Юридичні науки

УДК 343.9

Дрижакова Діна Юріївна

аспірант кафедри кримінально-правової політики та кримінального права

Київського національного університету імені Тараса Шевченка

Dryzhakova Dina

Postgraduate of the

Taras Shevchenko National University of Kyiv

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

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)

Анотація. *Швидкі темпи розвитку інформаційно-телекомунікаційних технологій, систем та мереж розширюють можливості їх використання у різних видах кримінально-протиправної діяльності. Зростання кількості користувачів кіберпростору сприяє не тільки скоєнню стосовно них кримінальних правопорушень, а й можливості їхньої участі у злочинній діяльності, у тому числі в її організованих формах.*

Нажаль, законодавство не встигає за розвитком зазначеної сфери, що приводить до неврегульованості більшості злочинів, вчинених на просторах інформаційної інфраструктури.

Бодай не кожна особа, може стати потерпілою внаслідок діяльності кіберзлочинців, адже бодай не всі особисті дані зберігаються в оцифрованому вигляді. Окрім цього, в період військового стану, неправомірний або несанкціонований доступ по цифрової інформації з подальшим зараженням їх шкідливими програмами може завдати значної шкоди національній безпеці.

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

Summary. *The rapid pace of development of information and telecommunication technologies, systems and networks expands the possibilities of their use in various types of criminal and illegal activities. The increase in the number of cyberspace users contributes not only to the commission of criminal offenses against them, but also to the possibility of their participation in criminal activity, including in its organized forms.*

Unfortunately, the legislation does not keep up with the development of the specified area, which leads to the unsolved nature of most crimes committed in the spaces of the information infrastructure.

Perhaps not every person can become a victim as a result of the activities of cybercriminals, because perhaps not all personal data is stored in digital form. In addition, during martial law, illegal or unauthorized access to digital information and its subsequent contamination with malware can cause significant damage to national security.

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

Постановка проблеми. 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» надається визначення таким поняттям як кібербезпека, кіберзлочин та ін. Так, під кіберзлочином (комп'ютерним злочином), згідно п. 8 ч. 1 цього Закону, мається на увазі суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

При цьому 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.

Аналіз досліджень і публікацій. Питання втручання в роботу інформаційних (автоматизованих), електронних, інформаційно-комунікаційних систем та електронних комунікаційних мереж присвячені праці наступних науковців: В.Г. Гончаренко, М.І. Панова, П.П. Андрушко, А.М. Ришелюк.

Формулювання цілей статті. Дослідження правового статусу предмета та об'єкта несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Виклад основного матеріалу. Стаття 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 КК України.

Об'єктом аналізованих злочинів можуть бути суспільні відносини у сфері комп'ютерної інформації.

Предметом злочину в класичній теорії кримінального права визнаються речі матеріального світу, діючи на які особа посягає на цінності (блага), що належать суб'єктам суспільних відносин [3, с. 21].

Підхід до визначення предмету злочинів, 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 поріднені з комп'ютерами, комп'ютерними системами та мережами" [3, с. 45].

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

Предмет злочину, передбаченого 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" [4, с. 234].

В.Г. Гончаренко предмет вказаного злочину визначає, 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" [5, с. 543].

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 [5, с. 567].

П.П. Андрушко до предмету вказаного злочину 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 [6, с. 435].

Наведені думки щодо кола предметів злочину, передбаченого статтею 361 КК України, мають значну низку розбіжностей. При цьому,

слід зауважити, що деякі фахівці не відносять до кола альтернативних предметів злочину комп'ютерну інформацію, яка прямо вказана в статті 361 КК України як предмет, на перекручення або знищення якого направлені дії злочинця. 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" [7, с. 783].

Якщо розглядати інформацію як об'єкт права власності, то об'єктом несанкціонованого втручання в роботу відповідних мереж, будуть суспільні відносини щодо створення, користування, володіння та забезпечення безпеки комп'ютерної інформації, оскільки комп'ютерна інформація є результатом розумової діяльності людини.

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Тут утворюється ситуація, коли одночасно існують щонайменше два види суспільних відносин: первісні – пов'язані з комп'ютерною інформацією, і вторинні – ті, що утворюються при убезпеченні суспільних відносин, пов'язаних із комп'ютерною інформацією.

Звичайно, що відокремлення одне від одного зазначених відносин - первісних і вторинних – є штучним, воно може бути здійснене лише у теоретичних викладках. Проте саме з позицій доктрини правильнішим видається встановлювати кримінально-правовий захист первісних суспільних відносин, а не вторинних - відносин безпеки (у нашому випадку суспільних відносин безпеки інформаційної). Адже злочин спрямовано на заподіяння шкоди насамперед первісним суспільним відносинам, шкода відносинам безпеки спричиняється, так би мовити, вимушено. Суб'єкт у процесі заподіяння шкоди первісним відносинам

очевидно має «зруйнувати» їх «захист», тобто заподіяти шкоду відносинам безпеки.

