УДК 342.9:342.352
DOI https://doi.org/10.32782/klj/2023.4.17

Рощина І. О.,
кандидат юридичних наук, доцент,
професор кафедри публічного та міжнародного права
Київського національного економічного університету
імені Вадима Гетьмана

Кришевич О. В.,
кандидат юридичних наук, професор,
професор кафедри кримінального права
Національної академії внутрішніх справ

КРИМІНАЛЬНО-ПРАВОВА ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ ЯК ОДИН ІЗ ЕЛЕМЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Анотація. В статті досліджуються питання пов'язані з вчиненням кримінальних правопорушень в сфері інформаційних відносин, розглядається досвід міжнародного законодавства у кримінально-правової протидії кіберзлочинності.

Інформаційні та телекомунікаційні технології стали невід'ємною частиною сучасного світу, і разом з їх широким використанням зростає і загроза кіберзлочинності. Так, кіберзлочинність стала актуальним явищем для багатьох країн, у тому числі й для України. У кіберпросторі розглядаються різноманітні злочини, такі як кібератаки, крадіжка особистої інформації, фішинг, вірусні атаки, атаки на критичну інфраструктуру та багато інших. Україна, як і багато інших країн, проводить заходи для боротьби з кіберзлочинністю. Це включає вдосконалення законодавства, розробку заходів з кіберзахисту, підвищення кваліфікації фахівців у сфері кіберзахисту та співпрацю з міжнародними партнерами для обміну інформацією та взаємодії в області кіберзахисту. Питання посилення кримінальної відповідальності за кримінальні правопорушення у сфері інформаційних технологій є актуальним у зв'язку зі зростанням кількості кіберзлочинів та зловживань у цій сфері. Розвиток технологій відкриває нові можливості для злочинців, і правова система повинна адаптуватися, щоб забезпечити ефективний захист від таких злочинців. Тому, однією з причин посилення кримінальної відповідальності є необхідність відповідати за вчинення кіберзлочинів, які можуть завдати серйозної шкоди інформаційним системам, економіці, а також приватним особам. Для зменшення масштабів кіберзлочинності та встановлення ефективної національної протидії кіберзлочинності в міжнародній політиці кіберпростору держави можуть використовувати різні стратегії та механізми. Також, держави повинні розробляти та вдосконалювати законодавство, спрямоване на кіберзлочини. Це повинно включати судові санкції та відповідальність за кіберзлочини, а також прозорі та чіткі процедури для розслідування та притягнення винних до відповідальності.

Крім того, світова спільнота активно працює над розробкою стандартів і міжнародної співпраці для ефективного протидії кіберзлочинності. Забезпечення кібербезпеки стає завданням для країни в сучасному інформаційному суспільстві.

Ключові слова: *інформаційні та телекомунікаційні технології, кіберзлочинність, норми кримінального права, інформаційна безпека, протидії кіберзлочинності.*

Roshchina I. O., Kryshevych O. V. Criminal-legal combat cybercrime as one of the elements of information security in Ukraine

Abstract. The article examines issues related to the commission of criminal offenses in the field of information relations, considers the experience of international legislation in the criminal-legal counteraction of cybercrime as one of the elements of information security in Ukraine.

Information and telecommunication technologies have become an integral part of the modern world, and along with their widespread use, the threat of cybercrime is also growing. Thus, cybercrime has become an actual phenomenon for many countries, including Ukraine. Cyberspace deals with various crimes such as cyber attacks, identity theft, phishing, virus attacks, attacks on critical infrastructure and many others.

Ukraine, like many other countries, is taking measures to combat cybercrime. This includes improving legislation, developing cyber security measures, improving the skills of cyber security specialists and cooperating with international partners to exchange information and interact in the field of cyber security. The

issue of strengthening criminal liability for criminal offenses in the field of information technology is relevant in connection with the increase in the number of cybercrimes and abuses in this field.

