МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

ВСТАНОВЛЕННЯ ОСОБИ НА МІСЦІ ВЧИНЕННЯ ЗЛОЧИНУ ЗА ДОПОМОГОЮ WI-FI РОУТЕРУ

Методичні рекомендації

Київ – 2022

УДК 343.98 : 343.132 : 351.746.2
В-858

Матеріали схвалено науково-методичною радою Національної академії внутрішніх справ від 6 жовтня 2022 р., протокол № 1.

Розробники:
Тіхонов Сергій Васильович – завідувач кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, кандидат юридичних наук, генерал поліції третього рангу;
Кобець Микола Вікторович – доцент кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник.

Рецензенти:
Яковенко О. В. – начальник науково-дослідної лабораторії спеціальних технічних засобів Державного науково-дослідного інституту МВС України кандидат технічних наук, старший науковий співробітник;
Василинчук В. І. – професор кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, доктор юридичних наук, професор, заслужений юрист України, полковник поліції.

Встановлення особи на місці вчинення злочину за допомогою wi-fi роутеру : методичні рекомендації. Київ : Національна академія внутрішніх справ, 2022. 37 с.

У методичних рекомендаціях розроблено сучасні теоретично-правові та організаційні засади зі встановлення особи на місці вчинення злочину, використовуючи технічні можливості wi-fi роутеру під час виявлення та розслідування кримінальних правопорушень.

Складається з п’яти розділів і містять основні відомості із загальних понять, дій працівників поліції під час встановлення особи, що здійснила кримінальне правопорушення в приватному чи багатоквартирному будинку.

Призначено для працівників органу досудового розслідування та оперативних підрозділів Національної поліції України. Методичні матеріали можуть бути корисним для науково-педагогічних працівників та науковців правоохоронних органів України.

ЗМІСТ

1. Терміни та визначення

Для найкращого сприйняття запропонованого матеріалу, у якому використовуються технічні терміни, наведемо деякі їх поняття та визначення.

MAC-адреса (від англ. *Media Access Control* – управління доступом до носія) – це унікальний ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж. Це номер мережевої плати, який встановлюється заводом-виробником. За допомогою цього номеру можна встановити місцезнаходження мережевого блоку, якщо він підключений до глобальної чи локальної мережі. Більшість мережевих протоколів канального рівня використовують один з трьох просторів MAC-адрес, керованих стандартом IEEE: MAC-48, EUI-48, EUI-64.

Структура MAC-адреси виглядає таким чином:

- перший біт MAC-адреси одержувача називається бітом I / G (individual (одиночний) / group (груповий)). В адресі джерела він називається індикатором маршруту від джерела (Source Route Indicator);
- другий біт визначає спосіб призначення адреси;
- три старші байти адреси називаються захисною адресою (Burned In Address, BIA) або унікальним ідентифікатором організації (Organizationally Unique Identifier, OUI);
- за унікальність наступних трьох байтів адреси відповідає сам виробник.

IP-адреса (від анг. *Internet Protocol address*) – це ідентифікатор мережевого рівня, що використовується для адресації комп'ютерів чи пристроїв у мережах, що побудовані з використанням протоколу TCP/IP (наприклад, мережа Інтернет).

IP-адресу називають статичною, якщо вона призначається користувачем у налаштуваннях пристрою, або якщо призначається автоматично під час підключення пристрою до мережі і не може бути присвоєна іншому пристрою.

IP-адресу називають динамічною (непостійною, змінною), якщо вона призначається автоматично під час підключення пристрою до мережі і використовується протягом обмеженого проміжку часу, зазначеного в сервісі, що призначав IP-адресу (DHCP).

IP-адреса складається з двох частин: номера мережі і номера вузла.

Wi-Fi – це протокол передачі даних за допомогою радіохвиль між пристроями, тобто wi-fi роутером і зовнішніми пристроями (девайсами), наприклад ноутбуком, планшетом, стільниковим радіотелефоном тощо, які підключаються до нього для доступу до мережі Інтернет.

Модем (*Modem* – скорочення від модулятор-демодулятор) – пристрій електрозв'язку для перетворення аналогового сигналу в дискретний (модуляція) та навпаки (демодуляція), що дозволяє комп'ютеру передавати дані фізичними лініями (телефонними лініями); він є пристроєм узгодження у електронних комунікаційних системах, системах автоматичного керування тощо.

2. Загальні поняття

Боротьба з кримінальною протиправністю є одним із важливих напрямів діяльності держави. Тому на сучасному етапі розвитку та становлення органи державної влади і уряд України вимагають постійного вдосконалення роботи правоохоронних органів.

У зв'язку з цим, особливого значення набуває розробка способів реалізації науково-технічних досягнень у боротьбі з кримінальною протиправністю, розширенням можливостей використання їх у процесі попередження, виявлення і розслідування кримінальних правопорушень.

Для оперативного виявлення та розслідування кримінальних правопорушень працівники правоохоронних органів повинні поширено використовувати досягнення науково-технічного прогресу, їхні технічні можливості. Тому слід постійно підвищувати технічний і професійний рівень працівників органів та підрозділів Національної поліції. Таке рішення пояснюється певними вимогами щодо підготовки спеціалістів вищої кваліфікації у сфері правоохоронної діяльності.

Для вмілого та ефективного використання технічних можливостей сучасних інформаційно-комунікаційних засобів для встановлення особи, що вчинила злочин у процесі попередження, виявлення та розслідування кримінальних правопорушень детальніше розглянемо загальні поняття, структуру та принцип роботи wi-fi роутерів.

Роутер (від англ. router; на російск. маршрутизатор) – спеціалізований пристрій, який пересилає пакети між різними сегментами мережі на основі правил та таблиць маршрутизації. Роутер з'єднується з користувачами (девайсами) інтернет-кабелем (скручена пара), тобто фізичним з'єднанням чи радіохвилями, використовуючи wi-fi протокол. Роутер з таким з'єднанням називається wi-fi роутером. Принцип роботи wi-fi роутера здійснюється таким чином: роутер з'єднується з мережею Інтернет інтернет-кабелем, використовуючи послуги провайдера, після чого wi-fi роутер надає користувачам (пристроям, девайсам), які знаходяться в зоні дії wi-fi протоколу

(його покриття), можливість роботи в мережі Інтернет (див. рис. 1).

Рис. 1. Загальна структурна схема роботи wi-fi роутера.

Загалом роутер має декілька режимів роботи. У режимі «router», який найчастіше використовується користувачами, цей пристрій зберігає в своїй вбудованій пам'яті таку необхідну нам інформацію як:

- mac-адреса;
- обліковий запис;
- пароль.

Принцип використання комп’ютерно-мережевих даних (ідентифікаторів) wi-fi роутера, які застосовуються для встановлення особи, що вчинила злочин, полягає в наступному. Пристрої (стільниковий радіотелефон, ноутбук, планшет тощо), які підключені до мережі wi-fi роутера мають свою MAC-адресу, яка фіксується в цій мережі. Інші комп’ютерно-мережеві дані (ідентифікатори), зокрема IP-адреса в цій локальній мережі не фіксуються, оскільки в мережі Інтернет обмін даними відбувається на основі IP-адрес, який надає постачальник електронних комунікаційних послуг (провайдер). При цьому на один роутер виділяється один IP-адрес, незалежно від кількості підключених користувачів. При включеному Wi-Fi модулі будь-який пристрій (ноутбук, планшет або стільниковий радіотелефон), який підключений до роутеру, розкриває свою MAC-адресу. Це є публічно доступна інформація, яку неможливо приховати без відмови від використання Wi-Fi модуля. Ця інформація не підпадає під юридичну відповідальність відповідно до Закону

України «Про захист персональних даних» та Закону України «Про електронні довірчі послуги», тому такі дії не відносяться до обмеження конституційних прав людини та громадянина.

Слід зазначити, що на застосування громадянами wi-fi роутеру дозволу Українським державним центром радіочастот не потрібно. Оскільки використання таких пристроїв, тобто використання точки доступу зі стандартної всенаправленної антени (< 6 дБ, потужність сигналу ≤ 100 мВт на 2,4 ГГц і ≤ 200 мВт на 5 ГГц) для внутрішніх (використання у приміщенні) потреб організації, передбачено рішенням Національної комісії з урегулювання зв'язку України від 6 вересня 2007 року № 914 «Про затвердження Переліку радіоелектронних засобів та випромінювальних пристроїв, для експлуатації яких не потрібні дозволи на експлуатацію». Для застосування зовнішніх антен на відкритій місцевості необхідно реєструвати радіопередавач і отримувати дозвіл на експлуатацію радіоелектронного засобу від ДП «Український державний центр радіочастот». Крім того, для діяльності з надання електронно комунікаційних послуг із застосуванням протоколу Wi-Fi необхідно отримати ліцензію від Національної комісії з урегулювання зв'язку.

