'язані з використанням інформаційно-комунікаційних систем.

У звітному періоді поліцейські активно протидіяли онлайн-шахрайствам та опрацьовували кіберінциденти, за необхідності координуючи свої дії з представниками інших суб'єктів забезпечення кібербезпеки в України, а також з представниками бізнесу та громадянського суспільства.

Слід зауважити, що найпоширенішими на сьогодні різновидами онлайн-шахрайств є недоставка товару / ненадання послуг (продаж неіснуючих товарів), дзвінки від імені представників банків, інших установ та організацій, фішинг, злам акаунтів у соцмережах з подальшим проханням про допомогу.

Загалом у зазначеній сфері поліцейські оголосили підозру майже **1 тис.** осіб та **696** особам правоохоронці вручили обвинувальні акти у вчиненні кримінальних правопорушень, припинили діяльність **21** організованої злочинної групи та організації.

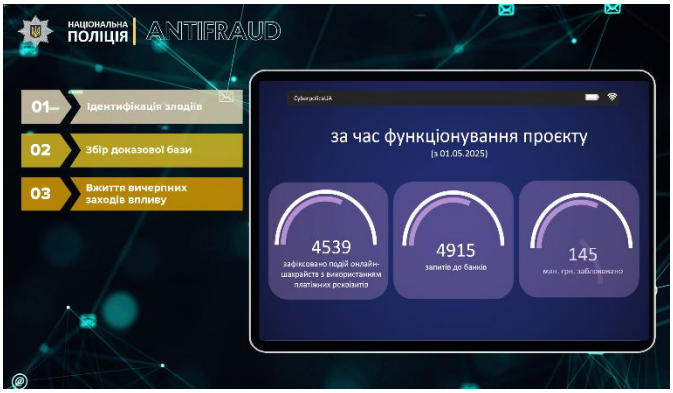
Характерні приклади:

*направлено до суду обвинувальний акт у кримінальному провадженні за **частинами другою - четвертою ст. 27, частиною третьою ст. 28, частиною п'ятою ст. 190, частиною другою ст. 361, частинами першою, другою ст. 255 Кримінального кодексу України** стосовно учасників злочинної організації, які за допомогою Інтернету (соціальні мережі, месенджери) здійснювали розповсюдження фішингових посилань щодо виплат грошової допомоги від Президента України, ООН, UNICEF та інших видів допомоги, що в подальшому давало змогу отримати доступ до електронного кабінету онлайн-банкінгу потерпілих. З метою заволодіння коштами громадян фігуранти здійснювали телефонні дзвінки потерпілим, у ході яких представлися працівниками служб безпеки банківських установ для підтвердження безпечності проведення фінансових транзакцій потерпілими. Крім того, учасники злочинної організації контролювали систему функціонування так званих «дропів», які з метою подальшого виведення коштів, здобутих протиправним шляхом, створили оголошення (ордери) щодо купівлі криптовалюти шляхом p2p-транзакцій у спеціалізованому криптоботі в месенджері «Т» під назвою «С». Від протиправних дій злочинної організації **13 потерпілим** завдано шкоди на загальну суму близько **1,8 млн грн.** Накладено **арешт** на майно фігурантів на суму **2 млн грн;***

*направлено до суду обвинувальний акт у кримінальному проваджені за **частинами четверною, п'ятою ст. 190, частиною другою ст. 255, частиною другою ст. 361 Кримінального кодексу України (53 епізоди)** стосовно злочинної організації у складі **20 осіб.** Протягом 2021-2023 років з метою прикриття злочинної діяльності створили та адміністрували Telegram-канал «Р», зокрема гр. А установив на пустий сервер, Telegram-бот під назвою «@inspireteambot» разом із системою, яка підробляє платформи онлайн-оголошень щодо продажу товарів та вводу банківських карток – надає фішингове (несправжнє) посилання на вебресурс, що візуально копіювало справжнє посилання сервісів доставки товарів, поштових сервісів або банківських установ, і в подальшому надав права доступу та адміністрування до Telegram-бота для створення фішингових посилань, забезпечував технічне обслуговування зазначеного Telegram-бота та контролював його роботу із генерації фішингових посилань, які надавались членам злочинної організації. Так, використовуючи «фішингові» посилання на вебплатформах «S», «B», «V» шахрайським шляхом під приводом здійснення платежів за купівлю або продаж побутових товарів, надання послуг заволодівали коштами громадян України, Польської, Чеської Республік та інших країн Європейського Союзу, у результаті шахрайських дій злочинної групи постраждали 20 осіб, яким спричинено матеріальних збитків на суму понад **1,5 млн грн.** Накладено арешт на майно підозрюваних у сумі **1,9 млн грн.***

