DOI: https://doi.org/10.26642/jen-2024-4(110)-145-158
УДК 004:007:351.86

С.В. Корзун, аспірантка
Державний університет «Житомирська політехніка»

Теоретико-методологічна конструкція державної кримінально-правової політики протидії кіберзлочинності

У сучасному світі, де інформаційні технології глибоко проникли в усі аспекти нашого буття, кіберзлочинність є однією з найсерйозніших небезпек. Становлення інформаційного суспільства нерозривно пов'язане зі зростанням впливу цифрових технологій, що водночас відкрило нові можливості для протиправних дій. Кіберзлочини здатні завдавати шкоди не лише окремим людям, а й становити значну загрозу для державних структур та міжнародних об'єднань.

Метою статті є дослідження теоретико-методологічної конструкції державної кримінально-правової політики протидії кіберзлочинності.

В процесі дослідження було розглянуто властивості кіберзлочинів та кіберзлочинності, що визначають її як особливий об'єкт державної кримінально-правової політики, а саме: екстериторіальність, інноваційна залежність, багатопрофільність, латентність, трансформаційність.

У статті представлено змістовне наповнення етапів формування та реалізації державної кримінально-правової політики протидії кіберзлочинності. В дослідженні здійснено аналіз наукової літератури щодо системних проблем розвитку державної кримінально-правової політики, це дозволило згрупувати проблеми за такими векторами: низька ефективність правоохоронної системи, невідповідність суб'єктної структури державного управління, відсутність механізмів адаптації до міжнародної системи протидії. Також у статті на основі обґрунтування впливу на носіїв публічних, приватних та суспільних інтересів було ідентифіковано стейкхолдерів; визначено вихідні положення державної кримінально-правової політики протидії кіберзлочинності; визначено напрями розвитку державної політики; визначено об'єкти державної політики та обґрунтовано суб'єктний склад; визначено методи та принципи реалізації державної політики; запропоновано ключові механізми реалізації.

Ключові слова: *кіберзлочинність; правопорушення; державна кримінально-правова політика; інформаційна війна; запобігання кіберзлочинності.*

Актуальність теми. Кіберзлочинність є однією найбільших загроз сьогодення, адже формування інформаційного суспільства визначило вплив інформаційних технологій на усі сфері суспільного життя. Кіберзлочини можуть становити загрозу як окремій особі, так і державним інституціям та міжнародним організаціям. Варто наголосити, що однією з особливостей, що значно ускладнює інструменти протидії кіберзлочинності, є неможливість ідентифікації територіальної приналежності як злочинця, так і жертви. Адже «Інтернет зруйнував бар'єри між країнами, спільнотами та громадянами, дав можливість взаємодіяти та обмінюватися інформацією та ідеями по всьому світу. Щоб кіберпростір залишався відкритим, вільним та безпечним, в інтернеті повинні застосовуватися ті самі норми, принципи та цінності, що існують в офлайн-режимі. У сучасному світі розвиток інформаційних технологій відкриває нові можливості для комунікації, бізнесу та науки. Однак, поряд з позитивними аспектами цифровізації, зростає і рівень кіберзлочинності, яка стає однією з найсерйозніших загроз для безпеки держав, організацій та окремих осіб. Кіберзлочинність охоплює широкий спектр кримінальних правопорушень – від крадіжки особистих даних і фінансових шахрайств до атак на критичні інфраструктури» [1].

Крім того, наслідки кіберзлочинності також неможливо ідентифікувати за окремими складовими та обсягами, адже вони можуть бути як матеріальними, фінансовими, природними, репутаційними, так і у вигляді людських жертв. Своєю чергу їх обсяги можуть мати як індивідуальний характер, так і впливати на цілі держави, їх об'єднання та регіони. «Сьогодні ми живемо в епоху інформаційного суспільства, коли фактично електронно-обчислювані машини та телекомунікаційні системи охоплюють усі сфери життєдіяльності, як держави в цілому, так і кожного окремого громадянина зокрема. Разом з тим запровадження глобальної диджиталізації в суспільство, поставило певні виклики, щодо можливостей зловживання інформаційними та телекомунікаційними технологіями. Наразі жертвами зловмисників, які здійснюють свою діяльність у віртуальному просторі (кіберсередовищі), можуть стати не лише окремі громадяни, але й цілі держави. При цьому безпека десятків тисяч користувачів, може виявитися залежною лише від декількох зловмисників. Варто зауважити, що кількість кримінальних правопорушень у кіберпросторі, зростає пропорційно кількості користувачів мережі «Інтернет» та кількості телекомунікаційних систем» [3]. Все це визначає складність державної кримінально-правової політики протидії кіберзлочинності, неможливість її реалізації відокремлено від міжнародної спільності та країн-

партнерів, а також формування інструментів протидії, що мають як правовий характер, так і організаційний, соціальний, економічний, технологічний та міжнародний.

Аналіз останніх досліджень. Питання формування та реалізації державної кримінально-правової політики протидії кіберзлочинам дослідженні такими вітчизняними вченими: Д.С. Азаров, О.Амелін, П.Д. Біленчук, В.М. Бутузов, С.В. Бєлай, В.О. Голубєв, Д.О. Грицишен, О.П. Дзьобань, О.Ю. Довженко, І.О. Драган, І.В. Європіна, М.В. Карчевський, М.О. Кравцова, В.В. Лісовий, О.В. Махницький, А.А. Музика, В.В. Пивоваров, В.Г. Пилипчук, Б.В. Романюк, С.О. Савчук, О. Столяр, К.В. Терещенко, В.С. Цимбалюк, К.В. Юртаєва та інші. Серед зарубіжних вчених зазначенні питання в своїх працях піднімали: М.Брюс, Н.Ванетик, Ф.Варезе, Д.Варзанде, С.Гордон, М.Давидян, Ф.Дінг, Дж.Донг, А.Ерола, Р.Кашьяп, М.Кіперберг, Х.Лаллі, Я.Люстхаус, Ф.Марбук, Д.Нерс, К.Фарахбод, Н.Фейр, Д.Форд, М.Хао, Д.Цзян, С.Чен, К.Шайо, Л.Шепард та інші.

Викладення основного матеріалу. На шляху забезпечення високого рівня національної безпеки в цілому та інформаційної, економічної, воєнної як її складових зокрема є потреба в перегляді сучасних підходів до формування державно-кримінальної політики протидії кіберзлочинності. «Сучасний стан розвитку інформаційних систем і технологій, рівень розвитку кіберзлочинності загострили наявні та спричинили виникнення нових проблем нормативно-правової регламентації організаційно-правових заходів протидії кіберзлочинності, захисту інформаційних ресурсів, інформаційно-телекомунікаційних систем, інформаційного простору держави загалом. Стала очевидною проблема відсутності системних підходів до політики кібернетичної безпеки держави» [16]. Кіберзлочинність має особливі властивості, які не характерні будь-яким іншим видам злочинів, а їх результативність залежить від суспільної свідомості, обізнаності та грамотності, що має бути враховано при формуванні досліджуваної державної політики.

