УДК 346.7:004
DOI https://doi.org/10.32837/npnuola.v28i0.693

М. Д. Василенко, В. О. Рачук, В. М. Слатвінська

ШКІДЛИВІ ПРОГРАМИ В КОНТЕКСТІ РОЗУМІННЯ КОМП'ЮТЕРНОЇ ВІРУСОЛОГІЇ ТА ТЕХНІКО-ПРАВОВОЇ ЗМАГАЛЬНОСТІ: МІЖДИСЦИПЛІНАРНЕ ДОСЛІДЖЕННЯ

Безпека є відвертання зла.
Платон

Постановка проблеми. Шкідливі програми, і передусім комп'ютерні вірусні програми, становлять серйозну небезпеку для інформації в комп'ютерних системах. Слід відзначити, що коли йдеться про комп'ютерну вірусну програму, вірус часто розуміють таким чином: вірус є те, що заражає інший «організм», тобто іншу програму. При цьому заражений файл може бути вилікуваний. Заражаючи файли, перші віруси працювали саме так. Фактично комп'ютерний вірус становить комп'ютерну програму, яка має здатність до прихованого саморозмноження. Оскільки назва «комп'ютерний вірус» походить від однойменного терміну з біології за її здатність до саморозмноження, то загалом можна говорити про комп'ютерну вірусологію як науку про шкідливі програми. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світі. Характерно, що в гуманітарному середовищі до комп'ютерних вірусів часто відносять інші види шкідливих програм. Однак для розуміння їхньої дії з позицій генези самих «шкідників», породжених шкідливими програмами, а також для успішної боротьби з ними слід таких «шкідників» розрізняти та класифікувати. Так, у роботі [1] наголошується, що шкідливе програмне забезпечення являє собою будь-яке програмне забезпечення, яке розроблене для того, щоби завдати шкоди комп'ютеру, серверу, клієнту або комп'ютерній мережі. Шкідливе програмне забезпечення завдає шкоди після того, як воно було певним чином внесено у комп'ютер. Воно може мати форму активного вмісту та іншого програмного забезпечення. У всякому разі воно має шкідливий намір, який діє проти інтересів користувача комп'ютера, проявляється через певний недолік, який зазвичай описується як помилка

програмного забезпечення [2]. Зазначимо, що в юридичній та міжгалузевій літературі робіт, присвячених комп'ютерним «шкідникам», небагато (див. [1, 5–11]). Водночас виникає питання про техніко-правову складову частину шкідливих програм і «шкідників», у тому числі і вірусів, а також про боротьбу з цими «негараздами» з урахуванням усіх можливостей і складників, як технічних, так і правових (законодавчих, кримінальних).

Метою статті є встановлення міждисциплінарних зв'язків для шкідливих програм, включаючи «шкідників» у системі комп'ютерної вірусології, виявлення техніко-правової змагальності між ними, засобами і галузями їх виявлення та боротьби.

Виклад основного матеріалу. Досліджуючи основні види шкідливого програмного забезпечення, можна говорити про їх розмаїття. Назва «шкідливі програми» співвідноситься з англомовним терміном "malware", утвореним від двох слів: "malicious" («зловмисний») і "software" («програмне забезпечення»). У побуті всі шкідливі програми часто називають комп'ютерними вірусами, хоча це термінологічно некоректно. До шкідливих програм відносять будь-яке програмне забезпечення, несанкціоновано проникливе в комп'ютерну техніку. Подібні додатки наносять прямий або непрямий збиток. Так, вони порушують роботу комп'ютера або викрадають особисті дані користувача. «Шкідники» завжди створюються для реалізації «благородної мети», а саме отримання вигоди від впровадження у комп'ютер жертви. Отже, залежно від механізму дії шкідливих програм їх поділяють на чотири класи: *комп'ютерні віруси, логічні бомби, хробаки, троянські коні*.

