Соціально-правові студії. 2020. Випуск 3 (9). С. 26-33
Social & Legal Studios. 2020. Issue 3 (9). P. 26-33

UDC (УДК) 343 3/7

Пелещак Олег Романович,
здобувач освітнього ступеня доктора філософії у галузі права
кафедри кримінального процесу та криміналістики
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: pelsh79@ukr.net
ORCID ID: 0000-0002-2785-7464

ДЕЯКІ АСПЕКТИ КРИМІНАЛЬНО-ПРАВОВОЇ ХАРАКТЕРИСТИКИ КІБЕРДИВЕРСІЙ

Анотація. Йдеться про кібердиверсію в окремій статті Кримінального кодексу України (КК України) як таку новітню форму диверсії (стаття 113 КК України), яка була створена на основі статей 361, 361-1, 361-2, 362, 363, 363-1 КК України, що передбачають покарання за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж.

Ключові поняття: диверсія, кібердиверсія, безпосередній об'єкт злочину, предмет злочину, суб'єктивна сторона злочину, механізм учинення злочину, кваліфікація злочину.

Peleshchak Oleh,
Postgraduate Student of the Department
of Criminal Procedure and Criminalistics,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: pelsh79@ukr.net
ORCID ID: 0000-0002-2785-7464

SOME ASPECTS OF CRIMINAL AND LEGAL CHARACTERISTICS OF CYBER DIVERSION

Abstract. The article deals with cyber diversion issues as a separate article of the Criminal Code of Ukraine as a new form of diversion (article 113 of the Criminal Code), which was created on the basis of articles 361, 361-1, 361-2, 363, 363-1 of Criminal Code, providing punishment for crimes in the sphere of using computers, systems and computer networks.

The author considers that the way, that allows assuming higher social safety in such crimes is their qualification according to the rules of a set of articles from other chapters of CC of Ukraine. In this particular case the link of art.113 CC of UA "Diversion" with art. 361, 361-1, 361-2, 362, 363, 363-1 of CC of UA that provide punishment for crimes in the sphere of computer applying, systems, and computer networks is substantiated.

Unlawful interference in analog-to-digital computers applying, their systems or computer networks, distorted computer information, destruction of computer information, the spread of the virus, software are suggested to define as determination of the latest forms of diversion that is the ways of committing cyber diversion.

The article points out that in the process of norms of criminal liability of crimes committing on the objects of critical informational infrastructure or objects that are essential for state viability there is the necessity of considering the mechanism of committing such infringements. In the case of committing cyber diversity with the aim of the destruction of information or focused attack of a particular control unit, the mentioned mechanism is characterized by applying particular computer information (tool-virus) for influencing other computer information (subject – critical informational structure). The absence of at least one of the elements of the mechanism must be testified as a lack of characteristics of such forms of crime as a cyber diversion.

Key concepts: diversion, cyber diversion, the direct object of the crime, the subject of the crime, subjective side of the crime, mechanism of the crime, qualification of the crime.

DOI 10.32518/2617-4162-2020-3-26-33

Вступ

Удосконалення кримінального законодавства щодо відповідальності за злочини проти основ національної безпеки передбачає: визначеність об'єкта кримінально-правової охорони; класифікацію злочинів проти основ національної безпеки України; визначення техніко-юридичних і змістовних компонентів окремих складів злочинів; кваліфікацію цих діянь; наповнення відповідного розділу КК України з позицій виявлення прогалин правового регулювання, колізій правових норм.

У теорії кримінального процесуального, кримінального права і правозастосовної діяльності важливо з'ясувати зміст понять *родового об'єкта* і *системи злочинів* проти основ національної безпеки України та *форм прояву* об'єктивної сторони складу цих злочинів, зокрема такого, як ***кібердиверсія,*** в контексті визначеного суспільно небезпечного діяння – ***диверсія*** – у ст. 113 та їх взаємозв'язку зі ст.ст. 361–363-1 КК України.

Кібердиверсії в поточних операціях із контролю над ресурсами, що здійснюються з метою встановлення контролю і перехоплення управління або виведення з ладу промислового обладнання, автоматизованих систем управління, об'єктів військової інфраструктури, – найбільш ефективний інструмент технології ураження систем життєзабезпечення і критичної інформаційної інфраструктури.

Які обставини зумовлюють необхідність виокремлення «комп'ютерних» злочинів у самостійну групу? Чому є недоцільним розширення меж традиційних складів злочинів, аби вони охоплювали й аналізовані діяння? Чи відповідає чинний КК України в частині встановлення відповідальності за сучасні форми диверсійної діяльності у кіберпросторі? Чи охоплюються поняттям «диверсія» кримінально карні діяння – кібердиверсії – відповідно до змісту цього злочину?

