are a number of differences between the concepts of «site inspection» and «housing inspection». There are some gaps, which in the course of investigative (search) actions on the territory of places of temporary isolation can lead to violation of the rights and freedoms of individual participants in criminal proceedings, among which are: security issues of all participants in the scene; compliance with the preservation of investigative and confidential information by all participants in the review; belonging to the evidence seized during the inspection of the scene in places of temporary isolation. The multidisciplinary issues of conducting an inspection of the scene and the need to standardize a single procedure for conducting this investigative (search) action on the territory of «places of temporary isolation» with the solution of the above problems.

The article emphasizes that certain provisions in scientific and practical activities, in our opinion, need to be standardized in the issue of inspection in places of temporary isolation the following aspects: preservation of information and information that will become known during the investigative (investigative) action (including, personal information of each of the participants), in particular the system using the system “Custody Records”, and the further admissibility of this evidence in criminal proceedings, which will be found during the inspection of the scene. Also, it should be noted that the legislator did not establish a term that would generalize and give the most approximate definition of places of detention.

Key words: procedural actions and decisions, inspection of the scene, place of imprisonment.

DOI: 10.36695/2219-5521.4.2020.72

УДК 004.056.5:378.1 (045)

І.О. ХАРИТОНЕНКО

*Ігор Олександрович Харитоненко, аспірант
Київського університету права НАН України**

ORCID: 0000-0002-1772-2312

ФЕНОМЕН КІБЕРЗЛОЧИННОСТІ В СУЧАСНІЙ КРИМІНОЛОГІЧНІЙ ТЕОРІЇ

Постановка проблеми. Питання формування системи забезпечення кібернетичної та інформаційної безпеки України є надзвичайно актуальним, адже інформаційні технології потенційно можуть бути використані як з метою забезпечення міжнародної стабільності й безпеки, так і з метою протилежною, спрямованою на примноження нових викликів. Масштаб загроз інформаційному простору не обмежується кордонами однієї держави, оскільки сучасні глобальні комп'ютерні мережі охоплюють переважну більшість країн світу, що додатково сприяє різкому підвищенню кримінального комп'ютерного професіоналізму та високої мобільності злочинців. Тому своєчасним є дослідження та аналіз системи швидкозмінних високотехнологічних кібернетичних загроз, тактики взаємодії у сфері інформаційної безпеки, яка впливає на формування сталого розвитку суспільства, на функціонування механізмів протидії інформаційним загрозам з урахуванням сучасних реалій.

Аналіз останніх досліджень та публікацій. Дослідженню феномена кіберзлочинності присвячено чимало наукових праць вітчизняних і зарубіжних фахівців у галузі кримінального права, кримінології, криміналістики, психології тощо. Зокрема, ця проблематика розглядалась у працях Д.С. Азарова, О.А. Баранова, П.Д. Біленчука, В.В. Василевича, А.А. Васильєва, В.О. Глушкова, В.О. Голубєва, Р.А. Калюжного, М.В. Карчевського, М.М. Коваленка, М.Й. Коржанського, М.О. Кравцової, В.В. Крилова, П.С. Матишевського, М.І. Мельника, А.А. Музики, В.О. Навроцького, В.В. Сташиса, Є.Л. Стрельцова, В.Я. Тація, М.І. Хавронюка та інших. Однак, не зважаючи на наявність значного масиву напрацювань із означеного напрямку, слід зауважити, що подальшого дослідження та висвітлення потребують питання щодо розробки науково обґрунтованої системи заходів запобігання кіберзлочинності на основі її сучасної кримінологічної характеристики. Важливими є дослідження з вивчення особи кіберзлочинця, вдосконалення вітчизняного законодавства у сфері охорони державної таємниці та службової інформації, міжнародної взаємодії у сфері забезпечення інформаційної безпеки, покращання змісту вищої освіти фахівців з інформаційної безпеки держави.

Формулювання мети статті. З огляду на викладене, метою цієї статті є дослідження феномена кіберзлочинності крізь призму показників, що її характеризують, зокрема рівень, динаміку, структуру, а також визначення соціальної обумовленості та основних тенденцій з урахуванням різнобічних чинників, які впливають на зміну кількісних та якісних показників.

Виклад основного матеріалу. Поняття «кіберзлочинність» часто вживається поряд із поняттями «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій», «високотехнологічна злочинність». Серед вищезазначених термінів поняття «кіберзлочинність» є найширшим та охоплює найбільше коло злочинних посягань у віртуальному середовищі, також його використання регулює міжнародне законодавство¹.