Найбільш відомими серед знаних «шкідників» є комп'ютерні віруси. Знання механізмів дії «шкідників», зокрема вірусів, дає змогу ефективно організувати протидію їм, звести до мінімуму вірогідність зараження і втрат від їх дії.

Фактично *комп'ютерні віруси* являють собою невеликі виконувані або такі, що так інтерпретуються, програми, які мають властивість поширення і самовідтворення в комп'ютерних системах. Віруси можуть виконувати зміну або знищення програмного забезпечення або даних, що зберігаються в комп'ютерних системах. У процесі поширення віруси можуть себе модифікувати. Усі комп'ютерні віруси класифікуються за такими ознаками: за місцем існування; за способом зараження; у міру небезпеки шкідницьких дій; за алгоритмом функціонування. Доречно зауважити, що за місцем існування комп'ютерні віруси підрозділяються на мережеві, файлові, завантажувальні та комбіновані. Середовищем мешкання мережевих вірусів є елементи комп'ютерних мереж. Файлові віруси розміщуються у виконуваних файлах. Завантажувальні віруси знаходяться в завантажувальних секторах зовнішніх пристроїв, що запам'ятовують. Комбіновані віруси розміщуються в декількох місцях існування. Відзначають, наприклад, завантажувально-файлові віруси.

За способом зараження місця існування комп'ютерні віруси ділять ся на резидентні та нерезидентні. Резидентні віруси після їх активізації повністю або частково переміщаються з місця існування в оперативну пам'ять комп'ютера. Ці віруси, використовуючи, як правило, привілейовані режими роботи, дозволені тільки операційній системі, заражають місце

існування і при виконанні певних умов реалізують шкідницьку функцію. Резидентні віруси активні не тільки в момент роботи інфікованої програми, але і після того, як програма закінчила свою роботу. Резидентні копії таких вірусів залишаються життєздатними аж до чергового перезавантаження, навіть якщо на диску знищені всі заражені файли. Часто від таких вірусів неможливо позбутися відновленням всіх копій файлів із дистрибутивних дисків або backup-копій. Резидентна копія вірусу залишається активною і заражає новостворювані файли. Правильно і те, що для завантажувальних вірусів такі «ліки», як форматування диска за наявності в пам'яті резидентного вірусу, не завжди виліковують диск, оскільки резидентні віруси заражають диск повторно після того, як він відформатований. Нерезидентні віруси потрапляють в оперативну пам'ять комп'ютера тільки на час їх активності, впродовж якого виконують шкідницьку функцію і функцію зараження. Потім вони повністю покидають оперативну пам'ять, залишаючись у місці існування.

У міру небезпеки для інформаційних ресурсів користувача віруси розділяються на нешкідливі, небезпечні та дуже небезпечні. Нешкідливі віруси створюються авторами, які не ставлять собі мети завдати якого-небудь збитку ресурсам комп'ютерної системи. Проте такі віруси все-таки завдають певного збитку: витрачають ресурси комп'ютерної системи та можуть містити помилки, що викликають небезпечні наслідки для інформаційних ресурсів. Так, віруси, створені раніше, можуть призводити до порушень штатного алгоритму роботи системи при модернізації операційної системи або апаратних засобів. Небезпечні віруси викликають істотне зниження ефективності комп'ютерної системи, але не призводять до порушення цілісності й конфіденційності інформації, що зберігається у пристроях, які запам'ятовують. Дуже небезпечні віруси мають такі шкідницькі дії: викликають порушення конфіденційності інформації; знищують інформацію; викликають безповоротну модифікацію (у тому числі й шифрування) інформації: блокують доступ до інформації; призводять до відмови апаратних засобів; завдають збитку здоров'ю користувачів.

За алгоритмом функціонування віруси підрозділяються на ті, що не змінюють середовище проживання під час їх поширення, та ті, що змінюють середовище проживання під час їх поширення.

