DOI: 10.18372/2307-9061.70.18502
УДК 343.9(045)

Д. Ю. Дрижакова,
здобувач вищої освіти третього (освітньо-наукового) рівня

ВИЗНАЧЕННЯ ОБ'ЄКТІВ ТА ПРЕДМЕТІВ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ), ЕЛЕКТРОННИХ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ, ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ (ст. 361, 361-1 КК УКРАЇНИ)

Київський національний університет імені Тараса Шевченка
вул. Володимирська, 64, 01601, Київ, Україна
E-mail: d.dryzhakova@gmail.com

Метою *статті є дослідження правового статусу безпосередніх об'єктів та предметів несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.* ***Методи дослідження:*** *у роботі використані діалектичний метод пізнання, загальнонаукові та спеціальні методи дослідження. Зокрема, структурно-функціональний, дедуктивний методи та метод наукового прогнозування.* ***Результати:*** *питання, висвітлені в статті, дозволяють дослідити проблематику, пов'язану зі стрімким розвитком технологій та збільшення кількості втручань в роботу інформаційних (автоматизованих), електронних, інформаційно-комунікаційних систем та електронних комунікаційних мереж, що приводить до необхідності удосконалення законодавства.* ***Обговорення:*** *у науковій статті надається кримінально-правова характеристика об'єкта та предмета несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.*

Ключові слова: *нормативно-правове регулювання; закон; інформаційно-телекомунікаційна система; кібертероризм; кіберзагроза; телекомунікаційна експертиза; комп'ютерно-технічна експертиза.*

Постановка проблеми та її актуальність. Із початком війни кібератаки активізуються у зв'язку зі зміною геополітичної ситуації, зростанням напруги між країнами та групами, а також через залучення різноманітних кіберзлочинців та хакерських груп. Кібератаки можуть використовуватись для підтримки військових операцій на землі, в повітрі або на морі, зокрема для руйнування комунікаційних мереж, завдання шкоди важливим об'єктам інфраструктури та іншими способами. Війна може призвести до збільшення заходів контролю за інформацією та спроби зламу інформаційних систем супротивників для отримання важливої інформації. У цій ситуації важливо приділяти увагу захисту критично важливих інформаційних і комунікаційних систем, зміцненню кібербезпеки та підвищенню обізнаності про кібернебезпеку.

Розпочата російською федерацією війна проти України триває не тільки у реальному просторі, але й у віртуальному – кіберпросторі. З початку 2022 р. Служба безпеки України нейтралізувала понад 4,5 тис. кібератак на Україну. Якщо у 2020 р. було зафіксовано майже 800 кібератак, у 2021 – 1400, то вже минулого року їхня кількість зросла більш як утричі [1].

Наведені дані свідчать про ведення проти України так званої кібервійни.

Разом з тим у законодавстві України поняття кібервійни не закріплене. Законом України

«Про основні засади забезпечення кібербезпеки України» надаються дефініції таких понять як кібербезпека, кіберзлочин та ін. Так, під кіберзлочином (комп'ютерним злочином), згідно п. 8 ч. 1 цього Закону, законодавець розуміє суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнане злочином міжнародними договорами України [2].

При цьому Кримінальний Кодекс (далі – КК) України не містить поняття кіберзлочину, а суспільно небезпечні діяння, що вчиняються у кіберпросторі та/або з його використанням, передбачені різними розділами Особливої частини.

Аналіз вироків по кримінальних провадженнях за ст. 361 КК України за період 2022 – початку 2023 років, внесених до Єдиного державного реєстру судових рішень, дозволяє стверджувати про відсутність на сьогоднішній день вироків щодо осіб, які здійснили кібератаки, спрямовані на втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж установ, підприємств та організацій України з метою пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення [3].

Питання визначення об'єкта та предмета злочину є важливими у кримінальному праві, оскільки без з'ясування цих питань неможливо досліджувати та вирішувати питання відповідальності за вчинені злочини.

Аналіз досліджень і публікацій з проблеми. Питання втручання в роботу інформаційних(автоматизованих), електронних, інформаційно-комунікаційних систем та електронних комунікаційних мереж присвячені праці таких науковців: В.Г. Гончаренка, М.І. Панова, П.П. Андрушка, А.М. Ришелюка.