Advances in technology present new opportunities for criminals, and the legal system must adapt to provide effective protection against such criminals. Therefore, one of the reasons for the strengthening of criminal responsibility is the need to be responsible for the commission of cybercrimes, which can cause serious damage to information systems, the economy, as well as private individuals.

States can use various strategies and mechanisms to reduce the scale of cybercrime and establish an effective national response to cybercrime in international cyberspace policy. States should develop and improve legislation targeting cybercrime. This should include judicial sanctions and accountability for cybercrime, as well as transparent and clear procedures for investigating and prosecuting perpetrators.

In addition, the global community is actively working on the development of standards and international cooperation to effectively combat cybercrime. Ensuring cyber security becomes a task for the country in the modern information society.

Key words: *information and telecommunication technologies, cybercrime, norms of criminal law, information security, countermeasures against cybercrime.*

Постановка проблеми. Впровадження інтернет-технологій в сферу повсякденного життя суттєво змінило спосіб функціонування суспільства. Інтернет грає важливу роль у полегшенні комунікації між людьми. Електронна пошта, соціальні мережі, відеодзвінки та миттєве спілкування дозволяють легко обмінюватися повідомленнями навіть у великому просторі. Державні органи, органи місцевого самоврядування та підприємства використовують інтернет-технології для покращення управління, моніторингу та звітності. Це може сприяти більш ефективному вирішенню різних завдань, включаючи соціальні, економічні та екологічні питання. Застосування електронних державних документів дозволяє швидко і безпечно обмінюватися інформацією між установами, приватними компаніями та громадянами. Це ефективність роботи, яка зменшує бюрократичні бар'єри. Загалом, інтернет-технології впливають на різні сфери життя, роблячи їх більш доступними, ефективними та зручними для користувачів. Однак, разом з перевагами, важливо також вирішити питання безпеки та етики використання цих технологій.

Проте в процесі науково-технічного прогресу та активного впровадження інтернет-технологій у всі сфери життєдіяльності суспільства, розвивається й злочинність.

Особливо це питання є актуальним сьогодні в Україні, адже в умовах воєнного стану кіберзлочинців активно залучають до зламу урядових серверів, дезінформування населення, використання при цьому фейкових профілів у соцмережах тощо. Поширеним на сьогодні є кібершахрайство, при якому злочинці під виглядом різноманітних виплат мають намір дізнатися банківські реквізити громадян з метою заволодіння коштами [1, с. 83].

Аналіз останніх досліджень і публікацій. Аналіз джерел і публікацій свідчить, що питання боротьби з кіберзлочинністю досліджують фахівці різних галузей науки, які пропонують шляхи протидії цьому негативному явищу.

Зазначеним питанням приділяли увагу такі дослідники як О.М. Бандурка, В.В. Голіна, Б.М. Головкін, А.П. Закалюк, О.М. Литвинов, В.В. Марков, М.І. Сащенко, В.І. Трапезніков, В.О. Туляков, І.В. Жук, О.М. Бодунова, та інші. Проте проблема запобігання кримінальним правопорушенням у сфері інформаційних технологій є такою, що не знайшла достатнього наукового аналізу та вивчення і тому потребує подальшої наукової розробки цієї проблематики.

Виклад основного матеріала дослідження. Активний розвиток кібертехнологій в останні роки сприяє вчиненню злочинів онлайн та у сфері інформаційних технологій. Інформаційний злочин (Information crime) – незаконні дії спрямовані на розкрадання або руйнування інформації в інформаційних системах і мережах, які виходять з корисливих або хуліганських спонукань. До основних видів кіберзлочинності можна віднести такі: розповсюдження шкідливого програмного забезпечення, крадіжка номерів кредитних карт і банківських рахунків, злом паролів, порушення авторських прав [2].