Процес зараження вірусом програмних файлів можна представити таким чином. У зараженій програмі код останньою змінюється так, щоб вірус отримав управління першим, до початку роботи програми вірусоносія. Під час передачі управління вірусу він якось знаходить нову програму і виконує вставку власної копії в початок або додавання її у кінець цієї, зазвичай ще не зараженої, програми. Якщо вірус записується в кінець програми, то він коригує код програми з тим, щоб отримати управління першим. Після цього управління передається програмі-вірусоносієві, і та нормально виконує свої функції. Витонченіші віруси можуть для отримання управління змінювати системні області накопичувача (наприклад, сектор каталогу), залишаючи довжину і вміст файлу, що заражається, без змін [3, с. 34].

Завантажувальні віруси набули значного поширення в останні роки. Дія цих вірусів структурована таким чином, що, на відміну від файлових вірусів, завантажувальні віруси проникають у завантажувальний сектор диска (Boot-сектор) або в сектор, що містить програму завантаження системного диска (Master Boot Record).

Для боротьби з комп'ютерними вірусами використовуються спеціальні антивірусні засоби й методи їх застосування. Антивірусні засоби виконують такі завдання: а) виявлення вірусів у комп'ютерних системах; б) блокування роботи програм-вірусів; в) усунення наслідків дії вірусів.

Виявлення вірусів і блокування роботи програм-вірусів здійснюється: 1) скануванням; 2) виявленням змін; 3) використанням евристичного аналізу; 4) використанням резидентних сторожів; 5) вакцинацією програм; 6) апаратно-програмним захистом.

Логічні бомби являють собою програми або їх частини, які постійно перебувають у комп'ютері або обчислювальній системі і стають виконуваними тільки у разі дотримання певних умов. Прикладами таких умов можуть бути: наступ заданої дати, перехід системи в певний режим роботи, наступ деяких подій із заданим числом разів тощо.

Хробаки являють собою програми, які виконуються кожного разу під час завантаження системи, мають здатність переміщатися в обчислювальних системах або в мережі та самовідтворювати копії. Лавиноподібне розмноження програм призводить до перевантаження каналів зв'язку, пам'яті та блокування системи. Механізми можуть бути дуже різними: електронна пошта, локальна мережа або USB-накопичувач. Так, хробак може скопіювати файли на флешку і створити відповідний файл автозавантаження, і як тільки ви під'єднаєте флешку до комп'ютера, на ньому відразу ж активізується хробак. При цьому слід зазначити, що хробаки, які поширюються через пошту або через флешки, практично ні в чому не відрізняються, вони лише використовують різні шляхи поширення.

Окремої уваги заслуговують *троянські програми (троянські коні)*. До цих програм відносять програми, що завдають руйнівні дії незалежно від умов, в яких вони діють. Так, вони нищать інформацію на дисках при кожному запуску, «завішують» систему тощо. Більшість відомих троянських коней є програмами, які під час написання «підробляють» під будь-які корисні програми, нові версії популярних утиліт або доповнення до них. Дуже часто вони розсилаються по BBS-станціях або по електронних конференціях. У порівнянні з вірусами «троянські коні» не отримують поширення з достатньо простих причин – вони або знищують себе разом з іншими даними на диску, або демаскують свою присутність і знищуються вже постраждалим користувачем. Отже, троянська програма становить собою програму, яка має певні приховані функції, оправдовуючи свою назву. Свого часу така назва виникла тому, що перші програми цього типу потрапляли на комп'ютери під виглядом корисних програм, які користувачі завантажували й запускали самостійно. Зараз такий варіант поширення також присутній, часто користувачі самі запускають подібні програми, намагаючись завантажити зламані неліцензійні версії програмного забезпечення або програми для генерації зламаних серійних ключів.

В результаті троянські програми під виглядом «кейгенів» і «кряків» досить часто потрапляють на комп'ютери з неліцензійним програмним забезпеченням. Окремо можна виділити «дропери», які проявляються у вигляді інсталяторів троянської програми. Оскільки троянська програма є багатокомпонентним ланцюгом, що вимагає встановлення певних драйверів та інших компонентів, то таке завдання виконують дропери. Після того як «дропер» стає активованим в системі, він встановлює всі частини троянської програми та активує її.

