ПЛУГАТИР М. В.,
кандидат юридичних наук,
старший викладач кафедри
адміністративного права і процесу
(Національна академія внутрішніх справ)

УДК 343.974:343.346.8

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА НЕСАНКЦІОНОВАНІ ЗБУТ АБО РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ, ЯКА ОБРОБЛЮЄТЬСЯ В ДЕРЖАВНИХ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСАХ

Статтю присвячено актуальним питанням кримінально-правової протидії кіберзлочинам, кваліфікації зазначених суспільно небезпечних діянь та питанням встановлення кримінальної відповідальності за їх вчинення.

Ключові слова: *комп'ютерний злочин, кіберзлочин, кібертероризм, інформаційна безпека, кримінальне законодавство.*

Статья посвящена актуальным вопросам уголовно-правового противодействия киберпреступлениям, квалификации указанных общественно-опасных деяний, а также вопросам уголовной ответственности за их совершение.

Ключевые слова: *компьютерное преступление, киберпреступление, кибертерроризм, информационная безопасность, уголовное законодательство.*

In this article actual problems of criminal responsibility for cybercrimes, its qualification and amendment of penal regulations are researched.

Key words: *computer crime, cybercrime, cyberterrorism, information security, criminal law.*

Вступ. З прийняттям Верховною Радою України 16 січня 2014 року Закону України «Про внесення змін до Закону України «Про судоустрій і статус суддів» та процесуальних законів щодо додаткових заходів безпеки громадян» № 721-VII до Кримінального кодексу України (далі – ККУ) було включено ст. 361^4 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка оброблюється в державних електронних інформаційних ресурсах» [1]. Включення даної норми у кримінальне законодавство потребує її дослідження з метою визначення ознак складу злочину, за який передбачається відповідальність. Необхідним є визначення об'єктивних та суб'єктивних ознак вказаного злочину, його кваліфікації та відмежування, шляхів удосконалення чинного законодавства, врахування позитивного попереднього досвіду у питанні протидії аналогічним посяганням тощо.

Зазначене обумовлює необхідність дослідження норм, що містяться у Розділі XVI Особливої частини КК України. Результати попередніх досліджень зазначеного розділу викладені в роботах таких науковців, як Д.С. Азаров, В.М. Бутузов, М.В. Карчевський, А.А. Музика, С.Л. Остапець, Н.А. Розенфельд, В.П. Шеломенцев та ін. Тому дослідження ст. 361^4 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка оброблюється в державних електронних інформаційних ресурсах» ККУ проводилось з урахуванням здобутків зазначених науковців, адже вони зробили вагомий внесок в наукову розробку злочинів у сфері комп'ютерної інформації.

Постановка завдання. Необхідно враховувати, що останні зміни у чинному законодавстві України про кримінальну відповідальність, а саме встановлення відповідальності за несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка оброблюється в державних електронних інформаційних ресурсах, вимагає подальшого проведення роботи у визначеному напрямку. Зазначена необхідність обумовлює мету даної статті, що полягає у встановленні сутності та ознак складу злочину, передбаченого ст. 361^4 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка оброблюється в державних електронних інформаційних ресурсах» ККУ.

Результати дослідження. В сучасних умовах соціально-економічного розвитку України комп'ютерна злочинність стала реальністю. Негативні тенденції обумовлені тим, що інформація стала першоосновою життя сучасного суспільства, предметом та продуктом його діяльності. Інформація стала об'єктом суспільних (інформаційних) відносин та набула товарних рис, оскільки є предметом купівлі-продажу. Можливо констатувати значний обсяг договірних відносин, пов'язаних із виготовленням, передачею, накопиченням та використанням інформації в різних її формах: науково-технічної документації, програмного забезпечення, систем управління базами даних та інше. Відсутність чіткого визначення комп'ютерної злочинності та єдиного розуміння змісту цього явища значно ускладнюють діяльність правоохоронних органів у протидії

таким видам злочинних посягань. Значною проблемою є відсутність добре збалансованої та ефективної нормативної бази в сфері використання комп'ютерних систем, що також стосується кримінального законодавства. Включення до нього останніх змін, а саме ст. 3614 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка оброблюється в державних електронних інформаційних ресурсах», потребує проведення дослідження сукупності ознак складу даного злочину, що визначає потребу у розгляді наступної низки елементів складу даного злочину.

