КОМІТЕТ ЗАХИСТУ ПРАВ АДВОКАТІВ ТА ГАРАНТІЙ АДВОКАТСЬКОЇ ДІЯЛЬНОСТІ НААУ

НАЦІОНАЛЬНА АСОЦІАЦІЯ АДВОКАТІВ УКРАЇНИ
КОМІТЕТ З ПИТАНЬ КІБЕРБЕЗПЕКИ ТА ВІРТУАЛЬНИХ АКТИВІВ

ЮРИДИЧНІ ТА ТЕХНІЧНІ ЗАХОДИ ЗАХИСТУ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

ЩОДО ЗАХИСТУ АДВОКАТСЬКОЇ ТАЄМНИЦІ В ЦИФРОВОМУ СЕРЕДОВИЩІ ТА ДІЙ АДВОКАТА У РАЗІ КІБЕРІНЦИДЕНТУ

ВЕРЕСЕНЬ 2026 РОКУ

Організаційні й технічні заходи мають рекомендаційний характер та застосовуються з урахуванням Правил адвокатської етики [1] та професійних обов'язків адвоката. Вони не замінюють вимог законодавства щодо адвокатської таємниці й процесуальних гарантій. Конкретні засоби захисту обираються з урахуванням пристрою та ризиків.

ЯК ПОБУДОВАНО ДОКУМЕНТ

Частини I і V-VIII містять правову складову: норми, їх межі, кваліфікацію неправомірного втручання, засоби реагування та алгоритм.

Частина II описує першочергові організаційні дії,

Частини III і IV – технічний захист і реагування на кіберінцидент. Частина III також охоплює фізичне зберігання носіїв, резервне копіювання, підготовку техніки до ремонту, перевірку після нього та виведення техніки з експлуатації; Частина IV - дії при втраті чи крадіжці пристрою.

Додаток А – самостійна картка швидкого реагування для друку; вона дублює частину інформації у стислому вигляді.

Додаток Б показує, на яку норму НПА посилається кожен розділ картки.

ЧАСТИНА І
ПРАВОВІ ЗАСАДИ ЗАХИСТУ АДВОКАТСЬКОЇ ТАЄМНИЦІ

1.1. Що становить адвокатську таємницю та обов'язки щодо її збереження

Відомості про клієнтів, листування, матеріали справ, проєкти документів та інша інформація, отримана під час адвокатської діяльності, можуть становити адвокатську таємницю незалежно від способу їх зберігання. Стаття 22 Закону України «Про адвокатуру та адвокатську діяльність» зобов'язує адвоката, адвокатське бюро та адвокатське об'єднання забезпечувати умови, що унеможливлюють доступ сторонніх осіб до такої інформації або її розголошення. Цей обов'язок необхідно враховувати і під час ремонту, налаштування, перевірки та дослідження техніки. [2]

Згода адвоката на технічну допомогу не повинна трактуватися як необмежений дозвіл на ознайомлення з інформацією клієнтів. Володіння комп'ютером саме по собі не дозволяє адвокату довільно скасовувати режим адвокатської таємниці. Зокрема, передбачена частиною другою статті 22 можливість втрати інформацією такого статусу пов'язана з письмовою заявою клієнта; для відомостей про третіх осіб додатково враховуються вимоги щодо захисту персональних даних. [2]

До надання доступу необхідно визначити його мету, правову підставу, виконавців і межі дослідження. Передання всього клієнтського архіву «для перевірки комп'ютера» потребує окремого обґрунтування.

1.2. Гарантії адвокатської діяльності та заборона втручання у спілкування

Вихідна конституційна гарантія сформульована у статті 31 Конституції України: «Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо». [19]

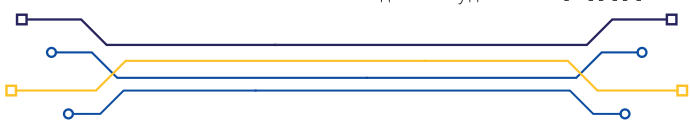
Та сама конструкція відтворена у статті 14 КПК України: втручання у таємницю спілкування можливе лише на підставі судового рішення у передбачених Кодексом випадках, а частина третя цієї статті обмежує використання здобутого: «Інформація, отримана внаслідок втручання у спілкування, не може бути використана інакше як для вирішення завдань кримінального провадження». [20]

Стаття 258 КПК України встановлює, що ніхто не може зазнавати втручання у приватне спілкування без ухвали слідчого судді, і перелічує чотири його різновиди: аудіо-, відеоконтроль особи; арешт, огляд і виїмка кореспонденції; зняття інформації з електронних комунікаційних мереж; зняття інформації з електронних інформаційних систем. [20]

Ключова норма. Частина п'ята статті 258 КПК України: «Втручання у приватне спілкування захисника, священнослужителя з підозрюваним, обвинуваченим, засудженим, виправданим заборонене». На відміну від частини першої, яка допускає втручання на підставі ухвали слідчого судді, частина п'ята механізму надання дозволу не передбачає. Її дія охоплює спілкування захисника з особою, яку він захищає у кримінальному провадженні; спілкування адвоката з клієнтом в інших справах (цивільних, сімейних, господарських тощо) захищається пунктом 9 частини першої статті 23 Закону, яким забороняється втручання у приватне спілкування адвоката з клієнтом. [20] [3]

Стаття 161 КПК України відносить до речей і документів, до яких заборонено доступ, «листування або інші форми обміну інформацією між захисником та його клієнтом або будь-якою особою, яка представляє його клієнта, у зв'язку з наданням правової допомоги», а також об'єкти, додані до такого листування. [20]

Стаття 162 КПК України окремо перелічує охоронювану законом таємницю, що міститься у речах і документах; серед позицій переліку - конфіденційна інформація, особисте листування особи та інші записи особистого характеру, персональні дані, а також інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента та надання телекомунікаційних послуг. Адвокатська таємниця як окрема позиція у цьому переліку не названа: її захист забезпечується статтею 161 КПК та статтями 22 і 23 Закону України «Про адвокатуру та адвокатську діяльність». [20] [2] [3]



Гарантії адвокатської діяльності, релевантні для ситуації прослуховування або несанкціонованого доступу, сконцентровані у частині першій статті 23 Закону: пункт 1 — заборона будь-яких втручань і перешкод здійсненню адвокатської діяльності; пункт 3 — оперативно-розшукові заходи чи слідчі дії стосовно адвоката, які проводяться виключно з дозволу суду, здійснюються на підставі судового рішення, ухваленого за клопотанням Генерального прокурора, його заступників, прокурора Автономної Республіки Крим, області, міста Києва та міста Севастополя; пункт 4 — заборона проведення огляду, розголошення, витребування чи вилучення документів, пов'язаних із здійсненням адвокатської діяльності; пункт 8 - заборона залучати адвоката до конфіденційного співробітництва, якщо воно пов'язане або може призвести до розкриття адвокатської таємниці; пункт 9 — «забороняється втручання у приватне спілкування адвоката з клієнтом». [3]

Частина третя статті 23 Закону покладає на органи державної влади, органи місцевого самоврядування та їх посадових і службових осіб обов'язок дотримуватися у відносинах з адвокатами Конвенції про захист прав людини і основоположних свобод та практики Європейського суду з прав людини. Це робить посилання на практику ЄСПЛ (Частина VII) не факультативним аргументом, а елементом національного правового обов'язку. [3]

1.3. Телефон і офіс: законний порядок зняття інформації

Телефонний трафік і зміст розмов. Зняття інформації з електронних комунікаційних мереж (стаття 263 КПК України) є різновидом втручання у приватне спілкування, що проводиться без відома особи на підставі ухвали слідчого судді. Ухвала додатково повинна містити ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, електронну комунікаційну мережу та кінцеве (термінальне) обладнання. Виконання покладається на уповноважені підрозділи органів Національної поліції, Бюро економічної безпеки України, Національного антикорупційного бюро України, Державного бюро розслідувань та органів безпеки; оператори зобов'язані сприяти таким діям і не розголошувати їх факт. [20]

Практичний наслідок: законне зняття інформації з електронних комунікаційних мереж здійснюють лише уповноважені підрозділи, перелічені в частині четвертій статті 263, на підставі ухвали слідчого судді з ідентифікаційними ознаками абонента, мережі та кінцевого обладнання (частина друга), а оператори електронних комунікацій зобов'язані сприяти таким діям і не розголошувати їх факт. Тому самі по собі технічні ознаки втручання не свідчать ні про законність, ні про незаконність заходу: правова оцінка можлива лише з використанням механізмів, описаних у пункті 5.1, а за відсутності законної підстави - за складами, наведеними в пункті 5.2. [20]

1.4. Комп'ютер, електронна пошта та хмарні сховища

Дані на пристрої та в облікових записах. Стаття 264 КПК України регулює пошук, виявлення і фіксацію відомостей в електронній інформаційній системі та доступ до неї без відома власника, володільця або утримувача - на підставі ухвали слідчого судді. Частина друга цієї статті встановлює виняток: дозволу слідчого судді не потребує здобуття відомостей із систем, «доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту». [20]

Практичне значення частини другої статті 264 КПК. Пароль, PIN-код, біометричне розблокування та шифрування диска є системою логічного захисту, тому негласний доступ до захищеного пристрою адвоката потребує ухвали слідчого судді. Водночас під час обшуку на підставі ухвали частина шоста статті 236 КПК надає слідчому, прокурору право долати системи логічного захисту, якщо присутня особа відмовляється їх зняти, а також здійснювати на місці пошук і фіксацію даних у комп'ютерних системах і мобільних терміналах, для виявлення яких дозвіл не надавався. Отже, відмова розблокувати пристрій під час обшуку доступ не зупиняє; засобами захисту залишаються заяви, що заносяться до протоколу (частина восьма статті 236), та посилання на статтю 161 КПК і пункт 4 частини першої статті 23 Закону. Добровільне розблокування поза процесуальною дією усуває саму ознаку «подолання захисту», тому межі добровільної згоди (пункт 1.5) мають пряме процесуальне значення. [20] [3]

Стаття 159 КПК передбачає тимчасовий доступ до електронних систем шляхом копіювання інформації без вилучення самих систем. Водночас стаття 168 встановлює винятки, за яких техніка може бути вилучена, зокрема за необхідності експертного дослідження або подолання логічного захисту. Тому шифрування не гарантує неможливості вилучення пристрою. [4]

На вимогу володільця особа, яка здійснює тимчасове вилучення комп'ютерних систем або їх частин, залишає йому копії інформації з них за наявності технічної можливості копіювання (абзац п'ятий частини другої статті 168 КПК). Для адвоката це засіб зберегти доступ до матеріалів клієнтів. Абзац шостий тієї ж частини поширює це правило на інформацію з обмеженим доступом лише в частині, що не суперечить встановленому порядку її обігу та захисту. [20]

1.5. Межі добровільного доступу та діагностики

До початку добровільного технічного дослідження слід письмово погодити конкретне завдання: перевірити певне підключення, підозрілий процес, програму або визначений період активності. Окремо зазначаються дозволені дії, перелік даних для збирання, можливість створення копій, місце їх зберігання та особи, які отримають доступ.

Розширення меж добровільного дослідження слід погоджувати окремо. Передання паролів, ключів відновлення, доступу до пошти або хмарних сховищ не слід автоматично включати до загальної згоди «перевірити комп'ютер». Технічні стандарти цифрових досліджень також передбачають попереднє визначення правових повноважень, обсягу роботи й обмежень щодо конфіденційної інформації. [5]

За процесуального доступу адвокату рекомендується клопотати про цільове копіювання потрібних даних, обмеження дослідження релевантним періодом та відокремлення матеріалів інших клієнтів. Погодження таких заходів має відбуватися в межах відповідної процедури.