Метою статті є дослідження правового статусу безпосереднього об'єкта та предмета несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. З урахуванням того, що розвиток інформаційно-телекомунікаційних систем та комп'ютерних мереж не стоїть на місці, а увага суспільства до кримінальних порушень, пов'язаних з їх використанням зростає, то виникає необхідність у вдосконаленні норм чинного законодавства, зокрема в питанні саме дефініцій об'єкта та предмета, адже станом на теперішній час ці визначення не врегульовані, що призводить до неможливості притягнення до кримінальної відповідальності за кримінальні правопорушення, юридичний склад яких передбачений дефініціями ст. ст. 361, 361-1 КК України.

Виклад основного матеріалу дослідження. Ст. 361 КК України передбачає відповідальність за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації. Створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж передбачає відповідальність за ст. 361-1 КК України.

Об'єктом несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних, інформаційно-комунікаційних систем, електронних комунікаційних мереж можуть бути різні компоненти, пристрої та ресурси, які використовуються для обробки, зберігання та передачі інформації. Деякі з основних об'єктів несанкціонованого втручання включають:

- Сервери інформаційних систем: Це центральні пристрої, які надають сервіси та ресурси для користувачів, такі як зберігання даних, обчислення та мережеві послуги. Несанкціоноване втручання може полягати в несанкціонованому доступі до цих серверів або в їх атаках для завдання шкоди або злому систем безпеки;

- Комп'ютери та робочі станції: Це індивідуальні пристрої, які використовуються користувачами для роботи з інформацією. Несанкціоноване втручання може включати в себе злам або компрометацію цих пристроїв, щоб отримати доступ до конфіденційної інформації або для розповсюдження шкідливого програмного забезпечення;

- Мережеве обладнання: Це включає в себе різні пристрої, такі як маршрутизатори, комутатори, файрволи та інші пристрої, які забезпечують з'єднання та забезпечують безпеку мережі. Несанкціоноване втручання може включати атаки на це обладнання для перехоплення або переривання мережевого трафіку;

- Бази даних: Це структуровані сховища даних, які зберігають велику кількість інформації, таку як особисті дані, фінансова інформація, медичні записи тощо. Несанкціоноване втручання може полягати в зламі баз даних для видалення, модифікації або крадіжки конфіденційної інформації;

- Канали зв'язку: Це фізичні та логічні засоби передачі даних, такі як кабелі, бездротові зв'язки, супутникові зв'язки тощо. Несанкціоноване втручання може включати перехоплення або зміну даних, які передаються по цих каналах, а також блокування або переривання зв'язку.

Загальна мета несанкціонованого втручання в такі об'єкти полягає в отриманні незаконного доступу до конфіденційної інформації, завданні шкоди або перешкоді в роботі інформаційних систем та мереж.

Основним безпосереднім об'єктом кримінального правопорушення, передбаченого ст. 361, як і основним безпосередніми об'єктом кримінального правопорушення, передбаченого ст. 361[1] є встановлений порядок обробки (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання) комп'ютерної інформації у інформаційних (автоматизованих) системах та/або порядок обробки, в тому числі передавання інформації мережами електрозв'язку (телекомунікаційними системами), а також встановлений порядок доступу до такої інформації.

Додатковим (обов'язковим) об'єктом даних кримінальних правопорушень є право власності на комп'ютерну інформацію та/або інформацію, що передається мережами електрозв'язку, в цілому чи його окремі складові частини (елементи) - право володіння, право користування та/або право розпорядження зазначеними видами інформації.

Предметом кримінального правопорушення, юридичний склад якого закріплений у ст. 361 КК України є: 1) електронно-обчислювальні машини (комп'ютери); 2) автоматизовані системи; 3) комп'ютерні мережі; 4) мережі електрозв'язку; 5) комп'ютерна інформація; 6) інформація, що передається мережами електрозв'язку.

