АКТУАЛЬНІ ПИТАННЯ КІБЕРБЕЗПЕКИ В КОНТЕКСТІ СУЧАСНИХ ПРОБЛЕМ ПРАВОЗНАВСТВА

ЗАГУМЕННА Юлія Олександрівна - професор кафедри теорії та історії держави і права Харківського національного університету внутрішніх справ, кандидат юридичних наук, доцент, м. Харків, Україна;
ORCID: https://orcid.org/0000-0003-0617-8363,
УДК 340.1
DOI

У статті проведено комплексне дослідження актуальних питань кібербезпеки в контексті сучасних проблем правознавства. Визначено шляхи вдосконалення правового регулювання боротьби з кіберзлочинністю в Україні. Виявлені тенденції щодо універсалізації підходів законодавців різних країн у напрями боротьби з кіберзлочинністю, у т.ч. як в Україні, так і у США встановлено відповідальність за шахрайство, пов'язане із застосуванням комп'ютерів та комп'ютерних мереж. Запропоновано авторському підході до розуміння поняття «кіберзлочинність». Під ним слід вважати певні протиправні дії, здійснені у кіберпросторі, відповідальність за які встановлено кримінальним законом. До найбільш поширених кіберзлочинів належать: крадіжки грошових коштів з банківських кредитних карток, створення сайтів з дитячою порнографією, комп'ютерні віруси, пропаганда расової нетертимості, інструкції з виготовлення саморобних вибухових приладів, комп'ютерні атаки на мережі органів державної влади, на військові, космічні комп'ютерні системи, промислове шпигунство, використання компромату в політичних цілях.

Проведено аналіз та виявлення чинників, що ускладнюють ефективне застосування законодавства про кіберзлочини в Україні. Серед них ключовою є складність притягнення до кримінальної відповідальності в Україні осіб, які скоїли кіберзлочини з-за кордону. Тому нагальною проблемою є організація міжнародно-правового співробітництва у пошуку та притягненні до кримінальної відповідальності осіб, що скоїли злочини за межами юрисдикції країни вчинення злочинних дій;

Подальшому розвитку напрацьованого вітчизняною аналітичною юриспруденцією наукового положення про те, що поняття «сфера правового регулювання суспільних відносин» має включати в т.ч. національний сегмент усесвітньої комп'ютерної мережі «Internet», який упорядковується органами держаної влади певної країни. Вдосконалено наукове твердження про те, що аналіз боротьби з кіберзлочинністю засвідчує те, що програмне забезпечення (цифровий продукт), що використовується правоохоронними органами у сфері боротьби з кіберзлочинністю, у т.ч. під час профілактичних заходів у вигляді обмеження або заборони доступу до тієї чи іншої інформації протиправного характеру, яка розміщена на сайтах, слід розглядати як якісно новий вид державного примусу.

Ключові слова: кіберзлочинність, боротьба з кіберзлочинністю, кібербезпека, пандемія COVID-19, національна безпека, інформаційна безпека.

Постановка проблеми

Актуальність досліджуваної тематики обумовлена необхідністю подальшого розвитку вітчизняної доктрини щодо правового регулювання інформаційних відносин та потребою у всебічному з'ясуванні можливостей юридичного впливу з боку держави на нове технологічне та людське середовище, яким є віртуальний простір.

Сьогодні неможливо не визнати той факт, що неухильний розвиток науково-технічного прогресу, який виявляється у всеосяжній цифровізації суспільного життя, об'єктивно диктує необхідність удосконалення засад правового регулювання боротьби з кіберзлочинністю, адже на сьогодні чинна вітчизняна нормативно-правова база у сфері протидії злочинам у кіберпросторі лише частково задовольняє потреби часу та не завжди охоплює всі ключові елементи, які необхідні для ефективної протидії кіберзлочинам всіх рівнів складності. Невипадково одним із пріоритетних напрямків Стратегії національної безпеки України, затвердженої Указом Президента від 14 вересня 2020 року, визначено посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі.

Загострення проблеми кіберзлочинності є актуальною соціальною проблемою, що породжує нові виклики, котрі в цілому стоять як перед суспільством, так і перед правом, адже наслідки злочинності у цифровому середовищі людство не може оперативно та одномоментно долати, через швидкий розвиток інформаційно-комунікаційних технологій, стрімку інновацію мобільних та комп'ютерних пристроїв, додатків, програмного забезпечення, низький рівень освіченості більшості людей у питаннях захисту власних інформаційно-комунікаційних пристроїв, неспроможність багатьох держав світу вести ефективну та стабільну політику захисту власних державних інформаційних ресурсів тощо. Однак, серед представлених вище факторів у 2020 році з'явився новий, найбільш актуальний каталізатор розвитку кіберзлочинності в 21-ому столітті – фактор пандемії COVID-19.

Світова пандемія коронавірусу змістила пріоритети політики різних держав світу, міжнародних організацій та інших організаційних структур на сферу медицини, соціального забезпечення громадян та збереження власної економічної стабільності. Така політика, звичайно, є прекрасною нагодою для розвитку кіберзлочинності на просторах Інтернету, державних та інших важливих стратегічних інформаційних ресурсів багатьох організацій. Адже все людство зараз вимушено перебувати в умовах віддаленої роботи і вчитися жити за її умовами. Саме через це питання захисту від кібернетичних загроз сьогодні є надважливим аспектом національної безпеки будь-якої країни світу. Актуальність теми кіберзлочинності в умовах пандемії ще пов'язана з тим, що вже багато країн переходять або вже перейшли на системи електронного ведення документообігу, великих баз даних, проведенням важливих робочих зустрічей або комунікацій через різні «месенджери». За таких умов будь-яка інформація, яка існує в умовах кібернетичного простору, може нести загрозу державі, організації, конкретній людині в «руках кіберзлочинців», саме тому аспекти безпеки кіберпростору зараз постійно удосконалюються для унеможливлення розвитку кіберзлочинності у світі. Саме такими сьогодні є перипетії навколо системи кіберпростору та паралельного розвитку кіберзлочинності в умовах пандемії COVID-19.