Крім того, з метою підвищення ефективності протидії онлайн-шахрайствам створено інноваційний проєкт «**Antifraud**», який є унікальною розробкою Національної поліції України, реалізованою в тісній співпраці з Національним

банком України, іншими банківськими установами та Українською міжбанківською асоціацією членів платіжних систем «ЄМА».



Проєкт «Antifraud» втілює сучасний підхід до запобігання фінансовим правопорушенням, забезпечуючи оперативне виявлення та блокування підозрілих транзакцій, мінімізацію ризиків для громадян і бізнесу, а також високий рівень міжвідомчої взаємодії на національному рівні. На цей час забезпечено функціонування пілотного проєкту «Antifraud» у 12 головних управліннях Національної поліції України в областях та м. Києва.

За час функціонування проєкту (з 01.05.2025) системою зафіксовано 4 539 (за яким сформовано 4 915) запитів до банківських установ.

За результатами вжитих заходів банківськими установами заблоковано кошти в сумі 145 млн грн., які належали потерпілим від онлайн-шахрайств.

У звітному періоді поліцією забезпечено проведення комплексу превентивних заходів, зокрема:

спільно з Національним банком України та Національним центром оперативно-технічного управління мережами телекомунікацій Держспецзв'язку заблоковано 72 803 «шкідливі» домени, що використовувались для створення фішингових посилань;

у співпраці з операторами та провайдерами телекомунікацій держави блокування абонентів IP-телефонії та відпрацювання номерів стільникового зв'язку, які використовуються правопорушниками для дзвінків від імені банківських та державних установ (ужито заходів реагування щодо 597 абонентів мобільного зв'язку та 1 543 абонентських номерів з кодом «044»).

Спільно з іноземними колегами українські поліцейські ініціювали та забезпечили участь у проведенні **22** міжнародних поліцейських операцій. У результаті було нейтралізовано загрозу з боку кількох потужних хакерських об'єднань, злочинна діяльність яких охоплювала країни всього світу.

*Наприклад, у межах проведення міжнародної операції «**Vicarius**» за участі правоохоронних органів Латвійської Республіки задокументовано діяльність організованої злочинної групи, учасники якої створили та координували роботу мережі call-центрів, орієнтованих на громадян держав Європи, зокрема Латвійської Республіки. Метою функціонування зазначених call-центрів було введення потерпілих в оману під приводом залучення інвестицій у криптовалюту через псевдоброкерські платформи. Злочинна діяльність здійснювалася із застосуванням методів соціальної інженерії, IP-телефонії, програмного забезпечення віддаленого доступу з подальшим заволодінням коштами потерпілих в особливо великих розмірах.*

*Задокументовано та підтверджено 19 епізодів злочинної діяльності на загальну суму понад **340 тис. євро.** Повідомлено про підозри 6 учасникам організованої злочинної групи.*

*Накладено арешти на рухоме та нерухоме майно, банківські рахунки та облікові записи на криптовалютних сервісах на загальну суму понад **500 тис. дол. США.***

Міжнародна операція за фактом документування шахрайського угруповання, діяльність якого спрямована на заволодіння коштами громадян України, під приводом пригону транспортних засобів, зокрема для потреб ЗСУ. Проведено ряд обшуків на території України та Республіки Молдова. За результатами реалізації організатора шахрайської схеми затримано та обрано запобіжний захід у вигляді тримання під вартою.

