УДК 343.326

***Юлія Безсусідня,***
*аспірант кафедри кримінального права*
*Національної академії внутрішніх справ України*

# СОЦІАЛЬНА ЗУМОВЛЕНІСТЬ КРИМІНАЛІЗАЦІЇ КІБЕРНЕТИЧНИХ АТАК ЯК СУСПІЛЬНО НЕБЕЗПЕЧНОГО ДІЯННЯ ПРОТИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

*Стаття присвячена визначенню чинників соціальної зумовленості криміналізації кібернетичних атак та внесенню змін до Кримінального Кодексу України з метою віднести таке діяння, як кібернетична атака, до складу злочину «диверсія», передбаченого статтею 113 цього Кодексу.*

**Ключові слова:** соціальна зумовленість, криміналізація, підстава криміналізації, кібернетична атака, інформаційна безпека, національна безпека, диверсія.

**Постановка проблеми.** Сьогодні для України існують ризики та небезпеки для її суверенітету, територіальної цілісності та недоторканності. Одним із проявів такої небезпеки є посягання на інформаційну безпеку шляхом здійснення так званих «кібернетичних атак». Важливим для теорії кримінального права і правозастосовної діяльності є вирішення питання криміналізації кібернетичних атак як загрози національній безпеці України шляхом внесення змін до кримінального законодавства України.

**Аналіз останніх досліджень та публікацій.** Правові аспекти кібернетичних атак розглядали Д. В. Дубов, О. А. Ільяшов, О. О. Климчук, С. В. Мельник, Н. А. Ожеван, О. О. Тихомиров, В. П. Шеломенцев та інші науковці, однак вони не визначили підстав для криміналізації кібернетичних атак.

**Метою статті** є висвітлення ознак та змісту чинників, які зумовлюють необхідність криміналізації кібернетичних атак як загрози національній безпеці України.

**Виклад основного матеріалу.** В Україні зафіксували наймасштабнішу кібератаку в історії. 27 червня 2017 року близько 11-00 години проти України була розпочата масована кібератака з використанням модифікованої під Україну версії вірусу «wannacry» - «cryptolocker». Стало відомо від компанії ESET, яка розробляє програмне забезпечення для боротьби зі шкідливими комп'ютерними програмами, що на Україну припало 75, 24 % атак вірусу Petya від загальної кількості у світі.

Незважаючи на широке використання терміна «кібератака», аналіз наукових джерел вказує на відсутність сталого поняття кібернетичної атаки (кібератаки).

Кібернетична атака – цілеспрямована дія (сукупність дій/операцій) у кіберпросторі, яка полягає у здійсненні кібернетичного впливу на певну комп'ютерну систему, спрямованого на пошук уразливостей цієї системи (її окремих елементів) та їх несанкціоноване використання, що може негативно вплинути на стан належного функціонування такої комп'ютерної системи [1, с. 342].

Інформаційна безпека – стан захищеності національних інтересів України в інформаційній сфері від загроз особі, суспільству, державі через неповноту, несвоєчасність інформації, несанкціоноване поширення та використання інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій [2, с. 175].

Інформаційна безпека є одним із найважливіших чинників національної безпеки України. Інформаційна і національна безпека повною мірою узгоджуються і співвідносяться між собою за схемою «частина» і «ціле». Сьогодні інформаційний складник не існує поза межами загальної національної безпеки, так само як і національна безпека не буде всеохоплюючою без інформаційної безпеки [3, с. 9].

Криміналізація як процес віднесення тих чи інших дій до злочинних за своєю суттю є кінцевою реакцією законодавця на потребу та необхідність у кримінально-правовому захисті від конкретного суспільно-небезпечного посягання, що виникло у суспільстві [4, с. 6].

Важливим моментом у криміналізації злочину є чітке визначення підстав криміналізації. Під підставами криміналізації розуміють процеси, що відбуваються в матеріальному і духовному житті суспільства, розвиток яких породжує об'єктивну необхідність кримінально-правової охорони тих чи інших цінностей. Підстави криміналізації – це те, що створює дійсну потребу у кримінально-правовій новелі, внутрішня необхідність виникнення правової норми [5, с. 9].

