2.5. Інноваційні техніко-криміналістичні засоби пошуку, виявлення та фіксації інформації на електронних носіях

При роботі з електронним носіями інформації під час огляду або обшуку можуть виникати одне або декілька наступних тактичних завдань: 1) пошук відомостей; 2) відновлення видалених відомостей; 3) фіксація виявлених відомостей. На реалізацію вказаних тактичних завдань можуть бути спрямовані системи тактичних прийомів, в тому числі пов'язаних із техніко-криміналістичним дослідженням електронних носіїв інформації.

Електронний носій інформації є технічним пристроєм, на якому із використанням певної технології зафіксовані значущі для органу кримінальної юстиції відомості, що можуть бути зчитані електронним засобом, перетворені у придатний для сприйняття людиною вигляд та використані у кримінальному судочинстві. В криміналістичній літературі запропоновані різні підходи до

[1] Див.: Про затвердження плану заходів на 2015 рік із запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : постанова КМУ й НБУ від 11 березня 2015 р. № 99. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua.

класифікації електронних носіїв інформації, однак з практичної точки зору є важливим те, наскільки простим та неускладненим є доступ до інформації, наявної на носії. В залежності від наявності керуючого пристрою, що опосередковує доступ до відомостей, що зберігаються, електронні носії інформації можна розділити на:

– прості електронні носії інформації – дискети, компакт-диски, пластикові картки із магнітною смужкою. Такі пристрої допускають безпосередній доступ до відомостей, що зберігаються;

– електронні носії інформації, що працюють під керуванням одного або декількох комп'ютерів – ноутбуки, планшети, мобільні телефони[1], USB-флеш накопичувачі, флеш-картки, смарт-картки тощо;

Потреба у електричному контакті для доступу до електронного носія інформації дозволяє розділити їх на дві групи:

– електронні носії інформації до яких доступ можна отримати лише при контактному підключенні – флеш-картки, контактні смарт-карти, USB-флеш накопичувачі та інші USB-пристрої;

– електронні носії, що допускають опосередкований та віддалений доступ – різноманітні безконтактні пристрої (Bluetooth чи Wi-Fi засоби, приймачі сигналів GPS, RFID смарт-картки оплати проїзду в метро), мобільні телефони, а також комп'ютери, підключені до мереж загального користування.

За своїм призначенням електронні носії можуть використовуватись для збереження:

– будь-якої інформації (USB-флеш накопичувачі, флеш-картки, оптичні диски, жорсткі диски ноутбуків тощо);

– спеціалізованої інформації, притаманної певному виду носія (наприклад, данні в іммобілайзері транспортного засобу, відомості в комп'ютері банкомату, ідентифікаційний ключ, що містить смарт-карта, зокрема, SIM-карта).

[1] Примітка : Тут і далі терміни «мобільний телефон», «термінал» використовується для іменування технічних пристроїв, що задовольняють вимогам, встановленим Законом України «Про телекомунікації» щодо кінцевого обладнання абонентів.

З урахуванням того, що електронні носії інформації можуть забезпечувати обмеження доступу (із використанням апаратних або логічних систем) до наявних в них відомостей, їх на цій підставі можна розділити на такі, що:

– не обладнані або мають відімкнену систему обмеження доступу;

– передбачають обмеження доступу на основі паролю, апаратного чи програмного електронного ключа, певної поведінки користувача тощо;

– передбачають розгалуження прав доступу користувачів (гостьові, користувачеві та адміністративні права доступу).

При роботі й дослідженні електронних носів інформації слідчий має виключити вплив наступних факторів – дія високої/низької температури; раптові перепади температури; потрапляння вологи; падіння; дія статичної електрики. Для роботи із електронними носіями інформації мають допускатись лише кваліфіковані спеціалісти, навички яких слідчий має попередньо перевірити.

Отже, для правильного використання електронних носів інформації у кримінальному судочинстві суддя, прокурор, слідчий має добре представляти, які відомості про вчинений злочин можуть міститися у електронному носії інформації, та вилучення яких відомостей можна вимагати від спеціаліста або експерта.

Розглянемо криміналістичний потенціал найбільш розповсюджених електронних носіїв інформації – мобільного телефону та комп'ютеру.

1. Попереднє техніко-криміналістичне дослідження мобільних телефонів.

