2.2 Особливості проведення огляду місця події при розслідченні кіберзлочинів: згідно законодавства України

Основною, кінцевою метою, яку має досягти «DEFR (Digital Evidence First Responder)» [47] під час проведення огляду місця події по кримінальному провадженню за фактом вчинення кіберзлочину, є отримання доказів, що відповідають вимогам належності та допустимості.

Плануючи проведення слідчої дії, DEFR повинен перш за все чітко усвідомити: які саме об'єкти він повинен відшукати. При цьому слід керуватися перш за все національним кримінальним процесуальним законодавством. Крім того, стануть у нагоді національні стандарти у галузі захисту комп'ютерної інформації, створені на основі міжнародних стандартів, а також рекомендації навчально-методичних посібників, розроблених експертними, науковими та навчальними установами.

«Належними є докази, які прямо чи непрямо підтверджують існування чи відсутність обставин, що підлягають доказуванню у кримінальному провадженні, та інших обставин, які мають значення для кримінального провадження, а також достовірність чи недостовірність, можливість чи неможливість використання інших доказів» [55]. «Належність доказів – це можливість використання їх для встановлення у кримінальному провадженні фактичних даних, а також обставин, що підлягають доказуванню, в силу існуючого між ними кримінально процесуального взаємозв'язку» [57].

«Доказ визнається допустимим, якщо він отриманий у порядку, встановленому Кримінальним процесуальним кодексом України» [55]. Допустимість доказів визначається законністю джерела, умов і способів їх одержання [57].

Остаточне рішення щодо належності та допустимості доказів приймає суд, «під час їх оцінки в нарадчій кімнаті під час ухвалення судового рішення» [55].

Вченими також виділяються наступні властивості доказів (крім зазначених у кримінальному процесуальному законодавстві України): «достовірність

доказів – означає, що вони правильно, адекватно відображають матеріальні і нематеріальні сліди події, що досліджуються; достатність доказів – це властивість доказів, яка надає можливість покласти їх сукупність в основу процесуального рішення. Ця ознака застосовується лише щодо певної сукупності доказів» [57].

«Настановами для ідентифікації, збирання, здобуття та збереження цифрових доказів (Guidelines for identification, collection, acquisition and preservation of digital evidence) встановлено наступні принципи (вимоги), на яких ґрунтуються цифрові докази:

– важливість (є змога показати, що здобуті матеріали є надійними для розслідування – тобто що вони містять величини, які допомагають у розслідуванні конкретного інциденту, та що є доречна причина для їхнього здобуття. За допомогою аудиту та юрисдикції DEFR повинен мати змогу описати підтримані процедури та пояснити, як було прийнято рішення для здобуття кожного елемента);

– надійність (усі процеси, використані під час оброблення потенційних цифрових доказів, потрібно піддавати аудиту та вони мають бути збіжними);

– достатність (DEFR повинен ураховувати, що достатню кількість матеріалів має бути зібрано, щоб дозволити зробити належні дослідження. DEFR повинен мати змогу з використанням аудиту та законодавства надати пояснення, яку кількість матеріалу, загалом, розглянуто та які процедури використано для вирішення питання, яку кількість та який матеріал здобуто); можливість аудиту (незалежні аудитори або інші зацікавлені сторони повинні мати змогу оцінювати діяльність DEFR та DES – Digital Evidence Specialist);

– можливість аудиту (незалежні аудитори або інші зацікавлені сторони повинні мати змогу оцінювати діяльність DEFR та DES);

– збіжність (використання такої самої процедури та методики; використання таких самих інструментів та за таких самих умов; може бути повторено в будь-який час після первісного тесту);

– відтворюваності (використання такої самої методики вимірювання; використання інших інструментів та за інших умов; може бути відтворено в будь-який час після первісного тесту);

– відповідність юрисдикції (DEFR повинен мати змогу доказати відповідність юрисдикції усіх дій та методів, застосованих під час оброблення потенційних цифрових доказів)» [47].

Оскільки вказані принципи не закріплені у кримінальному процесуальному законодавстві України, формально їх дотримання не впливає на визнання доказів належними та допустимими. Але, на думку авторів, їх DEFR у ході проведення огляду місця події повинен їх дотримуватись, виходячи з наступного: настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів закріплені Державним стандартом ISO/IEC 27037:2017; з міркувань криміналістичної тактики, оскільки вказані настанови розроблені шляхом узагальнення досвіду розслідування кіберзлочинів.