Під терміном «підстава криміналізації» можуть розуміти дійсні фактори, зумовлені соціальними причинами виникнення або зміни кримінально-правової норми. Отже, підстави криміналізації відсилають дослідження до іншої важливої категорії – соціальна зумовле-

ність. В. І. Борисов зазначив, що соціальна зумовленість кримінального закону визначається різноманітними за значущістю соціальними, економічними, політичними, психологічними та іншими чинниками, встановлення і розкриття яких дає можливість пояснити необхідність кримінально-правової охорони певних суспільних відносин [6, с. 288].

На погляд П. С. Тоболкіна, єдина умова для криміналізації діяння – його суспільна небезпечність [7, с. 49-53].

В. О. Навроцький вважає, що до соціальної зумовленості належать соціальні та соціально-психологічні фактори, що виражають суспільну необхідність і політичну доцільність встановлення кримінальної відповідальності за те чи інше діяння. До них відносять: суспільну небезпечність діяння, його відносну поширеність, домірність позитивних і негативних наслідків криміналізації та кримінально-політичну адекватність криміналізації [8, с. 14].

На думку автора, науковий підхід В. О. Навроцького найбільш об'єктивно відображає чинники для криміналізації діяння в сучасному суспільстві.

Як уже зазначено, основним фактором для криміналізації діяння є його суспільна небезпечність.

Суспільна небезпечність злочинних діянь полягає у здатності породжувати шкідливі з точки зору держави, громадян і суспільства зміни в охоронюваних кримінальним законом суспільних відносинах та створювати загрозу майбутніх шкідливих змін у цих відносинах [9, с. 75].

Для характеристики суспільної небезпечності використовують такі основні поняття, як характер та ступінь суспільної небезпечності, де характер є якісною властивістю, а ступінь – кількісною [5, с. 10].

Характер суспільної небезпечності кібернетичних атак полягає в тому, що цей злочин створює загрозу безпеці держави в усіх її сферах.

Ступінь суспільної небезпечності кібернетичних атак є високим. Тотальна інформатизація всіх сфер діяльності суспільства призвели до збільшення кількості загроз, актів кібертероризму та кіберзлочинів у всьому світі. Також збільшенню кількості інцидентів сприяють закладені в основу Інтернет-технологій принципи відкритості та анонімності.

Другий чинник соціальної зумовленості криміналізації кібернетичних атак – поширеність злочину. Про поширеність кібернетичних атак свідчать фактичні дані, згідно з якими вірус, який вразив державні і приватні комп'ютерні системи України, поширився також у Росії, Англії, Індії, США, загалом вірус поширився у 99 країнах. У Microsoft повідомили, що у світі було інфіковано близько 75 тисяч комп'ютерів.

Щодо третього чиннику соціальної зумовленості криміналізації кібернетичних атак – домірності позитивних і негативних наслідків криміналізації, то позитивний ефект від криміналізації такого діяння буде полягати в попередженні, запобіганні, караності такого діяння в Україні та зменшенні кількості цих діянь.

Четвертий чинник соціальної зумовленості криміналізації кібернетичних атак – кримінально-політична адекватність криміналізації – підтверджується актуальністю і поширеністю теми боротьби з кібернетичними злочинами у міжнародному співтоваристві та в Україні. Так, законом «Про ратифікацію Конвенції про кіберзлочинність» від 07 вересня 2005 року Україна ратифікувала Конвенцію про кіберзлочинність Ради Європи від 23 листопада 2001 року та Додатковий протокол до неї від 28.01.2003 і таким чином імплементувала положення міжнародного акта у вітчизняне законодавство. Однак у самій Конвенції та Додатковому протоколі до неї не міститься визначення поняття «кібератака», лише надається перелік діянь – правопорушень у кіберпросторі, за які на національному рівні пропонується встановити кримінальну відповідальність, та наводиться їх умовна класифікація.

У деяких країнах є приклади віднесення злочинних дій у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж до злочинів, які посягають на безпеку держави.

