**УДК 343.9:345.42**

***Шеломенцев Володимир Петрович —*** головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, кандидат юридичних наук

# Кримінологічна безпека у кіберпросторі: система понять

*Стаття присвячена розгляду проблемних питань розроблення категорійно-понятійного апарату кримінологічної безпеки у кіберпросторі.*

**Ключові слова**: кримінологічна безпека, кіберпростір, кіберзагрози, кіберзлочини, кіберзахист, кібербезпека.

У сучасних умовах стрімкого розвитку інформаційних технологій та їх широкого впровадження в усі сфери суспільного життя важливого значення набуває забезпечення кримінологічної безпеки людини, суспільства, держави в такому важливому сегменті інформаційного простору як кіберпростір.

Під кіберпростором (кібернетичним простором) розуміється штучне електронне середовище існування інформаційних об'єктів у цифровій формі, утворене в результаті функціонування кібернетичних комп'ютерних систем управління та оброблення інформації й забезпечує користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних обчислювальних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів (надання інформаційних послуг, ведення електронної комерції тощо) [1, с. 80].

Окремі аспекти забезпечення безпеки людини, суспільства, держави від злочинних посягань розглядались у працях В. А. Бодренкова, Г. Г. Горшенкова, С. Я. Лебедєва, В. О. Плешакова, А. А. Тер-Акопова, О. Ю. Шумилова та інших правників. Проблеми кримінологічної безпеки у сфері комп'ютеризованої обробки інформації розглядалися В. М. Бутузовим.

Проте, забезпечення кримінологічної безпеки у кіберпросторі не досліджувалось, що позначилося на низькому стані розроблення відповідного понятійно-категорійного апарату.

Серед проблем, що заважають створенню ефективно діючої системи протидії загрозам у кіберпросторі, дослідники виділяють термінологічну невизначеність. Відмічається, що першочерговим завданням є створення за участю зацікавлених відомств базового документу із визначеннями основних понять у кібербезпековій сфері — "кіберпростір", "кібербезпека", "кібератака", "кібернапад", "кіберзахист", "кібертероризм", "кіберзлочин". Слід погодитись з думкою дослідників про доцільність закласти ключові терміни кібербезпекової сфери (а заразом і сфери інформаційної безпеки в цілому) в нову редакцію Закону України "Про інформацію" [2].

Метою даної статті є розгляд системи понять, що відносяться до системи кримінологічної безпеки у кіберпросторі.

Аналіз наукових джерел дозволяє розглядати кримінологічну безпеку як один із видів юридичної безпеки, заснований на новітніх підходах у юридичних науках (перш за все, кримінології), до розгляду проблемних питань безпечного існування та розвитку людини, суспільства, держави, а також усунення неузгодженості цілей правоохоронної діяльності з інтересами окремої особи, суспільства, держави. Водночас, необхідність об'єктивного оцінювання результатів діяльності правоохоронних органів вимагає розробки на основі положень кримінологічної безпеки відповідних критеріїв оцінки стану захищеності життєво важливих прав та інтересів людини, суспільства, держави від кримінальних загроз.

Кримінологічну безпеку людини, суспільства, держави автор розглядає як об'єктивно-суб'єктивний стан захищеності життєво важливих прав та інтересів, людини, суспільства і держави від зовнішніх та внутрішніх кримінальних посягань і загроз таких посягань, який забезпечує умови реалізації цих прав та інтересів людини, функціонування й розвиток суспільства і держави [3, с. 219–220].

З огляду на те, що кіберпростір є, у певному сенсі, відображенням реального середовища, доцільно трансформувати основні поняття кримінологічної безпеки у реальному середовищі до потреб її забезпечення у віртуального середовищі (кіберпросторі).

Так, у системі кримінологічної безпеки у сфері комп'ютеризованої обробки інформації В. М. Бутузов виділяє найбільш суттєву її складову з точки зору державної безпеки – кібернетичну безпеку, під якою розуміє стан захищеності життєво важливих прав та інтересів людини, суспільства держави у кіберпросторі від внутрішніх та зовнішніх протиправних посягань та загроз таких посягань [4, с. 176].

Отже, кримінологічну безпеку людини, суспільства, держави у кіберпросторі пропонується розглядати як об'єктивно-суб'єктивний стан захи-

щеності їх життєво важливих прав та інтересів як у реальному, так і у віртуальному середовищі від зовнішніх та внутрішніх кримінальних посягань і загроз таких посягань, пов'язаних з використанням кібернетичних комп'ютерних систем. Даний стан забезпечує умови реалізації цих прав та інтересів людини, функціонування та розвиток суспільства і держави у кібернетичному просторі.

