ЗАХИСТ ІНФОРМАЦІЇ

УДК 621.3

О.В. Рибальський,
доктор технічних наук, професор,
Л.М. Тимошенко,
А.Я. Мушак

КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА ТА ІНФОРМАЦІЙНА БЕЗПЕКА

У статті показаний взаємозв'язок між судовою експертизою комп'ютерних систем і телекомунікаційних мереж з проектуванням, створенням та дослідженнями комплексної системи інформаційної безпеки в таких системах і мережах. Запропоновано взаємне використання теоретичних та практичних напрацювань, реалізованих у обох науках.

***Ключові слова**: інформаційна безпека, криміналістика, судова експертиза, комп'ютерні системи, телекомунікаційні мережі.*

В статье показана взаимосвязь между судебной экспертизой компьютерных систем и телекоммуникационных сетей с проектированием, созданием и исследованиями комплексной системы защиты информации в таких системах и сетях. Предложено взаимное использование теоретических и практических разработок, реализованных в обеих науках.

***Ключевые слова**: информационная безопасность, криминалистика, судебная экспертиза, компьютерные системы, телекоммуникационные сети.*

An interaction between judicial examination of computer systems and telecommunication networks with planning, creation and researches of the complex system of information security in such systems and networks is considered. Mutual use of theoretical and practical investigations, realized in both sciences, is offered.

***Keywords**: information security, criminalistics, judicial examination, computer systems, telecommunication networks.*

Досить часто багато видів криміналістичних експертиз, пов'язаних з інформаційними процесами, щільно перетинаються з питаннями інформаційної безпеки і фактично є її інколи несподіваними аспектами. До таких експертиз можна віднести, наприклад, фоноскопічну експертизу, де криміналістичні питання достовірності записів одночасно є аспектом захисту державних органів і громадськості від дезінформації [1].

Уважний розгляд окремих криміналістичних питань, що вирішуються комп'ютерно-технічною експертизою (КТЕ), дозволяє і її віднести до таких експертиз. У окремий рід експертиз вона була виділена порівняно недавно, коли потреба в криміналістичних дослідженнях комп'ютерної техніки та оброблюваної в ній

інформації зумовила необхідність залучення кваліфікованих фахівців, проведення необхідних теоретичних напрацювань і створення спеціальних методик та інструментарію для її виконання. Слід зазначити, що як теорія, так і розробка методик й інструментарію для проведення такої експертизи нині знаходяться в початковій стадії свого розвитку, оскільки питання її виділення в самостійний вид експертиз почали підніматися лише в 90-х роках XX століття [2–4]. Об'єктами такої експертизи "є комп'ютерні засоби: апаратні об'єкти; програмні об'єкти та інформаційні об'єкти (дані)" [3, 4]. У [3, 4] наведене визначення предмета такої експертизи, яким "є факти й обставини, що встановлюються на основі дослідження закономірностей розробки та експлуатації комп'ютерних засобів, що забезпечують реалізацію інформаційних процесів, які зафіксовані в матеріалах кримінальної, цивільної справи, справи про адміністративне правопорушення".

У [5] відповідно до своїх завдань і специфіки дослідження визначені такі види експертиз:

– апаратно-комп'ютерна експертиза, предметом якої є фактичні дані, що встановлюються при дослідженні технічних (апаратних) засобів комп'ютерної системи;

– програмно-комп'ютерна експертиза, предметом якої є закономірності створення і використання програмного забезпечення комп'ютерної системи, представленої на дослідження;

– інформаційно-комп'ютерна експертиза, як основний різновид КТЕ, в предмет якої входить встановлення фактичних даних у ході "пошуку, виявлення, аналізу та оцінки інформації, підготовленої користувачем або породженої програмами для організації інформаційних процесів у комп'ютерній системі";

– комп'ютерно-мережева експертиза, предмет якої охоплює дослідження фактів та обставин, пов'язаних з використанням мережевих і телекомунікаційних технологій, за завданням слідчого (суду) для встановлення істини у справі;

– телекомунікативна експертиза, "предметом якої є фактичні дані, що встановлюються на основі застосування спеціальних знань при дослідженні засобів телекомунікацій та зв'язку як матеріальних носіїв інформації про факт або подію будь-якої кримінальної або цивільної справи".