Виходячи із викладеного вважаю, що об'єктом несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних, комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж є суспільні відносини щодо безпеки реалізації потреб, що задовольняються обробкою та передачею інформації за допомогою інформаційно-телекомунікаційних систем, яким завдано шкоди чи щодо яких існує загроза такої шкоди.

Якщо коротко, то об'єкт злочину – це суспільні відносини, порушення яких становить соціальну суть злочину та, які безпосередньо охороняються законом.

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

Предмет злочину, передбаченого 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" [7, с. 784].

В.Г. Гончаренко предмет вказаного злочину визначає, 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" [7, с. 784].

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 [5, с. 568].

Наведені думки щодо кола предметів злочину, передбаченого статтею 361 КК України, мають значну низку розбіжностей. При цьому,

слід зауважити, що деякі фахівці не відносять до кола альтернативних предметів злочину комп'ютерну інформацію, яка прямо вказана в статті 361 КК України як предмет, на перекручення або знищення якого направлені дії злочинця. Вважаємо, що 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".

Під віртуальним слід розуміти такий предмет об'єктивного світу, який створений за допомогою спеціальних методів та (або) способів, є фізично відсутнім, але має зовнішнє представлення, або може набути такого представлення за допомогою спеціальних методів або способів впливу.

О.Н. 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 закон пов'язує наявність у діянні особи складу конкретного злочину [9, с. 156].

Однак, якщо аналізувати предмет злочину у відповідності з наведеним визначенням, під поняття предмета злочину підпадають усі речі і явища об'єктивного світу, з властивостями яких пов'язана наявність складу злочину в певних діях. При цьому діяння злочинця на них може не бути спрямована, та вони можуть не зазнавати злочинного впливу. Так, наприклад, поняття "час", для деяких злочинів є обов'язковою ознакою об'єктивного боку, через те, що закон пов'язує наявність конкретного часу, або повного виду часу з визначенням складу певного злочину. При цьому, час, не виступає предметом злочину, так як особа на нього не

впливає; поняття "час" належить до факультативних ознак об'єктивної сторони серед інших: місце, спосіб, обстановка та інші. Аналогічно необхідно відмежовувати знаряддя вчинення злочину від предмету злочинного посягання, розуміючи, що знаряддями можуть виступати також речі як матеріального, так і віртуального світу [8, с. 123].

Необхідно конкретизувати дане визначення, з урахуванням особливостей безпосередньо визначення поняття предмета злочину, як одного з обов'язкових елементів складу злочину.

Під предметом злочину 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 злочину.

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

Лишається з'ясувати поняття комп'ютерної інформації.

Дане поняття є спірним і має декілька визначень.

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 йде мова про комп'ютерну інформацію як таку, проте говориться про носії інформації та її форму електронний вигляд. З чого по суті можна зробити висновок, 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». Його суть полягає в тому, що дані зберігаються на численних, розподілених у мережі серверах, проте для клієнта вони постають як єдина система, під час втручання в один відбувається посягання на всю систему. За сучасних умов такі сховища є новим місцем зберігання комп'ютерної інформації, яке потребує належної кримінально-правової охорони. Пов'язано це з тим, що наразі відбувається активний перехід державних реєстрів на «системи хмарних обчислень», складовою яких є «хмарні сховища», при цьому більшість таких систем зараз є більш захищеними від стороннього впливу порівняно з локальними (нерозподіленими) носіями інформації.

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 злочину сукупності всіх програм, баз даних та файлів в електронно-обчислювальних машинах, втрачають сенс деякі з інших важливих положень. Наприклад, визначення в якості кваліфікуючої ознаки в ч. 2 ст.

361 КК України "заподіяння істотної шкоди" стає недоцільним, тому що за ч. 1 ст. 361 КК можна буде притягнути до кримінальної відповідальності лише особу, яка спричинила тотальну шкоду комп'ютеру, тобто, коли вона руйнівно вплинула на всю сукупність програмного забезпечення і інформації, що зберігалась в електронно-обчислювальній машині. В такому випадку відсутня диференціація між поняттям "шкода" і "істотна шкода", так як під поняття "шкода" підпадатиме виключно тотальний вплив на комп'ютерну систему – вплив на "сукупність всіх даних і програм". Якщо суб'єктом буде завдано шкоди одній програмі, така особа, відповідно до наведених тверджень, може уникнути кримінальної відповідальності.

Крім того, відсутній практичний сенс зазначати обов'язковою ознакою комп'ютерної інформації наявність у неї спеціального захисту, якщо злочин, що посягає на цілісність інформації не сформульовано як «Несанкціонований доступ до комп'ютерної інформації". Досить вказати на наявність авторизації інформації, тобто фіксації її приналежності певному власникові або користувачеві.

Слід звернути увагу, що програмне забезпечення електронно-обчислювальних машин, їх систем та комп'ютерних мереж, у відповідності з визначенням поняття "комп'ютерна інформація", безпосередньо належить до комп'ютерної інформації.