Предметом несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних, інформаційно-комунікаційних систем, електронних комунікаційних мереж може бути будь-яка дія або процес, спрямований на порушення їх нормальної роботи або використання з метою завдання шкоди чи отримання несанкціонованого доступу до інформації. До таких предметів можна віднести:

- Несанкціонований доступ: Це включає в себе нелегальне або несанкціоноване проникнення в систему, отримання доступу до захищених даних або ресурсів без відповідних дозволів або авторизації;

- Кібератаки: Такі як віруси, черви, троянські коні, деніал-сервіс атаки та інші форми шкідливого програмного забезпечення, спрямовані на завдання шкоди системам, даним або інфраструктурі;

- Перешкоджання роботі систем: Це може включати блокування доступу до послуг, відмову в обслуговуванні (DoS) або розподілену відмову в обслуговуванні (DDoS), перехоплення комунікацій або інші дії, які перешкоджають нормальному функціонуванню системи чи мережі;

- Маніпуляція або зміна інформації: Це включає в себе незаконне змінення, видалення або викривлення даних, що зберігаються в інформаційних системах;

- Шпигунство і шахрайство: Це може включати в себе витоки конфіденційної інформації,

крадіжку особистої ідентифікаційної інформації, фішинг, соціальне інженерство та інші методи отримання конфіденційних даних або зламу систем безпеки.

Ці предмети можуть бути використані для різних цілей, включаючи політичні, економічні, військові або кримінальні мотиви. Вони можуть призвести до серйозних наслідків, таких як втрата даних, порушення приватності, фінансові втрати та зниження довіри громадськості до інформаційних та комунікаційних систем.

Предметом кримінального правопорушення, склад якого передбачений ст. 361[1] КК України, є шкідливі програмні або технічні засоби, призначені для несанкціонованого втручання в роботу комп'ютерів, мереж електрозв'язку. Як предмет злочину комп'ютерні програми (програмні засоби) повинні бути шкідливими, тобто здатними забезпечити несанкціонований доступ до інформації, а також змінити, знищити, пошкодити, заблокувати комп'ютерну інформацію чи ту, яка передається мережами електрозв' язку.

Предметом злочину в класичній теорії кримінального права визнаються речі матеріального світу, впливаючи на які особа посягає на цінності (блага), що належать суб'єктам суспільних відносин [3, с. 134].

Підхід до визначення правопорушень, що посягають на безпеку використання комп'ютерних систем, в світі є неоднаковим. Так, Кримінальний кодекс штату Юта (США) під предметом таких злочинів розуміє «відчутні та невідчутні елементи, що пов'язані з комп'ютерами, комп'ютерними системами та мережами» [4].

Стосовно визначення предмета кримінального правопорушення, передбаченого ст. 361 КК України, висловлено декілька точок зору.

Предмет правопорушення, юридичний склад якого передбачено ст. 361 КК України, А.М. Ришелюк визначає як: «1) автоматизовані електронно-обчислювальні машини (комп'ютери, АЕОМ), у тому числі персональні; 2) їх системи; 3) комп'ютерні мережі» [5, с. 902].

В.Г. Гончаренко предмет вказаного злочину визначав, як «кілька елементів сфери електронного інформаційного забезпечення життя суспільства: електронно-обчислювальні машини (ЕОМ); програмні матеріали, що забезпечують нормальне функціонування ЕОМ; носії інформації; системи ЕОМ та комп'ютерні мережі» [6, с. 721].

На думку М.І. Панова, предметом злочину, що розглядається, є: 1) електронно-обчислювальна машина; 2) автоматизовані комп'ютерні системи (АКС); 3) комп'ютерні мережі; 4) носії комп'ютерної інформації; 5) комп'ютерна інформація [7, с. 363].

П.П. Андрушко до предмету вказаного правопорушення відносить:

1) автоматизовані електронно-обчислювальні машини;

2) системи АЕОМ або автоматизовані системи;

3) комп'ютерні мережі;

4) носії комп'ютерної інформації;

5) комп'ютерні віруси;

6) комп'ютерну інформацію;

7) програмні і технічні засоби, призначені для незаконного проникнення в автоматизовані електронно-обчислювальні машини, їх системи та комп'ютерні мережі [8, с. 783-784].

Наведені думки щодо кола предметів правопорушення, юридичний склад якого передбачено ст. 361 КК України, мають значну низку розбіжностей. При цьому, слід зауважити, що деякі фахівці не відносять до кола альтернативних предметів правопорушення комп'ютерну інформацію [5, с. 902], яка прямо вказана в ст. 361 КК України як предмет, на перекручення або знищення якого направлені дії суб'єкта правопорушення. Невизнання комп'ютерної інформації окремими фахівцями предметом злочину обумовлено «матеріалістичним» підходом класичної теорії кримінального права до визначення предмета злочину як певних матеріальних цінностей. В той час, комп'ютерна інформація є предметом віртуальним, тобто «умовним, фізично відсутнім, але за допомогою спеціальних методів наданим у розпорядження» [6, с. 702].

