РЕФЕРАТ

на тему:

“Комп’ютерна вірусологія:

криміналістична класифікація”

Створення та обробка інформації, в тому числі і документованої, можна було б, з точки зору інформатики, звести, в загальному вигляді, до вербалізації результатів аналізу природи отриманих сигналів та її підготовки до передачі. Процес створення (виготовлення) інформації є складною дією, яка містить в собі різноманітні операції, кожна з яких може залишати ідеальні та матеріальні сліди. Зрозуміло, що неточність під час опису як терміна створення (виготовлення), так і процесу створення інформації може суттєво відобразитися на описі кримінальної діяльності.

Розглянемо ситуацію на прикладі створення комп’ютерних вірусних програм (надалі КВП) для ЕОМ, маючи на увазі проблему в цілому. Ця діяльність може містити в собі:

- постановку завдання, визначення середовища існування і мети КВП;  
- вибір засобів і мов реалізації КВП;  
- написання безпосереднього тексту КВП;  
- відладка КВП (перевірка відповідності змісту інформації поставленому завданню);  
- запуск і безпосередню дію КВП (випуск, надання інформації)/

Дії щодо постановки завдання, визначення середовища існування і мети програми, вибору засобів і мов реалізації програм можуть знайти відображення в свідченнях свідків, документах бібліотек, листуванні, які вказують на зацікавленість суб’єкта в данній проблематиці. Дії щодо написання безпосереднього тексту програми, її відладки можуть відобразитися у чернетках на традиційних та магнітних носіях інформації, в свідченнях спостерігачів за процесом відладки або його результатами. Дії щодо запуску і безпосередньої роботи програми можуть бути зафіксовані як у свідченнях очевидців, так і під час матеріального відображення шкідливих суспільно небезпечних наслідків. Кожна з цих елементарних дій за умови існування наміру створення КВП та існуванні об’єктивно виражених слідів його існування можуть бути предметом криміналістичного дослідження і кримінально-правової оцінки.

Аналогічним чином, як складну дію, слід розглядати і будь який процес створення інформації – від порнографічних матеріалів до публічних закликів до розв’язання агресивної війни. Способами скоєння злочинів, які грунтуються на створенні (обробці та виготовленні) комп’ютерної інформації є:   
- створення КВП для ЕОМ, які блокують ЕОМ та (або) модифікують інформацію;  
- створення КВП для ЕОМ, які знищують, модифікують інформацію та (або) блокують ЕОМ;  
- створення КВП для ЕОМ для організації неправомірного доступу до чужих інформаційних ресурсів (банківських, страхових тощо).

Існують різні класифікації КВП. Але не всі вони мають значення для криміналістичних досліджень, тому що створення таких класифікацій частіше підпорядковане прикладним завданням виявлення та знищення вірусів. Для криміналістики цікавими є дані, які характеризують наслідки дій КВП та їх найбільш явні прояви, що дозволяє зафіксувати результати дій програм, наприклад, в свідченнях свідків.

Раніше в спеціальній літературі, присвяченій “комп’ютерній вірусології” вважалось, що в тих випадках, коли в результаті дій “вірусів” відбуваються суттєві зруйнування файлової системи, знищення інформації і т.і., “вірус” є небезпечним. Якщо в результаті його дії на екрані, наприклад, з’являються вірші, лайка і т.і., “вірус” вважається безпечним. Класифікація, яку ми пропонуємо, носить криміналістичний характер, оскільки відображає ознаки, що мають значення насамперед для криміналістичної, а не кримінально-правової оцінки.

**Перший клас КВП (“нешкідливі інфекції”)** – володіють властивостями самостійного розмноження в системах та мережах ЕОМ, не завжди призводять до суттєвих наслідків для інформаційних ресурсів, хоча в деяких випадках і модифікують інформацію, а іноді і блокують ЕОМ, їх мережі та системи. Розробник цього класу КВП не розглядає свою діяльність як суспільно-небезпечну, хоча об’єктивно вона є такою. Так, наприклад, 2 травня 1988 року “безпечний вірус”, який було запущено невідомою особою, спрацював, і близько 350 000 машин в усьому світі після завантаження висвітлили на екранах повідомлення “РЕАСЕ” (“МИР”). Після цього вірус знищив сам себе у всіх системах. Складніша справа відбулася з КВП “різдвяна листівка”(вірусна програма типу “черв’як” – паразитичний процес, який виснажує ресурси системи). Ця програма розповсюджувалася через електронну пошту і одночасно з демонстрацією привітань на екрані таємно зчитувала дані про всі адреси, які мав абонент, і розсилала за цими адресaми аналогічні повідомлення. Дана КВП за дуже короткий час заблокувала своїми копіями електронну пошту. Ознака самостійного розмноження відрізняє даний клас шкідливих програм від так званої “спем” (spem) – інформації. Остання уявляє собою рекламні об’яви, які розсилаються по мережам ЕОМ без згоди одержувачів За оцінками спеціалістів, частка цього “сміття” складає 10% всіх повідомлень електронної пошти в світі.

