УДК 621.396

П.Д. БІЛЕНЧУК*, *канд. юрид. наук, проф.*,
Д.П. БІЛЕНЧУК**, ***Л.В. БОРИСОВА*******, ***М.В. КОЗИР*******

*Національна академія внутрішніх справ**,
*Національний політехнічний університет "КПІ"***,
*Національний університет внутрішніх справ****

КРИМІНАЛЬНЕ КОМП'ЮТЕРНЕ ПРАВО: УКРАЇНСЬКЕ ТА ЄВРОПЕЙСЬКЕ

Розглянуто сучасний стан української та європейської правових систем та напрямки нормативного визначення у кримінальному законодавстві відповідальності за вчинення комп'ютерних злочинів

Різні країни мають свої національні правові системи. У деяких з них розвинуті спеціальні норми у кримінальному законодавстві, що передбачають відповідальність за вчинення комп'ютерних злочинів, інші тільки у процесі прийняття відповідних законів.

У багатьох державах відповідальність за вчинення комп'ютерних злочинів наступає за традиційними статтями кримінального законодавства, адаптованих до нових умов (крадіжка, шахрайство, підробка та інші).

На міждержавному рівні, у відповідності з рекомендаціями Комітету з питань законодавства Ради Європи 1990 р., прийнята у відповідності з зазначеною міжнародною класифікацією комп'ютерних злочинів, їх стисла характеристика. Подаємо її у порівняльному правовому аналізі згідно з чинним законодавством України.

1. Втручання та перехоплення.

1.1. Незаконний доступ. Код: QAH.

«Незаконний доступ до комп'ютерної системи або мережі».

Метою злочину є комп'ютерна система або мережа (два чи більше комп'ютери). Доступ означає проникнення в усю систему або його частину, до комп'ютерних програм та даних, які там містяться.

Засоби зв'язку не мають значення. Це може бути прямий фізичний доступ до комп'ютера або входження з віддаленого місця, наприклад, із застосуванням супутникового зв'язку або через іншу комп'ютерну систему.

У деяких країнах важливим елементом цього злочину є подолання системи захисту комп'ютера (наприклад, системи паролів). В інших – незаконним є будь-яка навмисна спроба несанкціонованого доступу до комп'ютерної системи або мережі. З розвитком міжнародних комп'ютерних мереж такі злочини можуть мати інтернаціональний характер у випадках, коли злочинець знаходиться в одній країні і незаконно входить до комп'ютерної системи (автоматизованого банку даних), розташованої в іншій країні.

(Подібно до норм статей 361–363 Кримінального кодексу (КК) України Розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж») [1].

1.2. Перехоплення. Код: QAI.

«Незаконне перехоплення за допомогою будь-яких технічних пристроїв та засобів зв'язку даних, які знаходяться в комп'ютерній системі або мережі, чи прямують до або з неї».

Метою злочину є будь-яка форма комп'ютерного зв'язку (телекомунікації). Найчастіше це стосується перехоплення інформації, яка передається громадськими або приватними системами телекомунікації. Це може бути зв'язок у середині єдиної комп'ютерної системи, між двома комп'ютерними системами, між двома комп'ютерами або комп'ютером та особою. Перехоплення, в технічному аспекті, може здійснюватися «прослуховуванням» змісту повідомлення, що може бути забезпечено через прямий

доступ та використання самої комп'ютерної системи, або через непрямий доступ з використанням електронних засобів підслуховування чи підключення. Протиправними є тільки ті випадки, коли такі дії вчинюються незаконно та навмисно.

(КК України: ст.359. «Незаконне використання спеціальних технічних засобів негласного отримання інформації»; ст.231–232. «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю» та інші, у сукупності зі ст.361–363).

1.3. Викрадення часу. Код: QAT.

«Неправомірне використання комп'ютера або комп'ютерної мережі з наміром уникнути оплати за користування».

Великі компанії по обслуговуванню комп'ютерних систем та мереж використовують засоби автоматичних розрахунків за користування з метою обліку користувачів та отримання належної оплати. Спроби ухилитись від оплати за використані послуги є формою крадіжки.

(КК України: ст.185-188, 190-194).

2. Зміна або пошкодження інформації (комп'ютерних даних). Код QD:

2.1. «Логічна бомба». Код: QDL.

«Незаконна заміна комп'ютерних даних або програм шляхом впровадження «Логічної бомби».