Форми сучасних диверсій мало досліджені у сфері кримінального права України, наслідком чого виявляється практична складність доведення факту диверсійної діяльності, яка охоплюється диспозицією ст. 113 КК України, та розслідування скоєних диверсійних діянь за іншими статтями чинного КК України.

Диверсія та основні форми її здійснення стали об'єктом наукових досліджень таких науковців, як О. О. Климчук [7], О. Д. Довгань [5], В. С. Картавцев [6], О. О. Черноног [15], О. А. Чуваков [16]. Слід зазначити, що дослідження диверсійної діяльності з позицій кримінально-правової науки переважно зосереджені на загальній характеристиці елементів складу цього злочину й лише деякі серед них (О. А. Чуваков) аналізують об'єктивну сторону злочину, передбаченого ст. 113 КК України. Окремі питання притягнення до кримінальної відповідальності за диверсії проти здоров'я громадян досліджені у дисертації Є. В. Фесенка [12]. Частково відповідальність за диверсійну діяльність досліджено у наукових працях В. С. Картавцева, О. Ф. Бантишева й О. В. Шамари [3], Ю. А. Луценка [8]. Проблеми притягнення до кримінальної відповідальності за диверсійну діяльність розглянуто у роботі О. Климчука, у якій проведено юридичний аналіз складу злочину, передбаченого ст. 113 КК України, досліджено особливості притягнення та звільнення від кримінальної відповідальності за диверсійну діяльність, розмежовано поняття об'єктів, що мають важливе народногосподарське й оборонне значення. Під предметом складу цього злочину вчений розуміє об'єкти матеріального світу (зокрема інформацію), незалежно від форми власності, що мають важливе народногосподарське чи оборонне значення, шляхом знищення яких винний намагається спричинити шкоду економічній або воєнній безпеці держави. Однак, зважаючи на кардинальну зміну політичної та економічної ситуацій в країні, чинної нормативно-правової бази в сфері захисту національної безпеки, це дослідження певною мірою не відповідає реаліям сьогодення у кваліфікації таких злочинних дій, як диверсія, та її новітніх форм.

Мета статті – з'ясування сутності кібердиверсій та обґрунтування взаємозв'язку ст. 113 КК України *(диверсія)* зі ст.ст. 361, 361-1, 361-2, 362, 363, 363-1 КК України, які передбачають покарання за *злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж,* що забезпечить повне визначення об'єкта, предмета, об'єктивної сторони злочину «кібердиверсія» та кваліфікацію його ознак.

1. Особливості кваліфікації злочинів проти основ національної безпеки України

Загалом під родовим об'єктом злочинів проти основ національної безпеки розуміють *суспільні відносини*, що забезпечують стабільність у функціонуванні державної влади, її окремих інститутів і органів. У системі Особливої частини КК України розділ щодо злочинів проти основ національної безпеки містить ст.ст. 109–114-1.

М. І. Хавронюк *родовим об'єктом* злочинів проти основ національної безпеки визначає національну безпеку України в різних її *сферах* [14, с. 25]. Його класифікація злочинів у цій сфері і є наслідком такого визначення [13, с. 243–271]:

– проти основ національної безпеки у *політичній* сфері: дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або захоплення державної влади (ст. 109 КК); посягання на територіальну цілісність і недоторканність України (ст. 110 КК); посягання на життя державного чи громадського діяча (ст. 112 КК);

– проти основ національної безпеки в *інформаційній, економічній, науково-технологічній і воєнній* сферах: державна зрада (ст. 111 КК); шпигунство (ст. 114 КК);

– проти основ національної безпеки в *економічній і воєнній* сферах (ст. 114 КК).

На думку В. К. Матвійчука [9], залежно від сфер суспільних відносин із основ національної безпеки України всі злочини, що входять до цього розділу, необхідно класифікувати так:

– злочини, котрі посягають на відносини, що забезпечують охорону основ національної безпеки у *політичній* сфері: дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або захоплення державної влади (ст. 109 КК); посягання на територіальну цілісність і недоторканість України (ст. 110 КК); посягання на життя державного чи громадського діяча (ст. 112 КК);

– злочини, що посягають на відносини, котрі забезпечують охорону основ національної безпеки України у сфері *державного суверенітету, територіальної цілісності та недоторканості, обороноздатності, державної, економічної, науково-технічної та інформаційної* безпеки України: державна зрада (ст. 111 КК); шпигунство (ст. 114 КК);

– злочини, які посягають на відносини, що забезпечують охорону основ національної безпеки в *економічній, екологічній сферах і сфері обороноздатност*і: диверсія (ст. 113 КК).

