**УДК 341.45:004.056**
**DOI https://doi.org/10.32841/2307-1745.2021.50.25**

***Леган І. М.,***
*orcid.org/0000-0003-2933-4971*
*кандидат економічних наук, доцент,*
*доцент кафедри економічної безпеки, публічного управління та адміністрування*
*Державного університету «Житомирська політехніка»*

# ОСОБЛИВОСТІ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ЩОДО ЗАПОБІГАННЯ І ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА КІБЕРТЕРОРИЗМУ

**Анотація.** Стаття присвячена тенденціям розвитку сучасної форми злочинності, що особливо актуалізується в умовах розвитку інформаційно-комп'ютерних технологій та соціальної ізоляції в умовах пандемії COVID-19, а саме кіберзлочинності. Розкрито сутність понять «кіберзлочинність» і «кібертероризм», здійснено класифікацію найбільш популярних кіберзлочинів в сучасних умовах. Досліджено характерні риси кіберзлочинності та визначено критерії, за якими вона відмежовується від інших видів злочинності, зокрема кібертероризму.

Зазначено, що у вітчизняній і зарубіжній літературі не сформовано єдиного визначеного понятійного апарату щодо сутності понять «кіберзлочинність» і «кібертероризм», їх характеристик, загальних тенденцій і перспектив розвитку. Доведено всю нинішню глобальність проблеми кіберзлочинності, адже сучасні кібератаки паралізують роботу не тільки приватних структур, а й державних органів влади. Окреслено, що від такого роду атак не застрахована жодна країна світу, а суб'єктами, які їх здійснюють, можуть бути не просто індивідуальні хакери чи групи хакерів, але й окремі держави, терористичні та організовані злочинні угруповання, в тому числі й транснаціональні.

Досліджено міжнародно-правову систему норм, спрямованих на створення правових засад співробітництва держав у сфері боротьби з кіберзлочинами. Проаналізовано основні нормативно-правові акти та міжнародні документи у цій сфері, визначено шляхи удосконалення її правового регулювання на майбутнє. Доведено, що національна безпека значним чином залежить від забезпечення інформаційної безпеки, а під час технічного прогресу ця залежність тільки зростає. Інформація, виступаючи економічною та соціальною гарантією стабільності існування та розвитку суспільства і держави, є об'єктом пильної уваги і впливу з боку держави. Охарактеризовано глобальність проблеми кіберзлочинності у світі загалом і в Україні зокрема.

Охарактеризовано, що з огляду на постійну еволюцію кіберзлочинності правоохоронним організаціям та органам необхідно ділитися інформацією та знаннями зі своїми колегами в усьому світі для розробки своєчасних і дієвих заходів у відповідь на проведені та реалізовані розвідувальні дії. Зазначено, що особливості функціонування інформаційних систем зумовлюють необхідність вирішення питань кібербезпеки шляхом ефективної взаємодії та співробітництва різних суб'єктів (як державних, так і приватних).

**Ключові слова:** кіберзлочинність, кібертероризм, злочини у кіберпросторі, транснаціональна злочинність, транскордонна злочинність.

**Постановка проблеми.** Стрімкий розвиток інформаційно-комп'ютерних технологій у світі супроводжується відповідним динамічним розвитком злочинів у цій сфері. Загальновідомим є факт, що будь-який прогрес, який привносить у суспільне життя нові блага та можливості, здебільшого супроводжується на протидію й відповідними негативними явищами. З кожним роком кіберзлочинність стає все більш масовішою та небезпечнішою.

**Метою статті** є характеристика особливостей та тенденцій розвитку міжнародного співробітництва щодо запобігання та протидії кіберзлочинності й кібертероризму.

**Виклад основного матеріалу дослідження.** Саме поняття «кіберзлочинність» вперше з'явилося в американській, а згодом і в іншій зарубіжній літературі на початку 1960-х рр. Так, за даними американської компанії McAfee, яка спеціалізується на комп'ютерній безпеці, та Центру стратегічних і міжнародних досліджень (CSIS) хакерські атаки у 2020 році завдали матеріальної шкоди світовій економіці на понад трильйон доларів. Завданий збиток вищий за аналогічний у 2018 році на 50%. Отже, завдані збитки становлять у 2020 році близько 1% світового ВВП.

