ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ВИКОРИСТАННЯ ЕЛЕКТРОННИХ НОСІЇВ ІНФОРМАЦІЇ З МЕДІА-КОНТЕНТОМ У ЯКОСТІ ДЖЕРЕЛ ДОКАЗІВ

Методичні рекомендації

Дніпро – 2019

Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів: методичні рекомендації / Авт. колектив: А.В. Захарко, А.Г. Гаркуша, В.В. Рогальська, І.В. Краснобрижий, О.В. Брягін – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2019. – 73 с.

РЕЦЕНЗЕНТИ:

Пиріг І.В. – професор кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, доцент

Макашов А.В. – заступник начальника відділу УЗЕ в Дніпропетровській області ДЗЕ Національної поліції України, кандидат юридичних наук, майор поліції

Санакоєв Д.В. – завідувач кафедри фінансово-економічної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент, підполковник поліції

Методичні рекомендації підготовлені згідно п.6 Переліку тем для підготовки методичних рекомендацій за дорученням ректора Дніпропетровського державного університету внутрішніх справ від 21 січня 2019 року №2 на замовлення Департаменту захисту економіки Національної поліції України від 7 грудня 2018 року № 14448/39/03-2018 (вх. №3283 від 14.12.2018).

З урахуванням сучасних потреб правоохоронної діяльності, стану розвитку інформаційних технологій та кримінальної процесуальної науки розглянуто кримінальний процесуальний порядок використання електронних носіїв інформації з медіа-контентом у якості джерел доказів.

Методичні рекомендації розраховані на працівників слідчих та оперативних підрозділів, здобувачів вищої освіти, викладачів вищих навчальних закладів юридичного профілю.

Розглянуто на спільному засіданні кафедри кримінального процесу та кафедри економічної та інформаційної безпеки 10 вересня 2019 року, протокол № 1.

Розглянуто та ухвалено до друку Науково-методичною радою Дніпропетровського державного університету внутрішніх справ 21 листопада 2019 року, протокол № 3.

ЗМІСТ

ВСТУП

Стрімкий всесвітній науково-технічний прогрес системно відображується на криміногенній обстановці в Україні. У звіті Голови Національної поліції України про результати роботи відомства за 2018 рік окрему увагу приділено як результатам роботи Департаменту кіберполіції (за звітний рік підрозділом виявлено близько 6 тисяч злочинів, вчинених у сфері використання високих інформаційних технологій, попереджено поширення 4 масових кібератак на території України, припинено діяльність понад 40 піратських сайтів, викрито 8 транснаціональних хакерських угрупувань тощо), так і боротьбі зі злочинами у сфері економіки (викрито 1800 фактів хабарництва, 3,7 тисяч фактів кримінальних правопорушень у бюджетній сфері, відмінено 2153 конкурсних торгів тощо) [1, с.14, 15][1]. Згідно з Положенням про Департамент захисту економіки Національної поліції України[2], до завдань Департаменту захисту економіки Національної поліції (далі – ДЗЕ), зокрема, належить виявлення, запобігання та припинення злочинів у сфері економіки, боротьба з корупцією й хабарництвом тощо. Вчинення злочинів зазначених категорій тісно пов'язане з використанням досягнень науково-технічного прогресу, використанням комп'ютерних даних, електронних носіїв інформації тощо. Тому якісна взаємодія працівників ДЗЕ з органами досудового розслідування, вчасне, системне й послідовне виявлення та збирання джерел доказів, професійно грамотне використання електронних носіїв інформації в якості джерел доказів є запорукою ефективної боротьби зі злочинами зазначених категорій.

З іншого боку, звернувшись до статистичних даних щодо розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку маємо звернути увагу на динаміку їх зростання. Порівняємо дані Єдиного звіту Генеральної прокуратури України про кримінальні правопорушення по державі за результатами 2014 і 2018 років [2, 3][3].

Протягом 2018 року, в порівнянні з даними 2014 року, кількість кримінальних правопорушень, передбачених у ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» КК України збільшилося більш, ніж утричі. За ст. 361-1 «Створення з метою використання, розповсюдження або збуту

---

[1] Звіт Голови Національної поліції України С. Князєва про результати роботи відомства за 2018 рік. Офіційний сайт Національної поліції. Річні звіти. URL: https://www.npu.gov.ua/activity/zviti/richni-zviti/ (дата звернення: 21.08.2019).

[2] затверджене наказом Національної поліції України від 7 листопада 2015 року №81

[3] Єдиний звіт про кримінальні правопорушення по державі за грудень 2014 року. Генеральна прокуратура України. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=111480&libid=100820# (дата звернення: 12.03.2019).

Єдиний звіт про кримінальні правопорушення по державі за грудень 2018 року. Генеральна прокуратура України. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113653&libid=100820&c=edit&_c=fo (дата звернення: 12.03.2019)

Єдиний звіт про кримінальні правопорушення по державі за січень-липень 2018 року. Генеральна прокуратура України. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113653&libid=100820&c=edit&_c=fo (дата звернення: 22.08.2019)

Єдиний звіт про кримінальні правопорушення по державі за січень-липень 2019 року. Генеральна прокуратура України. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113653&libid=100820&c=edit&_c=fo (дата звернення: 22.08.2019)

шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» КК України кількість зареєстрованих кримінальних правопорушень збільшилося більш, ніж у тринадцять (!) разів. За ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» КК України збільшилося більш, ніж у чотирнадцять (!) разів [4].

Згідно статистичних даних Єдиного звіту Генеральної прокуратури про кримінальні правопорушення за січень-липень 2019 року, протягом зазначеного періоду обліковано 902 кримінальні правопорушення за ознаками ст.361 КК України, 140 кримінальних правопорушень за ознаками ст.361-1 КК України, 28 кримінальних правопорушень за ознаками ст.361-2 КК України [5]. Протягом січня-липня 2018 року кількість облікованих кримінальних правопорушень за ознаками зазначених вище статей відповідно становила 729 за ст.361 КК України [4] (тобто, маємо динаміку зростання +173 за останній рік або +23,7%), 101 за ознаками ст.361-1 КК України (тут негативна динаміка -39 за останній рік або -38,6%), 33 за ознаками ст.361-2 КК України (тут динаміка зростання становить +5 за останній рік або +15,1%). І звісно, ефективність використання стороною обвинувачення електронних носіїв інформації в якості джерел доказів має значення не лише при розслідуванні злочинів проаналізованих категорій. Електронні носії інформації можуть використовуватися для отримання доказової інформації при розслідуванні будь-яких злочинів. Всеохоплюючий науково-технічний прогрес і глобальна комп’ютеризація в більшості галузей функціонування як суспільства, так і державних інституцій, відбувається в ситуації, коли в Україні навіть немає такої статистичної звітності, що могла б комплексно відобразити значущість ефективної роботи органів досудового розслідування з різноманітними електронними носіями інформації.

Таким чином, актуальність дослідження способів підвищення ефективності роботи як оперативних підрозділів, так і органів досудового розслідування в напрямку використання електронних носіїв інформації у якості джерел доказів є дійсно високою. І анонсована керівництвом МВС України ліквідації Департаменту захисту економіки Національної поліції, створення служби фінансових розслідувань жодним чином не зменшують актуальності досліджуваної в цих Методичних рекомендаціях тематики.

АНАЛІЗ ТЕРМІНОЛОГІЇ

Заявлення в назві зазначених методичних рекомендацій конструкції «Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів» зумовлює необхідність звернути увагу читачів на сталі терміни, що використовуються в нормативних актах та інших важливих спеціальних джерелах при позначенні аналізованого виду діяльності.

В методичних рекомендаціях «Організація розслідування фактів несанкціонованого переказу коштів з рахунків клієнтів банку, які обслуговуються за допомогою систем дистанційного обслуговування» зазначається, що інформація матеріалізується в носіях інформації, якими можуть бути фізичні об'єкти, поля і сигнали, хімічні середовища, нагромаджувачі даних в інформаційних системах. Носіями інформації в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку виступають тверді фізичні об'єкти (жорсткі диски, дискети, компакт-диски тощо), сигнали (у каналах зв'язку), поля (оперативна пам'ять ЕОМ та її периферійних пристроїв). Носії інформації можуть бути вилучені з володіння законного власника або пошкоджені чи знищені. Інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах, зберігається на носіях такої інформації у формі даних. Правова охорона інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах або пересилається каналами електрозв'язку, зумовлена не статусом цієї інформації як об'єкта власності, а її змістом, споживчою цінністю, здатністю задовольняти інформаційні потреби [6].

У Конвенції про кіберзлочинність, зокрема, визначаються такі терміни:

«комп'ютерна система» - означає будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більше з яких, відповідно до певної програми, виконує автоматичну обробку даних;

«комп'ютерні дані» - означає будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою.

Аналізуючи зміст Конвенції про кіберзлочинність та Закон України про її ратифікацію, доцільно виокремити актуальність напрямку роботи «збирання доказів у електронній формі» при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними [7, 8]. За змістом Конвенції цілком зрозумілим є використовуваний у ній логічний ряд, що являє собою: комп'ютерну систему (1) або її частину (2), комп'ютерні дані (3), що зберігаються в ній, і лише на 4 місці пишуть про «комп'ютерний» (не електронний!) носій інформації, на якому можуть зберігатися комп'ютерні дані.

А комп'ютерним носієм інформації, як зазначається у вище зазначених методичних рекомендаціях, може виступати фізичний об'єкт (1), електромагнітний

сигнал (2), електромагнітне поле (3), хімічне середовище (4), нагромаджувач даних (5) [6].

Тому пріоритетними з міркувань доказування конструкціями, що використовуватимуться в цих методичних рекомендаціях будуть терміни «комп'ютерний носій інформації», «комп'ютерні дані», «комп'ютерна система або її частина».

Термін «електронні носії інформації» вживається в Законі України (далі – ЗУ) «Про електронні документи та електронний документообіг» від 22 травня 2003 року №851-IV [9], а сфера дії цього закону поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів. Здійснена в КПК України нормативна регламентація використання електронних носіїв інформації в якості джерел доказів, терміном «електронні носії інформації» наразі майже не оперує. Найбільш придатні для використання близькі за змістом сталі конструкції – це «інші носії інформації (у тому числі електронні)», як вид документа (ст.99 КПК), носії комп'ютерної інформації (ст.105 КПК), технічні носії інформації (ст.107 КПК) [10] тощо.

Можна припустити, що це технічна помилка законодавця. Адже за сталим у широкому загалі розумінням, електронний носій інформації – це щось матеріальне, тобто, є речовим доказом, якщо оперувати кримінальною процесуальною мовою. Тобто, USB-накопичувач є речовим доказом, а файл на ньому – є електронним документом. У ЗУ «Про електронні документи та електронний документообіг» оперується термінами «дані», «електронний документ». В ЗУ «Про електронні довірчі послуги» оперується терміном «електронні дані» [11].

Втім, у ч.3 ст.9 КПК зазначається, що закони та інші нормативно-правові акти України, положення яких стосуються кримінального провадження, повинні відповідати цьому Кодексу. При здійсненні кримінального провадження не може застосовуватися закон, який суперечить цьому Кодексу.

В ч.2 ст.1 КПК України, зокрема, зазначається, що кримінальне процесуальне законодавство України складається також і з міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України. А в ч.4 ст.9 КПК України йдеться про те, що у разі, коли норми КПК України суперечать міжнародному договору, згода на обов'язковість якого надана Верховною Радою України, застосовуються положення відповідного міжнародного договору України. Звідси, знову ж таки приходимо до висновку про доцільність користування термінологією: «комп'ютерний носій інформації», «комп'ютерні дані», «комп'ютерна система або її частина».

Аналізуючи заявлену тему методичних рекомендацій, необхідно відразу звернути увагу ще й на такому аспекті.

В кримінальному процесуальному законі конструкція «Використання у якості джерел доказів» в контексті роботи слідчого органів досудового розслідування Національної поліції на стадії досудового розслідування в буквальному сенсі не вживається. В КПК чітко визначений процесуальний порядок здійснення

доказування, що полягає у збиранні, перевірці, оцінці доказів (тобто, фактичних даних), а не їх джерел.

Процесуальні джерела доказів – це форма збереження фактичних даних. А використовуються на стадії досудового розслідування не стільки форма збереження фактичних даних, як самі фактичні дані у процесі здійснення доказування. Форма збереження фактичних даних має значення лише в контексті забезпечення допустимості доказів, тобто процесуального порядку їх отримання та виконання вимог закону щодо зберігання речових доказів і документів (ст. 100 КПК України) та дотримання вимог Порядку зберігання речових доказів стороною обвинувачення [12].

Робота з процесуальними джерелами доказів регламентується в ст.290 КПК України під час відкриття матеріалів іншій стороні (до них надається доступ іншій стороні). Крім того, «речові докази» і «документи» досліджуються в суді на стадії судового розгляду (ст.357, 358 КПК), а саме оглядаються, подаються на ознайомлення учасникам, оголошуються, виключаються, піддаються експертизі.

Враховуючи вимоги глави 4 КПК «Докази і доказування» логічно стверджувати, що електронні носії інформації з медіа-контентом можуть бути віднесені до таких джерел доказів як «речові докази» або «документи». При цьому, немає жодних відмінностей у кримінальному процесуальному порядку та й технічному порядку обслуговування, залежно від того, медіа-, чи інший контент знаходиться на релевантному електронному носії інформації. Втім, студією он-лайн освіти Ed-era підготовлено спеціальний он-лайн курс з медіаграмотності[4], пройти який було б корисним для працівників правоохоронних органів з метою набуття навичок аналізу таких відомостей, і в якому залежно від способів передання медіа інформації, виділяють 6 типів контенту: інформування, судження, пропаганда, зв'язки з громадськістю (piar), соціальна реклама, комерційна реклама. В структурі процесу доказування виділяють такі етапи: 1) побудова (висування) і динамічний розвиток версій у кримінальному провадженні; 2) збирання доказів; 3) перевірка доказів; 4) оцінка доказів; 5) обґрунтування висновків, яких дійшли суб'єкти доказування. Врахування специфіки медіа-контенту має певне значення в структурі процесу доказування, що буде викладено нижче за змістом.

Якщо ж виходити з кримінальної процесуальної регламентації роботи з доказами, то будь-який контент є просто комп'ютерними даними, що мають певну споживчу цінність і здатні задовольнити інформаційну потребу сторони обвинувачення (чи захисту) під час доказування обставин, що належать до предмету доказування.

В КПК України (зокрема, ст.100) регламентується діяльність із зберігання речових доказів. Електронний носій інформації, якщо він відповідає дефініції «речового доказу» (ст.98 КПК, зокрема, якщо він є матеріальним об'єктом), може бути отриманий стороною обвинувачення, вилучений, взятий під контроль стороною обвинувачення за певним процесуальним порядком, оглянутий, сфотографований, описаний, скопійований, долучений до кримінального провадження, повернутий володільцю, збережений, втрачений або знищений тощо.

[4] розміщений за посиланням: https://verified.ed-era.com/ua/u1

ГЛОСАРІЙ

В цьому глосарії використано термінологію, як її визначено в ЗУ «Про телекомунікації» та в нормативному документі технічного захисту інформації НД ТЗІ 1.1-003-99

Абонент - споживач телекомунікаційних послуг, який отримує телекомунікаційні послуги на умовах договору, котрий передбачає підключення кінцевого обладнання, що перебуває в його власності або користуванні, до телекомунікаційної мережі;

Адреса мережі Інтернет - визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв;

Адресний простір мережі Інтернет - сукупність адрес мережі Інтернет;

Безпроводовий доступ до телекомунікаційної мережі (безпроводовийдоступ) - електрозв'язок з використанням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися із збереженням унікального ідентифікаційного номера в межах пунктів закінчення телекомунікаційної мережі, які під'єднані до одного комутаційного центру;

Голосова телефонія - обмін інформацією голосом у реальному часі з використанням телекомунікаційних мереж;

Дані - інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки;

Домен.UA - домен верхнього рівня ієрархічного адресного простору мережі Інтернет, створений на основі кодування назв країн відповідно до міжнародних стандартів, для обслуговування адресного простору українського сегмента мережі Інтернет;

Домен другого рівня - частина адресного простору мережі Інтернет, що розташовується на другому рівні ієрархії імен у цій мережі;

Інтернет - всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами;

Інформаційна безпека телекомунікаційних мереж - здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації;

Інформація - відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

Канал електрозв'язку - сукупність технічних засобів, призначених для перенесення електричних сигналів між двома пунктами телекомунікаційної мережі, і який характеризується смугою частот та/або швидкістю передачі;

Оператор телекомунікацій - суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж;

Передавання даних - передавання інформації у вигляді даних з використанням телекомунікаційних мереж;

Провайдер телекомунікацій - суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку;

Рухомий (мобільний) зв'язок - електрозв'язок із застосуванням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися в межах усіх пунктів закінчення телекомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільної станції;

Споживач телекомунікаційних послуг (споживач) - юридична або фізична особа, яка потребує, замовляє та/або отримує телекомунікаційні послуги для власних потреб;

Телекомунікації (електрозв'язок) - передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах;

Телекомунікаційна мережа - комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням;

Телекомунікаційна послуга (послуга) - продукт діяльності оператора та/або провайдера телекомунікацій, спрямований на задоволення потреб споживачів у сфері телекомунікацій;

Технічні засоби телекомунікацій - обладнання, станційні та лінійні споруди, призначені для утворення телекомунікаційних мереж;

АС — автоматизована система;
КЗЗ — комплекс засобів захисту;
КС — комп’ютерна система;
КСЗІ— комплексна система захисту інформації;
НСД — несанкціонований доступ;
ОС — обчислювальна система;
ПЗ — програмне забезпечення;
ПРД — правила розмежування доступу;
ТЗІ — технічний захист інформації.

Обчислювальна система; ОС (computer system) — сукупність програмних-апаратних засобів, призначених для обробки інформації;

Автоматизована система; АС (automated system) — організаційно-технічна система, що реалізує інформаційну технологію і об’єднує ОС, фізичне середовище, персонал і інформацію, яка обробляється;

Комп'ютерна система; КС (computer system, target of evaluation) — сукупність програмно-апаратніх засобів, яка подана для оцінки;

Загроза (threat) — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС;

Безпека інформації (information security) — стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації;

Комплексна система захисту інформації; КСЗІ — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС;

Комплекс засобів захисту; КЗЗ (trusted computing base; TCB) — сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації;

Захищена комп'ютерна система; захищена КС (trusted computer system, trusted computer product) — комп'ютерна система, яка здатна забезпечувати захист оброблюваної інформації від певних загроз;

Об'єкт комп'ютерної системи; об'єкт КС (product object, system object) — елемент ресурсу КС, що знаходиться під керуванням КЗЗ і характеризується певними атрибутами і поводженням;

Об'єкт-процес (process object) — виконувана в даний момент програма, яка повністю характеризується своїм контекстом (поточним станом регістрів бчислювальної системи, адресним простором, повноваженнями і т.ін.);

Користувач (user) — фізична особа, яка може взаємодіяти з КС через наданий їй інтерфейс;

Доступ до інформації (access to information) — вид взаємодії двох об'єктів КС, внаслідок якого створюється потік інформації від одного об'єкта до іншого і/або відбувається зміна стану системи;

Правила розмежування доступу; ПРД (access mediation rules) — частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів;

Тип доступу (access type) — суттєвість доступу до об'єкта, що характеризує зміст здійснюваної взаємодії, а саме: проведені дії, напрям потоків інформації, зміни в стані системи (наприклад, читання, запис, запуск на виконання, видаляння, дозапис).

Запит на доступ (access request) — звернення одного об'єкта КС до іншого з метою отримання певного типу доступу.

Санкціонований доступ до інформації (authorized access to information) — доступ до інформації, що не порушує ПРД;

Несанкціонований доступ до інформації; НСД до інформації (unauthorized access to information) — доступ до інформації, здійснюваний з порушенням ПРД;

Право доступу (access right) — дозвіл або заборона здійснення певного типу доступу;

Повноваження (privilege) — права користувача або процесу на виконання певних дій, зокрема на одержання певного типу доступу до об'єктів;

Авторизація (authorization) — надання повноважень; встановлення відповідності між повідомленням (пасивним об'єктом) і його джерелом (створившим його користувачем або процесом);

Авторизований користувач (authorized user) — користувач, що володіє певними повноваженнями;

Адміністратор (administrator, administrative user) — користувач, роль якого включає функції керування КС і/або КЗЗ;

Адміністратор безпеки (security administrator) — адміністратор, відповідальний за дотримання політики безпеки;

Порушник (user violator) — користувач, який здійснює несанкціонований доступ до інформації;

Критична інформація (sensitive information) — інформація, що вимагає захисту; будь-яка інформація, втрата або неправильне використання якої (модифікація, ознайомлення) може нанести шкоду власникові інформації або АС, або будь-якій іншій фізичній (юридичній) особі чи групі осіб;

Конфіденційність інформації (information confidentiality) — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом;

Атака (attack) — спроба реалізації загрози;

Проникнення (penetration) — успішне подолання механізмів захисту системи;

Вразливість системи (system vulnerability) — нездатність системи протистояти реалізації певної загрози або сукупності загроз;

Втрата інформації (information leakage) — неконтрольоване розповсюдження інформації, що веде до її несанкціонованого одержання;

Прихований канал (covert channel) — спосіб одержання інформації за рахунок використання шляхів передачі інформації, існуючих у КС, але не керованих КЗЗ, або спостереження за існуючими потоками інформації;

Відмова (fault, failure) — втрата здатності КС або її компонента виконувати певну функцію;

Відмова в обслуговуванні (denial of service) — будь-яка дія або послідовність дій, що призводять будь-яку частину (компонент) системи до виходу із ладу; нездатність системи виконувати свої функції (надавати декларовані послуги) внаслідок виходу із ладу якого-небудь компонента або інших причин;

Комп'ютерний вірус (computer virus) — програма, що володіє здатністю до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування КС і/або зумовити порушення політики безпеки;

Програмна закладка (program bug) — потайно впроваджена програма або недокументовані властивості програмного забезпечення, використання яких може призвести до обходу КЗЗ і/або порушення політики безпеки;

Люк (trap door) — залишені розробником недокументовані функції, використання яких дозволяє обминути механізми захисту;

Троянський кінь (Trojan horse) — програма, яка, будучи авторизованим процесом, окрім виконання документованих функцій, здатна здійснювати приховані дії від особи авторизованого користувача в інтересах розробника цієї програми;

Збирання сміття — загроза, що полягає в захопленні і аналізі користувачем або процесом спільно використовуваних об'єктів, звільнених іншим користувачем чи процесом, з метою одержання інформації, що в них знаходиться;

Ризик (risk) — функція ймовірності реалізації певної загрози, виду і величини завданих збитків;

Домен комп'ютерної системи; домен КС (domain) — ізольована логічна область КС, що характеризується унікальним контекстом, всередині якої об'єкти володіють певними властивостями, повноваженнями і зберігають певні відносини між собою;

Функціональний профіль (functionality profile) — упорядкований перелік рівнів функціональних послуг, який може використовуватись як формальна специфікація функціональності КС;

Ідентифікація (identification) — процедура присвоєння ідентифікатора об'єкту КС або встановлення відповідності між об'єктом і його ідентифікатором; впізнання;

Автентифікація (authentication) — процедура перевірки відповідності пред'яв-леного ідентифікатора об'єкта КС на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності;

Інформація автентифікації (authentication information) — інформація, що використовується для автентифікації;

Пароль (password) — секретна інформація автентифікації, що являє собою послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж йому буде надано доступ до КС або до інформації;

Персональний ідентифікаційний номер; ПІН (personal identification number, PIN) — вид паролю, що звичайно складається тільки із цифр, і який, як правило, має бути пред'явлений нарівні з носимим ідентифікатором;

Журнал реєстрації (audit trail) — упорядкована сукупність реєстраційних записів, кожен з яких заноситься КЗЗ за фактом здійснення контрольованої події;

Очищення пам'яті (memory clearing) — знищення даних в пам'яті шляхом встановлення полів цих даних в заданий або випадковий стан;

Аналіз прихованих каналів (covert channels analyse) — послуга, яка забезпечує гарантію того, що приховані канали в КС відсутні, знаходяться під наглядом або, принаймні, відомі;

Квота (quota) — обмеження можливості використання певного ресурсу КС користувачем або процесом;

Ініціалізація (initialization) — встановлення системи або об'єкта у відомий чи визначений стан;

Ядро захисту (security kernel) — частина КЗЗ, в якій зосереджено мінімально необхідний набір механізмів, що реалізують ПРД;

Криптографічне перетворення — перетворення даних, яке полягає в їх шифруванні, вироблення імітовставки або цифрового підпису;

Шифрування даних — процес зашифрування або розшифрування;

Зашифрування даних (data encryption) — процес перетворення відкритого тексту в шифртекст;

Розшифрування даних (data decryption) — процес перетворення шифртексту у відкритий текст;

Цифровий підпис (digital signature) — дані, одержані в результаті криптографічного перетворення блоку даних і/або його параметрів (хеш-функції, довжини, дати утворення, ідентифікатора відправника і т. ін.), що дозволяють приймальнику даних впевнитись в цілісності блоку і справжності джерела даних і забезпечити захист від підробки і підлогу;

1. ПОНЯТТЯ ТА ВИДИ ЕЛЕКТРОННИХ НОСІЇВ ІНФОРМАЦІЇ

Електронний носій інформації - матеріальний носій, який використовують для записування, зберігання та відтворення інформації, обробленої засобами комп'ютерної техніки (ДСТУ 7448:2013).