О.Е. Радутний, досліджуючи інформацію як предмет злочину, дійшов висновку, що сьогоденні реалії вимагають визнати в подальшому предметом злочину речі або інші явища об'єктивного світу (інформація, енергія тощо), з певними властивостями яких кримінальний за-

кон пов'язує наявність у діянні особи складу конкретного злочину [7].

Однак, якщо аналізувати предмет правопорушення у відповідності з наведеним визначенням, під поняття предмета правопорушення підпадають усі речі і явища об'єктивного світу, з властивостями яких пов'язана наявність складу кримінального правопорушення в певних діях. При цьому діяння суб'єкта правопорушення на них може не бути спрямована, та вони можуть не зазнавати злочинного впливу. Поняття «час», для деяких кримінальних правопорушень є обов'язковою ознакою.

Необхідно конкретизувати це визначення, з урахуванням особливостей безпосередньо визначення поняття предмета кримінального правопорушення, як одного з обов'язкових елементів складу кримінального правопорушення.

Під предметом кримінального правопорушення доцільно розуміти речі або інші явища об'єктивного світу, як матеріальні, так і віртуальні, з певним впливом на які кримінальний закон пов'язує наявність у діянні особи складу конкретного правопорушення.

Якщо говорити про предмет саме кримінального правопорушення несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних, інформаційно-комунікаційних систем, доцільно розглядати інформацію, яка міститься безпосередньо в зазначених системах. Тут вважаємо за доцільне виходити із мети правопорушення, а саме «втручання», яке за кінцеву ціль має нанесення матеріальної шкоди фізичним особам чи об'єктам інфраструктури.

Лишається з'ясувати поняття комп'ютерної інформації.

Дане поняття є спірним і має декілька визначень.

Так, поняття «комп'ютерна інформація» може мати різні визначення залежно від контексту використання і специфіки області знань. Однак, загальною основою для розуміння цього терміну є те, що комп'ютерна інформація - це будь-яка інформація, яка зберігається, обробляється або передається за допомогою комп'ютерної технології.

Комп'ютерною інформацією як даними в цифровому форматі можуть бути будь-якими даними, які зберігаються у цифровій формі, такими як текстові документи, зображення, відео, аудіофайли, програми тощо.

Інформація, оброблювана комп'ютером включає в себе будь-яку інформацію, яка обробляється або аналізується комп'ютерними програмами або системами, незалежно від формату даних.

Інформація, що передається по мережі також може бути будь-якою інформацією, яка передається через комп'ютерні мережі, такі як Інтернет, локальні мережі тощо. І вона також є комп'ютерною.

Електронні документи: комп'ютерна інформація часто асоціюється з електронними документами, які зберігаються у цифровому форматі і можуть бути відкриті та оброблені за допомогою комп'ютерних програм.

Дані, що можуть бути оброблені комп'ютером це також комп'ютерна інформація, а саме дані будь-якого типу, які можуть бути зрозумілі та оброблені комп'ютером, включаючи тексти, числа, графіки, відео, звук тощо.

Закон України «Про інформацію» в ст. 1 визначає інформацію як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Однак у даному Законі не йдеться про комп'ютерну інформацію як таку, проте говориться про носії інформації та її форму - електронний вигляд. З чого по суті можна дійти висновку, що комп'ютерна інформація - це сукупність символів, кодів, сигналів, команд, що виражені в комп'ютерних програмах, що забезпечують функціонування та керування комп'ютерною технікою, а також за допомогою яких певні відомості набувають електронної форми, забезпечують проведення різних операцій, проявляються назовні; відомості, які не виражені у формі програми, за допомогою яких здійснюється несанкціонований доступ (паролі, електронні сертифікати, ключі доступу). Комп'ютерна інформація характеризується наявністю носія, має власні змістовні та формальні властивості, існує незалежно від свідомості людини, може зберігатися на будь-

яких носіях: локальних (жорсткі та оптичні диски, флеш-накопичувачі); віддалених (різноманітні банки даних і сервери, в тому числі «хмарні сховища»). При цьому «хмарні сховища» - це специфічне місце зберігання інформації, яке зазвичай входить до «системи хмарних обчислень».