Криміналістичний потенціал мобільних телефонів визначається їх функціональністю, що випливає з підтримки ними можливості встановлення програмного забезпечення. З урахуванням цього мобільні телефони можна умовно розділити на дві групи – звичайні мобільні телефони та смартфони. Перші або не мають можливості для встановлення додаткового програмного забезпечення або програми, які все ж таки можна встановити, лише не-

значно розширюють можливості пристрою. Смартфони, навпаки, зорієнтовані на значне розширення власного функціоналу із використанням сторонніх програмних продуктів.

З мобільного телефону може бути вилучено:

– ідентифікаційні данні про мобільний телефон – модель, IMEI (International Mobile Equipment Identity / Міжнародний ідентифікатор мобільного обладнання);

– телефонну книгу;

– SMS-повідомлення;

– календар;

– нотатки;

– фотозображення;

– відео- та звукозаписи;

– збережену інформацію у браузерах.

На додаток до цього в смартфонах можна виявити:

– архіви програм обміну повідомленнями (ICQ, eBuddy Messenger, WhatsApp тощо);

– програми-клієнти для численних соціальних мереж (ВКонтакте, Facebook, Twitter тощо) до речі ці соціальні медіа часто стають платформами для вчинення злочинів;

– програми-клієнти для сервісів електронної пошти;

– браузери із збереженими даними облікових записів інтернет-сайтів;

– документи різноманітних форматів.

Означені можливості можуть значно змінюватись, розширюватись або звужуватись в залежності від конкретних моделей мобільного телефону та технічних можливостей з дослідження пристрою, що доступні слідчому.

Усю інформацію, що зберігається у терміналі, можна умовно розділити на аудіовізуальну, текстову та змішаного характеру. Серед аудіовізуальної інформації певне місце посідає така, що має особистий або розважальний характер – фотографії родичів затриманого, друзів, тварин, музичні та відео файли, а також звукозаписи (може бути використана слідчим при складанні психологічного

портрету особи, або в якості бази для встановлення психологічного контакту при проведенні слідчих дій). Часто, серед особистих відомостей віднаходяться такі, що мають безпосереднє відношення до вчинення злочинів – зображення потерпілих, механізму злочину, місця приховання слідів, звукозаписи перемовин та ін. Тому такі дані мають бути ретельно переглянуті та прослухані слідчим. Наприклад, звукозаписи перемовин мають бути розшифровані до стенограми. Відеозапис має знайти своє відображення в протоколі відносно осіб, що з'являються в кадрі, часу їх перебування, характеру дій та розшифровки звукового ряду. При цьому виявлені відео-, фотозображення та музичні файли розважального характеру, як правило, не описуються в протоколі слідчої дії.

В разі відсутності спеціаліста найбільш безпечним способом копіювання відомостей з терміналу є їх переписування з екрану пристрою до протоколу слідчого огляду. Певної автоматизації цього процесу можна досягти за допомогою програмного забезпечення з синхронізації відомостей в терміналі із програмним забезпеченням в комп'ютері, що може бути загружено з сайту відповідного виробника. Такі програми, як правило, мають нескладний інтерфейс та представляють базовий доступ до функцій терміналу, дозволяючи перенести адресну книгу, наявні в телефоні текстові повідомлення, замітки, заплановані справи з календарю та інші відомості. Слідчий має пересвідчитись в тому, що перед синхронізацією списку контактів з програми (наприклад, Microsoft Outlook) встановленої на комп'ютері за допомогою якого проводиться огляд видалено усі без винятку записи у календарі, а також немає жодного контакту у адресній книзі. Неврахування цього може призвести до завантаження контактів та дат справ з календарю, що зберігаються в комп'ютері до терміналу та, як наслідок, до змішування інформації. Серед розповсюджених програмних засобів, що використовуються слідчими при самостійному огляді мобільних телефонів Sony, Sony Ericsson – MyPhoneExplorer; Nokia – Nokia PC Suite; Samsung – Kies тощо.

Не можна вважати за прийнятну розповсюджену серед слідчих практику використання іншої SIM-картки при огляді мобільного телефону в разі відсутності доступу до нього із SIM-карткою з якою він був виявлений. Вжиття такого заходу є крайньою мірою, через те, що призводить до автоматичного та необоротного стирання журналу дзвінків, вхідних/вихідних повідомлень, дат календарю та у деяких моделях телефонів й до видалення адресної книги. В таких ситуаціях слідчий має дізнатися PIN оригінальної картки шляхом проведення допиту власника терміналу, огляду паперових записників та інших засобів зберігання такої інформації, або оперативним шляхом. Також необхідно пам'ятати, що при увімкненні мобільного телефону відбувається його реєстрація в мережі оператора із зазначенням відомостей про IMEI пристрою, IMSI (International Mobile Subscriber Identity / Міжнародний ідентифікатор користувача мобільного зв'язку) використовуваної слідчим картки, азимут антени базової станції мобільного зв'язку, дату, час тощо.

