Трибуна молодого науковця

УДК 343.9
DOI 10.33244/2617-4154.3(12).2023.309-317

А. В. Бенескул,
аспірант,
Державний податковий університет
e-mail: beneskula@gmail.com
ORCID ID 0009-0004-5315-3374

КРИМІНОЛОГІЧНА БЕЗПЕКА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: ПОНЯТТЯ, СУТНІСТЬ І ЗНАЧЕННЯ

Статтю присвячено дослідженню сутності, визначення і значення кримінологічної безпеки в умовах цифрової трансформації. Відзначається, що питання дослідження забезпечення безпеки людини, громадянського суспільства, держави загалом від різноманітних потужних можливостей сучасних цифрових та комп'ютерних технологій останнім часом відіграє досить вагому роль щодо забезпечення рівня кримінологічної безпеки.

Констатовано, що в період повномасштабного вторгнення росії в Україну питання безпеки загострилося найбільше, адже саме від її дотримання та забезпечення залежить життя громадян. Саме тому сучасні виклики все більше спонукають держави будувати безпечне майбутнє і дійсно розробляти ефективні заходи запобігання та нейтралізації численних загроз і забезпечення безпеки на різних її рівнях.

Метою дослідження є вивчення стану кримінологічної безпеки в умовах цифрової трансформації, а також її сутності і значення у кримінологічній науці.

У статті наголошується, що актуальність та прогресивність дослідження теорії кримінологічної безпеки викликані необхідністю формування нової ідеології протидії злочинності, переорієнтації правоохоронної системи з пошуків кримінологічних загроз (що видається вторинним) на реальне виконання основного завдання – забезпечення безпеки людей від злочинних посягань.

Відмічено, що постійна загроза кіберзлочинності сучасною та реальною. Широке використання цифрових технологій та інтернету в сучасному суспільстві привертає увагу кримінологів усе частіше, зокрема розширюється такий напрям у кримінології, як кіберкримінологія.

Доведено, той факт, що для того, щоб протистояти негативним проявам у мережі «Інтернет» та використовувати нові можливості, необхідно розуміти сутність та значення кібербезпеки, кіберзлочинності і загалом напрямів нових інформаційних технологій. Крім того, важливе значення має дослідження та вплив на такі напрями, як: середовище загроз кібербезпеки; потенційна вартість кібератаки для бізнесу для інших структур; оцінки ступеня безпеки підприємства, установи чи

організації; аналіз можливостей вчасно реагувати на негативні інциденти та способи використання нових цифрових технологій.

Автором наголошено у статті, що дослідження та вивчення теорії кримінологічної безпеки покликані сприяти визначенню основної її сутності, тобто захисту особи, суспільства та держави від такого негативного, антисоціального явища, як злочинність, тобто виокремлення тих головних цінностей, яким і гарантується на відповідному рівні кримінологічна безпека. Саме тому важливим та необхідним на рівні держави є ухвалення Стратегії кримінологічної безпеки України на 2023–2028 роки, адже це саме те завдання, яке повинно бути виконаним, щоб належно захистити права та свободи людини і громадянина від негативних посягань у кіберпросторі, з яким певним способом пов'язаний кожен громадянин нашої держави.

Ключові слова: *кіберзлочинність, кримінологічна безпека, кібербезпека, кібератака, кібершахрайство, цифрові технології, інформаційні технології, комп'ютерна злочинність, цифровізація, кримінологічна стратегія.*

Постановка завдання. Метою цього дослідження є вивчення стану кримінологічної безпеки в умовах цифрової трансформації, а також її сутності та значення у кримінологічній науці.

Постановка проблеми. Цифровізація у сучасному суспільстві полягає насамперед в інтеграції цифрових технологій у повсякденне життя. Застосування цифрових технологій, використання передових технологій та динаміки цифрових мереж, гігантського потоку інформації реалізовується у формі оновлення різноманітних процесів шляхом оцифрування. Саме тому цифровізація може бути застосована в багатьох галузях науки, включаючи, зокрема, гуманітарні та соціальні. Кримінально-правова наука серед гуманітарних і соціальних наук теж піддається впливу цифрової трансформації, адже кримінальне правосуддя останнім часом досить потужно зазнає впливу цифровізації та розвитку технологій.