Правовою межею добровільної згоди є частина друга статті 22 Закону: інформація або документи можуть втратити статус адвокатської таємниці за письмовою заявою клієнта. Отже, згода самого адвоката на технічне дослідження не знімає режим таємниці з матеріалів клієнтів — вона лише визначає обсяг технічних дій, які адвокат допускає, і не може бути ширшою за цей обсяг. [2]

1.6. Процесуальні гарантії під час обшуку, огляду та тимчасового доступу

Для заходів стосовно адвоката, які потребують судового дозволу, необхідно перевіряти дотримання спеціальних вимог статті 23 Закону, зокрема щодо належного суб'єкта звернення з клопотанням та конкретизації предмета відповідних дій. **Наявність ухвали не означає необмеженого дозволу досліджувати всі матеріали адвокатської діяльності:** стаття 23 містить спеціальні заборони щодо таких документів. [3]

Окремо стаття 161 КПК України забороняє тимчасовий доступ до пов'язаного з наданням правової допомоги листування та інших форм обміну інформацією між захисником і клієнтом або його представником, а також до доданих до них об'єктів. [4]

Під час дій, визначених частиною другою статті 23 Закону, передбачена участь представника ради адвокатів регіону та завчасне повідомлення відповідної ради. Представник має право ставити запитання, подавати зауваження й заперечення до протоколу. Водночас **його неявка за умови завчасного повідомлення ради не перешкоджає проведенню дії**. Участь членів комітетів не замінює цього представника й не є самостійною обов'язковою умовою кожної перевірки. [3]

Під час обшуку слід перевірити пред'явлення ухвали та вручення її копії, вимагати допуску адвоката, належної фіксації перебігу дії та внесення заперечень до протоколу. КПК передбачає допуск адвоката на будь-якому етапі обшуку й обов'язкову аудіо- та відеофіксацію обшуку житла чи іншого володіння за судовою ухвалою. [4]

Правову підставу доступу необхідно встановлювати окремо в кожному випадку, з урахуванням добровільного характеру допомоги, невідкладних випадків за статтею 233 КПК та спеціальних умов статті 615 КПК. Сам факт воєнного стану не дає загального дозволу діяти без суду: заміщення відповідних повноважень слідчого судді потребує встановлених законом обставин, зокрема об'єктивної неможливості їх виконання суддею. [4]

Уточнення, важливе для практики. Завчасне повідомлення ради адвокатів регіону є обов'язком службової особи, яка проводить процесуальну дію, а не завданням адвоката; неявка представника ради за умови завчасного повідомлення не перешкоджає проведенню дії (частина друга статті 23 Закону). Тому розрахунок на те, що відсутність представника зупинить обшук, є помилковим: реальним засобом захисту залишаються допуск адвоката, фіксація дії та внесення заперечень до протоколу. [3]

Воєнний стан. Пункт 2 частини першої статті 615 КПК передбачає, що за відсутності об'єктивної можливості виконання слідчим суддею повноважень, зокрема за статтями 163, 164, 233, 234, 235 і 245-248, такі повноваження виконує керівник відповідного органу прокуратури; рішення приймається постановою, яка має містити обґрунтування правомірності здійснення ним повноважень слідчого судді. Тому слід з'ясувати, що саме пред'явлено - ухвалу слідчого судді чи постанову керівника органу прокуратури, — і в другому випадку перевірити наявність такого обґрунтування. Скарги на рішення, дії чи бездіяльність прокурора, слідчого, прийняті на виконання цих повноважень, можуть бути подані до суду (частина четверта статті 615). Пункт 3 частини першої статті 23 Закону для слідчих дій стосовно адвоката вимагає саме судового рішення; співвідношення цих норм законом прямо не врегульоване і є предметом правової позиції в конкретній справі. [20] [3]

ЧАСТИНА ІІ
ПЕРШОЧЕРГОВІ ДІЇ АДВОКАТА

2.1. Встановлення осіб, правової підстави, мети та меж

У разі повідомлення про можливе зараження комп'ютера, витік інформації або використання пристрою третіми особами рекомендується спочатку встановити особи представників органу, їхні повноваження та характер запропонованих дій.

Необхідно з'ясувати, чи йдеться про добровільну допомогу в реагуванні на кіберінцидент, процесуальний огляд, обшук, тимчасовий доступ або інший захід. Для кожного випадку слід уточнити конкретну правову підставу. Формулювання «технічна перевірка» недостатньо для розуміння допустимого обсягу доступу.

Доцільно попросити надати доступні для розголошення технічні відомості: час виявленої активності, ознаки можливого втручання, пов'язані адреси чи файли, а також пояснення, чому перевірки потребує саме цей пристрій. Відсутність таких відомостей у первинній розмові слід зафіксувати, однак сама собою вона не доводить неправдивості повідомлення.

Рекомендується одразу повідомити про ситуацію раду адвокатів регіону, залучити іншого адвоката для правничої допомоги та звернутися до профільного комітету щодо участі технічного фахівця.

2.2. Формулювання позиції адвоката

Зразок повідомлення про наявність адвокатської таємниці:

«На цьому пристрої зберігається інформація, що становить адвокатську таємницю. Прошу повідомити правову підставу, мету та обсяг запланованих дій. Я готовий сприяти перевірці можливого кіберінциденту з дотриманням гарантій адвокатської діяльності. Прошу забезпечити фіксацію дій та розглянути можливість залучення незалежного технічного фахівця».

Розширений варіант цього формулювання, придатний для усного використання на місці, наведено у Додатку А (розділ 3).

2.3. Якщо доступ або копіювання вже відбулися

Необхідно невідкладно скласти хронологію подій із зазначенням осіб, які зверталися до адвоката, змісту їхніх повідомлень, пред'явлених документів, обсягу наданого доступу, запущених програм, підключених носіїв та переданих даних.

У належній правовій формі слід з'ясувати обсяг виконаних дій, зокрема створення образу накопичувача, копіювання окремих каталогів, відкриття клієнтських документів та встановлення засобів віддаленого доступу. Окремо необхідно встановити місце зберігання отриманих даних і порядок їх подальшого використання.

Після цього доцільно провести незалежну технічну оцінку й визначити правові засоби реагування. Питання інформування клієнтів слід вирішувати з урахуванням установлених обставин, можливих наслідків та застосовних обов'язків щодо повідомлення. При цьому повідомлення про інцидент саме може містити чутливу інформацію й потребує контрольованого поширення. [6]

Слід утримуватися від фізичного перешкоджання законним діям, видалення інформації, дистанційного очищення пристроїв або знищення потенційних доказів. Незгоду з діями та рішеннями необхідно оформлювати запереченнями, клопотаннями та належними засобами оскарження.

Деталізований перелік обставин, які підлягають фіксації у першу чергу, наведено у Додатку А (розділ 7).

2.4. Організація реагування радою адвокатів регіону

Раді адвокатів регіону рекомендується зареєструвати звернення, визначити відповідальну особу, забезпечити оперативну правову оцінку та координацію з Комітетом захисту прав адвокатів та гарантій адвокатської діяльності НААУ і Комітетом НААУ з питань кібербезпеки та віртуальних активів.

В окремому матеріалі реагування доцільно зберігати повідомлення адвоката, процесуальні документи, хронологію, зафіксовані заперечення та результати технічного дослідження. Поширення цих матеріалів усередині органів адвокатського самоврядування також слід обмежувати потребою конкретних виконавців у відповідній інформації.

ЧАСТИНА III
ТЕХНІЧНИЙ ЗАХИСТ АДВОКАТСЬКОЇ ТАЄМНИЦІ

Заходи цієї частини добираються з урахуванням пристрою, обсягу матеріалів і ризиків. Адвокат контролює порядок доступу та зберігання інформації; складне налаштування, відновлення даних і дослідження інциденту доручаються компетентному фахівцю. Згадані програми є прикладами засобів захисту, а не вимогою придбати конкретний продукт.

3.1. Шифрування комп'ютерів і носіїв

Рекомендований базовий захід — шифрування накопичувачів, на яких зберігається адвокатська таємниця, із перевіркою фактичного стану захисту.

Що таке шифрування. Це спосіб зберігання, за якого зміст файлів перетворюється на дані, непридатні для звичайного читання без відповідного ключа. Після дозволеного розблокування адвокат працює з документами у звичний спосіб.

Шифрування особливо важливе при втраті ноутбука або диска: фізичне володіння носієм не повинно автоматично давати доступ до матеріалів справ. [7] [8] [9]

Пароль входу та шифрування виконують різні завдання. Пароль обмежує вхід до робочого середовища. Шифрування додатково захищає самі дані на накопичувачі. Наявність вікна із запитом пароля ще не підтверджує, що диск зашифрований, тому необхідно перевірити відповідне налаштування, а не покладатися лише на блокування екрана. [7] [36]

Накопичувач — це внутрішній диск комп'ютера або окремий носій, наприклад зовнішній диск чи флешка. Рекомендується шифрувати кожний носій із клієнтськими матеріалами. Захист внутрішнього диска не поширюється автоматично на флешку, на яку скопійовано документ. [7] [36]

Система	Рекомендований підхід
Windows	BitLocker або функція «Шифрування пристрою» на сумісних конфігураціях. Перевірити, що захист активний і поширюється на потрібні диски. Для підвищеного ризику розглянути BitLocker із додатковим PIN-кодом перед завантаженням. Знайдіть відповідний пункт у системних налаштуваннях і перевірте, що захист не призупинено. Налаштування TPM - модуля безпеки комп'ютера — разом із додатковим PIN-кодом виконує фахівець. [7]
Linux	Шифрування на основі LUKS, переважно LUKS2/dm-crypt у підтримуваній конфігурації дистрибутива. Окремо перевірити охоплення робочих розділів і областей, куди система може записувати тимчасові дані. Налаштування виконує фахівець для конкретної версії системи. [8]
macOS	Увімкнути FileVault. На сучасних Mac апаратне шифрування накопичувача та ввімкнений FileVault мають відмінності: FileVault додає захист, пов'язаний з обліковими даними користувача. Стан FileVault перевіряється в системних параметрах; зазначена відмінність стосується сучасних Mac із процесором Apple або чипом T2. [9]

Для окремих зашифрованих контейнерів рекомендується використовувати VeraCrypt у підтримуваній конфігурації після налаштування фахівцем. Контейнер слід відкривати лише на час роботи. Після відкриття документів їхні незашифровані фрагменти можуть залишатися в оперативній пам'яті. [10]

Зашифрований контейнер можна уявити як окремий електронний сейф для файлів: після введення пароля він відкривається як додатковий диск, усередині якого можна зберігати папки окремих справ. Після роботи слід закрити документи й від'єднати контейнер через програму; закриття лише вікна папки недостатньо. Створення порожнього контейнера не шифрує документи, які залишилися поза ним. [10] [45]

Шифрування накопичувача насамперед захищає дані у стані зберігання. Воно не створює окремої перешкоди для програми чи особи, яка вже отримала доступ до розблокованої системи та відкритих матеріалів. [7]

Ключі відновлення необхідно зберігати захищено та окремо від пристрою. Слід перевірити, чи не збережені вони автоматично в особистому або корпоративному обліковому записі, і відповідно захистити цей обліковий запис. [7]

Ключ відновлення — це резервний засіб доступу на випадок, коли звичайне розблокування не спрацьовує, зокрема після несправності або зміни обладнання. Перевірте, у чиєму обліковому записі він міститься: адвоката, організації чи особи, яка налаштовувала техніку. Втрата всіх засобів розблокування може призвести до втрати доступу до даних. [7] [9]

Приклад. Викрадений зашифрований ноутбук із недоступними сторонній особі засобами розблокування має додатковий захист від прочитання даних. Переданий майстру вже розблокований ноутбук із відкритою папкою справ створює іншу ситуацію: доступні користувачу файли можуть бути доступні й особі, яка працює за комп'ютером. [7] [10]

Першочергове завдання адвоката – попросити фахівця показати, що саме зашифровано, як перевірити стан захисту та де зберігається ключ відновлення. Початкове налаштування і перенесення наявного архіву варто виконувати після перевіреного резервного копіювання (пункт 3.5). Не слід самостійно змінювати параметри дисків за випадковою інструкцією.

3.2. Захист смартфонів

Телефон слід розглядати як робочий носій: у ньому можуть бути листування, документи, фотографії матеріалів справ і доступ до пошти. Захист потрібний також тоді, коли адвокат відкриває документи лише через застосунки та не створює окремої папки «Клієнти».