Властивостями кіберзлочинів та кіберзлочинності, що визначають її як особливий об'єкт державної кримінально-правової політики, є такі:

– *екстериторіальність*. Так кіберзлочинність «має транснаціональний характер, оскільки кіберзлочинці в силу своєї приналежності до комп'ютерного «андеграунду» для отримання злочинних доходів та спрощення вчинення злочинних діянь на території двох і більше держав змушені, незалежно від національності, об'єднуватися в міжнародні злочинні групи» [14]. «Відсутність чітко визначених кордонів у кіберпросторі створює безліч труднощів у притягнення винних до кримінальної відповідальності, і єдине вирішення проблеми транскордонності кіберзлочинів проти власності, на нашу думку, полягає в розвитку тісного міжнародного співробітництва» [13]. Саме це характеризує кіберзлочинність як транснаціональну злочинність, що в свою чергу визначає специфіку підходів до системи протидії таким видам злочинності. Вітчизняна дослідниця проблем транснаціональної злочинності І.М. Леган вказує на таке: «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» [8]. Зазначене означає неможливість прив'язати скоєний кіберзлочин до певної території, жертва, виконавець та замовних злочину можуть навіть бути незнайомими та знаходитися на різних кінцях планети;

– *інноваційна залежність*. «Із першого дня існування всесвітнього віртуального простору в нього стали проникати різні правопорушники, зокрема й злісні злочинці. З'являються нові форми і види злочинних посягань у сфері високих технологій. Злочинці все частіше застосовують системних підхід до планування своїх дій, використовують сучасні технології та спеціальні засоби, створюють нові системи конспірації» [6]. «Кіберзлочинність є явищем новітньої, цифрової доби. Саме це й робить «кіберів» набагато небезпечнішими й ефективнішими за своїх «класичних» колег – шахраїв. Це люди, які працюють головою і роблять свої «справи», не відходячи від свого комп'ютера або сидячи на лавочці з ноутбуком і мобільним телефоном. Для сучасних «технарів» це часто ідеальний спосіб заробити і реалізувати себе. Злочинці не стоять на місці. Їхні методи вдосконалюються і стають дедалі складнішими» [4]. «Кіберзлочинність в Україні має високотехнологічний характер, що викликано використанням ІТ-технологій, інформаційно-телекомунікаційних мереж, комп'ютерних пристроїв, носіїв комп'ютерної інформації та інше, які виступають знаряддями і засобами вчинення кримінальних правопорушень» [11]. Це характеризує злочинців як високоінтелектуальних осіб, а інструменти скоєння злочину як високотехнологічні;

– *багатопрофільність*. Микитчик А.В. вказує на ключові риси кіберзлочинності, як характеризують її багатопрофільність: «отримала риси економічної злочинності, так як більшість кіберзлочинів відбувається в банківсько-фінансовому або корпоративному секторі (інтернет-банкінг, банківський фішинг, кібервимагання та ін.), а діяльність злочинців спрямована на вилучення доходів (прибутку); трансформується в злочинність політичного характеру, що пов'язано з активізацією протиправної діяльності в кіберпросторі представників хакерського руху, спецслужб і силових структур зарубіжних

держав, міжнародних екстремістських і терористичних організацій (DDoSатаки на урядові сайти, кібершпіонаж щодо інформаційних ресурсів органів державної влади, правоохоронних органів, підприємств оборонно-промислового комплексу, дипломатичних представництв та інше» [11]. Так, наслідки можуть проявлятися в: економічній сфері – крадіжка коштів, або інших ресурсів, зменшення прибутків, банкрутство та інше; репутаційній сфері – оприлюднення особистої інформації, або інформації, що становить комерційну чи державну таємницю, що може нашкодити репутації особі, інституції, державі чи міжнародній організації; політичній сфері – кібератаки можуть призвести до повалення політичного режиму, недійсності виборчих процесів та інше; воєнній сфері – кібервійни стали новим видом загроз для держави її територіальної цілісності та суверенітету. Відповідно обсяги наслідків можуть стосуватися як втрати певних економічних ресурсів та репутаційного капіталу особи, організації, держави, міжнародної інституції так людських жертв, руйнування інфраструктури, припинення та при зупинка функціонування певних інфраструктурних галузей, катастроф та інше;

– *латентність*. «Мають високий ступінь латентності, яка становить від декількох десятків до декількох тисяч відсотків з різних видів злочинних діянь, що обумовлено різними об'єктивними факторами (небажання жертв комп'ютерних злочинів звертатися до правоохоронних органів, неочевидність комп'ютерних злочинів для більшості населення в силу їх вчинення у віртуальному середовищі, складність виявлення комп'ютерних злочинів за відсутності необхідної кількості фахівців в правоохоронних органах та ін.)» [11]. Латентність є великою проблемою для правоохоронної системи, адже небажання повідомляти про скоєнні злочини в кіберпросторі призводить до безкарності та збільшенню можливостей для скоєння кіберзлочинів, які матимуть більш глобальні наслідки;

– *трансформаційність*. Кіберзлочинність модифікує інструменти скоєння злочинів в різних сферах суспільного життя. «Розвиток сучасних комп'ютерних технологій привносить у життя громадян не лише нові прогресивні можливості, але й ряд небезпечних аспектів, які знаходять своє відображення у кіберзлочинності. За допомогою доступу до мережі «Інтернет» були як модифіковані раніше відомі злочини – крадіжки, онлайн-шахрайства, вимагання, розповсюдження дитячої порнографії, так і з'явилися абсолютно нові, раніше не відомі види злочинів – скімінг, фішинг, кардінг, вішинг, шимінг та інші. Зважаючи на те, що кіберзлочини можуть вчинятися на території однієї держави, так і інших держав, до злочинних угруповань можуть входити представники різних національностей, перед міжнародним співтовариством постало питання боротьби з кіберзлочинністю. Характеристика кіберзлочинів як соціальних явищ передбачає їх актуальність для всього суспільства і потребує наявності стратегії держави в усіх сферах запобігання кіберзлочинності» [9]. Так, кіберзлочин на відміну від інших видів злочину може мати різносторонню мету та в більшості випадків виступає інструментів скоєння іншого виду злочину, зокрема політичного, економічного, терористичного, сексуального та інше.

Зазначене вказує на необхідність формування державної кримінально-правової політики, що характеризується наступними властивостями: багатовекторність – характеризує державну кримінально-правову політику як таку, що охоплює різні методи та способи протидії кіберзлочинам в різних сферах суспільних відносин; міжсистемність – визначає потребує при формуванні державно-кримінально-правової політики визначати взаємодію між різними суб'єктами реалізації державної кримінально-правової політики в різних сферах.

В контексті формування методології формування та реалізації державної кримінально-правової політики будемо притримуватися думки вітчизняного вченого Д.О. Грицишена, який виділяє наступні її етапи щодо реалізації державної політики в сфері протидії економічній злочинності, зміст яких можливо адаптувати та державної кримінально-правової політики протидії кібезлочинності: ідентифікація та виявлення симптомі проблеми в суспільному житті щодо економічної злочинності та їх впливу на національну безпеку; визначення стейкхолдерів та ідентифікація їх інтересів щодо запобігання та протидії економічній злочинності; обґрунтування змісту кримінальної політики як системи та як процесу запобігання та протидії економічній злочинності; формування об'єктно-предметного поля державної кримінальної політики в сфері запобігання та протидії економічній злочинності; визначення мети та завдань державної кримінальної політики в сфері запобігання та протидії економічній злочинності; обґрунтування напрямів формування та реалізації державної кримінальної політики в сфері запобігання та протидії економічній злочинності; визначення суб'єктів формування та реалізації державної кримінальної політики в сфері запобігання та протидії економічній злочинності; визначення об'єктів державної кримінальної політики в сфері запобігання та протидії економічній злочинності; встановлення взаємозв'язків із іншими видами державної політики в сфері запобігання та протидії економічній злочинності в сфері запобігання та протидії економічній злочинності; обґрунтування методів та принципів державної кримінальної політики в сфері запобігання та протидії економічній злочинності; встановлення механізмів державної кримінальної політики в сфері запобігання та протидії економічній злочинності [2].

