порівняльного матеріалу. Застосування методик при вирішенні такого класу завдань можливе лише при дотриманні певних вимог, які пред'являються до об'єкта дослідження. З урахуванням цього в межах класифікаційних завдань можуть бути умовно виділені завдання меншого ступеню спільності, а саме: видові, підвидові, групові й конкретні.

Першою підставою такої диференціації є вид об'єкту (текст); другою – склад тексту (буквений); третьою – об'єм буквеного тексту (великий); четвертою – ступінь виробленості почерку, яким він виконаний (великий, середній, низький).

Завдання судово-почеркознавчої експертизи можна диференціювати за ступенем складності. При визначенні питань, пов'язаних із систематизацією завдань за ступенем складності оперують поняттям «проблемність» завдання, яка характеризується ступенем визначеності. У визначеному завданні інформації достатньо для вирішення питання. Невизначене завдання характеризується недостатністю інформації, наявністю багатьох альтернатив. Відповідно в першому випадку завдання буде простим, в другому – складним.

В залежності від частоти повторюваності на практиці експертні завдання можуть бути поділені на типові та специфічні. До перших відносяться завдання, які зустрічаються часто, до других – відносно рідко.

Отже, розглянуті підстави систематизації завдань тісно пов'язані між собою. Серед експертних завдань більшого ступеню спільності можуть бути типові, тобто такі, що зустрічаються часто в експертній практиці та специфічні, які зустрічаються рідко. В свою чергу, типові завдання можуть бути як простими, так і складними.

Нізовцев Ю.Ю.

ЩОДО ПРОБЛЕМНИХ ПИТАНЬ ВИЗНАЧЕННЯ ТЕРМІНУ «ШКІДЛИВИЙ ПРОГРАМНИЙ ЗАСІБ»

Термін «шкідливий програмний засіб» (далі ШПЗ) є одним із найбільш суперечливих та дискусійних з огляду на його поширеність в інформаційних джерелах.

У Кримінальному кодексі України термін «шкідливий програмний засіб» детально не визначений. Але попри це стаття 361-1 КК України передбачає покарання за «Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку». Отже, стаття 361-1 КК України, визначаючи призначення шкідливого програмного засобу, не надає переліку (вичерпного чи невичерпного) ознак шкідливого програмного засобу.

Зазвичай при розслідуванні злочину, передбаченого ст. 361-1 КК України, слідчий призначає комп'ютерно-технічну експертизу, на вирішення якої ставить питання щодо віднесення виявлених програм до шкідливих

програмних засобів. Разом з тим, відсутність чіткого визначення терміну «шкідливий програмний засіб» обумовлює відсутність єдиного підходу до проведення такого роду експертиз. У кожному випадку судовий експерт вимушений на власний розсуд, спираючись на власні знання та досвід, визначати, які ознаки програми є визначальними для віднесення її до ШПЗ, а які є несуттєвими. Внаслідок цього різні експерти можуть дійти різних висновків щодо однієї і тієї самої програми.

На думку автора, можна умовно виділити три взаємопов'язані групи причин, які обумовлюють складнощі практичного застосування наведеного у ст. 361-1 КК України терміну «шкідливий програмний засіб». По-перше, це відсутність чіткого визначення ШПЗ у названій статті КК або посилання на інший нормативний документ, який би містив це визначення. По-друге, ст. 361-1 КК не розкриває зміст терміну «втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» (зазначене визначення відсутнє і в ст. 361 КК), а також що розуміється під «несанкціонованістю» такого втручання. По-третє, у нормативній базі існують кілька споріднених понять без чіткої диференціації між ними, а саме: програма, програмний засіб, програмне забезпечення, програмний продукт. Крім того, в низці нормативних документів закріплені визначення окремих різновидів програм, які за багатьма ознаками можуть вважатися шкідливими (комп'ютерний вірус, програмна закладка, люк, троянський кінь), без вказівки на співвідношення цих визначень із визначенням загального поняття «шкідливий програмний засіб» [1, 2].

Проаналізувавши наукові джерела, можна дійти висновку, що і в науковців не існує єдиного підходу до визначення ШПЗ. Окремі вчені застосовують термін «шкідливий програмний засіб» або його різновиди, не розкриваючи їх змісту. Наприклад, О.К. Юдін у своїй праці «Інформаційна безпека. Нормативно-правове забезпечення» одночасно застосовує терміни «шкідлива програма», «шкідливе програмне забезпечення» та «шкідливий код», при цьому не надаючи визначення жодному з них [3]. Уникають чіткого визначення як загального терміну ШПЗ, так і його різновидів також Б.В. Кузьменко та Ю.О. Заїка [4]. На думку автора, такий підхід є невірним, оскільки застосування термінології, пов'язаної з ШПЗ, без розкриття її змісту та формулювання дефініцій може призвести до хибного розуміння зазначених термінів і, таким чином, невірного тлумачення думки науковця в цілому.