У 2017 році масштабна хакерська атака вірусом «Petya» відбулася й в Україні. Робота українських банків, міжнародного аеропорту «Бориспіль», аеропорту Харкова, Чорнобильської АЕС, державних урядових сайтів, київського метрополітену та енергетичних компаній була заблокована. Це було перше масштабне вторгнення у роботу серверів нашої держави за весь період незалежності. На думку експертів Міжнародного валютного фонду, втрати держави від хакерської атаки вірусом «Petya» сягнули 850 мільйонів доларів США. При цьому постраждалі компанії, що зверталися до кіберполіції, не змогли відшкодувати понесені втрати та притягнути до відповідальності осіб, причетних до масштабної атаки, через неможливість ідентифікації кіберзлочинців.

Ще у 1991 році Інтерпол запропонував власну кодифікацію інформаційних (кібер) злочинів, серед яких:

1) QA – несанкціонований доступ та перехоплення;
2) QDT – троянський кінь;
3) QAT – крадіжка часу (ухилення від плати за користування);
4) QDV – комп'ютерний вірус;
5) QD – зміна комп'ютерних даних;
6) QFC – шахрайство з банкоматами;
7) QF – комп'ютерне шахрайство;

8) QZ – інші комп'ютерні злочини;
9) QR – незаконне копіювання;
10) QFT – телефонне шахрайство;
11) QS – комп'ютерний саботаж;
12) QFF – комп'ютерна підробка (та інші) [7].

Згідно з Конвенцією Ради Європи по боротьбі з кіберзлочинністю, яка була ратифікована Верховною Радою України, виділено чотири основних типи кіберзлочинів [6], а саме:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання в систему, зловживання пристроями);

2) правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами);

3) правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією);

4) правопорушення, пов'язані з порушення авторських або суміжних прав.

Класифікаційні ознаки та види сучасних кіберзлочинів представлені за допомогою табл. 1.

Нині кіберзлочинність – одна з найбільш розповсюджених і популярних форм транснаціональної злочинності. Складні кіберзагрози створюють нові проблеми для правоохоронних органів, включно з великими обсягами даних, міжнародні розслідування і нові знання у технічній галузі. З огляду на постійну еволюцію кіберзлочинності правоохоронним організаціям та органам необхідно ділитися інформацією та знаннями зі своїми колегами в усьому світі для розробки своєчасних і дієвих заходів у відповідь на проведені та реалізовані розвідувальні дії.

Саме з цією метою Інтерпол створив дві безпечні та гнучкі служби для сприяння контактам між поліцією та іншими зацікавленими сторонами для запобігання та протидії кіберзлочинності:

1) Cybercrime Knowledge Exchange workspace (CKE) – робочий простір обміну знаннями про кіберзлочинність, що обробляє загальну інформацію та дані якої відкриті для широкого загалу користувачів;

2) Cybercrime Collaborative Platform (CCP) – платформа для спільної роботи в сфері кіберзлочинності, включно з операціями для підтримки правоохоронних дій і заходів, доступ до яких обмежений [7].

На думку фахівців у сфері інформаційних технологій, ситуація із кіберзлочинністю у світі з кожним роком погіршується. Транснаціональна злочинність трансформується у кіберзлочинність, адже приховувати свою кримінальну діяльність в інтернет-просторі дедалі простіше. Існування мережі Darknet тільки підтверджує існування «чорного ринку» для реалізації зброї, наркотиків та інших незаконних товарів і послуг. Розвиток сучасних технологій забезпечує кіберзлочинцям анонімність у мережі, оскільки мережа Darknet є безконтрольною, а отже гарантує безпеку для кримінальної діяльності організованих злочинних угруповань, в тому числі й транснаціональних. Так, за офіційними даними Національної поліції України, кількість злочинних угруповань, які в своїй діяльності активно використовують сучасні інформаційні технології, протягом останнього року збільшилася на понад 30% [9].

З метою реалізації державної політики у сфері протидії кіберзлочинності в Україні 5 жовтня 2015 року був створений Департамент кіберполіції Національної поліції України. Серед основних завдань цього міжрегіонального територіального органу Національної поліції України виокремлено:

1) участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, мереж електрозв'язку;

2) сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень [8].

