processes that preceded and then accompanied the explosion process, appropriate scientific and methodological framework should be developed, which is currently unavailable. For the development of this scientific and methodological base in KNIISE is carried out the research work on the topic: "Guidelines for the expert studies the circumstances of explosions of oxygen cylinders".

УДК 343.98

Ю. Ю. Нізовцев
головний спеціаліст (експерт)

Український науково-дослідний інститут
спеціальної техніки та судових експертиз
Служби безпеки України

ПРОБЛЕМНІ ПИТАННЯ ЩОДО ВІДНЕСЕННЯ ПРОГРАМ ДО ШКІДЛИВИХ ПРОГРАМНИХ ЗАСОБІВ

Розглянуто проблемні питання щодо встановлення призначення програми як шкідливого програмного засобу в рамках судової експертизи. Окреслено межі компетенції експерта, а також розмежування повноважень експерта та слідчого у цьому питанні.

Стрімкий розвиток інформаційних технологій та їх впровадження у все більшу кількість сфер суспільного життя обумовило появу нової небезпеки для суспільства – кіберзлочинності. Одним з найбільш дієвих інструментів, що застосовуються кіберзлочинцями, є шкідливі програмні засоби, або англ. Malware.

Питанням протидії кіберзлочинності, у тому числі розслідуванням злочинів, пов'язаних з використанням шкідливих програмних засобів, присвятили свої роботи Д. С. Азаров, П. Д. Біленчук, А. С. Білоусов, В. М. Бутузов, В. О. Вітюк, О. П. Войтович, В. Д. Гавловський, Ю. В. Гаврилін, В. О. Голубєв, С. М. Гусаров, В. А. Каплун, М. В. Карчевський, Н. С. Козак, В. В. Крилов, С. А. Кузьмін, А. А. Музика, Л. П. Паламарчук, Д. В. Пашнєв, Н. А. Розенфельд, М. В. Рудик, Л. М. Соловйов, Т. Л. Тропіна, В. С. Цимбалюк, В. П. Шеломенцев та інші вчені. Разом з тим, досі залишаються недослідженими роль та можливості судової експертизи щодо віднесення програми до шкідливих програмних засобів.

За існуючою практикою, під час доказування події злочину, передбаченого ст. 361-1 Кримінального кодексу України (далі – КК України), слідчі, як правило, призначають судову комп'ютерно-технічну експертизу, на вирішення якої ставлять питання: чи є надана на дослідження програма шкідливим програмним засобом? Актуальність проблеми полягає в тому, що досі

залишаються невизначеними критерії «шкідливості» програми та межі компетенції судового експерта щодо встановлення цих критеріїв. У зв'язку з цим спробуємо проаналізувати чинне законодавство та з'ясувати можливості судового експерта щодо віднесення досліджуваної програми до шкідливих програмних засобів.

Дефініція шкідливих програмних засобів наводиться у ст. 361-1 Кримінального кодексу України, яка визначає, що шкідливі програмні засоби призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку [1].

Як правило, досліджувати шкідливі програмні засоби експертам доводиться у двох випадках.

По-перше, для встановлення належності програми до шкідливих програмних засобів. Таке дослідження є невід'ємною складовою доказування за ст. 361-1 КК України, яка передбачає відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

По-друге, коли необхідно встановити, чи було можливо за допомогою досліджуваної програми здійснити ті чи інші шкідливі дії. Як правило, такі дослідження проводяться під час розслідування злочинів, передбачених ст. 361 КК України, яка передбачає відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку [1].

Тобто, у першому випадку шкідливий програмний засіб є предметом злочину, а в другому – знаряддям чи засобом.

Якщо вести мову про встановлення функціональних можливостей програми, тобто, з'ясування, чи можливо за її допомогою здійснити ті чи інші дії, то можна дійти висновку, що серйозних проблем тут нема. Шляхом дослідження роботи програми у віртуальному середовищі та/чи дослідженням дизасембльованого коду програми кваліфікований експерт, який має достатні знання в галузі реверсінженерії, може встановити функціонал програми та відповісти на питання ініціатора проведення експертизи.