Об'єктом злочину несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, яка оброблюється в державних електронних інформаційних ресурсах, виступають суспільні відносини власності на комп'ютерну інформацію з обмеженим доступом.

Предметом злочину є інформація з обмеженим доступом, яка оброблюється в державних електронних інформаційних ресурсах, створена та захищена відповідно до чинного законодавства. Тобто інформація, що є предметом злочину, характеризується такими ознаками:

1) вона відноситься до інформації з обмеженим доступом;

2) оброблюється в державних електронних інформаційних ресурсах;

3) створена відповідно до чинного законодавства;

4) захищена відповідно до чинного законодавства.

До *інформації з обмеженим доступом* згідно зі статтею 30 Закону України «Про інформацію» [2] відноситься таємна і конфіденційна інформація.

До таємної інформації належать відомості, що становлять державну та іншу *передбачену законом* таємницю, розголошення якої завдає шкоди особі, суспільству, державі.

Державна таємниця – вид таємної інформації, яка охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України, які віднесено законом до державної таємниці й поставлено під охорону з боку держави. Віднесення інформації до державної таємниці та порядок її використання визначаються Законом України «Про державну таємницю» від 21 січня 1994 року [3]. Перелік відомостей, що становлять державну таємницю, затверджується наказом директора Служби безпеки України.

До таємної інформації, крім державної, відноситься також інша передбачена законом таємниця, розголошення якої завдає шкоди особі, суспільству, державі. Такою може бути, наприклад, таємниця страхування [4], таємниця усиновлення, таємниця досудового слідства тощо.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні *окремих фізичних або юридичних осіб,* розповсюджуються *на їх розсуд* і відповідно до передбачених ними умов. Виходячи з аналізу частини 3 статті 30 Закону України «Про інформацію» [2], можна залежно від характеру, змісту відомостей, що складають конфіденційну інформацію, виділити такі її види: професійна, ділова, виробнича, банківська, комерційна, іншого характеру. Громадяни та юридичні особи, котрі володіють інформацією професійного, ділового, комерційного та іншого характеру, придбаною на власні кошти або такою, що є предметом їх професійного, ділового, комерційного та іншого інтересу, самостійно визначають її належність до конфіденційної.

За конструкцією ***об'єктивної сторони*** злочин є формальним. Він вважається закінченим з моменту вчинення несанкціонованого збуту або несанкціонованого розповсюдження комп'ютерної інформації з обмеженим доступом.

Збут або розповсюдження інформації буде *несанкціонованим*, коли він вчиняється без дозволу власника цієї інформації.

Розповсюдження комп'ютерної інформації з обмеженим доступом являє собою оплатне або безоплатне надання копій цієї інформації або доступу до неї невизначеному колу осіб.

Під *збутом комп'ютерної інформації з обмеженим доступом* необхідно розуміти її оплатне або безоплатне відчуження.

Суб'єкт злочину – загальний. Якщо збут або розповсюдження інформації з обмеженим доступом вчиняє особа, якій інформацію було довірено у зв'язку з виконанням службових або професійних обов'язків, вчинене за наявності відповідних ознак суб'єктивної сторони, необхідно кваліфікувати за статтею 232 або 328 КК України.

Суб'єктивна сторона даного злочину характеризується виною у формі прямого умислу: особа усвідомлює суспільну небезпечність і протиправність збуту або розповсюдження комп'ютерної інформації з обмеженим доступом та бажає вчиняти такі дії. Особа усвідомлює, що комп'ютерна інформація, яку вона збуває або розповсюджує, є інформацією з обмеженим доступом; усвідомлює, що не має права або дозволу власника інформації на вчинення подібних дій.

Відмежування від 3612 ККУ за місцем обробки інформації (державні електронні інформаційні ресурси) та санкціями, у ст. 3614 ККУ вони більш суворі.

Кваліфікуючими ознаками злочинів, передбачених статтею 3614, ККУ виступають:

– вчинення комп'ютерного злочину повторно;

– вчинення комп'ютерного злочину за попередньою змовою групою осіб;

– вчинення комп'ютерного злочину, який заподіяв значну шкоду.