Отже, єдиною *підставою для класифікації злочинів* проти основ національної безпеки є суспільні відносини, що охороняються кримінальним законодавством. Під *злочинами проти основ національної безпеки* України необхідно розуміти передбачені КК України вчинені з прямим умислом і спеціальною метою суспільно небезпечні такі діяння (злочини): дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або захоплення державної влади (ст. 109 КК); посягання на територіальну цілісність і недоторканість України (ст. 110 КК); фінансування дій, вчинених з метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади, зміни меж території або державного кордону України (ст. 110-2 КК); державна зрада (ст. 111 КК); посягання на життя державного чи громадського діяча (ст. 112 КК); диверсія (ст. 113 КК) шпигунство (ст. 114 КК); перешкоджання законній діяльності Збройних Сил України та інших військових формувань (ст. 114-1).

Суб'єктами злочинів проти основ національної безпеки України можуть бути фізичні осудні особи, які до моменту вчинення злочину досягли 16-річного віку (суб'єктами злочинів, як передбачено ст.ст. 112 і 113 КК України, можуть бути особи, які до моменту вчинення злочину досягли 14-річного віку).

Зовнішня сторона злочинів має істотні дискусійні моменти, які впливають на застосування норм і законотворчу діяльність. Слід зазначити про відсутність єдності поглядів у юридичній літературі й щодо поняття об'єктивної сторони складу злочину, її складових і змісту. Вивчення об'єктивної сторони складу злочину у сучасних умовах зумовлене тим, що в цій сфері замість традиційних уявлень з'явилося багато нових підходів до удосконалення судової та слідчої практики. У з'ясуванні *об'єктивної сторони складу злочину*, її складових та змісту доцільно проаналізувати дослідження В. К. Матвійчука [10]. Його аналіз точок зору щодо *форм прояву* об'єктивної сторони складу злочину засвідчує, що всі автори визначають діяння (дію або бездіяльність), злочинний результат (наслідки, злочинний результат), причинний зв'язок, спосіб, час і місце вчинення злочину як ознаки об'єктивної сторони складу злочину. У науці кримінального права ці ознаки традиційно розділяють на обов'язкові та факультативні. Єдиної точки зору щодо обсягу перших, а також їх назви немає. Деякі вчені зараховують до них діяння, його наслідки і причинний зв'язок. Інші ж – лише діяння, бо наслідки і причинний зв'язок властиві тільки злочинам із матеріальним складом. Іще інші зараховують причинний зв'язок до факультативних ознак об'єктивної сторони складу злочину [10].

На підставі аналізу автор робить висновок, що об'єктивну сторону складу злочину становлять такі ознаки: діяння (дія або бездіяльність); наслідки; причинний зв'язок; спосіб учинення злочину; місце і час учинення злочину; обстановка вчинення злочину; засоби вчинення злочину; знаряддя злочину; джерела вчинення злочину.

2. Пропозиції щодо удосконалення норм про кримінальну відповідальність за злочини, які здійснюються на об'єктах критичної інформаційної інфраструктури

У процесі вдосконалення кримінального законодавства необхідно враховувати положення Конвенції про кіберзлочинність від 23 листопада 2001 р. Відповідно до цієї Конвенції, держава-учасник (зокрема Україна) має криміналізувати декілька груп посягань: 1) злочини проти конфіденційності,

цілісності і доступності комп'ютерної інформації та комп'ютерних систем (незаконний доступ до комп'ютерної системи; незаконне перехоплення закритої інформації; незаконний вплив на комп'ютерну інформацію; втручання в роботу комп'ютерної системи; зловживання пристроями та паролями); 2) злочини, що пов'язані з комп'ютерами (підроблення, пов'язане з комп'ютерами; шахрайство, пов'язане з комп'ютерами); 3) злочини, пов'язані зі змістом комп'ютерної інформації (володіння, придбання, пропонування, виготовлення з метою розповсюдження або розповсюдження дитячої порнографії в межах комп'ютерних систем); 4) злочини, пов'язані з порушенням авторських і суміжних прав.