*За координації Європолу задокументовано протиправну діяльність громадянина України, який, використовуючи можливості хостинг-провайдера «**AMAZON WEB SERVICES»,** отримав доступ до більш ніж 5 тис. облікових записів клієнтів AMAZON, на яких розгорнув роботу віртуальних машин для майнінгу криптовалюти, завдавши збитків указаній компанії на суму **4 млн доларів США.***

Крім того, відповідно до пункту 24^1 частини першої статті 23 Закону України «Про Національну поліцію» до завдань поліції належить здійснення протидії злочинним посяганням на об’єкти критичної інфраструктури, які загрожують безпеці громадян і порушують функціонування систем життєзабезпечення; захист об’єктів критичної інфраструктури, інтересів суспільства і держави від злочинних посягань у кіберпросторі, запобігання, виявлення, припинення та розкриття кіберзлочинів проти об’єктів критичної інфраструктури.

Так, з метою захисту власної інфраструктури в Національній поліції України на постійній основі здійснюються заходи із моніторингу стану кібербезпеки із застосуванням упроваджених безпекових рішень, зокрема Cisco Gateway C300, Cisco Secure Endpoint, ESET Endpoint Security, ESET Server Security, Anti DDoS, CrowdStrike, Cloudflare.

У межах централізації захисту робочих станцій працівників Національної поліції України впроваджено ліцензоване антивірусне програмне забезпечення Cisco Secure Endpoint. Станом на 31 грудня 2025 року зазначене програмне забезпечення встановлено на 19 063 персональних комп’ютерах.

Забезпечено також встановлення ESET Endpoint Security на 16 732 персональних комп’ютерах, а також ESET Mobile Security на 1 760 планшетних пристроях, що є складовою корпоративної IT-інфраструктури. Реалізовані заходи забезпечили багаторівневий захист від шкідливого програмного забезпечення, несанкціонованого доступу та інших кіберзагроз, а також посилили контроль за дотриманням вимог інформаційної безпеки під час службової діяльності.

Засобами протидії фішинговим та DDoS-атакам на поштовому домені POLICE.GOV.UA здійснюється постійний моніторинг активності зловмисників. Одночасно впроваджуються багаторівневі механізми аутентифікації та здійснюється моніторинг безпеки серверної інфраструктури.

Крім того, поліцією розгорнуто спеціалізовану платформу для збору та обміну інформацією про кіберзагрози MISP (Malware Information Sharing Platform), яка інтегрована до платформи MISP CERT-UA, забезпечується обмін інформацією в режимі реального часу щодо кібератак із CERT-UA.

Платформа MISP у режимі реального часу забезпечує обмін даними про кіберризики, атаки та інциденти, які оброблюються та додаються на платформу.

З метою підвищення рівня кібергігієни та дотримання вимог інформаційної безпеки при роботі з відомчими сервісами розроблено та наказом Національної поліції України від 10 березня 2025 року № 246 затверджено Політику кібергігієни та інформаційної безпеки під час роботи із сервісами Національної поліції України. Упровадження зазначеної Політики забезпечує:

підвищення обізнаності персоналу у сфері кібергігієни;

установлення єдиних вимог до користувачів щодо дотримання правил інформаційної безпеки;

визначення стандартів користування сервісами Національної поліції.

У 2025 році поліцією проведено системну роботу з підвищення кваліфікації персоналу, зокрема шляхом участі працівників у спеціалізованих навчальних програмах, тренінгах та CTF-заходах, а також проведення внутрішнього навчального курсу з реагування на кіберінциденти для 51 працівника спеціалізованих ІТ-підрозділів.

У межах розвитку системи захисту мобільних пристроїв уведено в експлуатацію програмний продукт BlackBerry Spark UEM Suite, до якого підключено 8 128 планшетних пристроїв територіальних органів поліції. Водночас рівень забезпеченості підрозділів планшетними пристроями з можливістю підключення до зазначеної системи становить 37 %, що зумовлює необхідність подальшого нарощування технічних спроможностей.

Після повномасштабного вторгнення фахівці кіберполіції активно залучалися до протидії державі-терористу в кіберпросторі, інформаційного захисту об’єктів критичної інфраструктури та відпрацювання пов’язаних з війною кіберінцидентів. З цією метою в Національній поліції у 2025 році створено галузевий центр реагування на інциденти кібербезпеки та кібератаки в інформаційно-комунікаційних системах у системі Міністерства внутрішніх справ України, спеціалісти якого в межах компетенції та можливостей забезпечують функціонування програмного та апаратного забезпечення. У постійній співпраці з представниками об’єктів моніторингу проводяться роботи з підключення додаткових джерел подій та налагодженню взаємодії.