Науковий дискурс щодо правового регулювання боротьби з кіберзлочинністю знайшов свій прояв у публікаціях Л. В. Борисової, С. А. Буяджи, А. В Войціховського, В. О. Голубєва, В. В.. Маркова, О.В. Манжая, та інших. Незважаючи на значну кількість юридичних наукових доробок, автори яких розглядали різноманітні підходи в означеній сфері, тому тема наукової статті є актуальною та своєчасною.

Метою статті є комплексне опанування актуальних питань кібербезпеки в контексті сучасних проблем правознавства та визначення шляхів удосконалення механізму правового регулювання боротьби із кіберзлочинністю.

Для досягнення поставленої мети були поставлені та послідовно виконані такі **завдання**:

- розглянути історичні етапи розвитку правового регулювання боротьби із кіберзлочинністю;

- з'ясувати специфіку національного правового регулювання боротьби з кіберзлочинністю;

- поглибити напрацьовані вітчизняною юриспруденцією знання праксеологічного характеру щодо розвитку та удосконалення правового регулювання боротьби з кіберзлочинністю в Україні.

Новизна дослідження полягає у формулюванні низки умовиводів як теоретичного, так і практичного характеру, що мають слугувати основою для подальшої боротьби з кіберзлочинністю в Україні, вдосконалення її нормативної та організаційної складової. Це виявляється у:

- виявленні тенденції щодо універсалізації підходів законодавців різних країн у напрями боротьби з кіберзлочинністю, у т.ч. як в Україні, так і у США встановлено відповідальність за шахрайство, пов'язане із застосуванням комп'ютерів та комп'ютерних мереж;

- авторському підході до розуміння поняття «кіберзлочинність». Під ним слід вважати певні протиправні дії, здійснені у кіберпросторі, відповідальність за які встановлено кримінальним законом. До найбільш поширених кіберзлочинів належать: крадіжки грошових коштів з банківських кредитних карток, створення сайтів з дитячою порнографією, комп'ютерні віруси, пропаганда расової нетерпимості, інструкції з виготовлення саморобних вибухових приладів, комп'ютерні атаки на мережі органів державної влади, на військові, космічні комп'ютерні системи, промислове шпигунство, використання компромату в політичних цілях.

- аналізі та виявленні чинників, що ускладнюють ефективне застосування законодавства про кіберзлочини в Україні. Серед них ключовим є складність притягнення до кримінальної відповідальності в Україні осіб, які скоїли кіберзлочини з-за кордону. Тому нагальною проблемою є організація міжнародно-правового співробітництва у пошуку та притягненні до кримінальної відповідальності осіб, що скоїли злочини за межами юрисдикції країни вчинення злочинних дій;

- подальшому розвитку напрацьованого вітчизняною аналітичною юриспруденцією наукового положення про те, що поняття «сфера правового регулювання суспільних відносин» має включати в т.ч. національний сегмент всесвітньої комп'ютерної мережі «Internet», який упорядковується органами держаної влади певної країни;

- подальшому вдосконаленні наукового твердження про те, що аналіз боротьби з кіберзлочинністю засвідчує те, що програмне забезпечення (цифровий продукт), що використовується правоохоронними органами у сфері боротьби з кіберзлочинністю, у т.ч. під час профілактичних заходів у вигляді обмеження або заборони доступу до тієї чи іншої інформації протиправного характеру, яка розміщена на сайтах, слід розглядати як якісно новий вид державного примусу.

Виклад основного матеріалу.

Історичні передумови виникнення і розвитку кіберзлочинності. Будь-яке явище чи процес має свої корені в минулому та через відображення в сьогоденні спрямоване до майбутнього, тобто існує в логіці причинно-наслідкових зв'язків історичного розвитку із сучасністю [1, с. 127].

Протягом усієї історії людства суспільство накопичувало знання і покращувало способи зберігання і обробки інформації. Із входженням суспільства в епоху інформаційних технологій з'явилися нові можливості зберігання і обробки величезних потоків інформації.

Саме кінець XX століття ознаменувався інтенсивним впровадженням інформаційних технологій в економіці, управлінні та, особливо, в кредитно – банківській діяльності, що обумовило виникнення нового класу злочинів – кіберзлочинів, що вчиняються за допомогою комп'ютерних технологій або злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж.

З моменту появи першого персонального комп'ютера та поширення мережі Інтернет злочинці ведуть активну роботу по застосуванню сучасних інформаційних тех-

нологій у своїй протизаконній діяльності. Ця діяльність включає в себе розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення персональної інформації, порушення правил експлуатації автоматизованих електронно-обчислювальних систем, але це далеко не повний перелік подібних злочинів. І з кожним етапом розвитку суспільства розширюється коло протизаконних діянь, що вчиняються у віртуальному просторі.

В історії кіберзлочинності можна виділити кілька етапів розвитку:

І етап. Поширення глобальної мережі Інтернет. На цьому етапі комп'ютерна злочинність ще не розвинена, але все ж відбуваються діяння, які несуть суспільну небезпеку. Так, у серпні 1962р. професор Джон Ліклайдер опублікував свою доповідь під назвою «GalacticNetwork». Автор пророкував появу в майбутньому глобальної мережі, отримати доступ до якої зможе будь-хто і яка з'єднає комп'ютери по всьому світу.