Іншим чином складається ситуація у випадку встановлення належності досліджуваної програми до шкідливих програмних засобів. Необхідно зазначити, що встановлення «шкідливості» програми є досить складним питанням. Ще у 1998 році Євген Касперський зазначав [2, с. 13], що основна складність, яка виникає при спробах дати чітке визначення комп'ютерного вірусу полягає у тому, що практично всі відмінні риси вірусів (вбудовування в інші об'єкти, прихованість, потенційна небезпека тощо) або притаманні іншим програмам, які ніяким чином не є вірусами, або існують віруси, які не містять вказаних відмінних рис.

Також у контексті визначення «шкідливості» програми варто зазначити, що в окремих випадках корисна програма може вдатися до шкідливих дій.

Це може трапитися, наприклад, внаслідок помилок у коді програми. Так, після оновлення антивірусних баз у жовтні 2013 року «Антивирус Касперского 6.0 для Windows Workstations» під управлінням операційної системи Windows 7 Service Pack 1 (32-bit) детектував системний файл «tcpip.sys» як шкідливий, поміщав цей файл в карантин і видаляв гілки реєстру, які відносяться до даного файлу [3]. І цей випадок непоодинокий, варто пригадати, як антивірус AVG ідентифікував системний файл «user32.dll» в операційній системі Windows XP як троян [4], як безкоштовний антивірус «Microsoft Security Essentials» ідентифікував веб-браузер «Google Chrome» як троянську програму «PWS: Win32 / Zbot», призначену для розкрадання паролів [5] та інші випадки. Якщо дослідити наведені програми з помилками у коді суто з технічної точки зору, можна дійти висновку, що вони були призначені для шкідливих дій. Разом з тим, умисел розробників зовсім не був спрямований на якісь протизаконні дії.

Не слід також забувати, що й без помилок у коді корисна програма може завдати шкоди, будучи запущеною з помилковими параметрами. В якості прикладу можна навести некоректний запуск утиліт для роботи з дисками («fdisk», «format» тощо), який може призвести до знищення всієї інформації на диску.

Як свідчить практика, зазвичай ініціатор експертизи питає, чи є надана на дослідження програма шкідливим програмним засобом? Отже, якщо слідувати логіці ініціатора експертизи, під час проведення дослідження експерт повинен встановити призначення програми та перевірити, чи відповідає це призначення описаному у диспозиції ст. 361-1 КК України.

На думку автора, досліджуючи проблему встановлення експертним шляхом призначення програми для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, можна умовно виділити дві складові: по-перше, це можливість експертним шляхом встановити початкове призначення програми, а по-друге, це можливість встановити призначення цієї програми саме для несанкціонованих дій.

Розглядаючи можливості експертним шляхом встановити початкове призначення програми, потрібно зазначити, що не існує однозначного зв'язку між функціональними можливостями програми та її призначенням, оскільки одну і ту саму функцію можна використовувати з різною метою. Наприклад, утиліту «ping» [6, 7] можна застосувати як для перевірки досяжності віддаленого мережевого вузла, так і для здійснення віддаленої атаки на відмову в обслуговуванні [8]. Програму для тестів на проникнення [9, 10] можна застосувати як для легальної перевірки захищеності сервера, так і для несанкціонованого втручання в його роботу.

Призначення програми, зазвичай, закладається ще на початковому етапі її розробки і, як правило, зазначається у технічному завданні [11]. Також у технічному завданні розкриваються вимоги до функціональних характерис-