Змістовне наповнення зазначених етапів формування та реалізації державної кримінально-правової політики протидії кіберзлочинності представлено в таблиці 1.

Таблиця 1

Методологічні положення формування та реалізації державної кримінально-правової політики протидії кіберзлочинності

<table>
<tr><td colspan="4">1. СУСПІЛЬНА ПРОБЛЕМ КІБЕРЗЛОЧИННОСТІ ЯК ОБ’ЄКТУ ДЕРЖАВНОЇ ПОЛІТИКИ</td></tr>
<tr><td colspan="4">ЗМІСТ ПРОБЛЕМИ
- динамічні тенденції розвитку інформаційного суспільства та активізація діяльності людини у віртуальному просторі, що зумовлює зростання кіберзлочинності, що становить загрозу національній безпеці та впливає на рівень глобальної безпеки</td></tr>
<tr><td colspan="4">СИМПТОМИ ПРОБЛЕМИ:</td></tr>
<tr><td colspan="4">що характеризують детермінантами розвитку кіберзлочинності</td></tr>
<tr><td>Геополітичні</td><td>Внутрішньополітичні</td><td>Економічні</td><td>Соціальні</td></tr>
<tr><td>Правові</td><td>Державно-управлінські</td><td>Технологічні</td><td>Віктимологічні</td></tr>
<tr><td colspan="4">що характеризують системні проблеми державної політики</td></tr>
<tr><td colspan="2">- низька ефективність правоохоронної системи</td><td>- невідповідність суб’єктної структури державного управління</td><td>- відсутність механізмів адаптації до міжнародної системи протидії</td></tr>
<tr><td colspan="4">наслідки, визначають вплив на рівень складових національної безпеки:</td></tr>
<tr><td>- інформаційна</td><td>- економічна</td><td>- енергетична</td><td>- продовольча</td></tr>
<tr><td>- соціальна</td><td>- воєнна</td><td>- екологічна</td><td>- політична</td></tr>
<tr><td colspan="4">2. СТЕЙКХОЛДЕРИ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ</td></tr>
<tr><td colspan="4">виплаває на носіїв інтересів:</td></tr>
<tr><td colspan="2">Публічних інтересів</td><td>Суспільних інтересів</td><td>Приватних інтересів</td></tr>
<tr><td colspan="4">3. ВИХІДНІ ПОЛОЖЕННЯ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ</td></tr>
<tr><td>Зміст державної кримінально-правової політики протидії кіберзлочинності</td><td colspan="3">- як процес: сукупність послідовних процесів організаційно-методологічного характеру, які полягають у розробці, формуванні, верифікації та реалізації та оцінки державно-управлінських рішень, що передбачають застосування сукупності інструментів та методів у відповідності із визначеними принципами, що є складовими правового, організаційного, інформаційного та економічного механізмів протидії кіберзлочинності її наслідкам;
- як система: система взаємодії суб’єктів законодавством, виконавчої та судової влади щодо формування та реалізації державно-управлінських рішень, що передбачають застосування сукупності інструментів та методів у відповідності із визначеними принципами, що є складовими правового, організаційного, інформаційного та економічного механізмів протидії кіберзлочинності її наслідкам</td></tr>
<tr><td colspan="4">Об’єктно-предметне поле державної кримінально-правової політики протидії кіберзлочинності</td></tr>
<tr><td colspan="2">Об’єкт державної політики</td><td colspan="2">Предмет державної політики</td></tr>
<tr><td colspan="2">- діяльність суспільних інститутів на різних рівням соціально-економічної системи, що реалізується у віртуальному просторі або з використанням інформаційно-комп’ютерних технологій із порушенням встановлених національним або міжнародним законодавством параметрів через кібернетичну злочинність та становлять загрозу національній безпеці держави в цілому та її окремим складовим зокрема</td><td colspan="2">- сукупність організаційно-методологічних положень правового, організаційного, інформаційного та економічного характеру щодо протидії кіберзлочинності, що полягає в порушенні встановлених національним або міжнародним законодавством параметрів діяльності суспільних інститутів, що реалізується у віртуальному просторі або з використанням інформаційно-комп’ютерних технологій</td></tr>
<tr><td colspan="4">Мета та завдання державної кримінально-правової політики протидії кіберзлочинності</td></tr>
<tr><td>Мета</td><td colspan="3">- розробка, формування, верифікація та впровадження державно-управлінських рішень та механізмів їх реалізації щодо протидії кіберзлочинності для забезпечення відповідного рівня національної безпеки в цілому та її складових зокрема</td></tr>
<tr><td colspan="4">Завдання</td></tr>
<tr><td>1. Модернізація суб’єктної структури системи державного управління в сфері протидії кіберзлочинності</td><td>2. Налагодження інформаційно-комунікаційної системи між суб’єктами реалізації державної кримінально-правової політики</td><td>3. Адаптація вітчизняного законодавства в сфері кіберзахисту та протидії кіберзлочинності до вимог ЄС</td><td>4. Налагодження інформаційно-комунікаційної системи з правоохоронними органами зарубіжних країн</td></tr>
</table>

Закінчення табл. 1

5. Налагодження інформаційно-комунікаційної системи з міжнародними урядовими та неурядовими організаціями	6. Налагодження інформаційно-комунікаційної системи з міжнародними поліцейськими організаціями	7. Реформування кримінального законодавства щодо встановлення відповідальності та протидії кіберзлочинам	8. Розробка та реалізація превентивних заходів щодо протидії кіберзлочинності серед населення
9. Розробка заходів із забезпечення інформаційної та іншої видів безпеки суб'єктів реалізації державної політики	10. Ратифікація міжнародних нормативно-правових актів щодо протидії кіберзлочинності та забезпечення кіберзахисту	11. Оптимізація фінансового забезпечення суб'єктів реалізації державної кримінально-правової політики протидії кіберзлочинності	12. Підвищення рівня кадрового потенціалу правоохоронної системи щодо протидії кіберзлочинності
4. НАПРЯМИ РОЗВИТКУ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ			
- реформування кримінального законодавства щодо протидії кіберзлочинності	- трансформація суб'єктної структури системи державного управління в сфері протидії кіберзлочинності	- розширення міжнародно-правового механізму реалізації державної кримінально-правової політики	
5. ОБ'ЄКТИ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ			
- регулювання суспільних відносин щодо використання інформаційно-комп'ютерних технологій	- регулювання діяльності суспільних інституцій в віртуальному просторі	- функціонування правоохоронної системи (діяльність правоохоронних органів) щодо протидії кіберзлочинності	- міжнародні відносини щодо протидії кіберзлочинам та забезпечення інформаційної безпеки держави
6. СУБ'ЄКТИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ			
Центральні органи виконавчої влади, що реалізують державну кримінально-правову політику протидії кіберзлочинності		*Суб'єкти правоохоронної діяльності на які покладаються функції з протидії кіберзлочинності*	
Міністерство цифрової трансформації України	Міністерство внутрішніх справ України	*прямо пов'язані із протидією кіберзлочинності*	
		Служба безпеки України	Національна поліція України
Міністерство закордонних справ	Міністерство оборони України		
Міністерство юстиції України	Міністерство фінансів України	Державне бюро розслідувань	
Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів		Адміністрація Державної служби спеціального зв'язку та захисту інформації України	
		опосередковано пов'язані із протидією кіберзлочинності	
Національне агентство з питань запобігання корупції	Державна служба фінансового моніторингу України	Національне антикорупційне бюро України	Бюро економічної безпеки України
7. ВЗАЄМОЗВ'ЯЗКИ ІНШИМИ ВИДАМИ ДЕРЖАВНОЇ ПОЛІТИКИ			
- політика в сфері правоохоронної діяльності	- політика в сфері митної діяльності	- політика в сфері охорони державного кордону	- інноваційна політика
- економічна політика	- інформаційна політика	- оборонна політика	- фінансова політика
- антикорупційна політика	- монетарна політика	- антитерористична політика	- зовнішня політика
8. МЕТОДОЛОГІЯ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ			
Методи прямого впливу		*Методи непрямого впливу*	
- укази	постанови	- соціально-психологічні	- інформаційні
- рішення	розпоряджень	- стимулюючі	- профілактичні
Принципи			
- обґрунтованості	- аналітичності	- системності	- прозорості	- ефективності
- комплексності	- послідовності	- аполітичності	- правомочності	- гуманізму
9. МЕХАНІЗМИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ			
- кримінально-правовий	- міжнародно-правовий	- фінансово-економічний	- організаційний