Слідчому необхідно мати на увазі, що неправильне застосування спеціального сервісного програмного забезпечення (що пропонується виробником або розроблено ентузіастами) несе суттєву небезпеку щодо цілісності даних збережених в терміналі.

На відміну від огляду SIM-картки, дослідження терміналу має особливості, що залежать від його виробника, механічної цілісності та роботи електронних компонентів. Через це огляд зазначеного пристрою рекомендується провести із залученням спеціаліста.

Обов'язковим компонентом мобільного телефону стандарту GSM є SIM-карта (Subscriber Identity Module / Модуль ідентифікації абонента). В залежності від кількості програм, що підтримується розрізняють однопрограмні й багатопрограмні смарт-карти. Перша група карт містить в собі одну програму, призначену для взаємодії з устаткуванням користувача (наприклад, SIM-карта містить лише програму, що забезпечує функціонування мобільного телефону стандарту GSM). Як правило, карти даного типу використовуються в мобільному устаткуванні стандарту GSM.

Друга група карт йменується UICC (Universal Integral Circuit Card / Універсальна інтегральна картка), та може містити в собі одну або декілька програм. До програм першого рівня відносять: SIM (програма, що забезпечує функціонування стандарті GSM); CSIM (програма, що підтримує доступ до мереж стандарту CDMA); USIM (програма, що надає доступ до мереж 3G); ISIM (забезпечує доступ до мультимедійним засобам). Ці карти при підключенні до мобільного устаткування, функціонують в UICC-сесіях. При роботі з мобільними станціями минулих років випуску дані карти також можуть працювати в сумісному режимі. Карти R-UIM, використовувані в мобільному устаткуванні стандарту CDMA2000, є різновидом UICC пристроїв.

Відомості, що зберігаються в смарт-картах, організовані в вигляді файлової системи й захищені апаратною архітектурою й встановленим програмним забезпеченням. Обмеження доступу до карт встановлюється цифровою послідовністю та для однопрограмних карт йменується CHV (Card Holder Verification / Перевірка власника карти), а для багатопрограмних – PIN (Personal Identification Number / Персональний ідентифікаційний номер).

Такий код є різновидом адміністративного паролю, що надає низький рівень доступу та не дозволяє здійснювати на карті суттєві зміни. Довжина даного коду в залежності від вибору користувача складає від 4 до 20 цифр. Для вводу PIN, в залежності від заводських налаштувань карти, надається від 3 до 10 спроб й у випадку помилки карта блокується до введення правильного PUK (Personal Unblocking Key / Персональний ключ розблокування). Питання про можливість усунення чи зняття PIN чи PUK, як правило, вирішується негативно, через відсутність загальнодоступних апаратних и програмних засобів для обходу вищевказаних кодів.

Смарт-карта може містити операційну систему, яка може виконувати програми призначені для обслуговування різних завдань/задач. Однією з таких програм є SIM програма, яка підтримує файловою системою смарт-карти за вибором оператора базові функції ідентифікації користувача у мережі мобільного зв'язку,

банкінгу, SIM-меню, ведення журналу дзвінків, телефонної книги, збереження SMS та ін. Відміни в наборах файлів, використовуваних програмами SIM, R-UIM, CSIM и USIM є важливими з криміналістичної точки зору та мають враховуватись програмним забезпеченням для огляду смарт-карт.

Криміналістичне дослідження телефонної книги, що знаходиться в SIM-карті, має базуватися на двоелементному джерелі – файлі скорочених номерів набору, доповнених відомостями з файлу розширень. USIM-картки мають набагато більш розвинену телефонну книгу. Так, кількість можливих записів не може бути меншою за 500, одній особі може бути співставлено декілька телефонних номерів, адреса електронної пошти, приналежність до групи тощо. Така телефонна книга утворюється сукупністю з 16 файлів.

Процедура огляду й використання інформації з смарт-карт доволі проста, й в сумі з складанням відповідного протоколу займає не більш 1 години для одного пристрою, однак цей час може суттєво відрізнятися в залежності від стану пристрою, наявності й готовності устаткування, можливості залучення спеціаліста. Додаткового часу потребує й подальший аналіз й розбір отриманих відомостей.