3. Дії працівників поліції під час встановлення особи, що вчинила злочин у приватному чи багатоквартирному будинку.

Швидке та повне виявлення та розслідування кримінальних правопорушень досягається шляхом збирання, отримання, накопичення та використання інформації про осіб, які вчинили злочин, а також про події і факти, що можуть сприяти їх розслідуванню і розкриттю. Тому після надходження до органу (підрозділу) поліції інформації про вчинення кримінального правопорушення здійснюється комплекс першочергових заходів та невідкладних слідчих (розшукових) дій, спрямованих на встановлення особи, яка вчинила кримінальне правопорушення, та з'ясування всіх обставин події. Особлива увагу приділяється обстеженню місця події.

У разі виявлення факту кримінального правопорушення в приватному чи багатоквартирному будинку, або у громадському місці, наприклад, закладів харчування (кафе, ресторан) чи в офісі фірми слідчо-оперативна група (далі – СОГ), що прибула на місце події, передусім повинна здійснити першочергові заходи та невідкладні слідчі (розшукові) дії, тобто провести відповідно до статті 237 Кримінального процесуального кодексу (далі – КПК України) огляд місця події, а саме огляд приміщень на наявність матеріальних слідів злочину, зокрема предметів, знарядь вчинення злочину тощо та вивчення матеріальної обстановки його здійснення. Такі дії щодо пошуку речових доказів та слідів злочину на місці події допоможуть встановити особу, що вчинила кримінальне правопорушення. При цьому оперативний працівник, який задіяний в групі СОГ на місці події, відповідно до пункту 9 «Працівник оперативного підрозділу на місці події» розділу ІІ «Організація взаємодії при надходженні до органу, підрозділу поліції заяв і повідомлень про кримінальні правопорушення та реагуванні на них» наказу МВС України від 07.07.2017 № 575 «Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні», повинен: 1) здійснити поквартирний чи подвірний обхід з метою виявлення

свідків учиненого кримінального правопорушення, збору відомостей, що можуть бути використані як докази; 2) установити час, місце і обставини вчинення кримінального правопорушення; кількість осіб, які його вчинили, їх прикмети; наявність у них зброї, транспортних засобів, слідів на одязі чи тілі, які могли залишитися через опір потерпілих або при подоланні перешкод; індивідуальні ознаки викрадених речей; напрямок руху осіб, які вчинили кримінальне правопорушення, інші відомості, необхідні для їх встановлення; використовує наявні джерела оперативної інформації з метою розкриття кримінального правопорушення; 3) негайно інформувати слідчого (дізнавача) про одержані дані щодо обставин вчинення кримінального правопорушення та осіб, які його вчинили, для їх подальшої фіксації шляхом проведення слідчих (розшукових) дій або негласних слідчих (розшукових) дій; 4) виконувати письмові доручення слідчого (дізнавача) про проведення слідчих (розшукових) та негласних слідчих (розшукових) дій.

Але трапляється, що виявлені сліди злочину не мають достатньої криміналістичної інформації для швидкої ідентифікації та встановлення особи, що вчинила кримінальне правопорушення. Для вирішення такої нагальної проблеми нами пропонується один із способів швидкого встановлення особи – це використання технічних можливостей роутера у випадку його виявлення під час огляду приміщень та його обстеження на місці вчинення злочину. Використання запропонованого нами способу встановлення особи, що перебувала на місці події, пов’язано з тим, що у роутері можуть зберігатися електронні (цифрові) сліди пристрою (девайсу), наприклад мобільного терміналу, зокрема стільникового радіотелефону, якщо ним користувалась особа, що вчинила злочин, чи свідок цієї події. Однак це можливо у випадку, якщо роутер підтримує логіювання мережевих з’єднань і логіювання активоване. Логіювання або журналювання – це функція автоматичної фіксації службової та статистичної інформації про дії програмного забезпечення або користувачів у хронологічному порядку. Така інформація зберігається у лог-файлах (англ. Log file). У лог-файлах може фіксуватись різна інформація, все

залежить від програмного забезпечення, якого стосується логіювання, та налаштувань цього логіювання. У розглянутому випадку інтерес для розслідування буде становити інформація щодо під'єднаних до Wi-Fi-мережі девайсів, що зазвичай може містити дані про мережеву назву пристрою, його MAC-адресу, IP-адресу, час підключення до мережі та тривалість сеансу. Фактично, ці дані є електронними (цифровими) слідами, за якими можна ідентифікувати мобільний термінал підозрюваної особи. Для встановлення стільникового радіотелефону особи, що перебувала на місці вчинення злочину спеціаліст повинен робити акцент на такий ідентифікатор мережевого інтерфейсу роутера як MAC-адреса девайса, що підключався до нього. MAC-адреса автоматично зберігається у роутері під час під'єднання стільникового радіотелефону до нього. Виявлені та задокументовані електронні (цифрові) сліди в роутері при правильному їх процесуальному оформленні може набути статус доказу.

Розглянемо запропоновану нами версію, відповідно до якої під час огляду місця події групою СОГ було взято до уваги припущення, що особа яка вчинила злочин, чи свідок цієї події, тривалий час спілкувалась із потерпілим, і можливо він користувався роутером. На таку версію може навести результат візуального обстеження матеріальної обстановки місця події, зокрема в приміщенні, наприклад, наявність пляшок з алкоголю, недопалок тощо.

Враховуючи зазначене надаємо послідовність дій слідчо-оперативної групи на місці події для встановлення особи, що вчинила злочин.

У випадку, якщо був виявлений на місці події роутер (комп'ютерна техніка) слід здійснити певні дії із забезпечення збереження інформації на цьому пристрої. Для цього потрібно:

- вжити заходів для збереження лог-файлів Wi-Fi роутера. Якщо мережа корпоративна, слід звернутись до адміністратора цієї мережі, повідомивши йому про необхідність забезпечення збереження журналу подій для його подальшого вилучення у процесуальному порядку;

- обмежити доступ будь-яких осіб до мережевого устаткування, аби

уникнути будь-яких маніпуляцій (навмисних, ненавмисних чи випадкових) з ним: від'єднання (роз'єднання), вимкнення, перезавантаження, знеструмлення, переналаштування тощо;

- не дозволяти нікому і, бажано, не проводити самому ніяких дій з комп'ютерною технікою чи роутером, до приїзду спеціаліста у цій сфері;

- не користуватись цим роутером.

При проведенні огляду та тимчасового доступу до роутеру (комп'ютерної техніки) слід враховувати можливість:

- упровадження особами, зацікавленими в прихованні злочину, заходів із знищення інформації й інших важливих даних;

- установки в комп'ютерній техніці (роутері) спеціальних засобів захисту від несанкціонованого доступу, які, не отримавши у встановлений час спеціального сигналу або коду, автоматично знищують всю інформацію, що зберігається на них, або найважливішу її частину, що цікавить слідство;

- установки в комп'ютерній техніці (роутері), до яких здійснюється тимчасовий доступ інших засобів захисту інформації від несанкціонованого доступу.

У такому випадку надзвичайно важливо участь спеціаліста відповідно до статті 71 КПК України під час огляду та тимчасового доступу до роутеру (комп'ютерної техніки). Вони не тільки допоможуть фахово розібратися в особливостях комп'ютерного обладнання і носіїв інформації, але й зазначать, що підлягає копіюванню і запобіжать умисному або випадковому знищенню інформації. Профіль і кваліфікація фахівця, якого необхідно залучити до огляду та тимчасового доступу до комп'ютерної техніки (роутеру) у провадженні цієї категорії, визначається залежно від мети і завдань відповідної слідчої (розшукової) дії з урахуванням отриманих первинних даних про характер злочину. У таких випадках зазвичай залучають працівника Департаменту кіберполіції НП України.

Розділом XV «Особливості організації взаємодії при досудовому розслідуванні кримінальних правопорушень у сфері використання комп'ютерів,

систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинів)» наказу МВС України від 07.07.2017 № 575 «Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні» передбачено порядок залучення працівника Департаменту кіберполіції НП України до складу СОГ. Відповідно до цього наказу слідчий повинен враховувати такі дії, а саме:

«1. Матеріали Департаменту кіберполіції НП України, його структурного підрозділу, який діє за міжрегіональним принципом, де зафіксовано фактичні дані про кримінальні правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку, що направляються до слідчого підрозділу для початку та здійснення досудового розслідування, мають містити:

1) письмове пояснення заявника, в якому зафіксовані відомі заявнику дані про вчинення кримінального правопорушення з відповідними додатками, що містять відомості, які підтверджують його вчинення (роздруківки або скріншоти (програмне фотографування зображення з екрана монітора) вікон програм), а також у разі наявності документи, що підтверджують право власності потерпілого на комп'ютерну інформацію та інформацію, що передається мережами електрозв'язку, чи програмно-технічні засоби;

2) установлені ідентифікаційні дані про використані електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі та мережі електрозв'язку (логін і пароль для доступу до мережі Інтернет, IP-адреса, WEB-адреса, номер абонента мережі електрозв'язку чи номер телефону, за допомогою яких було здійснено такий доступ, тощо).