Розроблена методологія формування та реалізації державної кримінально-правової політики ґрунтується на визначених властивостях кіберзлочинності та тенденцій розвитку інформаційного суспільства та активізації діяльності людини та інституцій у віртуальному просторі. Важливою складовою є визначення змісту проблеми, яку має вирішити державна політика. В даному контексті проблему пропонуємо визначати як: «динамічні тенденції розвитку інформаційного суспільства та активізація діяльності людини у віртуальному просторі, що зумовлює зростання кіберзлочинності, що становить загрозу національній безпеці та впливає на рівень глобальної безпеки».

Ця проблема характеризується сукупність симптомів, які пропонуємо групувати таким чином:

– симптоми проблеми, що характеризують детермінантами розвитку кіберзлочинності;

– симптоми проблеми, що характеризують системні проблеми державної політики.

В наукові літературі, що стосується розвитку державно кримінально-правової політики протидії кіберзлочинності досить часто визначають фактори, які призводять до поширення та розвитку кіберзлочинності. Комплексне бачення, що визначає як правові так і кримінологічні, економічні, політичні, державно-управлінські аспекти детермінант розвитку кіберзлочинності представлено в дослідженні Б.Головкіна [5]. Погоджуємося із результатами вказаного дослідження, та вважаємо, що такий підхід має стати підґрунтям розробки методології формування та реалізації державної кримінально-правової політики протидії кіберзлочинам (табл. 2).

Щодо системних проблем розвитку державної кримінально-правової політики, то в більші мірі вони стосуються власне правоохоронної системи. З даного приводу в наукові літературі існують різні точки зору. Маслова О.О., Никончук Н.С. визначають такі симптоми проблеми, що є загрозою поширення кіберзлочинності:

«– недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського права у вітчизняне законодавство, недостатня врегульованість цифрової складової частини розслідування злочинів, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері;

– відсутність у значної частини міністерств і відомств відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом. Фінансування робіт із кіберзахисту здійснюється за залишковим принципом з технологічними помилками;

– відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності країни, що вимагає суворого дотримання відповідних стандартів;

– невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі;

– відсутність законодавчого акта про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури;

– незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки;

– відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту» [12].

Головкін Б. вказує на наступні симптоми проблеми державної кримінально-правової політики протидії кіберзлочинам, як визначаються станом функціонування правоохоронної системи:

«– невизначеність державної політики боротьби із кіберзлочинністю, нерозробленість концепції запобігання і протидії кіберзлочинності, відсутність загальнодержавних та регіональних програм і протидії кіберзлочинності, несформованість стратегічних пріоритетів та відповідного їм комплексу заходів запобігання найбільш поширеним видам кіберзлочинів;

– недостатня спроможність суб'єктів боротьби з кіберзлочинністю ефективно здійснювати запобігання і протидію кіберзлочинам (недостатньо сил, засобів, матеріально-технічних ресурсів, кадрового потенціалу, бюджетного фінансування);

– відсутність центрального органу, відповідального за боротьбу з кіберзлочинністю в Україні, який би здійснював координацію діяльності усіх суб'єктів на загальнодержавному рівні, забезпечував міжвідомчу взаємодію та міжнародну співпрацю;

– брак кіберекспертів, оперативних працівників, слідчих, прокурорів, що спеціалізуються на запобіганні, виявленні, розслідуванні, припиненні кіберзлочинів;

– недостатня забезпеченість правоохоронних органів спеціальними технічними засобами виявлення та реагування на кіберпосягання, що містять ознаки кіберзлочинів» [5].

Таблиця 2

Характеристика детермінант запобігання кіберзлочинності за Б.Головкіним [5]

ПОЛІТИЧНІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ		
зовнішньополітичні або геополітичні		
розгортання в кіберпросторі шкідливого програмного забезпечення та проведення широкомасштабних кампаній з викрадення у політичних, економічних або військових цілях чутливої інформації	мілітаризація кіберпростору, використання його для проведення розвідувальної, терористичної, диверсійної та іншої підривної діяльності	
недостатній рівень кібернетичної стійкості мереж, інформаційних систем та об'єктів критичної інфраструктури	недотримання організаціями державного і приватного сектору різних держав міжнародних норм і стандартів кібербезпеки	
декларативність політики та недостатність координації превентивних заходів	перетворення кіберпростору на середовище геополітичного суперництва за технологічне домінування у цифровому світі	
нестабільність кіберпростору, постійне збільшення кількості та зміна характеру глобальних викликів і загроз для сталого функціонування національної інформаційної інфраструктури	фінансування та використання в геополітичних інтересах спеціальними службами і розвідувальними органами держав, що претендують на домінування у кіберпросторі	
широкі можливості для проведення у кіберпросторі глобальних дезінформаційних компаній		
внутрішньополітичні		
нерозвинений механізм комунікацій у сфері забезпечення кібербезпеки і боротьби з кіберзлочинністю, спрямованої на поширення достовірної інформації	непідкріплення політичної волі вищого керівництва держави щодо сталого розвитку інформаційного суспільства та створення безпечного комунікативного середовища	
недостатній рівень гармонізації міжнародних стандартів кібербезпеки із законодавством України	незавершеність реформування системи захисту інформації з обмеженим доступом	
недоліки в організації та проведення просвітницької роботи серед населення з питань безпечної поведінки у кіберпросторі	недоліки концепції державної політики у сфері забезпечення кібербезпеки та протидії кіберзлочинності	
неефективна система підготовки кваліфікованих фахівців з кібербезпеки	нерозвинена міжнародна співпраця з ключовими іноземними партнерами	
ЕКОНОМІЧНІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ		
недостатній обсяг державного фінансування цифрового сектору, у тому числі заходів з кібербезпеки	функціонування аутсорсингової моделі організованого злочинного бізнесу в кіберпросторі	низький внутрішній попит на високотехнологічні програмні продукти, технічні рішення і проривні технології
велика пропозиція в темній мережі, закритих групах зловмисного програмного забезпечення	розвинений у темній мережі кіберпростору незаконний обіг цифрових технологій, продуктів та послуг	інтенсивні темпи цифровізації фінансового сектору економіки і перехід на електронні платіжні системи
широкі можливості здійснення конфіденційних платежів, приховування коштів та легалізації доходів, одержаних від кіберзлочинів	інноваційна відсталість економіки та її низька конкурентоспроможність, експортна орієнтованість інформаційно-комунікаційних технологій	
заощадження витрат державними і приватними структурами на купівлі та експлуатації комп'ютерної техніки й обладнання	високий комерційний попит серед користувачів на зловмисне програмне забезпечення, кримінальні послуги операторів таких продуктів і хакерів	функціонування в національному сегменті мережі Інтернет незаконного обігу контрафактного програмного забезпечення
відсутність конкурентного ринку телекомунікаційних послуг	низькозатратність, малоризикованість та високодохідність кіберзлочинної діяльності	збільшення обсягів трудової зайнятості в IT-секторі