тик, яким повинна задовольняти програма задля того, щоб відповідати своєму призначенню. Але надання експерту на дослідження разом з програмою технічної документації на її створення є скоріше винятком, ніж правилом (це не стосується випадків дослідження широковідомого програмного забезпечення, інформацію про яке легко знайти в інформаційно-довідкових джерелах, наприклад «MS Windows», «MS Office», «Adobe Photoshop» тощо). Крім того слід зазначити, що програми з однаковим призначенням можуть мати дещо різні функціональні характеристики чи навіть базові принципи роботи. Одним з прикладів таких програм є утиліти «Tracert» (входить до складу операційної системи Windows) та «Traceroute» (входить до складу Unix/Linux-подібних операційних систем) [12]. Призначенням обох програм є відображення шляху інформаційного пакету до певного вузла в мережі Інтернет, та й виведення на екран результатів роботи «Tracert» та «Traceroute» дуже схоже. Робота «Tracert» заснована на протоколі icmp [13], а якщо точніше – на відправці пакетів ICMP Echo-Request [14]. Icmp є протоколом третього рівня мережевої моделі OSI [15]. Таким чином, застосувати «tracert» із вказівкою певного порту неможливо. «Traceroute» функціонує за іншим принципом, її дія грунтується не на ICMP Echo-Request, а на відправці udp-пакетів [16] й отриманні повідомлення про доступність/недосяжність порту [17]. Завдяки цьому утиліта «traceroute» дозволяє відпрацювати трасування із вказівкою конкретного порту призначення на кінцевому мережевому вузлі.

Отже, дві програми однакового призначення мають різні функціональні можливості.

Існують й випадки зі зворотнім ефектом, коли програми різного призначення мають схожі функціональні можливості. Наприклад, текстовий редактор «MS Word» має досить розвинені можливості щодо редагування графічних зображень, які не поступаються графічному редактору початкового рівня. Разом з тим, основне призначення «MS Word» – набір та редагування текстових документів.

Досліджуючи програмний код, експерт досліджує функціональні можливості програмного продукту на предмет відповідності його певним вимогам (це зафіксовано у п. 13.1 розділу ІІ Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень [18]). Вказані вимоги можуть бути зазначені у технічній документації до досліджуваної програми, у постанові ініціатора проведення експертизи або в інших документах. Але навіть встановивши відповідність програми певним вимогам, неможливо напевне стверджувати, яке було початкове призначення програми. Доказом цьому можуть слугувати наведені вище приклади, коли одна і та сама програма може застосовуватися за різним призначенням, коли при однаковому призначенні програми мають різні функціональні можливості, або навпаки, при різному призначенні мають схожі функціональні можливості. Саме тому типовими питаннями, що відносяться до згаданого предмету дослідження, є такі [18, п. 13.2 розділу ІІ]:

- «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?».

На думку автора, досліджуючи програму на предмет її призначення без надання технічної документації на її розробку, експерт по суті повинен дослідити умисел автора програми або її замовника, спрямований на створення програми для певних дій. Разом з тим, встановлення умислу є складовою частиною кваліфікації складу злочину, а відповідно до ч. 1 ст. 242 Кримінального процесуального кодексу України, не допускається проведення експертизи для з'ясування питань права [19].

Ще однією проблемою визначення належності програми до шкідливих програмних засобів є складність при встановленні її призначення саме до несанкціонованого втручання.

Якщо з суто технічної точки зору розглянути коди програм, які спеціально розроблювалися для несанкціонованого втручання, програм подвійного призначення та програм, створених виключно з корисною метою, але які, за умови певних налаштувань, можна використовувати як шкідливі програмні засоби, можна дійти висновку, що не існує чітких критеріїв для їх розмежування. Наприклад, програма, яка функціонально придатна виявляти вразливості певних серверних додатків, може бути застосована як спеціалістами з кібербезпеки для тестування серверу щодо його захищеності, так і кіберзлочинцями для несанкціонованого втручання.

Також суперечливості виникають, якщо розглянути семантичне значення терміну «несанкціоноване». Словник української мови визначає значення слова «санкціонувати» як давати санкцію на що-небудь; визнавати щось законним, правильним, затверджувати, схвалювати щось [20].

А отже, по суті, встановлення законності чи незаконності є правовим питанням, а тому не може вирішуватися експертним шляхом.

