УДК 343.974 : 343.346.8

Плугатир М. В., к.ю.н., ст. викладач кафедри адміністративного права і процесу НАВС

Кримінальна відповідальність за несанкціоноване втручання в роботу державних електронних інформаційних ресурсів та систем, критичних об'єктів національної інформаційної інфраструктури

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, ынформационная 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.

Актуальність. Після внесення 16 січня 2014 року Верховною Радою України змін до низки законодавчих актів, у Кримінальний кодекс України (далі – ККУ) включено ст. 361^3 «Несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури» [1]. Поява зазначеної норми потребує її дослідження з метою визначення ознак складу злочину, за який нею передбачається відповідальність. Адже тепер перед наукою кримінального права стоїть завдання щодо визначення об'єктивних та суб'єктивних ознак вказаного злочину, його кваліфікації та відмежування, шляхів удосконалення чинного законодавства та врахування позитивного попереднього досвіду у питанні протидії аналогічним посяганням тощо.

Аналіз останніх досліджень. Це обумовило активне дослідження норм, що містяться у Розділі XVI Особливої частини КК України, результати чого викладено в працях 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. 361^3 «Несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури» ККУ проводилось з урахуванням здобутків зазначених науковців, адже вони зробили вагомий внесок в наукову розробку злочинів у сфері комп'ютерної інформації. Разом з тим, останні зміни у чинному законодавстві України про кримінальну відповідальність,

а саме встановлення відповідальності за несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури, вимагає подальшого проведення роботи у визначеному напрямку.

Метою даної статті, яка обумовлена викладеним вище, є встановлення сутності та ознак складу злочину, передбаченого ст. 361^3 «Несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури» ККУ.

Виклад основного матеріалу. Пропонується у статті розглянути та визначити сутність ключових ознак складу злочину, за який передбачено відповідальність ст. 361^3 «Несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури» ККУ. Для цього необхідно розглянути наступні низку елементів складу злочину, що визначаються даною нормою.

Об'єкт злочину – право власності на комп'ютерну інформацію – сукупність права та можливості особи: володіти носієм інформації; використовувати інформацію, яка міститься на ньому, для задоволення своєї інформаційної потреби; дозволяти іншим особам використовувати інформацію, яка міститься на його носії, змінювати її, визначати долю носія.

Предметом злочину є: інформація – відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника і ціну. Аналіз об'єкта і форм об'єктивної сторони несанкціонованого втручання дає підстави стверджувати, що до предметів даного злочину відносяться також комп'ютерна інформація та інформація, що передається каналами зв'язку.

Об'єктивна сторона характеризується такою структурою: *діяння* – несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури; *суспільно небезпечні наслідки* – витік, втрата, підробка, блокування інформації, спотворення процесу обробки інформації, порушення встановленого порядку маршрутизації інформації (перелічені наслідки є альтернативними, тобто для наявності складу злочину достатньо настання хоча б одного з наслідків); *причинний зв'язок між діянням та наслідками.*

Втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури слід розуміти як зміну режиму роботи електронно-обчислювальної машини, системи, комп'ютерної мережі. *Фізична* ознака втручання виявляється в тому, що *воно полягає у впливі на матеріальний носій комп'ютерної інформації або засоби її автоматизованого опрацювання.* Суспільна небезпечність (*соціальна* ознака) несанкціонованого втручання визначається тим, що діяння ставить під загрозу функціонування державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури у

сфері зберігання, опрацювання, зміни, доповнення, передавання й одержання інформації, тобто заподіює шкоду суспільним відносинам права власності на комп'ютерну інформацію. *Протиправність* як обов'язкова ознака аналізованого діяння характеризується в законі за допомогою терміна "несанкціоноване". Відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року під несанкціонованими діями щодо інформації в системі розуміються дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

Викладене дозволяє дати таке визначення несанкціонованого втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури: *зміна режиму роботи державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури, вчинена шляхом впливу на носій комп'ютерної інформації або засоби її автоматизованого опрацювання, з порушенням встановленого відповідно до законодавства порядку доступу до інформації, що заподіює шкоду суспільним відносинам власності на комп'ютерну інформацію.*

До *критичних об'єктів* національної інформаційної інфраструктури законодавство відносить об'єкти, на яких наявна принаймні одна інформаційна (автоматизована), телекомунікаційна або інформаційно-телекомунікаційна система, порушення функціонування якої може призвести до:

- надзвичайної ситуації техногенного характеру або негативного впливу на стан екологічної безпеки держави;
- негативного впливу на стан енергетичної безпеки держави;
- негативного впливу на стан економічної безпеки держави, порушення сталого функціонування банківської або фінансової системи держави;
- порушення сталого функціонування транспортної інфраструктури держави;
- блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення та об'єктів підвищеної небезпеки;
- блокування роботи органів державної влади чи органів місцевого самоврядування;
- порушення сталого функціонування інформаційної або телекомунікаційної інфраструктури держави, у тому числі її взаємодії з відповідними інфраструктурами інших держав;
- блокування діяльності військових формувань інших суб'єктів сектору національної безпеки та оборони, органів військового управління, Збройних Сил України в цілому, систем керування зброєю;
- масових заворушень;
- розголошення державної таємниці.

До *наслідків* несанкціонованого втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури відносяться: 1) витік; 2) втрата; 3) підробка; 4) блокування комп'ютерної інформації; 5) спотворення процесу обробки комп'ютерної інформації; 6) порушення встановленого порядку маршрутизації комп'ютерної інформації.

Так, *витік* інформації, відповідно до статті 1 Закону України "Про захист

інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року, – це результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї [2]. Витік є порушенням такого повноваження власника комп'ютерної інформації, як право розпорядження.

Зміст наступного суспільно небезпечного наслідку – *"втрати комп'ютерної інформації"* раніше (до внесення змін 31 травня 2005 року) визначався Законом України "Про захист інформації в автоматизованих системах" як дія внаслідок якої інформація в АС перестає існувати для фізичних або юридичних осіб, що мають право власності на неї, в повному чи обмеженому обсязі [3]. Зараз це положення у чинній редакції закону відсутнє. Тому під *втратою комп'ютерної інформації пропонується розуміти такий вплив на носій комп'ютерної інформації, унаслідок якого вона перестає існувати у формі, яка дозволяє опрацьовувати її за допомогою комп'ютерної техніки.*

Суспільно-небезпечний наслідок – *підробка інформації* до 2005 року законодавством України визначалась як навмисні дії, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в автоматизованій системі [3]. Підробка комп'ютерної інформації, як видається, являє собою порушення такого повноваження власника як користування, адже через підробку власник повністю або частково втрачає можливість реалізовувати свою інформаційну потребу. Виходячи з цього можна так визначити підробку комп'ютерної інформації: *зміна без відома власника змісту відомостей, відображених на носії, що робить інформацію цілком або частково непридатною для задоволення інформаційної потреби особою, яка має право власності на таку інформацію.*

Блокування комп'ютерної інформації також є специфічною формою порушення повноваження користування інформацією. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року містить термін "блокування інформації в системі", який визначається таким чином: дії, унаслідок яких унеможливлюється доступ до інформації в системі. Отже, блокування являє собою ситуацію, коли комп'ютерна інформація не знищена, не підроблена, але можливість використовувати її відсутня. Можна сформулювати таке визначення: *блокування комп'ютерної інформації – відсутність у власника можливості використовувати інформацію для задоволення інформаційної потреби за умови, що її не втрачено та не підроблено.*

Спотворення процесу обробки комп'ютерної інформації. Обробка інформації в автоматизованій системі відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року являє собою виконання однієї або кількох операцій, зокрема збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів. З урахуванням вищезазначеного, *спотворення процесу обробки комп'ютерної інформації* можна визначити як *отримання в результаті операцій з комп'ютерною інформацією, які здійснювалися за допомогою технічних чи програмних засобів, результатів, що не відповідають характеристикам технічних засобів або алгоритму комп'ютерної програми.*

Порушення встановленого порядку маршрутизації комп'ютерної інформації

матиме місце, коли комп'ютерна інформація, що передається за допомогою комп'ютерної мережі конкретному абонентові (абонентам), ним не отримується або доступ до певних мережевих ресурсів здійснюється з порушенням встановленого порядку. На підставі положень Закону України "Про телекомунікації" від 18 листопада 2003 року № 1280-IV, можливо визначити, що маршрутизація полягає в забезпеченні передавання (отримання) інформації від одного адресата іншому [4].

Причинний зв'язок як обов'язкова ознака об'єктивної сторони несанкціонованого втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури полягає в тому, що діяння (несанкціоноване втручання) з необхідністю спричиняє настання наслідків: воно передує настанню зазначених суспільно небезпечних наслідків, містить у собі реальну можливість наслідків і в конкретному випадку є необхідною умовою, без якої б наслідки не настали.