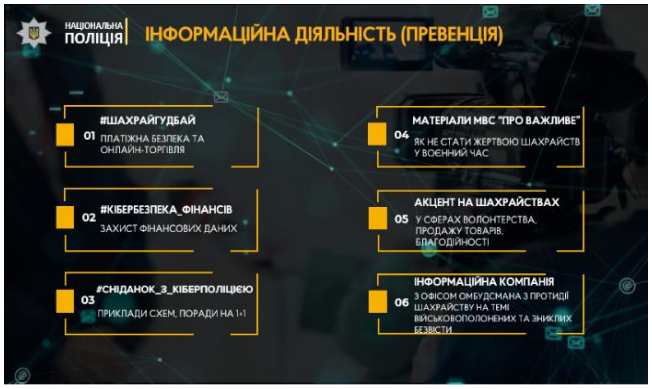
Крім того, на підставі частини третьої статті 5 Закону України «Про основи національного спротиву» працівники поліції залучалися до виконання завдань руху опору за рішенням Головнокомандувача Збройних Сил України.

З метою виконання завдань руху опору у кіберсфері працівники Національної поліції сприяли розвитку та реалізації проєкту «BRAMA». У відповідь на суспільну потребу волонтери (ІТ-спеціалісти, фрілансери, медійні особистості та лідери громадської думки) за координації кіберполіції створили цілу екосистему «BRAMA» для захисту українського інформаційного

простору від ворожих посягань, донесення правдивої інформації до людей. Отже, активісти проєкту «BRAMA» блокують осередки ворожої дезінформації та поширення протиправного контенту. Підписниками каналу https://t.me/stoprussiachannel на кінець звітного періоду забезпечено **24 млн** заходів щодо висвітлення інформації в медіапросторі.

Підрозділи Національної поліції здійснюють постійний моніторинг національних електронних комунікаційних мереж та інформаційних ресурсів, аналіз вторгнень у ці мережі та ресурси, а також виявлення в режимі реального часу недоліків їх функціонування. Для забезпечення захисту сервісів Національної поліції впроваджуються та використовуються сучасні програмно-технологічні рішення.

На виконання цілей Стратегії кібербезпеки України щодо розширення шляхом діалогу з міжнародними партнерами доступу правоохоронних органів України до ресурсів Європейського центру боротьби з кіберзлочинністю працівникам Національної поліції надано доступ до комунікаційної системи «Інтерпол І-24/7».



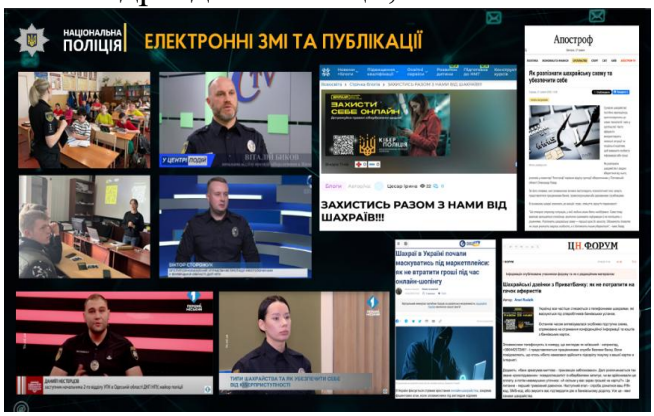
В умовах воєнного стану є важливим своєчасно інформувати громадян про роботу поліцейських як загальнодержавними, так і міжнародними новинними ресурсами, у тому числі Європолом.

У системі Національної поліції з метою покращення взаємодії з громадянами та надання їм кваліфікованої допомоги забезпечено диференційовані канали зв'язку, зокрема особисті та електронні звернення, телефонну інформаційну підтримку, функціонування офіційного вебресурсу з каналами зворотного зв'язку.

Упродовж 2025 року розпочато окремі загальнодержавні інформаційні кампанії для підвищення кіберграмотності українців, протидії насиллю над дітьми, кібербуллінгу та для розвитку безбар'єрного простору на підтримку визначеного керівництвом держави курсу євроінтеграції.

