в глобальній мережі Інтернет. Описується ситуація неможливості забезпечення безпеки даних існуючим Цивільним кодексом України. Запропоновано можливий вихід з такої ситуації.
Ключові слова: інтелектуальна власність, захист, Інтернет, безпека, авторське право.

This article discusses the protection of intellectual property rights in the global Internet. Describes the situations that can not ensure the data security due to the existing Code of Ukraine. Offered possible ways out.
Keywords: Intellectual Property, protection, internet, safety, copyright.

УДК 658.012

Г.М. ГАРЯЄВА, ст. викладач, НТУ «ХПІ»
Д.О. ШЕВЕРДІН, магістрант, НТУ «ХПІ»

НЕСАНКЦІОНОВАНЕ ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН, ЇХ СИСТЕМ ЧИ КОМП'ЮТЕРНИХ МЕРЕЖ

У статті пропонуються одержані результати, узагальнення і висновки, які можуть бути використані для подальшого дослідження сутності та ознак злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), їх систем та комп'юте-рних мереж; у правотворчій діяльності при підготовці змін та доповнень до чинного кримінального законодавства України; у навчальному процесі при викладанні курсу Особливої частини кримінального права, відповідного спецкурсу та при підготовці науково-практи-чних посібників і методичних рекомендацій. Бібліогр.: 3 назв.
Ключові слова: комп'ютерні мережі, несанкціоноване втручання, електронно-обчислювальні машини, дослідження, кримінальне право.

Вступ. Інформаційний розвиток суспільства та запровадження на державному рівні в Україні використання мережі Internet та інших комп'ютерних систем в усіх сферах суспільного життя, поряд із позитивними здобутками, супроводжується і негативними явищами. Особливу занепокоєність викликає збільшення кількості злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), комп'ютерних систем та мереж, як в світі, так і в Україні, оскільки такі злочини не лише гальмують позитивні тенденції розвитку, а й завдають шкоди суспільству, державі, суб'єктам інформаційних відносин в усіх сферах господарювання та окремим громадянам.

Тому мета роботи полягала в дослідженні правопорушень шкідливо-

го програмного забезпечення, яке може мати будь-який користувач, а також робота полягала у комплексному аналізі об'єктивних і суб'єктивних ознак складу злочину. Актуальність боротьби з вказаними злочинами, неоднозначність підходів та висновків наукових досліджень, щодо змісту ознак складу злочину та необхідність створення відповідної світовим вимогам належної вітчизняної правової бази в цій області, обумовили вибір теми цієї статті.

Небезпека комп'ютерних технологій. Велику небезпеку являє собою поява нових форм злочинної діяльності, пов'язаних з використанням високих технологій, які раніше не були відомі. З такими проявами поки що досить складно вести ефективну боротьбу, як з точки зору кримінального переслідування, так і застосування організаційно-управлінських і кримінологічних заходів з метою їх попередження. До таких злочинних посягань слід віднести умисне втручання в роботу автоматизованих систем, що призводить до збою чи знищенню комп'ютерної інформації або носіїв інформації, чи розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити збій або знищення інформації чи то носіїв інформації, кримінальна відповідальність за які в Україні була встановлена Законом України «Про внесення змін та доповнень до Кримінального кодексу України» від 20 жовтня 1994 р., за яким Кримінальний кодекс України 1960 р. було доповнено статтею 1981 «Порушення роботи автоматизованих систем». Чинний Кримінальний кодекс України також передбачив відповідальність за вчинення таких суспільно-небезпечних діянь у статті 361 «Незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж», в частині 1 якої передбачена відповідальність за «незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, що призвело до збою чи знищення комп'ютерної інформації або носіїв такої інформації, а також розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп'ютерні мережі і здатних спричинити збій або знищення комп'ютерної інформації чи носіїв такої інформації».

Аналіз статистичних даних. За аналізом статистичних даних: відповідно до вироків, що набрали законної сили, у 2008 р. було засуджено за статтями 361-363[1] Кримінального кодексу 57 осіб, що на 5 % менше, ніж у 2007 р. Із них за ст. 361 КК – 43 особи, за ст. 361[1] КК – три особи, за ст. 361[2] КК – чотири особи, за ст. 362 КК – сім осіб.

Найчастіше злочини, відповідальність за які передбачена у статтях 361-363[1] Кримінального кодексу, вчиняли особи у віці: від 30 до 50 років – 23 особи, або 40,4 % від кількості осіб, засуджених за ці злочини; від 18 до 25 років – 18 осіб, або 31,6 %; від 25 до 30 років – 11 осіб, або 19,3 %;

від 50 до 65 років – п'ять осіб, або 8,8 %. До позбавлення волі засуджено всього дві особи, або 3,5 % від кількості осіб, засуджених за ці злочини. Із них одну особу засуджено за ч. 2 ст. 361 Кримінального кодексу та одну особу – за ч. 1 ст. 361^2 КК. Штраф застосовано до 16 осіб, або 28,1 % від кількості засуджених за ці злочини, у тому числі за ст. 361 КК – до 13 осіб, за ст. 361^1 КК – до однієї особи, за ст. 361^2 КК – до однієї особи; за ст. 362 КК також застосовано штраф до однієї особи. Звільнено від покарання з випробуванням 38 осіб, що на 2,7 % більше, ніж у 2007 р. Кількість осіб, щодо яких справи за статтями 361-3631 КК закрито, становить 35 %, тобто така ж, як 2007 р.