Android. Рекомендується використовувати пристрій із підтримуваною системою, налаштованим блокуванням і штатним шифруванням. Для пристроїв, що виходять з Android 10 або новішою версією, файлове шифрування є обов'язковою вимогою платформи. На конкретному пристрої необхідно перевірити налаштування та фактичний стан захисту. Захист зовнішньої карти пам'яті оцінюється окремо. [11]

iPhone. Рекомендується встановити довгий унікальний буквено–цифровий код допуску. Код бере участь у захисті ключів шифрування; біометрія дозволяє зручно використовувати складніший код, однак не замінює його. [12]

Сам шестизначний код не є безпосередньо ключем шифрування кожного файла: він працює разом із вбудованими захисними механізмами телефона. Практичний висновок: особа, якій передано телефон і його код, може розблокувати пристрій та переглянути інформацію, що не захищена додатково. [12]

Код екрана, пароль Apple Account або Google Account та пароль окремого застосунку можуть бути різними; зміна одного з них не означає автоматичної зміни інших. Не використовуйте дату народження, очевидну послідовність або один код для всіх пристроїв. Face ID чи відбиток пальця полегшують щоденне використання складного коду; сам код потрібно зберігати в таємниці. [12] [34]

Адвокатам із підвищеним ризиком цільового стеження рекомендується увімкнути «Режим карантину» / Lockdown Mode, попередньо ознайомившись з обмеженнями його роботи. Apple позиціонує цей режим як додатковий захист від високотехнологічних цільових атак. Увімкнення режиму не підтверджує відсутності компрометації та не замінює дослідження пристрою. [13]

На обох платформах слід обмежити показ змісту робочих повідомлень на заблокованому екрані та встановити короткий період автоматичного блокування.

Перевірка проста: заблокуйте телефон і попросіть колегу надіслати тестове повідомлення без конфіденційних відомостей. Його зміст не повинен бути видимий сторонній людині.

3.3. Відокремлення клієнтських матеріалів і повсякденна кібергігієна

Кібергігієна в цих рекомендаціях означає щоденні дії, які зменшують ризик стороннього доступу: оновлення, захист паролів, перевірку повідомлень і контроль за тим, де залишаються копії документів.

Для роботи з клієнтськими матеріалами рекомендується використовувати окремий робочий пристрій. За відсутності такої можливості – окремий робочий обліковий запис і зашифроване сховище. Доступ помічників, працівників та технічних підрядників слід обмежувати їхніми завданнями.

Такий пристрій не передається для побутового користування. Обліковий запис – це власне робоче середовище користувача. Він допомагає розділити повсякденну роботу, але особа з правами адміністратора, тобто розширеними повноваженнями керування комп'ютером, може мати значно ширший доступ. [36] [37]

Під час налаштування необхідно враховувати розташування додаткових копій документів: у пошті, месенджерах, папці завантажень, автоматичних збереженнях і хмарній синхронізації. Слід мінімізувати кількість таких копій та не зберігати весь архів практики на кожному переносному пристрої.

Додаткові копії часто залишаються також на робочому столі. Хмарне сховище – це зберігання на обладнанні постачальника сервісу з доступом через інтернет. Передавання файла до захищеного архіву не прибирає попередні копії в інших місцях. На переносному пристрої доцільно тримати матеріали, потрібні для поточної роботи. [36] [38]

До базових заходів належать своєчасні оновлення, унікальні паролі, менеджер паролів, багатофакторна автентифікація для пошти й робочих сервісів та резервне копіювання. Для клієнтських матеріалів резервні копії також мають бути захищені, а можливість відновлення – періодично перевірена. [14]

Паролі та додаткова перевірка входу. Для пошти, хмарних сховищ і важливих сервісів використовуйте різні паролі. Менеджер паролів – це спеціальна програма для їх захищеного зберігання; основний пароль до неї потрібно особливо берегти. За двофакторної автентифікації після пароля сервіс вимагає підтвердження в застосунку, одноразовий код або спеціальний фізичний ключ. Це ускладнює сторонній вхід у разі викрадення пароля. [35] [46]

Не повідомляйте коди підтвердження іншій особі та не підтверджуйте запит на вхід, якого ви не розпочинали. Заздалегідь збережіть резервні коди доступу в захищеному місці: втрата телефона не повинна позбавити доступу до всієї робочої інформації. Увімкніть автоматичні оновлення системи, браузера та робочих програм і перевіряйте їх завершення. Порядок резервного копіювання викладено в пункті 3.5. [34] [46]

У разі неочікуваного звернення не слід запускати запропоновані «засоби перевірки», встановлювати програми віддаленого доступу або передавати коди підтвердження без незалежної перевірки ініціатора.

Приклад. Надходить лист нібито з матеріалами судової справи, але для відкриття пропонують установити «спеціальний переглядач». Не запускайте його за посиланням із листа. Уточніть повідомлення через відомий раніше номер або самостійно відкритий офіційний ресурс. Знайоме ім'я відправника саме по собі не підтверджує справжності звернення. [47]

Такий самий порядок застосовується до прохання «перевірити віруси», показати екран або встановити програму віддаленої допомоги. Спочатку перевіряються виконавець і завдання. Працівникам та підрядникам надається лише доступ, потрібний для їхньої роботи.

Ризик використання назви органу кіберзахисту для отримання доступу має практичні приклади: у січні 2025 року CERT-UA попереджала про спроби підключення через AnyDesk нібито від її імені. Цей приклад обґрунтовує необхідність перевіряти звернення, але не доводить такої схеми в описаному випадку з адвокатом. [15]

3.4. Фізичне зберігання та переміщення носіїв

Фізичний захист означає контроль за тим, хто може взяти пристрій, винести його або залишитися з ним наодинці. Шифрування потрібно поєднувати із захистом від крадіжки, пошкодження та втрати. До носіїв належать також зовнішні диски HDD і SSD, флешки, карти пам'яті та пристрої з резервними копіями. [36] [37]

Поза роботою зберігайте їх у замкненій шафі або сейфі відповідно до ризику. Для спільного офісу визначте осіб, які мають ключі та право отримувати носії. Доступ до приміщення для прибирання чи обслуговування не повинен автоматично означати доступ до незахищених клієнтських архівів.

Заведіть простий облік: умовне позначення носія, серійний номер за наявності, відповідальна особа, місце зберігання, стан шифрування, дата видачі й повернення. Наприклад: «Диск Б-02, резервна копія, зашифрований, шафа №1, відповідальна особа». Для такого обліку не потрібно розкривати прізвища клієнтів або зміст справ. Сам перелік також зберігається з обмеженим доступом. [37]

Під час поїздок тримайте техніку під особистим контролем. Не залишайте її без нагляду в автомобілі, переговорній або відкритій зоні офісу. Ураховуйте також пожежу, заливання, перегрів і механічне пошкодження. Несправні диски з даними зберігайте так само контрольовано, як робочі.

Приклад. Ноутбук і єдиний диск із резервною копією лежать в одній сумці. Її викрадення одночасно позбавляє адвоката обох примірників архіву. Резервну копію доцільно зберігати окремо від основного пристрою.

Після роботи блокуйте екран і закривайте зашифровані контейнери через відповідну програму. Не прикріплюйте пароль до ноутбука чи диска. Незахищений ключ відновлення в тій самій сумці також створює ризик стороннього доступу. [10] [45]

3.5. Резервне копіювання та перевірка відновлення

Резервна копія, або бекап, – це додатковий примірник інформації, з якого її можна відновити після поломки, викрадення, помилки чи кібератаки. Папка «Копія» на тому самому фізичному диску не захищає від виходу цього диска з ладу. Спочатку визначте, що потрібно для продовження практики: документи справ, робоче листування, контакти та інші необхідні матеріали. [38]

Схема 3–2–1 означає три примірники інформації разом із робочим, щонайменше на двох окремих пристроях або носіях, причому один примірник зберігається поза основним місцем роботи. Практичний варіант: робочий архів на зашифрованому ноутбуці, копія на зашифрованому зовнішньому диску та ще одна захищена копія в іншому місці або відповідному хмарному сервісі. [36] [48]

Одна копія має бути недоступна для звичайної зміни з робочого комп'ютера. Найпростіший приклад – диск, який підключають для копіювання та від'єднують після завершення. Інший варіант налаштовує фахівець: сховище, де робочий обліковий запис не може видалити захищені копії. Це важливо, оскільки шкідлива програма може пошкодити також дані на підключених носіях. [36] [38] [48]

Синхронізація з хмарою потребує окремої перевірки. Вона підтримує однаковий стан папки на кількох пристроях, тому помилкове видалення або зміна можуть передатися й до хмари. Перевірте разом із фахівцем, чи зберігає сервіс попередні версії, як довго вони доступні та хто може їх остаточно видалити. Сам значок успішної синхронізації ще не підтверджує можливості відновити вчорашній документ. [36]

Резервні копії слід шифрувати та захищати паролями й обмеженням доступу. Для локальної копії iPhone на комп'ютері у Finder або Apple Devices окремо ввімкніть «Зашифрувати локальну резервну копію». Шифрування самого телефона не означає автоматичного шифрування цієї копії. Її пароль також потрібно зберегти: він може відрізнятися від коду телефона. [37] [39]

Для активних справ рекомендується автоматичне щоденне копіювання та додаткова копія після значних змін. Доцільно щонайменше раз на місяць перевіряти відновлення кількох документів, зокрема без використання основного ноутбука. Це робочий орієнтир, який коригується залежно від обсягу роботи й допустимих втрат, а не встановлена законом періодичність.

Перевірка на практиці. Відновіть тестовий документ в окрему папку, відкрийте його та звірте зміст і дату потрібної версії. Переконайтеся, що доступні пароль до копії й додаткове підтвердження входу. Запишіть дату перевірки та результат. Не замінюйте робочий архів тестовими даними.

3.6. Підготовка до ремонту та відновлення даних

Спершу відрізніть плановий ремонт від інциденту. Коли є підозра на сторонній доступ або потрібно зберегти цифрові докази, не скидайте пристрій до заводських налаштувань, не очищуйте диск і не перевстановлюйте систему, а дійте за Частиною IV. Спочатку погодьте з фахівцем збереження слідів. Подальші рекомендації з підготовки без робочих даних стосуються планового обслуговування після перевірки потреби їх зберегти. [16] [17]

До передання з'ясуйте, хто виконуватиме роботи, чи залишиться техніка в цьому сервісі, для чого потрібне розблокування і чи можливе обслуговування без перегляду даних. Авторизований статус сервісу не скасовує необхідності підготувати пристрій. Не погоджуйте загальний доступ лише через усне пояснення «так потрібно для діагностики».

Збережіть дані. Якщо пристрій працює, створіть актуальну захищену резервну копію та перевірте відновлення. Ремонт може завершитися заміною накопичувача, скиданням або заміною всього пристрою. Єдина копія матеріалів не повинна залишатися лише в техніці, переданій виконавцю. [40] [41] [42]

Для ноутбука або комп'ютера спочатку з'ясуйте можливість перевірки обладнання без входу до робочої системи. Якщо вид ремонту й конструкція дозволяють, фахівець може вийняти диск із клієнтськими файлами та залишити його адвокату. Сервісу передається техніка без такого диска або з чистим тестовим носієм. Самостійно розбирати пристрій без підготовки не слід.

Коли диск залишається всередині, погоджуйте ремонт без його розблокування. Якщо це неможливо, для планового ремонту разом із фахівцем підготуйте пристрій без робочих матеріалів після перевіреного копіювання. Звичайне видалення папки не рівнозначне належному очищенню. Для Mac виробник описує використання FileVault або стирання даних перед обслуговуванням; конкретний варіант залежить від несправності. [41] [44]

Для смартфона перевірте підтримку штатного режиму ремонту. Наприклад, на сумісних Pixel він створює окреме середовище для діагностики, щоб майстер не працював у звичайному середовищі власника. Код власника передавати не потрібно. Резервна копія все одно необхідна: окремі ремонти вимагають скидання. [42]

Назви сервісних функцій різних виробників можуть бути схожими, а призначення відрізнятися. Статус Apple Ready for Repair or Trade In пов'язаний із сервісною процедурою та роботою функції пошуку пристрою. Його не слід сприймати як підтвердження, що всі клієнтські дані ізольовано від майстра. Перевіряйте інструкцію саме для своєї моделі. [43]

Якщо телефон не вмикається або диск пошкоджений, спочатку потрібна оцінка можливості збереження й захисту даних. Не погоджуйте скидання, коли метою є отримати єдину копію матеріалів. Відновлення доручайте визначеному фахівцю, погодивши обсяг доступу та місце зберігання результату. За невизначеності зверніться до профільного комітету до передання техніки (пункт 4.4).