Проблема забезпечення належного рівня безпеки громадянського суспільства, в яких би формах вона не виражалася (національна, суспільна, економічна, екологічна тощо), завжди залишається пріоритетною, оскільки від її вирішення залежить доля усієї цивілізації. На жаль, у період повномасштабного вторгнення росії в Україну питання безпеки загострилося найбільше, адже саме від її дотримання та забезпечення залежить життя громадян. Саме тому сучасні виклики все більше спонукають держави будувати безпечне майбутнє і розробляти ефективні заходи запобігання та нейтралізації численних загроз і забезпечення безпеки на різних її рівнях.

Серед таких загроз одне з перших місць сьогодення займає злочинність, яка суттєво гальмує цивілізоване реформування нашого суспільства. Загалом злочинність за своїми статистичними показниками становить не лише внутрішню небезпеку, але, що найгірше, загрожує інтересам міжнародної безпеки. Тому забезпечення відповідного контролю з боку державних органів, громадських організацій і громадян зокрема за злочинністю не може бути ефективним без вирішення проблеми безпеки особи, суспільства та загалом держави від злочинних посягань. Саме комплексність та повнота вказаного процесу і

зумовлює значення дослідження кримінологічної безпеки, особливо в сучасний стан цифрових технологій та використання різноманітних цифрових ресурсів.

Аналіз останніх досліджень і публікацій. Окремі аспекти дослідження, аналізу та вивчення кримінологічної безпеки загалом та безпеки у кіберпросторі зокрема були предметом досліджень у працях багатьох українських та закордонних учених, а саме: О. М. Бандурки [6], В. М. Бутузова [7], В. Д. Гавловського [8], О. М. Литвинова [9], Т. В. Мельничук [10], С. А. Мозоля [11], В. П. Шеломенцева [14;15] та інших, проте поряд з основними характеристиками кримінологічної безпеки досить важливим є дослідження стану забезпечення кримінологічної безпеки саме у сфері використання сучасних інформаційних та цифрових технологій, що й потребує ґрунтовного вивчення та дослідження.

Виклад основного матеріалу. У період переходу до інформаційного суспільства особливої актуальності набуває саме питання дослідження забезпечення безпеки людини, громадянського суспільства, держави загалом від різноманітних потужних можливостей сучасних цифрових та комп'ютерних технологій. Адже, як показує практика реального життя, вони можуть використовуватися не лише для підвищення і покращення якості життя людей, але й, на жаль, для порушення прав, свобод чи інтересів особи, а в окремих випадках, ще й нанесення шкоди суспільству, громадянам чи державі залежно від ситуації.

Тому все більшої підтримки серед науковців викликає необхідність застосування до цієї сфери концепції кримінологічної безпеки, що в останній період набуває особливої актуальності [8; 14; 15].

С. А. Мозолем наведено формулювання визначення системи забезпечення кримінологічної безпеки, яку він визначає як організовану на державному рівні сукупність суб'єктів (до яких він відносить посадових осіб та окремих громадян, громадських організацій, державних органів), які об'єднані спільними завданнями та цілями, що здійснюють узгоджену діяльність, відповідно до законодавства України, з метою захисту важливих інтересів особи, суспільства та держави від кримінального впливу злочинності та для підтримання соціально допустимого рівня забезпечення кримінологічної безпеки. Також ним наводиться система аргументів, які покладені в обґрунтування концепції багатовимірного комплексу основних об'єктів кримінологічної безпеки, до яких належать: особа – її права, обов'язки та свободи; суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності; держава – її конституційний устрій, суверенітет і територіальна цілісність та недоторканість; цивілізація – сукупність духовних сфер, культурних і матеріальних цінностей та форм організації управління суспільством [12, с. 5].

Отже, під кримінологічною безпекою в широкому розумінні слова можна визначити сукупність політичних, ідеологічних, економічних, соціально-психологічних, правових та інших заходів, що розробляються і здійснюються компетентними державними та громадськими структурами, а також громадянами щодо попередження злочинних посягань на права особи, суспільства та держави загалом.