«Логічна бомба» у комп'ютерних технологіях не має чіткого офіційного, законодавчого визначення. Це логічний засіб на рівні комп'ютерної програми, який впроваджується злочинцями і стає активним, коли система виконує специфічні завдання (наприклад, коли починає працювати комп'ютерна програма по виплаті заробітної платні).

Будучи у стані активності, «Логічна бомба» запускає невелику комп'ютерну програму, яка має шкідливий вплив на роботу комп'ютерної системи, мережі. Цей вплив може бути різним: комп'ютер може припинити роботу, згаснути екран чи будуть знищеними машинні дані.

Різновидом «Логічної бомби» є «Часова бомба», яка стає активною у чітко визначений день та час.

(КК України: ст.185-187, 191, 193 у сукупності зі ст.361–363).

2.2. «Троянський кінь». Код: QDT.

«Незаконна зміна комп'ютерних даних або програм шляхом впровадження «Троянського коня»

Так само, як і у випадку з «Логічною бомбою», поняття «Троянський кінь» не має законодавчого визначення. «Троянський кінь» – прихована комп'ютерна програма, що використовується злочинцями для отримання доступу до комп'ютера, незважаючи на систему захисту. Оскільки захисні функції комп'ютера контролюються системними програмами-утилітами, «Троянський кінь» при його впровадженні робить відповідні зміни.

(КК України: ст.185-187, 191, 193, у сукупності зі ст.361–363).

2.3. «Комп'ютерні віруси». Код: QDV.

«Незаконна зміна комп'ютерних даних або програм шляхом впровадження чи розповсюдження комп'ютерних вірусів».

«Комп'ютерний вірус» – це комп'ютерна програма або частина комп'ютерної програми, яка змінює дані або програми, порушуючи цілісність системи. «Комп'ютерні віруси» набули значного розповсюдження завдяки здатності заражених файлів інфікувати інші файли, «переходячи» з комп'ютера на комп'ютер (нерідко з допомогою дискет), Існує сотні різновидів вірусів, кожний з яких має власну характеристику, але всі вони змінюють або самі дані, або комп'ютерні програми. Вплив «комп'ютерних вірусів» може бути різний: від незначних незручностей у користуванні комп'ютером до повного знищення машинних даних, у тому числі комп'ютерного програмного забезпечення.

(КК України ст.361–363).

2.4. «Комп'ютерні черв'яки». Код: QDW.

«Незаконна зміна комп'ютерних даних або програм пересилкою, впровадженням або розповсюдженням комп'ютерних черв'яків по комп'ютерних телекомунікаційних мережах».

Законодавчого визначення категорії «комп'ютерних черв'яків» немає. Це логічний засіб (комп'ютерна програма), яка зроблена для того, щоб «мандрувати» по комп'ютерній мережі, пошкоджуючи чи змінюючи автоматизовані бази даних. Вони не так поширені, як комп'ютерні віруси. Відповідальність повинна наступати за ту шкоду, яку вони спричинили.

(КК України: ст.361–363).

3. Комп'ютерне шахрайство (пов'язане з використанням систем комп'ютера). Код: QF.

Комп'ютерне шахрайство відрізняється від звичайного тільки тим, що злочинці використовують переваги сучасних комп'ютерних технологій та мереж телекомунікації. Шахрайства, пов'язані з комп'ютерами, за відсутності специфічних правових норм, підпадають під існуючі в кримінальному законодавстві визначення диспозицій шахрайських дій. Метою злочину може бути отримання незаконного прибутку, результат злочину – заподіяння потерпілому економічних збитків.

3.1. Шахрайства з автоматами по видачі готівки. Код: QFC.

«Шахрайство та крадіжки з використанням автоматів по видачі готівки».

Електронні автомати по видачі готівкових грошей розповсюджені у багатьох країнах світу. Впроваджуються вони сьогодні і в Україні.

Одним із видів таких автоматів є використання карток при одержанні готівки із автоматичних касових машин (ATM – Automated Teller Machines). Деякі фінансові заклади випускають спеціальні картки для користування ATM. Для деяких видів цих автоматів використовуються закодовані пластикові банківські картки, типу Visa і Mastercard.

У будь-якому випадку картка використовується разом з персональним ідентифікаційним номером (так званий Pin – Personal Identification) для доступу до ATM. Персональний ідентифікаційний номер відомий тільки власникові картки.