3.7. Передання пристрою та доступ під час ремонту

Під час приймання зафіксуйте модель, серійний номер, зовнішній стан, комплектність, заявлену несправність і дозволені роботи. Укажіть наявність диска або карти пам'яті. Окремо погодьте створення копій, залучення іншого виконавця, заміну накопичувача та повернення старого компонента. Відомості мають залишитися в адвоката у документі приймання або письмовому погодженні. [37]

Не передавайте код робочого телефона, паролі основних облікових записів, ключі відновлення, одноразові коди входу чи основний пароль менеджера паролів. Зміна коду на «тимчасовий для майстра» не обмежує доступ до того самого вмісту телефона: після отримання такого коду стороння особа може працювати в розблокованому середовищі. [12] [40]

Коли для перевірки конкретної функції потрібне розблокування, погодьте цю операцію, введіть код самостійно та залишайтеся присутнім. Для перевірки камери, друку чи відкриття документа використовуйте тестові матеріали без інформації клієнтів. Контроль сеансу зменшує ризик, але не замінює попередньої підготовки пристрою. Apple також рекомендує не повідомляти сервісу код пристрою та пароль Apple Account. [40]

Приклад. Для заміни клавіатури сервіс просить пароль «від усього». Адвокат погоджує конкретну перевірку клавіш у тестовому середовищі або в його присутності. Коли виконавець наполягає на тривалому необмеженому доступі до робочої системи, порядок ремонту спочатку обговорюється з технічним фахівцем.

Окремий сервісний користувач може обмежити звичайний доступ, але не гарантує захисту від особи з правами адміністратора на розблокованому комп'ютері. Не погоджуйте вимкнення шифрування або передання ключа відновлення без оцінки наслідків і підготовки даних. [36] [37]

Віддалений доступ дозволяє іншій людині працювати з комп'ютером через мережу, інколи майже так само, як за вашим столом. Дозволяйте його лише перевіреному виконавцю для визначеного завдання. Спостерігайте за сеансом, закрийте робоче листування та контейнери. Після завершення переконайтеся разом із фахівцем, що подальше підключення без вашого погодження неможливе. [37]

3.8. Перевірка після повернення з ремонту

До відновлення роботи з матеріалами справ перевірте відповідність пристрою документу приймання та отримайте опис виконаних робіт і замінених компонентів. Зіставте результат із погодженим завданням, з'ясуйте долю старого накопичувача й створених під час робіт копій. [37]

Перевірте повернення захисту до робочого стану: чи ввімкнене шифрування, чи спрацьовує блокування екрана, чи працює резервне копіювання, чи завершено оновлення. Якщо використовувалася функція пошуку пристрою, перевірте також її налаштування. Для цього можна повторити прості перевірки, виконані до ремонту, і попросити фахівця пояснити результат. [40] [41]

Разом із фахівцем перевірте нових користувачів, невідомі програми й невідомі засоби підтвердження входу, зокрема додані біометричні дані. Окремої уваги потребують програми віддаленого доступу, профілі керування – налаштування, що можуть дозволяти організації керувати пристроєм, та VPN–конфігурації – налаштування передавання мережевого з'єднання через інший сервер. Їх поява може мати законне пояснення, але повинна відповідати погодженим роботам. [49]

Якщо пароль уже повідомлявся, змініть його та перевірте активні входи до пов'язаних сервісів. За підозри на сторонній доступ до облікових записів робіть це з іншого, довіреного пристрою. Активний сеанс означає, що браузер або програма вже увійшли до акаунта; його завершення слід перевірити окремо. Порядок заміни переданих ключів шифрування визначає фахівець. Зміна пароля не видаляє копії файлів, які інша особа могла зробити раніше.

3.9. Справність, заміна та виведення техніки з експлуатації

Для роботи з клієнтськими даними потрібна техніка, яка отримує оновлення безпеки. Старий ноутбук може справно відкривати документи, але більше не отримувати виправлень відомих помилок безпеки. У такому разі заплануйте перехід на підтримувану систему або заміну пристрою. Найновіша модель сама по собі не є обов'язковою умовою. [34]

Повторювані помилки відкриття файлів, зникнення диска або збої копіювання потребують діагностики. Коли на пристрої є єдина копія важливих матеріалів, припиніть експерименти з програмами «ремонту диска» та погодьте з фахівцем спосіб збереження даних.

Перед продажем, гарантійною заміною, утилізацією або переданням іншому працівнику перевірте всі носії: внутрішній диск, додаткові диски й карти пам'яті. Спочатку збережіть потрібні дані та перевірте, чи немає обов'язку залишити інформацію або пристрій для дослідження. [44]

Звичайне видалення файлів або швидке форматування не дають гарантії очищення носія: частина даних може залишатися доступною для відновлення. Для диска HDD, накопичувача SSD і смартфона застосовуються різні способи належного очищення. Виконавець має визначити придатний метод і перевірити його результат. [44]

Приклад. Сервіс замінив несправний диск. Старий диск може досі містити клієнтський архів, навіть коли комп'ютер його не розпізнає. Його повернення, контрольоване зберігання або належне знищення погоджуються окремо. Неможливість увімкнути пристрій не підтверджує зникнення даних. [44]

ЧАСТИНА IV

ТЕХНІЧНЕ ВИЯВЛЕННЯ ВТРУЧАННЯ ТА РЕАГУВАННЯ

4.1. Перші технічні дії при підозрі на втручання, втраті або крадіжці пристрою

Втрата або крадіжка. При втраті або крадіжці зафіксуйте час, обставини й останнє відоме місце. Запишіть, чи був пристрій заблокований, чи ввімкнене шифрування та які сервіси залишалися відкритими. З іншого довіреного пристрою використайте доступні штатні засоби блокування, перевірте активні входи й захистіть облікові записи. За втрати телефона зверніться до оператора щодо SIM/eSIM. Не відкладайте повідомлення про інцидент через те, що точний обсяг доступу ще невідомий. [34] [6]

Після виявлення підозрілої активності рекомендується припинити роботу з клієнтськими документами на відповідному пристрої та зв'язатися з фахівцем через інший, довірений засіб зв'язку.

Довірений пристрій у цьому випадку – той, щодо якого немає ознак стороннього доступу і який перебуває під вашим контролем. Збережіть повідомлення про підозрілий вхід, час події та відомості про вже виконані дії. [16] [6]

До первинної оцінки не слід самостійно перевстановлювати систему, видаляти підозрілі файли, очищувати журнали або запускати «лікування» комп'ютера. Перезавантаження та інші втручання можуть змінити або знищити відомості, потрібні для дослідження. Якщо певні дії вже виконано, їх потрібно точно повідомити фахівцю. [16]

Не встановлюйте також випадковий антивірус. Цифрові сліди – це записи та інші дані, за якими можна дослідити подію; частина з них існує лише під час роботи пристрою. Відсутність зовнішніх ознак не дозволяє самостійно виключити втручання. [16] [17]

За ознак активного несанкціонованого доступу слід оперативно вирішити з фахівцем питання мережевої ізоляції. Рішення про відключення мережі, збереження живлення чи вимкнення приймається з урахуванням поточної шкоди та можливості зберегти нестійкі дані. Вимкнення пристрою не є універсальною дією; порядок збирання даних залежить від стану конкретної системи. [17]

Якщо видно активне стороннє керування або масове пошкодження файлів, подальшу шкоду потрібно обмежити оперативно. Мережева ізоляція означає припинення з'єднань із мережею, наприклад від'єднання мережевого кабелю або вимкнення Wi-Fi. За можливості її виконують за вказівкою фахівця. За очевидної активної шкоди та відсутності негайного зв'язку з ним від'єднайте мережу, не стираючи файли, і зафіксуйте дію та час. [16] [17] [6]

Дистанційне стирання не є універсальною першою дією: воно може перешкодити дослідженню й знищити єдині копії інформації. Рекомендації щодо очищення перед плановим ремонтом (пункти 3.6, 3.9) не застосовуються автоматично під час інциденту. Для пристроїв, пов'язаних із процесуальними діями, технічні рішення узгоджуються також з адвокатом, який надає правничу допомогу.

4.2. Первинне дослідження на місці

За можливості адвокату доцільно залучати незалежного фахівця вже на початку перевірки. Його роль – визначити технічно обґрунтований обсяг робіт, оцінити ризик втрати слідів та запропонувати спосіб дослідження з мінімальним розкриттям клієнтських матеріалів. У процесуальній дії питання його залучення вирішується за відповідними правилами.

Повідомлення про «вірус» або «витік» потребує перевірки конкретних обставин. Самостійний перегляд екрана чи короткий запуск антивіруса не дозволяє достовірно встановити весь перебіг події; для цього залучається незалежний фахівець або спеціалізована лабораторія. До початку роботи погодьте з виконавцем ознаки події, період, обсяг доступу та результат, який він має надати. [16] [17] [5]

Первинне дослідження може охоплювати активні процеси, мережеві підключення, засоби віддаленого доступу, системні журнали, механізми автоматичного запуску й конкретні підозрілі файли. Починати з перегляду всіх матеріалів справ зазвичай немає потреби; належний обсяг визначається завданням і виявленими ознаками. [5]

Щоб розуміти запропоновані дії, адвокату достатньо розрізняти основні об'єкти дослідження:

Об'єкт	Пояснення для адвоката
Журнали подій (логи)	Записи системи або сервісів про входи, запуск програм, помилки та інші дії. Вони допомагають відтворити хронологію, але не обов'язково містять усі події. [16]
Мережевий трафік	Обмін даними між пристроєм та іншими системами. Аналіз може показати час і напрям підключень; зашифрований вміст з'єднання може залишатися недоступним для читання. [16]
Образ накопичувача	Технічна копія диска або його частини для дослідження. Залежно від способу створення вона може охоплювати файли, службові дані та залишки раніше видаленої інформації. [17] [18]
Дамп оперативної пам'яті	Копія тимчасової робочої пам'яті пристрою в певний момент. Вона може містити фрагменти відкритих документів, паролі та ключі, тому також потребує захисту. [16] [17]

Прошивка – це внутрішнє програмне забезпечення, яке керує обладнанням. Її копіювання та аналіз потрібні лише за відповідних технічних підстав і не є обов'язковими для кожного повідомлення про вірус. [16] [17]

Дамп оперативної пам'яті, образ накопичувача та копія прошивки є різними об'єктами дослідження. Аналіз прошивки не є універсальною дією під час первинного реагування. Дамп пам'яті може містити документи, паролі та ключі, тому його створення потребує захисту адвокатської таємниці навіть без безпосереднього відкриття клієнтських файлів. [17]

Дослідження організовується з мінімально необхідним доступом до матеріалів клієнтів. Повний образ диска не має створюватися автоматично «про всяк випадок». Якщо потрібний ширший обсяг, фахівець пояснює причину, можливі альтернативи й захист отриманих копій. Навіть без відкриття документів пам'ять, журнали або трафік можуть містити чутливі відомості. [17] [5]

4.3. Встановлення факту втручання та можливого витоку

Наявність шкідливої програми, стороннього доступу та передання клієнтських файлів необхідно встановлювати окремо. Під час дослідження фахівцю рекомендується:

- Визначити ознаки несанкціонованого доступу та період, до якого вони належать.
- Встановити виконані із системою дії та дані, до яких міг бути отриманий доступ.
- Перевірити сліди відкриття, копіювання, архівування або передання конкретної інформації.
- Окремо зазначити підтверджені висновки та обставини, для встановлення яких бракує даних.