У 1945 р Джон фон Нейман (1903-1957), американський учений, висунув ідею використання зовнішніх запам'ятовуючих пристроїв для зберігання програм і даних. Нейман розробив структурну принципову схему комп'ютера. Схемі Неймана відповідають всі сучасні комп'ютери.

Зовнішня пам'ять призначена для довготривалого зберігання програм і даних. Пристрої зовнішньої пам'яті (накопичувачі) є незалежними, вимикання живлення не призводить до втрати даних. Вони можуть бути вбудовані в системний блок або виконані у вигляді самостійних блоків, пов'язаних з системним через його порти. За способом запису і читання накопичувачі діляться, в залежності від виду носія, на магнітні, оптичні і магнітооптичні.

Кодування інформації - це процес формування певного уявлення інформації. Комп'ютер може обробляти тільки інформацію, представлену в числовій формі. Вся інша інформація (наприклад, звуки, зображення, показання приладів і т. д.) Для обробки на комп'ютері повинна бути перетворена в числову форму. Як правило, всі числа в комп'ютері представлені за допомогою нулів і одиниць (а не десяти цифр, як це звично для людей). Іншими словами, комп'ютери зазвичай працюють у двійковій системі числення, оскільки при цьому пристрої для їх обробки виходять значно простішими.

Зчитування інформації - вилучення інформації, що зберігається в пристрої, що запам'ятовує (ЗП), і передача її в ін. Пристрої обчислювальної машини. Зчитування інформації проводиться при виконанні більшості машинних операцій, а іноді є самостійною операцією.

Види електронних носіїв інформації:

Всі електронні носії інформації можливо розділити на види, які обусловлені фізичними принципами запису інформації на них та читанням цієї записаної інформації. Існують наступні види електронних носіїв інформації – оптичні; магнітно-оптичні; напівпровідникові; магнітні. Оптичні – CD-ROM; DVD-ROM. Магнітно-оптичні – (MO). Напівпровідникові – твердотільні на основі Flash пам’яті (SSD); USB Flash Drive (флешка). Магнітні – жорстки диски, дискети, стримери.

1. Стример (від англ. Streamer), також стрічковий накопичувач - пристрій на принципі магнітного запису на стрічковому носієві, з послідовним доступом до даних, за принципом дії аналогічний побутового магнітофона.

Основне призначення: запис і відтворення інформації, архівація і резервне копіювання даних.

2. Накопичувач на гнучких магнітних дисках (назараз рідко використовується).

Це пристрій використовує в якості носія інформації гнучкі магнітні диски - дискети, які можуть бути 5-ти або 3-х дюймовими. Дискета - це магнітний диск начебто платівки, поміщений в «конверт». Залежно від розміру дискети змінюється її ємність в байтах. Якщо на стандартну дискету розміром 5'25 дюйма поміщається до 720 Кбайт інформації, то на дискету 3'5 дюйма вже 1,44 Мбайт. Дисковод - пристрій паралельного доступу, тому всі файли однаково легко доступні. Диск покривається зверху спеціальним магнітним шаром, який забезпечує зберігання даних. Інформація записується з двох сторін диска по доріжках, які представляють собою концентричні кола.

3. Накопичувач на жорсткому магнітному диску (НЖМД - вінчестер).

Мережеві жорсткі диски

Мережеві жорсткі диски

Мережеві жорсткі диски

Є логічним продовженням розвитку технології магнітного зберігання інформації. Коротко про головне:

- велика ємність;
- простота і надійність використання;
- можливість звертатися до безлічі файлів одночасно;
- висока швидкість доступу до даних.

З недоліків можна виділити лише відсутність знімних носіїв інформації, хоча в даний час використовуються зовнішні вінчестери і системи резервного копіювання.

У комп'ютері передбачена можливість за допомогою спеціальної системної програми умовно розбивати один диск на кілька. Такі диски, які не існують як окрема фізична пристрій, а представляють лише частину одного фізичного диска, називаються логічними дисками. Логічним дискам присвоюються імена, в якості яких використовуються букви латинського алфавіту [З:], [D:], [E:], [F:] і т. Д.

4. CD-ROM

У цих пристроях використовується принцип зчитування сфокусованим лазерним променем борозенок на металлизированном несучому шарі компакт-диска. Цей принцип дозволяє досягти високої щільності запису інформації, а, отже, і великої місткості при мінімальних розмірах. Компакт-диск є відмінним засобом зберігання інформації, він дешевий, практично не схильний до будь-яких впливів середовища, інформація, записана на ньому не спотвориться і не зітреться, поки диск не буде знищений фізично, його ємність 650 Мбайт. Має тільки один недолік - порівняно невеликий обсяг зберігання інформації.

5. Магнітооптичний диск (МО, також допускається написання магнітно- оптичний диск) - носій інформації, що поєднує властивості оптичних і магнітних накопичувачів. Для читання інформації використовується оптична система, для запису - одночасно оптична і магнітна. Ще використовується як найбільш надійний пристрій для зберігання цифрової інформації (дискі, які були записані у 90 роках 20 віку і не мають фізичних пошкоджень сьогодні читаються).

6. DVD

А) Відмінності DVD від звичайних CD-ROM

Найголовніше відмінність - це, природно, обсяг записуваної інформації. Якщо на звичайний CD-диск можна записати 650 Мб (хоча останнім часом зустрічаються болванки і на 800 Мб, але далеко не всі приводи зможуть прочитати те, що записано на такому носії), то на один DVD-диск влізе від 4,7 до 17 Гб. В DVD використовується лазер з меншою довжиною хвилі, що дозволило істотно збільшити щільність запису, а крім того, DVD має на увазі можливість двошарового запису інформації, тобто на поверхні компакт-диска знаходиться один шар, поверх якого наноситься ще один, напівпрозорий, і перший зчитується крізь другий паралельно . У самих носіях теж відмінностей більше, ніж здається на перший погляд. Через те, що щільність запису істотно зросла, а довжина хвилі стала менше, змінилися і вимоги до захисного шару - для DVD він становить 0,6 мм проти 1,2 мм у звичайних CD. Природно, що диск такої товщини буде значно більш крихким, в порівнянні з класичною болванкою. Тому ще 0,6 мм зазвичай заливаються пластиком з двох сторін, щоб вийшли ті ж 1,2 мм. Але найголовніший бонус такого захисного шару в тому, що завдяки його малому розміру на одному компакті стало можливим записувати інформацію з двох сторін, тобто подвоювати його ємність, при цьому залишаючи розміри практично незмінними.

7. Твердотільний накопичувач на основі Flash пам'яті (SSD).

Швидко зростаючий ринок портативних жорстких дисків, призначених для транспортування великих обсягів даних, привернув до себе увагу одного з

найбільших виробників вінчестерів. Компанія Western Digital оголосила про випуск відразу двох моделей пристроїв під назвою WD Passport Portable Drive. У продаж надійшли варіанти ємністю 500 Гб. Портативні пристрої WD Passport Portable Drive засновані на 2,5-дюймових HDD WD Scorpio EIDE. Вони упаковані в міцний корпус, обладнані підтримкою технології Data Lifeguard, і не потребують додаткових джерел живлення (харчування через USB). Виробник зазначає, що накопичувачі не гріються, працюють тихо і споживають мало енергії. Вони можуть бути як вмонтовані, так і зовнішні (через USB інтерфейс).

8. USB Flash Drive

Новий тип зовнішнього носія інформації для комп'ютера, що з'явився завдяки широкому розповсюдженню інтерфейсу USB (універсальної шини) і переваг мікросхем Flash пам'яті. Досить велика ємність при невеликих розмірах, енергонезалежність, висока швидкість передачі інформації, захищеність від механічних і електромагнітних впливів, можливість використання на будь-якому комп'ютері - все це дозволило USB Flash Drive замінити або успішно конкурувати з усіма існуючими раніше носіями інформації.

9. SD Memory card (виконана на основі flash пам'яти).

Компактний електронний пристрій, що використовується для зберігання цифрової інформації. Сучасні карти пам'яті виготовляються на основі флеш-пам'яті, хоча принципово можуть використовуватися й інші технології. Карти пам'яті широко використовуються в електронних пристроях, включаючи цифрові фотоапарати, мобільні телефони, ноутбуки, портативні цифрові аудіопрогравачі.

Носії інформації (вінчестери, диски, флеш-накопичувачі тощо) можуть слугувати знаряддям вчинення чи приховання злочинів або зберігати на собі сліди злочинних дій.

2. ТАКТИЧНІ ОСОБЛИВОСТІ ОТРИМАННЯ СТОРОНОЮ ОБВИНУВАЧЕННЯ ДОСТУПУ ДО ЕЛЕКТРОННИХ НОСІЇВ ІНФОРМАЦІЇ ТА ВЗЯТТЯ ЇХ ПІД КОНТРОЛЬ

Під час вилучення комп'ютерів, електронних носіїв інформації та інформації з них виникає ряд загальних проблем, пов'язаних зі специфікою технічних засобів, що вилучаються. Так необхідно брати до уваги засоби безпеки, які застосовуються злочинцями з метою знищення речових доказів. Вони, наприклад, можуть використати спеціальне обладнання, яке в критичних випадках утворює сильне магнітне поле, що стирає магнітні записи. Дуже поширена історія про хакера Кевіна Мітника, який створив у дверному отворі магнітне поле такої сили, що воно знищувало інформацію з магнітних носіїв при винесенні їх агентами ФБР з його кімнати. Тому завжди слід враховувати, що злочинець має можливість включити до складу програмного забезпечення свого комп'ютера програму, яка примусить комп'ютер періодично вимагати пароль і, якщо декілька секунд правильний пароль не буде введений, дані в комп'ютері будуть автоматично знищені. Власники комп'ютерів встановлюють інколи приховані команди, що знищують чи виконують архівацію з паролем важливої інформації.

Розглянемо таке поняття як доказова електронна інформація. У загальному вигляді доказова електронна інформація – це сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах і має значення для об'єктивного розкриття всіх обставин справи. Особливість цих доказів полягає в тому, що вони не можуть сприйматися безпосередньо, а мають бути інтерпретовані певним чином та проаналізовані за допомогою спеціальних технічних засобів та програмного забезпечення.

Дуже часто правоохоронні органи мають справу з комп'ютерами, коли розслідуються звичайні види кримінальних злочинів: крадіжка, вимагання, шантаж, торгівля наркотиками тощо. Для криміналістів теж усе більш звичним стає пошук та аналіз у комп'ютерних системах інформації, яка може бути використана як доказ. Тому, хоча законодавчі процедури та правила вилучення й оформлення доказів відрізняються в різних країнах, однаковим є те, що визнання комп'ютерних доказів судами – процес важкий і потребує впевненості в тому, що докази були виявлені та вилучені співробітником, який має певні навички та підготовку для цієї діяльності.

У ході обшуку всі електронні докази, які знаходяться у комп'ютері чи комп'ютерній системі, мають бути зібрані в такий спосіб, щоб вони потім були визнані судом. Світова практика свідчить, що досить часто під тиском представників захисту в суді електронні докази не беруться до уваги. Для того щоб гарантувати їх визнання в якості доказів, необхідно суворо дотримуватися вимог кримінально-процесуального законодавства, а також стандартизованих прийомів та методик їх вилучення. Під стандартними прийомами та методиками розуміються такі, при дотримані яких докази в електронному вигляді безумовно прив'язуються до особи чи до підприємства, організації і не викликають сумнівів у суду.

Розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій, вимагає спеціальних знань. Якщо його буде доручено некваліфікованим

особам, то це може створити серйозні проблеми. Тому існує велика потреба у спеціалізованих „комп'ютерних" підрозділах або у кваліфікованих фахівцях.

Комп'ютери, що входять до складу інформаційної системи – це складне обладнання, яке потребує обережного поводження з ним під час роботи на місці події. Слід пам'ятати, що комп'ютери можуть містити в собі велику кількість даних, які належать сторонній особі або організації (наприклад, можуть бути об'єктом інтелектуальної власності). Тому обережність при поводженні з комп'ютером необхідна як з точки зору збереження важливої доказової інформації, так і з точки зору відвернення матеріальних збитків та збереження власності. Саме тому необхідно, щоб з комп'ютером на місці події мала справу дійсно кваліфікована особа.

Справедливим є твердження про те, що не існує такого поняття, як універсальний комп'ютерний експерт. В якості комп'ютерного експерта можливо залучати осіб з наступними спеціальностями: а) комп'ютерні науки та інформаційні технології б) інженер з технічного захисту інформації в) комп'ютерна інженерія г) системна інженерія д) програмна інженерія е) мережеві технології та системне адміністрування ж) аналітика комп'ютерних систем. Тому, збираючись на місце події, важливо з'ясувати, з якою технікою і з якою операційною системою доведеться мати справу. Перше, що необхідно встановити, – це тип операційної системи. Не всі комп'ютерні системи однаково розповсюджені, і тут теж можуть виникнути певні проблеми. Спеціаліст з операційної системи Windows може не володіти необхідними знаннями для управління машиною з іншою операційною системою, наприклад, Unix, Linux, OS/2, MacOS і інші. Але, незважаючи на певні труднощі, фахівець має визначитись, може він особисто працювати з даною операційною системою чи слід залучати іншого фахівця в цій галузі. В останньому випадку дії з обладнанням залучених осіб мають ретельно фіксуватися.

Найбільш простий випадок – коли йдеться про окремий комп'ютер. Але комп'ютери можуть бути пов'язані між собою в комп'ютерні мережі (наприклад, локальні), котрі, у свою чергу, можуть бути об'єднані через глобальні комп'ютерні мережі. Тому не виключена ситуація, що певна важлива інформація (яка може бути використана як доказ) буде передана через мережу в інше місце, не виключено, що й за кордон, а іноді важлива для кримінальної справи інформація може знаходитись на території кількох країн. У такому разі необхідно використати всі можливості (документацію, допити осіб, технічні можливості системи) для встановлення місцезнаходження іншої комп'ютерної системи, куди була передана інформація. Як тільки це буде зроблено, потрібно терміново надіслати запит (з дотриманням встановлених вимог) про надання допомоги (або правової допомоги, якщо така необхідна для виконання поставлених у запиті питань) до компетентного правоохоронного органу відповідної країни (по встановленим офіційним каналам, наприклад, Інтерпол). Саме на цьому етапі виникають найбільші труднощі в організації роботи щодо розслідування злочину, який вчиняється за допомогою комп'ютерних технологій, та кримінального переслідування злочинців.

Сучасні комп'ютерні технології дуже розвинуті та складні, ось чому існує небезпека, що слідство може втратити важливі докази, якщо особи, що ведуть його,

не будуть достатньо підготовлені для цього. Особливу цінність при розслідуванні в комп'ютерних мережах мають так звані „логи" – інформація, що міститься в логфайлах (текстова інформація). За допомогою цієї інформації можна, наприклад, встановити рахунок користувача, його ідентифікатор, час трансакції, мережну адресу, телефонний номер, а також те, які події відбувалися в системі – що було знищено, змінено, скопійовано, які ресурси були задіяні для цього.

Логи можуть збиратися в комп'ютерних системах на різному рівні: в операційній системі, у спеціально встановленому програмному забезпеченні (наприклад, програмному аудиті безпеки), в окремих модулях баз даних і навіть у деяких прикладних програмах. Фізично ця інформація може знаходитися в різних місцях – від робочої станції і серверу мережі до віддаленого серверу.

До підготовки будь-якої дії, пов'язаної з розслідуванням злочину, що вчиняється за допомогою комп'ютерних технологій (особливо вилучення інформації і комп'ютерного обладнання), доцільно з самого початку залучити фахівця з галузі інформаційних технологій. До початку операції необхідно також мати певну інформацію щодо операційних систем, периферійних пристроїв, засобів зв'язку та будь-які інші відомості про комп'ютерний комплекс, яка є об'єктом розслідування.

Отримана інформація має бути терміново доведена до фахівця, щоб він мав час для встановлення при потребі додаткового контакту з іншими фахівцями (або його залучення.

Якщо систему фізично неможливо вилучити й перемістити в інше місце, виникає необхідність копіювати інформацію на зовнішні пристрої зберігання даних. При можливості зробити повні копії окремих носіїв інформації за допомогою завантажувального зовнішнього пристрою та програми для створення образів жорстких чи твердотільних дисків, зробити копії окремих файлів.

Магнітні носії, на які передбачається копіювати інформацію, мають бути підготовлені (необхідно впевнитись, що на них нема ніякої інформації). Носії потрібно зберігати у спеціальних упаковках або загортати у чистий папір (не слід використовувати звичайні поліетиленові пакети). Слід пам'ятати, що інформація може бути зіпсована вологістю, температурним впливом або електростатичними (магнітними) полями.

Під час транспортування комп'ютерного обладнання слід поводитися з ним обережно, оскільки інформація на жорсткому диску може бути пошкоджена під час транспортування. Для транспортування великих комп'ютерних систем слід підготувати транспорт та спеціальні упаковки.

Прибувши на місце події (обшуку), необхідно насамперед „заморозити" ситуацію: вивести всіх осіб із зони доступу до обладнання, забезпечити неможливість втручання до системи через лінії зв'язку. Не дозволяти нічого змінювати в роботі системи. Система може бути дуже складною, тому, чітко не розібравшись у її конфігурації, не слід приймати жодного рішення.

Окрема увага має приділятися підозрюваній особі, адже можливо, що нею передбачені засоби знищення інформації шляхом натиснення на комп'ютері однієї лише клавіші. Бажано, щоб підозрюваний був присутній при огляді, оскільки саме він може надати найбільш важливу інформацію про систему – паролі, коди доступу,

перелік інстальованих програм та місцезнаходження окремих директорій (у тому числі прихованих). Причому його не слід допускати до комп'ютерного обладнання, щоб запобігти спробам знищення комп'ютерних доказів.

Після ретельного обстеження комп'ютерного обладнання робиться опис програмної та апаратної складової комп'ютерів. Під час опису комп'ютерів можливо використовувати наступні програмні продукти: AIDA64, Everest. Також можливо використовувати вбудовану утиліту «відомості про систему», для чого в вікні програми «виконати» (запуск виконується комбінацією клавіш **win + r**) набираємо **msinfo32** та тиснемо на кнопці **Enter**. Відомості про апаратні та програмні компоненти комп'ютерів заносяться до протоколу огляду комп'ютерної техніки та завіряться двома свідками. Документ з описом комп'ютера бажано зберігати разом з вилученою технікою. Корпус повинен бути опечатаний. Печатка завірена особою-ініціатором проведення виїмки та підписами свідків. Опечатування проводити у містах стику основного корпусу комп'ютера та бокових знімаючих кришках. Опечатувати необхідно також передню частину комп'ютера.

Доцільно також зробити оглядові та детальні фотографії місця події, при можливості провести аудіо- та відеозапис. Треба враховувати, що окремі компоненти системи можуть знаходитися в інших приміщеннях і навіть будівлях або бути добре прихованими. Схованки можуть бути обладнані в стінах будівлі, стелях, на горищах тощо.

Якщо це можливо, всі дослідження необхідно проводити за участю фахівців спеціальних підрозділів або в судових лабораторіях. Це запобігає випадковим помилкам та забезпечує цілісність вилученої доказової інформації. Всі операції, які здійснюються з системою, мають ретельно фіксуватися.

Перевезення й зберігання комп'ютерної техніки має здійснюватися в умовах, що виключають її пошкодження. При вилученні й перевезенні комп'ютерів не можна ставити їх один на один, розміщувати на них будь-які інші предмети.

Також слід дотримуватися чітких правил поводження з комп'ютерним обладнанням (саме тоді повною мірою перевіряється ступінь підготовленості працівників правоохоронних органів).

1. На будь-якому етапі роботи з комп'ютерним обладнанням та доказами комп'ютерного походження, якщо немає впевненості у власних силах, слід дочекатись прибуття експерта або забезпечити участь фахівця.

2. Якщо участь експерта або фахівця неможлива, потрібно дотримуватися певних вимог і послідовності дій (їх невиконання може призвести до втрати інформації або її доказової сили):

2.1. При охороні комп'ютера не можна дозволяти неспеціалісту включати комп'ютер, торкатися клавіатури, змінювати положення комп'ютера або пов'язаного з ним обладнання. Не можна рухати комп'ютер, якщо він підключений. Не можна вимикати принтер до закінчення друкування;

2.3. Треба зафіксувати з'єднання кожної частини комп'ютера та периферійних пристроїв, мережевого підключення і сфотографувати його (див. мал. № 1).

Мал. № 1

При роз'єднанні обладнання слід позначити (маркувати) обидва кінці кабелів. Необхідно сфотографувати як саме комп'ютерне обладнання, так і загальний вигляд кімнати, де знаходилась апаратура, і її підключення.

2.4. Слід записати в повному обсязі інформацію, яка є на екрані (екранах), і по можливості зафіксувати її фотографічним способом;

2.5. Слід забезпечити охорону комп'ютерної системи, після чого з'ясувати:

а) Чи підключений комп'ютер до локальної чи глобальної мережі, яким чином підключений (дротове з'єднання, бездротове з'єднання – WiFi, 3G, 4G модеми, інфрачервоне з'єднання.

б) Де знаходиться джерело струму (батареї, джерело безперервного живлення та інше);

в) Необхідно закрити активні програми, після чого можна вимкнути монітор, комп'ютер та відключити напругу;

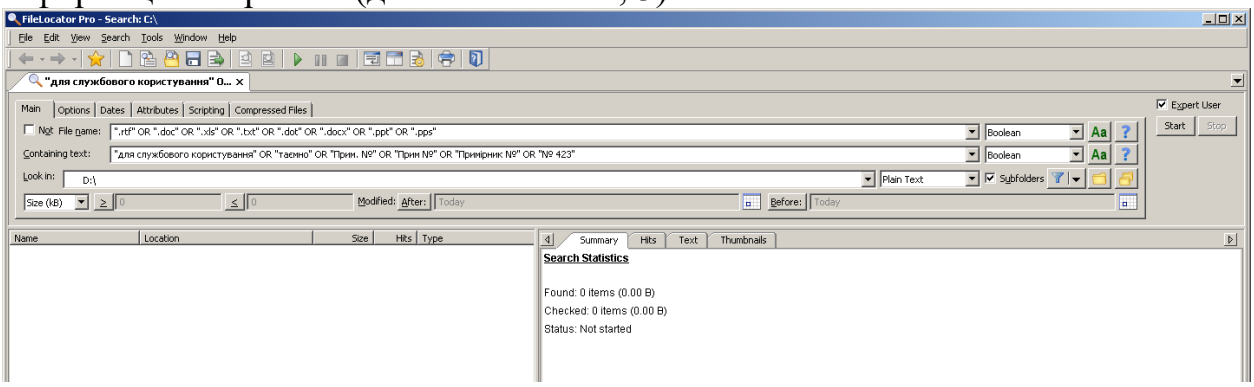
2.6. Від'єднати шнури струму, клавіатури, монітора, модема та принтера;

2.7. При вилученні жорсткого чи твердотільного диска його слід покласти в окремий пакет, опечатати та зазначити номер печатки. Якщо це портативний комп'ютер, то треба вкласти його до конверта, а потім до опечатаного пакета. Не слід самостійно відкривати портативний комп'ютер.