Як повідомляється в останній доповіді міжнародного об'єднання у захисті телекомунікаційних технологій Computer Security Institute (CSI), в минулому році більш 85% підприємств і установ Computer Security Institute зіткнулися з випадками вторгнення хакерів в їх комп'ютери, а 94 % мали неприємності від вірусів.

Попри зростаючу кількість наукових досліджень злочинів у сфері використання електронно-обчислювальних машин, їх систем та комп'ютерних мереж, вказані кримінально карані діяння залишилися недостатньо вивченими на рівні взаємопов'язаного й поглибленого аналізу всіх ознак та елементів складу злочину, передбаченого ст. 361 КК України.

Основна мета роботи полягає у комплексному аналізі об'єктивних і суб'єктивних ознак складу злочину, передбаченого статтею 361 («Несанкціоноване втручання в роботу електронно-обчислювальних машин автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку») Кримінального кодексу України, формулюванні пропозицій щодо вдосконалення кримінального законодавства та рекомендацій з питань правильної кваліфікації досліджуваного складу злочину, відмежування його від суміжних складів та кваліфікації його за сукупністю з іншими злочинами.

Відповідно до поставленої мети в роботі вирішуються такі основні завдання: визначення та узагальнення чинників, що обумовлюють кримінальну відповідальність за незаконне втручання в роботу ЕОМ, систем та комп'ютерних мереж; порівняльно-правовий аналіз міжнародно-правових актів, а також кримінального законодавства окремих зарубіжних країн в частині, що стосується кримінальної відповідальності за вчинення злочинів, які є незаконним втручанням в роботу ЕОМ, систем та комп'ютерних мереж; обґрунтування необхідності виокремлення юридичних складів злочинів, які визначені в диспозиції ст. 361 КК України як альтернативні діяння об'єктивної сторони передбаченого нею складу злочину, визначення їх як, відповідно, «Несанкціонований доступ до комп'ютерної інформації» та «Умисне розповсюдження шкідливих комп'ютерних програм»; визначення умисного розповсюдження шкід-

ливих комп'ютерних програм від суміжних складів злочинів; формулювання на підставі проведеного аналізу пропозицій щодо вдосконалення чинного кримінального законодавства, яким регламентується відповідальність за незаконне втручання в роботу ЕОМ, систем та комп'ютерних мереж.

Об'єктом дослідження є проблеми кримінальної відповідальності за злочини у сфері використання ЕОМ, їх систем та комп'ютерних мереж. Науково обґрунтована класифікація об'єктів злочину дозволяє правильно визначити місце конкретного об'єкта в загальній системі суспільних відносин, що є визначальним для точної кваліфікації злочинів. Об'єкт злочину можна визначити, як цінність, що охороняються кримінальним законом, проти яких спрямоване злочинне діяння і яким воно може заподіяти, або спричинити шкоду.

Що до суб'єкту злочину, то в теорії кримінального права загальноприйнятим було вважати під суб'єктом злочину – фізичну особу (людину), яка вчинила передбачене кримінальним законом суспільно-небезпечне діяння і спроможна понести за це кримінальну відповідальність. А також під суб'єктом злочину, передбаченого ст. 361 КК України, розуміють особу, яка вчинила діяння по несанкціонованому доступу до комп'ютерної інформації або умисному розповсюдженню шкідливих комп'ютерних програм у стані осудності, яка досягла 16-тирічного віку. Предметом дослідження є норми кримінального законодавства, що передбачають відповідальність за злочини в сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж.

Методи, які використовувалися в процесі здійснення дослідження це: діалектичний метод – при дослідженні правових механізмів охорони суспільних відносин у сфері використання електронно-обчислювальних машин, їх систем та комп'ютерних мереж; системно-структурний та функціональний методи – при дослідженні родового й безпосереднього об'єктів злочину, передбаченого ст. 361 КК України, а також ознак його об'єктивної та суб'єктивної сторони, суб'єкта цього злочину під кутом зору з'ясування змісту норм чинного законодавства та їх удосконалення; історико-правовий метод – при аналізі факторів, що зумовлюють кримінально-правову заборону зазначених діянь, та дослідженні розвитку законодавства у сфері правової охорони суспільних відносин у сфері використання електронно-обчислювальних машин, їх систем та комп'ютерних мереж від протиправних посягань на них; порівняльно-правовий і догматичний методи – при опрацюванні законодавчих і підзаконних нормативно-правових актів.