Коротке спостереження за трафіком не дозволяє виключити витік, що відбувся раніше. Крім того, шифрування мережевого обміну може приховувати його вміст від засобів спостереження. Висновки потребують зіставлення доступних джерел, а їхні обмеження мають бути прямо зазначені. [16]

Приклад. Адвокату повідомили, що з ноутбука передаються дані. Фахівець перевіряє доступні записи за відповідний період, мережеву активність і програми. Якщо під час десятихвилинного спостереження передавання не виявлено, це ще не означає, що його не було напередодні. У звіті мають бути зазначені межі перевірки. [16] [5]

Наявність шкідливої програми сама по собі не визначає перелік викрадених документів: підтверджені ознаки втручання, його можливий період і сліди доступу або передавання інформації у звіті зазначаються окремо. [16] [5]

Для первинної допомоги може залучатися компетентний фахівець із цифрових досліджень. Якщо результат потрібен як висновок експерта у кримінальному провадженні, необхідно забезпечити належне залучення експерта та дотримання процесуальних вимог. Звичайний технічний звіт не набуває цього статусу лише через назву «експертиза». [4]

4.4. Захист матеріалів дослідження та допомога профільного комітету

Для кожної створеної копії рекомендується фіксувати джерело, дату, спосіб отримання, виконавця, використані інструменти та подальші передання. Цілісність файлів і образів доцільно контролювати криптографічними хеш–значеннями. Саме хешування підтверджує можливість перевірити незмінність даних, проте не доводить законності їх отримання. [18]

Оригінал і робочі копії розмежовуються. Хеш–значення – це обчислений програмою цифровий «відбиток» файла; його порівняння допомагає перевірити, чи змінився вміст після копіювання або передавання. Хеш не приховує змісту й не замінює шифрування. Обчислення та перевірку виконує фахівець; адвокату важливо мати відомості про це у звіті. [18]

Копії та результати дослідження потрібно зберігати із шифруванням, персональним обліком доступу й визначеним порядком зберігання. Для повного образу накопичувача слід окремо обґрунтовувати необхідність його створення та правила доступу до нього. Договір про конфіденційність із виконавцем корисний, але сам собою не створює законної підстави для будь–якого розкриття адвокатської таємниці. [18]

До передавання погодьте місце зберігання, перелік осіб із доступом, строк, порядок повернення або видалення копій із дотриманням вимог збереження доказів. Не надсилайте повні архіви справ, образи чи дампи через відкриті посилання або звичайні групові чати. Для передавання використовуйте погоджений захищений канал із визначеним отримувачем. [18]

Практичне правило. Первинне прохання про допомогу не потребує надсилання всього архіву. Спочатку опишіть ситуацію. Потрібні матеріали передавайте після погодження завдання, способу захисту та обсягу доступу. Розширення кола отримувачів погоджується окремо.

За первинною консультацією, допомогою в залученні фахівця та формуванні завдання на дослідження адвокат може звернутися до Комітету НААУ з питань кібербезпеки та віртуальних активів. Після збереження необхідних матеріалів адвокату спільно з фахівцем слід визначити план безпечного відновлення роботи.

До Комітету рекомендується звертатися також при виборі шифрування, організації резервних копій, сумнівному запиті паролів, підготовці до ремонту, втраті носія, підозрі на втручання або потребі відновити дані. Адвокату не потрібно самостійно встановлювати технічну причину події перед зверненням.

У первинному повідомленні зазначте модель і систему пристрою, якщо вони відомі, його стан, час та обставини події, наявність резервної копії, уже наданий доступ і виконані дії. Якщо стан шифрування невідомий, так і напишіть. Паролі, ключі відновлення та самі клієнтські матеріали до повідомлення не додаються.

Зразок звернення. «Потрібна консультація щодо безпечного ремонту робочого ноутбука. Пристрій вмикається, на ньому є матеріали клієнтів. Сервіс просить пароль для діагностики. Резервна копія створена тиждень тому, стан шифрування не перевіряв. Пароль поки не передавав. Прошу допомогти визначити порядок підготовки пристрою та необхідність залучення фахівця».

Використовуйте перевірені офіційні контакти НААУ або звертайтеся через раду адвокатів регіону. Безпечний канал передавання даних і формат допомоги погоджуються під час звернення. За підозри на сторонній доступ технічна допомога організовується паралельно з правовим супроводом.

Радам адвокатів регіонів і профільним комітетам рекомендується визначити контактних осіб та підтримувати перелік фахівців із зазначенням їхніх компетенцій. Під час звернення окремо узгоджуються доступність фахівця, обсяг допомоги та строки реагування. Судова експертиза проводиться належно залученим експертом у відповідному процесуальному порядку.

ЧАСТИНА V
ПРАВОВА ОЦІНКА ВТРУЧАННЯ

5.1. Як встановити, чи було втручання санкціонованим

Технічні ознаки втручання (пункти 4.1–4.3) не відповідають на питання про його правову підставу. Для цього закон передбачає окремі механізми.

Повідомлення за статтею 253 КПК України. Особи, конституційні права яких були тимчасово обмежені під час проведення негласних слідчих (розшукових) дій, а також підозрюваний і його захисник мають бути письмово повідомлені прокурором або за його дорученням слідчим про таке обмеження. Повідомлення про факт і результати негласної слідчої (розшукової) дії повинно бути здійснене протягом дванадцяти місяців з дня припинення таких дій, але не пізніше звернення до суду з обвинувальним актом. Отримання такого повідомлення є найнадійнішим документальним підтвердженням того, що втручання мало процесуальний характер; його відсутність сама собою не доводить протилежного, оскільки строк повідомлення може ще не сплинути. [20]

Запит за Законом України «Про оперативно-розшукову діяльність». Частина дев'ята статті 9 цього Закону передбачає право осіб у встановленому законом порядку одержати від органів, на які покладено здійснення оперативно-розшукової діяльності, письмове пояснення з приводу обмеження їх прав і свобод та оскаржити ці дії. Водночас частина десята тієї ж статті забороняє оприлюднювати або надавати зібрані відомості, а також інформацію щодо проведення або непроведення стосовно певної особи оперативно-розшукової діяльності до прийняття рішення за її результатами, – тому негативна або ухильна відповідь не є доказом відсутності заходів. [22]

Перевірка ухвали, якщо її пред'явлено. Крім загальних вимог, для адвоката перевіряються: суб'єкт звернення з клопотанням (пункт 3 частини першої статті 23 Закону – Генеральний прокурор, його заступники, прокурор Автономної Республіки Крим, області, міста Києва та міста Севастополя); наявність в ухвалі ідентифікаційних ознак абонента, мережі та термінального обладнання (частина друга статті 263 КПК) або ідентифікаційних ознак електронної інформаційної системи (частина третя статті 264 КПК); для обшуку, огляду та тимчасового доступу – перелік речей і документів, що планується відшукати, виявити чи вилучити, та врахування пунктів 2–4 частини першої статті 23 Закону (частина друга статті 23). [3] [20]

Доступ до ухвали про дозвіл. У справі Yakymchuk v. Ukraine Суд зазначив, що суб'єктам спостереження має бути надано доступ до відповідних документів, «якщо відсутні вагомі підстави для відмови в цьому» (п. 74). У справі Denysyuk and Others v. Ukraine заявникам відмовили в наданні ухвал і документів з посиланням на їх таємний характер (пп. 20, 34), а резюме рішення, підготовлене Секретаріатом, серед підстав висновку за статтею 8 називає те, що заявникам було відмовлено в доступі до судових ухвал, а Суд не мав доступу до них. Тому клопотання про доступ до ухвали слід заявляти письмово, а відмову – фіксувати. [26] [23]

5.2. Склади кримінальних правопорушень

Якщо втручання не має законної підстави, воно може утворювати склади кримінальних правопорушень. Кваліфікація залежить від способу втручання, предмета посягання та статусу особи, яка його вчинила. Остаточну кваліфікацію визначає орган досудового розслідування; наведене нижче є орієнтиром для формулювання заяви.

Норма	Зміст складу та ключові кваліфікуючі ознаки
Ст. 163 КК	Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер. Частина друга – ті самі дії, вчинені повторно або щодо державних чи громадських діячів, журналіста, або вчинені службовою особою, або з використанням спеціальних засобів, призначених для негласного зняття інформації: позбавлення волі на строк від трьох до семи років. [21]
Ст. 182 КК	Порушення недоторканності приватного життя: незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями Кодексу. [21]
Ст. 359 КК	Незаконні придбання або збут спеціальних технічних засобів негласного отримання інформації, а також незаконне їх використання. Частина третя охоплює вчинення організованою групою або заподіяння істотної шкоди охоронюваним законом правам, свободам чи інтересам. [21]
Ст. 361 КК	Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно–комунікаційних систем, електронних комунікаційних мереж. Частина третя – якщо дії призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації. Частина п'ята – дії, передбачені частиною третьою або четвертою, вчинені під час дії воєнного стану: позбавлення волі на строк від десяти до п'ятнадцяти років. [21]
Ст. 362 КК	Несанкціоновані дії з інформацією, вчинені особою, яка має право доступу до неї. Частина друга – несанкціоновані перехоплення або копіювання такої інформації, якщо це призвело до її витоку. Ця норма охоплює сценарій, коли доступ було надано для технічного обслуговування чи дослідження, а використано ширше. [21]
Ст. 397 КК	Втручання в діяльність захисника чи представника особи: вчинення в будь–якій формі перешкод до здійснення правомірної діяльності захисника або «порушення встановлених законом гарантій їх діяльності та професійної таємниці». Частина друга – ті самі дії, вчинені службовою особою з використанням свого службового становища. [21]

5.3. Підслідність

Підслідність (стаття 216 КПК України). Досудове розслідування за статтею 359 КК здійснюють слідчі органів безпеки – ця стаття прямо названа у частині другій статті 216. Статті 163, 182, 361, 362 і 397 КК до спеціальної підслідності не віднесені, тому за загальним правилом частини першої статті 216 їх розслідують слідчі органів Національної поліції. Якщо ж кримінальне правопорушення вчинене працівником правоохоронного органу, суддею або іншою особою, переліченою у пункті 1 частини четвертої статті 216, розслідування здійснюють слідчі органів Державного бюро розслідувань.

Частина десята статті 216 дозволяє прокурору своєю постановою визначити підслідність усіх пов'язаних правопорушень, якщо їх неможливо виділити в окреме провадження. [20] [21]

Висновок для заяви. Спірна підслідність не є підставою відмовити у реєстрації: частина четверта статті 214 КПК прямо встановлює, що відмова у прийнятті та реєстрації заяви чи повідомлення про кримінальне правопорушення не допускається. Якщо відомості до реєстру вніс прокурор, частина сьома цієї статті зобов'язує його протягом п'яти робочих днів передати матеріали до відповідного органу досудового розслідування з дотриманням правил підслідності. [20]

ЧАСТИНА VI
ЮРИДИЧНА ФІКСАЦІЯ ТА ПРИПИНЕННЯ ВИТОКУ

6.1. Форми юридичної фіксації

Технічні матеріали (пункти 4.2–4.4) набувають правового значення лише у належній процесуальній чи документальній формі. Основні форми такі.

