IV Висновок

Підписання Україною Конвенції про кіберзлочини стало важливим етапом на шляху до інтеграції в Європу. Наступним логічним кроком має стати ратифікація зазначеної конвенції Верховною Радою України та практичні рішення щодо її реалізації. У зв'язку з цим слід зазначити, що розробка ефективних заходів протидії злочинам у сфері високих технологій вимагає співробітництва між державою і комерційними підприємствами, що працюють на ринку Інтернет-послуг. Держава може тільки тоді ефективно боротися з кіберзлочинами, коли діє в партнерстві з підприємцями, що здійснюють свою діяльність в глобальних інформаційних мережах. Відповідно до цього, правоохоронним органам слід організувати співробітництво з Інтернет-провайдерами, контент-провайдерами, фінансовими компаніями, що надають послуги в мережі Інтернет, а також з електронними магазинами по реалізації спільної протидії комп'ютерній злочинності, особливо в частині, що стосується виявлення та ідентифікації злочинців.

Література: 1. М. В. Гуцалюк Проблеми протидії комп'ютерній злочинності // Бюлетень з обміну досвідом роботи. Науково-практичне видання: МВС. – 2001. № 135. – С. 26-31. 2. Компьютерные террористы: Новейшие технологии на службе преступного мира./Автор- составит. Т. И. Ревяко. - Мн.: Литература, 1997. – 640 с. 3. Комп'ютерна злочинність. – К.: Атіка. – 2002. – 240 с. 4. М. Вест-Браун, К. Коссаковский Международная инфраструктура за глобальную безопасность и реагирование в сфере информационных технологий. – 1999 // http://bezpeka.com. 5. Указ Президента України від 6 грудня 2001 року № 1193/2001 Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України". 6. Постанова КМ України від 14 грудня 2001 р. № 1694 Про затвердження Програми реалізації положень Варшавської конференції щодо спільної боротьби проти тероризму.

УДК 681.3

КОМЕНТАР ДО СТАТЕЙ 361 – 363 КК УКРАЇНИ

Петро Андрушко
Київський Національний Університет України ім. Т. Шевченка

Анотація: **Дається науково-практичний коментар до статей 361 – 363 нового КК України, які встановлюють відповідальність за вчинення комп'ютерних злочинів.**
Summary: **This article is dedicated commenting the articles 361 – 363 of the new Crime Code of Ukraine, which dispose responsibility for committing computer crimes.**
Ключові слова: **Злочинність, кримінальний кодекс, злочин, автоматизовані електронно-обчислювальні машини (комп'ютери), їх системи та мережі, відповідальність, інформація.**

"Комп'ютерна" злочинність стала однією з міжнародних проблем, що зумовлено створенням міжнародних інформаційних систем, таких, наприклад, як мережа "Інтернет", яка об'єднує обчислювальні центри і системи більш як 70 країн і забезпечує обмін даними між різноманітними джерелами і користувачами, яких десятки мільйонів. В розвинених країнах "комп'ютерна" злочинність завдає величезних збитків власникам і користувачам автоматизованих систем, примушує їх витрачати значні кошти на розробку і впровадження програмних, технічних та інших засобів захисту від несанкціонованого доступу до інформації, її перекручення чи знищення. Останнім часом і в Україні спостерігається стрімке зростання злочинів, пов'язаних з втручанням в роботу автоматизованих систем, зокрема, в систему банківських електронних платежів. Як правило, втручання в їх роботу здійснюється з метою вчинення інших, більш тяжких злочинів: розкрадання майна; його вимагання під погрозою знищення чи спотворення інформації, яка обробляється чи зберігається в автоматизованих системах; ознайомлення з такою інформацією, її викрадення, знищення тощо.

Новий КК України від 05. 04. 2001 р. містить 3 статті, що передбачають відповідальність за вчинення так званих "комп'ютерних злочинів" – втручання до роботи автоматизованих електронно-обчислювальних машин (комп'ютерів, АЕОМ), їх систем та мереж: ст. 361, 362, 363 КК України.

Статтею 361 передбачена відповідальність за дві самостійні форми незаконного втручання в роботу автоматизованих електронно-обчислювальних машин (комп'ютерів), їх систем чи комп'ютерних мереж (КС): 1) незаконне втручання в роботу КС, що призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації; 2) розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних

засобів, призначених для незаконного проникнення в КС і здатних спричинити перекручення або знищення комп'ютерної інформації чи то носіїв такої інформації.