Продовження табл. 2

СОЦІАЛЬНІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ		
використання технологій соціальної інженерії для зміни способу мислення і характеру поведінки людей та їхніх об'єднань у кіберпросторі	зумовлені цифровізацією держави і суспільства зміни соціальної поведінки, що виражаються у переході на віртуальну модель комунікацій замість фізичної взаємодії	деформації моральної і правової свідомості користувачів під цілеспрямованим інформаційно-психологічним деструктивним впливом
зростання аудиторії користувачів та збільшення часу перебування у кіберпросторі	розмивання меж між реальним і віртуальним життям, що створює ілюзію безпеки	низький рівень цифрової грамотності користувачів Інтернету, Е-сервісів
НОРМАТИВНО-ПРАВОВІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ		
несформованість цілісної нормативно-правової бази у сфері забезпечення кібербезпеки і боротьби з кіберзлочинністю	нормативна неврегульованість питань щодо електронних комунікацій, використання штучного інтелекту, Інтернету речей	повільні темпи наближення національного законодавства у сфері захисту персональних даних до законодавства ЄС
неврегульованість в Законі України «Про телекомунікації» порядку взаємодії між суб'єктами забезпечення кібербезпеки та операторами, провайдерами телекомунікацій	недосконалість нормативно-правової бази у сфері електронних довірчих послуг, зумовлена неповною імплементацією Регламенту ЄС 910/214	недостатній рівень гармонізації національного законодавства про критичну інфраструктуру та її захист із нормами Директиви (ЄС)
низька ефективність захисту прав громадян та суб'єктів господарювання у кіберпросторі, зумовлена неповною імплементацією в національне законодавство Директиви 2002/58/ЄС	неврегульованість на законодавчому рівні питання запровадження ризик-орієнтованого підходу та механізму його реалізації в систему забезпечення кібербезпеки	нечітка правова регламентація форм і механізму участі операторів, провайдерів телекомунікаційних послуг та інших суб'єктів приватного сектору
недосконалий організаційно-правовий механізм державно-приватної взаємодії у сфері забезпечення кібербезпеки	неповна імплементація Конвенції про кіберзлочинність у КК України	
ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ		
організаційна незавершеність архітектури національної системи забезпечення кібербезпеки	недостатня інституційна спроможність суб'єктів протидії кіберзлочинності	
недостатнє для розвитку національної системи кіберзахисту і протидії кіберзагрозам державне фінансування	низький рівень підготовки і підвищення кваліфікації фахівців з інформаційної і кібернетичної безпеки	
недостатній рівень технічної захищеності державних інформаційних ресурсів	недостатньо розвинена міжнародна співпраця з питань кібербезпеки	
відсутність у значної частини державних органів, органів місцевого самоврядування, суб'єктів господарювання, віднесених до об'єктів критичної інфраструктури	нерозробленість механізму громадського контролю за законністю та ефективністю діяльності суб'єктів забезпечення кібербезпеки	
відсутність загальнодержавної програми цифрової грамотності населення	нездійснення аудиту стану кібербезпеки	

Закінчення табл. 2

ТЕХНОЛОГІЧНІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ	
висока технологічна залежність України від іноземних виробників продукції інформаційно-комунікаційних технологій	забюрократизованість порядку сертифікації й експертизи Комплексної системи захисту інформації
можливість проникати в локальні мережі підприємств, організацій, установ шляхом підключення за протоколом віддаленого робочого столу	порушення загальних вимог до кіберзахисту об'єктів критичної інфраструктури власниками або керівниками
використання застарілого антивірусного програмного забезпечення, ненадійних паролів, невпровадження інноваційних технологічних рішень	недотримання суб'єктами господарювання, які працюють на ринку ЄС, вимог Регламенту щодо захисту персональних даних
технологічна застарілість і неефективність програмно-апаратних засобів криптографічного і технічного захисту інформації з обмеженим доступом	відсутність у багатьох власників і користувачів державних інформаційних ресурсів служби захисту інформації та системних адміністраторів
використання неліцензованого і несертифікованого програмного забезпечення	технологічна і технічна відсталість цифрової інфраструктури України
використання у системах реєстрації та контролю доступу до інформаційних систем технологічно несумісних механізмів, алгоритмів та протоколів електронної ідентифікації та впізнання	ненадійна система кіберзахисту інформації з обмеженим доступом в юридичних осіб державної і приватної форми власності
незахищеність каналів зв'язку, електронної пошти, телекомунікаційних мереж, серверів і баз даних	відсутність Єдиного реєстру оцінки ризиків і загроз на різних рівнях і об'єктах кіберзахисту
відсутність безпечного DNS-сервера	відсутність захищеного обміну ідентифікаційними даними
ВІКТИМОЛОГІЧНІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ	
інтенсивний розвиток електронних послуг, зумовлений переходом на віддалений режим роботи під час світової пандемії	збільшення в рази кількості пристроїв підключених до глобальної мережі Інтернет та інших локальних мереж
високі ризики віктимізації державних службовців, які не дотримуються основ кібергігієни	заняття нелегальною електронною комерцією, а також надання нелегальних платних послуг користувачам мережі Інтернет
створення і самопоширення неповнолітніми компрометуючих матеріалів інтимного характеру та особистих даних у кіберпросторі	відвідування маловідомих сайтів і веб-сторінок інтернет магазинів, переходи на вкладки спливаючої реклами
професійна віктимність окремих категорій користувачів, які надають послуги та здійснюють господарську діяльність у кіберпросторі	нерозбірливі знайомства в Інтернеті, вступ до різних груп, відверте спілкування
надмірна довірливість при використанні послуг Інтернет-банкінгу	економія витрат на системах програмного і технічного захисту інформації

Колектив авторів монографічного дослідження за редакцією Д.О. Грицишена та В.В. Євдокимова, зазначають ключові системні проблеми, зокрема:

– заполітизованість правоохоронної системи держави, що у результаті призводить до низького рівня управління її функціональними та операційними процесами;

– низький рівень інформованості суспільства про реформування правоохоронної системи;

– відсутність комунікації між правоохоронними органами; правовий механізм мінливий до політичних сил, що, як наслідок, призводить до значних змін у законодавстві та прийняття недосконалих початкових законів;

– відсутність комплексності у реформуванні;

– відсутність комунікації між центральними органами виконавчої влади, що реалізують політику в різних сферах суспільного життя, які є суміжними до правоохоронної системи;

– недосконаліть структури правоохоронної системи;

– проблема фінансового забезпечення правоохоронної системи [7].