- Заява про кримінальне правопорушення. Стаття 214 КПК України зобов'язує слідчого, дізнавача, прокурора невідкладно, але не пізніше 24 годин після подання заяви внести відомості до Єдиного реєстру досудових розслідувань, розпочати розслідування та через 24 години з моменту внесення таких відомостей надати заявнику витяг з реєстру. Досудове розслідування розпочинається з моменту внесення відомостей до реєстру. Відмова у прийнятті та реєстрації заяви не допускається. [20]
- Внутрішній акт фіксації. Складається адвокатом (адвокатським бюро, об'єднанням) невідкладно та містить хронологію, перелік осіб, зміст їхніх повідомлень, пред'явлені документи, обсяг наданого доступу, перелік підключених носіїв і переданих даних (пункт 2.3, деталізований перелік – Додаток А, розділ 7). Акт не є процесуальним документом, але фіксує обставини на момент, коли вони ще відтворювані, і стає додатком до заяви.
- Технічний звіт і хеш-значення. Для кожної копії фіксуються джерело, дата, спосіб отримання, виконавець, інструменти та подальші передання, а цілісність контролюється криптографічними хеш-значеннями (пункт 4.4). Звичайний технічний звіт не набуває статусу висновку експерта лише через назву; для використання у кримінальному провадженні експерт має бути залучений у процесуальному порядку (пункт 4.3).
- Повідомлення ради адвокатів регіону та звернення до Комітету захисту прав адвокатів та гарантій адвокатської діяльності НААУ чи Комітету регіональної ради адвокатів (пункт 2.4). Окремо: частина друга статті 23 Закону вимагає завчасного повідомлення ради адвокатів регіону про обшук чи огляд житла, іншого володіння адвоката, приміщень, де він здійснює адвокатську діяльність, та тимчасовий доступ до речей і документів адвоката, а пункт 12 частини першої статті 23 зобов'язує орган або посадових осіб, які затримали адвоката або застосували до нього запобіжний захід, негайно повідомити про це відповідну раду адвокатів регіону. [3]
- Заперечення і зауваження до протоколу. Під час процесуальної дії представник ради адвокатів регіону має право ставити запитання, подавати свої зауваження та заперечення щодо порядку проведення процесуальних дій, що зазначаються у протоколі (частина друга статті 23 Закону). Незгода, не внесена до протоколу, згодом доводиться значно складніше. [3]
- Звернення до CERT-UA. Стаття 9 Закону України «Про основні засади забезпечення кібербезпеки України» визначає CERT-UA національною командою реагування на кіберінциденти, кібератаки, кіберзагрози, до завдань якої належать отримання та опрацювання обов'язкових та інших повідомлень про кіберінциденти, надання рекомендацій щодо заходів реагування і технічної підтримки, а також взаємодія із суб'єктами приватного сектору. Обов'язок невідкладного (протягом години) повідомлення за пунктом 17 Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 р. №1533, адресовано власникам або розпорядникам систем, в яких обробляються державні інформаційні ресурси, службова інформація чи державна таємниця, та операторам критичної інфраструктури, власникам або розпорядникам об'єктів критичної інформаційної інфраструктури; якщо адвокатське утворення до жодної з цих категорій не належить, звернення для нього є добровільним. Слід також ураховувати, що за пунктом 10 Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності, затвердженого постановою Кабінету Міністрів України від 13 листопада 2025 р. №1471, CERT-UA в установленому порядку надає правоохоронним органам і суб'єктам оперативно-розшукової діяльності доступ до технічних та інших деталей кіберінциденту. Тому обсяг відомостей у зверненні слід обмежувати технічними індикаторами: обов'язок за частиною третьою статті 22 Закону про адвокатуру зберігається і тут. [28] [29] [33] [2]

6.2. Правові засоби припинення витоку

Знищення матеріалів негласних дій. Частина перша статті 255 КПК України зобов'язує невідкладно знищити на підставі рішення прокурора відомості, речі та документи, отримані в результаті проведення негласних слідчих (розшукових) дій, які прокурор не визнає необхідними для подальшого досудового розслідування. Частина друга забороняє використання таких матеріалів для цілей, не пов'язаних з кримінальним провадженням, та ознайомлення з ними учасників провадження чи будь-яких інших осіб. Знищення здійснюється під контролем прокурора (частина четверта) і не звільняє його від обов'язку повідомлення за статтею 253 (частина п'ята). Частина третя зобов'язує прокурора повідомити власника речей або документів, отриманих у результаті негласних дій, про їх наявність і з'ясувати, чи бажає він їх повернути. У справі Denysyuk and Others v. Ukraine заявникам повідомляли лише про те, що матеріали знищено як такі, що не мали доказового значення, а їхні запити про документи відхиляли (пп. 8, 20, 32–34). Оскільки знищення за частиною першою статті 255 здійснюється на підставі рішення прокурора, доцільно клопотати про надання копії цього рішення. [20] [23]

Знищення відомостей про особисте життя, зібраних під час ОРД. Частина дванадцята статті 9 Закону України «Про оперативно-розшукову діяльність» встановлює, що одержані внаслідок оперативно-розшукової діяльності відомості, що стосуються особистого життя, честі, гідності людини, якщо вони не містять інформації про вчинення заборонених законом дій, зберіганню не підлягають і повинні бути знищені. Частина тринадцята забороняє передачу і розголошення таких відомостей та встановлює відповідальність за це. [22]

Блокування доказового ефекту. Стаття 87 КПК України визнає недопустимими докази, отримані внаслідок істотного порушення прав та свобод людини, а також будь-які інші докази, здобуті завдяки інформації, отриманій внаслідок такого порушення. Пункт 1 частини другої зобов'язує суд визнати істотним порушенням «здійснення процесуальних дій, які потребують попереднього дозволу суду, без такого дозволу або з порушенням його суттєвих умов». Пункт 3 частини третьої окремо стосується недопущення адвоката до обшуку житла чи іншого володіння особи, причому факт недопущення адвокат зобов'язаний довести в суді під час судового провадження. В умовах воєнного стану ця стаття застосовується з урахуванням особливостей статті 615 КПК. [20]

Оскарження бездіяльності. Пункт 1 частини першої статті 303 КПК України дозволяє заявнику оскаржити слідчому судді бездіяльність слідчого, дізнавача, прокурора, яка полягає у невнесенні відомостей про кримінальне правопорушення до Єдиного реєстру досудових розслідувань після отримання заяви, а також у нездійсненні інших процесуальних дій, які він зобов'язаний вчинити у визначений Кодексом строк. Пункт 5 тієї ж частини дозволяє оскаржити рішення про відмову у визнанні потерпілим, пункт 7 – відмову в задоволенні клопотання про проведення слідчих (розшукових) дій або негласних слідчих (розшукових) дій. Щодо скарг на самі негласні дії: у справі Vykhor v. Ukraine Суд, посилаючись на свої висновки в Denysyuk and Others v. Ukraine (пп. 131–132), зазначив, що засоби захисту за частиною другою статті 303 та частиною третьою статті 309 КПК були недостатньо чіткими в законодавстві та на практиці (Vykhor, п. 17); у Denysyuk Суд також указав, що жодна з цих процедур не може бути ініційована самостійно, оскільки суб'єкти спостереження мають чекати призначення підготовчого судового засідання (п. 126). Це має значення для оцінки вичерпання національних засобів перед зверненням до Суду. [20] [23] [31]

Поновлення прав і відшкодування шкоди. Частина восьма статті 9 Закону України «Про оперативно-розшукову діяльність» зобов'язує відповідні органи невідкладно поновити порушені права і відшкодувати заподіяні матеріальні та моральні збитки в повному обсязі у разі порушення прав і свобод під час здійснення оперативно-розшукової діяльності, а також якщо причетність особи до правопорушення не підтвердилась. Спеціальною нормою цивільного права є стаття 1176 Цивільного кодексу України: шкода від іншої незаконної дії, бездіяльності чи незаконного рішення органу, що здійснює оперативно-розшукову діяльність, органу досудового розслідування, прокуратури або суду відшкодовується на загальних підставах (частина шоста), до яких належить стаття 1174 ЦК, а порядок відшкодування встановлюється законом (частина сьома). Закон України №266/94-ВР у пункті 3 частини першої статті 1 прямо відносить до підстав відшкодування незаконне проведення оперативно-розшукових заходів, а в пункті 1 – незаконне проведення в ході кримінального провадження обшуку, виїмки та інших процесуальних дій, що обмежують права громадян; шкода в цих випадках відшкодовується в повному обсязі незалежно від вини посадових осіб. [22] [30] [32]

ЧАСТИНА VII
ПРАКТИКА ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ

Denysyuk and Others v. Ukraine, заяви №22790/19, 23896/20, 25803/20, 31352/20, рішення від 13 лютого 2025 року, остаточне з 13 травня 2025 року. Суд констатував порушення статті 8 Конвенції (повага до кореспонденції та приватного життя) і статті 38. Предметом були негласний аудіо– та відеоконтроль і прослуховування телефонних розмов заявників у кримінальних провадженнях щодо них; четвертий заявник – захисник. У резюме рішення, підготовленому Секретаріатом (воно не є обов'язковим для Суду), зазначено, що спілкування заявників з їхніми захисниками «було недостатньо захищене спеціальними та детальними нормами та процедурами» щодо виявлення та обробки таких розмов у разі випадкового прослуховування, а захисник має статус постраждалого незалежно від того, чи були фактично прослухані його розмови з клієнтами. [23]

У пункті 146 цього рішення Суд нагадав, що будь–яке спілкування захисників з їхніми клієнтами має право на посилений захист за Конвенцією, і для цілей статті 8 не є вирішальним, чи було на момент конкретної розмови укладено офіційний договір про надання правової допомоги. У пункті 54 Суд констатував, що Інструкція про організацію проведення негласних слідчих (розшукових) дій не містить положень, які детально описують процедури виявлення та обробки випадково отриманого таємного спілкування, зокрема спілкування захисників з клієнтами. [23]

Vykhor v. Ukraine, заява №36618/14, рішення від 22 січня 2026 року – порушення статті 8 та пункту 1 статті 6 Конвенції (тривалість провадження). Заявник – адвокат, щодо якого за ухвалами слідчого судді проводилися зняття інформації з транспортних телекомунікаційних мереж щодо двох його мобільних номерів та аудіо–, відеоконтроль. Суд указав, що в ухвалах відсутні вказівки на застосування критерію «необхідності в демократичному суспільстві» чи оцінку пропорційності, «враховуючи те, що заявник був практикуючим адвокатом» (п. 22), і дійшов висновку, що втручання не здійснювалося «згідно із законом» (п. 25). [31]

Yakymchuk v. Ukraine, заява №26519/16, рішення від 11 вересня 2025 року, остаточне з 11 грудня 2025 року.

Порушення статті 8 встановлено двічі: щодо негласної відеозйомки, виконаної працівниками СБУ щодо колишньої судді в її кабінеті, – через відсутність достатніх гарантій щодо законності цього заходу, і щодо негласного аудіозапису її розмови, здійсненого іншою особою на наданий працівником СБУ диктофон без попереднього дозволу суду (пп. 82–85).

Окремо встановлено порушення пункту 1 статті 6 (суд, встановлений законом; розумний строк) і статті 13 у поєднанні зі статтею 6 щодо тривалості провадження; ці порушення з негласними заходами не пов'язані. Для адвоката ключове положення – пункт 74 про доступ суб'єкта спостереження до відповідних документів (див. пункт 5.1). [26]

Vasil Vasilev v. Bulgaria, заява №7610/15, рішення від 16 листопада 2021 року, остаточне з 16 лютого 2022 року, – порушення статті 8, а також пункту 1 статті 6 Конвенції в частині публічності розгляду і проголошення рішення у цивільному провадженні. За резюме рішення (англійською мовою), предметом розгляду за статтею 8 були незаконний запис і подальше розшифрування розмови між адвокатом і його клієнтом унаслідок негласного контролю телефонної лінії клієнта, а також відсутність достатньої ясності правового регулювання та процесуальних гарантій, пов'язаних саме зі знищенням випадково перехоплених комунікацій адвоката з клієнтом. [24]

Dudchenko v. Russia, заява №37717/05, рішення від 7 листопада 2017 року, – порушення статті 8 Конвенції (повага до кореспонденції та приватного життя) поряд з іншими порушеннями. У справі поліція перехопила розмови заявника з його адвокатом (п. 101); на пункт 103 цього рішення Суд послався в Denysyuk and Others v. Ukraine як на джерело принципу посиленого захисту спілкування захисника з клієнтом. [27]

Michaud v. France, заява №12323/11, рішення від 6 грудня 2012 року, – порушення статті 8 не встановлено. Справа стосувалася обов'язку адвокатів повідомляти про підозри щодо відмивання коштів, а не негласного контролю, і наводиться як застереження: у резюме рішення, підготовленому Секретаріатом, зазначено, що «Професійна таємниця адвокатів не є недоторканною» і підлягає зважуванню з іншими суспільними інтересами. Національне регулювання в частині п'ятій статті 258 КПК сформульоване як заборона без механізму надання дозволу. [25]

Як це використовувати. Наведені рішення застосовуються не як абстрактний орієнтир, а через частину третю статті 23 Закону України «Про адвокатуру та адвокатську діяльність», яка зобов'язує органи влади дотримуватися Конвенції та практики ЄСПЛ у відносинах з адвокатами, і через статтю 87 КПК під час вирішення питання про допустимість доказів. Рішення Vykhor v. Ukraine доречно наводити у клопотаннях і скаргах щодо ухвал про негласні дії стосовно адвоката: Суд поставив ухвалам слідчого судді в провину відсутність вказівок на оцінку пропорційності, «враховуючи те, що заявник був практикуючим адвокатом» (п. 22). [3] [20] [31]

ЧАСТИНА VIII
АЛГОРИТМ ДІЙ АДВОКАТА

8.1. Послідовність дій

Технічні кроки виконуються за Частинами III і IV паралельно; нижче наведено юридичну послідовність. Строки вказано там, де вони встановлені законом.