SIM-картка може містити наступні важливі для слідчого відомості:

1) Скорочені номери викликів (телефонна книга) записи за якими складаються з телефонного номеру (до 24 цифр) та відповідного йому тексту латинськими або кириличними літерами (до восьмі символів). Записи можуть бути занесені як при виготовлені картки та й користувачем, та займають після цього постійне місце. Видалений запис знищується на картці, звільняючи місце для подальшого використання та не може бути відновлений, а виявлення пропущених місць серед записів свідчить про факт видалення інформації. Слід зазначити, що в залежності від налаштувань терміналу мобільного зв'язку актуальна телефонна книга може вестися засобами власне терміналу або на картці. Об'єм телефонної книги залежить від технічних даних SIM-картки та складає від 100 номерів.

2) Вхідні SMS також можуть зберігатися на картці в залежності від налаштувань терміналу мобільного зв'язку або використанні його моделей попередніх років випуску. SIM-картка може зберігати від 10 коротких повідомлень, однак слід враховувати, що довгі повідомлення розбиваються для зберігання на декілька частин, що займають вільне місце та відповідно на пристрої може зберігатись менше коротких повідомлень (SMS).

3) Виявлення на картці записів в розділі останніх набраних номерів, може свідчити про використання картки у застарілому терміналі.

Ситуації виявлення мобільного телефону (терміналу) можна розділити в залежності від стану в якому він був виявлений на такі: 1) виявлення вимкненого терміналу; 2) виявлення увімкненого терміналу.

У першій ситуації має бути встановлено цілісність та справність терміналу, працездатність акумулятора, наявність SIM-картки та картки флеш-пам'яті. Цілісність встановлюється шляхом візуального огляду, зсуву кришки акумуляторного відсіку із подальшим оглядом стану внутрішніх елементів терміналу, особливу увагу звертають на виявлених патьоків, слідів корозії та плісняви (що можуть вказувати на перебування пристрою у рідинах, ґрунті або на неналежне зберігання після вилучення), також перевіряється хід кнопок клавіатури. Працездатність акумулятора може бути встановлена із використанням аналогічного терміналу або шляхом вимірювання напруги та току на клемах акумулятору, несправний акумулятор необхідно замінити. Вмикання терміналу в зборі до проведення огляду складових не рекомендується.

Виявлена SIM-картка оглядається за вищезазначеною процедурою, а флеш-карта оглядається за відповідною технологією огляду.

Спорядивши термінал справним та повністю зарядженим акумулятором (флеш- та SIM-карта мають бути вилучено) можна перейти до встановлення справності терміналу. Для цього необхідно підключити зазначений пристрій із використанням сервісного

кабелю до комп'ютеру, та провести визначення терміналу засобами операційної системи та відповідного програмного забезпечення. Така процедура має певні особливості в залежності від моделі терміналу та має проводитись кваліфікованим спеціалістом. В результаті такої дії може бути встановлено не тільки працездатність терміналу, однак може бути скопійована його внутрішня пам'ять із метою її подальшого дослідження спеціалістом або експертом. Якщо термінал виявився несправним, то необхідно перейти до дій за відповідною ситуацією.

Друга ситуація є найбільш сприятливою, дозволяє слідчому провести :

1) моніторинг вхідних дзвінків отриманих після вилучення терміналу.

2) огляд навіть за відсутності відомостей щодо PIN карти та коду блокування терміналу.

Хоча в літературі існує думка щодо безпечності відключення терміналу відразу після його виявлення, однак слідчому не слід з цим поспішати. Треба враховувати, що увімкнений термінал надає доступ практично до всієї важливої для слідчого інформації, а вимкнення терміналу може призвести до блокування самого пристрою або картки за PIN. Код блокування пристрою не в усіх випадках може бути знятий програмними засобами без знищення інформації, що зберігається в терміналі. Натомість розблокування сім-карток програмними засобами на даний час є неможливим, а отримання відомостей щодо PIN або PUK від операторів мобільного зв'язку пов'язане з оформленням відповідних запитів. Зазначене призводить до суттєвої втрати часу і не завжди призводить до бажаних результатів, особливо в разі направлення відповідного запиту закордонному оператору. У випадках роботи із заблокованими картками з яких стерто ознаки оператора або клонованими картками в яких Ki (Authentication Key / Ключ аутентифікації) записаний на носії сторонніх виробників відновлення доступу до карток утруднено. Отже більш доцільним є забезпечення підзарядки акумулятора телефону із переведенням терміналу до

автономного режиму, якщо для цієї моделі пристрою це не призведе до активації коду доступу – в цьому разі рекомендується поміщення терміналу до пакета (коробки) Фарадея.

