УДК 343.985.7

Волков О. О. – здобувач кафедри криміналістики та судової медицини Національної академії внутрішніх справ, м. Київ

ПОНЯТТЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАСОБУ, ПРИЗНАЧЕНОГО ДЛЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

Проаналізовано сутність поняття «шкідливий програмний засіб». Визначено його криміналістичні ознаки. Досліджено деструктивні властивості, сформульовано визначення та критерії приналежності програмного засобу до категорії шкідливих.

Ключові слова: шкідливий програмний засіб, комп'ютерні віруси, кіберзлочинність, несанкціонований доступ, електронно-обчислювальна техніка.

Розвиток інформаційного суспільства в нашій державі передбачає, насамперед, дотримання прав людини, забезпечення її свободи, честі, гідності. Такі цінності є пріоритетними під час розбудови правової держави й інтеграції до європейського простору.

У цьому контексті важливим напрямом діяльності держави, зокрема правоохоронних органів, є протидія кіберзлочинності. Брак чіткого визначення терміна «шкідливий програмний засіб» (ШПЗ) унеможливлює формування єдиного підходу до кваліфікації протиправного діяння, пов'язаного з його використанням, пошуку та фіксації, а також проведення комп'ютерно-технічних експертиз.

У жодному чинному нормативному акті не запропоновано дефініцію поняття ШПЗ, не схарактеризовано криміналістичні ознаки та критерії віднесення їх до категорії шкідливих.

Мета цієї статті – сформулювати криміналістичне визначення ШПЗ, який створюють, використовують та розповсюджують для несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж і

мереж електрозв'язку (електронно-обчислювальна техніка, ЕОТ), для сприяння ефективній протидії кіберзлочинності.

Різним аспектам протидії кіберзлочинності, зокрема розслідуванню злочинів, пов'язаних із використанням ШПЗ, присвячували свої роботи П. Д. Біленчук, В. О. Вітюк, О. П. Войтович, В. А. Голубєв, В. А. Каплун, В. В. Крилов, Б. В. Романюк, Л. М. Соловйов, Т. Л. Тропіна, В. С. Цимбалюк та ін. Однак понятійний апарат у цій сфері не розроблено на належному рівні.

Застосування ШПЗ є одним із найпоширеніших злочинів у галузі комп'ютерних та Інтернет-технологій. Їх використовують для комп'ютерного тероризму, майнингу криптовалюти, викрадення електронних коштів і різноманітної інформації з електронних баз даних, порушення прав інтелектуальної власності, учинення шахрайства в електронних мережах тощо.

Повсякчас збільшується кількість як вітчизняних, так й іноземних користувачів мережі Інтернет і ЕОТ, що дає підстави прогнозувати зростання рівня кіберзлочинності.

Оскільки законодавство не містить визначення поняття ШПЗ, це надає можливість правопорушникам уникати відповідальності за їх застосування. Зазначене є додатковим чинником латентності цього виду кіберзлочинності, що також пов'язано з необізнаністю правоохоронців в аналізованій сфері, невжиттям заходів для відшкодування завданих збитків тощо.

Стаття 361 Кримінального кодексу (КК) України до 23 грудня 2004 року передбачала тільки відповідальність за розповсюдження комп'ютерного вірусу. Визначаючи засоби вчинення такого протиправного діяння, законодавець обмежився лише формулюванням терміна «комп'ютерний вірус», чим звузив практичне застосування цієї норми, оскільки комп'ютерний вірус є різновидом шкідливих програмних засобів, які можуть бути використані правопорушниками.

На думку М. І. Мельника та М. І. Хавронюка, розповсюдження комп'ютерного вірусу – це введення до ЕОМ, їх систем або комп'ютерної мережі шляхом застосування програмних засобів хоча б одного комп'ютерного вірусу – комп'ютерної програми, здатної в разі її активації порушувати нормальну роботу ЕОМ, системи чи комп'ютерної мережі, а також знищувати чи пошкоджувати комп'ютерну інформацію [1].