Теорія інформаційної безпеки визначає такі властивості інформації, що підлягають захисту, як конфіденційність, доступність та цілісність [21]. Шкідливі програмні засоби впливають на доступність та цілісність інформації шляхом блокування чи знищення інформації, а також порушення її цілісності. Порушення конфіденційності призводить до витоку інформації.

Відповідно до ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [22], блокування інформації – це дії, внаслідок яких унеможливлюється доступ до інформації в системі. Знищення інформації – дії, внаслідок яких інформація в системі зникає. Порушення цілісності інформації – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст. Витік інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юри-

дичним особам, що не мають права доступу до неї. Разом з тим, функції блокування (наприклад, захисту паролем), знищення (видалення) та внесення змін до вмісту інформації (редагування) є стандартними для більшості корисних програм. Що стосується витоку інформації, то тут прослідковується одразу два протиріччя. По-перше, чи мають право доступу до інформації певні особи, чи не мають – це правове питання, яке виходить за межі компетенції експерта. По-друге, витік є вже наслідком застосування шкідливого програмного засобу, разом з тим, склад злочину, передбаченого ч. 1 ст. 361-1 КК України, є формальним, тобто, не передбачає обов'язкового настання наслідків.

Автор розділяє думку А. С. Білоусова, який вважає, що шкідливість або корисність відповідних програм для ЕОМ визначається не їх призначенням, тобто здатністю знищити, блокувати, модифікувати, копіювати інформацію. Такі операції здійснюють і корисні комп'ютерні програми, що легально використовуються в роботі ЕОМ. Шкідливість програми передбачає, насамперед, те, чи мало місце попереднє повідомлення власника або легального користувача комп'ютерної інформації щодо характеру дій програми, а, по-друге, чи було отримано попередню згоду або дозвіл на реалізацію такої програми [23, с. 107].

Разом з тим, як свідчить практика, зазвичай ініціатор експертизи вимагає від експерта повної та чіткої відповіді, чи є програма шкідливим програмним засобом, чи ні? На думку автора, така постановка питання є докорінно невірною. По-перше, слід згадати відсутність у експерта достатніх можливостей для встановлення умислу розробника (замовника) програми та поінформованості та згоди чи незгоди легального користувача, оскільки для цього необхідно проводити різні слідчі (розшукові) дії (допити тощо). По-друге, вирішуючи як технічні, так і правові питання, експерт фактично сам дає повну юридичну оцінку вчиненому діянню, тим самим беручи на себе частину повноважень слідчого. Натомість порушення вимог Кримінального процесуального кодексу (насамперед вимог ст. 242) є достатньою підставою взагалі визнати джерело доказу (в даному випадку – висновок експерта) неналежним, та не враховувати під час розгляду справи.

На думку автора, під час дослідження програми на предмет її віднесення до шкідливих програмних засобів, експерт може лише встановити певні функціональні можливості програми, які можуть бути властиві шкідливим програмам. Але варто пам'ятати, що ці самі функціональні можливості можуть бути притаманні й корисній програмі.

Таким чином, віднесення певної програми до шкідливих програмних засобів неможливе в рамках суто судово-експертного дослідження, а потребує зусиль як експерта, який досліджує технічну сторону програми (встановлює її функціональні можливості), так і слідчого, який встановлює такі юридичні аспекти, як можливість застосування встановлених експертом функціональних можливостей програми для несанкціонованого втручання та умисел розробника програми, спрямований на розробку програми саме для несанкціо-

нованого втручання. При цьому потрібно зазначити, що експерт у висновку повинен не лише встановити функціональність програми, характерну для шкідливих програмних засобів, але й також зазначити, в яких випадках застосування цих функцій може бути шкідливим, а в яких – цілком корисним.

Остаточне рішення щодо віднесення програми до шкідливих програмних засобів приймає суд, вивчивши та оцінивши зазначені вище технічні й юридичні аспекти, встановлені слідчим і експертом, а також докази, подані іншими учасниками кримінального провадження.