Предметом цього злочину є:

1) Автоматизовані електронно-обчислювальні машини (комп'ютери) – це комплекси електронних пристроїв, побудованих на основі мікропроцесора, за допомогою яких здійснюються визначені комп'ютерною програмою чи користувачем операції (послідовність дій з обробки інформації і керування електронними пристроями) щодо символьної і образної інформації, зокрема, здійснюються її введення та виведення, знищення, копіювання, модифікація, передача інформації у системі чи мережі АЕОМ та інші інформаційні процеси. АЕОМ складається, як правило, із трьох частин: системного блоку, який включає в себе мікропроцесор і інші пристрої, необхідні для його роботи (нагромаджувачі даних, блок живлення тощо), клавіатури, за допомогою якої вводяться в АЕОМ символи, та монітора, на якому відображається текстова і графічна інформація.

2) Системи автоматизованих електронно-обчислювальних машин (системи АЕОМ) або автоматизовані системи (АС) – це системи, що здійснюють автоматизовану обробку даних, до складу яких входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення [1]. До складу системи АЕОМ входить, принаймні, одна АЕОМ (комп'ютер) та периферійні пристрої, що працюють на основі такої АЕОМ: принтер, сканер, модем, сітьовий адаптер, стример та ін.

3) Комп'ютерна мережа – це комплекс з'єднаних лініями електрозв'язку АЕОМ чи їх систем.

4) Носії комп'ютерної інформації – фізичні об'єкти, поля і сигнали, хімічні середовища, нагромаджувачі даних в інформаційних системах [2].

5) Комп'ютерні віруси – це комп'ютерні програми (програми-віруси), які заражають електронні обчислювальні машини (комп'ютери), внаслідок чого комп'ютер виконує несанкціоновані, небажані дії. Розрізняються "комп'ютерні віруси" і "логічні бомби". Особливістю "комп'ютерних вірусів" є їх здатність відтворювати себе в декількох примірниках, змінювати (модифікувати) комп'ютерну програму, до якої вони приєднались, тим самим порушуючи нормальне функціонування комп'ютерної програми, що використовується конкретним, "зараженим" комп'ютером. "Комп'ютерні віруси" і "логічні бомби" повністю чи частково виводять із ладу програму за певних умов, наприклад, при настанні певного часу. На відміну від "комп'ютерних вірусів", які можуть розповсюджуватися комп'ютерними мережами, "логічні бомби" не переходять в інші програми, а існують у певній комп'ютерній програмі. Кримінально-правове значення мають лише ті види комп'ютерних вірусів, які призначені не лише для незаконного проникнення в КС, але й для перекручення або знищення комп'ютерної інформації чи носіїв такої інформації.

6) Комп'ютерна інформація – це інформація, що використовується в АЕОМ, яка є сукупністю всіх даних і програм, які використовуються в АЕОМ незалежно від способу їх фізичного та логічного представлення [1], тобто це інформація, що використовується за допомогою АЕОМ (комп'ютера), яка містить відомості про певні факти, події, предмети, явища, процеси, окремих осіб тощо, а також програми для АЕОМ і бази даних, має ідентифікаційні реквізити власника, який визначив режим (правила) їх використання. Комп'ютерна інформація може знаходитись на носіях інформації, в АЕОМ, системі АЕОМ чи мережі АЕОМ.

7) Програмні і технічні засоби, призначені для незаконного проникнення в автоматизовані електронно-обчислювальні машини, їх системи чи комп'ютерні мережі.

Об'єктивна сторона злочину характеризується двома видами дій: 1) втручання в роботу КС; 2) розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в КС і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації.