Дослідники П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк тлумачили цей термін як передання комп'ютерних вірусів у будь-який спосіб і на будь-яких підставах (продаж, дарування, надання можливості копіювання тощо), «закладення» їх у комп'ютерні системи на стадії виготовлення, ремонту, реалізації з метою подальшого використання для несанкціонованого доступу до інформації; ознайомлення інших осіб зі змістом програмних засобів або технічними характеристиками чи технологією виготовлення і використання технічних засобів для незаконного проникнення в комп'ютерні системи [2].

Слушно зауважує О. Мазуренко, що в диспозиції ст. 361 КК України передбачено спосіб і засоби такого розповсюдження, проте це звужує сферу застосування зазначеної норми, оскільки комп'ютерний вірус може бути розповсюджений також іншим шляхом, без застосування визначених засобів або із використанням засобів, призначених для незаконного проникнення в ці машини, однак не спроможних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації, що теж унеможливлює застосування цієї норми в таких випадках [3].

Зміни, внесені в КК України, а саме доповнення ст. 361^1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» [4], сприяли розширенню тлумачення поняття «шкідливий програмний засіб».

Так, відповідно до змісту диспозиції цієї статті, основною ознакою віднесення будь-якого програмного засобу до категорії шкідливих є не фактичне його використання, а конструктивне (інженерне) призначення. За дефініцією, що містить Новий тлумачний словник української мови, шкідливий – це такий, що здатний завдавати і завдає шкоди, збитків кому-, чому-небудь [5]. З огляду на це, кримінальна відповідальність може наставати в таких випадках: створення ШПЗ з метою несанкціонованого втручання в роботу ЕОТ; створення ШПЗ з метою розповсюдження або його збуту; розповсюдження або збут ШПЗ.

Законодавець вимагає під час доказування вини правопорушника встановлювати та документально підтверджувати факт створення ШПЗ, мету його створення, а також задокументувати його розповсюдження або збут.

За такої конструктивної особливості ст. 361[1] КК України кримінальну відповідальність лише за зберігання ШПЗ і придбання (без його застосування, розповсюдження або збуту) не передбачено. Таким чином, кримінальна відповідальність настає за створення предмета злочину (ШПЗ) з метою використання, розповсюдження або збуту, а безпосередньо за використання відповідальності не встановлено.

За певних умов використання ШПЗ може утворювати ознаки складу злочину, передбаченого ст. 361 КК України, що призводить до конкуренції кримінально-правових норм. Усунення такої непослідовності законодавця слід вважати пропозицією стосовно вдосконалення аналізованої норми.

У своїх дослідженнях В. М. Бутузов, С. Л. Останець і В. П. Шоломивцев шкідливі програмні засоби визначають як створення або пристосування комп'ютерної програми, що призначена для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. На їхнє переконання, це, здебільшого, різноманітні види комп'ютерних вірусів [6].

Таке твердження, на нашу думку, не цілком правильне, оскільки, крім комп'ютерних вірусів, є чимало інших ШПЗ, а комп'ютерний вірус – це лише їх різновид.

Застосовуючи термін «вірус» (механізм поширення схожий на біологічне середовище), мають на увазі механізм несанкціонованого втручання, адже найпоширенішим програмним засобом для несанкціонованого втручання в ЕОТ (80 %) з-поміж ШПЗ є саме віруси. Таким чином, термін «вірус» як узагальнювальне поняття для всіх категорій ШПЗ є застарілим, а тому доцільніше використовувати термін «шкідливий програмний засіб».

В англійській мові поняття ШПЗ позначають як *malware,* що є скороченням двох слів: *malicious* – зловмисний і *software* – програмне забезпечення.

Програмний засіб – це складний продукт інтелектуальної діяльності, логічна послідовність виконання певних арифметичних алгоритмів, призначена для автоматизації заздалегідь визначених процедур. Програмні засоби нерозривно пов'язані із функціонуванням ЕОТ, вони сприяють посиленню розумових здібностей людини, швидкому опрацюванню значного

масиву інформації, виконанню складних і специфічних обчислень, що відповідає вимогам науково-технічного прогресу.

Електронно-обчислювальну техніку слід тлумачити як сукупність пов'язаних за допомогою програмних засобів ЕОМ, комп'ютерів, автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку, які забезпечують електронно-обчислювальні процеси, що в них відбуваються.