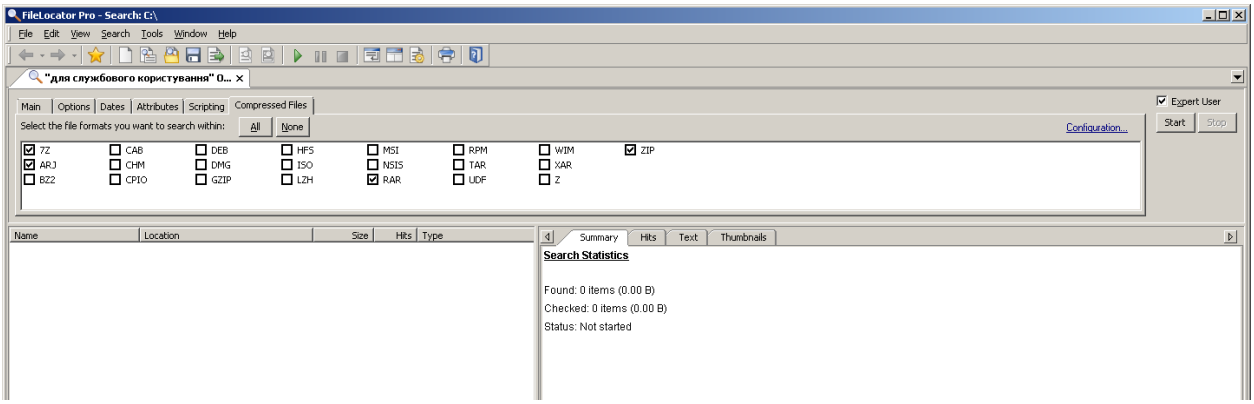
Слід перевірити, чи були вилучені такі речі:

- монітор;
- клавіатура;
- принтер;
- документація та інструкції по експлуатації;
- адаптери до портативних комп'ютерів;
- помічені кабелі та розмикаючи пристрої;
- зразки фірмових та інших бланків комп'ютерного походження;
- роздруковані комп'ютерні тексти, які можуть мати відношення до злочину (вони могли бути знищені на комп'ютері);
- функціональні обов'язки користувачів, адміністратора системи та інформаційної безпеки;
- іншу організаційно-технічну документацію, яка відображає політику безпеки даної установи.

При пошуці доказового медіаконтенту без вилучення комп’ютерної техніки можливо використовувати різноманітні програмні продукти для проведення пошуку. В якості програми-пошукача можливо використовувати програми під назвою: FileLocator Pro, Searchmyfiles, Lookdisk. Програма під назвою FileLocator Pro дозволяє шукати інформацію всередині файлів, пидтримує логічні оператори (наприклад: "для службового користування" **OR** "таємно" **OR** "Прим. №"), шукає інформацію в архівах (дивись мал. №2, 3).



Мал. 2



Мал. 3

Пошук медіаконтенту бажано проводити з правами адміністратора, так як адміністратор операційної системи може заборонити юзеру доступ до де яких файлів чи каталогів і якщо ми будемо працювати з правами юзера доступ до заборонених файлів та каталогів буде відсутній. Пропонується у даному випадку загрузитись з зовнішнього завантажувального носія інформації і провести пошук з зовнішньої операційної системи чи скинути або змінити пароль адміністратора. Дані операційні системи звуться LiveCD/USB. Пропонується використати LiveUSB під назвою Microsoft DaRT. Вбудований інструмент **Locksmith** дозволяє скинути чи змінити пароль адміністратора на локальном комп’ютері. Після чого перезавантажити комп’ютер та зайти в операційну систему з правами адміністратора.

3. ПОШУК В ІНТЕРНЕТ-ПРОСТОРІ ВЛАСНИКА, ВОЛОДІЛЬЦЯ, УТРИМУВАЧА МЕДІЙНОГО КОНТЕНТУ

Пошук за IP адресою.

IP адреса це неповторна, унікальна адреса комп'ютера або іншого пристрою, що підключено до мережі інтернет або локальної мережі. Іншими словами, під час поточного з'єднання, користувачеві мережі інтернет належить унікальна комбінація цифр, якої більше немає ні у одного користувача в світі. Власне ця унікальна комбінація цифр і є IP адресою. IP адрес може бути статичним або динамічним і призначається провайдером. Статична IP адрес - постійний, і не змінюється при кожному підключенні до мережі інтернет. Динамічний IP адрес - може змінюватися при підключенні до мережі інтернет (змінюється остання цифра в IP-адресі). Кілька комп'ютерів можуть мати одну IP адресу, якщо підключені через один сервер, і матимуть IP адреса ідентичні до серверного.

Управляє простором IP адрес американська некомерційна організація IANA - «Адміністрація адресного простору Інтернет». Вона виділяє блоки IP-адрес регіональним реєстраторам. Вони в свою чергу, ділять блоки адрес по великим провайдерам, які в свою чергу поділяють адреси серед дочірніх провайдерів і так далі, до тих пір, поки, одиночна IP адреса не видається вам, коли ви заходите в Інтернет. Отже, чи можна знайти конкретну людину за IP адресою? Теоретично в більшості випадків це можливо. На практиці ж, пошук людини за IP адресою - досить складне завдання, через низку різних причин. Наприклад, якщо IP адреса динамічна, необхідно визначити, кому з користувачів в час, який вас цікавить, була призначена дана IP адреса, тобто потрібно отримати доступ до логів і бази користувачів інтернет-провайдера. До речі, на сервері провайдера ведеться запис всіх адрес, які відвідував користувач, яку інформацію і з яких сайтів отримує, куди що відправляє, що шукав тощо. Далі, може виявитися, що IP адреса видавався мобільному пристрою, абонент якого не контрактник або воно вимкнене, викинуто і т.д. Ну і, зрештою, наявна IP адреса може належати до проксі-сервера, або декільком проксі-серверам. У даному випадку отримати доступ до їх логів буде практично не можливо, як власне і знайти людину за IP адресою.

З вище написаного, можна зробити висновок, можливо визначити приналежність IP адреси до країни і міста, тобто визначити провайдера інтернет-користувача!!!, але не знайти людину по IP адресу. Це можна зробити за допомогою Гео-IP - сервісів для визначення географічного розташування IP адреси або хоста. У втім і це залежить від точності внесеної провайдерами інформації про свої мережи.

Таким чином, в ряді випадків 100% точність визначення місця розташування IP адреси можлива тільки до рівня країни. Для подальшого пошуку людини по IP адресу необхідно звернутися до його інтернет-провайдера. Інтернет-провайдери ж, як правило, не надають інформацію про власника IP адреса, оскільки це порушує права людини і відповідно закон. А На законних підставах така інформація надається лише працівникам правоохоронних органів і тільки у встановленому законом порядку.

Пошук суб'єкта за допомогою сервіса Whois у відкритих джерелах.

WHOIS (від англ. Who is - «хто такий?") - мережевий протокол прикладного рівня, що базується на протоколі TCP (порт 43). WHOIS використовується для отримання інформації про доменне ім'я. Інформація, що видається включає в себе ім'я сервера, ім'я власника та адресу з телефоном. Тут можна дізнатися дату реєстрації та її закінчення, а також реєстратора, де домен був зареєстрований. Наявність служби WHOIS повинно розчарувати тих, хто сподівався на повну анонімність в інтернеті. Навпаки, тут залишаються і фіксуються всі сліди, що легко піддаються виявленню та аналізу. Основну частину їх і видає інтерфейс WHOIS. Крім всього іншого сервіс WHOIS показує дані про IP-адресу.

Сервіс WHOIS володіє базою даних, що включає всіх реєстраторів доменів. У базу даних входять всі існуючі доменні імена. Програма працює за звичайним принципом: отримавши запит у вигляді доменного імені, вона просіює базу даних і видає результат. Дані про домени, інформація про IP-адреси, їх приналежність до мереж, інформація про реальні персони або організаціях - всі ці відомості можуть знадобитися для пошуку правопорушника у мережі Інтернет.

Загалом механізм пошуку порушника авторських прав в мережі Інтернет може виглядати наступним чином:

1. За допомогою пошукових систем (Google, Meta, Yandex т.д.) найти піратський ресурс який розповсюджує заборонений контент на території України.
2. За допомогою сервіса WHOIS на сайті 2ip.ua визначити всю можливу інформацію по даному ресурсу, тобто де находиться даний сайт (в якій країні), хто надає йому площадку для розміщення сайту (адреса, сайт, телефон тостера), коли зареєстроване домене ім'я хто реєстратор та його дані.
3. Підготував офіційне звернення на ці організації можливо отримати IP адресу користувача або адміністратора сайту та за допомогою провайдера з'ясувати його адресу IP.

Можливо спробувати ще більш простіший метод. Переважна більшість сайтів з піратським контентом розміщують рекламу для монетизації сайту. Спроба зв'язатись з адміністратором сайту та пропозиція йому щодо розміщення своєї реклами дає потенційну можливість отримати реквізити банківської картки або розрахунковий рахунок для оплати реклами або інший спосіб оплати, за яким значно легше встановити власника.

Приблизний алгоритм відновлення знищеного контенту за допомогою програмних засобів.

З метою приховування протиправної діяльності поширеною є ситуація, що пов'язана із знищенням медійного контенту. Тому, на етапі розслідування виникає необхідність у відновленні такої інформації.

В більшості випадків видалена інформація може бути відновлена за допомогою програмних засобів. Часто їх застосування не представляє більшої складності, ніж використання типових програмних засобів обробки комп'ютерної інформації, призначених для вирішення повсякденних завдань: запису інформації на оптичний диск, архівації даних, роботи з файловими менеджерами і тому подібне.

Основні аспекти відновлення комп'ютерних даних за допомогою програмних засобів нами приведені нижче.

Програми, призначені для відновлення даних, працюють в цілому за єдиним алгоритмом, що складається з наступних основних дій.

1. Сканування жорстких дисків з метою визначення конфігурації логічних дисків.

2. Сканування певного розділу з метою пошуку видалених чи пошкоджених елементів даних.

3. Запис відібраних даних за новою адресою.

Програми часто включають в список таких, що підлягають відновленню, не тільки видалені користувачем файли, але і файли з «частковими» пошкодженнями, зокрема:

- з некоректним штампом дати і/або часу (Invalid Dates); .
- з некоректним набором атрибутів (Invalid Attributes);
- з неправильно вказаним розміром (Invalid File Size);
- у найменуванні яких присутні неприпустимі символи (Invalid characters).

При виборі програми для відновлення комп’ютерної інформації необхідно враховувати:

- типи носіїв, які підтримує програма;
- файлові системи і формати запису (для носіїв типу CD/DVD), які підтримує програма;
- уміння опрацьовувати довгі імена файлів та кирилицю;
- можливість запуску із зовнішнього носія, без інсталяції на жорсткий диск;
- здатність працювати на рівні логічних дисків і розділів, а також на фізичному рівні;
- уміння відшукувати логічні диски, втрачені унаслідок руйнування таблиці розділів або проведення реконфігурування диска;
- здатність враховувати формат відновлюваних файлів.

Крім того, для деяких типів файлів існують спеціалізовані засоби відновлення. Наприклад, пошкоджений файл архіву у форматі RAR слід спочатку спробувати відновити засобами архіватора WINRAR, і лише потім шукати інші способи його відновлення.

На момент проведення даного дослідження у якості найбільш перспективних нами виділені наступні програмні продукти, які дозволяють успішно відновлювати видалену інформацію, – Drive Rescue і EasyRecovery Pro. На прикладі їх алгоритму роботи ми пропонуємо розглянути основні етапи відновлення даних.

Програма Drive Rescue

Після запуску програми на екрані з'являється діалогове вікно з пропозицією обрати мову інтерфейсу. Потім необхідно вибрати один з трьох основних варіантів роботи, натиснувши на відповідну кнопку (мал. 1.)

- Recover deleted files (Відновлення видалених файлів) — пошук і відновлення файлів, видалених стандартним засобами Windows (минувши «корзину» або в результаті очищення останньої);

- Find lost data (Пошук втрачених даних) — пошук і відновлення файлів і каталогів, що стали недоступними в результаті яких-небудь некоректних дій користувача або помилок системи, а також в результаті «швидкого» форматування;

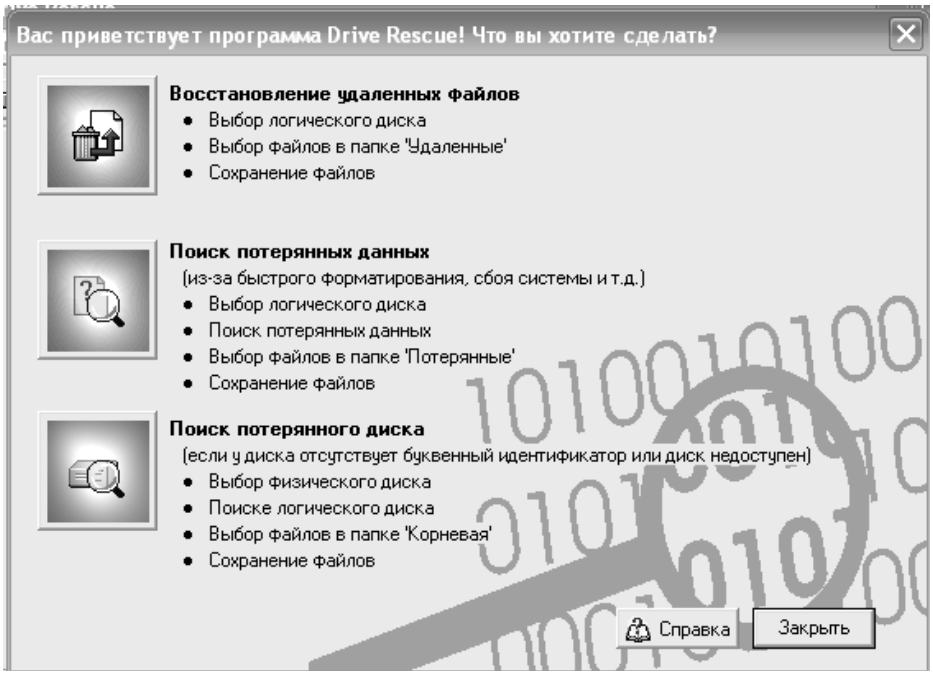
- Find lost drive (Пошук втрачених пристроїв) — пошук і відновлення логічних дисків, що стали недоступними в результаті яких-небудь некоректних дій користувача чи помилок системи (наприклад, в результаті псування таблиці розділів).

У будь-якому з трьох випадків Drive Rescue почне роботу зі сканування пристроїв (жорстких дисків, FDD, дисководів Jazz і Zip, а також накопичувачів типу Flash Card або SmartMedia) і виведе результати сканування в діалоговому вікні Select Drive (вибір пристрою) на вкладці Logical Drive (Логічний пристрій). Правда, результати сканування в кожному з трьох випадків можуть бути представлені різним чином (докладніше ці відмінності будуть розглянуті нижче).

Порядок подальших дій з відновлення даних залежить від конкретної ситуації. Найбільш типові випадки будуть розглянуті в подальших підрозділах. Можна відмовитися від запропонованого набору з трьох основних процедур, натиснувши кнопку Welcome to Drive Rescue на кнопці Close (Закрити) (див. мал. 1).

В цьому випадку ми отримаємо безпосередній доступ до основного вікна програми. Крім виклику довідки або отримання технічної підтримки через Інтернет можна скористатися однією з наступних команд:

мал. 1



Список логічних дисків, виявлених Drive Rescue

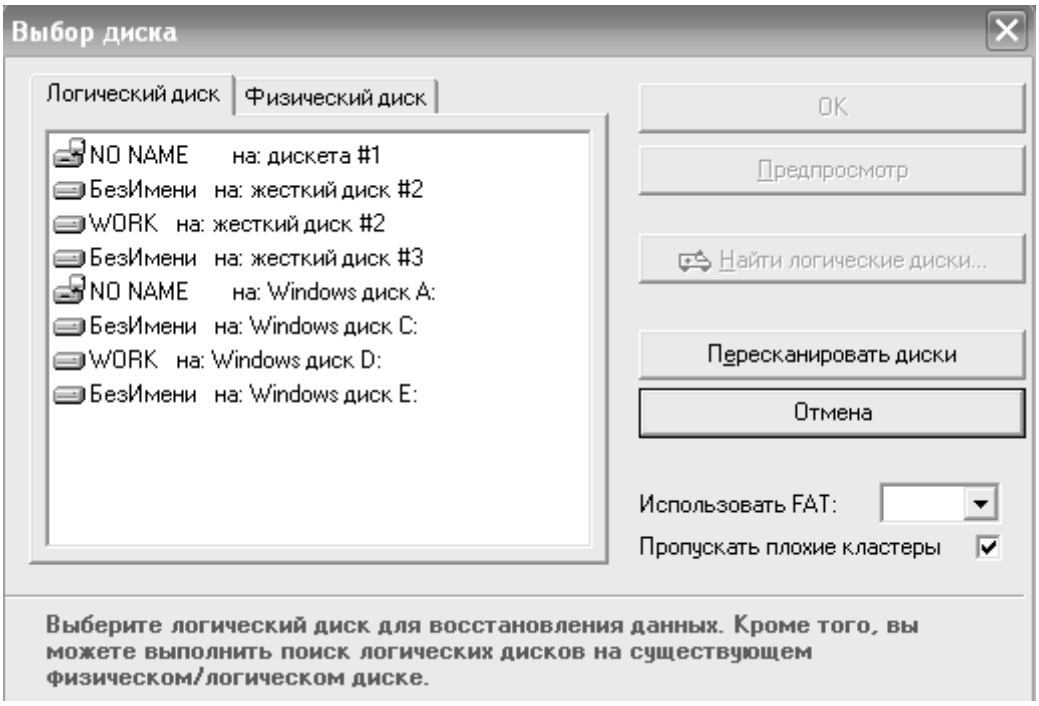
Object > Drive (Об'єкт > Пристрій) — ініціює процес сканування пристроїв, аналогічний тому, який може бути запущений з діалогового вікна Welcome to Drive Rescue;

Object > Options (Об'єкт > Параметри) — виклик вікна настройки параметрів роботи Drive Rescue;

Info > System Info (Відомості > Відомості про систему) — виклик вікна, що містить відомості про апаратну і програмну конфігурацію системи.

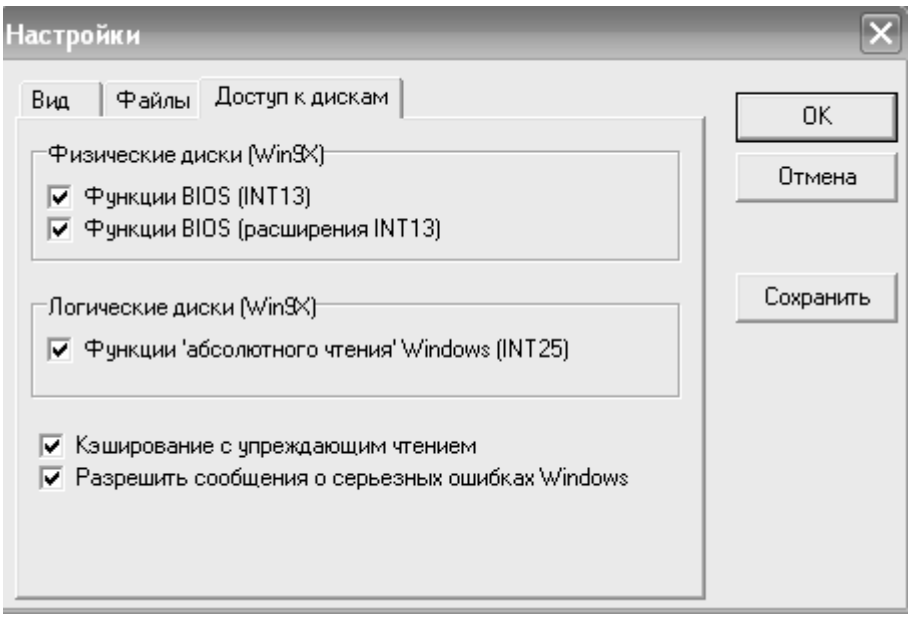
З погляду роботи Drive Rescue з відновлення даних найбільший інтерес

мал. 2.



представляє група параметрів, розміщених на вкладці Drive access (Доступні пристрої). Два прапорці з групи Physical drives (Фізичні диски) визначають, які засоби повинен використовувати Drive Rescue для прочитування даних з диска: стандартний сервіс BIOS (INT13), що використовує адресацію CHS, або розширений сервіс (INT13 Extension), який забезпечує повну підтримку LBA (мал. 3).

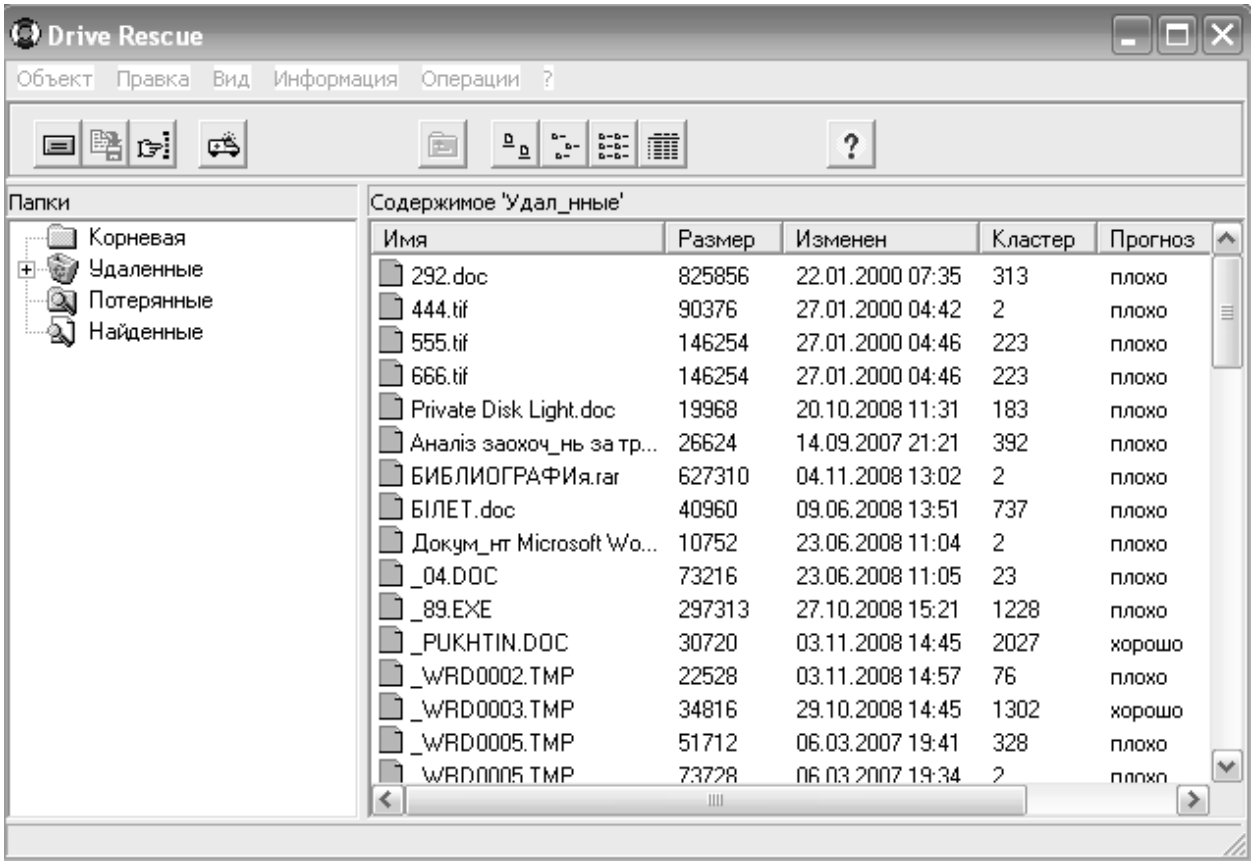
мал. 3.



Відновлення видалених файлів і каталогів

Щоб ініціювати процедуру відновлення видалених файлів і/або каталогів, натисніть у вікні Welcome to Drive Rescue на кнопку Recover deleted files. Після завершення сканування пристроїв на екрані з'явиться список логічних дисків, виявлених Drive Rescue.

Виберіть диск, на якому був видалений файл (каталог), і натисніть на розташованій праворуч від списку кнопці «ОК». В основному вікні програми будуть представлені результати аналізу диска (мал. 4).



мал. 4.