Незаконне втручання в роботу КС є **злочином з матеріальним складом**, оскільки, крім різноманітних дій у вигляді різного впливу на їх роботу, обов'язковими ознаками об'єктивної сторони цього злочину є також наслідки у вигляді перекручення чи знищення комп'ютерної інформації, тобто порушення її цілісності (руйнування, спотворення, модифікація і знищення) [2] і причинний зв'язок між вчиненими діями і наслідками. Відсутність наслідків у вигляді перекручення або знищення комп'ютерної інформації чи носіїв такої інформації при втручанні в роботу КС, залежно від мети такого втручання, може кваліфікуватися: 1) як замах на вчинення злочину, передбаченого ст. 361, якщо метою втручання було спотворити або знищити інформацію, її носії; 2) за статтями 114, 231 КК (за наявності ознак цих злочинів), якщо метою втручання в роботу КС було незаконне ознайомлення з інформацією, яка в них обробляється чи зберігається; 3) за іншими статтями КК, які передбачають відповідальність за злочини, спосіб вчинення яких може виражатись у незаконному втручанні в роботу КС, наприклад, як розкрадання майна, виготовлення з метою збуту чи використання підроблених недержавних цінних паперів (ст. 224 КК), незаконні дії з документами на переказ та іншими засобами доступу до банківських рахунків (ст. 200 КК).

Розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в КС і здатних спричинити перекручення або знищення комп'ютерної інформації

чи носіїв такої інформації, є **злочином з формальним складом,** оскільки об'єктивна сторона цього злочину виражається в самих діях, незалежно від того, спричинили вони чи ні наслідки у вигляді перекручення або знищення комп'ютерної інформації чи носіїв такої інформації.

Під **незаконним втручанням у роботу АЕОМ, їх систем чи комп'ютерних мереж** треба розуміти будь-які дії, що впливають на обробку інформації, яка в них вводиться, зберігається, чи передається для обробки в КС, тобто дії, що впливають на всю сукупність операцій (введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін каналами передачі даних. При втручанні в роботу КС здійснюється порушення їх роботи, яке спричиняє спотворення процесу обробки інформації, внаслідок чого перекручується або знищується сама комп'ютерна інформація чи її носії.

Знищення інформації – це її втрата, коли інформація в КС перестає існувати для фізичних і юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі. Як знищення, втрату інформації треба розглядати і її блокування, тобто припинення доступу до інформації користувачам КС. Втручання в роботу КС може бути і в формі впливу на канали передачі інформації як між технічними засобами її обробки і зберігання всередині КС, так і між окремими КС, внаслідок чого інформація, що передається для обробки, знищується чи перекручується. Такі дії можуть виражатись, наприклад, в електромагнітному, лазерному та іншому впливі на носії інформації, в яких вона матеріалізується або якими вона передається; в формуванні сигналів, полів, засобів і блоків програм, вплив яких на інформацію, її носії і засоби технічного захисту викликає порушення цілісності інформації, її знищення чи спотворення; у включенні до бібліотек програм спеціальних програмних блоків, зміни програмного забезпечення та інших подібних діях, що призводять до порушення цілісності інформації.

Перекручення інформації – це зміна її змісту, порушення її цілісності, в тому числі і часткове знищення.

Під **розповсюдженням** комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в КС, і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації, треба розуміти: 1) їх передачу будь-яким способом і на будь-яких підставах (продаж, дарування, обмін, надання можливості скопіювати тощо) з метою використання особами, які згідно з правилами розмежування доступу до інформації, встановленими власником інформації чи уповноваженою ним особою, не мають права доступу до такої інформації; 2) їх "закладку" в КС на стадії їх виготовлення, ремонту, реалізації, користування з метою використання в майбутньому для здійснення несанкціонованого доступу до інформації; 3) ознайомлення інших осіб із змістом програмних засобів чи технічними характеристиками або технологією виготовлення і використання технічних засобів для незаконного проникнення в КС.

Програмні засоби, призначені для незаконного проникнення в АЕОМ, їх системи чи комп'ютерні мережі – це спеціальні комп'ютерні програми (програмні блоки, програмне забезпечення), за допомогою яких можна здійснити несанкціонований доступ до інформації, яка зберігається чи обробляється в КС і які здатні спотворити або знищити інформацію (її носії) шляхом спотворення процесу обробки інформації.

Під комп'ютерною програмою розуміється набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах) [3].

Технічні засоби, призначені для незаконного проникнення в АЕОМ, їх системи чи комп'ютерні мережі – це різного роду прилади, обладнання, устаткування тощо, за допомогою яких можливе або безпосереднє підключення до КС чи каналів передачі даних, або які здатні шляхом формування сигналів, полів, середовищ створити умови для несанкціонованого доступу до інформації з метою ознайомлення з такою інформацією особами, які не мають права доступу до неї, або з метою впливу на процес обробки інформації в АЕОМ, порушення роботи КС, перекручення або знищення комп'ютерної інформації чи її носіїв.