Двома роками пізніше, в 1964 р., Леонард Клейнрок (співробітник Массачусетського технологічного інституту) обґрунтував те, що пакетний обмін даними «комутація пакетів» (передана інформація ділиться на частини пакета і відправляється по різних каналах, щоб у кінці знову з'єднатися в одне ціле) – ця схема є набагато надійніша циклічної комутації каналів, через яку дані передаються суцільним потоком по одному каналу [2, с. 882].

Початковим етапом появи мережі – інтернет, стало створення першої комунікаційної мережі ARPAnet (Advanc edResearchProjectsAgencyNetwork). Роком заснування мережі Arpanet вважають 1969рік. Вона була розроблена компанією «BoltBeranekandNewman» (BBN) на замовлення Агентства передових дослідницьких проектів (ARPA)Міністерства Оборони США з метою створення системи швидкого обміну інформацією між комп'ютерами, а також для відпрацювання методів підтримки зв'язку у випадку ядерного нападу[3, с. 195].

Уже в 1970-х роках з'являються перші комп'ютерні злочинці, яких почали називати «хакерами». Важко точно сказати, хто саме був першим хакером, але в більшості літературних джерел згадується Джон Дрейпер(JohnDraper) як перший професійний кіберзлочинець (також відомий якCap'nCrunch).

Діяльність Джона Дрейпера породила першу спеціалізацію хакерів - фрікери(phreaker), що означає зламування телефонних автоматів і мереж з метою отримання безкоштовних дзвінків. В рядах фрікерів у той час були навіть такі особи, як Стів Возняк (SteveWozniak) та Стів Джобс(SteveJobs), які в майбутньому заснували «AppleComputers». Вони налагодили виробництво пристроїв для злому телефонних мереж у домашніх умовах. І саме цей час можна вважати початком розвитку кіберзлочинності.

Починаючи з 1980-х років, телефонні фрікери починають займатися комп'ютерним хакерством, виникають перші системи електронних дошок оголошень (BBS), попередників груп новин «Usenet» і електронної пошти.

З часом електронні дошки оголошень з такими назвами, як «SherwoodForest» і «Catch-22», стають місцями зустрічей хакерів і фрікерів. Саме на цих платформах відбувається обмін досвідом по крадіжці паролів, номерів кредитних карт. Починають формуватися хакерські групи. Першими були «LegionofDoom» у США і «ChaosComputerClub» у Німеччині.

Взагалі, у 80-х роках починає спостерігатися істотне збільшення числа комп'ютерних атак. Так, якщо в 1988 р. було всього 6 звернень користувачів Інтернет з приводу комп'ютерних атак у центр Інтернет - безпеки CERT, що відкрився в 1988 р., то в 1989 р. - 132, а в 1990 р. - уже 252. Кіберзлочинність перестає бути рідкістю, а Інтернет починає використовуватися для більш широкого кола злочинів. Це стає початком другого етапу в розвитку кіберзлочинності, що характеризується появою нових спеціалізацій Інтернет-злочинців.

II етап. Розповсюдження кіберзлочинності, розширення спеціалізацій кіберзлочинності і груп хакерів.

У 1983 році у прокат виходить фільм «WarGames», який саме і представив субкультуру хакерів широкій громадськості. Це був перший фільм, що розповів про хакарську атаку та її масштаби.

У цьому ж році в США в штаті Мілуокі відбувся перший арешт Інтернет- злочинця, про якого стало відомо громадськості. Приводом для цього послужив перший зареєстрований Інтернет - злом, здійснений шістьма підлітками, які називали себе «група 414» (414 - міжміський телефонний код Мілуокі). Протягом дев'яти днів ними було зламано 60 комп'ютерів, серед яких були комп'ютери Лос-Аламоської державної лабораторії [4].

З початку 1984 року почав публікуватися хакерський журнал «2600». Вихід журналу став своєрідним плацдармом для обміну думок між хакерською спільнотою. Редактором журналу став Еммануїл Голдштейн(справжнє ім'я ЕрікКорлі). Навіть до сьогодні цей журнал не втрачає своєї популярності і становить платформу для виступу проти посиленого цифрового нагляду та відстоювання особистих та цифрових свобод, а також висвітлення сучасної хакерської культури.

У 1984 р. Фред Коен (Fred Cohen) опублікував відомості про розробку перших шкідливих комп'ютерних програм, які саморозмножуються, і застосував до них термін «комп'ютерний вірус». При цьому Фред Коен написав програму, що демонструвала можливість зараження одного комп'ютера іншим.

У 1986 році Конгрес США занепокоєний поширенням нового виду злочинності та зростанням хакерських атак, затверджує акт «The Computer FraudandAbuseAct»[5], який забороняв неавторизований доступ до будь-якої комп'ютерної системи і отримання секретної військової інформації. Саме прийняття цього документа ознаменувало визнання хакерських атак злочинними діями, що посягають на національну безпеку США. Але дія цього акту не поширювалася на неповнолітніх осіб.

Цього ж року з'явилася книга Лойда Бланкеншипа(LoydBlankenship), відомого як «Наставник» через книгу – «Маніфест хакера», що була написана під час відбування покарання у в'язниці. Ідеї, висловлені в цьому маніфесті, до сьогодні вважаються основою хакерської ідеології та культури, що широко розповсюджуються в мережі Інтернет.

Листопад 1988 року став катастрофою для комп'ютерного світу. Студент Корнельського університету Роберт Морріс розробив програму, яка самостійно розмножувала «комп'ютерного черв'яка» та проникла до майже 6000 університетських та урядових комп'ютерів по всій Америці, внаслідок чого було спричинено значну матеріальну шкоду [6, с. 294]. 26 липня 1989 року Морріс став першим звинуваченим у комп'ютерному шахрайстві (ComputerFraud) та акті зловживання (AbuseAct).