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації – диспозиція ст. 360 КК України, на підставі якої визначено [10, с. 25–31]: *основний безпосередній об'єкт* цього злочину − суспільні відносини у сфері комп'ютерної інформації та у сфері електрозв'язку. *Додатковим безпосереднім об'єктом* злочину є суспільні відносини власності щодо певної інформації. *Факультативний безпосередній об'єкт* − відносини у сфері забезпечення режиму обмеженого доступу до певної інформації. Зазначеним відносинам може заподіюватися шкода в разі витоку інформації.

Предметом злочину є інформація, форма представлення або фіксація якої у законі не конкретизована. Очевидно, що насамперед йдеться про *комп'ютерну інформацію* та *інформацію, що передається мережами електрозв'язку* («Загальні положення до розділу XVI Особливої частини Кримінального кодексу України»).

З об'єктивної сторони злочин характеризується:

− дією у вигляді несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

− наслідками, що можуть проявлятися у формі витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації;

− причинним зв'язком між зазначеними діями та наслідками.

Суб'єкт злочину – загальний. *Суб'єктивна сторона* характеризується виною у формі тільки прямого умислу. У кримінальному законі відсутня пряма вказівка на те, з якою формою вини може бути вчинене несанкціоноване втручання у роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Проте зміст поняття «втручання» обумовлює висновок: цей злочин необхідно вважати умисним.

Кваліфікуючими ознаками злочину є заподіяння ним *значної шкоди,* вчинення його *повторно* чи *за попередньою змовою групою осіб* («Загальні положення до розділу XVI Особливої частини Кримінального кодексу України»).

Слід зазначити, що несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку може використовуватися як спосіб вчинення інших злочинів, ознаки яких визначені у ст.ст. 111, 113, 114, 163, 182, 231, 256, 330 КК України. У таких випадках скоєне потрібно кваліфікувати за сукупністю злочинів, передбачених однією чи декількома з цих статей та ст. 361 КК України. У разі, коли зазначені дії призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації, порушення встановленого порядку її маршрутизації, вчинене потрібно кваліфікувати за сукупністю злочинів, передбачених ст. 361 та ст. 190 або ст. 200 КК України. Окремі суспільно небезпечні діяння, передбачені ч. 3 ст. 190 та ст. 200, а також їх співвідношення із посяганнями, виписані у ст.ст. 361–363-1 КК України.

Вивчення матеріалів слідчої та судової практики підтверджує, що є багато труднощів у застосуванні норм про кримінальну відповідальність за «комп'ютерні» злочини. Удосконалення вітчизняного кримінального законодавства про відповідальність за аналізовані злочини повинне здійснюватися з урахуванням досвіду, накопиченого в інших країнах. Крім того, міжнародний характер цих посягань зумовлює необхідність уніфікації відповідних кримінально-правових норм.

Серед трьох способів установлення кримінальної відповідальності за «комп'ютерні» злочини (створення нових кримінально-правових норм, які спеціально передбачають відповідальність за ці посягання; розширення меж складів «некомп'ютерних», більш традиційних злочинів; *за окремі посягання відповідальність встановлена спеціально створеними нормами, а частина злочинів охоплюється складами, що існували раніше*) українське законодавство, на думку А. Музики, повинне використати останній, змішаний спосіб. Нові норми потрібно створювати лише в тому випадку, коли певне суспільно небезпечне діяння не може охоплюватися вже існуючим складом, або розширення меж таких складів призведе до порушення внутрішньої структури відповідної кримінально-правової норми [10, с. 85–86]. «Криміналізація суспільно небезпечних діянь і внесення змін до будь-яких чин-

них кримінально-правових норм має здійснюватися з використанням системного підходу. В процесі удосконалення норм про кримінальну відповідальність за «комп'ютерні» злочини така системність може бути досягнута лише за умови врахування **механізму вчинення цих посягань**. Зазначений механізм характеризується використанням однієї комп'ютерної інформації (знаряддя) для здійснення впливу на іншу комп'ютерну інформацію (предмет). Відсутність хоча б одного з елементів цього механізму має свідчити про відсутність ознак «комп'ютерного» злочину. Посягання, лише предметом яких або лише знаряддям вчинення яких є комп'ютерна інформація, не мають якихось суттєвих особливостей, що зумовлювали б необхідність установлення кримінальної відповідальності за їх вчинення в окремих нормах» [11, с. 87].