На сьогодні поняття «хакерство» в світі набуло кримінально-правового змісту. Хакерами звуть осіб, які, володіючи зазначеними вище вміннями та досвідом, спрямовують свою діяльність на шкоду іншим особам, вчинюючи злочини в комп'ютерних системах. Суть несанкціоновано-

го доступу до комп'ютерної системи полягає в протиправному доступі до комп'ютерної інформації, що належить іншому власнику (користувачу). Хакери використовують безліч різних засобів для того, щоб розпізнати секретні паролі або взагалі обійти захист системи і «увійти» в комп'ютерну систему. Особливу увагу фахівців сьогодні привертає і злочинне розповсюдження комп'ютерного вірусу та інших шкідливих програмних засобів, здатних проникати в автоматизовані системи та руйнувати комп'ютерну інформацію шляхом впливу на програмному рівні. Комп'ютерний вірус – це програма для електронно-обчислювальної машини, яка здатна без відома власника (користувача) і всупереч його бажанню самостійно розмножуватись і розповсюджуватись, порушуючи належну роботу програмного забезпечення електронно-обчислювальної машини та цілісність інформації, що оброблюється такою машиною, системою або комп'ютерною мережею.

Висновки: отже, отримані результати підтверджують, що комп'ютерні технології можуть використовуватися не лише в корисних цілях, а й в якості інструментів для вчинення різних злочинів, починаючи з розповсюдження протизаконних матеріалів і комп'ютерного «піратства» закінчуючи пособництвом бізнесу, пов'язаному з шахрайством.

Список літератури: 1. *Сташис В.В., Тація В.Я.* Кримінальний кодекс України: Наук.-практ. коментар / За заг. ред. – К., 2006. – С. 969. **2.** *Голубєв В.О.* та ін. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. / За заг. ред. професора Р.А. Калюжного. – Запоріжжя: Просвіта, 2001. – 257 с. **3.** Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р. № 80/94-ВР.

Надійшла до редколегії 20.11.2012.

УДК 519.2

Несанкціоноване втручання в роботу електронно-обчислювальних машин, їх систем чи комп'ютерних мереж / Гаряєва Г.М., Шевердін Д.О. // Вісник НТУ «ХПІ». Серія: Актуальні проблеми розвитку українського суспільства. – Харків: НТУ «ХПІ», 2013. – № 6(980). – С. 55-60. Бібліогр.: 3 назв.

В статье предлагаются полученные результаты, обобщения и выводы, которые могут быть использованы для дальнейшего исследования сущности и признаков преступлений в сфере использования электронно-вычислительных машин (компьютеров), их систем и компьютерных сетей; в правотворческой деятельности при подготовке изменений и дополнений в действующем уголовном законодательстве Украины; в учебном процессе при преподавании курса Особенной части уголовного права, соответствующего спецкурса и при подготовке научно-практических пособий и методических рекомендаций.

Ключевые слова: компьютерные сети, несанкционированного вмешательства, электронно-вычислительные машины, исследования, уголовное право.

The article features the results obtained in the study, results and conclusions that can be used to further study the nature and characteristics of crimes in the use of computers (PCs), their systems and computer networks in the law-making activities in the preparation of amendments and additions to existing criminal Law of Ukraine in the learning process in teaching the course of the Special Part of Criminal Law, the relevant study course and in the preparation of scientific and practical manuals and guidelines.

Keywords: computer networks, unauthorized intervention, electronic computers, study criminal law.

УДК 347.78

Г.М. ГАРЯЄВА, ст. викладач, НТУ «ХПІ»
Р.С. СЕЛЕГЕЙ, магістрант, НТУ «ХПІ»

ПЛАГІАТ, ЯК ПОРУШЕННЯ АВТОРСЬКОГО ПРАВА

Робота присвячена проблемі плагіату в сфері авторського права, бо вона не лише приносить збитки певному суб'єкту права, але й наносить шкоду економічному, інтелектуальному та духовному розвитку країни. Дане питання потребує детального розгляду та обговорення задля того, щоб в подальшому не було сумнівів, що держава, за умови суспільної дискусії, удосконалить законодавчу базу і встановить чіткі механізми захисту галузі авторського права від плагіату. Бібліогр.: 4 назв.

Ключові слова: плагіат, авторське право, суміжні права, інтелектуальна власність, компіляція, закон.

Вступ. Плагіат, згідно з Законом України «Про авторське право і суміжні права», визначається як оприлюднення (опублікування), повністю або частково, чужого твору під іменем особи, яка не є автором цього твору [1]. Тобто, зафіксовані наступні ознаки, за якими використання твору може бути визнано як «плагіат», а саме:

1) *оприлюднення* (опублікування твору) повністю або частково *чужого твору*;

2) твір оприлюднюється *під іменем особи, яка не є автором цього твору.*

Предметом захисту авторських прав є суб'єктивні авторські права, а також законні інтереси. Суб'єктами права на захист є автори творів науки, літератури і мистецтва, їх спадкоємці та інші правонаступники. Порушниками авторських прав може бути будь-які фізичні або юридичні особи, які своїми діями (або бездіяльність) порушили закріплені в нормативно-правових атах положення, якими регулюються правовідносини у сфері авторського права прав [2].