Ситуація виявлення несправного або візуально ушкодженого терміналу потребує від слідчого особливої уважності. При цьому слідчий має зібрати та належно упакувати усі складові частини терміналу незалежно від їх зовнішнього вигляду. Оскільки термінал є складним багатокомпонентним пристроєм, різні системи якого можуть працювати незалежно одна від одної, тому слід розділяти повну та достатню працездатність терміналу. Так, наприклад, механічне або електричне ушкодження радіотракту, відеопідсистеми або клавіатури не виключають збереження даних в терміналі. Якщо повна працездатність мобільного телефону робить огляд більш зручним та швидким, то достатня працездатність може включати несправність екрану, частковий вихід з ладу клавіатури, відсутність фрагментів корпусу при збереженні доступу до внутрішньої пам'яті терміналу. Непрацездатний термінал має бути доведений до достатнього стану вже у лабораторних умовах, однак лише у разі впевненості спеціаліста у можливості збереження внутрішньої пам'яті пристрою.

2. Попереднє техніко-криміналістичне дослідження комп'ютерів.

Оскільки комп'ютери надзвичайно широко використовується у повсякденному житті, остільки різноманітним є й коло запитань, у розв'язанні яких зацікавлені слідчі, при дослідженні цього різновиду електронного носія інформації.

Комп'ютер можна розуміти в широкому сенсі – як будь-який електронний пристрій, споряджений процесором, оперативною й постійною пам'яттю, пристроями вводу виводу інформації. Однак, комп'ютер тут і далі розуміється у вузькому сенсі – як різноманітні електронні пристрої, що мають вигляд ноутбуку або персонального комп'ютера.

При характеристиці криміналістичного потенціалу комп'ютера необхідно враховувати як тактичні завдання, що стоять перед

слідчим при проведенні слідчої (розшукової) дії, так й криміналістичний різновид злочину, що розслідується. Отже, при розслідуванні підробки документів, посадових й господарських злочинів слідчого цікавить відбиття документального сліду в комп'ютерній техніці. В зв'язку з цим при проведенні слідчим обшуків, оглядів, призначенні експертиз в першу чергу мають бути досліджені комп'ютерні програми, що можуть використовуватись при веденні облікових операцій (1С, Парус, Microsoft Word, Microsoft Excel, програмне забезпечення власної розробки тощо), а також створені в них файли. Крім цього, для підробки графічних елементів реквізитів документів можуть використовуватись графічні редактори.

При розслідуванні злочинів, за якими сліди переважно локалізуються на матеріальних носіях інформація, що міститься в комп'ютерній техніці цікавить слідчого дещо в іншому аспекті. Сукупність слідів, що можуть бути виявлені за злочинами цієї категорії, випливає із прийомів використання комп'ютерів в способі злочину. Так, комп'ютерна техніка та програмне забезпечення (наприклад, в соціальних мережах чи в програмах з обміну текстовими повідомленнями) можуть застосовуватись, зокрема, для передавання погроз потерпілому, або при проведенні перемовин при замовленні злочину, або для спілкування злочинців при плануванні чи вчиненні злочину тощо. В ряді випадків на комп'ютерах опиняються цифрові фотографії, відео- звукозаписи механізму злочину в цілому або його частини.

З урахуванням того, що навіть попереднє техніко-криміналістичне дослідження комп'ютерної техніки потребує належного ступеня володіння спеціальними навичками необхідно рекомендувати залучення слідчим спеціалістів. Підбір спеціаліста має здійснюватись відповідно до завдань, які буде необхідно розв'язати при проведенні слідчої дії. Це можуть бути спеціалісти в галузі: мережевих технологій, програмного (системного, прикладного) чи апаратного забезпечення тощо. Слідчий повинен попередити спеціаліста про необхідність забезпечити збереження

даних, наявних у обчислювальній техніці. Кожна дія або комплекс дій спеціаліста, що можуть потягнути за собою знищення відомостей в комп'ютері мають бути узгоджені зі слідчим.