Характерними особливостями кримінальних правопорушень у сфері інформаційно-телекомунікаційних технологій є:

– необхідність широкого застосування спеціальних знань при виявленні та фіксації слідів кримінальних правопорушень в електронній формі;

– організованість та транскордонність (широкі міжрегіональні та міжнародні зв'язки);

– висока латентність, спричинена небажанням приватного сектора інформувати про такі кримінальні правопорушення через недовіру до потенційних можливостей правоохоронних органів та небажанням визнати слабкі місця своїх систем безпеки;

– високий рівень технічного забезпечення правопорушників [3, с. 108].

Необхідно констатувати, у теорії відсутня загальноприйнята правова дефініція досліджуваного поняття. Так, на доктринальному рівні можна зустріти низку аналогічних однорідних понять, зокрема: злочини, які вчиняються з використанням електронно-обчислювальної машин (ЕОМ), «комп'ютерний злочин», «злочин у сфері високих технологій», «комунікаційний злочин», «кіберзлочин», «злочин у сфері комп'ютерної інформації», «мережевий злочин» тощо. Зарубіжними дослідниками частіше вживаються поняття "high-tech crime", "cyber crime", "network crime", які, відповідно, перекладаються як «злочини у сфері високих технологій», «кіберзлочини», «злочини в комп'ютерних мережах» [4, с. 120].

Розвиток кіберзлочинності був обумовлений зростанням комп'ютеризації суспільства та широким впровадженням інформаційних технологій у різні сфери життя. Перші випадки комп'ютерних злочинів можна відзначити в 1970-х роках, коли почали з'являтися перші віруси та інші види кібернетичних загроз.

Термін «кіберзлочинність» був запропонований для визначення злочинів, пов'язаних з використанням комп'ютерних технологій, які стали актуальними з розвитком інформаційних технологій.

Поняття кіберзлочинності як сукупності злочинів поширюється на всі види злочинів, скоєних в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати (бути) предметом (метою) злочинних посягань, середовищем, в якому відбуваються правопорушення, і засобом або знаряддям злочину [4, с. 119].

Україна останніми роками дедалі більше відчуває на собі масштаби кібернетичних атак та їх негативні наслідки. Так, кількість кримінальних правопорушень у сфері інформаційних технологій постійно зростає. Зокрема, з огляду статистичних даних Генеральної прокуратури України випливає, що станом на 31 грудня 2022 року обліковано у звітному періоді 3 415 кримінальних правопорушень у сфері інформаційних технологій, що на 105 кримінальних правопорушень більше порівняно з 2021 роком та на 917 – більше порівняно з 2020 роком. Це свідчить в цілому про суттєве зростання, а саме – на 3,1% порівняно з 2021 роком та – на 26,8% порівняно з 2020 роком, кількості зареєстрованих кримінальних правопорушень [5].

Згідно аналітичних даних Департаменту кіберполіції у 2022 році припинено діяльність 23 організованих груп і злочинних організацій, що діяли в кіберпросторі. До складу зазначених угруповань входив 81 учасник (23 – організаторів та 51 – активний виконавець), якими вчинено 269 кримінальних правопорушень (у тому числі 240 тяжких та особливо тяжких), з яких: 178 – шахрайств, 59 – у сфері використання електронно-обчислювальних машин, 12 – у сфері обігу наркотичних засобів, 3 – за ст. 255 (Створення, керівництво злочинною спільнотою, а також участь у ній) Кримінального кодексу України, 2 – крадіжок, 3 – у сфері господарській діяльності (легалізації (відмиванню) майна, одержаних злочинним шляхом), 1 – привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем [6].

Також, протягом 2022 року, фахівці Держспецзв'язку зареєстрували в Україні понад 2 тисячі кіберінцидентів та ще більшу кількість кібератак. Зокрема, йдеться про кіберінциденти, які стаються в мережах органів державної влади, фінансових установах, логістичних компаніях, критичній інфраструктурі, енергетичному секторі, телерадіокомунікаційних компаніях, медіа та інших галузях [7].

Рівень латентності кіберзлочинів в Україні становить близько 95%, що дає змогу віднести їх до категорії високолатентних [8, с. 402].