Оскільки в розділі XVI Особливої частини КК України не передбачено повторності однорідних злочинів, комп'ютерний злочин слід вважати вчиненим ***повторно*** у випадках, коли особа два або більше рази вчинила злочин, який було кваліфіковано за однією статтею даного розділу. При цьому вчинення декількох таких злочинів не охоплювалося єдиним умислом (злочин не був продовжуваним), особа не звільнялася від кримінальної відповідальності за тотожний злочин, не закінчилися строки давності притягнення до кримінальної відповідальності за раніше вчинений злочин або судимість за нього не було погашено чи знято.

Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка оброблюється в державних електронних інформаційних ресурсах, будуть вважатися вчиненими ***групою осіб за попередньою змовою*** за наявності відповідних об'єктивних і суб'єктивних ознак. Об'єктивна сторона його може бути такою: діяння вчиняється двома або більше виконавцями, кожен із яких виконує всі дії, що утворюють об'єктивну сторону складу; злочин вчиняється двома або більше співвиконавцями, кожен із яких виконує частину дій, що характеризують об'єктивну сторону; злочин вчиняється двома або більше особами, при цьому лише одна з них відіграє роль виконавця, а інші є підбурювачами, пособниками або організаторами.

Кожен із співвиконавців повинен мати всі ознаки суб'єкта, тобто бути фізичною, осудною особою та досягти віку кримінальної відповідальності. У випадку, коли особа не була поінформована про те, що вчиняє комп'ютерний злочин разом із малолітнім або неосудним, її дії слід кваліфікувати за правилами фактичної помилки як замах на вчинення комп'ютерного злочину групою осіб за попередньою змовою.

До об'єктивних ознак вчинення злочину за попередньою змовою групою осіб відноситься також спільність, що характеризується взаємозумовленістю дій, загальним для всіх співучасників наслідком і наявністю причинного зв'язку між діями співучасників й злочином, який вчинив виконавець.

Значною шкодою в статті 361^4 ККУ, якщо вона полягає в заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів (примітка до статті 361 ККУ). Зазвичай ця шкода полягає в заподіянні *позитивних матеріальних збитків.* У такому випадку її необхідно оцінювати, виходячи з витрат власника на придбання комп'ютерної інформації. Але стосовно значної шкоди як кваліфікуючої ознаки комп'ютерного злочину слід зауважити, що іноді вона може виражатися і в *упущеній вигоді.*

Крім матеріальної шкоди, суспільно небезпечні наслідки при вчиненні комп'ютерного злочину можуть виражатись і в *нематеріальних видах шкоди*, що зумовлено використанням державних електронних інформаційних ресурсів для контролю над складними технологічними процесами, об'єктами та керування ними.

Висновки. В цілому ст. 361^4 ККУ побудована за тими самими принципами, як і 361^2 ККУ. Тому слід зазначити, що ст. 361^4 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка оброблюється в державних електронних інформаційних ресурсах» за своїм змістом є майже тотожною до ст. 361^2 «Несанкціонований збут або розповсюдження інформації з обмеженим доступом, що зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації». Відмінністю між ними є те, що злочинне діяння, передбачене у ст. 361^4 ККУ, створює загрозу функціонуванню державних електронних інформаційних ресурсів та пов'язане з посяганням на інформацію, яка оброблюється в зазначених ресурсах. А злочин, відповідальність за який встановлено у ст. 361^3 ККУ, ставить під загрозу функціонування електронно-обчислювальних машин, систем і комп'ютерних мереж у сфері зберігання, опрацювання, зміни, доповнення, передавання й одержання інформації, що не відносяться до державних електронних інформаційних ресурсів. Більш доцільним при встановленні кримінальної відповідальності за діяння, визначені у ст. 361^4 ККУ, було б внесення змін до ст. 361^3 ККУ шляхом формулювання в окремих частинах зазначеної статті кваліфікованих складів несанкціонованих збуту або розповсюдження інформації з обмеженим доступом.

Список використаних джерел:

1. Закон України «Про внесення змін до Закону України «Про судоустрій і статус суддів» та процесуальних законів щодо додаткових заходів безпеки громадян» від 16 січня 2014 року № 721-VII // Голос України. – № 10 (5760). – від 21 січня 2014 року. – С. 14-22.

2. Закон України «Про інформацію» від 2 листопада 1992 року № 2657-XII // Закони України. – Т. 4. – К., 1996. – С. 72-88.

3. Закон України «Про державну таємницю» від 21 січня 1994 року № 3855-XII // Закони України. – Т. 7. – К., 1997. – С. 38-50.

4. Закон України «Про страхування» від 07 березня 1996 року № 85/96-ВР // [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.