У лівій частині вікна відображається дерево каталогів, що містить 4 основних гілки:

■ Root (Кореневий) — перелік вкладених каталогів і файлів, зареєстрованих в кореневому каталозі диска;

■ Deleted (Видалені) — перелік каталогів і файлів, помічених як видалені;

■ Lost (Втрачені) — список «втрачених» файлів і каталогів;

■ Searched (Знайдені) — список знайдених файлів; список формується в результаті виконання функції пошуку, про яку буде розказано нижче.

Щоб побачити вміст будь-якої гілки, натисніть на її значку мишею. Вміст відображається в правій частині вікна. При пошуку видалених файлів і каталогів Drive Rescue заповнює тільки гілки Root і Deleted.

Видалені об'єкти відмічаються в лівому і правому списках зеленим кольором. У правому списку, реалізованому у вигляді таблиці, ви можете отримати наступну інформацію про видалений об'єкт:

■ Name (Ім'я) — ім'я об'єкту; у імені видаленого об'єкту можуть бути присутніми символи підкреслення, замінюючи втрачені символи початкового імені; в деяких випадках в списку можуть опинитися декілька однойменних файлів (наприклад, різні версії одного файлу); якщо потрібно відновити всі такі файли, заздалегідь їх потрібно перейменувати, вибравши в контекстному меню команду Rename (Перейменувати);

■ Size (Розмір) — розмір файлу в байтах; потрібно мати на увазі, що розмір зіпсованого файлу може не відповідати розміру файлу до видалення; іноді розмір файлу потрібно скоректувати вручну;

■ Date (Дата) — дата останньої зміни файлу;

■ Cluster (Кластер) — номер першого кластера файлу (каталогу); стовпець використовується при роботі з файловою системою FAT; для файлової системи NTFS замість нього використовується стовпець MFT Entry (Вхід MFT);

■ Condition (Стан) — стан видаленого файлу (каталогу) має такі можливі значення:

□ poor (поганий) — файл не може бути відновлений; проте така категорична оцінка не завжди справедлива: іноді файл, помічений як poor, все-таки вдається відновити;

□ fair (посередній) — файл може бути відновлений частково;

□ good (хороший) — файл може бути відновлений без втрат;

□ unknown (невідомо) — стан визначити не вдалося;

Type (Тип) — тип файлу відповідно до параметрів операційної системи.

Для відновлення видаленого об'єкту слід виконати наступні дії.

1. Натисніть на його значку правою клавішею миші і в контекстному меню виберіть команду Save to (Зберегти в).

2. У додатковому вікні (мал. 5):

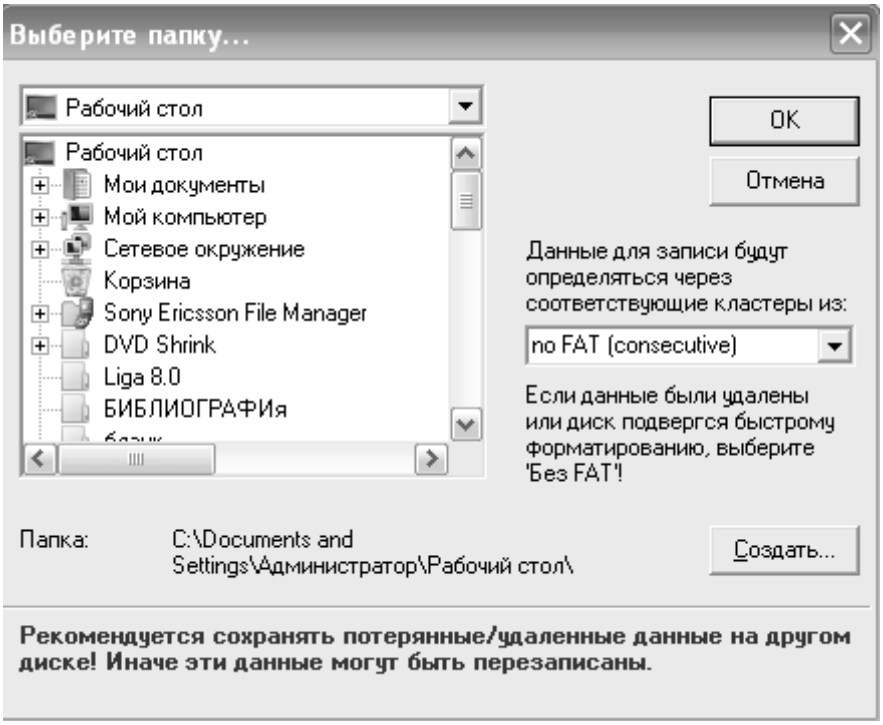
1) вкажіть диск і каталог, куди слід переписати відновлюваний об'єкт;

2) у списку, що розкривається, виберіть пункт no FAT (consecutive) (Не використовувати FAT, переглядати послідовно);

3) натисніть на кнопці ОК.

Потрібно пам'ятати, що відновлюваний об'єкт не можна записувати на той самий диск, на якому він розташований. Це може привести до пошкодження розміщених на цьому диску як самого об'єкту, так і інших об'єктів, що підлягають відновленню.

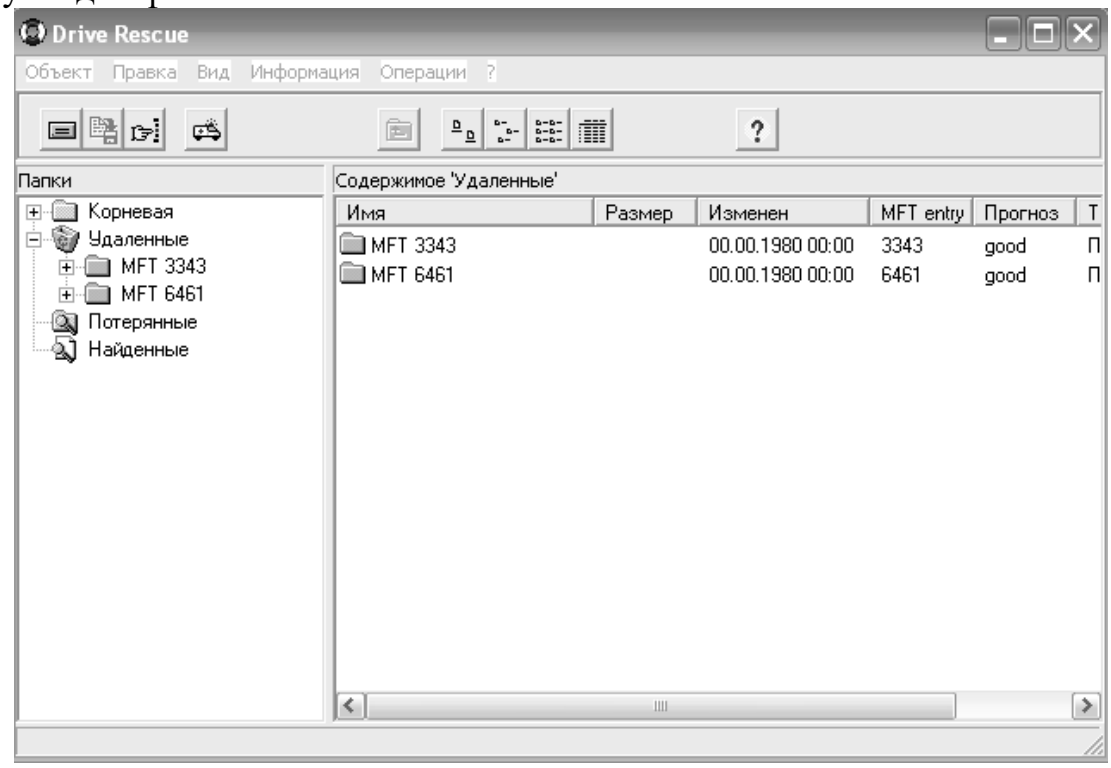
мал. 5



Після того, як видалений об'єкт був відновлений (записаний за новою адресою), він автоматично віддаляється з гілки Deleted.

Якщо пошук видалених файлів проводиться на диску з файловою системою NTFS, то результати пошуку виглядатимуть декілька інакше: знайдені об'єкти ідентифікуються за номерами записів (входів) до таблиці MFT (мал. 6). Відповідно в правому списку для знайдених об'єктів також указується не номер першого кластера, а номер запису в MFT.

В цілому, технологія відновлення даних на NTFS-диску аналогічна технології, розглянутій для файлової системи FAT.



мал. 6

Відновлення видалених файлів і каталогів

Виконання даної процедури може декілька розрізнятися залежно від причини втрати даних. У будь-якому випадку процес пошуку потрібно починати зі сканування наявних пристроїв. У сформованому списку виберіть диск, на якому розташовані видалені дані, і натисніть на кнопку ОК.

Для продовження пошуку виконаєте наступні дії.

1. У меню Tools (Сервіс) основного вікна програми виберіть команду Find lost data (Пошук втрачених даних).

2. У вікні Select cluster range (Вибір діапазону кластерів) за допомогою регуляторів необхідно встановити діапазон кластерів, в якому слід проводити пошук (якщо необхідна інформація відсутня, краще провести його по всьому доступному дисковому просторові).

Стан процесу пошуку і поточні результати відображаються в додатковому вікні, в якому роздільно виводяться число втрачених каталогів і число втрачених файлів. Після завершення сканування всі знайдені об'єкти поміщаються в гілку Lost основного вікна.

У лівому списку (Folders) представлені втрачені каталоги, що іменуються номерами їх перших кластерів.

У правому списку відображаються елементи, на які є посилання у вибраному каталозі.

Якщо ви не можете визначити за номером кластера відомості про те, який саме каталог вас цікавить, проглянете послідовно вміст всіх знайдених каталогів, вибираючи їх по черзі в лівому списку; знайшовши потрібний каталог, запам'ятайте або запишіть номер відповідного кластера.

Щоб відновити каталог, виконаєте наступні дії.

1. Натисніть в лівому списку на значку гілки Lost; при цьому всі втрачені каталоги (впорядковані за номерами кластерів) будуть показані в правому списку.

2. Перейменуйте каталог, давши йому осмислене ім'я; для цього натисніть правою клавішею миші в правому списку на значку каталогу (з номером записаного вами кластера), що цікавить, після чого в контекстному меню виберіть команду Rename і відредагуйте ім'я каталогу.

3. Натисніть в правому списку на значку каталогу правою клавішею миші і в контекстному меню виберіть команду Save to.

4. У додатковому вікні (див. мал. 5) вкажіть диск і каталог, куди слід переписати відновлюваний каталог. У списку, що розкривається, виберіть номер копії таблиці FAT, в якій ви більше упевнені (за умовчанням використовується перша, основна копія).

5. Натисніть на кнопку «ОК».

Щоб відновити конкретний файл (або вкладений каталог) в каталозі, що цікавить, слід виконати наступне.

1. У лівому списку натисніть на позначку каталога.

2. У правому списку перейменуйте, якщо потрібно, відновлюваний файл.

3. Натисніть правою клавішею миші на значок файлу і в контекстному меню

виберіть команду Save to.

4. У додатковому вікні (див. мал. 5) вкажіть диск і каталог, куди слід переписати відновлюваний файл. У списку, що розкривається, виберіть номер копії таблиці FAT, в якій ви більше упевнені, і натисніть на кнопці ОК.

Для деяких видалених файлів (наприклад, пошкоджених вірусом) в списку файлів може бути вказана нульова довжина. Існує вірогідність, що такий файл цілком «дієздатний», але недоступний для коректної роботи. Для його відновлення виконаєте наступні дії.

5. Натисніть правою клавішею миші на значку файлу і в контекстному меню виберіть команду Properties (властивості).

6. У додатковому вікні в полі Size (розмір) введіть відповідне значення (із запасом).

7. Збережіть файл описаним вище способом за новою адресою.

8. Відкрийте файл за допомогою асоційованої з ним програми і збережіть його за допомогою команди Зберегти як (Save as).

Якщо Drive Rescue не може визначити розмір знайденого файлу, він встановлює для нього розмір, вказаний в параметрах Drive Rescue, на вкладці Files (Файли) в полі Default file size (Розмір файлу за умовчанням).

Програма Easy Recovery Pro

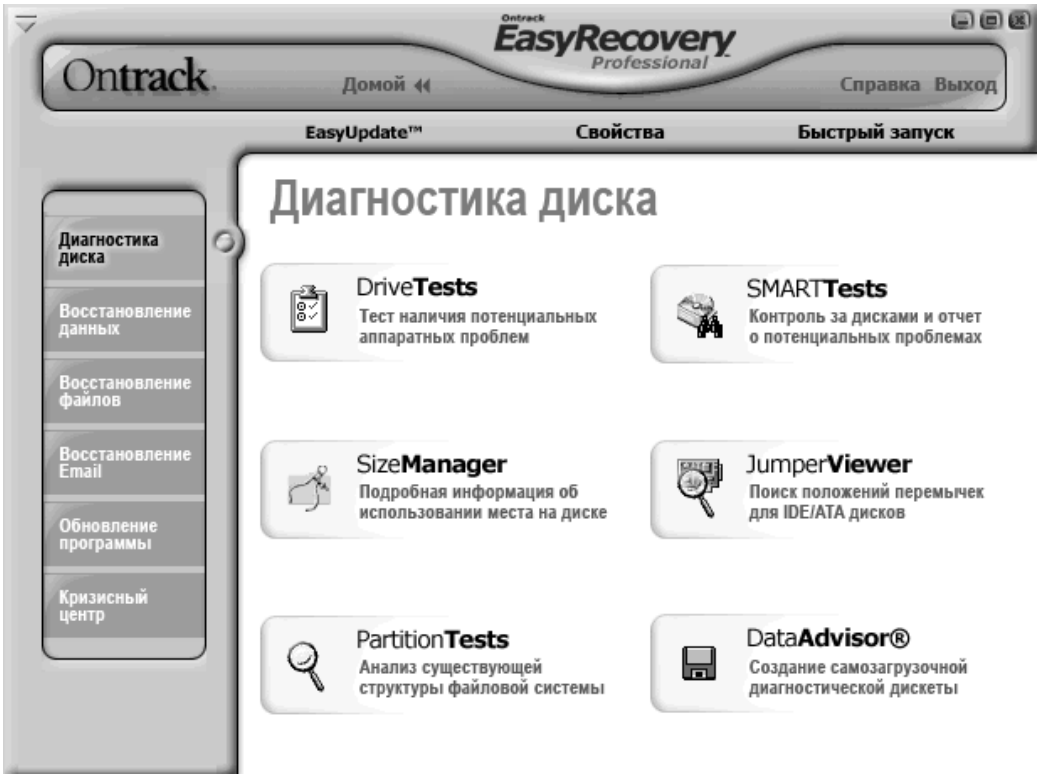
Інтерфейс Easy Recovery Pro реалізований так, щоб максимально полегшити користувачам доступ до основних функцій програми. Тому і знайомство з можливостями Easy Recovery зручно сумістити з описом інтерфейсу. Після завантаження програми на екрані з'являється вікно, в лівій частині якого розміщено меню у вигляді кнопок, що забезпечують доступ до чотирьох категорій функцій, а також до двох додаткових сервісів (мал. 7).

- Disk Diagnostics (Діагностика диска) — утиліти для перевірки фізичних параметрів диска і цілісності файлової системи;
- Data Recovery (Відновлення даних) — утиліти для пошуку і відновлення видалених і пошкоджених даних;
- File Repair (Відновлення файлів) — спеціалізовані утиліти для відновлення файлів, створених додатками програми MS Office (окрім Outlook), а також ZIP-архівів;

мал. 7

- Email Repair (Відновлення файлів електронної пошти) спеціалізована утиліта для відновлення файлів Outlook;
- Software Updates (Оновлення програми) — сервісні функції, що дозволяють отримувати інформацію і виконувати оновлення ліцензійної версії Easy Recovery через Інтернет;
- Crisis Center (Кризовий центр) — набір функцій, що забезпечують доступ до сервісних веб-служб компанії Ontrack.

Щоб отримати доступ до конкретної функції з тієї або іншої категорії, досить натиснути на відповідній кнопці меню і потім вибрати потрібну функцію в правій частині вікна; наприклад, на мал. 8 показано меню утиліт діагностування дисків.



мал. 8

Коротка характеристика утиліт, що входять до складу Easy Recovery Pro

- Утиліта DriveTests дозволяє перевіряти фізичний стан дисків. Використовувані в ній варіанти тестування засновані на читанні записаних даних і дозволяють оцінити стабільність фізичних параметрів жорсткого диска. DriveTests включає два види тестів:
- Quick Diagnostic Test (Швидкий діагностичний тест) — виконується протягом 90 секунд і забезпечує 90-процентну достовірність результатів тестування; його суть полягає в читанні секторів, вибраних випадковим чином, але з урахуванням геометрії диска; за наслідками тестування видається одне з двох повідомлень: Pass (пройдений) або Fail (помилка); тест завершується при виявленні першого ж збійного сектора;
- Full Diagnostic test (Повний діагностичний тест) — полягає в посекторному читанні всього диска;
- повторна спроба; за наслідками тестування видається одне з трьох повідомлень: Pass (Пройдений), Passed with minor errors (Пройдений з мінімальним числом помилок) або Fail (Помилка); тест завершується достроково при виявленні 20 збійних секторів.
- Утиліта SMARTTest дозволяє оцінити фізичні параметри диска на основі технології S.M.A.R.T.

Передбачено три варіанти тестування:

- Return S.M.A.R.T. status (Повернення S.M.A.R.T.-состояния) — прочитування поточних показників диска відповідно до технології S.M.A.R.T.;
- Run short Drive Self Test (Проведення скороченого самотестування диска) — припускає додаткове тестування диска в обмеженому режимі; тривалість тестування складає 1-2 хвилини;

- Run extended Drive Self Test (Проведення розширеного самотестування диска) — припускає додаткове тестування диска в повному об'ємі; тривалість тестування складає 20 хвилин або більше.

За наслідками всіх видів тестування формується докладний звіт. При виявленні тих або інших проблем звіт містить рекомендації з їх усунення. Всі тести можуть проводитися у фоновому режимі.

Утиліта PartitionTests призначена для проведення аналізу структури файлової системи диска. Вона виконує поглиблене обстеження елементів файлової системи з подальшою генерацією звіту про стан файлів даних. Для отримання коректних результатів рекомендується перед запуском утиліти закрити всі інші програми.

Загальним для всіх утиліт, що входять до складу Easy Recovery, є те, що вони працюють в режимі майстра: користувачеві пропонується вказати параметри виконання чергового кроку завдання і перейти до наступного кроку.

Категорія Data Recovery, до складу якої входять 6 утиліт:

- DeletedRecovery — пошук і відновлення видалених файлів і каталогів;
- AdvancedRecovery — пошук і відновлення видалених файлів і каталогів з можливістю додаткової настройки параметрів пошуку;
- FormatRecovery — відновлення даних в розділах, які випадково відформатували або видалених розділах;
- RawRecovery — відновлення даних в розділах з порушеною структурою;
- ResumeRecovery — сервісна функція, що дозволяє зберігати поточні параметри відновлення з метою їх використання в повторних сеансах роботи з EasyRccovery;
- EmergencyDiskette — утиліта для створення аварійного завантажувального гнучкого диска; такий диск містить системні файли дискової операційної системи Caldera DR-DOS, а також DOS-версию утиліт з категорії Data Recovery; утиліта має важливе достоїнство і два істотних недоліки: з одного боку, вона дозволяє створювати завантажувальний диск безпосередньо з середовища Windows XP, з іншого — на створюваному диску відсутній драйвер з підтримкою кирилиці, і тому файли і каталоги з російськими буквами стають невпізнанними; крім того, після завантаження з гнучкого диска потрібно виконати ряд додаткових операцій в режимі командного рядка, що під силу не кожному «рядовому» користувачеві.

Перші чотири з названих утиліт безпосередньо пов'язані з відновленням даних і працюють в цілому за єдиним алгоритмом, що складається з наступних основних дій.

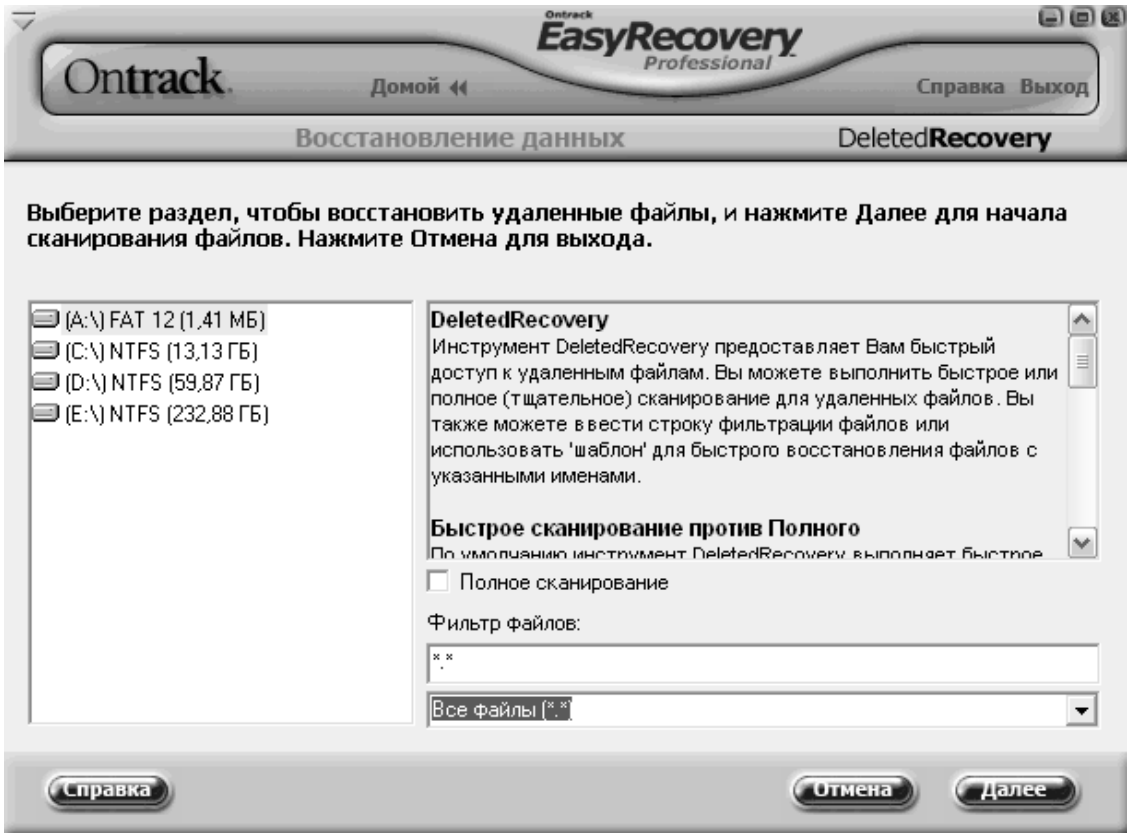
1. Сканування жорстких дисків з метою визначення конфігурації логічних дисків.

2. Сканування вказаного користувачем розділу з метою пошуку видалених або пошкоджених елементів даних.

3. Запис вибраних користувачем даних за новою адресою.

Для відновлення даних за допомогою DeletedRecovery необхідно виконати наступні дії.

1. У списку логічних дисків виберіть той, на якому потрібно відновити видалені файли (мал. 9).



мал.9

2. Щоб звузити діапазон пошуку, в полі File Filter (Фільтр файлів) введіть з клавіатури або за допомогою розташованого нижче списку маску для пошуку файлів.

3. Якщо після видалення файлу пройшло багато часу і він може бути пошкоджений, встановіть прапорець Complete Scan (Повний перегляд) для проведення повнішого аналізу диска.

4. Натисніть на кнопці Next (Далі), щоб перейти до наступного кроку; Easy-Recovery просканує диск і видасть результати в наступному вікні.

5. У лівій частині вікна (у дереві каталогів) виберіть каталог, де розташований відновлюваний файл, а в правому списку — натисніть на значок цього файлу.

6. Щоб полегшити перегляд списку, скористайтесь фільтром відбору знайдених файлів. Для цього натисніть кнопку Filter Options (Параметри фільтру) і у вікні настройок встановіть необхідні параметри.

7. Щоб знайти конкретний файл, можна застосувати функцію пошуку, що викликається кнопкою Find (Пошук); як критерії пошуку можуть бути використані ім'я файлу, його розмір, дата створення, а також стан після видалення.

8. Якщо потрібно заздалегідь подивитися на вміст відновлюваного файлу, натисніть на кнопці View File (Попередній перегляд файлу).