За оцінками експертів, латентність «комп'ютерних злочинів» у США сягає 80%, у Великобританії – 85%, у Німеччині – 75%. За даними Symantec Security, міжнародної служби захисту від кіберзагроз, 12 людей у всьому світі стають жертвами кібератак щосекунди, і щороку в усьому світі реєструється близько 556 мільйонів кіберзлочинів, збитки від яких складають понад 100 мільярдів доларів США [9, с. 46].

Так, на сучасному етапі кіберпростір став ключовою ареною для різноманітних геополітичних, економічних та військових змагань. Багато країн визнають важливість кібербезпеки та кібервійських можливостей, і тому інвестують у створення та розвиток відповідних структур.

Провідні активні країни формують кібервійськові підрозділи та центри з кібербезпеки. Ці організації призначені для захисту власної кіберінфраструктури, а також для здійснення кібероперацій у випадках потреби. Завдання таких підрозділів включає в себе самодіяльність та протидію кіберзагрозам, виконання кібершпігунства, а також реагування на кібератаки.

Деякі країни також сприяють розвитку кіберзброї та кіберздатності своїх збройних сил. Це може включати в себе створення спеціальних військових частин, призначених для проведення операцій у кіберпросторі, розробку атакуючих та захисних кіберзасобів, а також навчання військових фахівців у галузі кібербезпеки.

Загальний тренд полягає в тому, що країни розуміють важливість кіберпростору як стратегічного ресурсу і містять ресурси для забезпечення своєї кібербезпеки та розвитку кібервійських можливостей.

Так, у США, крім уже діючого Центру національної кібербезпеки (National Cyber Security Center), було сформовано Об'єднане кіберкомандування (Unified US Cyber Command) у складі збройних сил, яке на глобальному рівні має координувати зусилля всіх структур Пентагону під час бойових дій, надавати відповідну підтримку цивільним федеральним установам, а також взаємодіяти з аналогічними за завданнями відомствами інших. Водночас ці організації є частково підконтрольними відомствами, оскільки вищим керівним органом є Рада національної безпеки зі спеціальним 60 комітетом, до сфери відповідальності якого входить реалізація інформаційної стратегії, у тому числі боротьба з кіберзлочинністю. У Великій Британії реалізуються програми зі створення кіберзброї, щоб забезпечити стійкість уряду проти зростаючих кіберзагроз. В Австралії створено координаційну групу безпеки електронної пошти (ESCG). Основним завданням цієї групи є створення надійного електронного робочого простору як для державного, так і для приватного секторів [9, с. 46].

Україна, розуміючі небезпеку кіберзлочинності, 7 вересня 2005 року Україна ратифікувала Конвенцію про кіберзлочинність, підписану від імені України 23 листопада 2001 року в м. Будапешті, яка стала основою для гармонізації національного законодавства у сфері кіберпростору. У преамбулі цієї Конвенції вказано, що вона «є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва».

Конвенцією також запроваджено певний поділ кіберзлочинів на такі види:

1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем.

2. Правопорушення, пов'язані з комп'ютерами.

3. Правопорушення, пов'язані зі змістом.

4. Правопорушення, пов'язані з порушенням авторських і суміжних прав [10].

У березні 2016 року уряд прийняв Стратегію кібербезпеки України, яка має на меті

створення національної системи кібербезпеки. У червні 2016 року Президент України підписав Указ про створення Національного координаційного центру кібербезпеки [2].

У 2017 р. було прийнято Закон «Про основні засади забезпечення кібербезпеки України». Цей закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [11].

В Україні сфера інформаційних технологій посідає одне з найважливіших місць в економіці держави, а наші ІТ-фахівці є одними з найбажаніших у цій сфері та працюють по всьому світі в різноманітних компаніях і державних органах.

Однак, на жаль, нормативне регулювання цієї сфери в Україні не встигає за розвитком технологій, що загострює проблему кіберзлочинності. На рівні фізичних осіб кіберзлочинність пов'язана з використанням піратського програмного забезпечення: зловмисники можуть отримати доступ до персональних даних користувача [12].