Ми вважаємо, що такі види, як комп'ютерно-мережева експертиза (КМЕ) і телекомунікативна експертиза (ТКЕ) безпосередньо пов'язані з інформаційною безпекою як окремого підприємства або об'єкту, так і держави в цілому.

Зазначимо, що до загальних завдань інформаційної безпеки відноситься захист інформації від загроз будь-яких дій, спрямованих на порушення її цілісності, знищення, модифікацію або викрадення (як і створення та поширення дезінформації). Ці ж завдання ставляться як при розробці технічного завдання на проектування, так і при проектуванні комплексної системи захисту інформації (КСЗІ) в комп'ютерних системах і телекомунікаційних мережах. При цьому необхідно передбачити загальну низку напрямів захисту. До них, в першу чергу, слід віднести захист від несанкціонованого доступу, антивірусний захист, захист від витоку інформації по технічних каналах і тому подібне. Зрозуміло, для кожного окремого об'єкту захисту буде застосований певний профіль захисту, що передбачає індивідуальну деталізацію цих напрямів із врахуванням особливостей об'єкту захисту та інформації, що обробляється в системі. Дослідження забезпечення заданого рівня захищеності інформації у системі проводять за спеціальними

методиками, мета яких – визначення відповідності заданому профілю та рівню захисту.

А тепер розглянемо перелік питань [6], які, як правило, ставляться перед експертами при проведенні КМЕ та ТКЕ.

Чи відбувся доступ до телекомунікаційної системи та яким чином?

Чи використовувалися ресурси та інформація в телекомунікаційній системі та яким чином?

Чи була передача (отримання) інформації у телекомунікаційній системі та яким чином?

Чи є ознаки втручання в роботу телекомунікаційної системи?

Чи могли апаратні засоби об'єднуватися в телекомунікаційну мережу і за якими ознаками?

Встановити шляхи маршрутизації даних в телекомунікаційній системі.

Чи відповідають використовувані в програмах паролі та ідентифікаційні коди тим, що вводилися користувачем.

Яке програмне забезпечення використовується для функціонування комп'ютерної мережі? Чи є воно ліцензійним?

Яким чином здійснюється з'єднання комп'ютерів мережі? Чи є вихід на глобальні комп'ютерні мережі?

Які комп'ютери є серверами (головними комп'ютерами) мережі?

Яким чином здійснюється передача інформації на цьому підприємстві, установі, організації, фірмі або компанії по вузлах комп'ютерної мережі?

Чи використовуються для обмеження доступу до інформації комп'ютерної мережі паролі, ідентифікаційні коди? У якому виді вони використовуються?

Чи є збої в роботі окремих програм, окремих комп'ютерів при функціонуванні їх у складі мережі? Які причини цих збоїв?

Яка інформація передається, обробляється та модифікується з використанням комп'ютерної мережі?

Чи можливе використання телекомунікаційного засобу (устаткування) для зазначених цілей?

Яке призначення програмних продуктів? Для вирішення яких прикладних завдань вони призначені? Які способи введення та виведення інформації використовуються? Чи відповідають результати виконання програм потрібним діям?

Які програмні методи захисту інформації використовуються (паролі, ідентифікаційні коди, програми захисту і так далі)? Чи не робилися спроби підбору паролів або інші спроби неправомірного доступу до комп'ютерної інформації?

Яка інформація міститься у прихованих файлах?

Які технічні пристрої використовуються для захисту комп'ютерної інформації? Які їх технічні характеристики?

Чи є в наявності технічна документація на ці вироби? Відповідають параметри пристроїв тим, що викладені в документації?

Піддавалися чи ні засоби захисту програмній модифікації або фізичній дії? Використовуються чи ні штучні засоби захисту інформації?

Чи є на наданому магнітному носії стерті (видалені) файли? Якщо так, то які їх імена, розміри і дати створення, давність видалення?

Чи можливе відновлення раніше видалених файлів та який їх зміст?

Чи змінювався зміст файлів (вказати, яких саме), якщо так, то в чому це виявилося?

У якому вигляді зберігається інформація щодо результатів роботи антивірусних програм, програм перевірки контрольних сум файлів? Який зміст цієї інформації?

Чи є наявність збоїв у роботі окремих програм? Які причини цих збоїв?

У якому стані знаходяться файли, що містяться на магнітних носіях? Коли робилося останнє коригування цих файлів?