Предметом кримінального правопорушення, передбаченого ст. 361 КК України, судячи з диспозиції є інформація, але аналіз об'єкта і форм об'єктивної сторони несанкціонованого втручання дає підстави стверджувати, що до предметів даного злочину відносяться комп'ютерна інформація та інформація, що передається каналами зв'язку.

Специфіка комп'ютерної інформації як предмета кримінального правопорушення полягає в неможливості її віднесення ні до матеріальних, ні до нематеріальних предметів. Комп'ютерна інформація, як нематеріальний об'єкт, може бути включена в систему суспільних відносин за допомогою матеріального носія. Фізичний носій комп'ютерної інформації виступає як засіб передачі, зберігання та обробки цієї інформації. Різноманітні засоби зберігання і передачі даних, такі як дискети, оптичні та жорсткі диски, USB-накопичувачі, мережеві пристрої передачі даних тощо, служать в якості носіїв комп'ютерної інформації.

Фізичний носій інформації може бути використаний як матеріальний доказ у кримінальних справах, коли йдеться про кримінальні правопорушення, пов'язані з комп'ютерною інформацією, такі як хакерські атаки, крадіжки даних, вірусні атаки тощо. У таких випадках фізичний носій інформації може бути вилучений як доказ і використовуватися на суді для доведення вини чи невинуватості підозрюваного або обвинуваченого.

Отже, фізичні носії комп'ютерної інформації відіграють важливу роль у її передачі, зберіганні та обробці, а також у вирішенні кримінальних випадків, пов'язаних з використанням цієї інформації.

Інформація, як предмет правопорушень, може мати економічну цінність. Ця цінність визначається її змістом, корисністю та зацікавленістю споживача в одержанні цієї інформації.

Наприклад, деяка інформація може бути важливою для підприємств, організацій або осіб з економічної точки зору. Ця інформація може включати комерційні та конфіденційні дані, такі як бізнес-плани, патенти, торгові секрети, клієнтські списки тощо.

Інформація, яка допомагає в прийнятті рішень з економічних питань, також може мати значну цінність. Це може бути аналітична інформація, статистика, прогнози ринку та інші дані, які впливають на економічну діяльність. Компанії можуть витрачати значні ресурси на збір, обробку та аналіз інформації з метою отримання конкурентної переваги або збільшення ефективності своєї діяльності.

В деяких випадках інформація може бути об'єктом торгівлі. Це може бути продаж інформації між компаніями або особами, купівля конфіденційних даних для використання у конкурентній боротьбі тощо.

Отже, економічна цінність інформації визначається її значимістю для сторін, які можуть використовувати або володіти цією інформацією. Ця цінність може бути врахована в судових розглядах кримінальних правопорушень, де інформація виступає як об'єкт вкрадення, зламу або недозволеного доступу.

Необхідно вказати, що оцінювання комп'ютерної інформації виключно як сукупності (єдності) програм, даних, файлів є недоцільним, через те, що кожна програма, файл або база даних також є різновидом комп'ютерної інформації, і кримінальна відповідальність повинна наступати за порушення цілісності або руйнування хоча б одного з вказаних предметів. В іншому випадку, тобто в разі визнання предметом кримінального правопорушення сукупності всіх програм, баз даних та файлів в електронно-обчислювальних машинах, втрачають сенс деякі з інших важливих положень.

Програмне забезпечення (ПЗ) електронно-обчислювальних машин, систем та комп'ютерних мереж безпосередньо відноситься до комп'ютерної інформації. Воно є невід'ємною складовою цієї інформації і відіграє важливу роль у функціонуванні та управлінні комп'ютерними пристроями та системами.

Програмне забезпечення включає в себе програми, які використовуються для виконання різноманітних завдань на комп'ютерах, від операційних систем і програмного забезпечення офісного призначення до програм для розваг, наукових досліджень, розробки веб-сайтів та багато іншого. Це може бути як комерційне, так і вільне програмне забезпечення.

Так само, як і інша комп'ютерна інформація, програмне забезпечення може бути об'єктом правопорушень, таких як піратство програмного забезпечення, крадіжка конфіденційної інформації, створення та розповсюдження вірусів або іншого шкідливого програмного коду тощо. Такі дії можуть мати серйозні правові наслідки для осіб, що вчиняють подібні дії.