Незважаючи на засоби технічного захисту, злочинці постійно зламують ATM, застосовуючи, як чисто силові (фізичні) засоби (злом, руйнування тощо), так і шахрайські дії з маніпулюванням електронної інформації, записаної на магнітному носії пластикової картки тощо. У більшості випадків картку і персональний код злочинці отримують внаслідок крадіжки у законного власника, або обманним шляхом від відповідного фінансового закладу (банку тощо). Відомі випадки, коли шахраї телефонують до особи, яка загубила картку, представляючись інспектором банку, запитують, нібито з метою перевірки реєстрації картки, персональний ідентифікаційний номер. Після чого рахунок стає доступним для крадіжки через касові автомати. Відповідальність законного власника *картки за збитки, завдані в разі неправомірного* використання його картки і особистого коду, зазвичай не перевищує 50 доларів США. Фінансові компанії постійно наголошують, що клієнти несуть певну відповідальність за збереження персонального ідентифікаційного номера.

З поширенням банкоматів в Україні є ймовірність, що злочини з використанням їх, можуть поширитися й у нас.

Розвиток сучасних інформаційних технологій дозволяє робити різні маніпуляції з картками.

3.2. Комп'ютерна підробка. Код: QFF.

«Шахрайство та крадіжки пов'язані з виготовленням підроблених засобів із застосуванням комп'ютерних технологій».

Підробка програмного забезпечення комп'ютерної системи спостерігається, наприклад, тоді, коли до комп'ютера вводиться інша інформація на заміну існуючої або використовується дійсна інформація, але в шахрайських цілях. Це також може бути виготовлення даних на мікрочіпі – звичайний приклад підробки електронного серійного номера стільникового або інших видів мобільних телефонів.

Сучасні технології, зокрема розвиток лазерних кольорових принтерів, дозволяють робити копії документів, які раніше не можна було підробити. Це підробка грошових банкнотів, фінансових документів, таких як рахунки, облігації та інші цінні папери.

(КК України: ст.199, 200, 216, 217, 223, 224 у сукупності зі ст.361–363).

3.3. Шахрайства з комп'ютеризованими ігровими автоматами. Код: QFG.

«Шахрайство та крадіжки з використанням ігрових автоматів».

Сучасні ігрові автомати контролюються автоматизованою (комп'ютерною) програмою, яка записана на мікрочіпі. Ці чіпи розробляються компаніями з виробництва комп'ютерних програм і можуть бути об'єктом крадіжки, заміни даних або несанкціонованого копіювання. Технічний аналіз чіпа – це завдання для інженера-програміста.

(КК України: ст.185, 190, у сукупності зі ст.361–363).

3.4. Шахрайства шляхом неправильного введення/виведення (маніпулювання) комп'ютерними програмами. Код: QFM.

«Крадіжка шляхом шахрайства способом неправильного введення/виведення з

комп'ютерної системи інформації або маніпуляції з комп'ютерними програмами».

Неправильний вхід до комп'ютерної бази даних і заволодіння майном шляхом обману чи заволодіння довір'ям – звичайний спосіб вчинення шахрайства.

У таких випадках необхідний повний технічний опис системи, включаючи програмне забезпечення. Неправильний вихід менш розповсюджений і, як правило, стосується виготовлення підроблених документів або інших роздрукувань даних.

Існує три категорії комп'ютерного програмного забезпечення:

1) комп'ютерні програмні продукти (комп'ютерні програми та автоматизовані бази даних) для комерційного продажу;

2) безкоштовне експериментальне програмне забезпечення, яке було перероблене з конкретною метою;

3) унікальні, спеціальні комп'ютерні програмні продукти, написані для спеціальних цілей і не призначені для продажу та розповсюдження (у військових та інших державних чи комерційних цілях тощо).

(КК України: ст.190, у сукупності зі ст.361–363).

3.5. Шахрайства з засобами платежу. Код: QFP.

«Шахрайство та крадіжка, пов'язані з платіжними засобами та системами реєстрації платежів».

Ці системи, як правило, використовуються в пунктах роздрібної торгівлі. Вони належать таким фінансовим компаніям як банки, та захищені від стороннього доступу, оскільки ними передається інформація про переказ платежів по комп'ютерних закодованих телекомунікаційних лініях. Маються на увазі усі різновиди магнітних карток (кредитні, дебетні тощо).

(КК України: ст.190, у сукупності зі ст.361–363).

3.6. Телефонне шахрайство. Код: QFT.

«Несанкціонований доступ до електронних телекомунікаційних послуг з порушенням загальноприйнятих протоколів та процедур».

Шахрайство з телефонними розмовами може бути окреслене як неправильне використання телекомунікаційних послуг. Іноді ці злочини вчинюються з метою уникнути сплати рахунків за послуги, іноді – щоб уникнути підслуховування.