У тому разі, якщо комп'ютер є носієм важливих відомостей можна рекомендувати наступну послідовність дій:

1) проведення фотозйомки екрану;

2) перевірка наявності та відключення паролю заставки екрану, системного паролю, па також паролю BIOS;

3) встановлення використання шифрування (окремих контейнерів, дисків, файлових систем), в разі використання – копіювання відомостей з зашифрованих носіїв;

4) визначення підключення мережевих дисків;

5) фіксація віддалених вхідних/вихідних підключень;

6) здійснення скріншоту списку запущених процесів;

7) копіювання вмісту (дампу) оперативної пам'яті на флешносій;

8) створення образу запам'ятовуючого пристрою – за необхідності.

Комп'ютери, що доводиться досліджувати під час проведення слідчих (розшукових) дій умовно можна розділити на найпростіші, що мають мінімальну конфігурацію, необхідну для роботи й ускладнені. Ускладнені за конфігурацією комп'ютери це, як правило, сервери, а також персональні комп'ютери, призначені для виконання спеціалізованих завдань. В разі необхідності такі «ускладненні» комп'ютери бажано вилучати як є, тобто у виявленій конфігурації. Це пов'язано з тим, що така комп'ютерна техніка часто обладнується декількома жорсткими дисками, які під керуванням засобів операційної системи або із використанням відповідних RAID-контролерів можуть працювати разом, зберігаючи, з метою оптимізації швидкості доступу, частини одного й того самого файлу на декількох жорстких дисках. Отже вилучення комп'ютера у вихідній конфігурації забезпечить збереження апаратних налаштувань й полегшить наступне експертне дослідження таких систем.

Програмне забезпечення, що може застосовуватись при попередньому техніко-криміналістичному дослідженні комп'ютерів, умовно можна розділити на декілька груп – калькулятори хешів (HashTab, Rehash); шістнадцятирічні редактори (WinHEX, wxHexEditor); дуплікатори даних (dd), аналізатори (зображень, баз даних, OLE-файлів). Також використовуються програмні комплекси, що об'єднують декілька функцій в одному інтерфейсі (Forensic Toolkit, EnCase Forensic, Sleuth Kit).

Національна академія правових наук України

Науково-дослідний інститут вивчення проблем злочинності
імені академіка В. В. Сташиса

ІННОВАЦІЙНІ ЗАСАДИ ТЕХНІКО-КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ КРИМІНАЛЬНОЇ ЮСТИЦІЇ

Монографія

За редакцією
академіка НАПрН України В. Ю. Шепітька,
члена-кореспондента НАПрН України В. А. Журавля

Харків
2017

УДК 343.98 : 001.895
ББК 67.52
І 67

Рекомендовано до друку вченою радою Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса Національної академії правових наук України (протокол № 11 від 26 жовтня 2016 р.)

Рецензенти:
Коновалова В. О. – професор кафедри криміналістики Національного юридичного університету іменні Ярослава Мудрого, доктор юридичних наук, професор, академік Національної академії правових наук України
Степанюк Р. Л. – завідувач кафедри криміналістики та судової експертології факультету №1 Харківського національного університету внутрішніх справ, доктор юридичних наук, професор

Колектив авторів:
Шепітько В. Ю. – Передмова, §§ 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 3.1, 3.2; Журавель В. А. – Передмова, §§ 1.2, 4.1, 4.2, 4.3, 4.4; Авдєєва Г. К. – §§ 1.1, 1.2, 1.3, 1.4, 1.5, 2.3, 3.2, 3.3, 3.4; Білоус В. В. – §§ 2.1, 2.4; Великанов С. В. – §§ 2.5, 3.5; Гетьман Г. М. – § 2.2; Затенацький Д. В. – §§ 2.7, 2.8; Керик Л. І. – § 2.6; Павлюк Н. В. – §§ 4.2; 4.4; Резнікова О. І. – §§ 4.1; 4.4.

І 67 Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції : Монографія / кол. авт. В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за ред. В. Ю. Шепітька, В. А. Журавля. – Х.: Вид. агенція «Апостіль», 2017. – 260 с.

Монографію присвячено проблемам розроблення інноваційних засад техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції. У роботі розкрито сутність інновацій у техніко-криміналістичному забезпеченні діяльності органів кримінальної юстиції, досліджено проблеми застосування новітніх інформаційних технологій у діяльності органів досудового розслідування, інноваційні підходи до використання спеціальних знань у правозастосовній діяльності та питання техніко-криміналістичного забезпечення розслідування кримінальних правопорушень корупційної спрямованості.

Для науковців, працівників правоохоронних та судових органів, викладачів, аспірантів та студентів юридичних навчальних закладів.

ББК 67.52

ISBN