Так, у Кримінальному кодексі Грузії у главі XXXVIII «Тероризм» наявна стаття 324-1 «Кібертероризм», в якій зазначено, що кібертероризм – це протиправне заволодіння захищеною законом комп'ютерною інформацією, її використання чи загроза використання, що створює небезпеку настання тяжких наслідків та здійснене з метою залякування населення чи впливу на орган влади.

У Пенітенціарному кодексі Естонії, в розділі 3 «Винні діяння проти державної влади», міститься ст. 237 «Терористичний злочин», згідно з якою до *терористичного злочину* віднесено злочини, спрямовані проти міжнародної безпеки, проти особи, які містить загрозу життю та здоров'ю людини, злочини проти навколишнього середовища, злочини, спрямовані проти іноземної держави чи міжнародної організації, чи загально небезпечні діяння, виробництво, розповсюдження чи використання забороненої зброї, незаконне захоплення майна, пошкодження чи знищення майна в значних розмірах чи *втручання в комп'ютерні дані чи перешкоджання функціонуванню комп'ютерної системи, а також загрозу скоєння вказаних діянь, якщо вони здійснені з метою спонукати державу чи міжнародну організацію здійснити чи не здійснити які-небудь дії або серйозно порушити чи знищити систему політичного, конституційного, економічного чи суспільного устрою держави,* чи серйозно порушити чи знищити діяльність міжнародної організації, чи серйозно залякати населення.

Кримінальний кодекс Федеративної Республіки Німеччина у главі 3 «Створення небезпеки для демократичної правової держави» містить злочин, передбачений параграфом 88 «Саботаж, спрямований проти конституційних основ», в якому зазначено:

«Той, хто є керівником чи підбурювачем групи осіб, чи діє у складі групи осіб чи в її інтересах одноосібно і навмисно сприяє тому,

що у просторі дії даного закону за допомогою дезорганізуючих дій повністю чи частково *виводяться із ладу чи позбавляються можливості використання за призначенням:*

1. корпорації чи установки, які служать суспільному забезпеченню поштовими послугами чи громадського транспорту;

2. телекомунікаційних установок, які служать громадським цілям;

3.корпорації чи установки, які служать громадському забезпеченню водою, світлом, теплом чи енергією або іншим життєво важливим ресурсом для постачання населенню, чи

4.службових приміщень, установки, пристроїв чи предметів, які повністю або переважно служать цілям громадської безпеки чи порядку, і *тим самим навмисно підтримує прагнення, спрямовані проти стабільності чи безпеки Федеративної Республіки Німеччина чи проти її конституційних основ*».

У Кримінальному кодексі України наявний розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», а саме: ст. 361, ст. 361.1., ст. 361.2., ст. 362, ст. 363, ст. 363.1.

Дані злочини посягають на встановлений у суспільстві порядок інформаційних відносин і скоюються з використанням електронно-обчислювальних машин, тобто комп'ютерів, систем та комп'ютерних мереж. Об'єктом злочину зазначених правопорушень виступають інформаційні відносини у суспільстві, що охороняються законом, а предметом – електронно-обчислювальні машини (комп'ютери), системи і комп'ютерні мережі, а також комп'ютерна інформація, що обробляється за їх допомогою.

За змістом, характером, об'єктом посягання, суб'єктом, суб'єктивною стороною, мотивом та метою кібернетична атака має ознаки злочину «диверсія», передбаченого ст. 113 КК України.

Стаття 113 КК України визначає диверсію як вчинення з метою ослаблення держави вибухів, підпалів або інших дій, спрямованих на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, на зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення, а також вчинення з тією самою метою дій, спрямованих на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій.

Основний безпосередній об'єкт диверсії – безпека держави в економічній, екологічній, воєнній або в будь-якій іншій сфері відповідно до спрямованості конкретного акту диверсії.