Стосовно інформації, яка передається каналами електрозв'язку, то вона також може бути комп'ютерною, оскільки телефонні лінії та бездротові мережі стільникового зв'язку - це складові комп'ютерної мережі.

Висновки. З метою правильної кваліфікації кримінальних правопорушень, направлених на несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних, інформаційно-комунікаційних систем, електронних мереж, необхідно чітко визначити на законодавчому рівні дефініцію предмета цих кримінальних правопорушень та визначити, що входить до поняття комп'ютерної інформації. Окрім цього, законодавцю варто врахувати, що характеризуючою ознакою предмету даних правопорушень є саме постійний розвиток та розширення кола об'єктів.

Література

1. Кібервійна рф проти України: як працюють російські хакери та воюють українські кібервійська. URL: https://thepage.ua/-ua/politics/kibervijna-rf-proti-ukrayini-yak-voyuyut-ukrayinski- kibervijska.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. URL: https://zakon.rada.gov.ua/la-ws/show/2163-19#Tex.

3. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. URL: https://gp.gov.ua/ua/posts/ pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih- dosudovogo-rozsliduvannya-2.

4. Кравцов С.Ф. Предмет злочину: автореферат дисертації на здобуття наукового ступеня канд. юридичних наук. 12.00.08; Панов Н.І. Спосіб скоєння злочину та кримінальна відповідальність. Харків: Вища школа, 1982. С. 127-143.

5. 76-6-106.1. Criminal Code of State Utah. // http://www.utahcusa.-criminal.codes.ng.htm.

6. Науково-практичний коментар Кримінального кодексу України від 5 трав. 2001 року. За ред. Мельника М.І., Хавронюка М.І. Київ: Каннон, А.С.К., 2001. С. 902.

7. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю (аналіз складів злочинів): Дисертація к-та юрид. наук: 12.00.08. Національна юридична академія України імені Ярослава Мудрого. Харків, 2002. 240 с.

8. Науково-практичний коментар до Кримінального Кодексу України. Під загальною редакцією Потебенька М.О., Гончаренка В.Г. Київ: ФОРУМ, 2001. У 2-х ч. Особлива частина. 721 с.

9. Кримінальне право України: Особлива частина: підруч. для студ. вищ. навч. зал. освіти. Бажанов М.І., Тацій В.Я., Сташис В.В., Зінченко І.О. та ін.; за ред. професорів Бажанова М.І., Сташиса В.В., Тація В.Я. Київ: Юрінком Інтер; Харків: Право, 2001. С. 363.

10. Науково-практичний коментар до Кримінального кодексу України: за станом законодавства і Постанов Пленуму Верховного Суду України на 1 груд. 2001 р. За ред. Яценка С.С. Київ: А.С.К., 2002. С. 783-784.

11. П.1.47 ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Видання офіційне. Київ: Держстандарт України, 1994.

12. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю. Автореф. дис. канд. юрид. наук. Харків, Національна юридична академія України ім. Ярослава Мудрого, 2002. С. 10 (21 с.).

References

1. Kiberviijna rf proti Ukraini: yak pracyuyut rosijski hakeri ta voyuyut ukrainski kibervijska. URL: https://thepage.ua/ua/politics/kibervijna-rf-proti-ukrayini-yak-voyuyut-ukrayinski- kibervijska.

2. Pro osnovni zasadi zabezpechennya kiber-bezpeki Ukraini: Zakon Ukraini vid 05.10.2017 r. URL: https://zakon.rada.gov.ua/laws/ show/2163-19#Tex.

3. Pro zareyestrovani kriminalni pravopo-rushennya ta rezultati jih dosudovogo rozsli-duvannya. URL: https://gp.gov.ua/ua/posts/ pro-zareyestrovani -kriminalni-pravoporushennya-ta-rezultati-yih- dosudovogo-rozsliduvannya-2.

4. Kravcov S.F. Predmet zlochinu: Avtoreferat disertaciyi na zdobuttya naukovogo stupenya kandidat yuridichnih nauk. 12.00.08. Panov N.I. Sposib skoyennya zlochinu ta kriminalna vidpovi-dalnist. - Harkiv: Visha shkola, 1982. - s. 127-143.