Підводячи підсумок зазначеного вище, вбачаємо необхідність групування системних симптомів проблеми державної кримінально-правової політики протидії кіберзлочинності:

– низька ефективність правоохоронної системи, що визначається недостанім фінансуванням, низьким рівнем кадрового потенціалу, недосконалою матеріально-технічною базою, прогалинам в правовому забезпеченні реалізації положень кримінального законодавства щодо протидії кіберзлочинності, відсутністю комунікації між різними учасниками реалізації державної політики;

– невідповідність суб'єктної структури державного управління, адже питання кібербезпеки та протидії кіберзлочинам в більші мірі знаходить в системі Національної поліції, яка має обмеженні функції;

– відсутність механізмів адаптації до міжнародної системи протидії, зокрема на сьогодні законодавство України в сфері протидії кіберзлочинності має бути гармонізоване із директивами Європейського союзу, а також є необхідність повної ратифікації міжнародних нормативно-правових актів та налагодження тісної співпраці як із правоохоронними органами зарубіжних країн так і з міжнародними поліцейськими організаціями.

Ефективність реалізації державної кримінально-правової політики протидії кіберзлочинності залежить від якості врегулювання публічних, приватних та суспільних інтересів. «Право опиняється в епіцентрі проблеми інтересів у плані їх виявлення, нормативного закріплення та захисту. Складні суспільні явища, що підлягають регулюванню правом є поєднанням різних інтересів – економічних, соціальних, політичних тощо. Інтенсивний розвиток і диференціація соціальних інтересів висунули в розряд першочергових завдання адекватного правового їх вираження, забезпечення та захисту від посягань. Успішне виконання правом його функцій соціального регулювальника та засобу організації суспільного життя можливе лише при правильному поєднанні юридичних механізмів із соціальними інтересами людей, оскільки будь-яка норма права так чи інакше пов'язана з конкретним інтересом» [15].

Вперше питання вивчення правоохоронної системи як системи реалізації державної кримінально-правової політики протидії злочинності в контексті врегулювання інтересів було представлено в дослідженні К.В. Малишева [10], зокрема автор вивчає правоохоронну систему на перетині приватних публічних та суспільних інтересів:

«– правоохоронна система, як система забезпечення дотримання інтересів учасників суспільних відносин. Основною метою правоохоронної системи є забезпечення дотримання інтересів учасників суспільних відносин;

– правоохоронна система, як складова сукупності інтересів учасників суспільних відносин. При формуванні та реалізації державної політики у сфері трансформації правоохоронної системи різні суспільні групи намагаються сформувати власний інтерес у її розвитку. Відповідно, кожен механізм має бути спрямований на подолання конфлікту інтересів;

– правоохоронна система як інструмент порушення інтересів учасників суспільних відносин у контексті професійної діяльності. Під час виконання професійних завдань у правоохоронній діяльності, в окремих випадках, для забезпечення національних та публічних інтересів, суб'єкти правоохоронної системи можуть нехтувати приватними інтересами» [10].

Вбачаємо, що врегулювання інтересів стейкхолдерів має відбувати наступним чином:

– по-перше, при формуванні державної кримінально-правової політики протидії кіберзлочинності, зокрема на етапі визначення її мети, завдань цілей та інше;

– по-друге, при реалізації державної кримінально-правової політики протидії кіберзлочинності. Це стосується вивчення впливу механізмів реалізації державної політики на різних учасників суспільних відносин;

– по-третє, державна політика має сформувати таку сукупність інструментів, щоб врегулювати інтереси, а також захистити їх в інформаційному суспільстві та віртуальному просторі.

Представленні вихідні положення державної кримінально-правової політики протидії кіберзлочинності визначають два підходи до змісту, зокрема:

– як процес: сукупність послідовних процесів організаційно-методологічного характеру, які полягають у розробці, формуванні, верифікації та реалізації та оцінки державно-управлінських рішень, що передбачають застосування сукупності інструментів та методів у відповідності із визначеними принципами, що є складовими правового, організаційного, інформаційного та економічного механізмів протидії кіберзлочинності її наслідкам;

– як система: система взаємодії суб'єктів законодавством, виконавчої та судової влади щодо формування та реалізації державно-управлінських рішень, що передбачають застосування сукупності інструментів та методів у відповідності із визначеними принципами, що є складовими правового, організаційного, інформаційного та економічного механізмів протидії кіберзлочинності її наслідкам.

В контексті зазначено визначено зміст об'єкту, предмету та мети досліджуваної політики. Об'єктом державної політики є діяльність суспільних інститутів на різних рівням соціально-економічної системи, що реалізується у віртуальному просторі або з використанням інформаційно-комп'ютерних технологій із порушенням встановлених національним або міжнародним законодавством параметрів через кібернетичну злочинність та становлять загрозу національній безпеці держави в цілому та її окремим складовим зокрема. Під предметом запропоновано розуміти: сукупність організаційно-методологічних положень правового, організаційного, інформаційного та економічного характеру щодо протидії кіберзлочинності, що полягає в порушенні встановлених національним або міжнародним законодавством параметрів діяльності суспільних інститутів, що реалізується у віртуальному просторі або з використанням інформаційно-комп'ютерних технологій. Мету сформульовано наступним чином: розробка, формування, верифікація та впровадження державно-управлінських рішень та механізмів їх реалізації щодо протидії кіберзлочинності для забезпечення відповідного рівня національної безпеки в цілому та її складових зокрема. Відповідно до об'єктно-предметного поля та визначеної мети, а також зважаючи на симптоми проблеми, пропонуємо виділяти наступні завдання щодо розвитку державної кримінально-правової політики:

– модернізація суб'єктної структури системи державного управління в сфері протидії кіберзлочинності;

– налагодження інформаційно-комунікаційної системи між суб'єктами реалізації державної кримінально-правової політики;

– адаптація вітчизняного законодавства в сфері кіберзахисту та протидії кіберзлочинності до вимог ЄС;

– налагодження інформаційно-комунікаційної системи з правоохоронними органами зарубіжних країн;

– налагодження інформаційно-комунікаційної системи з міжнародними урядовими та неурядовими організаціями;

– налагодження інформаційно-комунікаційної системи з міжнародними поліцейськими організаціями;

– реформування кримінального законодавства щодо встановлення відповідальності та протидії кіберзлочинам;

– розробка та реалізація превентивних заходів щодо протидії кіберзлочинності серед населення;

– розробка заходів із забезпечення інформаційної та іншої видів безпеки суб'єктів реалізації державної політики;

– ратифікація міжнародних нормативно-правових актів щодо протидії кіберзлочинності та забезпечення кіберзахисту;

– оптимізація фінансового забезпечення суб'єктів реалізації державної кримінально-правової політики протидії кіберзлочинності;

– підвищення рівня кадрового потенціалу правоохоронної системи щодо протидії кіберзлочинності.

Зазначенні завдання характеризують такі напрями розвитку державної політики як: реформування кримінального законодавства щодо протидії кіберзлочинності; трансформація суб'єктної структури системи державного управління в сфері протидії кіберзлочинності; розширення міжнародно-правового механізму реалізації державної кримінально-правової політики. Відповідно визначенні наступні об'єкти державної політики: регулювання суспільних відносин щодо використання інформаційно-комп'ютерних технологій; регулювання діяльності суспільних інституцій в віртуальному просторі; функціонування правоохоронної системи (діяльність правоохоронних органів) щодо протидії кіберзлочинності; міжнародні відносини щодо протидії кіберзлочинам та забезпечення інформаційної безпеки держави.