Окрім механізму вчинення аналізованих посягань у створенні доктринальної моделі системи норм про відповідальність за їх учинення необхідно:

– зважити на відповідний родовий об'єкт – суспільні відносини у сфері здійснення їх суб'єктами правомірної інформаційної діяльності щодо комп'ютерної інформації;

– визначити аналізовані злочини як умисні суспільно небезпечні діяння, що посягають на відносини у сфері здійснення інформаційної діяльності стосовно комп'ютерної інформації, предметом і знаряддям вчинення яких є така інформація;

– врахувати вимоги до спеціалізованої термінології, яка вживатиметься у цих формулюваннях.

На цих підставах запропоновано логічну послідовність суспільно небезпечних діянь: 1) незаконний вплив на процес обробки комп'ютерної інформації; 2) комп'ютерний саботаж; 3) незаконні зміна, пошкодження чи знищення комп'ютерної інформації; 4) незаконний доступ до комп'ютерної інформації; 5) незаконне заволодіння комп'ютерною інформацією; 6) незаконні дії із шкідливими комп'ютерними програмами; 7) незаконне розповсюдження даних, які призначені для отримання доступу до комп'ютерної інформації.

У формулюванні складу суспільно небезпечного діяння слід урахувати мету, з якою діє суб'єкт, визначити відповідну кваліфікуючу обставину. Втім, недоцільно у зв'язку з цим створювати окрему статтю, якщо ознаки об'єктивної сторони вчиненого не змінюються.

Згідно з Коментарем до ст. 113 КК України [2], *основний безпосередній об'єкт диверсії* – безпека держави в економічній, екологічній, воєнній або будь-якій іншій сфері відповідно до спрямованості конкретного акту диверсії.

Предметом диверсії можуть бути об'єкти, від діяльності яких залежить життєдіяльність певних регіонів чи інших великих територій, належне функціонування певних галузей економіки, структур державного управління (електростанції, водо-, нафто-, газо-, нафтопродуктопроводи, мости, дамби, греблі, системи інформаційних комунікацій, вокзали, аеропорти, морські чи річкові порти, метрополітени, підприємства по виробництву грошових знаків України чи інші важливі підприємства, незалежно від форми власності, військові частини тощо).

Об'єктивна сторона диверсії проявляється в семи формах, кожна із яких передбачає вчинення суспільно небезпечних дій: 1) масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їх здоров'ю; 2) зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення; 3) радіоактивне забруднення; 4) масове отруєння; 5) поширення епідемій; 6) поширення епізоотій; 7) поширення епіфітотій.

До *дій,* спрямованих на масове знищення людей, на зруйнування або пошкодження об'єктів, належить також внесення вірусів у комп'ютерні системи з метою утруднення їхньої роботи або знищення накопиченої на магнітних носіях важливої інформації тощо.

Суб'єктивна сторона диверсії характеризується виною у виді прямого умислу і спеціальною метою. Характерною ознакою диверсії є те, що вчинення зазначених дій не є самоціллю, а використовується винним як засіб досягнення його головної мети – ослаблення держави. Склад злочину побудований як формальний, а тому на перший план виступає не фактичний результат (ослаблення держави чи принаймні реальна загроза такого ослаблення), а саме вороже ставлення особи до держави.

Кібердиверсії (а також хактивізм і кібершпигунство) – це злочини, що входять до групи геополітичних. Найнебезпечнішим є потенціал кібердиверсій, які здійснюються на об'єктах *критичної інформаційної інфраструктури* або об'єктах, важливих для життєдіяльності держави. Небезпеку становлять *віруси*, призначенням яких є не збирання інформації, а її знищення або цілеспрямоване атакування певних вузлів управління, що може не тільки зупинити їх роботу, а й призвести до людських жертв.

Визначення категорій, що подаються в науково-практичному Коментарі КК України до ст. 361 [2], а саме: *незаконне втручання в роботу АЕОМ, їх систем чи комп'ютерних мереж, комп'ютерна інформація, носії комп'ютерної інформації, перекручення комп'ютерної інформації, знищення комп'ютерної інформа-*

ції, розповсюдження комп'ютерного вірусу, програмні засоби, на нашу думку, слід тлумачити як дефініції новітніх форм диверсії, тобто як способів учинення кібердиверсії.

Об'єктом цього злочину є методи обробки інформації, робота та порядок використання комп'ютерів та комп'ютерних мереж, які набули інтернаціонального характеру. Предметом злочину є: автоматизовані електронно-обчислювальні машини (комп'ютери, АЕОМ), зокрема персональні; їх системи; комп'ютерні мережі. Об'єктивна сторона злочину проявляється у формі: 1) незаконного втручання у роботу АЕОМ, їх систем чи комп'ютерних мереж, що призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації; 2) розповсюдження комп'ютерного вірусу.