Існують щей інші «шкідливі програми». Так, відомі такі програми, як *бекдори* (програми «чорний хід»). Зазвичай вони відомі як шкідливі програми, які надають зловмисникові віддалений доступ та можливість управління комп'ютером користувача. Методи їх дії бувають різними; наприклад, така програма може відкрити мережевий порт, за допомогою якого зловмисник отримає повний доступ до ураженого комп'ютера, тобто зможе відправляти різні команди, запускати інші програми.

Заслуговує на увагу такий спеціальний вид троянських програм, як *руткіт,* головна мета якого – максимально глибоко встановитися в систему, щоб його було якомога важче знайти й видалити. Як правило, руткіти містять драйвери операційних систем і працюють на досить низькому рівні. Руткіти використовуються для маскування всіх інших компонентів троянця від детектування. Отже, руткіт в системі покликаний приховати роботу інших компонентів трояна. Головна проблема в тому, що руткіти дуже важко знайти та ще важче видалити з системи. Далеко не кожна антивірусна програма може з цим впоратися.

Можна відзначити ще таку програму, як *рекламний модуль*. Останнім часом вона, мабуть, стала найменш небезпечною з усіх шкідливих програм, але через дуже широку поширеність і просто величезну зухвалість їх авторів, яка стала вельми неприємним «подарунком». Як можна здогадатися з назви цього типу шкідників, завдання рекламного модуля – показати вам рекламу. Це може відбуватися в різних проявах, наприклад у вас можуть самостійно відкриватися певні сторінки в браузері, які користувач не відкривав. Це можливо будуть сайти з дивовижною рекламою або просто сайти, які не збиралися відвідувати, тобто зловмисники таким чином підвищують відвідуваність певного сайту або провокують користувача подивитися певну інформацію. Також рекламні модулі можуть показувати різні банери або навіть вставляти банери на той сайт, де їх не було, або ж підміняти рекламні повідомлення на сайтах. Наприклад, якщо ви шукаєте певну інформацію в ГУГЛ, то видача пошукового запиту містить як безплатні пошукові запити й рекламні повідомлення, так рекламні модулі з можливістю їх підміни.

Зауважимо, що останнім часом зловмисники часто використовують такі програми, як «загарбники паролів», що спеціально призначені для крадіжок паролів. При спробі входу в систему імітується введення імені та пароля, які пересилаються власникові програми-загарбника, після чого виводиться повідомлення про помилку введення й управління повертається операційній системі. Користувач, що думає, що припустив помилку при наборі пароля, повторює вхід і дістає доступ до системи.