**Другий клас КВП (“небезпечні інфекції”)** – руйнують інформаційні системи та наносять суттєву шкоду. Найпростішим прикладом такої програми є програма, яка розмножується сама під назвою “SURPRISE”, яка під час запуску виконує знищення всіх файлів в директорії, а потім виводить на екран надпис “SURPRISE” (“СЮРПРИЗ!”).

**Третій клас КВП (“інфекції проникнення”)** призначений для організації неправомірного доступу до чужих інформаційних ресурсів. Відомі випадки протиправного проникнення в ЕОМ демонструють, що зловмисники частіше вимушені, насамперед, змінювати різними способами, в тому числі шляхом впровадження КВП, програмні засоби (або порядок їх роботи), які забезпечують взаємодію ЕОМ між собою та з користувачем. Такі КВП, які забезпечують вхід у систему або привілейований режим роботи з нею, має назву “люків” (“back door”) або “троянські програми”. Робота таких програм зв’язана з існуванням в них поряд з зовнішньою користю, прихованого модуля, що виконує різні, частіше шкідливі для користувача, функції. Досить часто ці програми розповсюджуються як нові версії вже відомих програмних продуктів.

Різновидом “троянських програм” є “логічні бомби” та “бомби з годинниковим механізмом”. Робота вірусної програми починається за певних обставин – настанням будь якої дати, часу іншої значної події. Такі програми частіше використовуються скривдженими співробітниками як форма помсти наймачеві. Відомо, що під час проведення військової операції “ Буря в пустелі” в Персидській затоці система ППО Іраку виявилася заблокованою і не змогла адекватно реагувати на вторгнення сил супротивника в повітряний простір. Припускається, що придбана у Франції обчислювальна техніка, яка забезпечує системи ППО Іраку “електронні закладки”, які блокували роботу обчислювальної системи. До данного класу КВП треба віднести також багаточисельні програмні “вироби”, що призначені для зняття захисту від копіювання комерційних програмних продуктів. Такі КВП приносять суттєву шкоду авторам та розповсюджувачам програм та систем.

Проаналізуємо проблему використання КВП. Використання КВП припускає використання розроблених іншою особою КВП під час експлуатації ЕОМ та обробки інформації. Слід звернути увагу на ознаку санкціонування настання шкідливих наслідків під час дії КВП. Власник інформаційного ресурсу має право в необхідних випадках (наприклад, дослідницькі роботи щодо створення антивірусних засобів і т.і.) використовувати комп’ютерні вірусні програми. Зрозуміло, що для кваліфікації дій як користувача КВП необхідні докази того, що особа раніше знала про властивості програми, яку вона використовує, та наслідках її використання. При цьому достатньо щоб ця особа знала не про всі шкідливі властивості програми, а лише про деякі з них. Тому здаються неточними ствердження про те, що використання комп’ютерної вірусної програми є випуск у світ, відтворення та інші дії стосовно введення такої програми в господарчий обіг, тому що такі дії більше характерні для створення програми. Внесення змін шкідливого характеру в існуючу програму, яка перетворює її в вірусоносія, як правило, зв’язане з модифікацією програм, що за певних умов може бути розцінено як неправомірний доступ до комп’ютерної інформації.

Під розповсюдженням програм треба розуміти надання доступу до відтвореної у будь якій матеріальній формі програми для ЕОМ або бази данних, в тому числі мережевими та іншими способами , а також шляхом продажу, прокату, здавання в найм, надання позики, включаючи імпорт для будь якої з цих цілей. Це визначення можна розповсюдити і на КВП. Особи, які скоїли ці дії за необережністю, тобто за легковажністю або недбалістю, також підлягають відповідальності. Наприклад, особи, які виявили “вірусну програму”, але не застосували необхідних заходів до її локалізації, знищенню та дозволили її подальше розповсюдження, повинні бути притягнуті до відповідальності за свої дії.

Складним для правової оцінки питанням є проблема кваліфікації дій за окремими видами боротьби з КВП. Розроблені для автоматизованої ліквідації КВП в системі Іnternet програми, “автоматично” розповсюджуються в мережі для знищення КВП у всіх ввімкнених в мережу ЕОМ. При цьому, “вакцини”, звичайно без санкції власника мережі, змінюють та модифікують програми, які існують в системі.