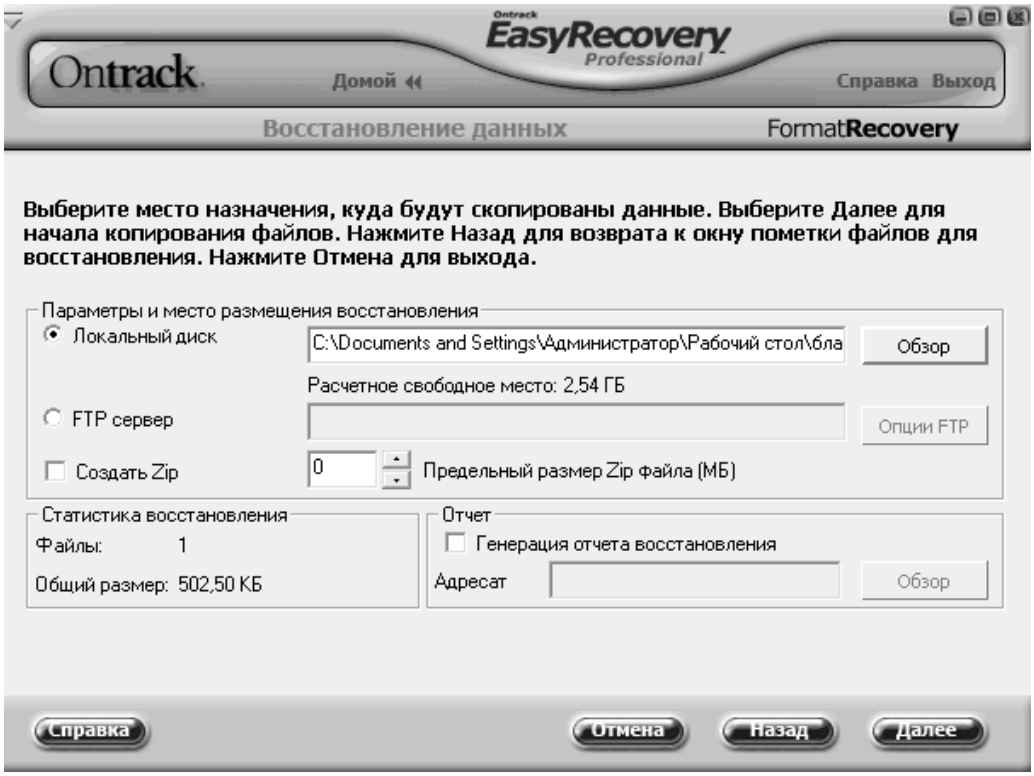
9. Завершивши вибір відновлюваного файлу (або каталогу), перейдіть до наступного кроку. Він полягає в записі відновлюваного об'єкту за новою адресою; які додаткові параметри ви можете вказати (мал. 10) необхідність архівації файлу, генерації звіту і пересилки файлу на FTP-сервер.

Відновлення даних за допомогою AdvancedRecovery

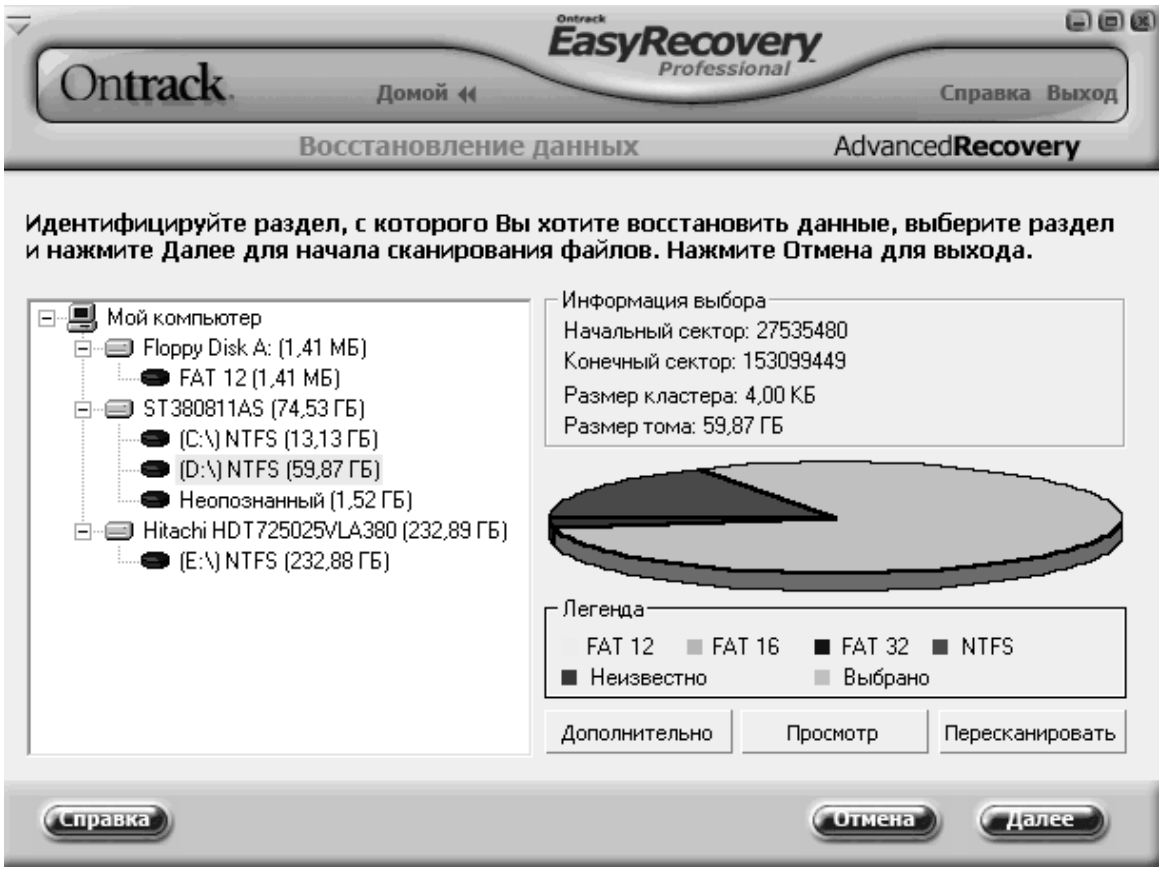
Основна відмінність AdvancedRecovery від утиліти DeletedRecovery полягає в можливості настройки більшого числа параметрів пошуку відновлюваних даних на логічному диску. Зокрема, користувач отримує можливість працювати не тільки з деревом каталогів, але й зі службовою інформацією розділу.

Після завершення сканування дисків AdvancedRecovery виводить на екран їх список і докладний звіт про параметри відповідного розділу (мал. 11).

Якщо програма AdvancedRecovery не змогла виявити який-небудь розділ або коректно визначити його параметри, ви можете змінити параметри сканування, задані за умовчанням.



мал. 10



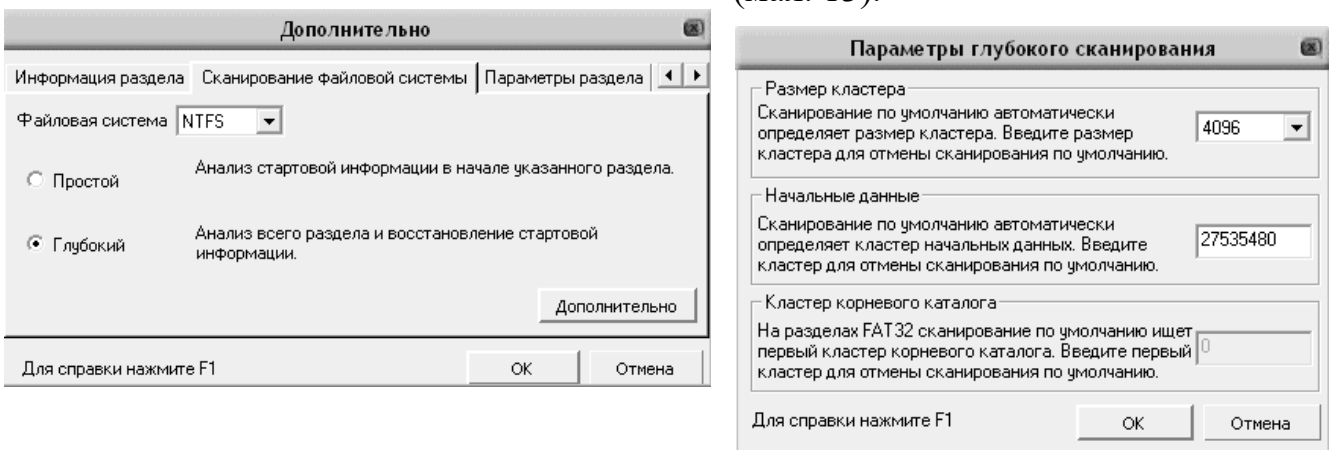
мал. 11

Для цього потрібно натиснути на кнопці Advanced Options (Додаткові параметри) і виконати необхідну настройку в додатковому діалоговому вікні.

Вікно настройок містить чотири вкладки. Перша з них, Partition Information (Відомості про розділ) дозволяє змінити номери першого і останнього кластерів розділу, щоб «допомогти» AdvancedRecovery виявити його на диску. Крім того, натиснувши на кнопці Hint (Підказка), ви отримаєте можливість змінювати розміри (межі) одного або декількох розділів (мал. 12). Мається на увазі не реконфігурація дисків, а зміна меж, в рамках яких Advanced-Recovery повинен шукати втрачені розділи.

мал. 12

Вкладка File System Scan (Сканування файлової системи) дозволяє обрати тип і параметри файлової системи для вибраного розділу, а також режим сканування (мал. 13).



мал. 13

При виборі режиму Advanced Scan (Розширене сканування) можна додатково вказати розмір кластера, номер першого кластера області даних і (для файлової системи FAT) номер першого кластера кореневого каталогу.

Вкладка Partition Settings (Параметри розділу) містить єдиний елемент управління — список, що розкривається, за допомогою якого можливо обрати джерело відомостей про наявні в розділі дані. Це джерело використовуватиме в своїй роботі AdvancedRecovery.

Набір варіантів, представлених в списку, залежить від файлової системи досліджуваного розділу.

Для розділів FAT список містить наступні варіанти:

■ Use FAT1 (Використовувати FAT1) — перегляд області даних виконується відповідно до інформації в першій копії FAT;

■ Use FAT2 (Використовувати FAT2) — пошук даних проводиться на основі другої копії FAT;

■ Use Best Math (Використовувати найбільш відповідну) — AdvancedRecovery спочатку порівнює фактичний вміст деякої частини диска з інформацією в обох копіях FAT, а потім застосовує для продовження роботи з диском найбільш відповідну копію FAT;

■ Ignore FAT (Ігнорувати FAT) — пошук даних проводиться па основі відомостей, що містяться в кореневому каталозі і в інших каталогах розділу; даний варіант доцільно застосовувати у тому випадку, коли обидві копії FAT зіпсовано (наприклад, в результаті швидкого форматування розділу).

Для розділів NTFS список містить два варіанти:

■ Use MFT (Використовувати MFT) — перегляд області даних виконується відповідно до записів в таблиці MFT;

■ Ignore MFT (Ігнорувати MFT) — аналіз диска проводиться без використання записів MFT.

■ Вкладка Recovery Options (параметри відновлення) дозволяє вказати Advanced Recovery, які файли слід включати в список тих, що підлягають

відновленню. За умовчанням до таких відносяться наступні файли:

- з некоректним штампом дати і/або часу (Invalid Dates);
- з некоректним набором атрибутів (Invalid Attributes);
- з неправильно вказаним розміром (Invalid File Size);
- помічені як видалені (Deleted);
- у імені яких присутні неприпустимі символи (Invalid characters).

Таким чином, можливість відновлення даних є вельми важливим напрямом добування оперативної та доказової інформації при документуванні злочинної діяльності фігурантів. В результаті відновлення комп'ютерної інформації з носіїв, доступ до яких отримано оперативним або слідчим шляхом, можуть бути здобуті відомості, раніше навмисно видалені фігурантом. В даному випадку сам факт такої його поведінки може указувати оперуповноваженому, а згодом слідчому, прокуророві і суду, на обставини, що викривають злочинця і що характеризують суб'єктивну сторону злочину. Крім того, в більшості випадків, відновлена інформація має не тільки орієнтуюче значення, але і може служити джерелом доказів у кримінальному судочинстві за умови дотримання законності добування такої інформації і можливості її легалізації.

4. ОСОБЛИВОСТІ ПРИЗНАЧЕННЯ СУДОВИХ ТЕХНІЧНИХ ЕКСПЕРТИЗ ЕЛЕКТРОННИХ НОСІЇВ ІНФОРМАЦІЇ

Рекомендовані джерела:

Інструкція про призначення та проведення судових експертиз та експертних досліджень: наказ Міністерства юстиції України від 8 жовтня 1998 року № 53/5. Дата оновлення: 02.02.2019. URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (дата звернення: 27.08.2019).

Організація розслідування фактів несанкціонованого переказу коштів з рахунків клієнтів банку, які обслуговуються за допомогою систем дистанційного обслуговування: методичні рекомендації / В.В. Корнієнко, В.І. Стреляний. – Х., 2015. – 71 с.

Інформаційний лист про підготовчі заходи та алгоритм дій при призначенні комп'ютерно-технічної експертизи. Київський міський НДЕКЦ МВС України. Київ – 2016. – 4 с.

Судово-мистецтвознавча експертиза. Інформаційний лист Експертної служби МВС України. Дніпро – 2017. – 5 с.

Інструкція про особливості здійснення судово-експертної діяльності атестованими судовими експертами, що не працюють у державних спеціалізованих експертних установах: наказ Міністерства юстиції України від 12 грудня 2011 року № 3505/5 (в редакції наказу Міністерства юстиції України від 7 вересня 2015 року № 1659/5). Дата оновлення: 15.09.2017. URL: https://zakon.rada.gov.ua/laws/show/z1431-11 (дата звернення: 01.09.2019).

Рекомендації щодо особливостей досудового розслідування та процесуального керівництва у кримінальних провадженнях про злочини, вчинені з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, схвалені рішенням науково-методичної ради (протокол №3 від 20 квітня 2017 року). Відділ науково-методичного забезпечення участі прокурорів у кримінальному провадженні Науково-дослідного інституту Національної академії прокуратури України. – 67 с.

Аналізуючи **Інструкцію про призначення та проведення судових експертиз та експертних досліджень** (далі – Інструкція), слід звернути увагу на те, що електронні носії інформації можуть використовуватися при проведенні різних судових експертиз.

Так, згідно з п.3.15 – 3.18 Інструкції, при призначенні експертиз стосовно документів, виготовлених за допомогою копіювально-розмножувальної техніки, необхідно вжити заходів для збереження її у такому стані, у якому вона перебувала на час вилучення. Не дозволяється здійснювати будь-які операції з такою технікою до її направлення на експертизу. Для розв'язання ідентифікаційних завдань щодо документів, виготовлених за допомогою комп'ютерної техніки, ця техніка надається в комплекті (системний блок комп'ютера, інсталяційний диск з драйвером принтера або багатофункціонального пристрою, з'єднувальні та мережеві кабелі, принтер). До

направлення комп'ютерної техніки на експертизу будь-яка робота на ній не дозволяється. Вирішення ідентифікаційних питань проводиться в межах комплексної комп'ютерно-технічної експертизи та технічної експертизи документів за наявності електронного оригіналу документа (файла). Вилучення комп'ютерної техніки, її огляд мають проводитися за участю спеціаліста у галузі комп'ютерно-технічних досліджень. Принтери (особливо струминні) слід направляти на експертизу у найкоротший термін, оскільки застигання барвника може призвести до змін у вигляді та характері нанесення барвника на папір. При призначенні експертиз стосовно документів, виготовлених за допомогою комп'ютерної техніки, необхідно з'ясувати, чи змінювались знімні частини (картриджі) або чи піддавались ремонту які-небудь вузли принтерів. Якщо картриджі лазерних принтерів змінювались, необхідно вжити заходів щодо розшуку відпрацьованих картриджів та подати їх на дослідження. Для проведення експертизи необхідно також вилучити вільні зразки, які були виготовлені на вилученому принтері в період, що відповідає періоду виготовлення досліджуваних документів.

Відповідно до п.13 Інструкції, до основних завдань експертизи комп'ютерної техніки і програмних продуктів належать:

установлення робочого стану комп'ютерно-технічних засобів;

установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;

виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях;

установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку [13].

Орієнтовний перелік вирішуваних питань:

Чи міститься на даному носії інформація стосовно (зазначити, яка інформація цікавить) і у якому вигляді?

Чи містить носій досліджуваного комп'ютера інформацію про певні (зазначити, які саме) дії користувача?

Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації?

Чи могла бути створена зазначена інформація на цьому комп'ютері чи вона перенесена з іншого носія?

Яким чином інформація (зазначити, яка саме) перенесена до досліджуваного комп'ютера (носія)?

Яка технологія та хронологія створення електронного документа (зазначити електронний документ та певний зміст)?

Які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію стосовно... (зазначити зміст)?

Чи містить накопичувач інформації досліджуваного комп'ютера певне (зазначити, яке саме - встановлене, не встановлене) програмне забезпечення?

Які функціональні несправності мають дане комп'ютерне обладнання або його окремі складові та пристрої і як ці несправності впливають на роботу обладнання в цілому?

Чи можливо виконання певних дій за допомогою даного програмного продукту?

Чи можливе вирішення певного завдання за допомогою даного програмного продукту?

Чи реалізовані у даному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?

Для дослідження інформації, що міститься на комп'ютерних носіях, експерту надається сам комп'ютерний носій, а за потреби комп'ютерний блок (комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій).

Для збереження наданих на дослідження носіїв інформації в робочому стані вони надаються в окремих пакуваннях. Системні блоки персональних комп'ютерів надаються в пакуваннях, що унеможливлюють доступ до носіїв інформації безпосередньо чи підключення системного блока до мережі живлення.

Для встановлення відповідності програмних продуктів певним параметрам експерту надається носій з копією досліджуваного програмного продукту або програмного коду.

Для дослідження робочого стану комп'ютерно-технічних засобів експерту надаються ці комп'ютерно-технічні засоби, а також технічна документація до них.

З метою визначення, які саме об'єкти слід надати експерту в кожному конкретному випадку, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта (спеціаліста) в галузі комп'ютерної техніки.

Електронні носії інформації можуть використовуватися при проведенні експертизи документів фінансово-кредитних операцій. Зокрема, відповідно до розділу ІІІ (Економічна експертиза) Інструкції, якщо ведення бухгалтерського та податкового обліку здійснювалось в електронно-обчислювальному вигляді, експерту надаються регістри бухгалтерського та податкового обліку у роздрукованому вигляді, обов'язково завірені в установленому порядку. Додатково вони можуть бути надані на вимогу експерта на електронних носіях інформації.

Більше про систему питань, відповіді на які можуть бути з'ясовані за допомогою проведення ряду видів експертиз (із використанням електронних носіїв інформації) можна дізнатися зі змісту Інструкції.

На цьому місці доцільно звернути увагу на ряд положень Методичних рекомендацій[5] щодо призначення судових експертиз.

Результат використання електронних носіїв інформації як джерела доказів залежить не лише від своєчасної та кваліфікованої участі спеціаліста при проведенні відповідних слідчих дій. Важко перебільшити кримінальне процесуальне значення подальшого дослідження й аналізу доказів у ході проведення відповідних судових експертиз.

Основний напрям проведення експертиз це – комп'ютерно-технічний. У відповідності з завданнями і специфікою об'єктів дослідження на теперішній час в рамках цього роду експертиз можливо виділити такі види:

---

[5] Організація розслідування фактів несанкціонованого переказу коштів з рахунків клієнтів банку, які обслуговуються за допомогою систем дистанційного обслуговування: методичні рекомендації / В.В. Корнієнко, В.І. Стреляний. – Х., 2015. – 71 с. С.58-61

- **технічні експертизи комп'ютерів і їх комплектуючих** (судова комп'ютерно-технічна експертиза: апаратно-комп'ютерна та комп`ютерно-мережева), які проводяться з метою вивчення конструктивних особливостей і стану комп'ютера, його периферійних приладів, магнітних носіїв, комп'ютерних мереж, а також причин виникнення порушень в роботі;

- **експертизи даних і програмного забезпечення** (програмно-комп'ютерна, інформаційно-комп'ютерна судові експертизи), які здійснюються з метою вивчення інформації, що зберігається в комп'ютері і на магнітних носіях.

Питання, які виносяться на вирішення комп'ютерно-технічної експертизи, по її виду можливо розділити також на дві групи.

1. Питання, які вирішуються технічною експертизою комп'ютерів і їх комплектуючих (діагностичні):

1) комп'ютер якої моделі наданий на дослідження; які технічні характеристики його системного блоку і периферійних приладів; які технічні характеристики даної обчислювальної мережі;

2) де і коли виготовлений і зібраний даний комп'ютер і його комплектуючі; складання комп'ютера здійснювалось в заводських або кустарних умовах;

3) чи співпадає внутрішня будова комп'ютера і периферія запропонованій технічній документації; чи не внесені в конструкцію комп'ютера зміни (наприклад, установка додаткових вбудованих приладів: вінчестерів, приладів для розширення оперативної пам'яті, зчитування оптичних дисків, інші зміни конфігурації);

4) чи справний комп'ютер і його комплектуючі; який їх знос; які причини несправності комп'ютера і периферійних приладів; чи містять фізичні дефекти носії інформації;

5) чи проводилась адаптація комп'ютера для роботи з специфічним користувачем (лівша, людина з вадами зору та інші);

6) які технічні характеристики інших електронних засобів прийому, накопичення і видачі інформації (електронна записна книжка, телефонний сервер); чи справні ці засоби; які причини поломки.

2. Питання, які вирішуються експертизою даних і програмного забезпечення (*діагностичні*):

1) яка операційна система використана в комп'ютері;

2) який зміст інформації, що зберігається на внутрішніх і зовнішніх магнітних носіях, в тому числі, які програмні продукти там знаходяться; яке призначення програмних продуктів; який алгоритм їх функціонування, способу вводу і виводу інформації; який час проходить з моменту вводу даних до вводу результатів при роботі з даною комп'ютерною програмою, бази даних;

3) чи являються дані програмні продукти ліцензованими (або несанкціонованими) копіями стандартних систем чи оригінальними розробками;

4) чи вносилися в програму даного системного продукту будь-які корективи (які), що змінюють виконання деяких операцій (яких);

5) чи співпадає даний оригінальний комп'ютерний продукт технічному завданню; чи забезпечується при його роботі виконання всіх передбачених функцій;

6) чи використовувалися для обмеження доступу до інформації паролі, приховані файли, програми захисту та інше; який зміст прихованої інформації; чи відбувалися спроби підбору паролю, злому технічних засобів та інші спроби несанкціонованого доступу;

7) чи можливе відновлення стертих файлів, дефектних магнітних носіїв інформації; який зміст відновлених файлів;

8) який механізм втрати інформації із локальних обчислювальних мереж і розподілених баз даних;

9) чи маються збої у функціонуванні комп'ютера, роботі окремих програм; які причини цих збоїв; чи не викликані збої в роботі комп'ютера впливом вірусу (якого); чи поширюється негативний вплив вірусу на більшість програм, чи він діє тільки на визначені програми; чи можливо відновити в повному обсязі функціонування даної програми (текстового файлу), пошкодженої вірусом;

10) який зміст інформації зберігається в електронній записній книжці та інше; чи зберігається в книжці прихована інформація і який її зміст;

11) коли проводилось останнє корегування даного файлу або інсталяція даного програмного продукту;

12) який був рівень професійної підготовки в галузі програмування і роботи з комп'ютерною технікою особи, яка виконувала дані дії.

Крім того, за допомогою комп'ютерно-технічних експертиз можливе вирішення деяких питань *ідентифікаційного* характеру:

1) чи мають комплектуючі комп'ютера (плати, магнітні носії, дисководи та інше) єдине джерело походження;

2) чи не написана дана комп'ютерна програма певною особою (вирішується комплексно при проведенні комп'ютерно-технічної і авторознавчої експертиз).

Об'єктами комп'ютерно-технічної експертизи виступають:

- зібрані комп'ютери, їх системні блоки;
- периферійні пристрої (монітори, принтери, дисководи, модеми, сканери, клавіатури, маніпулятори та інше), комунікаційні прилади комп'ютерів і обчислювальних мереж;
- магнітні носії інформації (жорсткі диски і зовнішні накопичувачі, оптичні диски);
- роздруківка програмних і текстових файлів;
- словники пошукових ознак систем (тезауруси), класифікатори та інша технічна документація, наприклад технічні завдання і звіти;
- електронні записні книжки, інші електронні носії текстової або цифрової інформації, технічна документація до них.