Проте його ім'я і пароль вже відомі власникові програми-загарбника. Перехоплення пароля може здійснюватися й іншим способом, за допомогою дії на програму, що управляє входом користувачів в систему і її набори даних. Методика дії шкідливих програм значною мірою залежить від організації обробки інформації в системі, розробленої політики безпеки можливостей встановлених засобів захисту, а також сумлінності адміністратора й оператора. Для реалізації несанкціонованого доступу існує два способи: 1) можна здолати систему захисту, тобто шляхом різних дій на неї припинити її дії відносно себе або своїх програм, що складно, трудомістко і не завжди можливо, зате ефективно; 2) можна постежити за тим, що «погано лежить», тобто які набори даних, що представляють інтерес для зловмисника, відкриті для доступу через недогляд або наміру адміністратора. Такий доступ, хоча і з деякою натяжкою, теж можна назвати несанкціонованим, його легко здійснити, але від нього легко і захиститися. Тож важливо відмітити, що наразі будь-якому користувачу мережі необхідно володіти не тільки комп'ютерною грамотністю – знаннями про призначення і можливості комп'ютера для обробки інформації, вміннями користуватися поширеними програмами, але й мати високий рівень інформаційно-технологічної культури [12, с. 618], щоб персональні дані залишались неушкодженими. Стрімкий розвиток інформаційних технологій із широким використанням Інтернету, крім очікуваних позитивних моментів, є причиною зростання порушень юридичних прав як на власність так і на права осіб. Закономірне виникає питання про запобігання порушень та балансом прав та свободою поширення, отриманням інформації та боротьбою зі шкідливим програмним забезпеченням. Стає все більш відчутним дисонанс у стабільності правочинних відносин та інформаційних технологій, який є одним із результатів зловмисного впливу шкідливого програмного забезпечення, що упереджено, усвідомлено вноситься зловмисниками в персональні комп'ютери кінцевих користувачів, в локальні мережі державних, юридичних, адміністративних, комерційних господарчих організацій, в їх бази даних з конфіденційною та службовою інформацією. І тут рішення можливе лише за умови спільних узгоджених дій як провідних експертів з галузі захисту та безпеки інформації, так і спеціалістів, аналітиків юридичного та нормативно-правового напряму з швидким оновленням діючого процесуального законодавства в напрямі боротьби з кіберзлочинами шляхом використання Інтернету та нормативно – правового визначення законодавчо встановленого порядку дослідження судами електронних доказів. На сучасному етапі розвитку суспільства юридичне право відстає, і логічно, що буде відставати, від удосконалення інформаційних технологій, а кіберзлочинці будуть продовжувати використовувати шкідливе програмне забезпечення, одним із результатів дії якого залишаються юридичні конфлікти, що виникають за електронно-паперового формату. І тільки після виконання спільних юридично-технологічних дій можна буде частково уникати проблем, які будуть пов'язані з використанням в Інтернеті такої інформації, що матиме доказове значення. Ефективність заходів у цій сфері повинна досягатися завдяки здійсненню оперативної оцінки

загроз організованої кіберзлочинності, що дозволить визначати сучасні загрози та ризики в кіберпросторі, а також їх завчасно ліквідовувати, і хоча інформаційно-комунікаційні системи існує в межах правового поля (інформаційного законодавства), проте першоосновою протидії кібератакам є технічна сторона питання. Рівні технічного захисту законодавчо не завжди встановлюються шляхом введення спеціальних (національних та міжнародних) стандартів, проте в цілому простежується взаємодія рівня розвитку технічних засобів й технологій та інформаційного законодавства. Випереджальні темпи розвитку технічної складової суспільства дедалі тільки посилюються (див. [4]). На додаток, враховуючи стрімкий ріст комп'ютерних технологій в останні десятиліття, підвищена увага до так званих «комп'ютерних злочинів» не є безпідставною. Річ у тому, що сьогодні практично нічого не робиться без участі комп'ютерів у сфері комунікацій, торгівлі, банківських і біржових операцій тощо. Разом з тим все більш зрозумілим стає те, що законодавчий рівень «запрограмований» на постійне відставання від технологічного розвитку галузі. При цьому всі найважливіші інформаційні функції сучасного суспільства, так або інакше залишаються «зав'язаними» на комп'ютери, комп'ютерних мережі та комп'ютерну інформацію. Тому такі традиційні злочини, як крадіжка, шахрайство, шпигунство, здирство тощо, трансформувалися в нові форми. Крім того, з'явилися специфічні для комп'ютерних систем і мереж злочини. Викреслилася тенденція щодо використання інформаційних технологій організованими злочинними групами й поширення їх діяльності на міждержавний рівень. Співробітники правоохоронних органів при розкритті та розслідуванні комп'ютерних злочинів неминуче натрапляють на великі труднощі, оскільки злочини у сфері комп'ютерної обробки інформації характеризуються високою скритністю, труднощами збору доказів по встановленню фактів їх здійснення, складністю доведення в суді. Суб'єкти злочинів – це, як правило, висококваліфіковані програмісти, інженери, фахівці в області телекомунікаційних систем тощо. Поняття «комп'ютерна злочинність» фактично охоплює злочини, здійснювані за допомогою комп'ютерів, інформаційно-обчислювальних систем і засобів телекомунікацій, або спрямовані проти них з корисливими або деякими іншими цілями. Так, комп'ютерний злочин представляється як кримінально-правове передбачене кримінальним законом умисне порушення чужих прав і інтересів щодо автоматизованих систем обробки даних, здійснене на шкоду правовій охороні прав та інтересів фізичних і юридичних осіб, суспільства і держави. Отже, зазвичай за створення та поширення шкідливих програм у багатьох країнах передбачена кримінальна відповідальність. Зокрема, створення і поширення комп'ютерних вірусів та інших шкідливих програм переслідується і карається відповідно до Кримінального кодексу України (див. ст. 361–363 КК України). Тим не менше не так давно, за інформацією [13], невідомий троян зібрав величезну базу даних з особистими файлами понад 3 мільйонів користувачів Windows; архів об'ємом 1,2 терабайта виявили в мережі. Отже, техніко-правова змагальність у галузі комп'ютерної вірусології продовжується з невизначеним строком змагань.