2. Утворення СОГ за участю оперативних працівників Департаменту кіберполіції НП України, його структурних підрозділів, які діють за міжрегіональним принципом, для розслідування кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку здійснюється за спільним наказом керівників органу досудового

розслідування та Департаменту кіберполіції НП України. Утворення СОГ у кримінальному провадженні, досудове розслідування у якому здійснюється Головним слідчим управлінням НП України, здійснюється за наказом Голови Національної поліції України або за наказом заступника Голови Національної поліції України - начальника Головного слідчого управління, погодженим керівництвом Департаменту кіберполіції НП України. Старшим СОГ є слідчий, якого керівником органу досудового розслідування визначено здійснювати досудове розслідування кримінального правопорушення.

3. Керівник Департаменту кіберполіції НП України, його структурного підрозділу, який діє за міжрегіональним принципом, оперативний працівник якого включений до складу СОГ або за матеріалами якого розпочато кримінальне провадження, забезпечує взаємодію з органом досудового розслідування Національної поліції України, який здійснює розслідування кримінальних правопорушень зазначеної категорії.».

4. Документальне оформлення процесуальних дій на місці вчинення злочину з урахуванням wi-fi роутеру

На початковій стадії проведення слідчих (розшукових) дій таких як обшук, виїмка, огляд слідчому чи оперативному працівнику у складі СОГ, на місці вчинення злочину з урахуванням виявленого wi-fi роутеру, необхідно:

1. Прибувши на місце проведення слідчої (розшукової) дії заборонити всім особам, що знаходяться в приміщенні де був вчинений злочин, торкатися до комп'ютерної техніки (роутерів), носіїв інформації, вмикати і вимикати пристрої й енергоживлення інакше такі дії можуть бути розцінені як спроба знищення речових доказів, що слід відобразити в протоколі огляду або тимчасового доступу до речей та документів.

2. Провести фото-, відеозйомку приміщення, де здійснюється огляд та тимчасовий доступ до роутеру (комп'ютерного обладнання).

3. У процесі проведення огляду або тимчасового доступу до роутеру (комп’ютерної техніки) спеціалістом, у присутності понятих, мають бути проведенні такі дії, а саме:

встановити схему мережі, з’ясувати, які пристрої забезпечують функціонування мережі (мережеве обладнання) та які до неї під’єднані постійно та тимчасово (клієнти – стаціонарні комп'ютери, ноутбуки, смартфони тощо);

зафіксувати дані, які зазвичай містяться у маркувальних позначеннях на корпусі пристроїв: марку, модель, серійний номер, MAC-адресу, стандартні дані автентифікації (ім’я користувача та пароль). У багатьох випадках ця інформація знаходиться на зворотній частині роутера (див. рис. 2);

Рис. 2. Загальні дані роутерів різних моделей, що знаходяться на зворотній їх частині.

підключитись до мережі. Для цього під’єднати до Wi-Fi-мережі службовий ноутбук або використати під’єднаний до мережі наявний комп'ютер. Використання комп'ютера власника має свої переваги і недоліки. Перевагою є те, що він вже підключений до мережі, а також можлива наявність у ньому автентифікаційних даних (якщо з нього здійснювалось адміністрування роутера). Недоліком може бути внесення змін до інформаційного вмісту носіїв інформації комп'ютера, що в окремих випадках це небажано. У випадку підключення службового ноутбуку чи іншого пристрою до Wi-Fi-мережі потрібно знати її назву (SSID, від англ. Service Set Identifier) та, якщо мережа захищена, пароль. При цьому слід враховувати, що SSID може бути скритим та/або підключення до мережі дозволене лише за білим списком MAC-адрес. Значна частина Wi-Fi роутерів підтримує підключення до Wi-Fi-мережі за допомогою функції WPS (від англ. Wi-Fi Protected Setup), що значно спрощує

під’єднання до мережі. Тобто за допомогою кнопки WPS можна підключати пристрої до Wi-Fi роутера без введення пароля від бездротової мережі. Така кнопка є практично у кожному роутері, також у налаштуваннях роутера є розділ WPS. Іноді кнопка WPS поєднана з функцією скидання налаштувань роутера і називається “WPS/RESET”. Коротке натискання активує функцію WPS, а триваліший (до 5 секунд) скидає налаштування роутера до заводських. Для активації WPS потрібно натиснути кнопку, коли функцію запущено, у роутері в більшості випадків починає блимати індикатор. Функція активується на час, доки блимає індикатор, в цей час нею можна скористатися. Запустити її повторно можна знову натиснувши кнопку. Отже під’єднання до Wi-Fi мережі реалізується одним з таких способів: за допомогою PIN коду (зазвичай вказаний на етикетці роутера), з натисканням push-кнопки, з використанням NFC або з використанням флеш-накопичувача для перенесення налаштувань з роутера на ноутбук. Також не слід відкидати можливість підключення до мережі за допомогою проводового з’єднання, адже більшість Wi-Fi-роутерів мають також і проводові інтерфейси для локальної мережі. В цьому випадку SSID та пароль не потрібен;

- здійснити вхід до інтерфейсу головного мережевого пристрою (Wi-Fi роутера). Слід враховувати, що вхід до адміністративного меню Wi-Fi роутера може бути заблокований з безпроводової мережі (дозволено лише з проводової локальної мережі), може бути дозволений вхід лише за білим списком MAC-адрес тощо. Для входу до веб-інтерфейсу роутера за допомогою інтернет-браузера необхідно в адресний рядок ввести адресу роутера. Для домашніх роутерів це зазвичай «http://192.168.0.1» або «http://192.168.1.1», але слід враховувати, що ця адреса може бути змінена у налаштуваннях. У випадку професійного мережевого обладнання доцільно з’ясувати параметри входу у системного адміністратора. У низці випадків може бути неможливо увійти до меню роутера через веб-інтерфейс. У такому випадку, якщо роутер підтримує доступ через термінал, можна використати доступ за протоколами Telnet чи SSH (останній краще, бо використовує зашифрований канал електрозв’язку).

Крім того, слід враховувати, що частина роутерів підтримують адміністрування за допомогою спеціального програмного забезпечення (фірмової утиліти);

здійснити візуальний огляд відображеної інформації на екрані комп'ютера з подальшою її фіксацією, відповідно статті 237 КПК України;

ввести автентифікаційні дані адміністратора. У багатьох Wi-Fi роутерів виробниками задаються стандартні параметри входу: ім'я admin і пароль admin (див. рис. 3). Разом з тим, стандартною є рекомендація змінити ці параметри відразу після першого входу. Іноді система може навіть не пропустити користувача до меню, доки він не змінить стандартні автентифікаційні дані. Крім того, для автентифікації може знадобитись ключ HASP (від англ. Hardware Against Software Piracy). Отже, бажано дізнатися параметри входу у власника Wi-Fi роутера або системного адміністратора. Вказані параметри слід зафіксувати у протоколі;

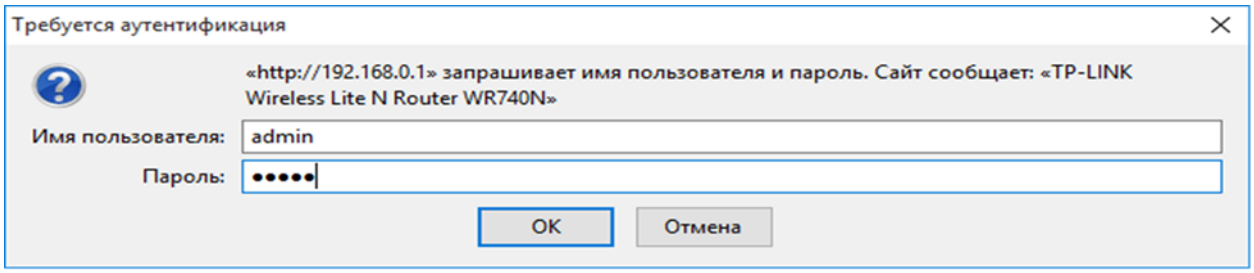

Рис. 3. Скриншот екрана (дисплея) комп'ютера з інформацією про введення пароля.