Актуальність і прогресивність дослідження теорії кримінологічної безпеки викликані необхідністю формування нової ідеології протидії злочинності, переорієнтації

правоохоронної системи з пошуків кримінологічних загроз (що видається вторинним) на реальне виконання основного завдання – забезпечення безпеки людей від злочинних посягань. У цьому випадку не можна не помітити, що поняття «забезпечення кримінологічної безпеки» та «кримінологічна безпека» відображають, з одного боку, специфіку діяльності (функціональний критерій), з іншого – мету та результат останньої (оціночний критерій), яким є, власне, стан кримінологічної безпеки певного об'єкта.

Значення та необхідність Стратегії кримінологічної безпеки обґрунтовує також і О. М. Литвинов: «Кримінологічна стратегія надає функціонуванню механізму протидії злочинності планомірності, стабільності, спрямованості, також забезпечує послідовність і безпосередність розробки завдань діяльності та їх диференціацію за рівнями та сферами застосування. Вона вбирає в себе фундаментальні надбання науки та новітні форми організації практичної сторони справи, виступає певною платформою для довгострокових і перспективних планів діяльності окремих суб'єктів, чітко визначає засоби, у тому числі обумовлені специфікою дії механізмів реалізації довгострокової кримінологічної політики» [9, с. 138].

Отже, з огляду на концепцію комплексної кримінологічної безпеки її забезпечення має перевищувати характер та спрямованість криміногенних і кримінальних загроз. Тому в ієрархії форм діяльності із забезпечення кримінологічної безпеки на першому місці стоїть саме захист від джерела загрози безпеці, а вже потім вплив на саме джерело. Хоча, зрозуміло, не можна виключати паралельності у здійсненні названих форм діяльності. Тому проблема кримінологічної безпеки набуває сьогодні принципово нового теоретичного та практичного значення для здійснення державної політики у сфері контролю над злочинністю, дає імпульс для оновлення існуючих у цій галузі наукових ідей.

Не потрібно ототожнювати поняття державної безпеки з поняттям «кримінологічна безпека», адже перше поняття є набагато ширшим та закріпленим на законодавчому рівні.

Так, відповідно до Стратегії забезпечення державної безпеки забезпечення державної безпеки – це створення умов для забезпечення захищеності державного суверенітету, територіальної цілісності та демократичного конституційного ладу й інших життєво важливих національних інтересів від реальних і потенційних загроз Україні. Державна політика у сфері державної безпеки спрямовується на попередження, своєчасне виявлення та запобігання зовнішнім і внутрішнім загрозам державній безпеці України, припинення розвідувальних, терористичних, диверсійних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що призводять до цих загроз і причин їх виникнення [13].

Поряд із забезпеченням кримінологічної безпеки загалом варто її розглядати і з погляду окремих сфер. Так, особливо принципового значення має дотримання належного її рівня забезпечення у сфері цифрових технологій, адже розвиток інформатизації та комп'ютеризації постійно розвивається, удосконалюється, що ставить і нові виклики перед державними та громадськими органами для оперативного реагування на прояви її порушення.

Кіберзлочинність – це загальний термін для незаконної діяльності, яка відбувається в інтернеті або коли цифрові технології виступають способом чи засобом вчинення таких кримінальних правопорушень. На сьогодні це один із найшвидше зростаючих кримінальних правопорушень у світі, який впливає на більшість підприємств. За даними Risk IQ, кіберзлочинність коштує світовій економіці 2,3 мільйона фунтів стерлінгів за хвилину [5]. Якщо зазначати більш точно, то сектор фінансових послуг незмінно є однією з найбільш поширених галузей, на які полюють кібершахраї [2]. У Великій Британії майже половина підприємств (46 %) і чверть благодійних організацій (26 %) повідомили про порушення кібербезпеки або атаки за 2020 рік. Характер кібератак також змінився з 2017 року. За цей період було зафіксовано зростання кількості компаній, які стикаються з фішинговими атаками (з 72 до 86 %), а також загрози поширення вірусів або інших шкідливих програм (з 33 до 36 %) [1].

Тож постійна загроза кіберзлочинності є сучасною та реальною. Широке використання цифрових технологій та інтернету в сучасному суспільстві привертає увагу кримінологів усе частіше, зокрема розширюється такий напрям у кримінології як кіберкримінологія. Кіберкримінологія є майже новою міждисциплінарною галуззю дослідження кримінологічної науки, яка направлена на дослідження проблеми комп'ютерної злочинності. З розвитком технологій і науки злочинність і кримінальна поведінка, як наслідок цьому, теж змінюються, тому необхідно вчасно реагувати та протидіяти проявам кримінальних правопорушень у цій сфері.