Несанкціоноване втручання буде закінченим з моменту настання суспільно небезпечних наслідків.

Суб'єкт *несанкціонованого втручання* загальний, ним є фізична, осудна особа, що досягла 16-річного віку.

Суб'єктивна сторона несанкціонованого втручання виражається в тому, що особа: а) усвідомлювала суспільну небезпечність втручання, тобто фактичні та соціальні ознаки діяння, його несанкціонованість; б) передбачала наслідки у вигляді витоку, втрати, підробки, блокування інформації, спотворенні процесу обробки інформації або порушенні порядку її маршрутизації; в) бажала або свідомо припускала настання цих наслідків. Тобто суб'єктивна сторона аналізованого складу може виражатися у вигляді як прямого, так і непрямого умислу.

Усвідомлення фактичних ознак несанкціонованого втручання полягає в тому, що особа усвідомлює закономірності функціонування державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури, використання яких дозволяє здійснювати втручання в їх роботу. Усвідомлення несанкціонованості в цьому складі злочину зумовлене насамперед розумінням об'єкта, котрим, як зазначалося вище, виступає право власності на чужу комп'ютерну інформацію. Отже, суб'єкт злочину знає про відсутність у нього такого права, розуміє, що він порушує встановлений власником інформації порядок використання державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури.

Мотив, мета та емоційний стан на кваліфікацію несанкціонованого втручання не впливають.

Відмежування від ст. 361 ККУ полягає в об'єктивній стороні злочину (згідно ст. 361 ККУ втручання здійснюється у роботу ЕОМ, систем, комп'ютерних мереж або мереж електрозв'язку, а згідно ст. 361^3 ККУ – державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури) та санкціях (ч. 1 ст. 361 ККУ передбачає альтернативні санкції у виді штрафу, обмеження волі, а також позбавлення волі тільки до трьох років). У ч. 1 ст. 361^3 ККУ

санкція більш сувора.

Кваліфікуючими ознаками злочинів, передбачених статтею 361^3, 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.

Комп'ютерний злочин буде вважатися вчиненим ***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 (наприклад, декілька осіб здійснюють несанкціоноване втручання з окремих терміналів і знищують певну інформацію);
- злочин вчиняється двома або більше співвиконавцями, кожен із яких виконує частину дій, що характеризують об'єктивну сторону (наприклад, одна особа вчиняє несанкціоноване втручання й перекручує комп'ютерну інформацію про користувачів комп'ютерної мережі та паролі їх доступу, а інша знищує комп'ютерну інформацію);
- злочин вчиняється двома або більше особами, при цьому лише одна з них відіграє роль виконавця, а інші є підбурювачами, пособниками або організаторами (наприклад, одна особа забезпечує іншу необхідним устаткуванням, а остання вчиняє розповсюдження шкідливої комп'ютерної програми).

При цьому 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 і злочином, який вчинив виконавець.

Значною шкодою в статті 361^3 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 або інформаційних,

телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури для контролю над складними технологічними процесами, об'єктами та керування ними.

Висновки. В цілому ст. 361^3 ККУ побудована логічно, та не викликає зауважень до її змісту. Дещо бентежить примітка до статті, оскільки її текст представляє собою одне речення, яке займає пів сторінки тексту, адже така побудова примітки ускладнює її розуміння.

Слід окремо зауважити на тому, що ст. 361^3 «Несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури» за своїм змістом є майже тотожною до ст. 361 «Несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку». Ключовою відмінністю між ними є те, що злочинне діяння, передбачене у ст. 361^3 ККУ, створює загрозу функціонуванню державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури. А злочин, відповідальність за який встановлено у ст. 361 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 або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури. Більш доцільним, при встановленні кримінальної відповідальності за діяння визначені у ст. 361^3 ККУ, було б внесення змін до ст. 361 ККУ шляхом формулювання в окремих частинах зазначеної статті кваліфікованих складів несанкціонованого втручання, що посягають на комп'ютерну інформацію, що оброблюється в державних електронних інформаційних ресурсах або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах, критичних об'єктах національної інформаційної інфраструктури.

ЛІТЕРАТУРА:

1. Закону 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 захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 року № 2594-IV // Відомості Верховної Ради. – 2005. – № 26. – ст. 347.

3. Закон України «Про захист інформації в автоматизованих системах» від 5 липня 1994 року № 80/94-ВР // Відомості Верховної Ради. – 1994. – № 31. – ст. 286.

4. Закон України «Про телекомунікації» від 18 листопада 2003 року № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – ст. 155.