Крім того, в Україні створене розгалужене нормативно-правове підґрунтя для боротьби з кіберзлочинністю, а саме:

1) Конституція України;
2) Кримінальний кодекс України;
3) Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації від 1 червня 2001 року;

Таблиця 1

**Класифікаційні ознаки та види сучасних кіберзлочинів**

<table>
<tr><td colspan="4">Кіберзлочини у сфері використання платіжних систем</td></tr>
<tr><td>скімінг (шимінг)</td><td>кеш-трапінг</td><td>кардінг</td><td rowspan="2">несанкціоноване списання коштів із банківських рахунків за допомогою систем дистанційного банківського обслуговування</td></tr>
<tr><td>незаконне копіювання вмісту треків магнітної смуги (чипів) банківських карток</td><td>викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки</td><td>незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем</td></tr>
<tr><td colspan="4">Кіберзлочини у сфері електронної комерції та господарської діяльності</td></tr>
<tr><td colspan="2">фішинг</td><td colspan="2">онлайн-шахрайство</td></tr>
<tr><td colspan="2">виманювання у користувачів інтернету їхніх логінів і паролів до електронних гаманців, сервісів онлайн-аукціонів, переказування чи обміну валюти</td><td colspan="2">заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку</td></tr>
<tr><td colspan="4">Кіберзлочини у сфері інтелектуальної власності</td></tr>
<tr><td colspan="2">піратство</td><td colspan="2">кардшарінг</td></tr>
<tr><td colspan="2">незаконне розповсюдження інтелектуальної власності в інтернеті</td><td colspan="2">надання незаконного доступу до перегляду супутникового та кабельного TV</td></tr>
<tr><td colspan="4">Кіберзлочини у сфері інформаційної безпеки</td></tr>
<tr><td>соціальна інженерія</td><td>шкідливе програмне забезпечення (англ. "malware")</td><td>протиправний контент</td><td>рефайлінг</td></tr>
<tr><td>технологія управління людьми в інтернет-просторі</td><td>створення та розповсюдження вірусів і шкідливого програмного забезпечення</td><td>контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства</td><td>незаконна підміна телефонного трафіку</td></tr>
</table>

4) Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 7 вересня 2005 року;

5) Закон України «Про інформацію» від 2 жовтня 1992 року;

6) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року;

7) Закон України «Про внесення змін до Закону України «Про платіжні системи та переказ грошей в Україні» від 6 жовтня 2004 року;

8) Закон України «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» (щодо відповідальності за комп'ютерні злочини)» від 23 грудня 2004 року;

9) Закон України «Про внесення змін до Закону України «Про захист інформації в автоматизованих системах» від 31 травня 2005 року;

10) Доктрина інформаційної безпеки від 25 лютого 2017 року;

11) Закон України «Про національну безпеку України» від 21 червня 2018 року;

12) Закон України «Про основні засади забезпечення кібербезпеки України» від 24 жовтня 2020 року;

13) інші міжнародні договори.

Крім того, варто зазначити про зв'язок кіберзлочинності і пандемії COVID-19. Через всесвітню соціальну ізоляцію та закритість кордонів країн більшість людей у світі перейшла на віддалену форму зайнятості та освіти, що призвело до активізації онлайн комунікацій не тільки у приватному, але й у державному секторі.

У зв'язку з необхідністю навчання та роботи онлайн представники різних вікових груп піддаються ризикам стати жертвами кіберзлочинців, навіть не підозрюючи про це. Останні ж намагаються максимально приховати свої сліди, що ускладнює збір доказів: вони використовують шифрування даних, заходять в мережу Інтернет із громадських і загальнодоступних місць, використовують чужі облікові записи.

Поряд із традиційними видами кіберзлочинності передові цілеспрямовані загрози (APT – Advanced Persistent Threats) продовжують удосконалюватися і використовуватися для отримання вигоди із ситуації з пандемією COVID-19. Основною метою APT-атак є критичні об'єкти інфраструктури, включно з лікарнями та лабораторіями по розробці вакцин. При цьому застосовуються шкідливі програми, програми-вимагачі, а також DDoS-атаки. Мотивом для подібних атак є не тільки отримання прибутку, але й можливість доступу до персональних даних та іншої конфіденційної інформації, що представляє цінність (наприклад, як оперативні та/або розвідувальні дані). Проте деякі провідні країни світу мають досить ефективну систему протидії здійсненню кіберзлочинності (табл. 2).