Згідно ст.242 КПК України, експертиза проводиться експертною установою, експертом або експертами за дорученням слідчого судді чи суду, наданим за клопотанням сторони кримінального провадження.

Відповідно до ст.244 КПК України, в разі якщо для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання, сторони кримінального провадження мають право звернутися з клопотанням про проведення експертизи до слідчого судді. У клопотанні зазначаються:

1) короткий виклад обставин кримінального правопорушення, у зв’язку з яким подається клопотання;

2) правова кваліфікація кримінального правопорушення із зазначенням статті (частини статті) закону України про кримінальну відповідальність;

3) виклад обставин, якими обґрунтовуються доводи клопотання;

4) вид експертного дослідження, що необхідно провести, та перелік запитань, які необхідно поставити перед експертом.

До клопотання також додаються копії матеріалів, якими обґрунтовуються доводи клопотання.

Клопотання розглядається слідчим суддею місцевого суду, в межах територіальної юрисдикції якого здійснюється досудове розслідування, не пізніше п’яти днів із дня його надходження до суду. Особа, яка подала клопотання, повідомляється про місце та час його розгляду, проте її неприбуття не перешкоджає розгляду клопотання, крім випадків, коли її участь визнана слідчим суддею обов’язковою.

Слідчий суддя, встановивши, що клопотання подано без додержання вимог частини другої цієї статті, повертає його особі, яка його подала, про що постановляє ухвалу.

Під час розгляду клопотання слідчий суддя має право за клопотанням учасників розгляду або за власною ініціативою заслухати будь-якого свідка чи дослідити будь-які матеріали, що мають значення для вирішення клопотання.

Слідчий суддя задовольняє клопотання, якщо особа, яка звернулася з відповідним клопотанням, доведе, що для вирішення питань, що мають істотне значення для кримінального провадження, необхідне залучення експерта.

Слідчий суддя самостійно визначає експерта, якого необхідно залучити, або експертну установу, якій необхідно доручити проведення експертизи. Особливості здійснення судово-експертної діяльності атестованими судовими експертами, що не працюють у державних спеціалізованих експертних установах, регламентовані Інструкцією про особливості здійснення судово-експертної діяльності атестованими судовими експертами, що не працюють у державних спеціалізованих експертних установах (наказ Міністерства юстиції України від 12 грудня 2011 року № 3505/5) [14].

До ухвали слідчого судді про доручення проведення експертизи включаються запитання, поставлені експертові особою, яка звернулася з відповідним клопотанням. Слідчий суддя має право не включити до ухвали запитання, поставлені особою, яка звернулася з відповідним клопотанням, якщо відповіді на них не стосуються кримінального провадження або не мають значення для судового розгляду, обґрунтувавши таке рішення в ухвалі.

Висновок експерта, залученого слідчим суддею, надається особі, за клопотанням якої він був залучений.

БІБЛІОГРАФІЧНИЙ СПИСОК

1. Звіт Голови Національної поліції України С. Князєва про результати роботи відомства за 2018 рік. Офіційний сайт Національної поліції. Річні звіти. URL: https://www.npu.gov.ua/activity/zviti/richni-zviti/ (дата звернення: 21.08.2019).

2. Єдиний звіт про кримінальні правопорушення по державі за грудень 2014 року. Генеральна прокуратура України. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=111480&libid=100820# (дата звернення: 12.03.2019).

3. Єдиний звіт про кримінальні правопорушення по державі за грудень 2018 року. Генеральна прокуратура України. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113653&libid=100820&c=edit&_c=fo (дата звернення: 12.03.2019)

4. Єдиний звіт про кримінальні правопорушення по державі за січень-липень 2018 року. Генеральна прокуратура України. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113653&libid=100820&c=edit&_c=fo (дата звернення: 22.08.2019)

5. Єдиний звіт про кримінальні правопорушення по державі за січень-липень 2019 року. Генеральна прокуратура України. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113653&libid=100820&c=edit&_c=fo (дата звернення: 22.08.2019)

6. Організація розслідування фактів несанкціонованого переказу коштів з рахунків клієнтів банку, які обслуговуються за допомогою систем дистанційного обслуговування: методичні рекомендації / В.В. Корнієнко, В.І. Стреляний. – Х., 2015. – 71 с.

7. Конвенція про кіберзлочинність, ратифікована законом від 07 вересня 2005 року № 2824-IV. Дата оновлення: 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 25.08.2019).

8. Про ратифікацію Конвенції про кіберзлочинність: закон України від 07 вересня 2005 року № 2824-IV. Дата оновлення: 14.10.2010. URL: https://zakon.rada.gov.ua/laws/show/2824-15 (дата звернення: 25.08.2019).

9. Про електронні документи та електронний документообіг: закон України від 22 травня 2003 року № 851-IV. Дата оновлення: 07.11.2018. URL: https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення: 25.08.2019).

10. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 року № 4651-VI. URL: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (дата звернення: 25.08.2019).

11. Про електронні довірчі послуги: закон України від 5 жовтня 2017 року № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення: 19.10.2019).

12. Порядок зберігання речових доказів стороною обвинувачення, їх реалізації, технологічної переробки, знищення, здійснення витрат, пов'язаних з їх зберіганням і пересиланням, схоронності тимчасово вилученого майна під час кримінального провадження: постанова Кабінету міністрів України від 19 листопада

2012 року №1104. Дата оновлення: 16.11.2016. URL: https://zakon.rada.gov.ua/laws/show/1104-2012-%D0%BF (дата звернення: 25.08.2019).

13. Інструкція про призначення та проведення судових експертиз та експертних досліджень: наказ Міністерства юстиції України від 8 жовтня 1998 року № 53/5. Дата оновлення: 02.02.2019. URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (дата звернення: 25.08.2019).

14. Інструкція про особливості здійснення судово-експертної діяльності атестованими судовими експертами, що не працюють у державних спеціалізованих експертних установах: наказ Міністерства юстиції України від 12 грудня 2011 року № 3505/5 (в редакції наказу Міністерства юстиції України від 7 вересня 2015 року № 1659/5). Дата оновлення: 15.09.2017. URL: https://zakon.rada.gov.ua/laws/show/z1431-11 (дата звернення: 01.09.2019).

15. Інформаційний лист про підготовчі заходи та алгоритм дій при призначенні комп'ютерно-технічної експертизи. Київський міський НДЕКЦ МВС України. Київ – 2016. – 4 с.

16. Судово- мистецтвознавча експертиза. Інформаційний лист Експертної служби МВС України. Дніпро – 2017. – 5 с.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Види електронних носіїв інформації?
2. За якими спеціальностями розподіляється профільність комп’ютерних експертів?
3. Якими є правила поводження з комп’ютерним обладнанням?
4. Як саме за IP адресою можна знайти власника медійного контенту?
5. Як шукати суб’єкта за допомогою сервіса Whois у відкритих джерелах?
6. Яким є алгоритм відновлення знищеного контенту за допомогою програмних засобів?
7. Як можна відновити видалені файли і каталоги?
8. Якими є основні завдання експертизи комп'ютерної техніки і програмних продуктів?
9. Якими є види комп’ютерно-технічної експертизи?
10. Які діагностичні питання вирішуються технічною експертизою комп’ютерів і їх комплектуючих?
11. Які діагностичні питання вирішуються експертизою даних і програмного забезпечення?
12. Які питання ідентифікаційного характеру можуть вирішуватися за допомогою комп’ютерно-технічних експертиз?

ЛАБОРАТОРНІ РОБОТИ

1. Оглянути мобільний телефон з метою фіксації відомостей для його ідентифікації. Скласти протокол огляду документа.

2. Оглянути планшет з метою фіксації відомостей для його ідентифікації. Скласти протокол огляду документа.

3. Оглянути смартфон з метою фіксації відомостей для його ідентифікації. Скласти протокол огляду документа.

4. Оглянути ноутбук з метою фіксації відомостей для його ідентифікації. Скласти протокол огляду документа.

5. Оглянути мобільний телефон на предмет комунікації з номером 0672786598. Скласти протокол огляду документа.

6. Оглянути ноутбук на предмет можливої наявності лог-файлів розміщення з цього пристрою оголошення на сервісі ОЛХ. Скласти протокол огляду документа.

7. Оглянути смартфон на предмет комунікації в Telegram, Watsap, Bip протягом останніх трьох днів.

8. Провести тимчасовий доступ до планшету з метою ознайомлення з коментарями, розміщуваними з цього пристрою в соціальній мережі Фейсбук, а також копіювання комунікації у Viber та вилучення фотографій, зроблених протягом останніх 4 днів та скрін-шотів, зроблених протягом останнього тижня.

9. Оглянути USB-носій і скопіювати весь його електронний вміст на диск.

10. Оглянути micro-SD карточку і скопіювати весь її електронний вміст на диск.

ДОДАТКИ

ДОДАТОК 1

Приклад клопотання про проведення комп'ютерно-технічної експертизи

Слідчому судді
Індустріального районного суду
м. Дніпропетровська

КЛОПОТАННЯ
про проведення комп'ютерно-технічної експертизи

місто Дніпро «____» вересня 2018 року

Слідчий слідчого відділу Кіровського ВП Дніпровського ВП ГУНП в Дніпропетровській області лейтенант поліції Петренко С.О., розглянувши матеріали кримінального провадження №12018040000000000 від 20.08.2018, за ознаками складу кримінального правопорушення, передбаченого ч. 1 ст. 361 КК України, -

ВСТАНОВИВ:

У провадженні слідчого відділу Кіровського ВП Дніпровського ВП перебувають матеріали досудового розслідування, внесені до Єдиного реєстру досудових розслідувань за № 12018040000000000 від 20.09.2018, розпочатого за ознаками кримінального правопорушення, передбаченого ч.1 ст. 361 КК України.

В ході проведення досудового розслідування встановлено, що 25.07.2018 невстановлена особа, здійснила несанкціоноване втручання в роботу комп'ютера, що використовується головним бухгалтером ТОВ «ДУСТ», що призвело до витоку та втрати інформації, що належить до власності підприємства, яка містить конфіденційну та комерційну інформацію, чим спричинила майнову шкоду підприємству, розмір якої на даний час встановлюється.

За даним фактом 20.08.2018 розпочато кримінальне провадження № 12018040000000000, за ознаками кримінального правопорушення, передбаченого ч.1 ст. 361 КК України.

Під час досудового розслідування допитано директора ТОВ «ДУСТ» Друзенко С.А., який показав, що 26 серпня 2018 року до нього звернувся бухгалтер Товариства Зибка Поліна Олегівна, 17.07.1984 р.н. та повідомила, що з її робочого комп'ютера зникли важливі файли, які вкрай необхідні для безперервної та стабільної роботи підприємства, а саме: файли та папки з інформацією яка містить комерційну та конфіденційну таємницю підприємства та її ділових партнерів. Більш того, в деяких папках на її комп'ютері відображено, що до них вносились якісь зміни 25.07.2018 р о 23:07, однак це була Неділя (вихідний день) і ніхто в цей час не працював.

В подальшому, в цей же день було проаналізовано стандартні сервіси операційної системи «Windows», що відображають історію внесених змін та історію виконаних на комп'ютері процесів і команд, також, оскільки для виробничої необхідності потрібно, щоб комп'ютер Головного бухгалтера постійно працював, було перевірено історію служби керування віддаленим доступом.

Проведеними заходами було з'ясовано, що невідома особа дійсно отримала доступ до службового комп'ютера головного бухгалтера Товариства за допомогою віддаленого доступу, тобто фізично за даним комп'ютером не знаходилась.

Невідомою особою використовувалась IP-адреса 178.000.199.000, що належить інтернет-провайдеру «Триолан», підключення відбувалось 25.07.2018 року о 21:59:40, 21:59:37, 22:25:11, 22:57:36, 22:57:37, 23:09:09, 23:09:10.

В подальшому було з'ясовано, що зниклі документи були створені та редагувались колишньою співробітницею ТОВ «ДУСТ», яка працювала на посаді бухгалтера, а саме: Рудою Оленою Миколаївною, 18.04.1987 р.н., користується абонентським номером +38(098)897-51-00. Зазначена особа звільнена з посади бухалтера ТОВ «ДУСТ» 21.06.2018 за власним бажанням, а її облікові робочі записи були заблоковані. Чи знала вона паролі доступу до інших робочих облікових записів Друзенко С.А. пояснити не зміг.

Також, слід зазначити, що відповідною службою операційної системи «Windows» відображено, що авторизація в системі та вхід до облікового запису було здійснено із використанням логіну та паролю бухгалтера підприємства, що на даний час працює в ТОВ «ДУСТ», а саме: Зибкої Поліни Олегівни, 17.07.1984 р.н.

В подальшому, оперативним шляхом було встановлено, що у вказаний у заяві дату та час зазначена IP-адреса була закріплена за абонентом – Руда Олена Миколаївна, 18.04.1987 р.н., за адресою: м. Дніпро, пр. Б. Хмельницького, б. 42, кв. 3, користується мобільним телефоном +38(098)000-51-00.

Під час досудового розслідування 27.08.2018 директором ТОВ «ДУСТ» Друзенком С.А. надано для проведення дослідження флеш-накопичувач «Apacer» біло-салатового кольору, ємністю 8Гб, серійний номер: dAP8GAH335981736120402, на якій мається копія системного журналу «Windows» з жорсткого диску комп'ютера бухгалтера ТОВ «ДУСТ», яку поміщено в паперовий конверт білого кольору та скріплено підписом директора та печаткою підприємства.

27.08.2018 проведено огляд речі, в ході якого оглянуто наданий директором ТОВ «ДУСТ» Друзенком С.А., паперовий конверт білого кольору в якому знаходиться, флеш-накопичувач «Apacer» біло-салатового кольору, ємністю 8Гб, серійний номер: dAP8GAH335981736120402, на якій мається копія системного журналу «Windows» з жорсткого диску комп'ютера бухгалтера ТОВ «ДУСТ». Зазначений паперовий конверт поміщено у спецпакет № 0015000.

Так, відповідно до ст. 84 КПК України доказами у кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів.

Відповідно до п. 6 ч. 2 ст. 242 КПК України слідчий або прокурор зобов'язані звернутись з клопотанням до слідчого судді для проведення експертизи щодо визначення розміру матеріальних збитків, шкоди немайнового характеру, шкоди довкіллю, заподіяної кримінальним правопорушенням.

Відповідно ст. 243 КПК України – експерт залучається за наявності підстав для проведення експертизи за дорученням слідчого судді чи суду, наданим за клопотанням сторони кримінального провадження.

Враховуючи, що для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання в області комп'ютерної техніки, керуючись ст. ст. 40, 110, 242, 243, 244 КПК України, -

ПРОШУ:

1.Задовольнити клопотання слідчого СВ Кіровського ВП Дніпровського ВП ГУНП в Дніпропетровській області лейтенанта поліції Петренка Сергія Олеговича про призначення та проведення комп'ютерно-технічної експертизи, проведення якої доручити експертам Дніпропетровського НДЕКЦ МВС України.

2. На вирішення експерту поставити такі питання:

1) Чи містяться на наданому на дослідження флеш-накопичувачі Apacer, білого-салатового кольору, ємністю 8Гб, серійний номер: dAP8GAH335981736120402, на якій мається копія журналу «Windows» з жорсткого диску комп'ютера бухгалтера ТОВ «ДУСТ» інформація про віддалене підключення до вказаного комп'ютера, що мало місце 25.07.2018 р.? Якщо так, то прошу вказати зазначену інформацію.

2) Чи містяться на наданому на дослідження флеш-накопичувачі Apacer, білого-салатового кольору, ємністю 8Гб, серійний номер: dAP8GAH335981736120402, на якій мається копія журналу «Windows» з жорсткого диску комп'ютера бухгалтера ТОВ «ДУСТ» інформація про виконані процеси, що здійснювались на вказаному комп'ютері, що мало місце 25.07.2018 р.? Якщо так, то прошу вказати зазначену інформацію.

3. Для дослідження експертам представити:

- флеш-накопичувач «Apacer» біло-салатового кольору, ємністю 8Гб, серійний номер: dAP8GAH335981736120402, упакований в паперовий конверт білого кольору та скріплено підписом директора та печаткою підприємства і запакований у спецпакет № 0015000;

4. У разі необхідності доручити слідчому надати експертам матеріали кримінального провадження № 12018040000000000.

5. Дозволити експертам Дніпропетровського НДЕКЦ МВС України, згідно ст. 69 КПК України, ст. 5 ЗУ «Про судову експертизу, провести дослідження, під час яких об'єкти дослідження можуть бути пошкоджені або витрачені лише у тій мірі, в якій це необхідно для дослідження.

Додатки: 1) витяг з ЄРДР № 12018040000000000 від 28.08.2018 року;

2) матеріали на ___ аркушах.

Слідчий слідчого відділення
Кіровського ВП Дніпровського ВП
ГУНП в Дніпропетровській області
лейтенант поліції **С.О. Петренко**

ДОДАТОК 2
Приклад клопотання про проведення комп'ютерно-технічної експертизи

Слідчому судді
Індустріального районного суду
м. Дніпропетровська

КЛОПОТАННЯ
про проведення комп'ютерно-технічної експертизи

місто Дніпро «____» вересня 2018 року

Слідчий слідчого відділу Кіровського ВП Дніпровського ВП ГУНП в Дніпропетровській області лейтенант поліції Петренко С.О., розглянувши матеріали кримінального провадження №12018040000000000 від 20.08.2018, за ознаками складу кримінального правопорушення, передбаченого ч. 1 ст. 361 КК України, -

ВСТАНОВИВ:

У провадженні слідчого відділу Кіровського ВП Дніпровського ВП перебувають матеріали досудового розслідування, внесені до Єдиного реєстру досудових розслідувань за № 12018040000000000 від 20.09.2018, розпочатого за ознаками кримінального правопорушення, передбаченого ч.1 ст. 361 КК України.

В ході проведення досудового розслідування встановлено, що 25.07.2018 невстановлена особа, здійснила несанкціоноване втручання в роботу комп'ютера, що використовується головним бухгалтером ТОВ «ДУСТ», що призвело до витоку та втрати інформації, що належить до власності підприємства, яка містить конфіденційну та комерційну інформацію, чим спричинила майнову шкоду підприємству, розмір якої на даний час встановлюється.

За даним фактом 20.08.2018 розпочато кримінальне провадження № 12018040000000000, за ознаками кримінального правопорушення, передбаченого ч.1 ст. 361 КК України.

Під час досудового розслідування допитано директора ТОВ «ДУСТ» Друзенко С.А., який показав, що 26 серпня 2018 року до нього звернувся бухгалтер Товариства Зибка Поліна Олегівна, 17.07.1984 р.н. та повідомила, що з її робочого комп'ютера зникли важливі файли, які вкрай необхідні для безперервної та стабільної роботи підприємства, а саме: файли та папки з інформацією яка містить комерційну та конфіденційну таємницю підприємства та її ділових партнерів. Більш того, в деяких папках на її комп'ютері відображено, що до них вносились якісь зміни 25.07.2018 р о 23:07, однак це була Неділя (вихідний день) і ніхто в цей час не працював.

В подальшому, в цей же день було проаналізовано стандартні сервіси операційної системи «Windows», що відображають історію внесених змін та історію

виконаних на комп'ютері процесів і команд, також, оскільки для виробничої необхідності потрібно, щоб комп'ютер Головного бухгалтера постійно працював, було перевірено історію служби керування віддаленим доступом.

Проведеними заходами було з'ясовано, що невідома особа дійсно отримала доступ до службового комп'ютера головного бухгалтера Товариства за допомогою віддаленого доступу, тобто фізично за даним комп'ютером не знаходилась.

Невідомою особою використовувалась IP-адреса 178.000.199.000, що належить інтернет-провайдеру «Триолан», підключення відбувалось 25.07.2018 року о 21:59:40, 21:59:37, 22:25:11, 22:57:36, 22:57:37, 23:09:09, 23:09:10.

В подальшому було з'ясовано, що зниклі документи були створені та редагувались колишньою співробітницею ТОВ «ДУСТ», яка працювала на посаді бухгалтера, а саме: Рудою Оленою Миколаївною, 18.04.1987 р.н., користується абонентським номером +38(098)897-51-00. Зазначена особа звільнена з посади бухалтера ТОВ «ДУСТ» 21.06.2018 за власним бажанням, а її облікові робочі записи були заблоковані. Чи знала вона паролі доступу до інших робочих облікових записів Друзенко С.А. пояснити не зміг.

Також, слід зазначити, що відповідною службою операційної системи «Windows» відображено, що авторизація в системі та вхід до облікового запису було здійснено із використанням логіну та паролю бухгалтера підприємства, що на даний час працює в ТОВ «ДУСТ», а саме: Зибкої Поліни Олегівни, 17.07.1984 р.н.

В подальшому, оперативним шляхом було встановлено, що у вказаний у заяві дату та час зазначена IP-адреса була закріплена за абонентом – Руда Олена Миколаївна, 18.04.1987 р.н., за адресою: м. Дніпро, пр. Б. Хмельницького, б. 42, кв.3.

На підставі ухвали слідчого судді Індустріального районного суду м. Дніпропетровська від 30.08.2018 р., проведено 13.09.2018 р. обшук за місцем мешкання Рудої Олени Миколаївни, 18.04.1987 р.н. та її чоловіка Рудого Миколи Петровича, 17.04.1987 р.н. за адресою: м. Дніпро, пр. Б. Хмельниицького, буд. 42, кв. 3, в ході якого було вилучено:

- ноутбук «Asus», модель X5DI, с\н A5N0AS675911200, чорного кольору;
- жорсткий диск комп'ютера фірми «WD» s\n WCC1S1959900;
- роутер фірми «Asus», чорного кольору.

Так, відповідно до ст. 84 КПК України доказами у кримінальному провадженні є фактичні данні, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів.

Відповідно до п. 6 ч. 2 ст. 242 КПК Згідно України слідчий або прокурор зобов'язані звернутись з клопотанням до слідчого судді для проведення експертизи щодо визначення розміру матеріальних збитків, шкоди немайнового характеру, шкоди довкіллю, заподіяної кримінальним правопорушенням.

Відповідно ст. 243 КПК України – експерт залучається за наявності підстав для проведення експертизи за дорученням слідчого судді чи суду, наданим за клопотанням сторони кримінального провадження.

Враховуючи, що для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання в області імунології, керуючись ст. ст. 40, 110, 242, 243, 244 КПК України, -

ПРОШУ:

1.Задовольнити клопотання слідчого слідчого відділу Кіровського ВП Дніпровського ВП ГУНП в Дніпропетровській області лейтенант поліції Петренка Сергія Олеговича про призначення та проведення комп'ютерно-технічної експертизи, проведення якої доручити експертам Дніпропетровського НДЕКЦ МВС України.

2. На вирішення експерту поставити такі питання:

1) Чи містяться на наданому на дослідження ноутбуці «Asus», модель X5DI, с\н A5N0AS675911200, чорного кольору, який вилучений 13.09.2018 в ході обшуку за адресою: м. Дніпро, пр. Б. Хмельниицького, буд. 42, кв. 3, інформація про віддалене підключення в вказаного ноутбука, що мало місце 25.07.2018 р.? Якщо так, то прошу вказати зазначену інформацію? Прошу вказати технічні характеристики мережевої карти наданого на дослідження ноутбука?

2) Чи містяться на наданому на дослідження жорсткому диску комп'ютера фірми «WD» s\n WCC1S1959900, який вилучений 13.09.2018 в ході обшуку за адресою: м. Дніпро, пр. Б. Хмельниицького, буд. 42, кв. 3, інформація про віддалене підключення з вказаного жорсткого диска комп'ютера, що мало місце 25.07.2018 р.? Якщо так, то прошу вказати зазначену інформацію?

3) Чи містяться на наданих на дослідження ноутбуці «Asus», модель X5DI, с\н A5N0AS675911200, чорного кольору та жорсткому диску комп'ютера фірми «WD» s\n WCC1S1959900, які вилучені 13.09.2018 в ході обшуку за адресою: м. Дніпро, пр. Б. Хмельниицького, буд. 42, кв. 3, інформація про виконані процеси, що здійснювались на вказаних ноутбуці та жорсткому диску комп'ютера, що мало місце 25.07.2018 р.? Якщо так, то прошу вказати зазначену інформацію.