Сучасна суб'єктна структура державного управління в сфері протидії кіберзлочинам, представлена: 1) центральними органами виконавчої влади, що реалізують держану кримінально-правову політику протидії кіберзлочинності (Міністерство цифрової трансформації України, Міністерство внутрішніх справ України, Міністерство оборони України, Міністерство юстиції України, Міністерство фінансів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, Національне агентство з питань запобігання корупції, Державна служба фінансового

моніторингу України); 2) суб'єкти правоохоронної діяльності на які покладаються функції з протидії кіберзлочинності, що прямо пов'язані із протидією кіберзлочинності (Служба безпеки України, Національна поліція України, Держане бюро розслідувань, Служба зовнішньої розвідки України); 3) суб'єкти правоохоронної діяльності на які покладаються функції з протидії кіберзлочинності, що опосередковано пов'язані із протидією кіберзлочинності (Національне антикорупційне бюро України, Бюро економічної безпеки України, Державна прикордонна служба України, Національна гвардія України, Державна митна служба України, Управління державної охорони України). Така суб'єктна структура визначає взаємодію з різними видами державної політика.

Методологія реалізація державно-кримінальної політики ґрунтується на методах прямого (укази, постанови, рішення, розпорядження) та непрямого впливу (соціально-психологічні, інформаційні, стимулюючі, профілактичні), а також принципах (обґрунтованості, аналітичності, системності, прозорості, ефективності, комплексності, послідовності, аполітичності, правомочності, гуманізму).

Висновки. Проведене дослідження дозволило розробити комплексну теоретико-методологічну конструкцію державної кримінально-правової політики, що складається з таких послідовних етапів:

1) визначення суспільної проблеми та її симптомів, зокрема симптоми згруповано за детермінантами розвитку кіберзлочинності, системними проблемами правоохоронної діяльності та впливом кіберзлочинності на складові національної безпеки);

2) ідентифікація стейкхолдерів, що здійснено на основі обґрунтування впливу на носіїв публічних, приватних та суспільних інтересів;

3) вихідні положення державної кримінально-правової політики протидії кіберзлочинності;

4) визначення напрямів розвитку державної політики (реформування кримінального законодавства щодо протидії кіберзлочинності; трансформація суб'єктної структури системи державного управління в сфері протидії кіберзлочинності; розширення міжнародно-правового механізму реалізації державної кримінально-правової політики);

5) визначення об'єктів державної політики;

6) обґрунтування суб'єктного складу;

7) визначення методів та принципів реалізації державної політики;

8) запропоновано ключові механізми реалізації.

Список використаної літератури:

1. *Аніщук В.В.* Проблема протидії кіберзлочинності: порівняльно-правовий аналіз / *В.В. Аніщук, С.Г. Зицик* // Науковий вісник Ужгородського Національного Університету. Серія : Право. – 2024. – Вип. 83, Ч. 3. – С. 19–23 [Електронний ресурс]. – Режим доступу : https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/4-2.pdf.
2. *Грицишен Д.О.* Державна політика в сфері запобігання та протидії економічній злочинності : монографія / *Д.О. Грицишен*. – Житомир : Вид. О.О. Євенок, 2020. – 384 с.
3. *Думчиков М.О.* Становлення та генеза кримінальної відповідальності за кримінальні правопорушення у кіберпросторі на тернах України / *М.О. Думчиков, І.В. Каріх* // Юридичний науковий електронний журнал. – 2022. – № 5. – С. 476–478 [Електронний ресурс]. – Режим доступу : http://lsej.org.ua/5_2022/113.pdf.
4. *Заворуєв Р.С.* Протидія кіберзлочинності в Україні / *Р.С. Заворуєв, В.А. Резніченко* // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., 23–25 листоп. – Кропивницький : КНТУ, 2016. – С. 49–50 [Електронний ресурс]. – Режим доступу : https://core.ac.uk/download/pdf/84825476.pdf.
5. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / *Б.М. Головкін, О.І. Денькович, В.В. Луцик, Д.М. Цехан* ; за ред. канд. юрид. наук, доц. *О.Денькович*, д-р права, проф. *Г.Шмельцер*. – Львів : ЛНУ ім. Івана Франка. – 2022. – 298 с. [Електронний ресурс]. – Режим доступу : https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf.
6. *Косиця О.* Актуальні питання вдосконалення законодавства у сфері протидії кіберзлочинності / *О.Косиця* // Jurnalul juridic national: teorie şi practică. – 2017. – № 2. – С. 81–84 [Електронний ресурс]. – Режим доступу : https://ibn.idsi.md/sites/default/files/imag_file/81_84_Aktual%27n%D1%96%20pitannja%20vdoskonalennja%20zakonodavstva%20u%20sfer%D1%96%20protid%D1%96%D1%97%20k%D1%96berzlochinnost%D1%96.pdf.
7. Криза правоохоронної системи України : монографія / За заг. ред. *В.В. Євдокимова*, *Д.О. Грицишена*. – Житомир : Видавничий дім «Бук-друк», 2023. – 584 с.
8. *Леган І.М.* Особливості міжнародного співробітництва щодо запобігання і протидії кіберзлочинності та кібертероризму / *І.М. Леган* // Науковий вісник Міжнародного гуманітарного університету. Сер. : Юриспруденція. – 2021. – № 50. – С. 118–121 [Електронний ресурс]. – Режим доступу : https://vestnik-pravo.mgu.od.ua/archive/juspradenc50/27.pdf.
9. *Лугіна Н.А.* Порівняльний аналіз вітчизняного та європейського законодавства з питань запобігання кіберзлочинності / *Н.А. Лугіна, А.М. Лучук* // Ірпінський юридичний часопис: науковий журнал. – 2023. – Вип. 1 (10). – С. 180–186 [Електронний ресурс]. – Режим доступу : https://ojs.dpu.edu.ua/index.php/irplegchr/article/view/83/82.
10. *Малишев К.В.* Державна політика в сфері трансформації правоохоронної системи: теорія, методологія, організація : монографія / *К.В. Малишев*. – Житомир : Вид. О.О. Євенок, 2022. – 300 с.
11. *Микитчик А.В.* Заходи запобігання кіберзлочинності в Україні / *А.В. Микитчик* // Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку : зб. тез доп.

міжнар. наук.-практ. конф. до 25-річчя ХНУВС, 18 квіт. – Харків : ХНУВС, 2019. – С. 137–138 [Електронний ресурс]. – Режим доступу : https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/63.pdf.

12. *Никончук Н.С.* Кіберзлочинність в Україні: виклики сучасності / *Н.С. Никончук, О.О. Маслова* // Юридичний науковий електронний журнал. – 2021. – № 9. – С. 202–205 [Електронний ресурс]. – Режим доступу : http://www.lsej.org.ua/9_2021/51.pdf.
13. *Піцик Ю.М.* Напрями протидії кіберзлочинам проти власності / *Ю.М. Піцик* // Jurnalul juridic national: teorie şi practică. – 2018. – Т. 2, № 3. – С. 52–54 [Електронний ресурс]. – Режим доступу : http://www.jurnaluljuridic.in.ua/archive/2018/3/part_2/11.pdf.
14. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / *О.Є. Користін, В.М. Бутузов, В.В. Василевич та ін*. – Київ : Скіф, 2012. – 728 с.
15. *Чубоха Н.Ф.* Співвідношення інтересу та суб'єктивного цивільного права / *Н.Ф. Чубоха* // Юридичний науковий електронний журнал. – 2019. – № 4. – С. 56–59 [Електронний ресурс]. – Режим доступу : http://www.lsej.org.ua/4_2019/15.pdf.
16. Стан та особливості протидії кіберзлочинності в Україні в умовах пандемії COVID-19 / *О.М. Шинкарук, В.В. Сеник, О.І. Зачек, Т.В. Магеровська* // Соціально-правові студії. – 2021. – Вип. 3 (13). – С. 68–76 [Електронний ресурс]. – Режим доступу : https://sls-journal.com.ua/web/uploads/pdf/S&LS_2021_Vol.%204,%20No.%203_68-76.pdf.