Поняття «тероризм» не є новим для вітчизняної юридичної науки, однак в силу певних глобалізаційних та інтеграційних процесів це явище трансформувалося у такі нові його вияви як «кібертероризм». Термін «кібертероризм» з'явився у 1980-х роках. Вперше він був вжитий Б. Колліном, фахівцем Інституту безпеки і розвідки в Каліфорнії, під яким вчений запропонував розуміти можливість терористичних атак у кіберпросторі. Це явище набуло швидкого розповсюдження здебільшого у розвинених країнах світу у зв'язку з комп'ютеризацією і цифровізацією економіки та практично усіх видів діяльності людини і людства. Однак міжнародна наукова та правоохоронна спільноти досі не виробили єдиного визначення поняття «кібертероризм», що значно уповільнює розробку методів протидії та запобігання цьому виду злочину.

Кібертероризм (cyberterrorism, cyberterrorizm, від лат. "terror" – «страх, жах») – це найбільш небезпечний різновид кіберзлочинності, що включає в себе:

1) здійснення терористичних актів з використанням інформаційних та комп'ютерно-телекомунікаційних технологій (ІКТ);

2) політично- або ідеологічно-мотивоване використання ІТ-технологій для проведення атак на системи управління об'єктами життєзабезпечення, комп'ютерні системи, популярні інформаційні ресурси з метою дестабілізації ситуації у регіоні або в країні у напрямі безпеки, заподіяння серйозних наслідків для критично важливих інфраструктур і/або виклику паніки та нагнітання страху серед цивільного населення.

У 2021 році всі країни світу та великі організації надають величезне значення боротьбі із кібертероризмом. Сучасний кібертероризм є складником гібридних воєн і одним із дієвих важелів реалізації важливих політичних цілей на міжнародній арені. Сучасні кібертерористи (cyber-terrorist),

Таблиця 2

**Особливості забезпечення кібербезпеки в різних країнах світу**

| Країна / Country | Участь у Конвенції про кібербезпеку (Participation in Cybercrime Convention) | Розробка Конвенції ООН «Про забезпечення міжнародної інформаційної безпеки»/ Development of UN Convention "On International Information Security" | Основні організації в області кібербезпеки / Key agencies responsible for cybersecurity |
|---|---|---|---|
| Великобританія | + | - | Група безпеки електронної комунікації при Центрі правового зв'язку при МЗС; підрозділ Міністерства оборони щодо захисту від віртуальних загроз |
| Німеччина | + | - | Спеціальна група при МВС ФРН |
| Індія | + | - | Аналітичний і дослідницький відділи зовнішньої розвідки і розвідувальне бюро внутрішньої розвідки |
| Китай | - | + | Реалізація програми захисту від несанкціонованого підключення до комп'ютера |
| РФ | - | + | Управління «К» МВС і відділи «К» регіональних управлінь МВС; Національний контактний пункт при БСТМ МВС Росії |
| США | + | - | Центр національної кібербезпеки; Об'єднане кібернетичне командування Збройних сил США |
| Україна | + | - | Департамент кіберполіції при Національній поліції України |

які володіють кіберзброєю, тобто відповідними технічними та програмними засобами ведення війни в кіберпросторі, однією із головних задач ставлять захоплення (взяття під контроль), руйнування або порушення роботи комп'ютерних мереж і систем великих організацій, галузей або країн, а в деяких випадках – і міжнародних організацій. При певних умовах акції кібертерористів можуть призвести до виникнення великомасштабних екологічних, економічних катастроф і масової загибелі людей.

В Законі України «Про основні засади забезпечення кібербезпеки України» від 24 жовтня 2020 року визначено, що кібертероризм – це терористична діяльність, що здійснюється у кіберпросторі або з його використанням [4].

Злочини, вчинені у кіберпросторі, часто є міжнародними, тобто існує значна вірогідність того, що злочинці діють в одній державі, а їх жертви – знаходяться в іншій. Тому для запобігання та протидії такому виду злочину особливу актуальність та значення має міжнародне співробітництво. Однак подекуди дефіцит міжнародного співробітництва дозволяє кіберзлочинності залишатися безкарною.