В даний час у Кримінальному кодексі України (далі КК України) ці кримінальні правопорушення закріплені в розд. XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» і представлено такими нормами:

– ст. 361 – несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж;

– ст. 361-1 – створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;

– ст. 361-2 – несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

– ст. 362 – несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;

– ст. 363 – порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється;

– ст. 363-1 – перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку [13].

З аналізу назви вищезгаданих статей видно, що вони досить повно охоплюють усі проблеми та напрямки боротьби у сфері інформаційних технологій. У той же час аналіз санкцій цих статей свідчить про те, що заходи покарання не тільки не сприяють боротьбі у сфері інформаційних технологій, а навпаки, створюють впевненість і можливість правопорушнику знову вчиняти подібні кримінальні правопорушення. Наприклад, ст. 361 КК України має шість частин. Частина перша визначає такі заходи покарання:

1. Штраф від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян.

2. Обмеження волі на строк до трьох років.

Ці незначні заходи покарання за досить небезпечні для держави кримінальні правопорушення явно не відповідають і не сприяють боротьбі з ними.

Необхідність у посиленні кримінальної відповідальності за кримінальні правопорушення у сфері інформаційних технологій назріла давно. Посилення санкцій та додаткова криміналізація окремих діянь здатні частково стримати потенційних злочинців від вчинення нових кримінальних проавопорушень. Норми кримінального права поввинні

служити тим цілям, які чітко і однозначно випливають із ст. 3 Конституції і викладені в ч. 1 ст. 1 КК України. Якщо цього не відбувається, то суспільство не підтримує такі норми, а отже вони виявляються неефективними і не мають профілактичного ефекту. Тому, з метою підвищення ефективності норм кримінального права у попередженні кримінальних правопорушень у сфері інформаційних технологій, на нашу думку, необхідно заходи покарання статті 361 КК України викласти у наступній редакції:

Частина 1 – карається позбавленням волі на строк від трьох до п'яти від п'яти до семи років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Частина 2 – від п'яти до семи, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Частина 3 – караються позбавленням волі на строк від семи до десяти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

Частина 4 – караються позбавленням волі на строк від десяти до дванадцяти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

Частина 5 – караються позбавленням волі на строк від дванадцяти до п'ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Необхідність у посиленні кримінальної відповідальності за кримінальні правопорушення у сфері інформаційних технологій назріла давно. Посилення санкцій та додаткова криміналізація окремих діянь здатні частково стримати потенційних злочинців від вчинення нових кримінальних проавопорушень.

Тут слід зазначити, що міра покарання «позбавлення волі» або «обмеження волі», що застосовується в КК України, взагалі не піддається ніякому розумінню та поясненню. Як суд може позбавити чи обмежити волі людини.

Поняття терміна «воля» у філософській, психологічній і юридичній літературі тлумачаться по різному. На нашу думку, найбільш вдалим і науково обґрунтованим є визначення поняття «воля», подане в українському радянському енциклопедичному словнику: «Воля — складний психічний процес, що виявляється в активному прагненні людини досягнути свідомо наміченої мети, в регулюванні труднощів. Вольові дії відрізняються від мимовільних (імпульсивних, інстинктивних) тим, що вони є усвідомленими й цілеспрямованими. Воля у людини виникла і розвинулась історично, у процесі праці й суспільної діяльності. Воля є функцією мозку, однією з форм активного відображення рельної діяльності» [14, с. 336].

На нашу думку, найбільш вдалим і науково обґрунтованим є визначення терміна «свобода», подане в юридичній енциклопедії, виданій в Україні. А саме: поняття «свобода» у широкому філософському розумінні — природний стан народу або окремої людини, який характеризується можливістю діяти на власний розсуд. У вузькому розумінні — суб'єктивна можливість людини й громадянина.здійснювати або не здійснювати певні дії, що ґрунтуються на його конституційних правах і свободах. Основні постулати вчення про свободу: усі люди вільні від народження і ніхто не має права відчужувати їхні природні права [15, с. 441].