Суб'єкт злочину загальний. Суб'єктивна сторона злочину характеризується умисною виною. Злочинні дії можуть бути вчинені лише з прямим умислом, тоді як ставлення винного до наслідків злочину може характеризуватись як прямим, так і непрямим умислом. Кваліфікуючими ознаками (ч. 2 ст. 361) злочину є вчинення його: 1) повторно; 2) за попередньою змовою групою осіб; 3) заподіяння ним істотної шкоди.

Частиною 1 ст. 361 охоплюються як випадки проникнення (впливу) у працюючу АЕОМ, систему чи мережу (як-от проникнення до системи одного працюючого персонального комп'ютера з іншого персонального комп'ютера), так і несанкціоноване увімкнення непрацюючої машини і проникнення до її системи (вплив на її роботу), якщо воно здійснюється за допомогою зазначених у цій статті знарядь. Закон передбачає обов'язкову властивість застосовуваних для вчинення цього злочину програмних і технічних засобів: їх здатність спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації. Злочин у першій його формі вважається закінченим з моменту настання хоча б одного із зазначених наслідків.

У статті 363 КК України розкрито зміст порушення правил експлуатації автоматизованих електронно-обчислювальних систем [1; 2].

Об'єктом злочину є встановлений порядок експлуатації АЕОМ, їх систем чи комп'ютерних мереж. Об'єктивна сторона злочину полягає у порушенні правил експлуатації АЕОМ, їх систем чи комп'ютерних мереж. Порушення правил вважається злочинним у разі, коли його наслідком було: 1) викрадення; 2) перекручення чи знищення комп'ютерної інформації, засобів її захисту; 3) незаконне копіювання комп'ютерної інформації; 4) істотне порушення роботи АЕОМ, їх систем чи комп'ютерних мереж. Під істотним порушенням роботи АЕОМ, їх систем чи комп'ютерних мереж слід розуміти, зокрема, вихід з ладу на тривалий час інформаційної системи, що обслуговує значну кількість машин, припинення на тривалий час роботи комп'ютерної мережі, втрату інформації, що має важливе значення, блокування на тривалий час доступу до такої інформації тощо.

Суб'єкт злочину спеціальний. Це особа, яка відповідає за експлуатацію АЕОМ, їх систем чи комп'ютерних мереж. Суб'єктивна сторона злочину визначається його наслідками і характеризується необережною формою вини. Кваліфікуючою ознакою цього злочину (ч. 2 ст. 363 КК України) є заподіяння істотної шкоди, яка може бути як безпосереднім результатом діяння винного, так і наслідком протиправних дій інших осіб.

Висновки

Характер суспільної небезпеки комп'ютерних злочинів обумовлюється специфікою їхнього об'єкта – суспільних відносин у сфері комп'ютерної інформації, які містять сегменти інших галузей життєдіяльності. Проблеми кваліфікації цих злочинів пов'язані із порушенням у їх вчиненні не тільки щодо свого безпосереднього об'єкта, а й інших об'єктів кримінально-правової охорони. Способом, що дозволить урахувати підвищену суспільну небезпеку таких злочинів, є їх кваліфікація за правилами сукупності зі статтями інших розділів КК України. У цьому випадку обґрунтовано взаємозв'язок ст. 113 КК України «Диверсія» зі ст.ст. 361, 361-1, 361-2, 362, 363, 363-1 КК України, які передбачають покарання за злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж.

Категорії, зміст яких визначено в Коментарі ККУ до ст. 361 [2], а саме: незаконне втручання в роботу АЕОМ, їх систем чи комп'ютерних мереж, комп'ютерна інформація, носії комп'ютерної інформації, перекручення комп'ютерної інформації, знищення комп'ютерної інформації, розповсюдження комп'ютерного вірусу, програмні засоби, слід тлумачити як дефініції новітніх форм диверсії, тобто як способів учинення кібердиверсії.

У процесі удосконалення норм про кримінальну відповідальність за злочини, які здійснюються на об'єктах *критичної інформаційної інфраструктури* або об'єктах, важливих для життєдіяльності держави, необхідно врахувати механізм учинення цих посягань. У випадку вчинення кібердиверсії з метою знищення інформації або цілеспрямованого атакування певних вузлів управління зазначений механізм характеризується використанням

однієї комп'ютерної інформації (знаряддя – *вірус*) для здійснення впливу на іншу комп'ютерну інформацію (предмет – *критична інформаційна структура*). Відсутність хоча б одного з елементів цього механізму має свідчити про відсутність ознак такої форми злочину, як кібердиверсія.