При цьому, враховуючи особливості функціонування кіберпростору, кримінологічну безпеку в ньому можна розглядати як кримінологічну кібербезпеку, а зазначені кримінальні посягання і загрози – як кримінальні кіберпосягання та кіберзагрози, стан захищеності – як стан кіберзахищеності.

Водночас, вважаємо, що не можна обмежувати поняття кібербезпеки (кібернетичної безпеки) лише середовищем її забезпечення — кіберпростором (кібернетичним простором). Слід ураховувати, що в основі поняття кібербезпеки все ж таки лежить використання кібернетичних систем: з одного боку, – для забезпечення захисту певних об'єктів кіберпростору; з іншого, – для готування вчинення кіберпосягання, реалізації кіберзагроз.

До структурних елементів кібербезпеки В. М. Бутузов відносить: державну політику щодо забезпечення кібербезпеки; державні й громадські інститути й організації, а також суб'єктів приватного сектору, що правомочні вживати заходів для забезпечення безпеки людини, суспільства й держави в кіберпросторі; засоби, способи й методи забезпечення кібербезпеки [4, с. 170].

Також, структурними елементами системи понять кримінологічної безпеки у кіберпросторі є: кримінальні кіберпосягання, кіберзагрози та їх джерела, об'єкти та суб'єкти кримінологічної кібербезпеки, забезпечення кримінологічної кібербезпеки, кіберзахист інформаційних об'єктів тощо.

Під кримінальними кіберпосяганнями слід розуміти кіберзлочини, перелік яких наведено у Конвенції Ради Європи про кіберзлочинність [5] і Додатковому протоколі до неї, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [6]. Хоча у даних актах не дається поняття кіберзлочину, аналіз їх положень дозволяє визначити кіберзлочини як злочини, пов'язані з несанкціонованим втручанням у роботу кібернетичних комп'ютерних систем чи протиправним використанням таких систем.

Водночас, слід ураховувати, що втручання в роботу кібернетичних комп'ютерних систем може здійснюватись як із середини такої системи, так і зовні. Причому, зовнішній злочинний вплив може здійснюватись і з реального середовища (наприклад, на технічні засоби, що забезпечують функціонування кіберпростору, його окремого елементу, окремого об'єкта кіберпростору).

Кримінальна кіберзагроза (кіберзагроза кримінального характеру) являє собою об'єктивно існуючу можливість учинення кіберзлочинів, у результаті чого можуть наступити несприятливі наслідки (завдання шкоди) як у реальному, так і віртуальному середовищі для життєво важливих інтересів об'єкта. Поняття кримінальної кіберзагрози також пов'язане з існуванням певних причин та умов як у реальному, так і віртуальному середовищі, що стимулюють, підвищують вірогідність учинення кіберзлочинів, а значить і ймовірність реалізації кримінальної кіберзагрози.

При цьому, слід відрізняти поняття "кримінальна кіберзагроза" та "кримінальна загроза об'єктам кіберпростору". Останнє є більш ширшим, тому що охоплює як внутрішні кримінальні загрози у кіберпросторі (кіберзагрози), так і зовнішні кримінальні загрози існуванню певного об'єкту кіберпростору (наприклад, на технічні засоби, що забезпечують його функціонування). Крім того, вбачається, що поняття кіберзагроз кримінального характеру є складовою значно ширшого поняття кіберзагроз, які можуть мати будь-який характер (воєнний, техногенний тощо).

Також, при розгляді феномену кримінологічної кібербезпеки доцільно звертатися й до її антитези – кримінологічної кібернебезпеки, під якою слід розуміти такий стан, при якому об'єктивно існуючі кримінальні кіберзагрози (наприклад, можливість учинення конкретного кіберзлочину або впливу на технічні засоби, що забезпечують функціонування кіберпростору) здатні завдати шкоди (збитків) життєво важливим правам та інтересам людини, суспільства, держави.

Аналіз наукових праць дозволяє розглядати джерела кримінальних кіберзагроз як фактори, здатні призвести до реалізації кримінальної кіберзагрози та завдання шкоди. До цих джерел слід віднести фізичних осіб, від яких можна очікувати вчинення кіберзлочинів – кіберзлочинців та осіб, схильних до вчинення кіберзлочинів.