4) «Чи містяться в пам'яті наданого на дослідження роутера «Asus» чорного кольору, який вилучений 13.09.2018 в ході обшуку за адресою: м. Дніпро, пр. Б. Хмельниицького, буд. 42, кв. 3 налаштування підключення до мережі «Інтернет» та MAC-адреси. Якщо так, то прошу викласти деталізацію налаштувань»? «Чи встановлювались оновлення програмного забезпечення наданого на дослідження роутера «Asus», чорного кольору та чи змінювалась його MAC-адреса? Якщо так то прошу скопіювати зазначену інформацію»?

5) «Чи містяться на наданих на дослідження ноутбуці «Asus», модель X5DI, с\н A5N0AS675911200, чорного кольору та жорсткому диску комп'ютера фірми «WD» s\n WCC1S1959900, які вилучені 13.09.2018 в ході обшуку за адресою: м. Дніпро, пр. Б. Хмельниицького, буд. 42, кв. 3, файли форматів

*.doc, *.docx, *.txt, *.rtf, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlt, *.xltm, *.xlam? Якщо так то прошу скопіювати зазначену інформацію»?

6) «На які веб-адреси мережі Інтернет та коли здійснювався вихід з наданих на дослідження об'єктів, а саме: ноутбуці «Asus», модель X5DI, с\н A5N0AS675911200, чорного кольору та жорсткому диску комп'ютера фірми «WD» s\n WCC1S1959900, які вилучені 13.09.2018 в ході обшуку за адресою: м. Дніпро, пр. Б. Хмельниицького, буд. 42, кв. 3?»

3. Для дослідження експертам представити:

- ноутбук «Asus», модель X5DI, с\н A5N0AS675911200, чорного кольору та жорсткий диск комп'ютера фірми «WD» s\n WCC1S1959900, запаковані у спец пакет № EXP0409500;
- роутера «Asus», чорного кольору, запакований у спец пакет № 0016400.

4. У разі необхідності доручити слідчому надати експертам матеріали кримінального провадження № 12018040000000600.

5. Дозволити експертам Дніпропетровського НДЕКЦ МВС України, згідно ст. 69 КПК України, ст. 5 ЗУ «Про судову експертизу, провести дослідження, під час яких об'єкти дослідження можуть бути пошкоджені або витрачені лише у тій мірі, в якій це необхідно для дослідження.

Додатки: 1) витяг з ЄРДР № 12018040000000600 від 20.09.2018 року;
2) матеріали на ___ аркушах.

Слідчий слідчого відділення
Кіровського ВП Дніпровського ВП
ГУНП в Дніпропетровській області
лейтенант поліції **С.О. Петренко**

ДОДАТОК 3
Приклад клопотання про тимчасовий доступ до речей і документів

Слідчому судді
Індустріального районного суду
м. Дніпропетровська

КЛОПОТАННЯ
про тимчасовий доступ до речей і документів

місто Дніпро «__» травня 2018 року

Слідчий слідчого відділу Кіровського ВП Дніпровського ВП ГУНП в Дніпропетровській області лейтенант поліції Петренко С.О., розглянувши матеріали кримінального провадження №12017040000000000 від 30.03.2017, за ознаками складу кримінального правопорушення, передбаченого ч. 3 ст. 190 КК України, -

ВСТАНОВИВ:

До слідчого відділу Кіровського ВП Дніпровського ВП ГУНП надійшли матеріали перевірки Придніпровського управління кіберполіції ДКП в Дніпропетровській області, згідно яких невстановлені особи, діючи на території Дніпропетровської області вчиняючи незаконні операції з використанням електронно- обчислювальної техніки, на Інтернет-сайті «olx.ua» та аналогічних Інтернет-аукціонах в Українському сегменті, шахрайським шляхом привласнюють грошові кошти громадян після чого здійснюють їх зняття у банкоматах розташованих на території вказаної області.

Крім того, до слідчого відділу Кіровського ВП Дніпровського ВП ГУНП надійшли матеріали звернення, Кирпи Ігоря Васильовича,1.09.1985 р.н. щодо вчинення стосовно нього протиправних дій з використанням можливостей глобальної мережі Інтернет, відомості за вказаним фактом внесено до ЖЄО № 605 від 11.07.2018 та долучено до матеріалів кримінального провадження №12017040000000000.

Установлено, що 03.03.2018 року в соціальній мережі Instagram Кирпою І.В. було здійснено замовлення товару, а саме туфлі, після чого сплачено його вартість у розмірі 3225 грн на банківську картку № 4149-5170-1284-0000, однак в подальшому замовлений товар так і не отримав.

За відомостями Київського управління кіберполіції ДКП НП України встановлено, що картковий рахунок відкритий в ПАТ «Райффайзен Банк Аваль» на ім’я Козлової (Кабацкая) Вікторії Вадимівни, 1.09.1993 р.н. користується мобільний номером +38(098)933-55-00.

Також встановлено, що кошти з карти одразу після переказу Кирпі І.В. знімались у банкоматі за адресою: м. Дніпро, вул. Б. Хмельницького, буд. 1.

Мобільний телефон Козлової В.В. +38(098)933-55-00, 26.05.2018 був активний за адресою: м. Дніпро, вул. Б. Хмельнцького, буд. 16.

Таким чином, для встановлення осіб, причетних до вчинення кримінального правопорушення щодо зазначеного громадянина, необхідно отримати тимчасовий доступ до інформації та документів, що перебувають у володінні ПАТ «Райффайзен Банк Аваль» (ЄДРПОУ 14305909), адреса: м. Київ, вул. Лескова, буд. 9.

Згідно з п. 2 ст.62 Закону України «Про банки та банківську діяльність», інформація щодо юридичних та фізичних осіб, яка містить банківську таємницю, зокрема стосовно операцій за рахунками конкретної юридичної особи або фізичної особи - суб'єкта підприємницької діяльності за конкретний проміжок часу, розкривається банками за рішенням суду. Крім цього, відповідно до ст.91 КПК України сама подія кримінального правопорушення підлягає доказуванню, яке полягає у збиранні, перевірці та оцінці доказів з метою встановлення обставин, що мають значення для кримінального провадження.

Беручи до уваги вищевикладене та враховуючи, що у матеріалах кримінального провадження вбачається наявність достатніх підстав вважати, що вказані документи мають суттєве значення для встановлення важливих обставин у кримінальному провадженні, керуючись ст. ст. 40, 84, 85, 92, 93, 131, 132, 159-164 КПК України, ст. 290 ЦПК України, ст. 60-62 Закону України «Про банки та банківську діяльність» -

ПРОШУ:

1. Надати тимчасовий доступ до інформації та оригіналів документів з можливістю вилучення (виїмки) їх копій, в тому числі на оптичних дисках для лазерних систем зчитування, слідчому слідчого відділу Кіровського ВП Дніпровського ВП ГУНП в Дніпропетровській області лейтенанту поліції Петренку Сергію Олександровичу, членам слідчо-оперативної групи у вказаному провадженні – інспектору ВПК у м. Києві Київського управління кіберполіції ДКП НП України лейтенанту поліції Рогову Руслану Максимовичу та інспектору відділу протидії кіберзлочинам в Дніпропетровській області Придніпровського УКП ДКП НПУ лейтенанту поліції Сичу Олександру Максимовичу, що перебувають у володінні ПАТ «Райффайзен Банк Аваль» (ЄДРПОУ 14305909), адреса: м. Київ, вул. Лескова, буд. 9, а саме:

- довідки-інформацію про рух грошових коштів по платіжним пластиковим карткам з зазначенням анкетних даних про особу, на яку оформлено картковий рахунок, повних даних про контрагентів і призначення платежів за період з 01.01.2017 року по теперішній час:
    1) 4149-5170-1284-7000;
- документи на відкриття зазначених карткових рахунків;
- даних систем відеоспостереження і фотофіксації зняття грошових коштів з банківських терміналів при оформленні та одержанні грошових коштів за рахунками:
    1) 4149-5170-1284-7000;

- інформацію отриману банком під час обслуговування зазначених платіжних карток, а саме номери телефонів, адреси проживання, місце роботи, рід занять, родинні зв'язки, особи які надають поруку, довірені (довірителі) особи;
- IP адрес підключення до Інтернет банкінгу, по зазначеним платіжним карткам, з інформацією про MAC-адреси комп'ютерів, з яких відбувалося з'єднання з системою, з зазначенням дати та часу за Київським часом в форматі: день, місяць, рік, години, хвилини, секунди таких з'єднань за відповідні періоди;
- надати інформацію стосовно наявних відкритих в ПАТ «Райффайзен Банк Аваль» додаткових банківських рахунків у осіб власників вищезазначених карток:

  1) 4149-5170-1284-7000;

  з наданням довідок-інформації про рух грошових коштів за період з моменту відкриття таких рахунків по теперішній час; даних систем відеоспостереження і фотофіксації зняття грошових коштів з банківських терміналів при оформленні та одержанні грошових коштів за наявними у вказаної особи рахунками з 01.01.2017 року по теперішній час.

2. Зобов'язати керівництво ПАТ «Райффайзен Банк Аваль» видати слідчому та членам СОГ у кримінальному провадженні вказану інформацію, речі та документи для здійснення тимчасового доступу.

3. З метою недопущення знищення або спотворення вказаної інформації та документів, які мають суттєве значення для кримінального провадження, керуючись ч. 2 ст. 163 КПК України розглянути дане клопотання без виклику представників ПАТ «Райффайзен Банк Аваль».

Додатки:

- витяг з Єдиного державного реєстру кримінальних проваджень № 12017040000000000 на 1 арк.;
- копії матеріалів, якими обґрунтовуються доводи клопотання на «___» арк.

Слідчий слідчого відділення
Кіровського ВП Дніпровського ВП
ГУНП в Дніпропетровській області
лейтенант поліції **С.О. Петренко**

ПОГОДЖЕНО
Прокурор відділу прокуратури
Дніпропетровської області
юрист 3 класу **С.Г. Бровін**

ДОДАТОК 4
Приклад протоколу огляду документа
(електронного носія інформації, на виконання п.7 ч.1 ст.162 КПК: тимчасовий доступ до інформації про зв'язок, абонента, надання телекомунікаційних послуг)

ПРОТОКОЛ ОГЛЯДУ ДОКУМЕНТА

місто Дніпро «___» _____ 2019 року

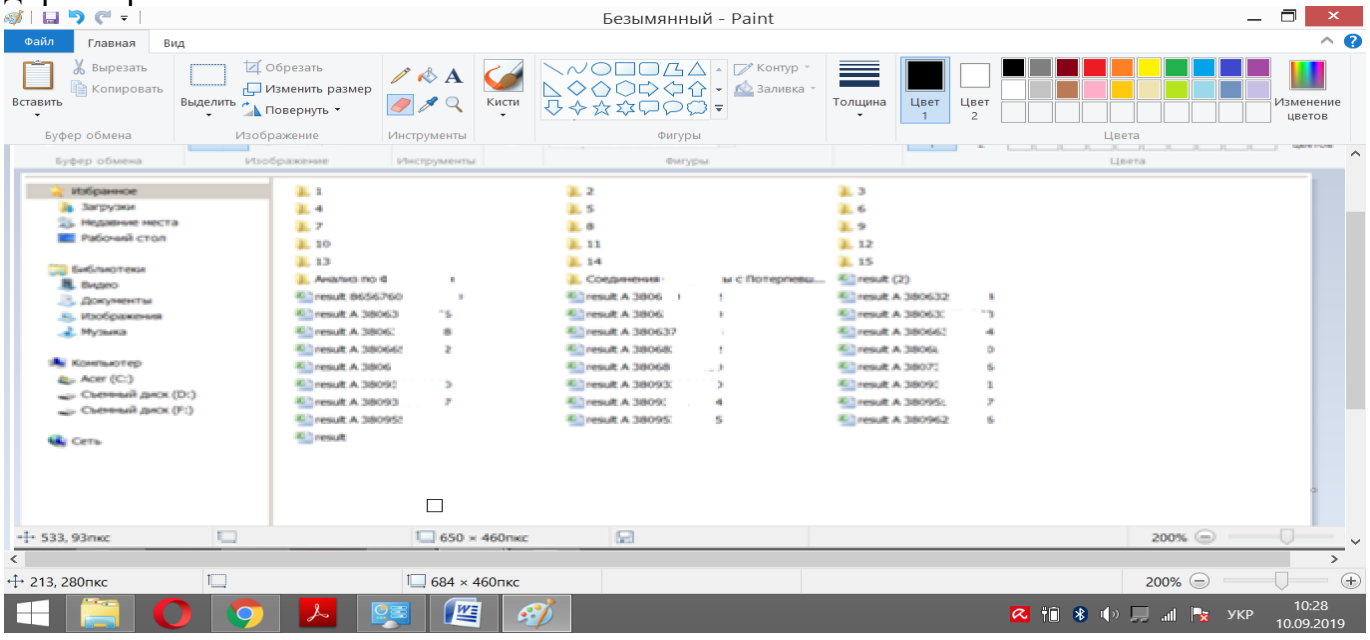
Огляд почато о «__» год. «__» хв. Огляд закінчено о «__» год. «__» хв.

Інспектор ВПК в Дніпропетровській області ПКП ДКП НП України, ст. лейтенант поліції Петренко Т.В. у приміщенні службового кабінету №00 розташованого за адресою: м. Дніпро, вул. Купки 23, за дорученням слідчого СУ ГУНП в Дніпропетровській області Рись О.О. №_____ від _____2019 року у кримінальному провадженні №12017040330000100, у відповідності до вимог статей 104, 105, 106, 107, 223 та 237 КПК України, із застосуванням ноутбуку ACER, без участі інших осіб, при природньому освітленні провів огляд матеріалів
_____
_____
_____

Так, під час огляду встановлено:

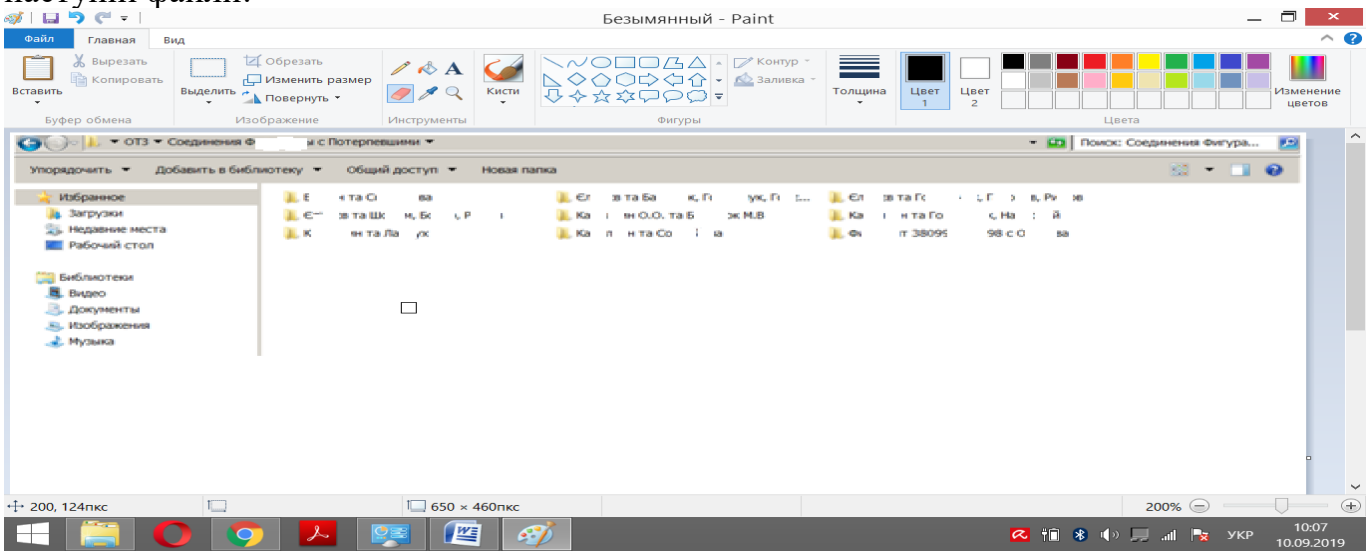
Оптичний носій інформації – диск систем лазерного зчитування кольору, виробника _____, з надписом на лицевій стороні диску «_____»

При зчитуванні інформації наявної на диску було встановлено наступні записані директорії пам’яті носія:



Всього 43 елементи загальним об’ємом пам’яті 29,0 МБ.

В каталозі під назвою «Соединения Купсика с Потерпевшими» містяться наступні файли:

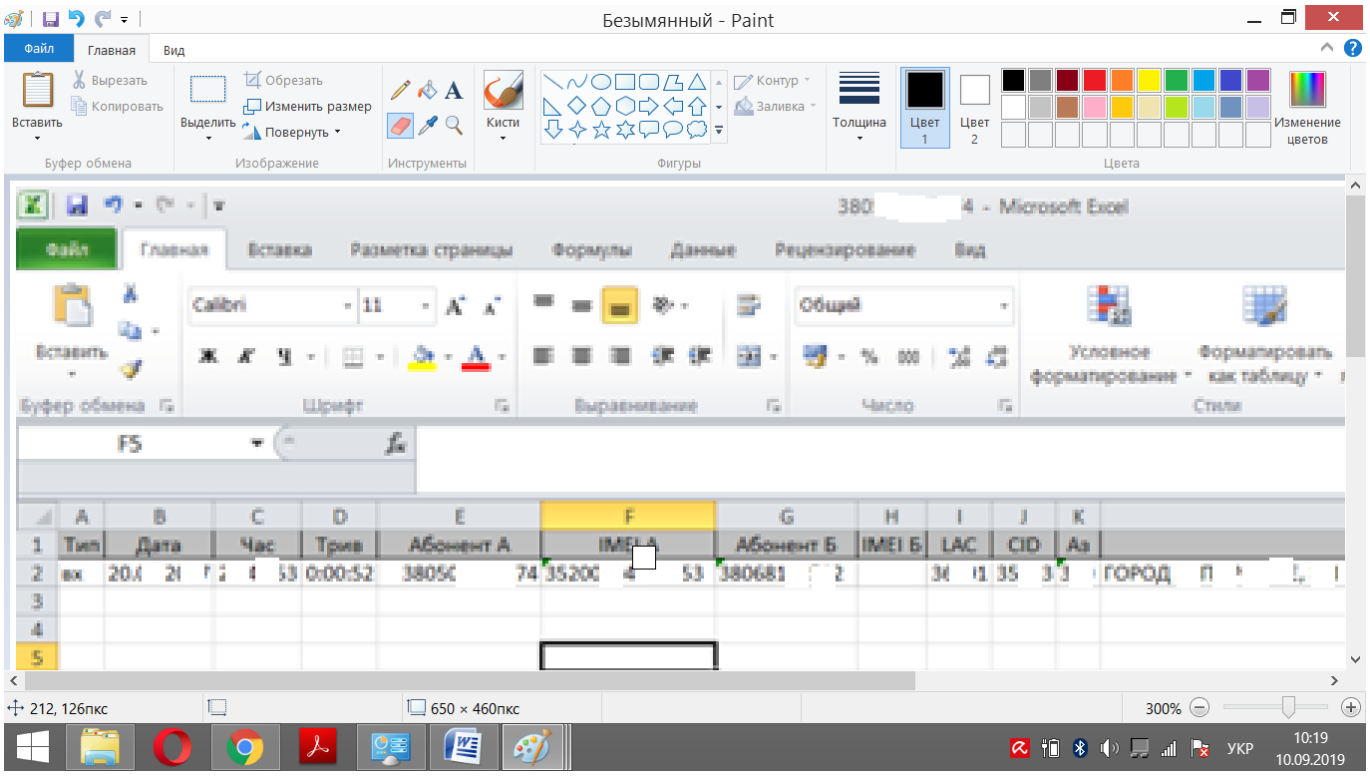


Всього 9 каталогів загальним об’ємом пам’яті 106 КБ.

При відкритті каталогу «Хакин та Солова», встановлені наступні файли: «380682060000.xlsx».

Файл представляє собою електронну таблицю об’ємом пам’яті 10,8 КБ в якій зазначається технічна інформація про зв'язок абонента «+380682060000» з іншими учасниками мережі.

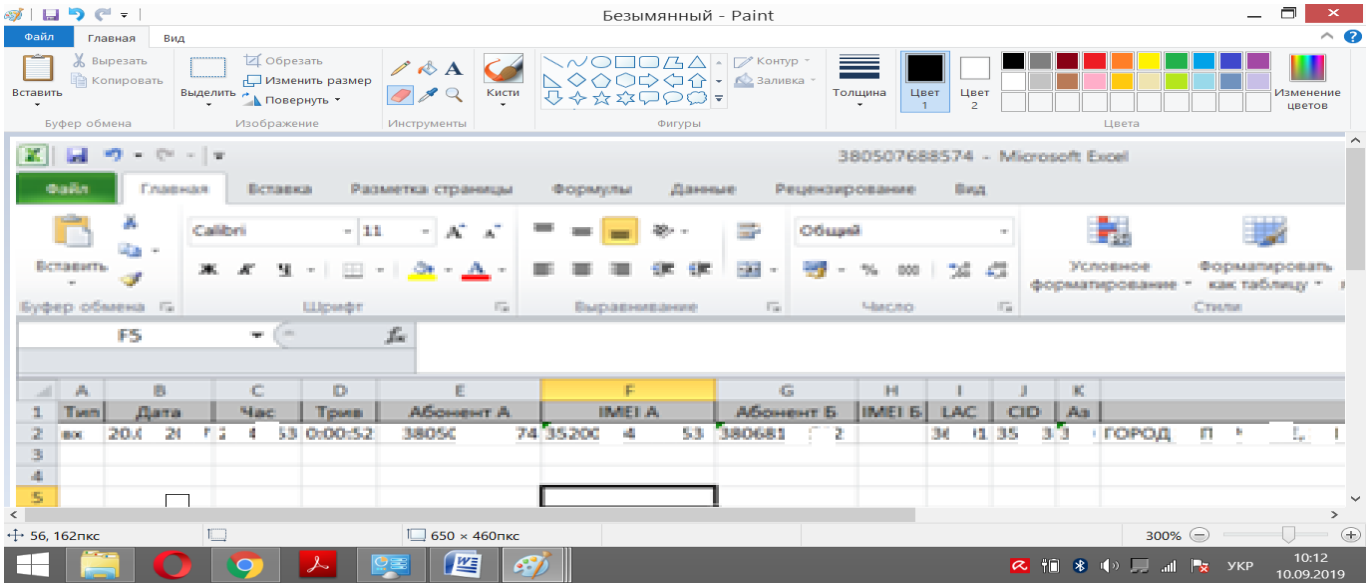
В ході огляду таблиці виявлений факт наявності телефонних розмов підозрюваного Калкіна Олександра Олеговича з потерпілим Соловою Іриною Олексіївною (+380661953000):



При відкритті каталогу «Калкин та Лах», встановлені наступні файли: «380507688000.xlsx».

Файл представляє собою електронну таблицю об’ємом пам’яті 11,4 КБ в якій зазначається технічна інформація про зв'язок абонента «+380507688000» з іншими учасниками мережі.

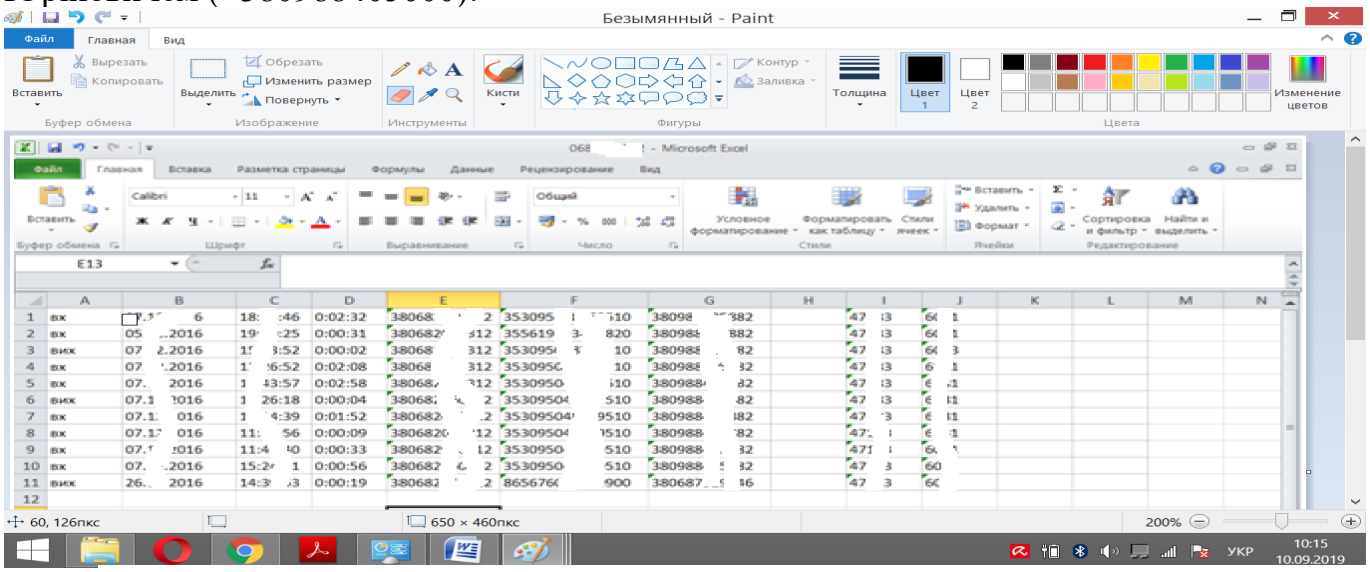
В ході огляду таблиці виявлений факт наявності телефонних розмов підозрюваного Калкіна Олександра Олеговича з потерпілим Лах Олегом Анатолійовичом (+380681005000):



При відкритті каталогу «Калкин та Гочик», встановлені наступні файли: «0682060000.xlsx».