Прикладом телефонного шахрайства є застосування спеціального пристрою, який може маніпулювати обміном телефонними переговорами. Пристрій генерує звуки, на які автоматизована телефонна станція відповідає з'єднанням без включення лічильника рахунку часу розмови.

Іншим прикладом є неправомірне використання стільникових телефонів (у тому числі автомобільних). При цьому немає необхідності у фізичному контакті. Розмова може відбутися шляхом підключення за допомогою сканування номера-коду законного користувача. Можливе також перепрограмування коду стільникового телефону, після чого злочинець буде використовувати телефон, а рахунки надійдуть до іншої особи чи організації.

(КК України: ст.185, 190 у сукупності зі ст.361–363).

4. Несанкціоноване копіювання комп'ютерної інформації, комп'ютерне піратство. Код: QR.

4.1. Несанкціоноване копіювання комп'ютерної гри. Код: ORG.

«Несанкціоноване копіювання, розповсюдження або публікація комп'ютерних ігор».

(КК України: ст.136. «Порушення авторського права»).

4.2. Несанкціоноване копіювання комп'ютерних програмних продуктів (комп'ютерних програм, автоматизованих баз даних). Код: QRS.

«Несанкціоноване копіювання, розповсюдження або публікація комп'ютерних програмних продуктів, захищених авторським правом».

У більшості країн авторське право поширюється на твори науки, літератури і мистецтва. Воно становить інституцію права власності, його складової – права інтелектуальної власності чи інформаційного права. Комп'ютерні програми відносяться також до об'єктів авторського права.

(КК України: ст.176, 177. «Порушення авторського права і суміжних прав»).

4.3. Несанкціоноване копіювання топології напівпровідникової продукції (інтегральних мікросхем). Код: QRT.

Аналогічно до пункту 4.2.

5. Комп'ютерний саботаж. Код: QS.

5.1. Комп'ютерний саботаж апаратного

(технічного) забезпечення. Код: QSH.

«Внесення, зміна, пошкодження або знищення комп'ютерних даних або програм, а також втручання до комп'ютерної системи, з наміром перешкоджати функціонуванню комп'ютера або телекомунікаційної системи».

Головна мета цього злочину – перешкоджати функціонуванню комп'ютера або телекомунікаційної системи. Цей склад злочину охоплює ширше коло діянь, ніж пошкодження комп'ютерних даних.

Комп'ютерний саботаж включає всі види втручання до комп'ютерної системи, в тому числі, введення неправильних даних або несанкціоноване введення даних для того, щоб порушити роботу системи. Сюди також відносяться усі види фізичного руйнування комп'ютера, відключення напруги.

Наприклад, хакери можуть досягти цієї мети за допомогою модифікації системних файлів.

(КК України: ст.361–363.)

5.2. Комп'ютерний саботаж програмного забезпечення. Код: QSS.

«Незаконне пошкодження, порушення, викривлення та знищення комп'ютерних даних або програм».

Пошкодження даних аналогічно руйнуванню фізичного об'єкта. Знищення та викривлення інформації є практично зміною даних, при якій втрачається практична вартість пошкодженої програми чи даних. Такі дії є злочинними лише тоді, коли вони скоєні навмисно.

(КК України: ст.361–363. У сукупності зі ст.359).

6. Інші злочини, пов'язані з комп'ютерними технологіями. Код: QZ.

До комп'ютерних злочинів відноситься і крадіжка комерційної таємниці, що відомо у світі як комп'ютерне промислове шпигунство, коли інформація міститься у пам'яті комп'ютера.

(КК України: ст.231–232. «Незаконне збирання з метою використання відомостей, що становлять комерційну таємницю»).

6.1. Зберігання або розповсюдження матеріалів, які є об'єктом судового переслідування. Код: QZS.

«Використання комп'ютерних систем або мереж для зберігання або пересилки матеріалів, які є об'єктом судового переслідування»

Матеріалами, які є об'єктами судового переслідування, можуть бути порнографія (у тому числі дитяча), пропаганда насильства та жорстокості, расової дискримінації.

6.2. Незаконне використання електронної дошка об'яв (BBS). Код: QZB.

«Використання BBS для приховування, обміну та розповсюдження матеріалів, пов'язаних з кримінальними злочинами».