5. 76-6-106.1. Criminal Code of State Utah. http: www.utahcusa.criminal.codes.ng.htm.

6. Naukovo-praktichnij komentar Kriminalnogo kodeksu Ukrayini vid 5 trav. 2001 roku. Za red. Melnika M.I., Havronyuka M.I. – Kyiv: Kannon, A.S.K., 2001. - S. 902.

7. Radutnij O.E. Kriminalna vidpovidalnist za nezakonne zbirannya, vikoristannya ta rozgoloshennya vidomostej, sho stanovlyat komercijnu tayemnicyu (analiz skladiv zlochiniv): Disertaciya k-ta yurid. nauk: 12.00.08. Nacionalna yuridichna akademiya Ukrayini imeni Yaroslava Mudrogo. – Kharkiv, 2002. – 240 s.

8. Naukovo-praktichnij komentar do Kriminal-nogo Kodeksu Ukrayini. Pid zagalnoyu redakciyeyu Potebenka M.O., Goncharenka V.G. – Kyiv, - *«FORUM»*, 2001., u 2-h ch. – Osobliva chastina. – S. 721.

9. Kriminalne pravo Ukrayini: Osobliva chastina: Pidruch. dlya stud. vish. navch. zal. Osviti. Bazhanov M.I., Tacij V.Ya., Stashis V.V., Zinchenko I.O. ta in. Za red. Profesoriv Bazhanova M.I., Stashisa V.V., Taciya V.Ya. – Kyiv: Yurinkom Inter; Kharkiv: Pravo, 2001. - S. 363.

10. P.1.47 DSTU 2226-93. Avtomatizovani sistemi. Termini ta viznachennya. Vidannya oficijne. - Kiyiv: Derzhstandart Ukrayini, 1994.

11. Naukovo-praktichnij komentar do Kriminalnogo kodeksu Ukrayini: Za stanom zakonodavstva i Postanov Plenumu Verhovnogo Sudu Ukrayini na 1 grud. 2001 r. Za red. Yacenka S.S. – Kyiv: A.S.K., 2002. –s. 783-784.

12. Radutnij O.E. Kriminalna vidpovidalnist za nezakonne zbirannya, vikoristannya ta rozgoloshennya vidomostej, sho stanovlyat komercijnu tayemnicyu. Avtoref. dis. kand. yurid. nauk. –Harkiv, Nacionalna yuridichna akademiya Ukrayini im. Yaroslava Mudrogo, 2002. – S. 10 (21 s.).

Dina Dryzhakova

DEFINITION OF THE SUBJECT AND OBJECT OF UNAUTHORIZED INTERFERENCE IN THE WORK OF INFORMATION (AUTOMATED), ELECTRONIC, INFORMATION AND COMMUNICATION SYSTEMS, ELECTRONIC COMMUNICATION NETWORKS (ARTICLES 361, 361-1 OF THE CRIMINAL CODE OF UKRAINE)

Taras Shevchenko National University of Kyiv
64 Volodymyrska St., 01601, Kyiv, Ukraine
E-mail: d.dryzhakova@gmail.com

The purpose *of the article is to study the legal status of the subject and object of unauthorized interference with the operation of information (automated), electronic, information and communication systems and electronic communication networks.* ***Research methods:*** *the article uses the dialectical method of cognition, general scientific and special research methods. In particular, structural-functional, deductive methods and the method of scientific forecasting.* ***Results:*** *the issues raised allow us to explore the problems associated with the rapid development of technology and the increasing number of interventions in the work of information (automated), electronic, information and communication systems and electronic communication networks, which leads to the need to improve legislation.* ***Discussion:*** *the article provides a criminal law description of the subject and object of unauthorized interference with the operation of information (automated), electronic, information and communication systems and electronic communication networks.*

The author concludes that to properly classify criminal offences related to unauthorised interference with the operation of information systems, it is necessary to clearly define the subject matter of these offences at the legislative level. This includes electronic, information and communication systems, and electronic networks. It is important to determine what is included in the concept of computer information. Additionally, legislators should consider that these offences involve constantly evolving and expanding objects.

Key words: *regulatory and legal regulation; law; information and telecommunication system; cyber terrorism; cyber threat; telecommunication expertise; computer and technical expertise.*

Стаття надійшла до редакції 18.03.2024