Крім очевидних, пов’язаних з демонстраційним ефектом, який є характерним для конкретної КВП, ознаки, які вказують зараження програми, можуть бути такими: змінення довжини командного процесора (COMMAND.COM); повідомлення про помилки читання (запису) під час читання інформації, під час завантаження програм з дискет та інших зовнішніх пристроїв; зміна довжини та (або) дати створення програми; виконання програми повільніше ніж звичайно; збільшення часу завантаження, зациклювання під час завантаження; звернення до дискети та файлів на захищених дисках, які не мають пояснення; втрата працездатності деяких резидентних програм та драйверів; аварійне завершення нормально функціонуючих раніше програм; зависання та перевантажування системи, які не мають пояснення; зменшення об’єму системної пам’яті або вільної пам’яті після завантажування; різьке зменшення доступної дискової пам’яті, хоча файли не додавалися та не знищувалися ; появлення додаткових прихованих файлів або інших змін файлової системи.

Стандартною реакцією користувача в таких випадках є повторний запуск ЕОМ, тобто вимкнення та нове вмикання ЕОМ. За умови появи цих ознак, користувач, в залежності від рівня своєї компетентності та встановленого володарем або власником інформаційних ресурсів порядку використання ЕОМ, або намагається вирішити проблеми самостійно, або звертається до адміністратора системи. Зрозуміло, що в цей момент користувач та адміністратор системи найбільше зацікавлені у відновленні працездатності системи та ліквідації втрат інформації, ніж фіксації ознак протиправних дії з ЕОМ. В цьому випадку виявлення перших ознак комп’ютерних злочинів під час розслідування можуть знайти відбиток у свідченнях свідків (за винятком випадків, коли мають місце фізичні пошкодження ЕОМ). Перші випадки проникнення в ЕОМ, де зберігається не дуже важлива інформація, сторонніх осіб чи КВП не викликає у адміністратора активних дій. Лише повторення таких випадків ініціює активний пошук джерела проблем та застосування заходів протидії. Більшість сучасних операційних систем забезпечують режим колективного доступу до ресурсів окремої ЕОМ і приєднання локальної ЕОМ до інших ЕОМ, перефірійних приладів та мереж ЕОМ. У складі таких операційних систем містяться засоби розділення ресурсів між окремими користувачами (категоріями користувачів) та засоби контролю з боку адміністратора системи за діями певного користувача в області ресурсів, які йому надані. Володарям або власникам інформаційних ресурсів, які визначають порядок дій, доцільно внутрішніми актами встановити обов’язок фіксації таких ознак.

**Ефекти, які можуть бути викликані КВП, кваліфікуються за наступними основними категоріями:**

- відмова комп’ютера від виконання стандартної функції;  
- виконання комп’ютером дій, які не передбачені програмою;  
- руйнування окремих файлів, управляючих блоків та програм, а іноді всієї файлової системи (в тому числі шляхом знищення файлів, форматирування диску, тощо);  
- видача неправдивих, дратівливих, непристойних або відволікаючих повідомлень;  
- створення сторонніх звукових та візуальних ефектів;  
- інсценування помилок або збоїв у програмі або в операційній системі, перевантаження або “зависання” програм чи систем;  
- блокування доступу до системних ресурсів;  
- імітація збоїв внутрішніх та переферійних апаратних пристроїв;  
- прискорення зносу обладнання або спроби його ушкодження.

Під час виникнення “вірусних” проблем з окремою ЕОМ, яка входить до складу мережі, адміністратор мережі намагається локалізувати цю ЕОМ з метою недопущення розповсюдження КВП у мережі, виявлення та ліквідації цієї КВП. Одночасно здійснюється пошук джерел проникнення КВП до ЕОМ. Найчастішим випадком проникнення “вірусу” до системи є робота користувача з інфікованими дискетами. Тому адекватною реакцією адміністратора системи є фізичне закінчення роботи всіх користувачів системи з дисководами і вимога перевірки всіх дискет, які належать користувачам. Іноді остання дія дає результат і за поясненням користувача, який приніс інфіковану “вірусом” дискету, вдається встановити, де саме відбулося зараження. Успішне запобігання зараження передбачає поєднання методів безпечної обробки данних та притягнення третьої сторони, наприклад, використання антивірусного продукту. За допомогою спеціальних антивірусних програм уявляється можливим ідентифікувати КВП, тобто встановити тип, а іноді й найменування КВП. Надалі маємо абстрактну можливість прослідкувати крок за кроком шляхи його “доставки” до конкретної ЕОМ.

На підставі вищезазначеного слід відмітити, що для успішного запобігання вірусу необхідно зробити перший крок – пізнати свого ворога.  
  
  
**Список літератури:**

1. Біленчук Д.П., Біленчук П.Д., Котляревський О.І. Комп’ютерний злочинець: поняття, характеристика, класифікація // Вісник АПСВ, 1998, №2. – с.193-202  
2. Біленчук П.Д., Котляревський О.І. Основи комп’ютерної криміналістики // Криміналістика. Підручник. – Київ,1998. – 416с.  
3. Бачило И.Л. Правовое регулирование процессов информатизации // Гос. и право. - 1994. №12. – с.72