Файл представляє собою електронну таблицю об’ємом пам’яті 11,2 КБ в якій зазначається технічна інформація про зв'язок абонента «+380682060000» з іншими учасниками мережі.

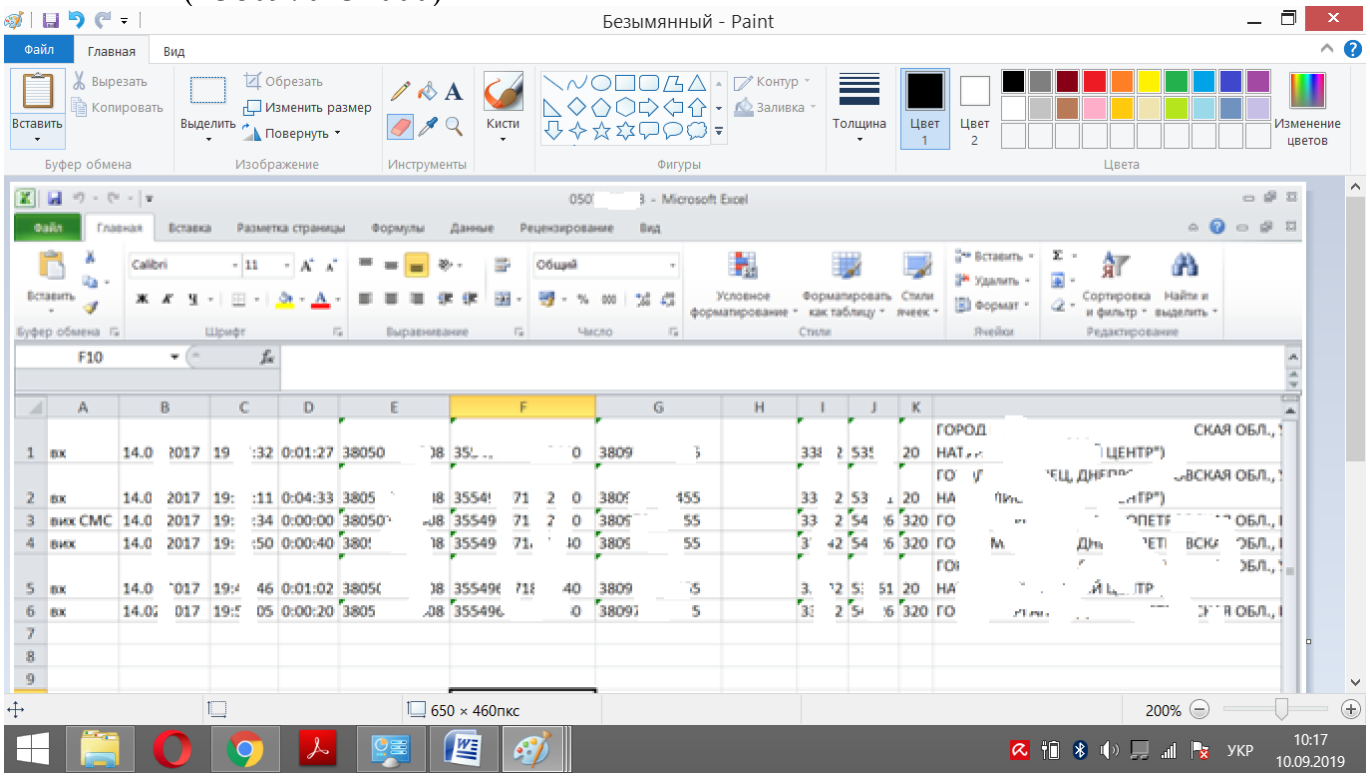
В ході огляду таблиці виявлений факт наявності телефонних розмов підозрюваного Калкіна Олександра Олеговича з потерпілим Голом Євгенієм Юрійовичем (+380988405000):



При відкритті каталогу «Хакин О.О. та Барак М.В», встановлені наступні файли: «0507690300.xlsx».

Файл представляє собою електронну таблицю об’ємом пам’яті 11,1 КБ в якій зазначається технічна інформація про зв'язок абонента «+380507000000» з іншими учасниками мережі.

В ході огляду таблиці виявлений факт наявності телефонних розмов підозрюваного Какіна Олександра Олеговича з потерпілим Бараком Миколаєм Веновичем (+380970131000):



Огляд провів:
Інспектор ВПК
в Дніпропетровській області
ПКП ДКП НП України
лейтенант поліції **С.В. Букін**

ДОДАТОК 5
Приклад протоколу огляду речі, документа

ПРОТОКОЛ ОГЛЯДУ РЕЧІ, ДОКУМЕНТА

м. Дніпро «___» липня 2017 року

Огляд почато о “10” год. “30” хв.
Огляд закінчено о “15” год. “00” хв.

Слідчий слідчого відділення Кіровського ВП Дніпровського ВП лейтенант поліції Репа Н.К. в кримінальному провадженні № 12017040440000100 від 07.04.2017 року, відкритого за ч. 3 ст. 190 КК України, у відповідності до ст.ст. 104, 105, 106, 234, 237, 223 КПК України в службовому кабінеті № ____ СУ ГУНП в Дніпропетровській області, провів огляд CD-R диску «Verbatim» вилученого 09.05.2018 р. в ПАТ КБ «Приват Банк» на підставі ухвали слідчого судді Бабушкінського районного суду м. Дніпропетровська.

При огляді використовувалась виписка про рух грошових коштів по картковому рахунку, вилученої в ПАТ КБ «Приват Банк» на підставі дозволу зазначеного суду.

В ході огляду встановлено:

CD-R диску «Verbatim», пошкоджень не має. Після перегляду інформації, записаному на вказаному диску за допомогою «DVD RAM», дисководу персонального комп’ютера, встановлено наявність на ньому фото файлів, на яких зафіксовано дії особи (осіб), який отримував за допомогою пластикової картки грошові кошти з банкоматів та здійснював інші банківські операції за допомогою даної картки в певний період часу. На фото знизу вказана інформація щодо дати часу проведення зйомки, номер банківської картки яка використовується для проведення банківської операції.

В ході проведення огляду фото файлів встановлено наступні факти:

1. Картковий рахунок 5168745600114000 відкритого в ПАТ КБ «Приват Банк» на гр. Куценко Олену Григоровну:

12.04.2017 о 12:36:17, 12:36:29, 12:36:51 фотокамера спостереження банкомата ПАТ КБ «Приват Банк» CADN 5100 (розташованого за адресою: смт. Кринички, вул. Комсомольська 9), зафіксувала зняття готівкою грошових коштів в сумі 800 грн. за допомогою платіжної картки № 5168745600114000 відкритої в ПАТ КБ «Приват Банк» на гр. Куценко О. Г.

За допомогою принтеру та персонального комп’ютера зроблено фотографії №№ 1-3 .

13.04.2017 о 08:06:59, 08:07:09, 08:07:41, 08:07:50 фотокамера спостереження банкомата ПАТ КБ «Приват Банк» CADN 8900 (розташованого за адресою: смт. Кринички, вул. Кірова 9), зафіксувала зняття готівкою грошових коштів в сумі 500 грн. за допомогою платіжної картки № 5168745600114000 відкритої в ПАТ КБ «Приват Банк» на гр. Куценко О. Г.

За допомогою принтеру та персонального комп'ютера зроблено фотографії №№ 4-7 .

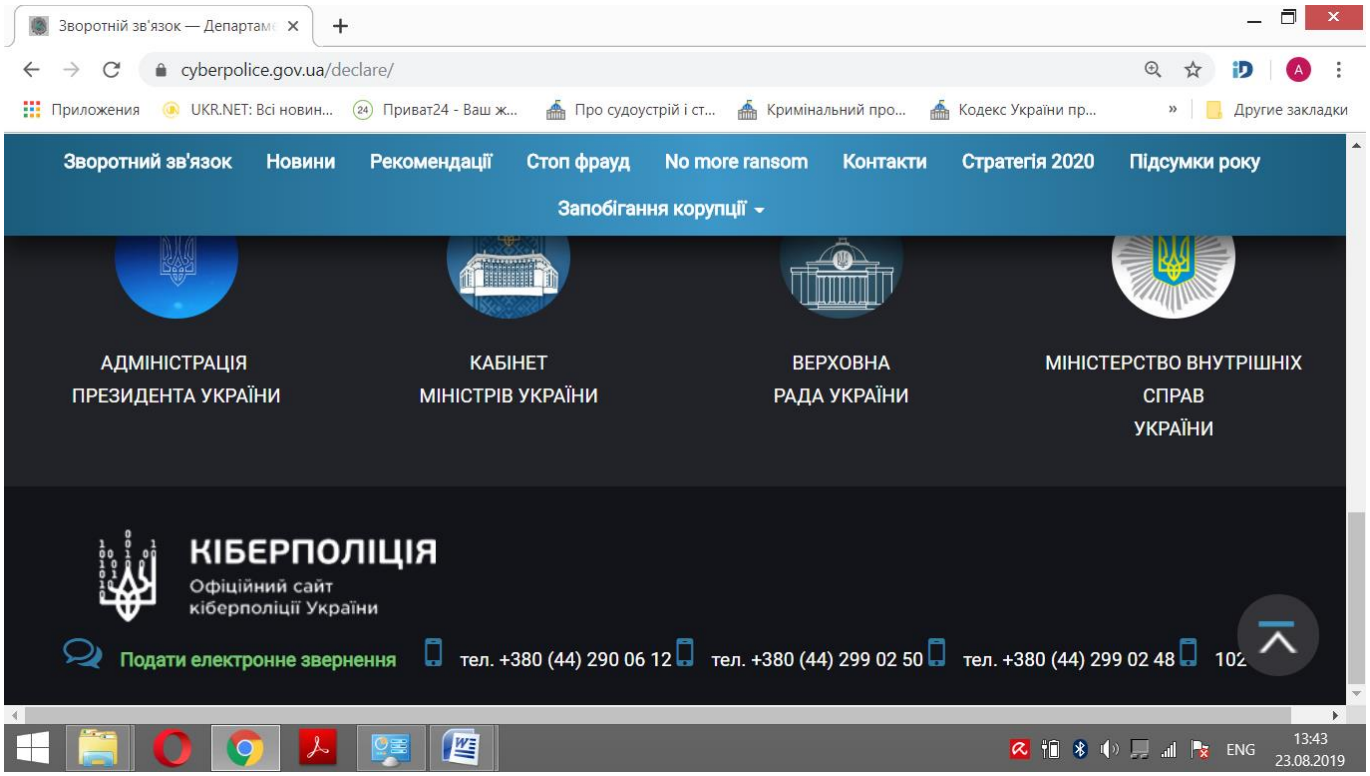
31.04.2017 о 11:22:27, 11:23:05, 11:23:13 фотокамера спостереження банкомата ПАТ КБ «Приват Банк» CAK 23000 (розташованого за адресою: м. Київ, вул. Здолбунівська 2), зафіксувала зняття готівкою грошових коштів в сумі 200 грн. за допомогою платіжної картки № 5168745600114900 відкритої в ПАТ КБ «Приват Банк» на гр. Куценко О. Г.

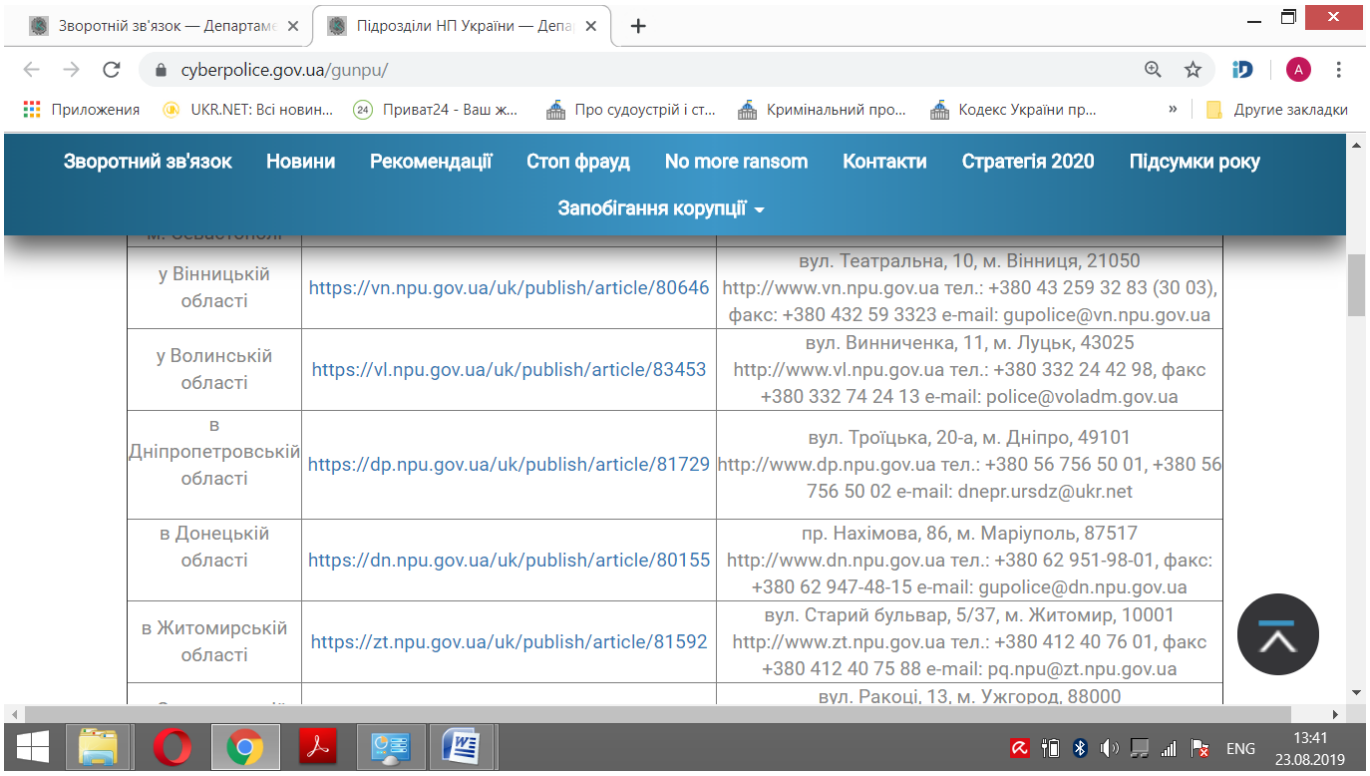
За допомогою принтеру та персонального комп'ютера зроблено фотографії №№ 8-10.

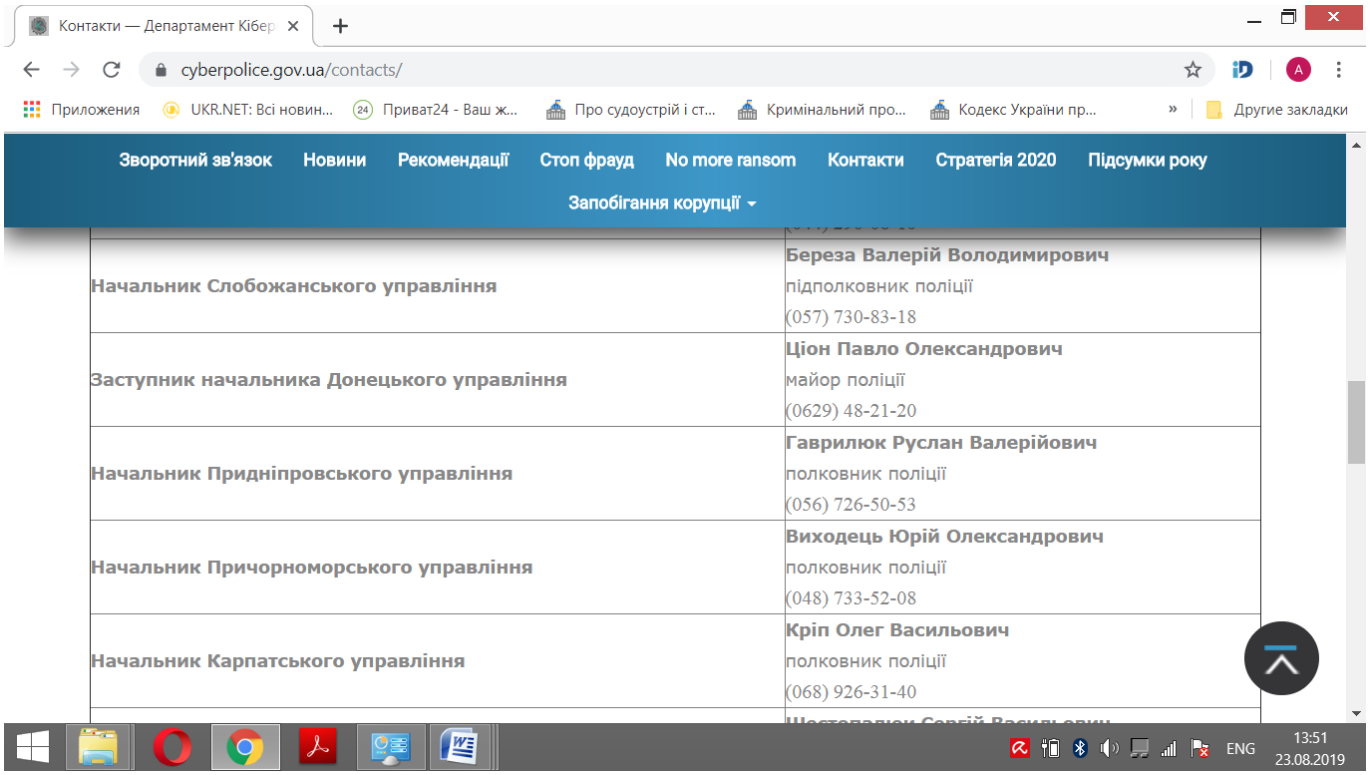
До протоколу огляду додається фото таблиця.

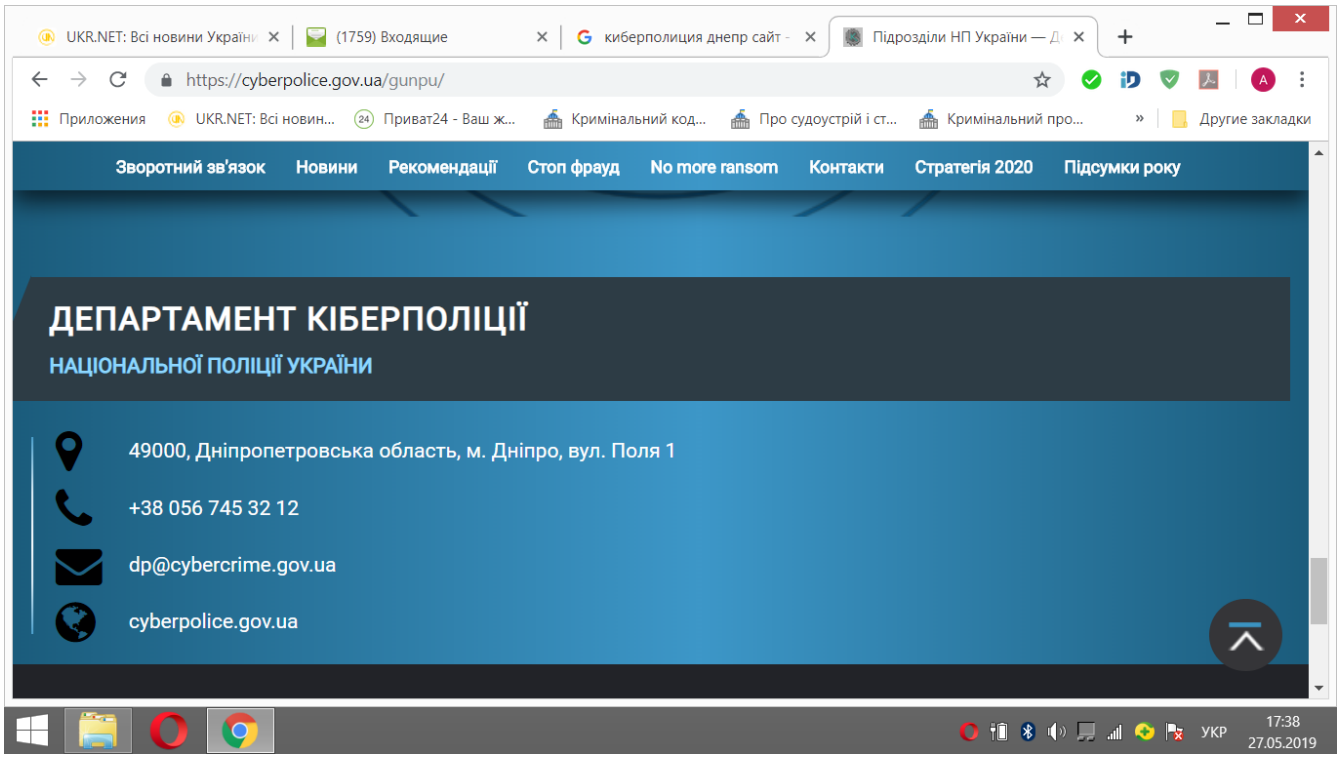
Огляд провів:
слідчий слідчого відділення
Кіровського ВП Дніпровського ВП
ГУНП в Дніпропетровській області
лейтенант поліції **Н.К. Репа**

ДОДАТОК 6
Скріншоти сайтів інформаційної та методичної підтримки






Контакти — Департамент Кібер
cyberpolice.gov.ua/contacts/
Приложения
UKR.NET: Всі новин...
Приват24 - Ваш ж...
Про судоустрій і ст...
Кримінальний про...
Кодекс України пр...
Другие закладки
Зворотний зв'язок
Новини
Рекомендації
Стоп фрауд
No more ransom
Контакти
Стратегія 2020
Підсумки року
Запобігання корупції
Начальник Слобожанського управління
Береза Валерій Володимирович
підполковник поліції
(057) 730-83-18
Заступник начальника Донецького управління
Ціон Павло Олександрович
майор поліції
(0629) 48-21-20
Начальник Придніпровського управління
Гаврилюк Руслан Валерійович
полковник поліції
(056) 726-50-53
Начальник Причорноморського управління
Виходець Юрій Олександрович
полковник поліції
(048) 733-52-08
Начальник Карпатського управління
Кріп Олег Васильович
полковник поліції
(068) 926-31-40
ENG
13:51
23.08.2019


UKR.NET: Всі новини Україн
(1759) Входящие
киберполиция днепр сайт -
Підрозділи НП України — Д
https://cyberpolice.gov.ua/gunpu/
Приложения
UKR.NET: Всі новин...
Приват24 - Ваш ж...
Кримінальний код...
Про судоустрій і ст...
Кримінальний про...
Другие закладки
Зворотний зв'язок
Новини
Рекомендації
Стоп фрауд
No more ransom
Контакти
Стратегія 2020
Підсумки року
ДЕПАРТАМЕНТ КІБЕРПОЛІЦІЇ
НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
49000, Дніпропетровська область, м. Дніпро, вул. Поля 1
+38 056 745 32 12
dp@cybercrime.gov.ua
cyberpolice.gov.ua
УКР
17:38
27.05.2019