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 даного дослідження і перспективи подальших досліджень у даному напрямку. З метою правильної кваліфікації злочинів, направлених на несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних, інформаційно-

комунікаційних систем, електронних мереж, необхідно чітко визначити нормативно, що є предметом даних злочинів та визначити, що входить до поняття комп'ютерної інформації.

Література

1. Толуб Н. Кібервійна рф проти України: як працюють російські хакери та воюють українські кібервійська. *The Page.* 2023. URL: https://thepage.ua/ua/politics/kibervijna-rf-proti-ukrayini-yak-voyuyut-ukrayinski-kibervijska (дата звернення:13.12.2023).
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. *Відомості Верховної Ради.* 2017. № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 13.12.2023).
3. 76-6-106.1. Criminal Code of the Republic of Ukraine. URL: https://sherloc.unodc.org/cld/uploads/res/document/ukr/2001/criminal-code-of-the-republic-of-ukraine-en_html/Ukraine_Criminal_Code_as_of_2010_EN.pdf (дата звернення: 13.12.2023).
4. Науково-практичний коментар Кримінального кодексу України від 5 травня 2001 року / За ред. М.І. Мельника, М.І. Хавронюка. К.: Каннон, А.С.К., 2001. 1104 с.
5. Науково-практичний коментар до Кримінального Кодексу України / За заг. ред. Потебенька М.О., Гончаренка В.Г. У 2-х ч. Особлива частина. К.: "ФОРУМ", 2001. 721 с.
6. Кримінальне право України: Особлива частина: Підруч. для студ. вищ. навч. зал. освіти / М.І. Бажанов, В.Я. Тацій, В.В. Сташис, І.О. Зінченко та ін.; За ред. Професорів М.І. Бажанова, В.В. Сташиса, В.Я. Тація. К.: Юрінком Інтер; Х.: Право, 2001. 764 с.

7. Науково-практичний коментар до Кримінального кодексу України: За станом законодавства і Постанов Пленуму Верховного Суду України на 1 грудня 2001 р. / За ред. С.С. Яценка. К.: А.С.К., 2002. 967 с.
8. П.1.47 ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Видання офіційне. Київ: Держатсндарт України, 1994. 321 с.
9. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю: дис. ... канд. юрид. наук. Харків, Національна юридична академія України ім. Ярослава Мудрого, 2002. 204 с.

References

1. Tolub N. Kiberviina rf proty Ukrainy: yak pratsiuiut rosiiski khakery ta voiuiut ukrainski kiberviiska. The Page. 2023. URL: https://thepage.ua/ua/politics/kibervijna-rf-proti-ukrayini-yak-voyuyut-ukrayinski-kibervijska
2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 r. Vidomosti Verkhovnoi Rady. 2017. № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. 76-6-106.1. Criminal Code of the Republic of Ukraine. URL: https://sherloc.unodc.org/cld/uploads/res/document/ukr/2001/criminal-code-of-the-republic-of-ukraine-en_html/Ukraine_Criminal_Code_as_of_2010_EN.pdf
4. Naukovo-praktychnyi komentar Kryminalnoho kodeksu Ukrainy vid 5 travnia 2001 roku / Za red. M.I. Melnyka, M.I. Khavroniuka. K.: Kannon, A.S.K., 2001. 1104 s.
5. Naukovo-praktychnyi komentar do Kryminalnoho Kodeksu Ukrainy / Za zah. red. Potebenka M.O., Honcharenka V.H. U 2-kh ch. Osoblyva chastyna. K.: "FORUM", 2001. 721 s.

6. Kryminalne pravo Ukrainy: Osoblyva chastyna: Pidruch. dlia stud. vyshch. navch. zal. osvity / M.I. Bazhanov, V.Ia. Tatsii, V.V. Stashys, I.O. Zinchenko ta in.; Za red. Profesoriv M.I. Bazhanova, V.V. Stashysa, V.Ia. Tatsiia. K.: Yurinkom Inter; Kh.: Pravo, 2001. 764 s.
7. Naukovo-praktychnyi komentar do Kryminalnoho kodeksu Ukrainy: Za stanom zakonodavstva i Postanov Plenumu Verkhovnoho Sudu Ukrainy na 1 hrudnia 2001 r. / Za red. S.S. Yatsenka. K.: A.S.K., 2002. 967 s.
8. P.1.47 DSTU 2226-93. Avtomatyzovani systemy. Terminy ta vyznachennia. Vydannia ofitsiine. Kyiv: Derzhatsndart Ukrainy, 1994. 321 s.
9. Radutnyi O.E. Kryminalna vidpovidalnist za nezakonne zbyrannia, vykorystannia ta rozgholoshennia vidomostei, shcho stanovliat komertsiinu taiemnytsiu: dys. ... kand. yuryd. nauk. Kharkiv, Natsionalna yurydychna akademiia Ukrainy im. Yaroslava Mudroho, 2002. 204 s.