Кіберзлочинність включає у себе злочинну діяльність з використанням технологій і цифровізації, які складаються з протиправних дій щодо доступу до інформації, її перехоплення чи пошкодження даних, втручання в роботу комп'ютерної системи чи пристрою тощо.

Кіберпростір усе частіше стає новим місцем для вчинення кримінальних правопорушень, тому забезпечення належного рівня кримінологічної безпеки в умовах цифрової трансформації є одним з першочергових завдань правоохоронних органів.

Як стверджує Джайшанкар, засновник кіберкримінології, «кримінологія раніше не надавала важливого значення феномену кіберзлочинності та важливості дослідження кіберпростору, проте зі зміною природи, масштабів та загалом віктимізації у галузі цифрових технологій, кіберзлочинність стала міждисциплінарною галуззю і включає в себе дослідження причинно-наслідкового зв'язку кримінальних правопорушень, що вчиняються в кіберпросторі, та його впливу на фізичний простір особи» [4]. Крім того, генеральний директор ITRS Group Гай Уоррен зазначив: «Перехід до «цифрового бізнесу» збільшує кількість точок входу в IT-системи та даних різних компаній. Злочинці знайдуть точку найменшого захисту, зокрема, через мобільні додатки, щоб отримати все більше точок входу на різні портали» [3].

Підприємства, установи, організації і просто фізичні особи прагнуть стимулювати свій розвиток, ефективність і головне фінансову віддачу та все частіше роблять це з використанням цифрових технологій. Але з цим виникає безліч ризиків, на які необхідно вчасно реагувати та запобігати. Адже нові технології та цифрова еволюція також створюють нові можливості для кримінальних правопорушень, оскільки світ

цифрових технологій надає різноманітні можливості злочинцям щодо удосконалення злочинних способів доступу до цінної інформації, отримання несанкціонованого доступу до інформації про різноманітні компанії та клієнтів, витоку персональних даних, комерційної таємниці тощо.

Висновки. Отже, на сучасному етапі розвитку цифрових технологій, коли світ постійно удосконалюється та стає все більш цифровим, продовжує зростати потреба в застосуванні і нових технологій, щоб зуміти забезпечити себе належним рівнем у цьому цифровому середовищі. Саме тому питання кримінологічної безпеки в сучасному світі цифрових трансформацій набуває все більш актуального характеру, тому дослідження вказаної проблематики є досить важливим, а головне необхідним.

Адже навички та знання, які необхідні сьогодні, швидко розвиваються. Тому важливо, щоб підприємства, установи та організації забезпечували свій персонал необхідним практичним навчанням, щоб допомогти їм бути в безпеці у кіберпросторі. Тому відмінне розуміння нових технологій і кібербезпеки потрібне не лише ІТ-відділам, а загалом кожен користувач мережею «Інтернет» має бути захищеним від кібершахрайств. Потрібно, щоб інші розуміли наслідки та можливості роботи в цифровому світі для зменшення загальних ризиків та ефективного використання цифрових технологій, щоб не потрапити на кібершахраїв.

Отже, щоб протистояти негативним проявам у мережі «Інтернет» та використовувати нові можливості, необхідно розуміти сутність і значення кібербезпеки, кіберзлочинності і загалом напрямів нових інформаційних технології. Крім того, важливе значення має дослідження та вплив на такі напрями, як: середовище загроз кібербезпеки; потенційна вартість кібератаки для бізнесу для інших структур; оцінки ступеня безпеки підприємства, установи чи організації; аналіз можливостей вчасно реагувати на негативні інциденти та способи використання нових цифрових технологій.

Враховуючи вказані положення, віктимізація кіберправопорушень останнім часом набуває все більшого поширення, тому доцільним, на нашу думку, є дослідження кіберзлочинності не лише щодо форм і способів їх вчинення та заходів запобігання, а ще й з точки зору жертви цих видів правопорушень, тобто з погляду кібервіктимізації та виокремлення окремої галузі віктимології – кібервіктимології.