Ураховуючи те, що однією з детермінант учинення кіберзлочинів є кіберграмотність та рівень усвідомлення цінності персональних даних, з метою запобігання їх витоку поліцією здійснювалася підготовка та розміщення матеріалів Всеукраїнської інформаційної кампанії **#КібербезпекаФінансів** (спільно з Національним банком України та Держспецзв'язку), яка має за мету поширення знань про правила платіжної безпеки та формування в споживачів фінансових послуг навичок захисту фінансових даних у віртуальному просторі та є продовженням інформаційної кампанії **#ШахрайГудбай.** Запроваджено також спільну рубрику Департаменту кіберполіції та ранкового шоу «Сніданок з 1+1», яка спрямована на підвищення цифрової грамотності громадян, де фахівці інформують про найпоширеніші шахрайські схеми, надаючи дієві поради щодо захисту особистих даних тощо.

Крім того, Національною поліцією в минулому році підготовлено та розміщено на офіційних вебресурсах (сайти Департаменту кіберполіції, Національної поліції України, регіональних підрозділів поліції, Youtube-канали Національної поліції, офіційних сторінках у соціальних мережах Facebook та X, спільнотах у месенджері Viber та Telegram-каналах) 87 матеріалів з метою донесення до населення інформації про роботу кіберполіції, підвищення рівня цифрової грамотності громадян та обізнаності людей у сфері кібербезпеки і зниження віктимності в кіберпросторі.



Для посилення безпеки дітей під час користуванням Інтернетом забезпечено партнерство з міжнародними організаціями (Представництво Дитячого фонду ООН (ЮНІСЕФ) в Україні, Рада Європи, Канадська поліцейська місія в Україні), зокрема щодо виявлення та протидії фактам сексуального насильства стосовно дітей, створення безпечного цифрового середовища, захисту прав і законних інтересів дітей в інформаційному просторі. Проведено окремі семінари-тренінги, онлайн-дискусії, робочі зустрічі.

Поліцейськими проводяться просвітницько-профілактичні заходи з учнями закладів загальної середньої, професійної освіти, а також здійснюється моніторинг соціальних мереж, форумів, чатів для виявлення деструктивного контенту, зокрема участі дітей в онлайн-стрімах як новій мішені для зловмисників, захисту від онлайн-загроз (кібербулінг, сексторшен), основних онлайн-ризиків для дітей у воєнний час, вербуванню підлітків у соціальних мережах, а також небезпечний контент, що пропагує самокалічення, небезпечні «челенджі» та екстремальні дії. Забезпечено своєчасне та оперативне реагування на такі факти, а також на звернення громадян, пов’язані з інтернет-загрозами.

Так, поліцейськими розроблено інформаційні матеріали щодо цифрової грамотності та безпеки в інтернеті для дітей, а саме: у межах проведення інформаційно-профілактичних заходів протягом 2025 року здійснено SMS-розсилки з альфа-іменем «Cyberpolice» на абонентські номери операторів мобільного зв’язку ПрАТ «ВФ Україна», ПрАТ «Київстар» та ТОВ «Лайфселл».

Перша інформаційна кампанія проведена впродовж червня–липня 2025 року щодо безпеки дітей в Інтернеті з посиланнями на інформаційний ресурс: https://chatovi.online/articles/d1fs65 та https://chatovi.online/articles/sf134aw, а також упродовж листопада 2025 року з нагоди Дня захисту дітей, що мали профілактичний характер. Абонентам нагадували про небезпеку онлайн-експлуатації дітей через стріми та соцмережі, закликали до уважності в цифровому житті та надавали рекомендації щодо безпечної поведінки онлайн, зокрема не надсилати особисті фото та відео навіть «для гри». Для детального

ознайомлення адресатам надано посилання на інформаційний ресурс: https://chatovi.online/articles/nbMdo1.

Крім того, у Національній поліції створено нормативні і організаційно-технічні умови для проведення загальнонаціональних інформаційних роз'яснювальних кампаній щодо дій громадян у разі, коли вони стикаються із кібершахрайством та іншими кіберзлочинами. Актуальна інформація постійно розміщується на офіційних вебресурсах Національної поліції.

Департамент кіберполіції
Національної поліції України