Міжнародне співробітництво у боротьбі із кібертероризмом здійснюється в рамках діяльності ООН, Ради Європи, Міжнародної організації експертів Інтерполу, Європолу. Центральна роль у координації цієї боротьби відводиться ООН, особливо її основним органам: Генеральній Асамблеї, Раді Безпеки, а також різним багатостороннім неформальним партнерствам. Більшість із цих міжнародних організацій включають у напрями своєї діяльності розробку нормативної бази для сприяння співпраці у боротьбі з кіберзлочинами та створення відповідних органів з метою налагодження такої співпраці. В рамках роботи ООН прийнято низку резолюцій з різних аспектів запобігання кібертероризму. Так, у 2006 році була заснована Міжнародна організація по боротьбі з кібертероризмом «ІМПАКТ», основною метою створення якої є об'єднання представників державного та приватного сектору для протидії і пошуку методів ефективного протистояння кібертероризму.

**Висновки.** Варто розуміти, що кіберзлочинність і кібертероризм можуть порушувати інтереси як цілої держави, так і окремого громадянина. Безперечно, що особливості функціонування інформаційних систем зумовлюють необхідність вирішення питань кібербезпеки шляхом ефективної взаємодії та співробітництва різних суб'єктів (як державних, так і приватних). Однак саме на державі лежить відповідальність за повномасштабну протидію кіберзлочинності та створення належних умов для забезпечення надійної системи інформаційного захисту як фізичних, так і юридичних осіб нашої держави.

***Література:***


1. Legan I.M., Bondarenko K.S. Features of the free legal aid system in Ukraine and the European Union countries / *Держава та регіони*. Серія: ПРАВО. 2020. № 3(69). С. 148–151.
2. Ануфрієв М.І., Кісілевич-Чорнойван О.М. Міжнародно-правові засади співробітництва у боротьбі з кіберзлочинами. URL: file:///C:/Users/USER/Downloads/Nashp_2017_3_11.pdf.
3. Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій : навч. посібник / за заг. ред. доктора юридичних наук, професора Р.А. Калюжного. Запоріжжя : ГУ «ЗІДМУ». 2002. 292 с.
4. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 24 жовтня 2020 року. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
5. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606.
6. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.
7. Офіційний сайт Інтерполу. URL: https://www.interpol.int/.
8. Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/.
9. Офіційний сайт Національної поліції України. URL: https://www.npu.gov.ua/.


**Legan I. Peculiarities of international cooperation on preventing and combating cyber crime and cyberterrorism**


**Summary.** The article is devoted to the trends of the modern form of crime, which is especially relevant in the development of information and computer technology and social isolation in the context of the COVID-19 pandemic, namely cybercrime. The essence of the concepts "cybercrime" and "cyberterrorism" is revealed, the classification of the most popular cybercrimes in modern conditions is carried out. The characteristic features of cybercrime are studied and the criteria by which it is distinguished from other types of crime, in particular cyberterrorism, are determined.

It is noted that in the domestic and foreign literature there is no single defined conceptual apparatus to the essence of the concepts of cybercrime and cyberterrorism, their characteristics, general trends and prospects. The whole global nature of the problem of cybercrime today has been proved, because modern cyberattacks paralyze the work not only of private structures, but also of public authorities. It is stated that no country in the world is safe from such attacks and the perpetrators can be not only individual hackers or groups of hackers, but also individual states, terrorist and organized criminal groups, including transnational ones.

The international legal system of norms aimed at creating the legal basis for cooperation between states in the fight against cybercrime is studied. The main normative legal acts and international documents in this field are analyzed and the ways of improving its legal regulation for the future are determined. It has been proven that national security largely depends on information security and in the course of technical progress this dependence is only growing. Information, acting as an economic and social guarantee of the stability of existence and development of society and the state, is the object of close attention and influence of the state.

The global nature of the problem of cybercrime in the world in general and in Ukraine in particular is described. It is described that given the constant evolution of cybercrime, law enforcement agencies and authorities need to share information and knowledge with their counterparts around the world to develop timely and effective measures in response to conducted and implemented intelligence actions. It is noted that the peculiarities of the functioning of information systems necessitate the solution of cybersecurity issues through effective interaction and cooperation of various entities, both public and private.



**Key words:** cybercrime, cyberterrorism, crimes in cyberspace, transnational crime, cross-border crime.