у разі входу до адміністративного меню варто спочатку переглянути налаштування логіювання, а потім – наявність лог-файлів за потрібний проміжок часу;

виявлені дані слід вивести на екран ноутбука та переглянути учасникам слідчої (розшукової) дії, зокрема, понятим;

указані дані слід зафіксувати у протоколі слідчої (розшукової) дії, до якого доцільно долучити роздруківки відповідних знімків екрану ноутбука (скріншоти);

виявлені лог-файли слід вилучити. Залежно від моделі Wi-Fi роутера та наявного у СОГ обладнання це можна зробити шляхом копіювання лог-файлу, експорту логів у текстовий чи табличний файл, виділенням та копіюванням необхідної інформації у текстовий файл або скріншотами;

отриманий файл або декілька файлів слід засвідчити електронним підписом особою, яка здійснює ці процесуальні дії. У випадку, якщо файлів декілька, їх можна помістити до архіву та підписати (обрахувати хеш) лише цього одного архівного файлу. Файл записати на носій інформації (оптичний диск тощо), який додати до протоколу слідчої (розшукової) дії.

Усі дії на екрані комп'ютера рекомендується фіксувати не лише у протоколі, але й шляхом створення знімків екрану (скріншотів), які потім можна роздрукувати та записати на цифровий носій інформації.

Дії зі встановлення MAC-адреси пристроїв, які підключались до роутера, розглянемо на прикладі інтерфейсу «1xUSB 2.0» роутера типу «ASUS RT-N10». Для цього слід здійснити такі дії, а саме:

1. Після ведення пароля доступу до роутера на екран (дисплей) комп’ютера виводиться загальна картинка інтерфейса роутера та проводиться огляд і фіксація відповідної інформації (див. рис. 4).

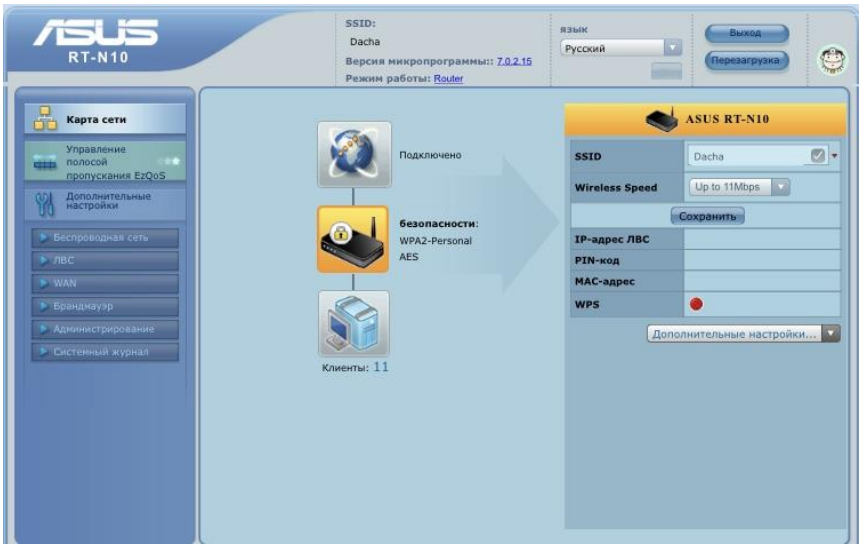

Рис. 4. Скриншот екрана (дисплея) комп’ютера, на якому міститься інформація з роутера.

2. На екрані (дисплеї) комп’ютера вибираючи необхідну функцію управління роутером встановлюються і фіксуються MAC-адреси девайсів, які підключались до цього пристрою (див. рис. 5, 6).

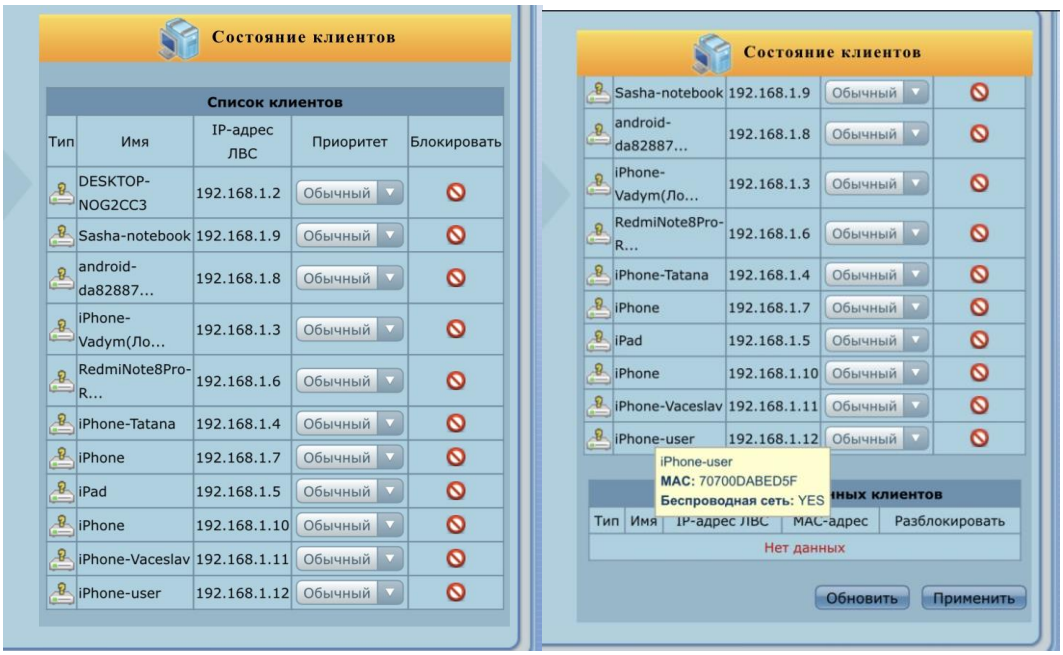

Рис. 5. Скриншот екрана (дисплея) комп’ютера зі списком користувачів, які підключались до роутеру.

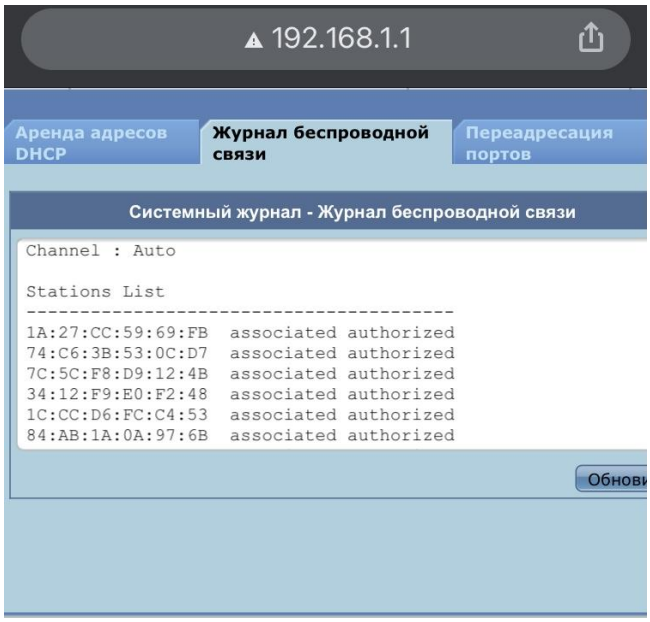

Рис. 6. Скриншот екрана (дисплея) комп’ютера із системним журналом, у якому міститься інформація про MAC-адреси девайсів, які підключалися до роутеру.

3. Виявленні MAC-адреси вивчаються та аналізуються. Визначаються невідомі MAC-адреси, що не належать мобільним терміналам (стільниковим радіотелефонам) встановленим особам (користувачам).

Для цього слід переглянути налаштування пристроїв встановлених осіб, зафіксувати їх MAC-адреси та порівняти з адресами, зафіксованими у лог-файлах.

Залежно від виробника роутера визначається дата, час підключення невідомого користувача до мережі, а також часовий проміжок його підключення (див. рис. 7).