Перелік посилань

1. *Кримінальний кодекс* України [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/2341-14
2. *Касперский Е. В.* Компьютерные вирусы: что это такое и как с ними бороться. Москва, 1998. 288 с.
3. *«АНТИВИРУС КАСПЕРСКОГО»* принял за вирус системній файл TCPIP.SYS / журнал «Хакер» [Електронний ресурс]. Режим доступу: https://xakep.ru/2013/10/27/61498/
4. *AVG incorrectly* flags user32.dll in Windows XP SP2/SP3 [Електронний ресурс]. Режим доступу: http://arstechnica.com/information-technology/2008/11/avg-incorrectly-flags-user32-dll-in-windows-xp-sp2sp3/
5. *Microsoft* приняла браузер Google за вирус [Електронний ресурс]. Режим доступу: http://www.cnews.ru/news/top/microsoft_prinyala_brauzer_google_za_virus
6. *ping(8)* - Linux man page [Електронний ресурс]. Режим доступу: http://linux.die.net/man/8/ping
7. *FreeBSD* Man Pages [Електронний ресурс]. Режим доступу: http://www.freebsd.org/cgi/man.cgi?query=ping&sektion=8&manpath=FreeBSD+4.3-RELEASE
8. *DDOS* стандартными средствами винды [Електронний ресурс]. Режим доступу: https://forum.xeksec.com/f17/t829/
9. *Этичный взлом* по шагам: колонка Юрия Гольцева / журнал «Хакер» [Електронний ресурс]. Режим доступу: https://xakep.ru/2015/04/09/195-goltsev/
10. *Площадка* для взлома: головоломки для хакера / журнал «Хакер» [Електронний ресурс]. Режим доступу: https://xakep.ru/2010/06/03/52289/
11. *ГОСТ 34.602-89*. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы [Електронний ресурс]. Режим доступу: http://tzi.com.ua/downloads/34.602-89.pdf
12. *Tracert vs Traceroute* [Електронний ресурс]. Режим доступу: https://habrahabr.ru/post/281272/
13. *Internet* Control Message Protocol (ICMP). Basics / Microsoft Support [Електронний ресурс]. Режим доступу: https://support.microsoft.com/en-us/kb/170292
14. *Internet* Control Message Protocol (ICMP) Parameters / Internet Assigned Numbers Authority (IANA) [Електронний ресурс]. Режим доступу: www.iana.org/assignments/ icmp-parameters/icmp-parameters.xhtml
15. *Рівні моделі* OSI / Комп'ютерні мережі [Електронний ресурс]. Режим доступу: http://comp-net.at.ua/index/rivni_modeli_osi/0-10
16. *RFC 768*. User Datagram Protocol (UDP) / Internet Engineering Task Force (IETF) [Електронний ресурс]. Режим доступу: https://tools.ietf.org/html/rfc768

17. *Service* Name and Transport Protocol Port Number Registry / Internet Assigned Numbers Authority (IANA) [Електронний ресурс]. Режим доступу: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
18. *Науково-методичні* рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень, затверджені наказом Міністерства юстиції України від 08.10.1998 № 53/5 «Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень» [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/z0705-98
19. *Кримінальний процесуальний* кодекс України [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/4651-17
20. *Словник* української мови: в 11 тт. / АН УРСР. Ін-т мовознавства; за ред. І. К. Білодіда. Київ, 1970. Т. 9. 1980. С. 54.
21. *Юдін О. К.* Інформаційна безпека: нормативно-правове забезпечення. Київ, 2010. 708 с. іл.
22. Про захист інформації в інформаційно-телекомунікаційних системах: закон України [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/80/94-вр
23. *Білоусов А. С.* Криміналістичний аналіз об'єктів комп'ютерних злочинів: дис. … канд. наук: 12.00.09 / Класичний приватний університет. Запоріжжя, 2008. 245 с.

ПРОБЛЕМНЫЕ ВОПРОСЫ ПО ОТНЕСЕНИЮ ПРОГРАММ К ВРЕДОНОСНЫМ ПРОГРАММНЫМ СРЕДСТВАМ

Ю. Ю. Низовцев

Вопросам противодействия киберпреступности, в том числе расследованию преступлений, связанных с использованием вредоносных программных средств, посвятили свои работы многие ученые. Вместе с тем, до сих пор остаются неисследованными роль и возможности судебной экспертизы по отнесению программы к вредоносным программным средствам.