Обов'язковою ознакою (властивістю) програмних і технічних засобів, призначених для незаконного проникнення в КС для визнання їх предметом злочину, що коментується, є їх здатність впливати на процес обробки інформації, його спотворення, в результаті чого інформація (її носії) може бути знищена чи перекручена. Якщо ж такі засоби за своїми технічними характеристиками не мають такої властивості, їх розповсюдження складу злочину, передбаченого ст. 361 КК, не утворює. Використання таких програмних і технічних засобів, наприклад, для незаконного ознайомлення з інформацією, яка обробляється чи зберігається в КС, може кваліфікуватися за статтями 114 або 231 КК.

Суб'єктивна сторона злочинів, передбачених ч. 1 ст. 361 КК, характеризується умислом щодо дій, які вчинюються винним, а психічне ставлення винного до наслідків у вигляді перекручення чи знищення комп'ютерної інформації або її носіїв може характеризуватись як прямим чи непрямим умислом, так і необережністю в обох її видах. При розповсюдженні комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в КС, умисел лише прямий, оскільки суб'єктивну

сторону цього злочину визначає психічне ставлення винного до вчинюваних ним дій. Мотиви і мета вчинення злочинів можуть бути різними і свідчити про те, що робота КС порушена, наприклад, з метою вчинення інших злочинів.

Прямий умисел при умисному втручанні в роботу КС, що призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації, матиме місце тоді, коли метою такого втручання є, в кінцевому підсумку, перекручення чи знищення комп'ютерної інформації, що використовується (обробляється) КС, або ж знищення носіїв такої інформації.

Непрямий умисел при втручанні в роботу КС матиме місце у випадках, коли втручання мало метою здійснити несанкціонований доступ до інформації для незаконного ознайомлення з нею, наприклад, з метою одержати відомості, що містять державну чи іншу, охоронювану законом, таємницю, наприклад, комерційну таємницю чи відомості конфіденційного характеру, ознайомлення з якою, її використання чи розголошення може заподіяти шкоду суспільству і державі, юридичним і фізичним особам. Неправомірне одержання інформації з обмеженим доступом, тобто отримання її з порушенням правил розмежування доступу, встановлених власником інформації чи уповноваженою ним особою, може здійснюватись технічними засобами космічної, повітряної, морської, наземної розвідок або шляхом порушення правил розмежування доступу до інформації з обмеженим доступом в КС, засобах обчислювальної техніки, лініях зв'язку – шляхом несанкціонованого доступу до неї [2]. Неправомірне одержання інформації може супроводжуватись перекрученням або знищенням комп'ютерної інформації чи носіїв такої інформації. При цьому особа усвідомлює, що неправомірне отримання комп'ютерної інформації може бути поєднане з перекрученням або знищенням самої комп'ютерної інформації чи її носіїв, і, не бажаючи таких наслідків, свідомо допускає їх настання. Втручання в роботу КС, що призвело до перекручення або знищення інформації чи її носіїв, вчинене з метою незаконного отримання інформації, залежно від змісту такої інформації і мети її неправомірного одержання, повинно кваліфікуватися за сукупністю злочинів: за ст. 361 КК і, відповідно, за ст. ст. 114 чи 231 КК.

Суб'єктом злочину може бути будь-яка фізична особа, яка досягла 16-річного віку. Ним можуть бути і особи з персоналу КС – фізичні особи, яких власник такої КС або уповноважена ним особа чи розпорядник КС визначили для здійснення функцій управління та обслуговування КС, і сторонні особи. Суб'єктами злочину у формі розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в КС і здатних спричинити перекручення або знищення комп'ютерної інформації чи її носіїв, можуть бути розробники таких програмних і технічних засобів, їх виготовлювачі, зокрема, виробники (розробники) програм з комп'ютерними вірусами, так звані "технопацюки", "хакери" та інші, в середовищі яких вважається, що чим складніша система захисту в автоматизованій системі, тим престижніше її зламати, і які витрачають на таку діяльність величезну працю, ставлячи перед собою єдину мету – спричинити шкоду значній кількості користувачів КС.