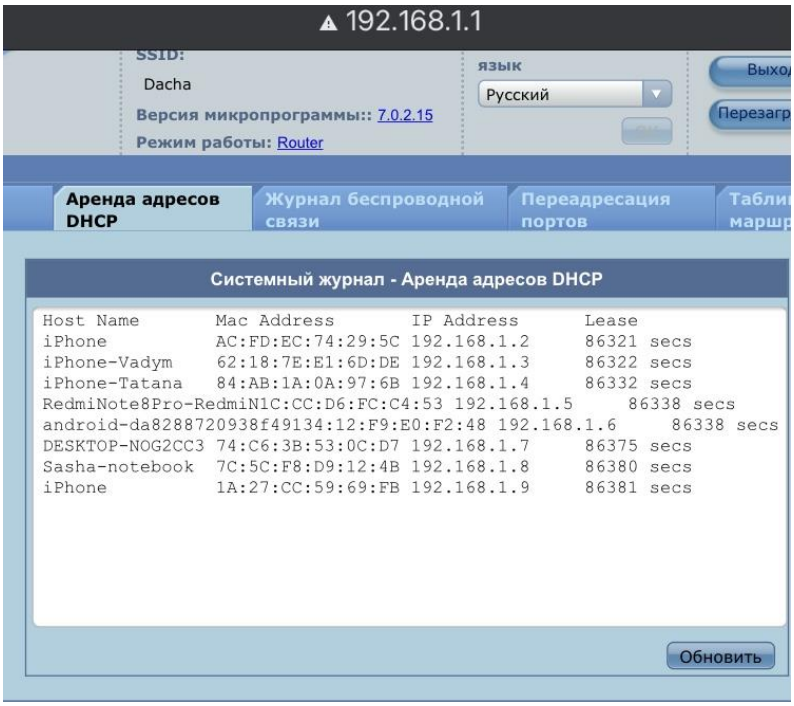

Рис. 7. Скриншот екрана (дисплея) комп’ютера із системним журналом, у якому міститься інформація про дату та час підключення користувача до мережі.

На завершальній стадії огляду та тимчасового доступу до комп’ютерної техніки (роутеру), у цьому випадку, необхідно:

1. Визначити за допомогою спеціаліста (з урахуванням використання комп'ютера як засіб вчинення злочину або джерела доказів), де зберігається на комп’ютерній техніці (роутері) необхідна інформація, яка підлягає копіюванню.

2. Слід враховувати, що є багато моделей роутерів, які під час їх відключення від електричної мережі втрачають змінні дані. Тому у присутності понятих слід здійснити на місці події огляд та фіксацію відповідної інформації (комп’ютерних даних) згідно статті 237 КПК України. Для цього виведена на екран (дисплей) комп’ютера необхідна для доказу інформація з роутера має бути записана на цифровий диск на зразок CD-R, DVD-R (носій інформації, який конструктивно та функціонально передбачений тільки для разового запису, що у подальшому унеможливлює додаткових питань зі сторони захисту під час судового розгляду) у виді файла, засвідчений електронним підписом

особою, що здійснює ці процесуальні дії. Відповідно до рішення Верховного Суду України колегії суддів Касаційного господарського суду у справі №922/51/20 від 29 січня 2021 року електронний підпис прирівняний до власноручного підпису відповідно до Закону України «Про електронні довірчі послуги».

3. Оформити протокол огляду (див. Додаток № 2) та тимчасового доступу до речей та документів (див. Додаток № 3), в якому поетапно фіксуються всі дії спеціаліста (з урахуванням особливої специфіки діянь, що розслідуються, це рекомендується робити під його диктовку та у присутності понятих), а саме:

- указується місце розташування комп'ютерної техніки (роутера), до яких здійснюється огляд та тимчасовий доступ до речей (предмета), і їх взаємне розташування щодо один одного і навколишніх предметів;

- описується зовнішній вигляд комп'ютерної техніки (роутеру), порядок з'єднання різних вузлів і деталей між собою з вказівкою наявних особливостей (кольору, штампів, написів і т. і.);

- записуються серії і номери пристроїв, до яких здійснюється огляд та тимчасовий доступ до речей (предмета), інші його ідентифікаційні ознаки;

- описується процедура копіювання інформації з комп'ютерної техніки (роутеру);

- заносять всі заяви присутніх під час огляду та тимчасового доступу до речей (предмета), що стосуються технічних та процесуальних моментів слідчої (розшукової) дії, що проводяться.

До протоколу додаються: схеми плану приміщень з приміткою, де був розміщений роутер; матеріали фото-, відеозйомки, що проводились під час слідчої (розшукової) дії; скріншоти зображення з екрану (дисплея) комп’ютера, де відображені MAC-адреси девайсів, які підключались до роутеру; цифровий носій інформації (диск), на якому зафіксовано скріншоти.

Протокол підписується слідчим й іншими учасниками слідчої (розшукової) дії (спеціалістами, понятими, особою, у якої проведено огляд та тимчасовий доступ), а також іншими присутніми (представниками адміністрації, технічного

персоналу), що мають відношення до роботи комп'ютерної мережі (під час проведення слідчої (розшукової) дії в службових приміщеннях) (див. Додаток).

Забороняється зазначати в протоколі та зберігати в будь-якому іншому виді відомості, що стосуються особистого життя, честі, гідності людини, якщо вони не містять інформації про вчинення заборонених законом дій.

4. У робочому приміщенні роздрукувати з цифрового носія інформації (диску) скріншоти виведених на екран (дисплей) комп’ютера MAC-адрес девайсів, які підключались до роутеру за певний проміжок часу, вчинення злочину.

Розглянемо питання щодо використання скріншоту в правовому полі як електронний документ.

У пункті 1 частини 2 статті 99 КПК України зазначається «До документів, за умови наявності в них відомостей, передбачених частиною першою цієї статті, можуть належати:

1) матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп’ютерні дані);

3) складені в порядку, передбаченому цим Кодексом, протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії;».

Згідно частини 3 статті 99 КПК України «Оригіналом документа є сам документ, а оригіналом електронного документа – його відображення, якому надається таке ж значення, як документу». При цьому відповідно до частини 4 статті 99 КПК України « … комп’ютерні дані, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп’ютерних системах, їх невід’ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа».

Також у частинах 1 та 3 статті 100 «Електронні докази» Цивільного процесуального кодексу України (далі – ЦПК України) передбачено, що електронними доказами є інформація в електронній (цифровій) формі, що

містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет). Учасники справи мають право подавати електронні докази в паперових копіях, посвідчених у порядку, передбаченому законом. Паперова копія електронного доказу не вважається письмовим доказом.

При цьому у частинах першій-третій статті 89 ЦПК України передбачено, що суд оцінює докази за своїм внутрішнім переконанням, що ґрунтується на всебічному, повному, об`єктивному та безпосередньому дослідженні наявних у справі доказів. Жодні докази не мають для суду заздалегідь встановленої сили. Суд оцінює належність, допустимість, достовірність кожного доказу окремо, а також достатність і взаємний зв`язок доказів у їх сукупності. Суд надає оцінку як зібраним у справі доказам в цілому, так і кожному доказу (групі однотипних доказів), який міститься у справі, мотивує відхилення або врахування кожного доказу (групи доказів).

5. Встановлення місцезнаходження девайсів, які перебували у місці вчиненого злочину, за їх MAC-адресою.

Після оформлення протоколу на місці події слід здійснити подальші слідчі (розшукові) дії для встановлення місцезнаходження девайсів, які перебували у місці вчиненого злочину, за їх MAC-адресою. Для цього необхідно встановити назву та IMEI девайсу, тобто мобільного терміналу. Таку інформацію можна отримати використовуючи довідникові джерела у мережі Інтернет виробника девайса, наприклад Інтернет-сайт https://www.imei.info/services/mac-address-checker/de8058bd-4080-4bc8-9eaa-6fee596dab2e/ (див. рис. 8), вписуючи в запиті дані MAC-адрес виявлених в роутері (див. рис. 9). Маючи інформацію щодо виробника пристрою можна припустити тип девайсу – смартфон, планшетний комп'ютер, ноутбук, окремий мережевий інтерфейс (плата) тощо. Однак є деякі фірми, наприклад Xiaomi Communications Co Ltd, які виготовляють значну кількість різних типів девайсів: смартфони, планшетні комп'ютери, ноутбуки, мережеве обладнання тощо, і все це має мережеві інтерфейси з MAC-адресами. Тому за точною інформацією слід звернутись до виробника. Якщо запитуваний девайс має стільниковий мережевий інтерфейс (тобто, окрім Wi-Fi також може підключитись до стільникової радіомережі, наприклад, ноутбук чи планшетний комп'ютер – через вбудований 3G/4G модем), від виробника можна отримати інформацію про IMEI (від англ. International Mobile Equipment Identity – міжнародний ідентифікатор мобільного обладнання – серійний номер стільникового радіотелефону, який встановлюється заводом-виробником) вказаного девайса. Тобто за MAC-адресою можна встановити IMEI, який відстежується операторами стільникового радіозв'язку. Якщо за IMEI у довідникових інтернет-джерелах можна, зазвичай, встановити точну модель девайса, то за MAC-адресою – лише виробника.