Bulletin Board Systems (BBS) – це так звані електронні дошки об'яв у регіональних і глобальних комп'ютерних мережах телекомунікації, де можуть накопичуватись повідомлення і здійснюватися обмін інформацією. Висловлюючись образно, це зустріч великої кількості осіб, які можуть спілкуватись, не називаючи себе. Дошки електронних об'яв дозволяють дуже швидко розповсюджувати інформацію. Найчастіше вони використовуються злочинцями для розповсюдження порнографії (зокрема дитячої), інформації для хакерів (паролі, рахунки), нелегально скопійованих комп'ютерних програмних продуктів. Наприклад, у комп'ютерних мережах типу Інтернет дошки електронних об'яв можуть поширювати інформацію у будь-які країни.

(КК України: ст.300–301).

6.3. Викрадення комерційної таємниці. Код: QZE.

«Незаконне привласнення або розголошення, передавання або використання комерційної таємниці з наміром спричинити економічні збитки або отримати незаконні економічні вигоди».

Нелегальне комп'ютерне програмне забезпечення та ін. Розповсюдження таких матеріалів, як правило, переслідується кримінальним законом у більшості країн світу. Використання з цією метою сучасних комп'ютерних телекомунікаційних технологій стає все більш соціально небезпечним, оскільки збільшуються швидкість та територія розповсюдження такої інформації.

(КК України: ст.231–232).

ЛІТЕРАТУРА

1. Кримінальний кодекс України. -К.: Право, 2001. –174 с.

Надійшла до редколегії 13.03.2002

БИЛЕНЧУК П.Д., БИЛЕНЧУК Д.П., БОРИСОВА Л.В., КОЗЫРЬ М.В. КРИМИНАЛЬНОЕ КОМПЬЮТЕРНОЕ ПРАВО: УКРАИНСКОЕ И ЕВРОПЕЙСКОЕ
Рассмотрено современное состояние украинской и европейской правовых систем и направления нормативного определения в криминальном законодательстве ответственности за совершение компьютерных преступлений.

***

BILENCHUK P.D., BILENCHUK D.P, BORISOVA L.V., KOZYR' M.V. THE CRIMINAL COMPUTER RIGHT: UKRAINIAN AND EUROPEAN
Here are described modern condition of Ukrainian and European law systems and directions of normative definition of responsibility for committed cyber-crimes in the criminal law.

УДК 343.126

А.П. БУЩЕНКО

Национальная юридическая академия им. Ярослава Мудрого

К КОНЦЕПЦИИ ЗАКЛЮЧЕНИЯ ПОД СТРАЖУ

Рассмотрены проблемы судебного усмотрения при решении вопроса о досудебном аресте обвиняемого, приведена критика комментария нового законодательства, предложенного в одном из недавних обзоров и указано на некоторые последствия неосторожных дефиниций.

Любой решительный поворот в законодательной политике непременно создает тенденцию к сопротивлению, которая может проявиться, в том числе, и в попытках толковать новые законодательные правила так, чтобы в наименьшей степени изменить устоявшиеся представления и практику. В недавнем комментарии к новому законодательству в сфере заключения под стражу П.П. Пилипчук дал толкование ряда положений [1, с.44-49], которое при ближайшем рассмотрении может показаться проявлением этой тенденции к «адаптивному» толкованию.

Новеллы Уголовно-процессуального кодекса Украины [2], помимо известных изменений в процедуре решения вопроса о предварительном заключении под стражу, затронули также и материальный аспект системы мер пресечения. До этого уголовное судопроизводство имело ясные критерии для разрешения вопроса о заключении под стражу, основанные на признаке тяжести обвинения. В зависимости от своей тяжести преступления распадались на несколько видов. Первый – это преступления, подпадающие под правило бывшей ч.2 ст.155 УПК, где сам факт подозрения в совершении одного из перечисленных преступлений был достаточным основанием для заключения под стражу. Второй – преступления, предусматривающие лишение свободы до года включительно, когда заключение под стражу не применялось, кроме как в исключительных случаях. Третий вид определялся этими границами, и здесь решение вопроса о заключении под стражу зависело от свободной оценки обстоятельств каждого случая.

Июньскими изменениями 2001 года законодатель, во-первых, отменил ч.2 ст.155 УПК, тем самым признав, что заключение под стражу не может применяться только исходя из тяжести обвинения, что отмечает и П.П. Пилипчук: «законодатель отказался от положения о том, что одна лишь опасность определенного преступления, в совершении которого обвиняется лицо, является достаточным основанием для избрания меры пресечения в виде содержания под стражей» [1, с.45]. Действительно, «содержание под стражей может быть оправдано в каждом случае, если существуют конкретные указания на подлинные интересы общества, которые, несмотря на презумпцию невиновности, перевешивают правило уважения личной свободы»