Дослідження та вивчення теорії кримінологічної безпеки покликані сприяти визначенню основної її сутності, тобто захисту особи, суспільства та держави від такого негативного, антисоціального явища, як злочинність, тобто виокремлення тих головних цінностей, яким і гарантується на відповідному рівні кримінологічна безпека. Саме тому важливим та необхідним на рівні держави, вважаємо, є прийняття Стратегії кримінологічної безпеки України на 2023–2028 роки, адже це саме те завдання, яке повинно бути виконаним, щоб належно захистити права та свободи людини і громадянина від негативних посягань у кіберпросторі, з яким певним способом пов’язаний кожен громадянин нашої держави. Тому розробка, прийняття та затвердження вказаної Стратегії кримінологічної безпеки України на державному рівні надасть законодавчого дотримання належного рівня кримінологічної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cyber Security Breaches Survey 2020. Department for Digital, Culture, Media and Sport Cyber Security Breaches Survey 2020: Statistical Release. URL : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf (дата звернення: 03.05.2023).

2. Global Threats Report. URL : https://jp.security.ntt/ (дата звернення: 03.05.2023).

3. Guy Warren. URL : https://uk.linkedin.com/in/guy-warren-itrs (дата звернення: 03.05.2023).

4. Jaishankar K. Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*. Vol 1. Issue 2. July 2007. URL : https://www.cybercrimejournal.com/pdf/Editoriaijccjuly.pdf (дата звернення: 03.05.2023).

5. RiskIQ «The Evil Internet Minute». 2019. URL : https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-threat-intelligence (дата звернення: 03.05.2023).

6. Бандурка О. М., Литвинов О. М. Стратегія і тактика протидії злочинності : монографія. Харків : Видавництво «Золота миля», 2012. 287 с.

7. Бутузов В. М. Протидія комп'ютерній злочинності в Україні: (системно-структурний аналіз) : монографія / Рада національної безпеки і оборони України, Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю. Київ : КИТ, 2010. 407 с.

8. Гавловський В. Д., Бутузов В. М. Протидія організованій злочинності у сфері інформаційних технологій як окремий аспект кримінологічної безпеки. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. Вип. 22. С. 236–246.

9. Литвинов О. М. Кримінологічна стратегія як компонент стратегії національної безпеки України. *Право і безпека* : науковий журнал. 2010. № 3. С. 137–141.

10. Мельничук Т. В. Кримінологічна безпека економічної діяльності : навч.-метод. посібник / ред. : Є. Л. Стрельцов, Л. І. Аркуша ; НУ «ОЮА». Одеса : Гельветика, 2018. 96 с.

11. Мозоль С. А. Кримінологічна безпека в Україні : монографія. Харків : Константа, 2018. 482 с.

12. Мозоль С. А. Кримінологічна безпека в Україні: феномен та наукові засади забезпечення : автореф. дис. на здобуття наук. ступеня д-ра юрид. наук (д-ра наук) : 12.00.08 / МВС України, Харк. нац. ун-т внутр. справ. Харків, 2018. 37 с.

13. Стратегія забезпечення державної безпеки : Указ Президента України від 16 лютого 2022 року № 56/2022. URL : https://www.president.gov.ua/documents/562022-41377 (дата звернення: 03.05.2023).

14. Шеломенцев В. П. Безпека людини, суспільства і держави в Україні: кримінологічний аспект. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2009. № 22. С. 215–222.

15. Шеломенцев В. П. Кримінологічна безпека у кіберпросторі: система понять. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. № 23. С. 342–348.

REFERENCES

1. Cyber Security Breaches Survey 2020. Department for Digital, Culture, Media and Sport Cyber Security Breaches Survey 2020: Statistical Release. URL : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf (access date: 03.05.2023).

2. Global Threats Report. URL : https://jp.security.ntt/ (дата звернення: 03.05.2023).

3. Guy Warren. URL : https://uk.linkedin.com/in/guy-warren-itrs (access date: 03.05.2023).

4. Jaishankar K. Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*. Vol 1. Issue 2. July 2007. URL : https://www.cybercrimejournal.com/pdf/Editoriaijccjuly.pdf (access date: 03.05.2023).

5. RiskIQ «The Evil Internet Minute». 2019. URL : https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-threat-intelligence (access date: 03.05.2023).

6. Bandurka O. M., Litvinov O. M. Crime prevention strategy and tactics : monograph. Kharkiv : Publishing house Golden Mile, 2012. 287 p.