Системний аналіз положень Кримінального процесуального кодексу України, які регулюють питання, пов’язані із доказами та доказуванням, дозволяє зробити висновок про те, що відносно належності та допустимості доказів існує тільки два варіанти: «так» чи «ні». Доказ не може бути визнано судом частково належним або частково допустимим. Тому під час проведення огляду місця події DEFR, приймаючи будь-яке рішення, повинен виходити з відповіді на питання: забезпечить прийняте рішення збирання належного та допустимого доказу або не забезпечить.

Вітчизняне кримінальне процесуальне законодавство передбачає всього чотири варіанти можливого процесуального джерела доказу, а саме «показання, речові докази, документи, висновки експертів» [55].

Оскільки допит, у ході якого можуть бути отримані показання, та призначення експертиз не відносяться до огляду місця події, у DEFR під час проведення огляду місця події фактично залишається два варіанти процесуальних джерел доказів: речові докази та документи. При проведенні огляду місця події DEFR повинен визначитись, чи може об’єкт, який є

потенційним джерелом доказів, відноситись до речових доказів або до документів.

«Речовими доказами є матеріальні об'єкти, які були знаряддям вчинення кримінального правопорушення, зберегли на собі його сліди або містять інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження, в тому числі предмети, що були об'єктом кримінально протиправних дій, гроші, цінності та інші речі, набуті кримінально протиправним шляхом або отримані юридичною особою внаслідок вчинення кримінального правопорушення» [55].

Законодавством України закріплено вимоги до зберігання речових доказів які мають зберігатись відповідно до «Порядку 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», затвердженого Постановою Кабінету Міністрів України № 1104 від 19.11.2012 р. «Про реалізацію окремих положень Кримінального процесуального кодексу України» [56].

Законодавство України надає наступне визначення документу:

1. «Документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. До документів, за умови наявності в них зазначених відомостей, можуть належати: 1) матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні); 2) матеріали, отримані внаслідок здійснення під час кримінального провадження заходів, передбачених чинними міжнародними договорами, згоду на обов'язковість яких надано Верховною Радою України; 3) складені в порядку, передбаченому цим Кодексом, протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії; 4) висновки ревізій та акти перевірок» [55].

2. «Документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі» [58].

3. «Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством. Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.» [59].

Таким чином, під час огляду місця події при розслідуванні кіберзлочинів DEFR повинен скерувати свої дії та дії групи, якою він керує, на пошук речових доказів та документів, вимоги яких зазначені в кримінальному процесуальному законодавстві України.

Законодавство України не встановлює, які саме об'єкти слід відшукувати та вилучати під час проведення оглядів місця події за фактом вчинення кіберзлочинів. Тому в даному випадку на допомогу DEFR мають прийти методичні рекомендації. Проаналізуємо позиції вчених з цього питання.

А.С. Білоусов слушно зазначає, що «в інформаційному розумінні електронний документ не відрізняється від інших, але без застосування апаратних і програмних засобів не можна отримати відомостей щодо змісту цього документа. Тому його можна назвати документом у загальному розумінні тоді, коли людина може сприйняти і зрозуміти його зміст; з огляду на специфіку комп'ютерних об'єктів, пов'язану з природою їх походження, варто вести мову про комп'ютерні об'єкти як різновид предметів матеріального світу, що можуть бути речовими доказами, тому запровадження такої категорії об'єктів в криміналістику й теорію кримінального процесу є своєчасним і відповідає реаліям сьогодення» [61].

Л. В. Борисова «при дослідженні слідової картини комп'ютерних злочинів (як одного з елементів їх криміналістичної характеристики) слушно виділяє

наступні її особливості: локалізація слідів інформації на пристроях; локалізація слідів інформації в програмних продуктах; локалізація слідів інформації на носіях» [66].

Н. С. Козак, у ході дослідження «слідової картини комп'ютерних злочинів, як елементу їх криміналістичної характеристики, розділяє вказані сліди на традиційні та нетрадиційні (інформаційні); вчена аналізує слідову картину комп'ютерних злочинів залежно від місця вчинення злочину із зазначенням джерел отримання інформації про дані сліди: 1) на носіях комп'ютерної інформації, з використанням яких діяв злочинець на своєму «робочому місці»; 2) на транзитних (мережних) носіях комп'ютерної інформації, за допомогою яких злочинець здійснював зв'язок з комп'ютером, що зазнав впливу; 3) на носіях інформації комп'ютера, на який було здійснено злочинний вплив» [62].

Отже, характерні особливості слідів підготовки, вчинення та приховування кіберзлочинів обумовлюють специфіку проведення слідчих дій по кримінальних провадженнях за фактами їх вчинення.