Загалом програмне забезпечення можна визначити як сукупність програмних засобів комп'ютерної техніки, що використовують для управління функціонуванням конкретної ЕОМ, комп'ютера, автоматизованої системи, комп'ютерної мережі, мережі електрозв'язку й електронно-обчислювальними процесами, що в них відбуваються.

Одночасно з активним застосуванням ЕОТ з'явилися програмні засоби, які не виконували корисних для користувача завдань, а мали, переважно, прихований функціонал деструктивного спрямування.

У правозастосовній діяльності ШПЗ розглядають як знаряддя вчинення злочину під час кваліфікації дій, пов'язаних із застосуванням їх для несанкціонованого втручання в ЕОТ (ст. 361 КК України). Дії, які містять самостійний склад злочину, передбаченого ст. 361^1 КК України, кваліфікують за сукупністю з основним злочином.

Правопорушники з різних мотивів (корисливих, самоствердження, виконання протиправних вказівок, на замовлення, у військовій сфері) за допомогою ШПЗ здійснюють несанкціоноване втручання в роботу ЕОТ. Наслідком такого втручання є фізичне знищення ЕОТ, блокування їх роботи, викрадення, знищення та шифрування інформації, яку там зберігають. Відповідно до положень теорії кримінального права, ШПЗ в контексті складу злочину, передбаченого ст. 361^1 КК України, визнають як предмет учинення злочину, а не засіб.

Характерна особливість кіберпростору (середовища ЕОМ, комп'ютерів, автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку) полягає в тому, що програмні засоби, інформація, процеси, які в ньому взаємодіють, не мають зовнішнього вияву. Наприклад, Верховний суд США визначає, що кіберпростір – це унікальне середовище, що не розташоване в географічному просторі, проте доступне кожній людині в будь-якій точці світу завдяки мережі Інтернет [7].

Тому процеси, що відбуваються під впливом ШПЗ, у такому середовищі мають інформаційне слідоутворення, що не варто ототожнювати з наслідками, які можуть виявлятися і в матеріальній формі (виведення з ладу обладнання тощо). Такими слідами В. О. Мещеряков пропонує вважати «сліди, що зберігаються в пам'яті технічних пристроїв, в електромагнітному полі, на носіях машиночитної інформації, що є проміжними між матеріальними й ідеальними» [8].

До цього простору належать носії такої інформації, а саме пристрої для зберігання інформації в ЕОМ, комп'ютерах (HDD, SSD), периферійні пристрої (електромагнітні та флеш-накопичувачі, оптичні диски, комп'ютерні пристрої зв'язку, мережеві пристрої, мережі електрозв'язку, «хмарні» середовища зберігання інформації. У вузькому значенні носії інформації слід визначати як електронно-оптичні пристрої, що формують і підтримують у придатному для зчитування вигляді фізичний обсяг, який використовують для тривалого зберігання й оперативного опрацювання електронної інформації.

Судова практика засвідчує, що програмні засоби можуть бути шкідливими, якщо вони за своїми ознаками здатні несанкціоновано порушити конфіденційність, доступність і цілісність інформації, яку опрацьовують через автоматизовану систему або передають мережами електрозв'язку [9].

Саме прихованість, деструктивність і несанкціонованість є визначальними ознаками ШПЗ. Тобто для віднесення програмного засобу до категорії шкідливих спеціаліст, експерт мають, насамперед, визначити саме такі його риси.

У разі створення програмного засобу виключно для несанкціонованого проникнення до ЕОТ, його слід вважати ШПЗ. Якщо програмний засіб створено для інших цілей і за своїм конструктивним задумом не містив ознак шкідливості, проте був схожий на ШПЗ і використаний для несанкціонованого втручання в роботу ЕОТ (наприклад, перевірка систем захисту комп'ютерних мереж, стійкості до втручання інших програмних засобів), то його необхідно вважати програмним засобом, який пристосований для несанкціонованого втручання, оскільки, крім шкідливих ознак, він виконує й конструктивні завдання, закладені під час створення. В інших джерелах такі програмні засоби визначають як програми подвійного призначення [10].