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 грома-

дянина, 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 кібербезпеки². У законі дається визначення наступних термінів:

- кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

- кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

- кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

- кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості й надійності функціонування комунікаційних, технологічних систем;

- кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

- кіберзлочинність – сукупність кіберзлочинів.

Проте, як зазначають науковці, очевидно, що на сьогодні бракує як високих технологій, так і належних світових стандартів і методологій з кібербезпеки. Нині фактично відсутня імплементація реальних заходів кіберзахисту в IT-інфраструктурах, слабкий процес навчання і підвищення обізнаності в питаннях кібербезпеки. Очевидно, що закони – це не якась окрема від всіх нас сутність. Їх виконання – це наш головний обов'язок³.

Серед характерних ознак показників кіберзлочинності виокремлюють: стабільне зростання частки тяжких злочинів, груповий характер їх вчинення, а також рецидив злочинів, залежність географії поширення від фактору урбанізації. Відтак, і самі посягання характеризуються, по-перше, специфічною, комбінаційно-цифровою, обстановкою кіберпростору, по-друге, технологічно, системно-технічно та програмно визначеною операційною складовою кримінальної активності, спрямованою на віртуальні компоненти суспільних відносин, спричинення істотної шкоди яким знаходить свій опосередкований прояв у реальній дійсності. Рівень латентності кіберзлочинів становить близько 95 %, що дає змогу віднести їх до категорії високолатентних. Серед факторів їх латентності виділено три основні групи: 1) фактори, що зумовлюють природну латентність, в силу яких про вчинений кіберзлочин відомо лише самому винному; 2) фактори, пов'язані з негативною поведінкою жертви (очевидців) злочину та їх незверненням до правоохоронних органів, неповідомленням про факт вчинення злочину; 3) фактори, пов'язані з недоліками роботи правоохоронних органів у частині реагування на звернення та повідомлення про кіберзлочини: а) пов'язані з помилками при прийнятті працівниками правоохоронних органів рішень щодо наявності чи відсутності у вчиненому діянні складу злочину або щодо його кваліфікації; б) пов'язані з приховуванням злочинів від обліку. Також існує проблема невідповідності судової практики щодо призначення покарань за кіберзлочини характеру й ступеня їх суспільної небезпечності. У переважній більшості засуджені особи звільняються судом від кримінальної відповідальності; в половині випадків призначається більш м'яке покарання, ніж передбачено законом; лише в незначній кількості випадків суд призначає додаткове покарання у виді конфіскації майна (3 %). Аналіз географії кіберзлочинів в Україні виявив залежність її поширення від фактору урбанізації. Найвища кіберкримінальна активність фіксується в Дніпропетровській області, місті Києві, а також Харківській, Запорізькій та Черкаській областях. Найнижча – у Чернівецькій, Херсонській, Сумській, Кіровоградській областях. Крім того, слід відзначити випадки реєстрації кіберзлочинів на залізниці (Одеська залізниця), що засвідчує поступову експансію кіберзлочинності на більшість сфер життєдіяльності нашого суспільства⁴.

Основними ознаками кіберзлочинності є те, що: 1) кіберзлочини вчиняються у віртуальному просторі або в межах комп'ютерних мереж. Віртуальний простір – це модульований за допомогою комп'ютера інформаційний простір, в якому містяться дані про осіб, факти, явища, процеси, представлені в математичному, символічному чи іншому вигляді. Ці відомості знаходяться в процесі руху локальними і глобальними комп'ютерними мережами, зберігаються в пам'яті будь-якого фізичного або віртуального пристроїв, спеціально призначених для їх зберігання, переробки та передачі. Крім того, кіберзлочини можуть вчинятися за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

Таким чином, електронно-обчислювана техніка може бути як засобом вчинення, так і предметом злочину; 2) кіберзлочинність має інтелектуальний характер – здійснення кіберзлочину вимагає певного набору знань. Крім того, інтелектуальність серед кіберзлочинців пропагується субкультурою хакерів, що дає їм стимул до розумового саморозвитку; 3) кіберзлочини, на відміну від інтелектуальних злочинів, доступні людям невисоких соціальних і вікових можливостей; 4) кіберзлочини є анонімними та неперсоніфікованими; 5) злочинця та жертву можуть розділяти тисячі кілометрів (віддаленість кіберзлочинів); 6) збиток від кіберзлочину часто здається жертві незначним порівняно з процедурою розслідування, яка здатна забрати час, але не гарантує притягнення до відповідальності винного та компенсації збитку (висока латентність кіберзлочинності)⁵.