У 1994 р. світова спільнота дізналася про так звану «справу Володимира Левіна», віднесену міжнародною кримінальною поліцією до категорії «транснаціональних мережевих комп'ютерних злочинів», який зламав систему управління рахунками корпоративних клієнтів американського «Сітібанку» - одного з найбільших банківських установ планети і викрав таким чином понад 12 мільйонів доларів [7]. Це стає початком третього етапу в розвитку кіберзлочинності, що характеризується транснаціональністю та появою кібертероризму.

III етап. Набуття транснаціонального характеру та початок становлення кібертероризму. Так, британський хакер Гарі Мак Кіннон (GaryMcKinnon) був переконаний, що військові приховують факти, що стосуються НЛО, і в 2001-2002 рр. він вирішив зламати один з серверів NASA. Незабаром були виявлені сліди злому комп'ютерів, що належать армії США, Міністерству обороні Пентагону. У цілому Мак Кіннон отримав несанкціонований доступ до 97 комп'ютерів, і кожен раз він шукав у них інформацію про літальні тарілки.

У 1993 р терористи в Литві погрожували підірвати Ігналінську АЕС за допомогою перехоплення комп'ютерного

контролю над нею та запуску вірусної комп'ютерної програми типу «троянський кінь». А в червні 1998 року міжнародна група хакерів «Milw0rm» отримала доступ до Індійського центру атомних досліджень BhabhaAtomicResearchCenter (BARC) і створила фальшиву сторінку сайту додавши свій контент загрозливого характеру. Оцінка цих діянь призвела до появи нових термінів, таких як «комп'ютерний тероризм» або «кібертероризм». Так у 1997 р спеціальний агент ФБР Марк Поллітт ввів в обіг новий юридичний термін, запропонувавши вважати кібертероризмом будь-яку «навмисну, політично вмотивовану атаку на інформацію, комп'ютерні системи, програми та дані, які призводять до насильства щодо невійськових цілей, груп населення або таємних агентів»[8].

Американський дослідник Ден Вертон вважає, що багато терористичних організацій створили в Інтернеті бази розвідувальних даних,які використовуються при підготовці атак [9, с.72]. Розслідування деяких терактів підтвердило це судження. Наприклад, доведено, що японське терористичне угруповання «АумСінрікьо», що здійснило газову атаку в токійському метро в 1995 р, попередньо створило комп'ютерну програму,яка була здатна перехоплювати повідомлення поліцейських радіостанцій і відслідковувати маршрути руху поліцейських автомобілів.

IV etan. Використання Інтернету в політичних цілях, цілеспрямоване використання кібератак проти урядів держав. Так, конфлікт у Косово вважається першою Інтернет - війною, у якій різні групи комп'ютерних активістів використовували мережу Інтернет для засудження військових дій як Югославії, так і НАТО, навмисно порушуючи при цьому роботу урядових комп'ютерів і отримуючи контроль над сайтами з подальшою зміною змісту [10].

У липні 2016 року напередодні президентських виборів у результаті кібератаки на сервер Національного комітету Демократичної партії США (DNC) майже 20 тисяч електронних листів були опубліковані на порталі «WikiLeaks». Хакери також атакували комітет Демократичної партії під час виборів до Конгресу (DCCC)[11].

27 червня 2017 року Україна стала жертвою масової хакерської атаки: вірус Petya. Вірус шифрує файли на зараженому комп'ютері і виводить на екран повідомлення з вимогами. За даними компанії ESET, яка займається розробкою антивірусного програмного забезпечення, на Україну припало 75,2% заражень від загального числа у світі, на Німеччину - 9%, на Польщу - 5,8%. [12].

Першим етапом правого регулювання протидії кіберзлочинам в Україні були здійснені у 1994 році, а саме внесено зміни до Кримінального кодексу 1960 року, відповідно до яких ст. 198-1 «Порушення роботи автоматизованих систем» було передбачено кримінальну відповідальність за умисне втручання у роботу автоматизованих систем, що призвело до перекручення чи знищення інформації або носіїв інформації, чи розповсюдження програмних і технічних засобів, призначених для незаконного проникнення до автоматизованих систем і здатних спричинити перекручення або знищення інформації чи носіїв такої інформації. У 2001 році було прийнято Кримінальний кодекс України (КК України), відповідно до якого ця діяльність вийшла на якісно новий рівень.

У наукових дослідженнях з цієї проблематики охоплюють наступну термінологію: «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку»; «комп'ютерні злочини»; «кіберзлочини»; «злочини у сфері IT технологій»; «високотехнологічні злочини»; «інтернет-злочини»; «злочини у сфері високих технологій»; «е-злочини»; «злочини у сфері інформаційно-телекомунікаційних систем» та ін. Не слід ототожнювати ці визначення, хоча вони мають схожість, але між ними є відмінності, що відображено у законодавстві. Так у сфері протидії кіберзлочинності основоположною є Конвенція про кіберзлочинність від 23 листопада 2001 року (далі - Конвенція). Сьогодні вона ратифікована 18 державами

та підписана 25 країнами, серед яких є і Україна від 7 вересня 2005 року [13].

У липні 2006 року було ратифіковано додатковий протокол до Конвенції, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (Додатковий протокол) [14]. Термінологія, яка вживається у Конвенції та додатковому протоколі до неї, не знайшла повного відображення у вітчизняному законодавстві. У тексті Конвенції та Додаткового протоколу до неї також не міститься визначення поняття «кіберзлочин» та суміжних з ним понять, однак наявний перелік діянь, за які на національному рівні пропонується встановити кримінальну відповідальність, та наводиться їх умовна класифікація залежно від об'єкта правовідносин [15, с. 4].