В. ч. 2 ст. 361 КК передбачена відповідальність за три кваліфікованих види складу злочину: 1) спричинення істотної шкоди; 2) вчинення злочину повторно; 3) вчинення злочину за попередньою змовою групою осіб.

Визнання заподіяної шкоди при порушенні роботи КС істотною залежить від багатьох обставин: 1) вартості комп'ютерної інформації чи її носіїв, знищених чи перекручених; 2) збитків, спричинених неможливістю використання знищеної або перекрученої комп'ютерної інформації чи її носіїв; 3) затрат на відновлення змісту перекрученої або знищеної комп'ютерної інформації чи її носіїв; 4) збитків внаслідок використання неправомірно одержаної комп'ютерної інформації тощо. При цьому не повинні враховуватись витрати, які несуть власники, розпорядники і користувачі КС для технічного захисту інформації в них від несанкціонованого доступу до інформації, її приховування, затрати на заходи з технічної дезінформації тощо.

Слід розглянути також кваліфікуючі ознаки злочину, передбаченого ст. 361 КК.

Повторним є злочин, вчинений особою, яка раніше вчинила будь-який із злочинів, передбачених ч. 1 чи ч. 2 ст. 361, незалежно від того, чи була вона раніше засуджена за вчинений злочин. При цьому необхідно, щоб судимість за раніше вчинений злочин не була знята чи погашена і не скінчились строки давності притягнення до кримінальної відповідальності чи строки давності виконання вироку.

Вчинення порушення роботи КС **за попередньою змовою групою осіб** передбачає домовленість двох або більше осіб про спільне вчинення незаконного втручання в роботу КС, чи про спільне розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в КС і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації. При цьому не обов'язково, щоб усі особи безпосередньо виконували в повному обсязі дії, зазначені в ч. 1 ст. 361 КК (наприклад, одна особа може займатись виготовленням програм з комп'ютерними вірусами, друга – їх тиражуванням, третя – їх реалізацією, четверта – розробкою технічних засобів для незаконного проникнення в КС, неправомірного одержання інформації, яка зберігається чи обробляється в АЕОМ). При цьому дії співучасників, які безпосередньо не вчинили дій, що утворюють об'єктивну сторону незаконного втручання в роботу КС, повинні кваліфікуватися з посиланням на ст. 27 КК. У разі вчинення злочину, передбаченого ст. 361,

організованою групою з розподілом ролей, дії всіх членів такої групи повинні кваліфікуватися безпосередньо за ст. 361.

Незаконне втручання в роботу КС може бути способом вчинення інших, найчастіше більш тяжких, злочинів: диверсії (ст. 113 КК), шпигунства (ст. 114 КК), розкрадання майна (ст. 190 КК), виготовлення з метою збуту або використання підроблених недержавних цінних паперів (ст. 224 КК) та інших. У таких випадках дії винного повинні кваліфікуватися за сукупністю злочинів: за ст. 361 КК і відповідною статтею КК, яка передбачає відповідальність за злочин, вчинений шляхом незаконного втручання в роботу КС.

Предметом злочину, передбаченого ст. 362 КК України, є комп'ютерна інформація, поняття якої вже розглядалося вище.

Інформація, в т. ч. і комп'ютерна, є об'єктом права власності громадян, організацій (юридичних осіб) і держави, вона може бути об'єктом права власності як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження. Підставами виникнення права власності на інформацію є її створення своїми силами і за свій рахунок, договір на створення інформації або договір, що містить умови переходу права власності на інформацію до іншої особи. Власник інформації має право здійснювати щодо неї будь-які законні дії [4].

Комп'ютерна інформація не є окремим видом інформації, вона є формою зберігання статистичної, масової, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру, інформації про діяльність державних органів влади та органів місцевого і регіонального самоврядування, наукової, технічної та іншої інформації на носіях комп'ютерної інформації.

Право власності на комп'ютерну інформацію, створену як вторинну в процесі обробки в КС, встановлюється з урахуванням норм авторського права на підставі угоди між власником вхідної інформації і користувачем АЕОМ. Якщо такої угоди немає, то така інформація належить користувачу АЕОМ, який здійснив цю обробку. Доступ до інформації, яка зберігається, обробляється і передається в АЕОМ, здійснюється лише згідно з правилами розмежування доступу, встановленими власником інформації чи уповноваженою ним особою [1].