Однією з ознак ШПЗ є функція подолання захисту систем ЕОТ, перешкоджання її нормальній діяльності. Ключовим моментом дії ШПЗ є відсутність добровільної згоди, обізнаності щодо такого втручання в роботу ЕОТ.

Здатність програмного засобу до несанкціонованого втручання слід трактувати як можливість її самовідтворення за певних умов, масове розсилання, самокопіювання на диск, причому як на вільні місця, так і шляхом заміни іншої інформації на жорсткому диску комп'ютера або її шифрування.

Ці засоби становлять підвищену небезпеку для користувачів ЕОТ, оскільки вони є джерелом підвищеної небезпеки для користувачів, інформації, що зберігається, і нормальної роботи обладнання. Притаманна їм здатність несанкціонованого втручання, знищення, перешкоджання роботі комп'ютерів, мережевого оточення, тобто деструктивний вплив, є їхньою об'єктивною та визначальною ознакою.

Подеколи ШПЗ можуть бути придатними для подолання систем захисту та можливості діяти без згоди користувача ЕОТ, впливу на інформацію, роботу ЕОТ, завдавати матеріальних збитків.

Здебільшого ШПЗ – це самостійний програмний код, у якому для шкідливого функціоналу використовують заздалегідь визначені, створені системи команд. Значну кількість програмних засобів, які мають за функціоналом схожі ознаки, можуть визнавати системи захисту ЕОТ (так звані антивірусні програми, брендмауери, фаєрволи) як шкідливі, однак вони такими не є.

Шкідливий програмний засіб має відповідати критеріям, що визначають цільове призначення ШПЗ, зокрема це несанкціоноване втручання в роботу ЕОТ. Отже, ШПЗ можна вважати будь-який програмний засіб, що має приховану деструктивну властивість, за таких умов:

1) призначений для несанкціонованого втручання, зміни, модифікації, блокування, копіювання або знищення інформації, споживання технічних ресурсів ЕОТ, використовує спеціально для цього розроблений програмний код (сигнатуру, модуль), що заздалегідь визначений розробником;

2) наявність середовища, через яке здійснено проникнення (локально, через Інтернет, окремі оптичні, магнітні носії або конкретна команда на ЕОТ);

3) наявність певної події яка передувала проникненню ШПЗ, або системного алгоритму, завдяки якому почав діяти ШПЗ (наприклад, встановлений клієнт-банк, Інтернет-гаманець електронних грошей тощо);

4) самодостатність програмного коду ШПЗ для втілення задуму розробника;

5) достатня стійкість ШПЗ до подолання систем захисту ЕОТ.

Щоб констатувати приналежність програмного засобу до категорії шкідливих, він має відповідати одночасно всім окресленим критеріям. Для встановлення їх наявності потрібні спеціальні знання, тому для аналізу ШПЗ призначають судову комп'ютерно-технічну експертизу [11], різновидом якої є програмно-комп'ютерна експертиза [12].

За конструктивними особливостями ШПЗ може бути як нескладним програмним засобом з обмеженим функціоналом, призначеним для виконання окремих, конкретно визначених дій, так і складним програмним комплексом зі значною кількістю модулей, частини яких, залежно від програмно значущих подій або вказівк користувача, оператора (розробника), можуть підключатися (завантажуватися через мережу) для використання за певним цільовим призначенням (наприклад, ШПЗ виявив, що на ЕОТ встановлено програмний засіб «клієнт-банк», але для перехоплення інформації необхідно встановити певний модуль).

Окремо слід проаналізувати програмні засоби, метою створення яких була генерація ліцензійних ключів до інших програмних засобів, або «зламування» ідентифікатора ліцензії (кейлогер).

Досліджуючи криміналістичний аспект створення, використання та розповсюдження таких програмних засобів, можна дійти висновку, що до категорії шкідливих належать лише програмні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку.

Єдиною метою створення кейлогера є несанкціоноване стосовно правовласника такого програмного засобу втручання в його роботу для подолання або оминання систем захисту ліцензійних умов легального користування програмним засобом, а неліцензійне використання програмного засобу призводить до нестабільності роботи ЕОМ (комп'ютера) загалом.