Етап	Зміст дій і правова підстава
Етап 1. Перші години	Припинити роботу з клієнтськими матеріалами на пристрої та зв'язатися з фахівцем через інший канал (пункт 4.1). Скласти хронологію (пункт 2.3). Повідомити раду адвокатів регіону та залучити іншого адвоката для правничої допомоги (пункти 2.1, 2.4). Не видаляти дані, не перевстановлювати систему, не очищати журнали.
Етап 2. Перша доба	Подати заяву про кримінальне правопорушення з попередньою кваліфікацією за пунктом 5.2 та додатками (акт фіксації, технічні дані). Вимагати реєстрації: відмова у прийнятті та реєстрації не допускається. Через 24 години з моменту внесення відомостей отримати витяг з ЄРДР (стаття 214 КПК). [20]
Етап 3. Перший тиждень	Права потерпілого виникають з моменту подання заяви про вчинення щодо особи кримінального правопорушення (частина друга статті 55 КПК), тому в заяві слід прямо зазначити шкоду, завдану адвокату; постанова про відмову у визнанні потерпілим може бути оскаржена слідчому судді (частина п'ята статті 55, пункт 5 частини першої статті 303). Заявити слідчому клопотання про проведення експертизи вилучених образів і журналів та про отримання від оператора електронних комунікацій відомостей про з'єднання і переадресацію: такі відомості є охоронюваною законом таємницею (пункт 7 частини першої статті 162 КПК), доступ до них здійснюється на підставі ухвали слідчого судді (частина друга статті 159). Відмову в задоволенні клопотання про проведення слідчих (розшукових) дій оскаржують за пунктом 7 частини першої статті 303 КПК. [20]
Етап 4. Перевірка законності втручання	Направити запит про письмове пояснення з приводу обмеження прав і свобод (частина дев'ята статті 9 Закону про ОРД). Перевірити, чи надходило повідомлення за статтею 253 КПК. Письмово клопотати про доступ до ухвали (Yakymchuk v. Ukraine, п. 74). За наявності ухвали – перевірити суб'єкта клопотання, конкретизацію предмета та оцінку пропорційності щодо адвоката (Vykhor v. Ukraine, п. 22); в умовах воєнного стану – з'ясувати, чи не діяв керівник органу прокуратури за пунктом 2 частини першої статті 615 КПК (пункти 1.6, 5.1). [20] [22] [3] [26] [31]
Етап 5. Припинення обігу матеріалів	Клопотання прокурору про знищення матеріалів, що не використовуються у провадженні, про заборону ознайомлення з ними та про надання копії рішення про знищення (стаття 255 КПК); вимога про знищення відомостей про особисте життя (частина дванадцята статті 9 Закону про ОРД). Пункт 6.2. [20] [22]
Етап 6. Захист у справах клієнтів	У провадженнях, де могли бути використані відомості з витоку, заявити про недопустимість доказів за статтею 87 КПК, у тому числі похідних доказів. [20]
Етап 7. Оскарження і відшкодування	Скарга слідчому судді на бездіяльність (пункт 1 частини першої статті 303 КПК). Вимога поновлення прав і відшкодування шкоди (частина восьма статті 9 Закону про ОРД; стаття 1176 ЦК України; Закон №266/94-ВР). Звернення до ЄСПЛ за статтею 8 Конвенції – з урахуванням висновків Суду щодо ефективності національних засобів захисту (пункт 6.2, Частина VII). [20] [22] [30] [32]
Етап 8. Робота з клієнтами та відновлення	Визначити коло клієнтів, чиї матеріали могли бути охоплені, з урахуванням установлених обставин і застосовних обов'язків щодо повідомлення (пункт 2.3). Виконати обов'язок забезпечити умови, що унеможливлюють доступ сторонніх осіб до адвокатської таємниці (частина третя статті 22 Закону), – переглянути облікові записи, ключі, резервні копії (пункти 3.1–3.3, 3.5). [2]

8.2. Дії, яких адвокату слід уникати

Самостійне застосування засобів негласного отримання інформації. Стаття 359 КК України встановлює відповідальність за незаконні придбання, збут або використання спеціальних технічних засобів негласного отримання інформації; мотив до ознак складу не належить. Тому спроба самостійно «перевірити» підозри щодо інших осіб із застосуванням таких засобів створює ризик кримінальної відповідальності. [21]

Самостійне дослідження чужих систем. Перевірка чужих пристроїв, мереж або облікових записів, навіть з метою встановлення джерела втручання, може підпадати під статтю 361 КК України. [21]

Видалення даних та «лікування» пристрою до первинної оцінки. Крім технічної шкоди (пункт 4.1), такі дії ускладнюють доказування у вже розпочатому провадженні та можуть тлумачитися проти адвоката.

Надмірне розкриття у власних зверненнях. Заява про кримінальне правопорушення, звернення до CERT-UA, скарга або позов не повинні містити відомостей про клієнтів понад мінімально необхідний обсяг: обов'язок зберігати адвокатську таємницю та забезпечувати умови, що унеможливлюють доступ сторонніх осіб до неї, зберігається і в цих процедурах (частини перша і третя статті 22 Закону). [2]

Ототожнення перевірки з виною клієнта. Пункт 16 частини першої статті 23 Закону забороняє ототожнення адвоката з клієнтом; це самостійний аргумент у разі, коли заходи стосовно адвоката обґрунтовуються обставинами справ його клієнтів. [3]

Оперативний перелік того, чого не варто робити під час самої перевірки, наведено у Додатку А (розділ 10).

Правило для юридичної частини: спершу зафіксувати й зареєструвати, потім перевіряти законність підстави, і лише після цього вимагати припинення обігу матеріалів та оскаржувати. Порушення цієї послідовності зазвичай призводить до втрати і слідів, і строків.

Основне правило для адвоката: перед наданням доступу встановити його підставу й межі; при підозрі на втручання зберегти цифрові сліди; правову та технічну допомогу організовувати паралельно.

ДОДАТОК А
КАРТКА ШВИДКОГО РЕАГУВАННЯ

Додаток А відтворює коротку практичну методичку і призначений для окремого друку та щоденного користування. Він навмисно повторює у стислому вигляді частину основного тексту і не замінює його: правові підстави кожного розділу наведено у Додатку Б.

1. Головне правило

Комп'ютер, телефон, флеш-накопичувач, хмарне сховище чи електронна пошта адвоката можуть містити інформацію, яка становить адвокатську таємницю.

Сам факт надання доступу до технічного пристрою не означає автоматичної згоди на ознайомлення з усіма матеріалами клієнтів.

Перед будь-яким доступом потрібно визначити:

- хто отримує доступ;
- на якій правовій підставі;
- з якою метою;
- до яких саме даних;
- на який період;
- чи допускається копіювання інформації.

2. Якщо до вас звернулися з вимогою перевірити комп'ютер

НЕОБХІДНО:

- **Встановити особу представників органу.** Перевірте їхні документи, посади та повноваження.
- **З'ясувати правову підставу.** Поставте пряме питання: «На якій правовій підставі планується доступ до мого пристрою та інформації на ньому?» Фраза «технічна перевірка» сама по собі не визначає меж доступу.
- **Визначити мету перевірки.** Попросіть повідомити, що саме перевіряється:
  - можливе зараження;
  - конкретний файл чи програма;
  - підозріле підключення;
  - конкретний період активності;
  - можливий несанкціонований доступ.
- **Повідомити про адвокатську таємницю.** На пристрої можуть міститися матеріали різних клієнтів, адвокатське листування, проєкти процесуальних документів та інша захищена інформація.

3. Рекомендована позиція адвоката

Можна використовувати таке формулювання:

«На цьому пристрої зберігається інформація, що становить адвокатську таємницю. Прошу повідомити правову підставу, мету та конкретний обсяг запланованих дій. Я готовий сприяти перевірці можливого кіберінциденту з дотриманням гарантій адвокатської діяльності. Прошу забезпечити належну фіксацію всіх дій та, за можливості, залучити незалежного технічного фахівця».

4. Добровільна технічна перевірка

Якщо адвокат погоджується на добровільне дослідження пристрою, не варто надавати необмежений доступ.

До початку перевірки бажано письмово визначити:

- що саме перевіряється;
- які дії дозволені;
- які дані можуть бути скопійовані;
- чи може створюватися повний образ накопичувача;
- де зберігатимуться отримані дані;
- хто матиме до них доступ;
- чи допускається підключення зовнішніх носіїв;
- чи допускається доступ до пошти або хмарних сховищ.

Важливо: загальна згода на «перевірку комп'ютера» не повинна автоматично означати згоду на:

- копіювання всього накопичувача;
- відкриття всіх документів;
- передачу паролів;
- доступ до електронної пошти;
- доступ до хмарних сховищ;
- отримання матеріалів усіх клієнтів.

5. Якщо йдеться про процесуальну дію

Необхідно встановити, що саме проводиться:

- обшук;
- тимчасовий доступ;
- огляд;
- вилучення;
- експертне дослідження;
- інша процесуальна дія.

Для кожної процедури існують свої правові підстави та межі.

Особливо важливо для адвоката. Стаття 23 Закону України «Про адвокатуру та адвокатську діяльність» встановлює спеціальні гарантії адвокатської діяльності. Також КПК України містить спеціальні положення щодо доступу до інформації, пов'язаної з наданням правової допомоги. Тому наявність судової ухвали не означає автоматичного права отримати весь адвокатський архів.

6. Під час обшуку

Адвокату варто:

- Перевірити ухвалу суду та її зміст.
- Отримати копію ухвали.
- Забезпечити участь представника ради адвокатів регіону.
- Забезпечити участь адвоката.
- Вимагати належної фіксації процесуальної дії.
- Заявляти заперечення.
- Вимагати внесення зауважень до протоколу.
- Звертати увагу на матеріали, які містять адвокатську таємницю та не підлягають огляду та вилученню.

Не чиніть фізичного опору законним діям. Заперечення щодо законності дій фіксуються процесуальними засобами та оскаржуються у встановленому законом порядку.

7. Якщо пристрій уже перевіряли або копіювали інформацію

Необхідно якомога швидше зафіксувати:

- хто отримував доступ;
- дату та час;
- які документи пред'являлися;
- до якого пристрою отримано доступ;
- які програми запускалися;
- які носії підключалися;
- які файли або каталоги відкривалися;
- що саме копіювалося;
- чи створювався образ накопичувача;
- куди передано отриману інформацію;
- хто отримав доступ до копій.

Після цього доцільно провести незалежне технічне дослідження.

8. Якщо є ознаки кіберінциденту

Необхідно:

- **Не знищувати інформацію.** Не видаляйте файли та не очищуйте пристрій.
- **Не змінювати без потреби налаштування системи.** Це може знищити важливі цифрові сліди.
- **Зафіксувати обставини.** Збережіть повідомлення, журнали, скриншоти, сповіщення та інші доступні дані.
- **Залучити технічного фахівця.** Бажано – незалежного спеціаліста з цифрової криміналістики.
- **Забезпечити юридичний супровід.** Особливо якщо до ситуації залучені правоохоронні органи.

9. Куди звертатися адвокату

У разі виникнення проблеми доцільно оперативно повідомити:

- **раду адвокатів відповідного регіону**;
- **Комітет захисту прав адвокатів та гарантій адвокатської діяльності НААУ**;
- **профільний комітет НААУ з питань кібербезпеки та віртуальних активів**;
- іншого адвоката для забезпечення правничої допомоги;
- незалежного технічного спеціаліста – за необхідності.

10. Чого адвокату НЕ варто робити

- передавати весь клієнтський архів лише через вимогу «перевірити комп'ютер»;
- без необхідності передавати паролі та ключі доступу;
- погоджуватися на невизначений обсяг технічного дослідження;
- дозволяти необмежене копіювання інформації;
- самостійно видаляти потенційні докази;
- дистанційно очищати пристрій після інциденту;
- фізично перешкоджати законним процесуальним діям.

11. Чек-лист адвоката

Перед доступом до пристрою:

- Хто отримує доступ?
- Які повноваження?
- Яка правова підстава?
- Яка мета?
- Який обсяг доступу?
- Які дані можуть бути скопійовані?
- Чи містить пристрій адвокатську таємницю?
- Чи потрібен представник ради адвокатів?
- Чи потрібен незалежний технічний фахівець?