Література

1. Бойко В.Д., Василенко М.Д., Золотоверх Д.С. Безпека комп'ютерних систем в контексті законодавства та запобігання кіберзагрозам. *Юридичний вісник*. О. : ВД «Гельветика». 2019. № 2. С. 70–76.

2. Actions to be performed on infected objects. Лабораторія Касперського *:* веб-сайт. URL: https://web.archive.org/web/20150809113716; http://latam.kaspersky.com/knowledgebase-article/1526

3. Ясенев В.Н. Конспект лекций по информационной безопасности. Нижний Новгород: Изд. НГУ им. Н.И. Лобачевского. 2017. 252 с.

4. Василенко М.Д. Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість в контексті удосконалення інформаційного законодавства. *Юридичний вісник*. О. : ВД «Гельветика». 2018. № 3. С. 17–34.

5. Василенко М.Д., Золотоверх Д.С., Рачук В.О. Кібербезпека: кіберзагрози та захищеність технічних (інформаційних) систем. *Кібербезпека в сучасному світі:* матеріали всеукраїнської науково-практичної конференції (м. Одеса, 29 листопада 2019 р.) / за ред. О. В. Дикого. Одеса: Видавничий дім «Гельветика», 2019. С. 77–81.

6. Василенко М.Д., Козін О.Б., Право в теорії ризиків: генеза ризиків від правової до інфомаційної складових (інституційний підхід). *Юридичний вісник*. – О. : ВД «Гельветика». 2019. № 4. С. 43–51.

7. Коваленко Д.М., Олещенко Л.М., Юрчишин В.Я. Деякі питання безпеки в інформаційних системах. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки*. Т. 29 (68). Ч. 1. № 3. 2018. С. 141–145.

8. Гломозда Д. Комп'ютерна вірусологія : навчальний посібник. Київ : ВПЦ НаУКМА, 2012. 116 с.

9. Савенко О.С. Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти – Національний університет «Львівська політехніка», Львів, 2019. 425 с.

10. Прищепа О., Доценко О. Огляд статичних методів аналізу зловмисного програмного забезпечення. *Комп'ютерні науки та кібербезпека*. 2020. № 2. С. 15–24.

11. Лисенко С.М., Щука Р.В. Аналіз методів виявлення шкідливого програмного забезпечення в комп'ютерних системах. *Вісник Хмельницького національного університету*. 2020 № 2. (283). С. 101–107.

12. Баландіна Н.М., Слатвінська В.М. Інформаційна культура інформатизованого суспільства. *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру:* у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 21 трав. 2021 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2021. Т. 1. С. 616–618.

13. Невідомий вірус зібрав величезну базу даних з особистими файлами. URL: https://tech.24tv.ua/nevidomiy-virus-zibrav-velicheznu-bazu-danih-novini-tehnologiy_n1656434

Анотація

Василенко М. Д., Рачук В. О., Слатвінська В. М. **Шкідливі програми в контексті розуміння комп'ютерної вірусології та техніко-правової змагальності: міждисциплінарне дослідження.** – Стаття.