Інший варіант отримання у виробника інформації про мобільний термінал, тобто його назву та IMEI (ідентифікатор) – використання правових інституцій, тобто шляхом запиту про міжнародну правову допомогу передбаченою главою 43 КПК України.

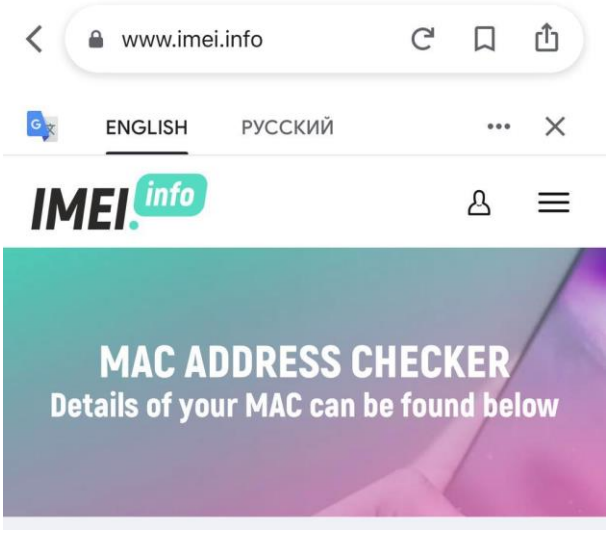

Рис. 8. Скриншот екрана стільникового радіотелефону сайту виробника для встановлення назви мобільного терміналу, використовуючи його MAC-адресу.

Рис. 9. Скриншот екрана стільникового радіотелефону сайту виробника для встановлення IMEI мобільного терміналу, використовуючи його назву та MAC-адресу.

Є інший спосіб установлення мобільного терміналу на місці вчинення кримінального правопорушення це проведення радіомоніторингу місця події та здійснення вибірки телефонних номерів, які перебували в час вчинення злочину. За телефонним номером можна встановити ідентифікатор абонента IMSI (від англ. International Mobile Subscriber Identity – міжнародний ідентифікатор користувача мобільного радіозв'язку), який міститься у

SIM/USIM/R-UIM картці. За цим кодом оператор стільникового радіозв'язку також може відстежити місцезнаходження мобільного терміналу.

Отримавши відповідну інформацію слідчий готує клопотання, погодженої з прокурором, про отримання тимчасового доступу до інформації (документів), які знаходяться в операторів і постачальників електронних комунікаційних послуг та містять інформацію про зв'язок, абонента, надання електронних комунікаційних послуг, у тому числі отримання послуг, їх тривалість, зміст, маршрути передавання тощо (трафіку) відповідно до частини 2 статті 159 та пункту 7 частини 1 статті 162 КПК України для отримання ухвалу слідчого судді суду першої інстанції такої дії. Слідчий (оперативний працівник) на підставі ухвали слідчого судді суду першої інстанції направляє запит до мережевих операторів стільникового радіозв’язку з метою перевірки MAC-адрес, які були встановленні під час огляду місця події, та встановлення даних користувача (IMEI, номеру телефону та інші дані), які є в системі баз даних постачальника електронних комунікаційних послуг стільникового радіозв'язку.

У разі визначення конкретного місця, дати та часу з’єднання технічного засобу (стільникового радіотелефону) з роутером, відповідно до статті 268 КПК України, провадять таку негласну слідчу (розшукову) дію як установлення місцезнаходження радіообладнання (радіоелектронного засобу), що може надати можливість встановити місцезнаходження технічного засобу, який був підключений до Wi-Fi мережі (роутера) у момент вчинення злочину. Порядок її проведення внормовано главою 21 «Негласні слідчі (розшукові) дії» КПК України. Загальні засади та єдині вимоги до організації проведення негласних слідчих (розшукових) дій слідчими органів досудового розслідування або за їх дорученням чи дорученням прокурора уповноваженими оперативними підрозділами, а також використання їх результатів у кримінальному провадженні окреслено наказом ГПУ, МВС, СБУ, АДПС, МФ, МЮ України від 16 листопада 2012 року №114/1042/516/1199/936/1687/5 «Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні».

Додаток № 1

ПРОТОКОЛ
огляду місця події

Місто (сел.) _Дніпро__ «20» 09.2022 року

Огляд почато о “20” год. “40” хв.
Огляд закінчено о “22” год. “50” хв.

Слідчий СВ Індустріального ВП Дніпровського ВП ГУ НП у Дніпропетровській області капітан поліції Іванов І.І. _____
(слідчий, найменування органу, прізвище, ім’я, по батькові)
на підставі заяви Сомова С.С. про розбійний напад на нього, _____
відповідно до ст.ст. 104, 105, 106, 223, 234, 237 КПК України:
у присутності понятих:
1) _Козіна Альберта Федоровича, 28.02.1965 р. н., який мешкає у м. Дніпро, ___ вул. Косіора, 71, кв. 15; _____
(прізвище, ім’я, по батькові, дата народження, місце проживання)
2) _Буніна Валерія Миколайовича, 21.01.1983 р. н., який мешкає у м. Дніпро, __ вул. Косіора, 71, кв. 4, _____
(прізвище, ім’я, по батькові, дата народження, місце проживання)
яким відповідно до ст. 11, 13, 15, 223 КПК України роз’яснено їхні права і обов’язки.

1) _____ 2) _____
(підпис) (підпис)

За участю потерпілого:
___Сомова Сергія Семеновича, 14.02.1975 р. н., який мешкає у м. Дніпро, _____ вул. Косіора, 71, кв. 10_____,
(прізвище, ім’я, по батькові, дата народження, місце проживання)
якому відповідно до ч. 1, 2 ст. 56, ст. 57 КПК України роз’яснено його права і обов’язки.

_____
(підпис)

За участю спеціаліста:
інспектора-криміналіста НДЕКЦ у Дніпропетровській області лейтенанта_____ поліції Котова Сергія Івановича_____,
(прізвище, ім’я, по батькові, місце роботи)
якому відповідно до ч.4,5 ст.71 КПК України роз’яснено його права і обов’язки.

_____
(підпис)

За участю власника (користувача) приміщення чи іншого володіння особи
Сомова Сергія Семеновича, який мешкає у м. Дніпро, вул. Косіора, 71, кв. 10
(прізвище ім'я, по батькові, адреса)

_____
(підпис)

Перед початком огляду місця події зазначеним особам роз'яснено їхнє право бути присутніми при всіх діях, які проводяться в процесі огляду, робити зауваження, що підлягають занесенню до протоколу. Особам, які беруть участь у проведенні огляду, також роз'яснено вимоги ч. 3 ст. 66 КПК України про їх обов'язок не розголошувати відомості щодо проведеної процесуальної дії, а також про застосування технічних засобів фіксації, умови та порядок їх використання.

Під час огляду застосовано технічні засоби: 1) цифровий фотоапарат «Nikon» 2) цифрова відеокамера «Sony».

(вказується застосування фото-, відеозйомки, інших технічних та спеціальних засобів, їх найменування, технічні параметри)

Проведеним оглядом встановлено: об'єктом огляду є двокімнатна квартира на третьому поверсі дев'яти поверхневого панельного (односекційного) житлового будинку за адресою: м. Дніпро, вул. Косіора, 71, кв. 10.

Під час огляду виявлено: WI-FI роутер типу «ASUS RT-N10» чорного кольору прямокутної плоскої форми з однією антеною, під'єднаний шнуром до електричної мережі та інтернет-кабелем до роутера.

Виявлено під час огляду місця події та вилучено: WI-FI роутер типу «ASUS RT-N10», після здійснення відповідних процесуальних дій щодо огляду роутера та тимчасового доступу до нього, поміщений у поліетиленовий пакет чорного кольору, горловина якого зав'язана капроновою ниткою білого кольору. На вузол зав'язаної нитки наклеєна паперова бірка. На бірці зазначено: 20 вересня 2021 року Індустріальний ВП Дніпровського ВП ГУ НП у Дніпропетровській області, WI-FI роутер типу «ASUS RT-N10» потерпілого Сомова С.С.

поняті:

1) Козін А.Ф. /підпис/;
2) Бунін В.М. /підпис/;
спеціаліст Котов С.І. /підпис/;
слідчий Іванов І.І. /підпис/

Під час огляду місця події застосовано технічні засоби: відеокамерою «Sony» здійснювалась безперервна фіксація огляду місця події; фотоапаратом "Nikon" зроблені п'ять фотознімків, з яких два орієнтуючих (прив'язка місця події до інших орієнтирів в квартирі), один оглядовий (загальний вигляд WI-FI роутеру типу «ASUS RT-N10» в кімнаті квартири), два вузлових (один наближений вигляд, інший – вигляд днища роутера, з фіксацією його даних).