Список використаних джерел

1. Кримінальний кодекс України від 05.04.2001 № 2341-III (зі змінами і доповненнями в редакції станом на 01.05.2016р.). URL: http://zakon5.rada.gov.ua/laws/show/2341-14 (дата звернення 07.07.2020).
2. Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. 9-те вид., перероб. та допов. Київ : Юридична думка, 2012. 1316 с.
3. Бантишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації) : монографія. 2-ге вид., перероб. та допов. Київ : Наук.-вид. відділ НА СБ України, 2010. 168 с.
4. Відповідь СБУ на депутатський запит Сюмар В. І. URL: http://nacburo.org/wp-content/uploads/2015/04/SBU-separ1.jpg (дата звернення: 07.07.2020).
5. Довгань О. Д., Хлань В. Г. Кібертероризм як загроза інформаційному суверенітету держави. *Інформаційна безпека людини, суспільства, держави.* 2011. № 3 (7). С. 49–53.
6. Картавцев В. С. Кримінальна відповідальність за злочини проти основ національної безпеки України (наукові засади кваліфікації) : навч. посібник. Київ : Вид-во Національної академії СБ України, 2004. 57 с.
7. Климчук О. О. Кримінальна відповідальність за диверсію по законодавству України : дис ... канд. юрид. наук : 12.00.08. НА СБ України. Київ, 2003. 269 с.
8. Луценко Ю. В. Звільнення від кримінальної відповідальності за злочини проти основ національної безпеки України : монографія. Харків : Право, 2015. 200 с.
9. Матвійчук В. К. Злочини проти основ національної безпеки: поняття та загальна характеристика. *Кримінальне право. Юридична наука*. 2013. № 9. С. 80–87.
10. Матвійчук В. К. Об'єктивна сторона злочину: її складові та зміст. *Держава та регіони. Серія: Право*. 2013. № 1 (39). С. 163–168.
11. Музика А. А., Азаров Д. С. Законодавство України про кримінальну відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення. Київ : Вид. Паливода А. В., 2005. 120 с.
12. Фесенко Є. В. Злочини проти здоров'я населення та системи заходів з його охорони : монографія. Київ : Атіка, 2004. 280 с.
13. Хавронюк М. І. Злочини проти основ національної безпеки. Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001 р. / за ред. М. І. Мельника, М. І. Хавронюка. Київ : Каннон, 2001. С. 243–271.
14. Хавронюк М. І. Злочини проти основ національної безпеки України. Кримінальне право України. Особлива частина : підручник / Ю. В. Александров, О. О. Дудоров, В. А. Клименко та ін. / за ред. М. І. Мельника, В. А. Клименка. Київ : Юридична думка, 2004. С. 25–36.
15. Черноног О. О. Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління. *Междисциплинарные исследования в науке и образовании*. 2015. URL: mino.esrae.ru/178-1484 (дата звернення: 07.07.2020).
16. Чуваков О. А. Деякі види диверсійних актів у сучасних умовах. *Актуальні проблеми держави і права*. Одеса : Юрид. літ., 2010. Вип. 55. С. 222.
17. SCADA OS: первая в мире защищённая операционная система. URL: http://www.xakep.ru/post/59488/12 mino.esrae.ru/178-1484 (дата звернення: 07.07.2020).

References

1. Kryminalnyy kodeks Ukrainy vid 05.04.2001 № 2341-III (zi zminamy i dopovnennyamy v redaktsiyi stanom na 01.05.2016 r.) [Criminal Code of Ukraine]. Retrieved from http://zakon5.rada.gov.ua/laws/show/2341-14 [in Ukr.].
2. Naukovo-praktychnyy komentar Kryminalnoho kodeksu Ukrainy [Scientific and practical commentary of Criminal Code of Ukraine]. Za red. M. I. Melnyka, M. I. Khavroniuka. 9-te vyd., pererob. ta dopov. K.: Yurydychna dumka [in Ukr.].
3. Bantyshev, O. F., & Shamara, O. V. (2010). Kryminalna vidpovidalnist za zlochyny proty osnov natsionalnoi bezpeky Ukrainy (problemy kvalifikatsiyi) [Criminal liability for crimes against foundations of national safety of Ukraine (problems of qualification)]. K.: Nauk.-vyd. viddil NA SB Ukrainy [in Ukr.].