Висновки. У час глобалізації та електронних комунікацій однією з нагальних проблем є проблема кібербезпеки. Виходячи з вищенаведеного, можна виокремити наступні ознаки феномена кіберзлочинності крізь призму показників, що її характеризують:

- масштаб загроз інформаційному простору не обмежується кордонами однієї держави;
- зміна кількісних та якісних показників кіберзлочинності, зокрема різке підвищення кримінального комп'ютерного професіоналізму та високої мобільності злочинців;
- рівень кіберзлочинності тісно пов'язаний з економічним рівнем розвитку суспільства в різних державах та регіонах;
- кібернетичні загрози швидкозмінні та високотехнологічні;
- високий рівень латентності;
- залежність географії поширення від фактору урбанізації;
- кіберзлочинність – це соціальне явище, що проявляється в сукупності кіберзлочинів.

Також слід зазначити, що з метою попередження даних злочинів необхідне подальше проведення досліджень соціального та кримінологічного напрямку щодо вивчення психофізіологічних властивостей кіберзлочинців, вдосконалення вітчизняного законодавства у сфері охорони державної таємниці та службової інформації, міжнародної взаємодії у сфері забезпечення інформаційної безпеки, поліпшення змісту вищої освіти фахівців з інформаційної безпеки держави.

¹ Іванченко О.Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. № 3. С. 172–177.

² Про основні засади забезпечення кібербезпеки України: Закон України. *Відомості Верховної Ради (ВВР)*. 2017. № 45. Ст. 403.

³ Біленчук П.Д., Обіход Т.В. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму. *Часопис Київського університету права*. 2018. № 3. С. 235–239.

⁴ Кравцова М.О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. ... канд. юрид. наук. Харків, 2016. 19 с.

⁵ Голіна В.В., Головін Б.М. Кримінологія: загальна та особлива частини: навч. посіб. Харків: Право, 2014. 513 с.

Резюме

Харитоненко І.О. Феномен кіберзлочинності в сучасній кримінологічній теорії.

У статті розглянуто поняття та ознаки кіберзлочинності, досліджено феномен кіберзлочинності крізь призму показників, що її характеризують, зокрема рівень, динаміку, структуру. Визначено соціальну зумовленість та сучасний стан з урахуванням різнобічних чинників, які впливають на зміну кількісних та якісних показників. Підкреслено глобалізм, високий рівень суспільної небезпеки і масовість наслідків кібернетичних загроз.

Ключові слова: кібербезпека, інформаційний простір, кіберзлочинність, національна безпека, кіберзагроза, держава, інформаційна безпека, кримінологічна характеристика.

Резюме

Харитоненко И.А. Феномен киберпреступности в современной криминологической теории.

В статье рассмотрено понятие и признаки киберпреступности, исследован феномен киберпреступности через призму показателей, ее характеризующих, в частности уровень, динамику, структуру. Определены социальная обусловленность и современное состояние с учетом разносторонних факторов, влияющих на изменение количественных и качественных показателей. Подчеркнуто глобализм, высокий уровень общественной опасности и массовость последствий кибернетических угроз.

Ключевые слова: кибербезопасность, информационное пространство, киберпреступность, национальная безопасность, киберугрозы, государство, информационная безопасность, криминологическая характеристика.

Summary

Ihor Kharytonenko. The phenomenon of cybercrime in modern criminological theory.

The article considers the concepts and signs of cybercrime, the phenomenon of cybercrime through the prism of indicators that characterize it, in particular the level, dynamics, structure. The social conditionality and the current state are determined taking into account various factors that influence the change of quantitative and qualitative indicators. Globalism, a high level of public danger and the massive consequences of cyber threats are emphasized.

It is pointed out that the scale of threats to the information space is not limited to the borders of one country, as modern global computer networks cover the vast majority of countries, which further contributes to a sharp increase in criminal computer profes-

nalism and high mobility of criminals. Therefore, it is timely to study and analyze the system of rapidly changing high-tech cyber threats, tactics of interaction in the field of information security, which affects the formation of sustainable development of society, the functioning of mechanisms to counter information threats taking into account modern realities.