Після доступу:

- Зафіксувати всі обставини.
- Отримати копії процесуальних документів.
- Встановити обсяг скопійованої інформації.
- З'ясувати місце зберігання копій.
- Провести незалежний технічний аналіз.
- За необхідності – оскаржити дії.
- Оцінити необхідність повідомлення клієнтів.

Головний принцип

Захист адвокатської таємниці в цифровому середовищі – це не відмова від законної перевірки чи співпраці з державними чи правоохоронними органами. Це чітке визначення правової підстави, мети та меж доступу до інформації клієнтів і належна фіксація кожної дії з цифровими даними. При перевірці техніки адвоката предметом має бути конкретний кіберінцидент, а не автоматичний доступ до всього цифрового архіву адвокатської діяльності.

ДОДАТОК Б
ПРАВОВІ ПРИВ'ЯЗКИ РОЗДІЛІВ ДОДАТКА А

Таблиця показує, на яку норму спирається кожен розділ картки швидкого реагування і де ця норма розкрита в основному тексті. Усі норми наведено за чинними редакціями.

Розділ Додатка А	Норма та місце в основному тексті
1. Головне правило	Частина перша статті 22 Закону – адвокатською таємницею є, серед іншого, інформація, що зберігається на електронних носіях; частина третя – обов'язок забезпечити умови, що унеможливлюють доступ сторонніх осіб. Пункт 1.1. [2]
2. Правова підстава доступу	Частини перша і друга статті 264 КПК – негласний доступ до електронної інформаційної системи лише за ухвалою слідчого судді, крім систем, доступ до яких не обмежений або не пов'язаний з подоланням логічного захисту; частина шоста статті 236 КПК – повноваження долати логічний захист під час обшуку. Пункт 3 частини першої статті 23 Закону – суб'єкт клопотання. Пункти 1.2, 1.4, 5.1. [20] [3]
3. Позиція адвоката	Пункти 1 і 9 частини першої статті 23 Закону – заборона будь–яких втручань і перешкод та заборона втручання у приватне спілкування адвоката з клієнтом; частина п'ята статті 258 КПК – для спілкування захисника з підзахисним. Пункти 1.2, 2.2. [3] [20]
4. Добровільна перевірка	Частина друга статті 22 Закону – статус адвокатської таємниці втрачається за письмовою заявою клієнта, а не за згодою адвоката; частина друга статті 264 КПК – добровільне розблокування знімає ознаку подолання логічного захисту. Пункти 1.4, 1.5. [2] [20]
5. Процесуальна дія	Стаття 161 КПК – листування захисника з клієнтом як речі, до яких заборонено доступ; частина друга статті 23 Закону – ухвала має містити перелік речей і документів; стаття 168 КПК – межі вилучення техніки і право на копії інформації. Пункти 1.2, 1.4, 1.6. [20] [3]
6. Під час обшуку	Частина друга статті 23 Закону – присутність представника ради адвокатів регіону, завчасне повідомлення ради, право подавати зауваження і заперечення до протоколу; неявка за умови завчасного повідомлення не перешкоджає дії. Стаття 236 КПК – допуск адвоката на будь–якому етапі, обов'язковий аудіо– та відеозапис. Пункт 3 частини третьої статті 87 КПК – недопустимість доказів у разі недопущення адвоката до обшуку, причому факт недопущення адвокат зобов'язаний довести в суді. В умовах воєнного стану – пункт 2 частини першої статті 615 КПК. Пункти 1.6, 6.2. [3] [20]
7. Якщо доступ уже відбувся	Стаття 214 КПК – заява про кримінальне правопорушення, внесення відомостей до ЄРДР не пізніше 24 годин і витяг заявнику. Стаття 253 КПК – повідомлення про обмеження прав під час негласних дій. Пункти 2.3, 5.1, 6.1. [20]
8. Ознаки кіберінциденту	Статті 361 і 362 КК – несанкціоноване втручання в роботу систем і мереж та несанкціоновані перехоплення чи копіювання особою, яка має право доступу, якщо це призвело до витоку. Стаття 9 Закону про кібербезпеку – CERT–UA. Пункти 5.2, 6.1. [21] [28]
9. Куди звертатися	Пункт 12 частини першої та частина друга статті 23 Закону – повідомлення ради адвокатів регіону. Пункти 2.4, 6.1. [3]
10. Чого не варто робити	Стаття 359 КК – незаконне використання спеціальних технічних засобів негласного отримання інформації; стаття 361 КК – дослідження чужих систем; частини перша і третя статті 22 Закону – межі розкриття у власних зверненнях. Пункт 8.2. [21] [2]
11. Чек–лист	Зведення Частин I, II, V і VI; послідовність дій після доступу – етапи 1–8 пункту 8.1.

ДЖЕРЕЛА ТА НОРМАТИВНІ ПОСИЛАННЯ

Нумерація відповідає посиланням у тексті. Джерела [1]–[18] обслуговують організаційні та технічні положення (Частини I–IV), джерела [19]–[33] – правову частину (Частини I, V–VIII і Додаток Б). Під час застосування рекомендацій слід враховувати чинні редакції нормативних актів і документацію для відповідної версії пристрою або програмного забезпечення. Джерела [34]–[49] доповнюють технічні положення Частин III і IV.

Настанови іноземних організацій не встановлюють обов'язкових вимог для адвокатів України. Назви пунктів меню, доступність функцій і порядок обслуговування залежать від моделі та версії системи. Приклади, форми звернень і рекомендована періодичність перевірок у Частинах III і IV адаптовані до адвокатської практики та не є цитатами з документів виробників. Дата опрацювання технічної документації: 21 вересня 2026 року.

[1] Правила адвокатської етики

[2] Закон України «Про адвокатуру та адвокатську діяльність», стаття 22 «Адвокатська таємниця». Текст статті 22

[3] Закон України «Про адвокатуру та адвокатську діяльність», стаття 23 «Гарантії адвокатської діяльності». Текст статті 23

[4] Кримінальний процесуальний кодекс України: статті 101, 159, 161, 168, 233, 236, 615. Стаття 101 · Стаття 159 · Стаття 161 · Стаття 233 · Стаття 236

[5] SWGDE. Best Practices for Computer Forensic Examinations, документ 18-F-001. Версія 2.0 від 28.07.2025 (затверджена). Документ SWGDE

[6] NIST SP 800-61 Rev. 3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management. Документ NIST

[7] Microsoft Learn. Документація BitLocker. Довідка для користувачів: BitLocker overview · Документація Microsoft

[8] Ubuntu Security Documentation. Full disk encryption. Документація Ubuntu

[9] Apple Platform Security. Volume encryption with FileVault. Документація Apple

[10] VeraCrypt. Unencrypted Data in RAM. Документація VeraCrypt

[11] Android Open Source Project. File-based encryption. Документація Android

[12] Apple Platform Security. Passcodes and passwords. Документація Apple

[13] Apple Support. «Режим карантину» / Lockdown Mode. Документація Apple

[14] National Cyber Security Centre. Top tips for staying secure online. Рекомендації NCSC

[15] CERT-UA. Попередження щодо спроб підключення через AnyDesk нібито від імені CERT-UA, січень 2025 року. – Повідомлення CERTUA

[16] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Документ NIST

[17] SWGDE. Best Practices for Computer Forensic Acquisitions, документ 17-F-002. Версія 2.0 від 15.06.2023 (затверджена). Документ SWGDE

[18] NISTIR 8387. Digital Evidence Preservation: Considerations for Evidence Handlers. Документ NIST

[19] Конституція України, стаття 31 (таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції). Чинна. Текст Конституції

[20] Кримінальний процесуальний кодекс України (чинний): статті 14, 55, 87, 159, 161, 162, 168, 214, 216, 236, 253, 255, 258, 263, 264, 303, 615. Текст Кодексу

[21] Кримінальний кодекс України (чинний): статті 163, 182, 359, 361, 362, 397. Текст Кодексу

[22] Закон України «Про оперативно-розшукову діяльність» №2135-XII (чинний), стаття 9 «Гарантії законності під час здійснення оперативно-розшукової діяльності». Текст Закону

[23] ЄСПЛ, Denysyuk and Others v. Ukraine, заяви №22790/19, 23896/20, 25803/20, 31352/20, рішення від 13.02.2025, остаточне 13.05.2025 (порушення статей 8 і 38 Конвенції). Переклад українською Офісу Уповноваженого; текст англійською – HUDOC 001-241747. HUDOC

[24] ЄСПЛ, Vasil Vasilev v. Bulgaria, заява №7610/15, рішення від 16.11.2021, остаточне 16.02.2022 (порушення статті 8 і пункту 1 статті 6 Конвенції). Текст англійською. HUDOC

[25] ЄСПЛ, Michaud v. France, заява №12323/11, рішення від 06.12.2012 (порушення статті 8 Конвенції не встановлено). Резюме рішення українською (Інформаційне повідомлення №158). HUDOC

[26] ЄСПЛ, Yakymchuk v. Ukraine, заява №26519/16, рішення від 11.09.2025, остаточне 11.12.2025 (порушення статті 8, пункту 1 статті 6 і статті 13 у поєднанні зі статтею 6 Конвенції). Переклад українською Мін'юсту. HUDOC

[27] ЄСПЛ, Dudchenko v. Russia, заява №37717/05, рішення від 07.11.2017 (порушення статті 8 Конвенції поряд з іншими). HUDOC

[28] Закон України «Про основні засади забезпечення кібербезпеки України» №2163–VIII (чинний), стаття 9 «Національна система реагування на кіберінциденти, кібератаки, кіберзагрози». Текст Закону

[29] Постанова Кабінету Міністрів України від 26.11.2025 №1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози»; Національний план реагування на кіберінциденти, кібератаки та кіберзагрози, пункт 17. Текст Постанови

[30] Цивільний кодекс України (чинний), статті 1174 і 1176 (відшкодування шкоди, завданої органами державної влади та органами, що здійснюють оперативно-розшукову діяльність, досудове розслідування). Текст Кодексу

[31] ЄСПЛ, Vykhor v. Ukraine, заява №36618/14, рішення від 22.01.2026 (порушення статті 8 і пункту 1 статті 6 Конвенції). Переклад українською Мін'юсту. HUDOC

[32] Закон України «Про порядок відшкодування шкоди, завданої громадянинові незаконними діями органів, що здійснюють оперативно-розшукову діяльність, органів досудового розслідування, прокуратури і суду» №266/94-ВР (чинний), стаття 1. Текст Закону

[33] Постанова Кабінету Міністрів України від 13.11.2025 №1471 «Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності»; Порядок, пункт 10. Текст Постанови

[34] NCSC. Small organisations guide: Protecting your devices. Рекомендації NCSC

[35] NCSC. Managing your passwords. Рекомендації NCSC

[36] NCSC. 10 Steps to Cyber Security: Data security. Рекомендації NCSC

[37] NIST SP 800-53 Rev. 5. Зокрема MP-4, MP-5, MA-2, CP-9: захист носіїв, обслуговування та резервні копії. Документ NIST

[38] NCSC. Small organisations guide: Backing up your data. Рекомендації NCSC

[39] Apple Support. About encrypted backups on your iPhone, iPad, or iPod touch. Документація Apple

[40] Apple Support. Prepare your iPhone or iPad for a service appointment. Документація Apple

[41] Apple Support. Get your Mac ready for service. Документація Apple

[42] Google Pixel Help. Use Repair Mode for repair services. Документація Google

[43] Apple Support. How to use Ready for Repair or Trade In. Документація Apple

[44] NIST SP 800-88 Rev. 2 (2025). Guidelines for Media Sanitization. Документ NIST

[45] VeraCrypt. Beginner's Tutorial: створення та використання зашифрованого контейнера. Документація VeraCrypt

[46] NCSC. Setting up 2-Step Verification (2SV). Рекомендації NCSC

[47] NCSC. Small organisations guide: Spotting cyber attacks. Рекомендації NCSC

[48] NCSC. Offline backups in an online world. Рекомендації NCSC

[49] Apple. Install or remove configuration profiles on iPhone. Документація Apple