Комп'ютерна інформація є об'єктом права інтелектуальної власності, але не є майном, тобто не є предметом злочинів, передбачених статтями 185–187, 189–191 КК, а тому, незалежно від вартості викраденої інформації чи інформаційної продукції чи розміру завданої її викраденням шкоди, дії винного не можуть кваліфікуватися як розкрадання за ст. ст. 185–187 чи 189–191. В той же час викрадення комп'ютерної інформації, її привласнення чи заволодіння нею шляхом шахрайства чи зловживання службової особи своїм службовим становищем разом з матеріальним носієм, на якому вона зафіксована, залежно від вартості носія інформації та способу незаконного заволодіння таким носієм має кваліфікуватися, за наявності підстав, за сукупністю злочинів – за ст. 362 та статтями 185–187, 189–191 КК чи ст. 51 КпАП України, оскільки матеріальний носій є майном, тобто предметом злочинів проти власності.

З об'єктивної сторони злочин виражається у викраденні, тобто у заволодінні комп'ютерною інформацією шляхом крадіжки, грабежу чи розбою, її привласненні або заволодінні нею шляхом шахрайства чи зловживання службовою особою своїм службовим становищем, або у вимаганні такої інформації.

Поняття "викрадення" вживається у КК як родове щодо позначення таких способів заволодіння чужим майном як "крадіжка", "грабіж" та "розбій".

Про поняття "крадіжка", "грабіж", "розбій", "вимагання", "шахрайство", "привласнення", "заволодіння шляхом зловживання службовою особою своїм службовим становищем" та про момент закінчення таких дій див. коментарі до ст. ст.185–187, 189–191 КК.

Способи викрадення комп'ютерної інформації чи заволодіння нею можуть бути різними: копіювання інформації, вилучення матеріальних носіїв інформації, на яких вона зберігається, чи заволодіння ними. Здебільшого викрадення комп'ютерної інформації вчинюється таємно шляхом несанкціонованого доступу (втручання в роботу) до КС, у яких вона зберігається чи обробляється. Якщо такий несанкціонований доступ буде пов'язаний із перекрученням чи знищенням комп'ютерної інформації чи її носіїв, дії винного мають додатково кваліфікуватися і за ст. 361 КК за наявності всіх інших необхідних ознак передбаченого нею злочину.

Застосування насильства при відкритому викраденні комп'ютерної інформації чи її вимаганні не охоплюється ст. 362 КК і має кваліфікуватися додатково за статтями КК, що передбачають відповідальність за злочини проти здоров'я.

Викрадення комп'ютерної інформації шляхом незаконного використання спеціальних технічних засобів негласного отримання інформації має кваліфікуватися за сукупністю злочинів – за ст. 362 та ст. 359 КК.

Незаконне ознайомлення з інформацією, не пов'язане із її викраденням чи заволодінням нею, а також її незаконне розголошення, не може кваліфікуватись за ст. 362. Такі дії, за наявності підстав, можуть кваліфікуватися за ст. ст. 114, 163, 182, 231 чи 330 КК.

Із **суб'єктивної сторони** злочин характеризується лише умисною виною, вид умислу прямий. Як правило, передбачені ч. 1 ст. 362 КК дії вчинюються з корисливих мотивів і мети, але можуть бути вчинені і з іншою метою, наприклад, з метою розголошення відомостей, що містяться у комп'ютерній інформації.

Суб'єктом злочину у формі викрадення комп'ютерної інформації шляхом крадіжки, грабежу чи розбою, заволодіння нею шляхом шахрайства, а також вимагання комп'ютерної інформації може бути будь-яка особа, що досягла 16-річного віку. Суб'єкт злочину у формі привласнення комп'ютерної інформації та заволодіння нею шляхом зловживання службовою особою своїм службовим становищем спеціальний: особа, що має доступ до комп'ютерної інформації у зв'язку з виконанням нею роботи з управління, експлуатації чи обслуговування КС або службова особа.

Кваліфікованими видами злочину є викрадення, привласнення, вимагання комп'ютерної інформації чи заволодіння нею шляхом шахрайства чи зловживання службовим становищем, вчинене повторно або за попередньою змовою групою осіб або якщо воно заподіяло істотну шкоду.