Слід зазначити, що в українському законодавстві визначено лише перелік злочинів, які вчиняються з використанням комп'ютерів, комп'ютерних систем та мереж електрозв'язку, закріплених у Розділі XVI КК України. Хоча у деяких законодавчих актах згадуються деякі поняття, проблематику формулювання яких ми розглядаємо, проте в жодному із нормативних актів так і не надано їх визначення. У «Доктрині інформаційної безпеки України» 2009 року використовувались категорії «комп'ютерна злочинність» та «комп'ютерний тероризм» [16, ст. 1783], але у прийнятій відповідній доктрині у 2017 році взагалі не вживається вказана термінологія.

Частково питання визначення термінології мав би вирішити Закон України «Про кібернетичну безпеку України», проект якого було зареєстровано ще 4 червня 2013 року. Проте він не містив визначення кіберзлочину і так і не був прийнятий. Дещо пізніше Указом Президента України від 1 травня 2014 року № 449/2014 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» було поставлено завдання розробити проєкти Стратегії кібернетичної безпеки України і Закону України «Про кібернетичну безпеку України», а також привести національне законодавство у відповідність із міжнародними стандартами з питань інформаційної та кібернетичної безпеки, удосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України.

У Стратегії національної безпеки, затвердженої Указом Президента України від 14 вересня 2020 року № 392/2020, вживаються терміни «кіберзлочинність», «кіберзагроза», «кібербезпека», «кіберпростір» [17]. Після затвердження Стратегії національної безпеки України, відповідно доп. 2 ст. 31 Закону України «Про національну безпеку України» починається організація підготовки Стратегії кібербезпеки України, яка здійснюється за дорученням Президента України Національним координаційним центром кібербезпеки [18]. На сьогодні Стратегія кібербезпеки України на стадії розробки та ще не прийнята. Стратегія визначатиме пріоритети національних інтересів України у сфері кібербезпеки, а також основні підходи та напрями до формування питань кіберзахисту.

Тим часом, як повідомляє Інтерфакс-Україна, Єврокомісією прийнято нову Стратегію кібербезпеки, яка передбачає підвищення стійкості життєво важливих інфраструктур, протидію кібератакам ззовні, у тому числі шляхом санкцій [19].

У Законі України «Про основи національної безпеки України» тільки згадується у статті 31 про Стратегію кібербезпеки України. [20, ст. 351]. Законом України «Про основні засади забезпечення кібербезпеки України» надано визначення поняття - кіберзлочин. Кіберзлочин (комп'ютерний злочин) є суспільно небезпечним винним діянням у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [21, ст. 1].

Попри наявність чинних нормативно-правових актів вітчизняне законодавство лише частково задовольняє потреби сьогодення, оскільки не містить визначення по-

нять, які є відправними у сфері формування державної інфраструктури інформаційної безпеки. Розв'язання проблеми потребує вдосконалення нормативно-правових актів, які є підґрунтям єдиної державної політики забезпечення інформаційної (кібернетичної) безпеки та її реалізації [15,- с. 7; 17, С.181].

Деякі шляхи вдосконалення правового регулювання боротьби з кіберзлочинністю в Україні. Пандемія COVID-19 значно прискорила процеси, які до того розвивалися досить повільно. Зокрема, глобальна ізоляція населення за місцем проживання зумовила більш глибоке занурення у віртуальний кіберпростір, у якому люди більше зазнають впливу інформаційного цунамі, причому переважно деструктивного характеру. Припинення діяльності цілих секторів економіки підштовхнуло найсильнішу за останні часи економічну кризу. Нові специфічні обмежувальні заходи щодо захисту населення водночас уможливили здійснення державою тотального контролю за громадянами. У світі посилилися радикальні настрої і загострилося протистояння між так званими «глобалістами» і «державниками» [22, С. 8].

Зазначені процеси відбуваються на тлі взаємопов'язаних системних криз, які умовно можна визначити як санітарно-епідеміологічну, кіберінформаційну, фінансову, соціально-економічну і політичну кризи.

Окрім безпосередньої шкоди, від можливих випадків несанкціонованого доступу до приватної чи комерційної інформації, інформації з обмеженим доступом, зростають випадки фішингу, DDOS-атак, інформаційних кібератак пов'язаних із маніпулюванням ситуації з COVID-19, актів кібершпигунства, витоку персональних даних громадян та інших злочинів у цій сфері. При цьому ми можемо спостерігати негативну тенденцію підвищення суспільної небезпеки зазначених діянь.

Жертвами кіберзлочинців стають не тільки пересічні громадяни, компанії чи установи, але й цілі корпорації, а також об'єкти критичної інфраструктури, та дедалі частіше - лікарні. Надзвичайною є загроза кібератак, що спрямовані на підрив нормального функціонування закладів охорони здоров'я в умовах пандемії. Так 12 березня 2020 року в результаті кібератаки на заклад охорони здоров'я «University Hospital» в м. Брно Республіка Чехія лікарня була змушена відкласти термінові хірургічні операції та перенаправити нових гострих пацієнтів до сусідніх відділень. Цього ж дня дві інші лікарні «Children's Hospital» і «Maternity Hospital» також постраждали від хакерських атак [23].- У травні 2020 року в результаті кібератаки постраждав ряд об'єктів Національної системи охорони здоров'я (NHS) Великобританії. Хакери вимагали викуп за відновлення роботи комп'ютерних мереж медичних установ у період COVID-19 [24]. Зазначені кібератаки мають тенденцію до зростання і не завжди правоохоронні органи спроможні успішно протидіяти цим злочинним посяганням. Це викликає необхідність здійснення широкомасштабних, довгострокових, системних та науково – обґрунтованих запобіжних заходів як на державному, так і на транснаціональному рівні, що охоплюватиме організаційно – управлінський, кримінально – правовий, адміністративний, медичний та інші напрямки і передбачатиме:

1) удосконалення національного та міжнародного законодавства, що регулює протидію кіберзлочинності, з урахуванням нових сучасних ризиків викликаних захворюваністю на COVID-19. Динамічність поширення комп'ютерних технологій та їх метаморфози зобов'язують законодавця і правоохоронні органи, що протидіють комп'ютерній злочинності, збільшувати швидкість реакції на появу нових способів протиправної діяльності в цьому напрямку, на випередження злочинів;

2) підвищення ефективності взаємодії між правоохоронними органами України і ряду зарубіжних країн. Чітка взаємодія, як форма взаємозв'язку та взаємної підтримки, значення якої важко переоцінити, полягає у тому, що правоохоронні органи в цілому, конкретні їх служби та структурні підрозділи або працівники у взаємодії один з одним досягають значно більших

результатів у менші строки із найменшими витратами сил;

3) посилення співпраці із спеціалізованими органами інших країн у питаннях протидії кіберзлочинності, що повинно проявлятися не лише в обміні досвідом, а також у проведенні спільних операцій, спрямованих на виявлення, попередження та розслідування будь-яких фактів кіберзлочинності, що мають міжнародний характер;

4) забезпечення правоохоронних органів, які уповноважені здійснювати заходи протидії кіберзлочинності новітніми засобами техніки на всіх рівнях роботи. Адже складність виявлення дій комп'ютерного злочинця полягає в його можливості скоювати злочини в кіберпросторі, у якого немає державних кордонів, що багаторазово збільшує ступінь їх суспільної небезпеки;

5) підвищення професіоналізму кадрового складу підрозділів, що займаються питанням протидії кіберзлочинності. Отримання і аналіз доказів у справах про злочини у сфері комп'ютерної інформації – одне з основних і важко вирішуваних на практиці завдань. Це вимагає не лише розробки тактики проведення слідчих і організаційних заходів, але і наявності спеціальних знань у сфері комп'ютерної техніки і програмного забезпечення, а також внесення поправок до чинного законодавства. Співробітники, які безпосередньо займаються розслідуванням цього роду злочинів, і працівники судової системи часто не володіють спеціальними знаннями у сфері нових комп'ютерних технологій, що часто ускладнює процес розслідування злочинів;

6) використання у діяльності підрозділів боротьби з кіберзлочинністю результатів наукових розробок з тематики, що стосується протидії кіберзлочинам. На практиці часто виникають помилки при кваліфікації та документуванні злочинних діянь, частими причинами чого є відсутність достатньої кількості методичних рекомендацій і роз'яснень із розслідування цих злочинів, узагальненої судової практики.

Якщо звертатись прикладних статистичних даних з питань впливу пандемії коронавірусу на різні регіони світу, то за інформацією, представленою Інтерполом за травень 2020 року, шляхом опитування громадян було визначено, що існують різні тенденції проявів кіберзлочинності в умовах пандемії коронавірусу за регіонами. Наприклад, в Африці респонденти активно скаржились на:

1. Необхідність посиленого використання електронних або безготівкових платежів з моменту початку пандемії, через що громадськість піддалася масивним кібератакам з цього приводу.

2. У більшості організацій та компаній примушують працювати вдома, за таких умов вразливість такого типу роботи привела до сплеску афер з відповідною тематикою фішингу, вимагання та благодійності.

3. Активне розповсюдження та тираж фейкових новин, пов'язаних з COVID-19, у соціальних мережах також було збільшено кількість «спаму» із новинами про коронавірус.

4. Діяльність державно-приватного партнерства була відносно низькою на рахунок проявів кіберзлочинності, сприяючи збільшенню кількості невирішених кіберзлочинів [25].

Для порівняння тенденцій по регіонах та здійснення аналізу представлених даних, слід привести ще приклади відповідей респондентів зафіксованих в регіонах Америки та Європи. Щодо американських респондентів, то вони найбільше скаржились на:

1. Різке збільшення тематичних фішингових та шахрайських кампаній, пов'язаних із COVID-19.

2. Те, що багато компаній в Америці впровадили роботу в режимі телемережі, і за таких обставин кіберзлочинці частіше стали орієнтуватися на працівників, як потенційних жертв, щоб отримати контроль через віддалений доступ до корпоративних мереж з метою крадіжки конфіденційної інформації.

3. Роботу соціальних медіа, які все частіше використовуються злочинцями для пропаганди сексуальної поведінки дітей в Інтернеті та їх подальшої експлуатації.

4. Правопорушниками в мережі Інтернет було скоєно багато проявів жорстокого поводження з дітьми, що вплинуло на їх психологічний стан та здоров'я [40].

Аналізуючи дані, представлені респондентами різних регіонів світу, слід зазначити, що кібернетичні злочини, пов'язані з пандемією коронавірусу є схожими.- В основному кіберзлочинці користувалися загальною неготовністю представників різних держав світу щодо захисту власних даних, інформації та, загалом, безпечного перебування у кіберпросторі. Усі приклади кіберзлочинності, звісно, стосувалися отримання матеріальної вигоди або морального задоволення кіберзлочинців.

Враховуючи огляд усіх існуючих на сьогодні тенденцій, проявів, обставин розповсюдження кіберзлочинів в умовах COVID-19, останнім, на що слід звернути увагу, є проєкт CyberEast. Сутність створення цього проєкту в 2019-ому році, що фінансується Європейським Союзом, стосувалася побудови взаємної правової допомоги та поліцейського міжнародного співробітництва. За умови існування коронавірусу цей проєкт також був залучений до питання вирішення проблем із кіберзлочинністю. Основною метою цього проєкту було збільшення потенціалу судових та правоохоронних органів, налагодження міжнародної співпраці, побудова довіри у сфері кримінального правосуддя та активне вирішення, розслідування існуючих кіберзлочинів у рамках пандемії коронавірусу. Також завдяки представленому проєкту були значно розширені можливості щодо боротьби з кіберзлочинністю та електронними доказами, у вирішенні кримінальних справ.