У кримінальній кіберзагрозі можна виділити такі складові, що впливають на імовірність її реалізації: особистісні якості та суб'єктивні наміри кіберзлочинця (як основного джерела кримінальних кіберзагроз) та об'єктивні можливості реалізації такої загрози (наявність відповідних причин і умов, що сприяють збереженню або зростанню кіберзлочинності, а також осіб, від яких можна очікувати злочинів даного виду).

Об'єктом кримінологічної безпеки як у реальному, так і віртуальному середовищі є людина, суспільство, держава. Їх кримінологічна безпека у кіберпросторі забезпечується шляхом захисту від кримінальних посягань і загроз їх життєво важливим інтересам у кіберпросторі, до яких слід віднести: для людини – конституційні права і свободи щодо доступу до інформації та її використання; для суспільства — його духовні, морально-етичні, культурні, історичні, інтелектуальні цінності, інформаційні ресурси; для держави – її конституційний лад, суверенітет, недоторканність інформаційного простору.

При цьому, слід враховувати, що користувачі (особи, громадські організації, державні органи тощо) проявляються у кіберпросторі як певні інформаційні об'єкти. Тому, забезпечення кримінологічної кібербезпеки можна розглядати й як забезпечення безпечного існування відповідних інформаційних об'єктів кіберпростору, їх діяльності щодо використання його ресурсів та взаємодії з іншими об'єктами у віртуальному середовищі.

Серед суб'єктів забезпечення кримінологічної кібербезпеки можна виділити загальні та спеціальні. До загальних суб'єктів забезпечення кримінологічної безпеки можна віднести всі державні органи та громадські організації, діяльність яких у межах компетенції спрямована на протидію кіберзлочинності (в основному шляхом впливу на її детермінанти), до спеціальних суб'єктів – правоохоронні органи (як уповноважені на здійснення активного впливу на злочинність і злочинців у кіберпросторі).

Відповідно до чинного законодавства питання протидії зовнішнім і внутрішнім кібернетичним загрозам в Україні належать до компетенції Служби безпеки України, Міністерства внутрішніх справ України, Державної служби спеціального зв'язку та захисту інформації України. До зазначеної діяльності також залучатимуться Міністерство оборони України, Міністерство України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи, інші органи виконавчої влади. Крім того, у рамках Спільної робочої групи Україна-НАТО з питань воєнної реформи високого рівня у 2009 році утворено робочу підгрупу з питань кіберзахисту [7].

На думку В. М. Бутузова, поняття кібербезпеки тісно пов'язане з поняттям "забезпечення кібербезпеки", під яким він пропонує розуміти засновану на принципах комплексного прогнозування і планування діяльність держави, суспільства в цілому та їх інститутів, що має за мету досягнення та підтримання соціально прийнятного рівня захищеності життєво важливих та інших інтересів людини суспільства держави від злочинних посягань у кіберпросторі. Система забезпечення кібербезпеки розглядається ним як сукупність суб'єктів забезпечення кібербезпеки, заходів політичного, правового, організаційного, наукового та іншого характеру, спрямованих на підтримку соціально прийнятного рівня кібербезпеки, а також фінансове, ресурсне та інше забезпечення реалізації цих заходів [4, с. 170–177].

Автор пропонує більш ширше визначення поняття забезпечення кримінологічної кібербезпеки — як діяльності уповноважених суб'єктів щодо досягнення та утримання соціально прийнятного рівня захищеності життєво важливих прав та інтересів особи, суспільства й держави від кримінальних загроз у кіберпросторі. Змістом цієї діяльності є здійснення як у реальному, так і у віртуальному середовищі відповідного впливу на кримінальні кіберзагрози (джерела цих загроз) об'єктам захисту з метою їх мінімізації та усунення. Здійснення впливу на кримі-

нальні кіберзагрози (джерела цих загроз) передбачає реагування як на детермінанти кіберзлочинності, так і на конкретні акти її прояву.

Також, забезпечення кримінологічної кібербезпеки доцільно розглядати як реакцію суб'єкта на виявлені загрози (джерела загроз), що полягає у використанні відповідних прийомів, засобів, знарядь, різних видів ресурсів, спрямованих на досягнення та забезпечення соціально прийнятного рівня захищеності життєво важливих прав та інтересів об'єктів у кіберпросторі від кримінальних посягань і загроз цих посягань.