Кейлогер активується з дозволу користувача ЕОТ. Несанкціоноване втручання в такому разі слід розглядати з позиції, що програмний засіб, який підлягає зламуванню, установлений на ЕОМ (комп'ютер) і призначений для належного та злагодженого його функціонування, а втручання кейлогера в роботу програмного засобу спричиняє дестабілізацію роботи ЕОТ. Втручання в роботу будь-якого програмного засобу шляхом підбирання або зламування ліцензійних умов користування слід вважати опосередкованим несанкціонованим втручанням у роботу ЕОТ, тобто без наявності відповідного дозволу (ліцензії) з боку володільця правами цього програмного засобу, що є безпосереднім порушенням прав інтелектуальної власності.

Отже, кейлогери слід відносити до категорії шкідливих, причому всі антивірусні засоби трактують їх як ШПЗ.

Будь-який програмний засіб, якщо в ньому міститься хоча б одна деструктивна (шкідлива) або прихована функція, що діє без згоди користувача або оператора, становить суспільну небезпеку. Наприклад, легальне програмне забезпечення, що містить приховану функцію надання віддаленого доступу до комп'ютера користувача та здійснення такого несанкціонованого втручання без згоди його власника або користувача, необхідно визнавати як ШПЗ.

Неоднозначними є питання кваліфікації програмних засобів, які за низкою ознак належать до категорії шкідливих, однак такими не є. Це, зокрема, програмні засоби, які хоч і розроблені для несанкціонованого втручання в роботу ЕОТ, однак мають спеціальне призначення – їх застосовують працівники правоохоронних органів для документування протиправної діяльності (перехоплення електронної пошти, паролів, закриття доступу до протиправного контенту, військового, лабораторного чи дослідницького призначення).

Також такими програмними засобами користується спеціаліст, який перевіряє (проводить аудит) ступеня захищеності ЕОТ від несанкціонованого втручання. Такі програмні засоби за своїм призначенням, конструктивними особливостями та дією схожі на ШПЗ.

До цієї категорії програмних засобів О. А. Парфило відносить і шкідливі програмні засоби, які спеціально для цього створені, однак їх використовують з дозволу керівництва суб'єкта господарювання для стеження за підлеглими з метою

профілактики вчинення ними протиправних дій або неефективного використання робочого часу. Працівників попереджають про встановлення на ЕОТ, якими вони користуються, таких ШПЗ [13].

Такі програмні засоби, здебільшого, проходять реєстрацію, мають необхідну ліцензію, їх використання в кожному конкретному випадку санкціоноване відповідними державними органами або керівництвом суб'єкта господарювання, хоча використання їх є негласним.

Крім цього, є програмні засоби, які, на перший погляд, належать до ШПЗ (розповсюджують у збірниках для зламування), однак лише імітують таку діяльність і не впливають на роботу ЕОТ й інформацію, що там зберігають. Це недоопрацьовані, нефункціональні програмні засоби або виконані із системними помилками в коді. Мета їх збуту передбачає лише одержання коштів від потенційних правопорушників, які прагнуть заволодіти «хакерськими» програмними засобами.

Якщо правопорушник, який створив, заволодів або мав намір використати нефункціональне ШПЗ, помилково вважаючи його цілком функціональним і таким, що може бути використаний за протиправним призначенням, його дії слід кваліфікувати як замах на вчинення злочину за ст. 15 і відповідною частиною ст. 361^1 КК України. Оскільки предмет злочину є ознакою об'єкта злочину, у такому разі відбувається помилка в об'єкті, що кваліфікують як замах на злочин. Заволодіння такою особою нефункціональним ШПЗ (наприклад, імітаційні ШПЗ) і приведення його в придатний до використання за неправомірним призначенням стан необхідно кваліфікувати як незаконне створення ШПЗ. Так само можна кваліфікувати дії підозрюваного й тоді, коли для виготовлення придатного для використання ШПЗ частину коду було використано з іншого програмного засобу (певний модуль), а решту розроблено самостійно.

Таким чином, програмні засоби визначають як шкідливі не лише за технічним, а й за цільовим призначенням.