Останнім, що слід згадати, враховуючи сучасні перипетії та обставини навколо тематики кіберзлочинності на тлі пандемії коронавірусу є рекомендації щодо питань безпеки громадян у кіберпросторі. Ці рекомендації були розроблені Європейським Союзом у вигляді норм та правил для організації захисту населення під час їх перебування в кіберпросторі. Цими рекомендаціями є: постійна зміна паролю від Wi-fi роутеру; встановлення винятково якісного програмного забезпечення, антивірусу; перевірка можливостей програм, контроль за її доступом до галереї, документів, карток пам'яті; створення максимально складних паролів для електронної пошти та інших видів ресурсів, на яких перебуває людина; організація автоматичного збереження важливих даних у хмарне сховище; захист електронних девайсів від кібернетичних зломів шляхом встановлення пін-кодів, сканерів відбитки пальців, голосового інтерфейсу; постійна перевірка налаштувань приватності при перебуванні акаунту людини в мережі Інтернет; покупка через мережу Інтернет тільки на сертифікованих сайтах, які гарантують захист вашої особистої інформації; забезпечте системою захисту перебування дітей у мережі Інтернет, шляхом встановлення спеціальних програм; не робіть зайвих переказів грошових ресурсів, якщо не впевнені в надійності сайту, мережі, у якій збираєтесь зробити транзакцію [26].

Висновки

Осмислення актуальних питань кібербезпеки в контексті сучасних проблем правознавства вказує на те, що:

1. Окремі технологічні характеристики всесвітньої комп'ютерної мережі «Internet» є найбільш впливовими чинниками розвитку майже всього спектру сучасних суспільних відносин. Водночас, саме вони й криміналізують сферу кіберпростору. До них належать: - всесвітній (глобальний) характер мережі «Internet» та відсутність географічних кордонів; - можливість для користувачів залишатися анонімними під час її використання; - відсутність матеріальної форми в інформації, що поширюється у цій мережі, її здатність циркулювати у цій мережі безконтрольно; - наявність електронних зв'язків між користувачами мережі «Internet».

2. Рівень правового захисту персональних даних людини, розміщених у мережі «Internet», не відповідає сучасним світовим стандартам у цій галузі, а зміст поняття «персональні дані людини» за своїм об'ємом є значно вужчим, ніж у країнах ЄС та США. Ця обставина є одним із чин-

ників, що сприяють поширенню кіберзлочинності у вітчизняному сегменті мережі «Internet».

3. Вагомою проблемою, яка виникає під час розслідування злочинів, вчинених у кіберпросторі, є фіксація точного моменту вчинення злочину, адже в цілому існують труднощі у тому, щоб визначити та зафіксувати точний момент здійснення того чи іншого акту або певної події у цьому середовищі, чимало користувачів мережі «Internet» діють у ній анонімно, без будь-якої ідентифікації, крім того між ними немає реальних контактів та вони можуть знаходитися у різних частинах світу. Тому практично всі стадії процедури розслідування кіберзлочинів (від збирання та аналізу фактичних даних до юридичної кваліфікації та притягнення злочинців до відповідальності) повинні бути адаптовані до реалій віртуального простору. Це також виявляється в тому, що особи, котрі відбувають покарання за вчинення злочинів у пенітенціарних закладах, мають бути абсолютно позбавлені можливості доступу до комп'ютерних технологій.

4. У науковому середовищі вже не має дискусії про те, чи є кіберзлочинність загрозою національній безпеці України. Основні питання точаться навколо того, який зміст має вкладатися в поняття «кіберзлочинність», її ознаки та види.

5. Ключовою проблемою, що впливає на стан боротьби з кіберзлочинністю є неузгодженість термінологічної бази, як і вільне використання значної кількості термінів (та їх синонімів), що часто не узгоджені між собою. Так, у Законі України «Про національну безпеку України» згадується поняття «кібербезпека України». Водночас, цей термін не має свого визначення.

У Законі України «Про боротьбу з тероризмом» поняття «комп'ютерний тероризм» не згадується взагалі, а ті елементи, що можуть до нього відноситись, прописані як складова частина поняття «технологічний тероризм». Отже, можна констатувати, що вітчизняне нормативно-правове поле у сфері інформаційної (кібернетичної) безпеки оперує термінами визначень, яких фактично немає.

6. Питання кіберзлочинності в умовах COVID-19 стало розвиватися активніше. Пандемія коронавірусу сьогодні дозволяє кіберзлочинцям застосовувати різні методи для обману та шахрайства різного роду. Для того щоб вміти правильно протистояти впливу кібернетичних загроз, світова спільнота постійно повинна приймати ефективні рішення щодо створення спеціальних алгоритмів захисту власного населення від подібних діянь. Якщо згадувати статистичні дані з приводу пандемії коронавірусу та взаємозалежності її з різними проявами кібернетичних злочинів, то слід констатувати, що подібні злочинні діяння будуть збільшуватися з кожним роком.

Література

1. Колпаков В. К. Деліктний феномен в адміністративному праві України: дис. … докт. юрид. наук: 12.00.07. К., 2005. 590 с.

2. Зверянская Л. П. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений. *Научно-методический журнал «Концепт»*. 2016. Т. 15. С. 881–885.

3. Загуменна Ю. О., Расторгуєва Н. О. Історичні передумови виникнення та розвитку кіберзлочинності. *Сучасна юридична наука: проблеми доктринальної комунікації:* Міжнародна науково-практична конференція (19 квітня 2019 року). Харків: Харківський національний університет імені В. Н. Каразіна 2019 с. 195 .

4. Лукацкий А. Хакеры управляют реактором. URL: http://www.crime-research.ru/library/Lukac0103.html (дата звернення: 30.01.2021).