Повторним слід вважати повторне вчинення особою у будь-якій послідовності передбачених ч. 1 ст. 362 КК дій за умови, що вони не охоплюються єдиним умислом і не утворюють у своїй сукупності єдиного продовжуваного злочину, тобто умисел на їх вчинення кожен раз виникав самостійно.

Вчиненим за **попередньою змовою групою осіб** викрадення, привласнення, вимагання комп'ютерної інформації чи заволодіння нею шляхом шахрайства чи зловживання службовою особою своїм службовим становищем буде у разі, коли зазначені дії вчинені двома або більше особами, які попередньо домовились про спільне їх вчинення.

Комп'ютерні програми і комп'ютерні бази даних є об'єктами авторських і суміжних прав, а тому їх викрадення, привласнення чи незаконне заволодіння ними і наступне незаконне відтворення чи розповсюдження має кваліфікуватись за сукупністю злочинів за ст. 362 та ст. 176 КК.

Викрадення інформації, її привласнення чи незаконне заволодіння інформацією, що містить відомості про об'єкти права промислової власності (винахід, корисна модель, промисловий зразок, кваліфіковане зазначення походження товарів, топографія інтегральних схем, сорт рослин) та її наступне незаконне використання, має кваліфікуватись за сукупністю злочинів за ст. 362 та ст. 177 КК. База даних – це сукупність творів, даних або будь-якої іншої незалежної інформації у довільній формі, в тому числі – електронній, підбір і розташування складових частин якої та її упорядкування є результатом творчої праці, і складові частини якої є доступними індивідуально і можуть бути знайдені за допомогою спеціальної пошукової системи на основі електронних засобів (комп'ютера) чи інших засобів [3].

Стаття 363 КК встановлює відповідальність за порушення правил експлуатації АЕОМ.

Технічний захист комп'ютерної інформації в КС забезпечується комплексом конструкторських, організаційних, програмних і технічних заходів на всіх етапах їх створення й експлуатації. Основними методами та засобами технічного захисту комп'ютерної інформації є: використання захищених засобів; регламентування роботи користувачів, технічного персоналу, програмних засобів, елементів баз даних і носіїв інформації (розмежування доступу); регламентування архітектури автоматизованих систем і засобів обчислювальної техніки; інженерно-технічне оснащення споруд і комунікацій, призначених для експлуатації автоматизованих систем і засобів обчислювальної техніки; пошук, виявлення і блокування закладних пристроїв [2].

З **об'єктивної сторони** злочин виражається у порушенні правил експлуатації КС (дія чи бездіяльність), визначених їх 1) власником, уповноваженою ним особою чи розпорядником таких КС чи 2) виробником КС чи їх програмного забезпечення. Обов'язковими ознаками об'єктивної сторони є наслідки у вигляді: 1) витоку інформації внаслідок її викрадення чи копіювання; 2) викрадення засобів захисту комп'ютерної інформації; 3) перекручення або знищення комп'ютерної інформації чи засобів її захисту; 4) істотного порушення роботи КС, а також причинний зв'язок між зазначеними діяннями і наслідками. Витік інформації може бути пов'язаний також із її втратою (знищенням чи пошкодженням).

Наслідки у вигляді перекручення або знищення комп'ютерної інформації чи засобів її захисту та істотного порушення роботи КС, можуть бути спричинені діями (бездіяльністю) як осіб, які здійснюють їх експлуатацію чи відповідають за технічне чи інше забезпечення їх належної експлуатації, так і діями інших, сторонніх осіб, а у вигляді викрадення комп'ютерної інформації, її копіювання чи викрадення засобів захисту комп'ютерної інформації – лише діями сторонніх осіб, які не є відповідальними за експлуатацію КС.

Порушення правил експлуатації КС може виражатись у порушенні правил експлуатації або апаратного забезпечення, або програмного забезпечення. Порушенням правил експлуатації АЕОМ має визнаватись також невиконання чи неналежне виконання обов'язків з технічного забезпечення захисту комп'ютерної інформації, зокрема з пошуку, виявленню і блокуванню закладних пристроїв тощо.