Водночас, під кримінологічним кіберзахистом об'єктів пропонується розуміти систему заходів правового, організаційного, ресурсно-фінансового, програмно-технічного та іншого характеру, спрямовану на створення умов, за яких виключаються або суттєво утрудняються злочинні посягання на об'єкти такого захисту (певні інформаційні об'єкти кіберпростору). Забезпечення кримінологічного кіберзахисту — це діяльність у кіберпросторі з охорони певних його об'єктів від злочинних посягань (кіберзлочинів) і створення перешкод у реалізації кіберзагроз кримінального характеру.

Аналіз наукових джерел дозволяє визначити такі рівні кримінальної кібербезпеки людини, суспільства, держави:

— соціально прийнятний рівень кримінологічної кібербезпеки, коли користувачі кіберпростору (людина, суспільні та державні інститути) відчувають себе достатньо захищеними від кримінальних кіберпосягань і кіберзагроз, при якому забезпечуються безпечні умови існування відповідних інформаційних об'єктів у кіберпросторі, що дозволяє найбільш повно реалізувати людині свої життєво важливі права та інтереси, успішно функціонувати й розвиватися суспільству та державі;

— рівень відносної кримінологічної кібербезпеки, що створює складності функціонування відповідних об'єктів у кіберпросторі, що не дозволяє у повному обсязі реалізувати людиною свої життєво важливі права та інтереси, перешкоджає нормальному функціонуванню інститутів суспільства й держави у кіберпросторі;

— рівень недостатньої кримінологічної кібербезпеки, що не дозволяє користувачам кіберпростору благополучно реалізувати свої життєво важливі права та інтереси, призводить до стагнації, застою діяльності суспільства й держави у кіберпросторі;

— рівень низької кримінологічної кібербезпеки, коли користувачі кіберпростору (людина, інститути суспільства та держави) не відчувають себе захищеними від кримінальних кіберпосягань і кіберзагроз, що не забезпечує безпечних умов користування кіберпростором, що граничить із повною відсутністю можливості у людини реалізувати свої життєво важливі права та інтереси, веде до деградації діяльності інститутів суспільства й держави у кіберпросторі.

У запропонованій системі понять сфери кримінологічної безпеки у кіберпросторі було зроблено спробу критично осмислити наведену

в різних літературних джерелах термінологію та представити її як можливу основу, в рамках якої можна продовжувати подальшу роботу щодо формування розгорнутої термінології сфери протидії кіберзлочинності.

Систематизація понять кримінологічної безпеки у кіберпросторі має не тільки теоретичне, а й прикладне значення для вдосконалення організації боротьби з кіберзлочинністю, розмежуванню компетенції суб'єктів цієї боротьби, визначення змісту заходів боротьби з кіберзлочинності.

### *Список використаних джерел*

1. Погорецький М. А. Поняття кіберпростору як середовища вчення злочину / М. А. Погорецький, В. П. Шеломенцев // Інформаційна безпека людини, суспільства, держави : наук.-практ. журнал. — К. : НАСБУ. — 2009. — № 2 (2). — С. 77–81.

2. Сучасні тренди кібербезпекової політики : висновки для України : аналітична записка Нац. ін-ту стратегічних досліджень при Президентові України [Електронний ресурс]. — Режим доступу : http://www. niss. gov. ua/articles/294/.

3. Шеломенцев В. П. Безпека людини, суспільства і держави в Україні : кримінологічний аспект / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика) : наук.-практ. журнал ; Міжвід. наук.-досл. центр з проблем б-би з орг. злоч. при РНБО України. — 2010. — № 22. — С. 215–222.

4. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : [монографія] / В. М. Бутузов. — К. : КИТ, 2010. — 408 с.

5. Про кіберзлочинність : Конвенція Ради Європи // Офіц. вісник України. — 2007. — № 65. — С. 107. — Ст. 2535. — Код акту 40846/2007. — 10 верес.

6. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи // Офіц. вісник України. — 2006. — № 31. — С. 29. — Ст. 2202. — 16 серп.

7. Про затвердження Річної національної програми на 2010 рік з підготовки України до набуття членства в Організації Північноатлантичного договору : Указ Президента України від 3 лют. 2010 р. № 92/2010 // Урядовий кур'єр. — 2010. — № 30. — 17 лют.

*Статья посвящена рассмотрению проблемных вопросов разработки категориально-понятийного аппарата криминологической безопасности в киберпространстве.*

*The article is devoted to the consideration of the problems concerning the development of the category-concept mechanism of the criminology safety in the cyberspace.*

*Стаття надійшла до редакції журналу 21 грудня 2010 року.*