Крім цього, для диверсії характерним є обов'язковий додатковий об'єкт, який має різний зміст у різних формах цього злочину: це життя і здоров'я особи, власність, навколишнє середовище. Предметом диверсії можуть бути: будівлі, споруди та інші об'єкти, які мають важливе народногосподарське чи оборонне значення, від діяльності яких залежить життєдіяльність певних регіонів чи інших великих територій, належне функціонування певних галузей економіки, структур державного управління (електростанції, нафтопродуктопроводи, мости, дамби, греблі, системи інформаційних комунікацій, вокзали, аеропорти, морські чи річкові порти, метрополітени, підприємства з виробництва грошових знаків України чи інші важливі підприємства, незалежно від форми власності, військові частини тощо), у тому числі підприємства, зруйнування чи пошкодження яких саме по собі є фактором небезпеки (хімічні, біологічні підприємства, підприємства з виготовлення вибухових матеріалів і виробів, пожежонебезпечні виробництва чи сховища тощо); сільськогосподарські об'єкти та виробництва, що мають велике значення в житті окремих регіонів і країни.

Об'єктом кібернетичної атаки є така складова частина національної безпеки держави, як інформаційна безпека. Обов'язковим додатковим об'єктом є інформаційні відносини у суспільстві, що охороняються законом.

Об'єктивна сторона диверсії згідно зі ст. 113 КК проявляється в семи формах, кожна з яких передбачає вчинення суспільно небезпечних дій (зокрема, вибухів і підпалів), спрямованих на: 1) масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому 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.

Деякі науковці схиляються до думки, що диверсія з використанням комп'ютерних мереж та систем (комп'ютерів) є окремою формою диверсії.

Так, на думку О. А. Чувакова, кібердиверсія є особливим видом диверсії (диверсії по відношенню до комп'ютерів та комп'ютерних мереж), а способи здійснення комп'ютерних злочинів доцільно підрозділяти на три групи: способи безпосереднього доступу до комп'ютерної інформації' способи віддаленого доступу до комп'ютерної інформації' способи розповсюдження технічних носіїв інформації, які вміщують шкідливі програми для ЕОМ [10, с. 376].

А. А. Васильєв та Д. В. Пашнєв зазначають, що знищення певної надзвичайно важливої для обороноздатності країни коп'ютерної інформації з метою ослаблення держави шляхом несанкціонованого втручання, яке спричинило істотну шкоду, є диверсією і повинно кваліфікуватись лише за ст. 113 КК України та не належить до злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [11, с. 40].

Автор підтримує погляди вищеназваних науковців та вважає, що кібернетичну атаку доцільно віднести до об'єктивної сторони диверсії, доповнивши диверсію такою формою її здійснення: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж, розповсюдження або збут шкідливих програмних чи технічних засобів.

Суб'єкт диверсії – фізична осудна особа, що досягла 14-річного віку.

Суб'єктивна сторона диверсії характеризується прямим умислом.

За суб'єктом і суб'єктивною стороною кібернетична атака збігається з диверсією. Справді, враховуючи соціальну небезпеку злочину, вік кримінальної відповідальності доцільно встановити із 14 років, а умисел щодо вчинення організованої кібернетичної атаки може бути лише прямим.

Мотиви диверсії можуть бути різними (помста, користь, політична ненависть до існуючого конституційного ладу тощо). Обов'язковою ознакою суб'єктивної сторони диверсії є мета – ослаблення держави. Саме за ознакою спеціальної мети (не беручи до уваги деякі інші ознаки) диверсію треба відмежовувати від таких суміжних умисних злочинів, як, наприклад, умисне вбивство двох чи більше осіб або вбивство способом, небезпечним для життя багатьох осіб, терористичний акт, екоцид тощо.

Метою останньої масованої кібернетичної атаки також є ослаблення обороноздатності та нормального функціонування держави Україна. Мотиви кібернетичної атаки можуть бути аналогічними мотивам диверсії, тобто помста, користь, політична ненависть до існуючого конституційного ладу тощо.

За результатами аналізу кібернетична атака має всі ознаки злочину – диверсії. Наявні всі фактори соціальної зумовленості криміналізації кібернетичних атак, вчинених з метою ослаблення держави: мета – забезпечення безпеки держави в різних її сферах, статистичні, правові, політичні.

