УДК 347.948.2

**П.П. Харківський**, *начальник сектору Науково-дослідного експертно-криміналістичного центру при ГУМВС України в Запорізькій області*

# КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА: ПРОБЛЕМНІ ПИТАННЯ

Розкрито проблеми та визначено вектор розвитку комп'ютерно-технічної експертизи в системі МВС України.

*Ключові слова:* комп'ютерно-технічна експертиза, проблемні питання, методичні рекомендації, програма підготовки.

Раскрыты проблемы и определен вектор развития компьютерно-технической экспертизы в системе МВД Украины.

The paper outlines current and future problems and goals of the IT-examination in the Forensic Service of the Ministry of Internal Affairs of Ukraine.

Стрімкий розвиток інформаційних технологій, електронних систем обробки даних і комп'ютерних мереж просуває громадянське суспільство вперед, водночас роблячи його вразливішим. Групи кіберзлочинців знаходять вразливі місця в нових комунікаційних технологіях і використовують їх у своїх злочинних цілях (розкрадання коштів, розповсюдження порнографії, створенням мереж для DDoS-атак[1] тощо).

Конвенція Ради Європи «Про злочинність в кіберпросторі», що набула чинності в липні 2006 року, є єдиним міжнародно-правовим документом у цій сфері. Її положення дозволяють державам сформувати повномасштабну законодавчу базу з боротьби з кіберзлочинністю. В українському законодавстві для забезпечення кібернетичної безпеки країни розроблено Закон України «Про основи національної безпеки України», а також проект Закону України «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» [1; 2].

Загрози кіберзлочинності в сучасних умовах розвитку українського суспільства ставлять нові завдання перед Експертною службою МВС України. Адже поява нових об'єктів, які використовують для вчинення злочину, і розширення кола експертних завдань потребують удосконалення експертних технологій, упровадження в експертну діяльність сучасних апаратних приладів, які застосовують у

[1] DDoS (скор. від англ. Distributed Denial of Service — відмова від обслуговування) — тип мережевої атаки, що базується на організації великої кількості запитів до сервера (ресурсу) з метою його відмови в обслуговуванні та відповіді на запити.

міжнародній практиці, постійного підвищення професійного рівня експертів-комп'ютерщиків.

Як свідчить аналіз експертної практики, відсутність чітких уявлень про предмет експертизи, її видовий розподіл, застаріла класифікація об'єктів експертизи тощо перешкоджають системній розробці методів експертного дослідження, налагодженню активної взаємодії між підрозділами, які проводять досудове розслідування злочинів.

Наприкінці 1990-х років О.І. Усов надав таку видову класифікацію комп'ютерно-технічної експертизи:

– апаратно-комп'ютерна експертиза;

– програмно-комп'ютерна експертиза;

– інформаційно-комп'ютерна експертиза (експертиза даних);

– комп'ютерно-мережева експертиза [3].

Суттю апаратно-комп'ютерної експертизи є діагностичне дослідження технічних (апаратних) засобів (об'єктів) комп'ютерної системи, визначення її функціональних можливостей, фактичного і початкового стану, технології виготовлення, експлуатаційних режимів тощо. До апаратних об'єктів належать: комп'ютери (персональні, сервери), периферійні пристрої, мережеві апаратні засоби, інтегровані системи (органайзери, пейджери, мобільні телефони тощо), вбудовані системи на базі мікропроцесорних контролерів, різні комплектуючі (апаратні блоки, плати розширення, мікросхеми тощо).

Програмно-комп'ютерна та інформаційно-комп'ютерна експертизи вирішують питання щодо наявності відповідної інформації на носіях пристроїв, її відновлення та дослідження.

Суть комп'ютерно-мережевої експертизи ґрунтується на функціональному призначенні комп'ютерних засобів, які реалізують мережеву інформаційну технологію. Окремо слід виділити експертизу з дослідження засобів телекомунікаційних систем і засобів як матеріальних носіїв, що містять відомості про факт чи подію, на основі яких модулюється технологія вчинення злочинів за виявленою слідовою інформацією.

Якщо з проведенням програмно-комп'ютерної та інформаційно-комп'ютерної експертиз особливих питань не виникає (наявні певні методики, методичні рекомендації, розроблені в системі МВС України, закуплені програмно-апаратні комплекси), то проведення апаратно-комп'ютерної та комп'ютерно-мережевої експертиз пов'язано з певними наявними проблемами, а саме відсутністю:

– методик і методичних рекомендацій з питань діагностики наданого на експертизу обладнання, дослідження об'єктів у межах комп'ютерно-мережевої експертизи, мобільних телефонів, планшетних комп'ютерів під керуванням операційних систем Android OS, iOS, а також навчальних тренінгів;

– належного (бажано уніфікованого) оснащення лабораторій відповідними сучасними апаратними пристроями;

– достатнього обсягу знань у експертів.