(вказується застосовування фото-, відеозйомки, інших технічних та спеціальних засобів, їх технічні параметри)

Огляд проводився в квартирі за адресою: м. Дніпро, вул. Косіора, 71, кв. 10 при штучному освітленні

(вказуються погодні умови, освітлення, температура повітря, інші необхідні дані)

До протоколу огляду місця події додаються: план (схематичний); схема огляду місця події; носії інформації з відеокамери «Sony» та фотознімки з_____
(план (схематичний чи масштабний); схема місцевості; схема огляду місця події; схема доріжки слідів; схема сліду низу взуття; схема сліду знаряддя зламу; інше)
фотоапарату "Nikon", WI-FI роутер типу «ASUS RT-N10».
(носії комп'ютерної інформації та інші матеріали, які пояснюють зміст протоколу)

Протокол прочитано, записано слідчим зачитаний вголос, записано в точній відповідності до проведених процесуальних дій та отриманих результатів.____
Зауважень від учасників не надійшло._____
(зауваження учасників огляду)

З протоколом ознайомлені:

учасники:

1. Котов С.І._____ /_____/
(прізвище, ім'я, по батькові) (підпис)
2. Сомов С.С._____ /_____/
(прізвище, ім'я, по батькові) (підпис)

поняті:

1. Козін А.Ф._____ /_____/
(прізвище, ім'я, по батькові) (підпис)
2. Бунін В.М. _____ /_____/
(прізвище, ім'я, по батькові) (підпис)

Огляд провів та протокол склав:
слідчий СВ Індустріального ВП Дніпровського ВП
ГУ НП України в Дніпропетровській області
капітан поліції /_____/ **І.І. Іванов**

Додаток № 2

ПРОТОКОЛ
огляду предмета

Місто (сел.) _Дніпро__ «20» 09.2022 року

Огляд почато о “20” год. “40” хв.
Огляд закінчено о “22” год. “50” хв.

Слідчий СВ Індустріального ВП Дніпровського ВП ГУ НП у Дніпропетровській області капітан поліції Іванов І.І. _____
(слідчий, найменування органу, прізвище, ім’я, по батькові)
на підставі _кримінального провадження № 12012160_____
відповідно до ст.ст. 104, 105, 106, 223, 237 КПК України:
у присутності понятих:
1) _Козіна Альберта Федоровича, 28.02.1965 р. н., який мешкає у м. Дніпро, вул. Косіора, 71, кв. 15;_____
(прізвище, ім’я, по батькові, дата народження, місце проживання)
2) _Буніна Валерія Миколайовича, 21.01.1983 р. н., який мешкає у м. Дніпро, вул. Косіора, 71, кв. 4,_____
(прізвище, ім’я, по батькові, дата народження, місце проживання)
яким відповідно до ст. 11, 13, 15, 223 КПК України роз’яснено їхні права і обов’язки.

1) _____ 2) _____
(підпис) (підпис)

За участю потерпілого:
Сомова Сергія Семеновича, 14.02.1975 р. н., який мешкає у м. Дніпро, вул. Косіора, 71, кв. 10_____,
(прізвище, ім’я, по батькові, дата народження, місце проживання)
якому відповідно до ч. 1, 2 ст. 56, ст. 57 КПК України роз’яснено його права і обов’язки.

_____
(підпис)

За участю спеціаліста:
інспектора-криміналіста НДЕКЦ у Дніпропетровській області лейтенанта поліції Котова Сергія Івановича_____,
(прізвище, ім’я, по батькові, місце роботи)
якому відповідно до ч.4,5 ст.71 КПК України роз’яснено його права і обов’язки.

_____
(підпис)

За участю власника (користувача) приміщення чи іншого володіння особи
Сомова Сергія Семеновича, який мешкає у м. Дніпро, вул. Косіора, 71, кв. 10
(прізвище ім'я, по батькові, адреса)

_____
(підпис)

у квартирі за адресою: м. Дніпро, вул. Косіора, 71, кв. 10 провів огляд виявленого предмета WI-FI роутеру типу «ASUS RT-N10» чорного кольору прямокутної плоскої форми з однією антеною, що належить потерпілому Сомову С.С. та добровільно наданий ним для огляду.

Перед початком огляду предмета зазначеним особам роз'яснено їхнє право бути присутніми при всіх діях, які проводяться в процесі огляду, робити зауваження, що підлягають занесенню до протоколу. Особам, які беруть участь у проведенні огляду, також роз'яснено вимоги ч. 3 ст. 66 КПК України про їх обов'язок не розголошувати відомості щодо проведеної процесуальної дії, а також про застосування технічних засобів фіксації, умови та порядок їх використання.

Під час огляду застосовано технічні засоби: цифровий фотоапарат "Nikon"
(вказується застосування фото-, відеозйомки, інших технічних та спеціальних засобів, їх найменування, технічні параметри)

Проведеним оглядом встановлено: об'єктом огляду є WI-FI роутер типу «ASUS RT-N10». Роутер має пластиковий корпус чорного кольору прямокутної плоскої форми з однією антеною, під'єднаний шнуром до електричної мережі та інтернет-кабелем до роутера.

Під час огляду виявлено: на нижній частині роутера містяться такі дані:
model «RT-N10»; Factory Default Settings: IC: 3568A-RT N10;
IP address: 192.168.1.1; User name: admin; Password: admin;
F/W Ver.: V3.0.0.4.374_168; H/W Ver.: D1; PIN Code 04855445;
MAC BCEE786D4B38; S/N DBIEOQ001934.

Виявлено під час огляду та вилучено: оглянутий WI-FI роутер типу «ASUS RT-N10», після здійснення відповідних процесуальних дій щодо тимчасового доступу до роутера, поміщений у поліетиленовий пакет чорного кольору, горловина якого зав'язана капроновою ниткою білого кольору. На вузол зав'язаної нитки наклеєна паперова бирка. На бирці зазначено «20 вересня 2021 року Індустріальний ВП Дніпровського ВП ГУ НП у Дніпропетровській області, WI-FI роутер типу «ASUS RT-N10» потерпілого Сомова С.С.».

поняті:
1) Козін А.Ф. /підпис/;
2) Бунін В.М. /підпис/;
спеціаліст Котов С.І. /підпис/;
слідчий Іванов І.І. /підпис/

Під час огляду застосовано технічні засоби: фотоапаратом "Nikon" зроблені три фотознімки: один оглядовий (загальний вигляд WI-FI роутеру типу «ASUS RT-N10» в кімнаті квартири), два вузлових (один наближений вигляд, інший – вигляд днища роутера, з фіксацією його даних.
(вказується застосовування фото-, відеозйомки, інших технічних та спеціальних засобів, їх технічні параметри)

Огляд проводився в квартирі за адресою: м. Дніпро, вул. Косіора, 71, кв. 10 при штучному освітленні

(вказуються погодні умови, освітлення, температура повітря, інші необхідні дані)

До протоколу огляду додаються: WI-FI роутер типу «ASUS RT-N10»,

(план (схематичний чи масштабний); схема місцевості; схема огляду місця події; схема доріжки слідів; схема сліду низу взуття; схема сліду знаряддя зламу; інше)

фотознімки з фотоапарату "Nikon".

(носії комп'ютерної інформації та інші матеріали, які пояснюють зміст протоколу)

Протокол прочитано, записано слідчим зачитаний вголос, записано в точній відповідності до проведених процесуальних дій та отриманих результатів.

Зауважень від учасників не надійшло.

(зауваження учасників огляду)

З протоколом ознайомлені:

учасники:

1. Котов С.І. /_____/
   (прізвище, ім'я, по батькові) (підпис)
2. Сомов С.С. /_____/
   (прізвище, ім'я, по батькові) (підпис)

поняті:

1. Козін А.Ф. /_____/
   (прізвище, ім'я, по батькові) (підпис)
2. Бунін В.М. /_____/
   (прізвище, ім'я, по батькові) (підпис)

Огляд провів та протокол склав:
слідчий СВ Індустріального ВП Дніпровського ВП
ГУ НП України в Дніпропетровській області
капітан поліції _____ **І.І. Іванов**

(підпис)

Додаток № 3

ПРОТОКОЛ
тимчасового доступу до речей та документів

Місто (сел.) _Дніпро__ «20» 09.2022 року

Тимчасовий доступ почато о “20” год. “40” хв.
Тимчасовий доступ закінчено о “22” год. “50” хв.