7. Butuzov V. M. Combating computer crime in Ukraine: (systemic and structural analysis) : monograph. Council of National Security and Defense of Ukraine / Inter-departmental Research Center on Combating Organized Crime. Kyiv : WHALE, 2010. 407 p.

8. Havlovsky V. D., Butuzov V. M. Combating organized crime in the field of information technologies as a separate aspect of criminological security. *Fight against organized crime and corruption (theory and practice).* 2010. Issue 22. P. 236–246.

9. Litvinov O. M. Criminological strategy as a component of the national security strategy of Ukraine. *Law and security* : Scientific journal. 2010. No. 3. P. 137–141.

10. Melnychuk T. V. Criminological security of economic activity : *educational method. Manual* / rec. : E. L. Streltsov, L. I. Arkusha ; NU "OYUA". Odesa : Helvetica, 2018. 96 p.

11. Mozol S. A. Criminological security in Ukraine : monograph. Kharkiv : Constanta, 2018. 482 p.

12. Mozol S. A. Criminological security in Ukraine: phenomenon and scientific principles of security: autoref. thesis doctor of law Sciences (Dr. Sciences): 12.00.08. Ministry of Internal Affairs of Ukraine, Kharkiv. national University of Internal Affairs affairs Kharkiv, 2018. 37 p.

13. Strategy for ensuring state security. Decree of the President of Ukraine dated February 16, 2022 No. 56/2022. URL : https://www.president.gov.ua/documents/562022-41377 (date of application: 05.03.2023).

14. Shelomentsev V. P. Security of man, society and the state in Ukraine: criminological aspect. *Fight against organized crime and corruption (theory and practice).* 2009. No. 22. P. 215–222.

15. Shelomentsev V. P. Criminological security in cyberspace: a system of concepts. *Fight against organized crime and corruption (theory and practice).* 2010. No. 23. P. 342–348.

A. Beneskul. Criminology security in the conditions of digital transformation: concept, essence and meaning

The article is devoted to the study of the essence, definition and meaning of criminological security in the conditions of digital transformation. It is noted that the research issue of ensuring the safety of people, civil society, and the state in general from the various powerful capabilities of modern digital and computer technologies has recently played a rather important role in ensuring the level of criminological security.

It was established that during the full-scale invasion of Russia into Ukraine, the issue of security became the most acute, because the lives of citizens depend on its observance and provision. That is why modern challenges increasingly encourage states to build a safe future and really develop effective measures to prevent and neutralize numerous threats and ensure security at various levels.

The purpose of the study is to study the state of criminological security in the conditions of digital transformation, as well as its essence and significance in criminological science.

The article emphasizes that the relevance and progressiveness of the study of the theory of criminological security is caused by the need to form a new ideology of combating crime, to reorient the law enforcement system from the search for criminological threats (which seems to be secondary) to the real implementation of the main task - ensuring the safety of people from criminal encroachments.

It has been noted that the constant threat of cybercrime is very present and very real. The widespread use of digital technologies and the Internet in modern society attracts the attention of criminologists more and more often, in particular, such a direction in criminology as cybercriminology is expanding.

It has been proven that in order to resist negative manifestations on the Internet and use new opportunities, it is necessary to understand the essence and meaning of cyber security, cybercrime and, in general, directions of new information technologies. In addition, it is important to research and influence such areas as: the cyber security threat environment; the potential business cost of a cyber attack to other entities; assessment of the degree of security of the enterprise, institution or organization; analysis of opportunities to respond in time to negative incidents and ways of using new digital technologies.

The author emphasized in the article that the research and study of the theory of criminological security is designed to contribute to the definition of its main essence, that is, the protection of the individual, society and the state from such a negative, antisocial phenomenon as crime, that is, the identification of those main values that guarantee criminological security at the appropriate level. That is why it is important and necessary at the state level to adopt the Criminological Security Strategy of Ukraine for 2023–2028, because this is exactly the task that must be completed in order to properly protect the rights and freedoms of people and citizens from negative encroachments in cyberspace, with which every citizen of our country is connected in a certain way.

Keywords: *cyber crime, criminological security, cyber security, cyber attack, cyber fraud, digital technologies, information technologies, computer crime, digitalization, criminological strategy.*

Стаття надійшла до редколегії 11 травня 2023 року