Неоднозначність віднесення до шкідливих виникає під час дослідження програмного засобу, який спеціально розроблений для масового розсилання електронної пошти.

До категорії шкідливих він належатиме за умови, якщо розсилання поштових повідомлень здійснюють без згоди або всупереч бажанню отримувача («спам») чи з метою порушення роботи поштового сервера. У разі масового замовлення особами розсилання новин, анонсів, біржових зведень тощо ознак шкідливості не буде.

Отже, під час розроблення нормативно-правових актів, які будуть регламентувати сферу протидії несанкціонованому втручанню в роботу ЕОТ за допомогою ШПЗ, необхідно визначити поняття «шкідливий програмний засіб». На нашу думку, це програмний засіб у вигляді коду, скрипта, активного контенту, програмного забезпечення, який наявний у кібернетичному середовищі, спеціально створений, конструктивно призначений і технічно придатний для несанкціонованого втручання в роботу ЕОТ та не має будь-якого іншого програмного, технічного, господарського, а також прикладного призначення, призводить до зміни, модифікації, блокування, копіювання або знищення інформації, споживання технічних ресурсів ЕОТ. Така дефініція відповідає запитам сьогодення у сфері протидії кіберзлочинності.

До визначальних ознак ШПЗ належать несанкціонованість, прихованість, деструктивність і здатність долати системи захисту. Ключовим аспектом несанкціонованості слід вважати відсутність добровільної згоди користувача або правовласника програмного засобу на його модифікацію. Також ШПЗ повинен відповідати спеціальним критеріям, мати не тільки технічне (інженерне), а й цільове призначення.

Розмежування ШПЗ і програмних засобів, пристосованих для несанкціонованого проникнення до ЕОТ, необхідно проводити експертним шляхом під час компютерно-технічної або програмно-компютерної експертизи.

Недосконалість законодавства в цій сфері призводить до того, що частина протиправних дій, а саме придбання та зберігання ШПЗ, знаходиться поза межами правового регулювання, це надає можливість правопорушникам уникати відповідальності.

Шкідливий програмний засіб є джерелом підвищеної суспільної небезпеки, що полягає в їхньому конструктивному призначенні – несанкціонованому втручанні в роботу ЕОТ,

а також здатності до маскування. Досліджуючи такий програмний засіб, необхідно дотримуватися правил техніки безпеки з метою запобігання його деструктивному впливу.

Результати викладеного у статті дослідження можуть бути використані під час розроблення нормативно-правової бази у сфері протидії кіберзлочинності, підготовки методичних рекомендацій для практичних працівників правоохоронних органів, а також у навчальному процесі здобувачів вищої освіти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. – Київ : Атіка, 2003. – 1056 с.

2. Біленчук П. Д. Комп'ютерна злочинність : навч. посіб. / [П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін.]. – Київ : Атіка, 2002. – 240 с.

3. Мазуренко О. Стаття 361 КК України: проблеми об'єктивної сторони злочину / О. Мазуренко // Підприємництво, господарство і право. – 2004. – № 7. – С. 116–120.

4. Про внесення змін до Кримінального та Кримінально-процесуального кодексів України [Електронний ресурс] : Закон України від 1 груд. 2005 р. № 3169-IV. – Режим доступу: http://zakon.rada.gov.ua/go/3169-15. – Назва з екрана.

5. Новий тлумачний словник української мови : у 4 т. / уклад.: В. Яременко, О. Сліпушко. – Київ : Аконіт, 2001. – Т. 3. – 811 с.

6. Бутузов В. М. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : наук.-практ. комент. / В. М. Бутузов, С. Л. Остапець, В. П. Шоломенцев. – Київ : МВС України, 2005. – 86 с.

7. Дашян Н. Обзор Конвенции Совета Европы о киберпреступности / Н. Дашян // Современное право. – 2002. – № 11. – С. 20.

8. Мещеряков В. А. Преступления в сфере компьютерной информации / В. А. Мещеряков. – Воронеж : Воронеж. гос. ун-т, 2002. – 176 с.

9. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку [Електронний ресурс] / Офіційний веб-сайт Верховного Суду України. – Режим доступу: http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(print)/AFB1E90622E4446FC2257B7C00499C02. – Назва з екрана.

10. Тест на проникновение (Пентест) [Электронный ресурс]. – Режим доступа: http://pentest.com.ua. – Загл. с экрана.

11. Про судову експертизу [Електронний ресурс] : Закон України від 25 лют. 1994 р. № 4038-XII. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/4038-12. – Назва з екрана.

12. Усов А. И. Методы и средства решения задач компьютерно-технической экспертизы : учеб. пособие / А. И. Усов. – М. : ГУ ЭКЦ МВД России, 2002. – 200 с.

13. Парфило О. А. Актуальні питання судово-експертного дослідження шкідливих програмних засобів у межах протидії кібертероризму [Електронний ресурс] / О. А. Парфило, Ю. Ю. Нізовець // Криміналістичний вісник. – 2016. – № 1 (25). – С. 78–84. – Режим доступу: http://nbu.gov.ua/UJRN/KrVis_2016_1_15. – Назва з екрана.

REFERENCES

1. Melnyk, M.I., & Khavroniuk, M.I. (Ed.). (2003). *Naukovo-praktychnyi komentar Kryminalnoho kodeksu Ukrainy [Scientific and Practical Commentary of the Criminal Code of Ukraine].* Kyiv: Atika [in Ukrainian].

2. Bilenchuk, P.D., Romaniuk, B.V., & Tsymbaliuk, V.S. (et al.). (2002). *Kompiuterna zlochynnist [Computer crime].* Kyiv: Atika [in Ukrainian].

3. Mazurenko, O. (2004). Stattia 361 KK Ukrainy: problemy obiektyvnoi storony zlochynu [Article 361 of the Criminal Code of Ukraine: problems of the objective side of crime]. *Pidpryiemnytstvo, hospodarstvo i pravo, Entrepreneurship, economy and law, 7,* 116-120 [in Ukrainian].

4. Zakon Ukrainy "Pro vnesennia zmin do Kryminalnoho ta Kryminalno-protsesualnoho kodeksiv Ukrainy": vid 1 hrud. 2005 r. No. 3169-IV [The Law of Ukraine "On Amendments to the Criminal and Criminal Procedural Codes of Ukraine" from December 1, 2005, No. 3169-IV]. (n.d.). *zakon.rada.gov.ua.* Retrieved from http://zakon.rada.gov.ua/go/3169-15 [in Ukrainian].

5. Yaremenko, V., & Slipushko, O. (2001). *Novyi tlumachnyi slovnyk ukrainskoi movy [New Explanatory Dictionary of the Ukrainian Language].* (Vols. 1-4). Kyiv: Akonit [in Ukrainian].

6. Butuzov, V.M., Ostapets, S.L., & Sholomentsev, V.P. (2005). *Zlochyny u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku [Crimes in the field of the use of electronic computers (computers), systems and computer networks and telecommunication networks].* Kyiv: MVS Ukrainy [in Ukrainian].

7. Dashian, N. (2002). Obzor Konvencii Soveta Yevropy o kiberprestupnosti [Review of the Council of Europe Convention on Cybercrime]. *Sovremennoe pravo, The modern law, 11,* 20 [in Russian].

8. Mesceriakov, V.A. (2002). *Prestupleniia v sfere kompiuternoi informacii [Crimes in the field of computer information].* Voronej: Voronej. gos. un-t [in Russian].

9. Ofitsiinyi veb-sait Verkhovnoho Sudu Ukrainy Sudova praktyka rozhliadu sprav pro zlochyny u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), avtomatyzovanykh system ta kompiuternykh merezh i merezh elektrozviazku [Official website of the Supreme Court of Ukraine Trial practice in dealing with crimes in the field of the use of electronic computers (computers), automated systems and computer networks and telecommunication networks]. *www.scourt.gov.ua.* Retrieved from http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(print)/AFB1E90622E4446FC2257B7C00499C02 [in Ukrainian].

10. Test na proniknovenie (Pentest) [Penetration test (Pentest)]. (n.d.). *pentest.com.ua.* Retrieved from http://pentest.com.ua [in Russian].