4. Vidpovid SBU na deputatskyi zapyt Syumar V. I. [Reply of SSU on deputy record Syumar V. I.]. Retrieved from http://nacburo.org/wp-content/uploads/2015/04/SBU-separ1.jpg [in Ukr.].
5. Dovhan, O. D., & Khlan, V. H. (2011). Kiberteroryzm yak zahroza informatsiinomu suverenitetu derzhavy [Cyber terrorism as a threat of informational sovereignty of a state]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy (Informational safety of an individual, society, a state),* 3 (7), 49–53 [in Ukr.].
6. Kartavtsev, B. C. (2004). Kryminalna vidpovidalnist za zlochyny proty osnov natsionalnoyi bezpeky Ukrainy (naukovi zasady kvalifikatsiyi) [Criminal liability for crimes against basics of national safety of Ukraine (scientific principles of qualification)]. K.: Vyd-vo Natsionalnoyi akademiyi SB Ukrainy [in Ukr.].
7. Klymchuk, O. O. (2003). Kryminalna vidpovidalnist za dyversiyu po zakonodavstvu Ukrainy [Criminal liability for diversion according to the legislature of Ukraine]. K. [in Ukr.].
8. Lutsenko, Yu. V. (2015). Zvilnennia vid kryminalnoyi vidpovidalnosti za zlochyny proty osnov natsionalnoyi bezpeky Ukrainy [Release from criminal liability for crimes against basics of national safety of Ukraine]. Kh.: Pravo [in Ukr.].
9. Matviychuk, V. K. (2013). Zlochyny proty osnov natsionalnoyi bezpeky: poniattia ta zahalna kharakterystyka [Crimes against basics of national safety: notion and general characteristics]. *Kryminalne pravo. Yurydychna nauka (Criminal law. Judicial science),* 9, 80–87 [in Ukr.].
10. Matviychuk, V. K. (2013). Obyektyvna storona zlochynu: yiyi skladovi ta zmist [Objective part of a crime: its components and content]. *Derzhava ta rehiony. Seriia: Pravo (State and regions. Issue: Law),* 1 (39), 163–168 [in Ukr.].
11. Muzyka, A. A., & Azarov, D. S. (2005). Zakonodavstvo Ukrainy pro kryminalnu vidpovidalnist za «kompyuterni» zlochyny: naukovo-praktychnyi komentar i shlyakhy vdoskonalennia [Legislature of Ukraine concerning criminal liability for "computer" crimes: scientific and practical commentary and its ways of improvement]. K.: Vyd. Palyvoda A. V. [in Ukr.].
12. Fesenko, Ye. V. (2004). Zlochyny proty zdorovia naselennia ta systemy zakhodiv z yoho okhorony [Crimes against population health and system of measures of its safety]. K.: Atika [in Ukr.].
13. Khavroniuk, M. I. (2001). Zlochyny proty osnov natsionalnoyi bezpeky. Naukovo-praktychnyi komentar Kryminalnoho kodeksu Ukrainy vid 5 kvitnia 2001 r. [Crimes against basics of national safety. Scientific and practical commentary of Criminal Code of Ukraine]. K.: Kannon [in Ukr.].
14. Khavroniuk, M. I. (2004). Zlochyny proty osnov natsionalnoi bezpeky Ukrainy. Kryminalne pravo Ukrainy. Osoblyva chastyna [Crimes against basics of national safety of Ukraine. Criminal Law of Ukraine. Special Part]. K.: Yurydychna dumka [in Ukr.].
15. Chernonoh, O. O. (2015). Napriamy pidvyshchennia efektyvnosti zabezpechennia kiberbezpeky informatsiinykh tekhnolohii v systemi publichnoho upravlinnia [Directions of increase efficiency of the providing cyber safety of informational technologies in the system of public administration]. *Mezhdystsyplynarnye yssledovanyia v nauke y obrazovanyy (Multidisciplinary research in science and education)*. Retrieved from mino.esrae.ru/178-1484 [in Ukr.].
16. Chuvakov, O. A. (2010). Deyaki vydy dyversiinykh aktiv u suchasnykh umovakh [Some types of subversive acts in current conditions]. *Aktualni problemy derzhavy i prava (Actual problems of a state and law).* O.: Yuryd. Lit., 55, 222 [in Ukr.].
17. SCADA OS: pervaya v mire zashchyshchyonnaia operatsyonnaia systema [SCADA OS: one of the first secure operating system in the world]. Retrieved from http://www.xakep.ru/post/59488/ 12 mino.esrae.ru/178-1484 [in Russ.].

Стаття: надійшла до редакції 03.08.2020
прийнята до друку 23.09.2020

The article: is received 03.08.2020
is accepted 23.09.2020