The signs of the phenomenon of cybercrime through the prism of indicators that characterize it are highlighted:

- the scale of threats to the information space is not limited to the borders of one state;
- changes in the quantitative and qualitative indicators of cybercrime, in particular a sharp increase in criminal computer professionalism and high mobility of criminals;
- the level of cybercrime is closely related to the economic level of development of society in different countries and regions;
- cyber threats are fast-changing and high-tech;
- high level of latency;
- the dependence of the geography of distribution on the factor of urbanization;
- Cybercrime is a social phenomenon that manifests itself in a set of cybercrimes.

It is noted that in order to prevent these crimes it is necessary to conduct further research in social and criminological areas to study the psychophysiological properties of cybercriminals, improve domestic legislation in the field of state secrets and official information, international cooperation in information security, improve the content of higher education information security professionals states.

Key words: cybersecurity, information space, cybercrime, national security, cyberthreat, state, information security, criminological characteristics.

DOI: 10.36695/2219-5521.4.2020.73

УДК 343.41+343.451

А.О. ХЛОПОВ

*Артем Олександрович Хлопов, аспірант Харківського національного університету внутрішніх справ**

ORCID: 0000-0001-5342-9183

СУТНІСТЬ СТАЛКІНГУ ЯК СУСПІЛЬНО НЕБЕЗПЕЧНОГО ДІЯННЯ ТА РОЛЬ ІНФОРМАЦІЇ ПРИВАТНОГО ХАРАКТЕРУ З ОЗНАКАМИ ТАЄМНИЦІ У ФОРМУВАННІ ТАКТИКИ ПОВЕДІНКИ ПЕРЕСЛІДУВАЧА

Постановка проблеми. Ефективність правового регулювання напряду залежить від здатності закону адаптуватися до сучасних реалій суспільних відносин та відповідати на виклики сьогодення. В іншому випадку громадяни позбавляються можливості відстоювати свої права і свободи, а держава за відсутності відповідного правового інструментарію не здатна забезпечити правопорядок та безпеку. Одним із таких неврегульованих питань є відсутність профільного регулювання «переслідування», так званого «сталкінгу» з англ. – «stalking». Окремлене діяння є видом протиправної поведінки, що визнається формою домагання і залякування, характеризуючись непередбачуваністю наслідків. На жаль, в Україні проблемі сталкінгу майже не приділяється уваги, більше того, переслідування у більшості випадків не визнається протиправною поведінкою. Мовчить щодо цього і вітчизняний закон, адже в чинному Кримінальному кодексі України (далі – КК України), як і в усьому масиві законодавства, відсутнє відповідне правове регулювання. Немає й статистики щодо кількості осіб, які зазнали переслідування. Проте це не означає, що сталкінг як явище в Україні відсутнє – це означає лише, що українці не захищені з боку закону й залишені наодинці з кривдником. Особливо це стосується втручання в приватне життя людини, адже саме недоторканність цієї сфери насамперед. У результаті чого сталкером незаконно отримується інформація приватного характеру щодо різних аспектів життєдіяльності особи, яка надалі використовується кривдником у власних цілях, проти самого власника цієї інформації. Крім того, суспільна небезпека сталкінгу полягає в непередбачуваності наслідків, що виражаються в цілому спектрі проявів, у тому числі тяжких. Саме декілька гучних кримінальних справ, де жертвами виступили публічно відомі особи, спонукали законодавців ряду країн визнати сталкінг кримінально карним діянням. Справедливо вказати, що природа сталкінгу досі активно вивчається й по-різному трактується дослідниками, однак безперечним є факт прискіпливої уваги до цього діяння з боку наукової спільноти та законодавців західних країн. Однак попри всю складність сталкінг несе у собі значний рівень загрози, що закладає тренд на пошук шляхів протидії цьому діянню, у тому числі за допомогою проведення відповідної кримінально-правової політики.

Аналіз останніх досліджень і публікацій. Попри активну увагу та численні дослідження такого явища, як сталкінг за кордоном, з боку вітчизняних науковців ці питання майже повністю проходили повз них. Серед зарубіжних вчених доцільно згадати кількох із них, які внесли вагомий уклад у вивчення природи сталкінгу: С. Boyd, В. Bjerregaard, К.Е. Davis, J.R. Coleman, І.Н. Frieze, F.R. Farnham, Foster A. James,