Порушення встановлених норм і вимог технічного захисту комп'ютерної інформації поділяються на три категорії: перша – невиконання норм і вимог технічного захисту комп'ютерної інформації, в результаті чого

створюється реальна можливість порушення цілісності цієї інформації або її витоку технічними каналами; друга – невиконання норм і вимог технічного захисту комп'ютерної інформації, в результаті чого створюються передумови для порушення цілісності цієї інформації або її витоку; третя – невиконання інших вимог технічного захисту інформації з обмеженим доступом [2].

Про поняття "викрадення" комп'ютерної інформації, "перекручення чи знищення" комп'ютерної інформації вже йшлося вище. Викрадення комп'ютерної інформації може бути вчинене шляхом несанкціонованого доступу до неї, приймання й аналізу побічних електромагнітних випромінювань і наводок, використання закладних пристроїв.

Засоби захисту комп'ютерної інформації – це технічні пристрої і (або) технологічні розробки, призначені для створення технологічної перешкоди несанкціонованого доступу до комп'ютерної інформації.

Копіювання комп'ютерної інформації – це її відтворення у електронному вигляді, перенесення на інший носій інформації з використанням програмних та (або) технічних засобів АЕОМ. Копіювання комп'ютерної інформації без використання програмно-технічних засобів АЕОМ, наприклад, шляхом сканування випромінювання монітора спеціальним технічним засобом, має розглядатись як її викрадення.

Визнання порушення роботи КС істотно залежить від тривалості переривання їх роботи, складності і тривалості їх ремонту тощо.

Із **суб'єктивної сторони** злочин, передбачений ч. 1 ст. 363 КК, характеризується непрямим умислом чи необережністю щодо наслідків у вигляді викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, незаконного копіювання комп'ютерної інформації чи істотного порушення роботи КС. Саме ж порушення правил експлуатації КС може бути як умисним, так і необережним.

Суб'єкт злочину спеціальний – особа, яка відповідає за експлуатацію КС. До таких осіб відносяться особи, які безпосередньо здійснюють експлуатацію КС, управління ними, а також особи, які забезпечують належну їх експлуатацію або здійснюють їх обслуговування і на яких покладена відповідальність за належну їх експлуатацію. Це може бути оператор АЕОМ, особа технічного персоналу, на яку покладені обов'язки з забезпечення безпечної експлуатації АЕОМ, їх ремонту, профілактичного обслуговування, охорони від несанкціонованого доступу до них, забезпечення технічного захисту комп'ютерної інформації, її приховування та ін.

Кваліфікованим видом злочину є порушення правил експлуатації КС, якщо воно заподіяло **істотну шкоду**. Шкода може бути як матеріальною, так і не матеріальною.

Порушення правил експлуатації КС особою, яка відповідає за їх експлуатацію, з метою незаконного копіювання комп'ютерної інформації, її привласнення чи заволодіння нею службовою особою шляхом зловживання своїм службовим становищем, за відсутності інших наслідків, передбачених ст. 363 КК, має кваліфікуватися лише за ст. 362 КК, оскільки таке порушення є способом вчинення злочину, передбаченого ст. 362, і додаткової кваліфікації за ст. 363 КК не потребує. Якщо ж внаслідок зазначеного порушення матиме місце витік, викрадення, перекручення чи знищення комп'ютерної інформації, або викрадення засобів її захисту іншими особами, або істотне порушення роботи КС, то дії особи мають кваліфікуватися за сукупністю злочинів за ст. 362 та ст. 363 КК.

Література: 1. Закон України "Про захист інформації в автоматизованих системах" від 05. 07. 1994 р. // ЗУ. Том 7. – К., 1997. – С. 296. 2. Положення про технічний захист інформації в Україні, затв. постановою КМ України від 09. 09. 1994 р. № 632 // ЗП України. – 1994. – № 12. – С. 302. 3. Закон України "Про авторське право і суміжні права" від 23. 12. 1993 р. в ред. 11. 07. 2001 р. // ГУ, 2001, 16. 08. 4. Закон України "Про інформацію" від 02. 10. 1992 р. ст. 38. \\ ВВРУ, 1992, № 48, С. 650.

УДК 638.235.231

АУДИТ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ПРОБЛЕМЫ И РЕШЕНИЯ

Юрий Борсуковский
Фирма «Бартек»

Аннотация: **Рассмотрены вопросы аудита систем информационной безопасности.**
Summary: **The audit questions of information safety are considered in the given report.**
Ключевые слова: **Информация, информационная безопасность, тест, аудит, обследование.**