Таким чином, умови сьогодення потребують внесення певних коректив у зазначену класифікацію, а отже, більш виправданою сьогодні є така класифікація:

– експертиза комп'ютерної техніки стосовно її функціонування, технічного стану, придатності до вирішення певних завдань;

– експертиза носіїв інформації та програмних продуктів, у тому числі дослідження комп'ютерних програм, виявлення слідової інформації, відновлення видаленої інформації тощо;

– комп'ютерно-мережева експертиза, встановлення факту втручання у роботу комп'ютерних систем, пошук слідової інформації за вчиненими з використанням різних засобів зв'язку злочинами, дослідження мережевих операційних систем і програм для комп'ютерних мереж;

– експертиза мобільних телефонів і комунікаторів;

– експертиза відеореєстраторів.

Крім того, потребує вдосконалення і програма підготовки фахівців МВС України з проведення комп'ютерно-технічних експертиз з метою підвищення кваліфікації експертів, досконалого вивчення ними методологічних матеріалів, набуття високопрофесійних практичних навичок. Її зміст доцільно пов'язати із запропонованою класифікацією комп'ютерно технічної експертизи, з поетапним вивченням всіх п'яти напрямів.

Це дозволить експертам, які спеціалізуються на будь-якому з напрямів комп'ютерно-технічної експертизи, поетапно набути знань за кожним напрямом.

Насамперед це стосується поглиблених знань стосовно форматів зберігання даних на накопичувачах, характеристик окремих операційних систем, баз і банків даних, мов програмування тощо.

Зрозуміло, що специфічні особливості судової комп'ютерно-технічної експертизи слід враховувати не лише під час перепідготовки та підвищення кваліфікації судових експертів, а й під час добору кандидатів на посади експертів.

Розробка методик дослідження об'єктів комп'ютерно-технічної експертизи (у тому числі накопичувачів інформації, накладок на банкомати, диктофонів, мобільних терміналів) потребує від їх розробників (найчастіше експертів-практиків) як чіткого розуміння мети та завдань експертного дослідження, так і глибоких знань щодо принципів побудови, конструкції та функціонування досліджуваної техніки. Упродовж останніх років експерти МВС України розробили низку методик і методичних рекомендацій, що вже апробовані та впроваджені в експертну практику.

Згідно з чинним законодавством у висновку експерт повинен вказувати, яку методичну базу використано для дослідження, а отже, до питань її розробки та апробації слід підходити надзвичайно ретельно.

Крім того, активного розвитку потребує міжвідомча співпраця з питань розробки та впровадження нових наукових розробок.

Станом на червень 2014 року в експертній практиці МВС України і досі не використовують зареєстровані в Міністерстві юстиції України методичні матеріали з проведення комп'ютерно-технічних експертиз, у тому числі з:

– дослідження поштових програм і програм обміну електронними повідомленнями (реєстраційний код 10.9.02);

– пошуку та дослідження графічної інформації на персональному комп'ютері (реєстраційний код 10.9.03);

– дослідження інформації на цифрових носіях (реєстраційний код 10.9.07);

– дослідження роботи користувача персонального комп'ютера в мережі Інтернет (реєстраційний код 10.9.08);

– дослідження реляційних баз даних при проведенні судових комп'ютерно-технічних експертиз (реєстраційний код 10.9.03).

Підбиваючи підсумки, слід зазначити, що для подолання наявних проблем і забезпечення подальшого розвитку комп'ютерно-технічної експертизи доцільно вжити таких організаційно-практичних заходів:

– вирішити питання щодо впровадження в практичну діяльність експертних підрозділів МВС України зазначених методичних матеріалів Мін'юсту України, провести відповідні тренінги з їх використання;

– створити на базі ДНДЕКЦ МВС України банк даних програмно-апаратних комплексів і відповідних експертних програм, за потреби забезпечити доступ до них регіональних підрозділів;

– створити форум на кшталт селекторної наради для вирішення поточних проблемних питань (так званого мозкового штурму) для вирішення експертних завдань;

– періодично проводити тренінги з актуальних питань дослідження нових об'єктів комп'ютерно-технічної експертизи, у тому числі дослідження програмного забезпечення щодо виявлення слідової інформації, яку використовують зловмисники в мережі Інтернет;

– удосконалити програму підготовки фахівців з проведення комп'ютерно-технічної експертизи відповідно до запропонованої класифікації;

– враховуючи специфіку формування кадрового резерву, опрацювати питання щодо створення на базі Національної академії внутрішніх справ та Харківського університету внутрішніх справ груп підготовки фахівців за напрямом судової комп'ютерно-технічної експертизи.

**Список використаної літератури**

1. *Закон* України від 19 червня 2003 року № 964-IV «Про основи національної безпеки України» зі змінами та доповненнями [Електронний ресурс]. — Режим доступу : http://zakon4.rada.gov.ua/laws/show/964-15.

2. *Проект* Закону України «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» [Електронний ресурс]. — Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998.

3. *Усов А.И.* Методы и средства решения задач компьютерно-технической экспертизы : учеб. пособ. / А.И. Усов. — М. : ГУ ЭКЦ МВД России, 2002. — 200 с.