__Слідчий СВ Індустріального ВП Дніпровського ВП ГУ НП України в Дніпропетровській області капітан поліції Іванов І.І._____
(слідчий, найменування органу, прізвище, ім’я, по батькові)
на підставі _кримінального провадження № 12012160_____
відповідно до ст. 40, 104, 105, 106, 159, 223 КПК України:
у присутності понятих:
1) _Козіна Альберта Федоровича, 28.02.1965 р. н., який мешкає у м. Дніпро,___ вул. Косіора, 71, кв. 15;_____
(прізвище, ім’я, по батькові, дата народження, місце проживання)
2) _Буніна Валерія Миколайовича, 21.01.1983 р. н., який мешкає у м. Дніпро,__ вул. Косіора, 71, кв. 4,_____
(прізвище, ім’я, по батькові, дата народження, місце проживання)
яким відповідно до ст. 11, 13, 15, 223 КПК України роз’яснено їхні права і обов’язки.

1) _____ 2) _____
(підпис) (підпис)

За участю потерпілого:
___Сомова Сергія Семеновича, 14.02.1975 р. н., який мешкає у м. Дніпро,____ вул. Косіора, 71, кв. 10_____,
(прізвище, ім’я, по батькові, дата народження, місце проживання)
якому відповідно до ч. 1, 2 ст. 56, ст. 57 КПК України роз’яснено його права і обов’язки.

_____
(підпис)

За участю спеціаліста:
оперуповноважений Управління кіберполіції НП України у Дніпропетровській області Сидоренка Юрія Івановича_____,
(прізвище, ім’я, по батькові)
якому відповідно до ч.4,5 ст.71 КПК України роз’яснено його права і обов’язки.

_____
(підпис)

За участю власника (користувача) приміщення чи іншого володіння особи
Сомова Сергія Семеновича, який мешкає у м. Дніпро, вул. Косіора, 71, кв. 10
(прізвище ім'я, по батькові, адреса)

_____
(підпис)

здійсненний тимчасовий доступ до виявленого предмета WI-FI роутеру типу «ASUS RT-N10» чорного кольору прямокутної плоскої форми з однією антеною, що належить потерпілому Сомову С.С. та добровільно наданий ним для тимчасового доступу.

Перед початком тимчасового доступу до роутера зазначеним особам роз'яснено їхнє право бути присутніми при всіх діях, які проводяться в процесі тимчасового доступу, робити зауваження, що підлягають занесенню до протоколу. Особам, які беруть участь у проведенні тимчасового доступу, також роз'яснено вимоги ч. 3 ст. 66 КПК України про їх обов'язок не розголошувати відомості щодо проведеної процесуальної дії.

Під час тимчасового доступу застосовано технічні засоби: ноутбук «Samsung Galaxy Book Pro NP950XDB»

(вказується застосування фото-, відеозйомки, інших технічних та спеціальних засобів, їх найменування, технічні параметри)

Здійснено тимчасовий доступ до речей та встановлено: спеціаліст Управління кіберполіції НП України у Дніпропетровській області Сидоренко Ю.І. обстежив WI-FI роутер типу «ASUS RT-N10» чорного кольору прямокутної плоскої форми з однією антеною, під'єднаний шнуром до електричної мережі та інтернет-кабелем до роутера, та підключив цей роутер до ноутбуку «Samsung Galaxy Book Pro NP950XDB». За допомогою цього ноутбука було здійснено вхід до інтерфейса WI-FI роутера типу «ASUS RT-N10». При цьому спеціаліст наголосом озвучував послідовність своїх дій. Встановлено інформація про MAC-адреси девайсів, які підключалися до роутеру в період вчинення злочину.

Під час тимчасового доступу виявлено: в інтерфейсі WI-FI роутеру типу «ASUS RT-N10» було виявлено інформація зі списком користувачів, які підключались до роутеру, системний журнал, у якому міститься інформація про MAC-адреси девайсів, які підключалися до роутеру, системний журнал, у якому міститься інформація про дату та час підключення користувача до мережі.

Виявлено під час тимчасового доступу, зафіксовано та вилучено: отримана інформація з інтерфейса WI-FI роутера типу «ASUS RT-N10» у виді скріншот з ноутбука «Samsung Galaxy Book Pro NP950XDB» копійована на цифровий диск «CD-R» (№YH05035339) у виді файла «провадження № 12012160», засвідчений електронним підписом спеціаліста. Цифровий диск «CD-R» (№YH05035339) покладений у паперовий білий конверт заклеєний та підписаний слідчим, спеціалістом та понятими. На пакет наклеєно паперову бирку. На бирці зазначено: «20 вересня 2021 року Індустріальний ВП Дніпровського ВП ГУ НП у Дніпропетровській області, цифровий диск «CD-R» (№YH05035339)».

поняті:
1) Козін А.Ф. /підпис/;
2) Бунін В.М. /підпис/;
спеціаліст Сидоренко Ю.І. /підпис/;
слідчий Іванов І.І. /підпис/

Під час тимчасового доступу до речей застосовано технічні засоби:
використовуючи ноутбук «Samsung Galaxy Book Pro NP950XDB» здійснено тимчасовий доступ до даних роутера, які були занесені на цифровий диск «CD-R» (№ YH05035339).
(вказується застосовування фото-, відеозйомки, інших технічних та спеціальних засобів, їх технічні параметри)

Тимчасовий доступ до речей проводився в квартирі за адресою: м. Дніпро, вул. Косіора, 71, кв. 10.

До протоколу додаються: розпечатані скріншоти зображення з екрану ноутбука, де відображені MAC-адреси девайсів, які підключались до роутеру; цифровий носій інформації («CD-R» (№ YH05035339»), на якому зафіксовано відповідні скріншоти.

Протокол прочитано, записано слідчим зачитаний вголос, записано в точній відповідності до проведених процесуальних дій та отриманих результатів. Зауважень від учасників не надійшло.
(зауваження учасників огляду)

З протоколом ознайомлені:
учасники:
1. Сидоренко Ю.І. /_____/
(прізвище, ім'я, по батькові) (підпис)
2. Сомов С.С. /_____/
(прізвище, ім'я, по батькові) (підпис)

поняті:
1. Козін А.Ф. /_____/
(прізвище, ім'я, по батькові) (підпис)
2. Бунін В.М. /_____/
(прізвище, ім'я, по батькові) (підпис)

Протокол склав:
слідчий СВ Індустріального ВП Дніпровського ВП
ГУ НП України в Дніпропетровській області
капітан поліції _____ **І.І. Іванов**
(підпис)

Список використаних джерел

1. Використання електронних (цифрових) доказів у кримінальних провадженнях : методичні рекомендації / М.В. Гуцалюк, В.Д. Гавловський та ін. Київ : Нац. ак. вн. справ, 2020. 104 с.

2. Кобець М. В., Кобець Р. М. Використання можливостей wi-fi роутерів під час виявлення та розслідування кримінальних правопорушень. *Криміналістичний вісник* : науково-практичний збірник. Київ : Держ. наук.-дослід. експерт.-кримінал. центр МВС України, 2022. № 2 (38). С. 36-47.

3. Криміналістика : [підручник] / За заг. ред. А.Ф. Волобуєва; МВС України, Харк. нац. ун-т внутр. справ. Харків : ХНУВС, 2011. 666 с.

4. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI.

5. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 07.07.2017 № 575.

6. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГПУ, МВС, СБУ, АДПС, МФ, МЮ України від 16.11.2012 № 114/1042/516/1199/936/1687/5.

7. Про затвердження Переліку радіоелектронних засобів та випромінювальних пристроїв, для експлуатації яких не потрібні дозволи на експлуатацію : рішення Національної комісії з урегулювання зв'язку України від 06.09.2007 № 914.

8. Про електронні довірчі послуги : Закон України 05.10.2017 №2155-VIII.

9. Про захист персональних даних:Закон України від 01.06.2010 №2297-VI.

10. Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 р. // Відомості Верховної Ради, 1992. № 22. Ст. 303.

11. Кобець М. В., Кобець Р. М. Використання можливостей wi-fi роутерів під час виявлення та розслідування кримінальних правопорушень.

Криміналістичний вісник : науково-практичний збірник. Київ : Держ. наук.-дослід. експерт.-кримінал. центр МВС України, 2022. № 2 (38). С. 36-47.

12. Разумков Э.О., Молибога М.П. Практическое руководство по осмотру места происшествия: теория, тактика, техника : учеб.-практ. пособ. / Под ред И.П. Красюка. Киев : Вид-во УкрДГРІ, 2015. 750 с.

13. Спеціальна техніка: основні поняття, терміни та визначення : навчальний посібник / М. В. Кобець, Б. В. Жуков, П. П. Артеменко. Київ : Аванпост-Прим, 2013. 192 с.

14. Цивільний процесуальний кодекс України : Закон України від 18 березня 2004 р. № 1618-IV.