Характерно, що у Конституції України, коли йдеться про арешт, тримання під вартою, вибір місця проживання або вільне вираження своїх поглядів і переконань, то вживається слово «свобода», а не «воля». Так, у ст. 29 Конституції України зазначено, що кожна людина має право на свободу та особисту недоторканність. Ніхто не може бути заарештований або триматися під вартою інакше, як за вмотивованим рішенням суду і тільки на підставах та в порядку, встановлених законом. У статті 33 Конституції України також використовується слово «свобода» в такому поєднанні: кожному, хто на законних підставах перебуває на території України, гарантується свобода пересування, вільний вибір місця проживання, право вільно залишати територію Україні,

за винятком обмежень, які встановлюються законом. Аналізуючи викладені вище статті Конституції України про права і свободи людини, слід зазначити, що в жодній із них замість терміна «свобода» не вживається термін «воля».

У цьому сенсі характерно, що розділ 2 Конституції України має назву «Права, свободи та обов'язки людини і громадянина», без вживання терміна «воля». Отже, в Конституції України правильно і науково обґрунтовано використовується термін «свобода».

Висновки. Підбиваючи підсумок аналізу термінів «воля» і «свобода», а також їх використання у Кримінальному кодексі та Конституції України, слід констатувати, що термін «воля» у КК України використовується абсолютно неправильно. Адже застосовуючи до людини міру покарання за скоєння злочину, держава обмежує її лише у свободі місця знаходження, спілкуванні з рідними, виборі своїх дій тощо, але не позбавляє її волі, тобто функції мозку. Тому необхідно у КК України термін «воля» замінити на термін «свобода».

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Бодунова О. М. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні. *Науковий вісник Ужгородського університету: серія: Право* / голов. ред. Ю. М. Бисага. Ужгород: Видавничий дім «Гельветика», 2023. Т.2. Вип. 75. С. 83–87. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/276140/271014

2. Інформаційні злочини. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96_%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%B8

3. Марков В.В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і Безпека*. 2015. № 2. С. 107–113. URL: https://core.ac.uk/reader/187222390

4. Шемчук В.В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : *Юридичні науки*. 2018. Т. 29 (68), № 6. С. 119–124. URL: https://www.juris.vernadskyjournals.in.ua/journals/2018/6_2018/23.pdf

5. Кіберзлочинність: виклики часу. URL: https://law.chnu.edu.ua/kiberzlochynnist-vyklyky-chasu/

6. Звіт про результати роботи Департаменту кіберполіції у 2022 році. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--roczi-969/

7. У 2022 році в Україні зареєстрували 2194 кіберінциденти — Держспецзв'язку. URL: https://suspilne.media/397220-u-2022-roci-v-ukraini-zareestruvali-2194-kiberincidenti-derzspeczvazku/

8. Харитоненко І.О. Феномен кіберзлочинності в сучасній кримінологічній теорії. *Часопис Київського університету права*. 2020. № 4. С. 401–404. URL: https://chasprava.com.ua/index.php/journal/article/view/601

9. Лисько Т. Д., Меланіч В. В., Славіта Ю. В. Протидія кіберзлочинності: сучасний стан вітчизняного законодавства та досвід зарубіжних країн. URL: https://web.archive.org/web/20230216083315id_/http://apdp.in.ua/v96/4.pdf

10. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text

11. Про основні засади забезпечення кібербезпеки України: Закон України вд 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

12. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL: https://gurt.org.ua/articles/34602/

13. Кримінальний кодекс України від 05 квітня 2001 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр

14. Український радянський енциклопедичний словник. 2-ге вид. К., 1986. Т. 1. 751 с.

15. Юридична енциклопедія. К., 1998. Т. 5. 672 с.