Деякі вчені схильні надавати визначення різновидам ШПЗ, не надаючи загального визначення даного терміну. Наприклад, М.І. Мельник та М.І. Хавронюк не визначаючи ШПЗ, дають визначення таким його різновидам, як «комп'ютерні віруси», «програми, призначені для нейтралізації паролів та інших засобів захисту комп'ютерних програм чи комп'ютерної інформації від несанкціонованого доступу» та «програми-шпигуни» [5]. Аналогічного підходу дотримується О.М. Черкун [6], надаючи визначення лише окремим різновидам шкідливих програм: «комп'ютерний

вірус», «комп'ютерний черв'як», «троянська програма», «вірус-вимагач». На думку автора, такий підхід також є невірним. По-перше, за відсутності загального визначення ШПЗ стає незрозумілим, за якими критеріями окремі його різновиди об'єднуються під цим загальним терміном. По-друге, надаючи визначення кільком різновидам ШПЗ, осторонь залишаються інші різновиди, а отже і їх ознаки. По-третє, наразі диференціація між різними видами ШПЗ є дуже умовною. Це пов'язано з тим, що останнім часом зловмисниками створюється все більше універсальних шкідливих програмних засобів, які можуть об'єднувати в собі властивості одночасно кількох «класичних» різновидів ШПЗ. Часто застосовується модульна побудова ШПЗ, коли на атакований комп'ютер встановлюється невелика програма-агент, яка потім завантажує той чи інший модуль ШПЗ з необхідним зловмисникові функціоналом.

Іншого підходу дотримуються О.П. Войтович, В.О. Вітюк, В.А. Каплун, які у своїй статті [7] навели визначення ШПЗ, приведене також на сайті Тернопільського національного технічного університету імені Івана Пулюя [8]. Відповідно до цього визначення, під терміном «шкідливе програмне забезпечення» розуміють програмні засоби, що несанкціоновано впроваджують у комп'ютерну систему і які здатні викликати порушення політики безпеки, завдавати шкоди інформаційним ресурсам, а в окремих випадках – і апаратним ресурсам комп'ютерної системи. Однак і це визначення не позбавлене недоліків. Корисним є наведення такої ознаки ШПЗ, як «порушення політики безпеки». Разом з тим, не розкривається така ознака, як «несанкціонованість впровадження у комп'ютерну систему», а також не розкривається, що розуміється під «завданням шкоди інформаційним та апаратним ресурсам комп'ютерної системи».

Більш розгорнуте визначення ШПЗ надають А.І. Кунинець та Ю.І. Грицюк [9], відповідно до якого шкідливе програмне забезпечення (англ. *malware, malicious software* – шкідлива програма, зловмисне програмне забезпечення) – будь-яке програмне забезпечення, призначене для отримання несанкціонованого доступу до обчислювальних ресурсів самого комп'ютера або до інформаційних ресурсів, які зберігаються на ньому, призначене для несанкціонованого власником їх використання чи спричинення шкоди (нанесення збитку) власникові комп'ютера, інформації чи комп'ютерній мережі шляхом копіювання, спотворення даних, видалення або підміни інформації.

На думку автора, зазначене визначення є одним з найбільш вдалих, але разом з тим і не позбавленим недоліків, якщо розглядати його з точки зору застосування у судово-експертній практиці, оскільки на його основі складно виділити чіткі критерії віднесення досліджуваних програм до ШПЗ.

Отже, залишається актуальною необхідність вироблення чіткого визначення терміну «шкідливий програмний засіб», яке б ґрунтувалося на положеннях нормативних актів і містило в собі достатній перелік ознак, які могли б використовуватися судовими експертами під час проведення відповідних експертиз.

Список використаних джерел

1. Державний стандарт України (ДСТУ 3396.2-97) Захист інформації. Технічний захист інформації. Терміни та визначення. Чинний від 01.01.1998р. [Електронний ресурс]. – Режим доступу: http://tzi.com.ua/478.html

2. Нормативний документ системи технічного захисту інформації (НД ТЗІ) 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999р. № 22.) [Електронний ресурс]. – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article;jsessionid=FC395885747985DC56DE509319440413.app1?showHidden=1&art_id=102106&cat_id=46556&ctime=1344502446343

3. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення. – К., 2010 – 708 с. іл..

4. Кузьменко Б.В., Заїка Ю.О. Типи сучасного особливо небезпечного (шкідливого) програмного забезпечення: правові та технічні аспекти / Юридична наука. – № 7/2013. – С. 29-35.

5. Науково-практичний коментар Кримінального кодексу України / За ред. М.І. Мельника, М.І. Хавронюка. – 7-ме вид., переробл. та допов. – К.: Юридична думка, 2010. – 1288 с.

6. Черкун О.М. Сучасні технології комп'ютерної безпеки. Монографія. Науковий керівник Р.М. Літнарович. МЕГУ. – Рівне, 2012. – 90 с.

7. Войтович О.П., Вітюк В.О., Каплун В.А. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів / Інформаційні технології та комп'ютерна інженерія, 2013. – № 3. – С. 4-6.

8. Шкідливе програмне забезпечення / Розділ Wiki офіційного сайту Тернопільського національного технічного університету імені Івана Пулюя. [Електронний ресурс]. – Режим доступу: http://wiki.tntu.edu.ua/Шкідливе_програмне_забезпечення

9. Кунинець А.І., Грицюк Ю.І. Інформаційні загрози та проблеми забезпечення інформаційної безпеки промислових компаній / Науковий вісник НЛТУ України. – 2013. – Вип. 23.2. – С. 352-360.

Охріменко О.І.

СТАН ТА ПЕРСПЕКТИВИ ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ В СБУ, ОКРЕМІ ПРОБЛЕМНІ ПИТАННЯ

Експертні дослідження в рамках завдань, отриманих від органів досудового слідства і суду, а також оперативних підрозділів здійснюються силами центру судових і спеціальних експертиз (ЦССЕ) з дислокацією в місті Києві та шістнадцяти відокремлених експертних підрозділів (ВЕП) в регіонах, відповідно до зон обслуговування.

Зазначені дослідження проводяться за п'ятнадцятьма видами судових експертиз в рамках 34 експертних спеціальностей. Ближчим часом