У статті досліджено міждисциплінарні зв'язки під час виявлення шкідливих програм, що складають систему комп'ютерної вірусології. Показано, яким чином залежно від механізму дії шкідливих програм їх поділяють на відповідні класи (комп'ютерні віруси, «хробаки», троянські коні, «кейгени», «кряки» «дропери», бекдори, рекламні модулі, руткіти, «загарбники паролів» тощо). Розглянуто процес зараження вірусом програмних файлів. Найбільш відомими серед знаних «шкідників» виділено комп'ютерні віруси, які являють собою невеликі програми і мають властивість поширення і самовідтворення в комп'ютерних системах. Знання механізмів дії «шкідників», зокрема вірусів, дозволяє ефективно організувати протидію їм, звести до мінімуму вірогідність зараження і втрат від їх дії. Відзначено особливості троянських програм, які завдають руйнівні дії незалежно від умов, в яких вони діють. Так, вони нищать інформацію на дисках при кожному запуску, «завішують» систему тощо. Обговорено ефективність заходів у сфері організованої кіберзлочинності, визначаю-

чи межу між технічною та правовою складниками загалом та в боротьбі з нею. Показано, що рівні технічного захисту законодавчо не завжди встановлюються шляхом введення спеціальних стандартів. Однак простежується взаємодія рівня розвитку технічних засобів й технологій та інформаційного законодавства. Визначається, що випереджальні темпи розвитку технічної складової в суспільстві дедалі тільки посилюються. Зазначено, що законодавчий рівень «запрограмований» на постійне відставання від технологічного розвитку галузі. Наголошено на тому, що злочини у сфері комп'ютерної обробки інформації характеризуються високою скритністю, труднощами збору доказів по встановленню фактів їх здійснення, складністю доведення в суді. Приділено увагу міждисциплінарним зв'язкам між шкідливими програмами, комп'ютерною вірусологією та техніко-правовою змагальністю.

Ключові слова: шкідливі програми, комп'ютерна вірусологія, кіберпростір, захист інформації, законодавство, техніко-правова змагальність

Summary

Vasilenko M. D., Rachuk V. A., Slatvinska V. M. **Malicious programs in the context of understanding computer virology and technical and legal competition: an interdisciplinary study.** – Article.

The article examines interdisciplinary connections in the detection of malicious programs that make up the computer Virology system. It shows how, depending on the mechanism of action of malicious programs, they can be divided into appropriate classes (computer viruses, "worms", Trojan horses, "keygens", "cracks", "droppers", backdoors, advertising modules, rootkits, "password invaders", etc.). The process of virus infection of Program Files is considered. The most well-known among the known "pests" are computer viruses, which are small programs and have the property of spreading and self-reproducing in computer systems. Knowledge of the mechanisms of action of "pests", in particular viruses, allows you to effectively organize their counteraction, minimize the likelihood of infection and losses from their action. The features of trojans that cause destructive actions regardless of the conditions in which they operate are noted. So, they destroy information on disks at each launch, "hang" the system, etc. The effectiveness of measures in the field of organized cybercrime was discussed, defining the line between the technical and legal components in general and in the fight against it. It is shown that the levels of technical protection are not always established by law by introducing special standards. However, there is an interaction between the level of development of technical means and technologies and information legislation. It is determined that the faster pace of development of the technical component in society is only getting stronger. It is noted that the legislative level is "programmed" to constantly lag the technological development of the industry. It is noted that crimes in the field of computer information processing are characterized by high secrecy, difficulties in collecting evidence to establish the facts of their commission, and difficulty in proving them in court. Attention is paid to interdisciplinary connections between malware, computer virology, and technical and legal competition.

Key words: malware, cybersecurity, computer virology, cyberspace, security, information security.