**Висновки**

Таким чином, для комплексного кримінально-правового захисту інтересів національної безпеки необхідно криміналізувати кібернетичну атаку, яка посягає на безпеку держави, та віднести дане діяння до складу злочину – диверсії.

На підставі викладеного автор пропонує доповнити статтю 113 Кримінального кодексу України «Диверсія», а саме:

«Стаття 113. Диверсія

Вчинення з метою ослаблення держави вибухів, підпалів або інших дій, спрямованих на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, на зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення, а також вчинення з тією самою метою дій, спрямованих на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій, *а також вчинення з тією самою метою несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж, розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів) автоматизованих систем, комп'ютерних мереж».*

Прийняття таких поправок до кримінального закону дозволить кваліфікувати кібернетичну атаку, вчинену з метою ослабити безпеку держави, як диверсію, що відповідає справжній сутності таких злочинних дій.

**Список використаних джерел:**

1. Шеломенцев В. П. Поняття та сутність кібернетичної атаки / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К.: Науково-практичний журнал. – 2011. – № 25. – С. 338-344.

2. Шатун В. Т. Інформаційна безпека – невід'ємна складова національної безпеки України / В. Т. Шатун, О. В. Гладун // Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія». – 2016. – Т. 267. – Вип. 255. – С. 174-180. – (Серія: Державне управління).

3. Корнейко О. Застосування та визначення терміна «інформаційна безпека» в національному законодавстві / О. Корнейко, С. Корнейко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Науково-технічний збірник, 2009. – Вип. 2(19). – С. 9-13.

4. Фріс П. Л. Криміналізація і декриміналізація у кримінально-правовій політиці / П. Л. Фріс // Вісник Асоціації кримінального права України. – 2014. – № 1(2). – С. 19-28.

5. Політова А. С. Соціальна обумовленість криміналізації злочину, передбаченого ст. 203-2 КК України щодо зайняття гральним бізнесом / А. С. Політова. – Науковий вісник Міжнародного гуманітарного університету. – 2013. – Вип. 6-2(2). – С. 95-98. – 9 Серія: Юриспруденція).

6. Кримінальне право України: Загальна частина : підручник / М. І. Бажанов. – К.: Юрінком Інтер, 2005. – 480с.

7. Тоболкин П. С. Социальная обусловленность уголовно-правовых норм. – Свердловск: Средне-Урал книга, 1983. – 176 с.

8. Брич Л. П. Кримінально-правова кваліфікація ухилення від оподаткування в Україні : монографія / Л. П. Брич. – К: Аттіка, 2000. – 258 с.

9. Мицкевич А. Ф. Уголовное наказание: понятие, цели и механизмы действия. – СПб: Юрид. Центр Пресс, 2005. – 329 с.

10. Чуваков О. А. Деякі види диверсійних актів у сучасних умовах / О. А. Чуваков // Актуальні проблеми політики : Збірник наукових праць. – Одеса, 2010. – Вип. 39. – С. 372-378.

11. Васильєв А. А. Особливості кваліфікації злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку / А. А. Васильєв, Д. В. Пашнев // Вісник Кримінологічної асоціації України. – 2013. – № 5. – С. 34-42.

*Статья посвящена определению факторов социальной обусловленности криминализации кибернетических атак и внесению изменений в Уголовный кодекс с целью отнести такое деяние, как кибернетическая атака, к составу преступления «диверсия», предусмотренного ст. 113 УК.*

**Ключевые слова:** социальная обусловленность, криминализация, основания криминализации, кибернетическая атака, информационная безопасность, национальна безопасность, диверсия.

*The article is devoted to determination of factors of social conditionality of criminalization of cybernetic attacks and introduction of amendments to the Criminal Code of Ukraine in order to attribute such an act as a cybernetic attack to the crime of „sabotage" stipulated by art. 113 of the Criminal Code.*

**Key words:** social conditionality, criminalization, basis of criminalization, cybernetic attack, information security, national security, sabotage.