References:

1. Anishchuk, V.V. and Zytsyk, S.H. (2024), «Problema protydii kiberzlochynnosti: porivnialno-pravovyi analiz», *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu*. Seriia. *Pravo*, Issue 83, Part 3, pp. 19–23, [Online], available at: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/4-2.pdf
2. Hrytsyshen, D.O. (2020), *Derzhavna polityka v sferi zapobihannia ta protydii ekonomichnii zlochynnosti*, monohrafiia, Vyd. O.O. Yevenok, Zhytomyr, 384 p.
3. Dumchykov, M.O. and Karikh, I.V. (2022), «Stanovlennia ta heneza kryminalnoi vidpovidalnosti za kryminalni pravoporushennia u kiberprostori na ternakh Ukrainy», *Yurydychnyi naukovyi elektronnyi zhurnal*, No. 5, pp. 476–478, [Online], available at: http://lsej.org.ua/5_2022/113.pdf
4. Zavoruiev, R.S. and Reznichenko, V.A. (2016), «Protydiia kiberzlochynnosti v Ukraini», *Aktualni zadachi ta dosiahnennia u haluzi kiberbezpeky*, materialy Vseukr. nauk.-prakt. konf., 23–25 lystop., KNTU, Kropyvnytskyi, pp. 49–50, [Online], available at: https://core.ac.uk/download/pdf/84825476.pdf
5. Holovkin, B.M., Denkovych, O.I., Lutsyk, V.V. and Tsekhan, D.M. (2022), *Kiberzlochynnist ta elektronni dokazy = Cybercrime and digital evidence*, navch. posibnyk, in kand. yuryd. nauk, dots. Denkovych, O. and d-r prava, prof. Shmeltser, H. (ed.), LNU im. Ivana Franka, Lviv, 298 p., [Online], available at: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf
6. Kosytsia, O. (2017), «Aktualni pytannia vdoskonalennia zakonodavstva u sferi protydii kiberzlochynnosti», *Jurnalul juridic national: teorie şi practică*, No. 2, pp. 81–84, [Online], available at: https://ibn.idsi.md/sites/default/files/imag_file/81_84_Aktual%27n%D1%96%20pitannja%20vdoskonalennja%20zakonodavstva%20u%20sfer%D1%96%20protid%D1%96%D1%97%20k%D1%96berzlochinnost%D1%96.pdf
7. Yevdokymov, V.V. and Hrytsyshen, D.O. (ed.) (2023), *Kryza pravookhoronnoi systemy Ukrainy*, monohrafiia, Vydavnychyi dim «Buk-druk», Zhytomyr, 584 p.
8. Lehan, I.M. (2021), «Osoblyvosti mizhnarodnoho spivrobitnytstva shchodo zapobihannia i protydii kiberzlochynnosti ta kiberteroryzmu», *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu*. Ser. *Yurysprudentsiia*, No. 50, pp. 118–121, [Online], available at: https://vestnik-pravo.mgu.od.ua/archive/juspradenc50/27.pdf
9. Luhina, N.A. and Luchuk, A.M. (2023), «Porivnialnyi analiz vitchyznianoho ta yevropeiskoho zakonodavstva z pytan zapobihannia kiberzlochynnosti», *Irpinskyi yurydychnyi chasopys: naukovyi zhurnal*, Issue 1 (10), pp. 180–186, [Online], available at: https://ojs.dpu.edu.ua/index.php/irplegchr/article/view/83/82
10. Malyshev, K.V. (2022), *Derzhavna polityka v sferi transformatsii pravookhoronnoi systemy: teoriia, metodolohiia, orhanizatsiia*, monohrafiia, Vyd. O.O. Yevenok, Zhytomyr, 300 p.
11. Mykytchyk, A.V. (2019), «Zakhody zapobihannia kiberzlochynnosti v Ukraini», *Kryminalno-pravovi ta kryminolohichni zasoby protydii zlochynam proty hromadskoi bezpeky ta publichnoho poriadku*, zb. tez dop. mizhnar. nauk.-prakt. konf. do 25-richchia KhNUVS, 18 kvit., KhNUVS, Kharkiv, pp. 137–138, [Online], available at: https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/63.pdf
12. Nykonchuk, N.S. and Maslova, O.O. (2021), «Kiberzlochynnist v Ukraini: vyklyky suchasnosti», *Yurydychnyi naukovyi elektronnyi zhurnal*, No. 9, pp. 202–205, [Online], available at: http://www.lsej.org.ua/9_2021/51.pdf
13. Pitsyk, Yu.M. (2018), «Napriamy protydii kiberzlochynam proty vlasnosti. Jurnalul juridic national: teorie şi practică», Vol. 2, No. 3, pp. 52–54, [Online], available at: http://www.jurnaluljuridic.in.ua/archive/2018/3/part_2/11.pdf
14. Korystin, O.Ye., Butuzov, V.M., Vasylevych, V.V. et al. (2012), *Protydiia kiberzlochynnosti v Ukraini: pravovi ta orhanizatsiini zasady*, navch. posib., Skif, Kyiv, 728 p.
15. Chubokha, N.F. (2019), «Spivvidnoshennia interesu ta subiektyvnoho tsyvilnoho prava», *Yurydychnyi naukovyi elektronnyi zhurnal*, No. 4, pp. 56–59, [Online], available at: http://www.lsej.org.ua/4_2019/15.pdf
16. Shynkaruk, O.M., Senyk, V.V., Zachek, O.I. and Maherovska, T.V. (2021), «Stan ta osoblyvosti protydii kiberzlochynnosti v Ukraini v umovakh pandemii COVID-19», *Sotsialno-pravovi studii*, Issue 3 (13), pp. 68–76, [Online], available at: https://sls-journal.com.ua/web/uploads/pdf/S&LS_2021_Vol.%204,%20No.%203_68-76.pdf

Корзун Світлана Вікторівна – аспірантка Державного університету «Житомирська політехніка».
https://orcid.org/0000-0002-8360-6766.
Наукові інтереси:
– протидія кіберзлочинності.

Korzun S.V.

Theoretical and methodological construction of state criminal law policy to combat cybercrime

In the modern world, where information technologies have deeply penetrated all aspects of our existence, cybercrime is one of the most serious dangers. The formation of an information society is inextricably linked with the growing influence of digital technologies, which, at the same time, has opened up new opportunities for illegal actions. Cybercrimes can harm not only individuals, but also pose a significant threat to state structures and international associations.

The purpose of the article is to study the theoretical and methodological construction of the state criminal law policy to combat cybercrime.

In the process of research, the properties of cybercrime and cybercrime were considered, which define it as a special object of state criminal law policy, namely: extraterritoriality, innovation dependence, multidisciplinary, latency, transformability.

The article presents the content of the stages of formation and implementation of the state criminal law policy to combat cybercrime. The study analyzed the scientific literature on systemic problems of the development of the state criminal law policy, which allowed grouping the problems according to the following vectors: low efficiency of the law enforcement system, inconsistency of the subject structure of state administration, lack of adaptation mechanisms to the international counteraction system. Also, the article, based on the justification of the impact on the bearers of public, private and social interests, identified stakeholders; determined the initial provisions of the state criminal law policy to combat cybercrime; determined the directions of state policy development; determined the objects of state policy and substantiated the subject composition; determined the methods and principles of state policy implementation; proposed key implementation mechanisms.

Keywords: cybercrime; offense; state criminal law policy; information warfare; prevention of cybercrime.

Стаття надійшла до редакції 28.10.2024.