5. Computer Fraud and Abuse Act. URL: http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act. - Wikipedia The free encyclopedia (дата звернення: 30.01.2021).

6. Ричка Д. О. Історичні аспекти кіберзлочинності. Матеріали VII Міжнародної наукової конференції студентів, аспірантів та молодих вчених «Сучасний стан і перспективи розвитку держави і права». Дніпропетровськ, 2015. С. 293-295.

7. LemosRobert.Cyberterrorism: Therealrisk. RobertLemos; Центр дослідження комп'ютерної злочинності. URL:

http://www.cnme- research. org/library/ Robert (дата звернення: 22.01.2021).

8. Krasavin, S. WhatisCyber-terrorism? Computer Crime Research Center (CCRC). URL: http://www.crime-research.org/library/Cyber-terrorism.htm (дата звернення: 22.11.2020).

9. Verton, D. BlackIce: TheInvisibleThreatofCyber-Terrorism. N. Y. : McGraw-HillOsborneMedia, 2003. 273 p.

10. Андреев А. Об информационном противоборстве в ходе вооруженного конфликта в Косово. URL: http://www.psyfactor.org/warkosovo.htm. (дата звернення: 22.01.2021).

11. Доповідь експертів компанії Microsoft. URL:https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/ (дата звернення: 30.01.2021).

12. "Petya" Ransomware: WhatweknownowESET reportURL:https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now/ (дата звернення: 25.11.2020).

13. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV (у ред. 14.10.2010.). URL: https://zakon.rada.gov.ua/laws/show/2824-15 (дата звернення: 29.01.2021р.).

14. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21.07.2006- № 23-V (ратифікація 21.07.2006). URL: https://zakon.rada.gov.ua/laws/show/994_687 (дата звернення: 29.01.2021р.).

15. Амелін О.Ю. Визначення кіберзлочинів у національному законодавстві. *Науковий часопис Національної академії прокуратури України*. 2016. Вип. № 3. С. 1–10.

16. Про Доктрину інформаційної безпеки України: Указ Президента України від 25.02.2017 № 47/2017. Офіційний вісник України від 10.03.2017. № 20, стор. 8, стаття 554, код акта 85081/2017.

17. Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text. (дата звернення: 29.01.2021р.).

18. РНБО розпочали розробку Стратегії кібербезпеки України. URL: https://www.ukrinform.ua/rubric-polytics/3105556-u-rnbo-pocali-rozroblati-strategiu-kiberbezpeki-ukraini.html/ (дата звернення: 29.01.2021р.).

19. ЕС представил новую Стратегию кибербезопасности. URL: https://interfax.com.ua/news/general/710351.html/

20. Про основи національної безпеки України: Закон України від 21.06. 2018 № 2469-VIII. *Відомості Верховної Ради України* від 03.08. 2018 р., № 31, стор. 5, стаття 241. (дата звернення: 29.01.2021р.).

21. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 29.01.2021р.).

22. Горбулін В. П., Даник Ю. Г. Національна безпека України: фокус пріоритетів в умовах пандемі. *Наука і суспільство. Вісник НАН України*. 2020. №5. С.3-18.

23. Catalin Cimpanu «Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak». URL: https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/ (дата звернення: 19.01.2021).

24. Sam Jones for The Guardian «NHS seeks to recover from global cyber-attack as security concerns resurface». URL: https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack (дата звернення: 19.11.2020).

25. Interpole, Cybercrime, «COVID-19 impact», August 2020.

26. Europol, Public awareness and prevention, «Make your home a cyber safe stronghold». URL: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold (дата звернення: 19.01.2021).

Yuliia Oleksandrivna Zahumenna,
Professor of the Department of Theory and History of State and Law of Kharkiv National Universdity of Internal Affairs, PhD in Law, associate professor, Kharkiv City, Ukraine;

TOPICAL ISSUES OF CYBER SECURITY IN THE CONTEXT OF MODERN PROBLEMS OF LEGAL SCIENCE

The author of the article has carried out a comprehensive research of topical issues of cyber security in the context of modern problems of legal science. Ways of improving the legal regulation of the fight against cybercrime in Ukraine have been defined. The author has identified the tendencies for the universalization of approaches of legislators of different countries regarding the fight against cybercrime, including both in Ukraine and in the United States; has established liability for fraud related to the use of computers and computer networks. The author has suggested own approach to understanding the concept of "cybercrime". It should be considered as certain illegal actions committed in cyber space, the liability for which is stipulated by criminal law. The most common cybercrimes include: theft of money from bank credit cards, creation of websites with child pornography, computer viruses, propaganda of racial intolerance, instructions for producing homemade explosive devices, computer attacks on government networks, on military, space computer systems, industrial espionage, use of compromising materials for political purposes.

The author has carried out the analysis and has defined factors that complicate the effective application of legislation on cybercrimes in Ukraine. The key one among them is the difficulty of prosecuting those who have committed cybercrime in Ukraine from abroad. Therefore, the urgent problem is the organization of international and legal cooperation for searching and prosecuting persons who have committed crimes outside the jurisdiction of the country, where criminal actions were committed.

Further development of the scientific position developed by the domestic analytical jurisprudence that the concept of "sphere of legal regulation of public relations" should include, in particular the national segment of the global computer network "Internet", which is organized by state authorities of a particular country. The author has improved the scientific assertion that the analysis of the fight against cybercrime demonstrates that the software (digital product) used by law enforcement agencies in the fight against cybercrime, including during preventive measures in the form of restricting or prohibiting the access to any information of illegal nature posted on the websites, should be considered as a qualitatively new type of state coercion.

Key words: cybercrime, fight against cybercrime, cyber security, COVID-19 pandemic, national security, information security.