До яких саме файлів зверталася програма (вказати, яка саме), представлена на машинному носії, і які інформаційні файли вона створювала?

Чи міститься на цьому носії інформація (вказати, яка інформація цікавить) і якщо так, то яка саме?

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

Чи здійснювалися спроби знищення зазначеної інформації?

Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації?

Чи створена зазначена інформація на цьому комп'ютері або перенесена з іншого носія?

Яким чином інформація (вказати, яка саме) перенесена до досліджуваного комп'ютера (її носій)?

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

Яка дата і час створення (друк, видалення, занесення тощо) файлів (вказати зміст)?

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

Яким чином і коли це програмне забезпечення встановлене?

При аналізі цих питань стає очевидним їх перетин з цілями і завданнями, що виникають при проектуванні, розробці і дослідженнях КСЗІ. А у випадках реалізації загроз витоку інформації та виявлення "слабких місць" у захисті ці питання пов'язані найбезпосереднішим чином.

Таким чином, існує так званий науковий "стик" між вирішенням завдань інформаційної безпеки комп'ютерних систем і телекомунікаційних мереж і криміналістикою, що займається проведенням КМЕ і ТКЕ. З історії розвитку науки відомо, що найпродуктивніші наукові та технічні рішення завжди виникали і реалізовувалися на таких "стиках". Тому ми вважаємо, що є прямий сенс у взаємному використанні напрацювань кожної з цих наук.

При цьому слід зазначити, що, незважаючи на відносну "молодість" такої експертизи, в ній напрацьований цілком серйозний програмний інструментарій для практичних досліджень і вимірів, що видно з приведеного переліку питань, які вирішуються такою експертизою. Вважаємо, що багато що з цього інструментарію може використовуватися при дослідженнях реального рівня захищеності комп'ютерних систем і телекомунікаційних мереж.

При цьому зазначимо, що основною теоретичною базою криміналістики, до якої відноситься експертиза, є давно розроблена і багаторазово перевірена на практиці теорія криміналістичної ідентифікації, що дозволяє точно визначити вимоги до ідентифікаційних ознак і допустимість їх застосування у дослідженнях, використовуваних в кожній конкретній експертній методиці. Ми вважаємо, що її

Вважаємо, що і деякі методики, способи та засоби, що використовуються при створенні КСЗІ комп'ютерних систем і телекомунікаційних мереж (наприклад, методики профілізації, методики оцінки ризиків і тому подібне), цілком можуть використовуватися при проведенні КТЕ.

З усього наведеного вище можна зробити такі **висновки.**

1. Експертні завдання, що вирішуються при проведенні окремих видів комп'ютерно-технічної експертизи, близькі до завдань, що вирішуються при проектуванні, створенні та дослідженнях комплексних систем захисту інформації у комп'ютерних системах і телекомунікаційних мережах.

2. Методики, способи та інструментарій, використовувані в криміналістиці і захисті інформації, можуть взаємно доповнювати один одного.

3. Застосування теоретичної і практичної бази обох наук сприяло б їх взаємному збагаченню та розвитку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Рыбальский О.В.* Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе / О.В. Рыбальский, Ю.Ф. Жариков. – К. : НАВСУ, 2003. – 300 с.

2. Криминалистика : Учебник для ВУЗов / под ред. Р.С. Белкина. – М., 1999.

3. *Россинская Е.Р.* Судебная экспертиза в уголовном, гражданском и арбитражном процессе / Е.Р. Россинская. – М., 1996. – 459 с.

4. *Россинская Е.Р.* Судебная компьютерно-техническая экспертиза / Е.Р. Россинская, А.И. Усов. – М., 2001. – 306 с.

5. *Зинин А.М.* Судебная експертиза : Учебник / А.М. Зинин, Н.П. Майлис. – М., 2002. – С. 50.

6. *Меликов А.С.* Основания назначения судебной компьютерно-технической экспертизы (компьютерной экспертизы) / А.С. Меликов [Электронный ресурс]. – Режим доступа : http : // juranalytic.ru/2012/05/20/rassledovanie-kompyuternyx-i-drugix-prestuplenij/osnovaniya-naznacheniya-sudebnoj-kompyuterno-texnicheskoj-ekspertizy-kompyuternoj-ekspertizy/.

Отримано 05.02.2014