11. Zakon Ukrainy "Pro sudovu ekspertyzu": vid 25 liut. 1994 r. No. 4038-XII [Law of Ukraine "On Forensic Examination" from February 25, 1994, No. 4038-XII]. (n.d.). *zakon5.rada.gov.ua.* Retrieved from http://zakon5.rada.gov.ua/laws/show/4038-12 [in Ukrainian].

12. Usov, A.I. (2002). *Metody i sredstva resheniia zadach kompiuterno-tehnicheskoi ekspertizy [Methods and means of solving problems of computer and technical expertise].* Moscow: GU EKC MVD Rossii [in Russian].

13. Parfilo, O.A., & Nizovets, Yu.Yu. (2016). Aktualni pytannia sudovo-ekspertnoho doslidzhennia shkidlyvykh prohramnykh zasobiv u mezhakh protydii

kiberteroryzmu [Topical issues of forensic expert research of malicious software in the framework of counteraction to cyberterrorism]. *Kryminalistychnyi visnyk, Forensic messenger, 1(25),* 78-84. Retrieved from http://nbu.gov.ua/UJRN/KrVis_2016_1_15 [in Ukrainian].

Стаття надійшла до редколегії 31.01.2018

Volkov O. *– Resrarcher of the Department of Criminalistics and Forensic Medicine of the National Academy of Internal Affairs, Kyiv, Ukraine*

Concept of a Harmful Software Intended for Disabled Interference in the Operation of Electronic Computer Equipment

The main purpose of the article is to provide forensic detection of a malicious software program that is created for unauthorized interference with the work of computers, computers, automated systems, computer networks and telecommunication networks, in order to promote effective counteraction to cybercrime. Such a need arises in connection with the lack of a unified approach to the definition of «malware» and criteria for assigning programs to harmful ones.

The article analyzes the essence and content of the notion of «malware». Its characteristic forensic features and properties are determined. The destructive features were investigated, definitions and criteria for assigning the software to the category «harmful» were given.

A clear definition of the term «malware» results from the definition of a unified approach to the qualification of such an illegal act, the search and fixing of traces of such an offense, as well as computer-technical expertise.

In the scientific article for discussion are proposed to consider the scientific views of scientists on this topic, a detailed study author of the concept of «harm» in relation to software.

The lack of a clear definition of «malware» means that offenders may in some cases avoid being held responsible for their actions. This factor can be considered as an additional sign of the latency of this type of cybercrime, which is explained not by the awareness of law enforcement officers in identifying malicious software, the

remoteness of the confidence of the injured party in punishing the perpetrators, without the use of measures to reimburse the damage and the need to preserve prestige, especially as it relates to private business entities.

It should be noted that when applying the term «virus» (the mechanism of distribution is similar to the biological environment), the mechanism of unauthorized interference is used, since the most common program for unauthorized interference with electronic computing (80 %) of all malicious software is the viruses, in the notion of a malicious software. Thus, the term «virus» as a generalization of the concept of the entire category of «malware» is obsolete, and therefore for the generalization of the entire category of such software means should be used as a «malware».

Taking into account the statement outlined in the article, it should be noted that when adopting regulatory acts that will regulate the sphere of counteracting unauthorized interference with the work of electronic computers by means of malicious software, it is necessary to define the notion of «malicious software», namely «Malware is a software tool in the form of code, script, active content, software that exists in a cybernetic environment, specially created, constructively designed and technically fit for unauthorized interference with the work of electronic computers, and does not have any other software, technical, economic, and also applied purpose and leads to change, modification, blocking, copying or destruction of information, consumption of technical resources electronically. injecting equipment». Such a definition in our opinion will most accurately meet the requirements of the present and the relevance of measures to combat cybercrime.

A malicious software tool is a specific source of increased risk. This specificity of a malicious software is precisely in their constructive purpose regarding unauthorized interference with the work of electronic computers, as well as the ability to disguise. Therefore, researching such a software tool must adhere to certain safety precautions to prevent its destructive effect.

Keywords: malicious software, computer viruses, cybercrime, unauthorized access, electronic computing.