Автор считает сомнительной возможность определить «вредоносность» программы, изучая сугубо техническую ее сторону, по целому ряду причин. Например, вредные действия может выполнить и полезная программа вследствие ошибок кода или ошибочных параметров запуска.

Также следует учесть, что не существует прямой взаимосвязи между первоначальным назначением программы и ее функционалом. Одну и ту же программу (функцию программы) можно применить как с благими целями, так и с противоправными. Программы, имеющие одинаковое назначение, могут иметь разные базовые принципы работы и функционал, и наоборот, программы разного назначения могут иметь схожие функции.

Кроме того, установление назначения программы именно для несанкционированного вмешательства требует определения умысла автора на создание программы для указанных целей, а также такого критерия, как «несанкционированность», который является правовым. Решение же правовых вопросов экспертным путем запрещено ст. 242 КПК Украины.

Как показывает практика, обычно инициатор проведения экспертизы требует от эксперта четкого ответа, является программа вредоносным программным средством, или нет?

По мнению автора, такая постановка вопроса в корне неверна. Во-первых, эксперт не имеет достаточных возможностей для установления умысла разработчика программы, так как для этого необходимы определенные следственные (розыскные) действия (допросы и т.д.). Во-вторых, решая как технические, так и правовые вопросы, эксперт фактически сам дает полную юридическую оценку совершенному деянию, тем самым беря на себя часть полномочий следователя.

Отнесение программы к вредоносным программным средствам, по мнению автора, невозможно в рамках сугубо судебно-экспертного исследования. Для этого требуются усилия как эксперта, который исследует техническую сторону программы, так и следователя, который устанавливает такие юридические аспекты, как возможность применения выявленных экспертом функциональных возможностей программы для несанкционированного вмешательства и умысел разработчика программы, направленный на разработку программы именно для указанных действий.

PROBLEMS IN THE CONTEXT OF ASCRIPTION OF SOFTWARE TO MALICIOUS SOFTWARE TOOLS

Iu. Nizovtsev

Many scientists dedicated their papers to the issue of combating cybercrime, including the investigation of crimes involving the use of malicious software. At the same time role and potential of forensic examination in the domain of ascription of software to malicious software tools remain unexplored.

For several reasons the author considers that determination of the "harmfulness" of the software, studying nothing but technicality, is dubious and disputed. For example, a harmful action can be performed by useful computer program due to code error or incorrect launch parameters.

It is also worth noting that there is no direct link between the original purpose of the program and its functionality. The same software (function of the program) can be used both with good intentions and with unlawful purposes. Programs that have the same function can have different basic principles of operation and functionality, and vice versa, programs of different object matter can have similar functions.

In addition, the attribution of the software to malware for snooping and tampering requires the ascertainment of the fact of the author's intention to create a computer program for this purpose, and also it requires determination of such criteria as "Unauthorized," which is legal. The solutions of the legal problems by experts are forbidden by Criminal Procedural Code of Ukraine (paragraph № 242).

Experience has proven that the initiator of the expert examination usually requires a simple answer of the expert whether the program is malicious software tool or not?

According to the author's judgment such approach is fundamentally wrong. Firstly, expert does not have sufficient capacity to ascertain malicious intent of the software developer, since it requires certain investigation actions (interrogations, etc.). Secondly, addressing both technical and legal issues, expert actually gives complete legal evaluation of the offense, thereby assuming the part of the investigator's authority.

In accordance with the author's opinion the attribution of software to malicious software (malware) is impossible to implement merely within the framework of forensic investigation. This process demands efforts of both an expert, who explores the technical aspects of the software, and an investigator, who establishes legal points. These legal points concern the possibility, identified by the expert, to apply functionality of software with a purpose of tampering, and also software developer's criminal intent to produce computer program specifically for these actions.