УДК 343.91

КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА: ОСОБА КІБЕРЗЛОЧИНЦЯ

FORENSIC CHARACTERISTIC: THE PERSON OF A CYBERCRIMINAL

Ахтирська Н.М., к.ю.н., доцент,
доцент кафедри правосуддя
Київський національний університет імені Тараса Шевченка

Неділько Я.В., магістрант юридичного факультету
Київський національний університет імені Тараса Шевченка

Статтю присвячено дослідженню особи кіберзлочинця як елемента криміналістичної характеристики. Проведено аналіз наукової літератури з питань визначення поняття і класифікації особи кіберзлочинця як елемента криміналістичної характеристики. Визначено, що аналіз різних точок зору щодо особистості злочинця дає змогу зробити висновок, що особливості, які характеризують ідентичність кіберзлочинця, варто поділити на такі основні групи: соціально-демографічні, моральні та психологічні.
Ключові слова: кіберпростір, кіберзлочини, криміналістична характеристика, особа злочинця, особа кіберзлочинця.

Статья посвящена исследованию лица киберпреступника как элемента криминалистической характеристики. Проведен анализ научной литературы по вопросам определения понятия и классификации лица киберпреступника как элемента криминалистической характеристики. Определено, что анализ различных точек зрения относительно личности преступника позволяет сделать вывод, что особенности, характеризующие идентичность киберпреступника, следует разделить на следующие основные группы: социально-демографические, нравственные и психологические.
Ключевые слова: киберпространство, киберпреступления, криминалистическая характеристика, личность преступника, личность киберпреступника.

The article is devoted to the study of the identity of a cybercriminal as an element of forensic characteristics. It was emphasized that the offender's personality should be the subject of a comprehensive research.

It is determined that the analysis of different points of view regarding the offender's personality makes it possible to conclude that the features that characterize the identity of a cybercriminal should be divided into the following main groups: socio-demographic, moral and psychological. Socio-demographic features include gender, age, education, occupation, marital status, residence, social origin, role in society and in the family and everyday life. A group of moral attributes characterizing the offender's personality contains information about the outlook, interests and needs, orientation, predispositions and habits. Signs of psychological content characterize psychological properties and features: the level of mental development and intelligence, emotionality, temperament, skills and ability of the offender.

It is noted that despite the variety of opinions in the forensic literature about the forensic character of the offender's personality, his analysis during the pre-trial investigation is crucial in criminal proceedings.

It is indicated that today the most suitable classification of cybercriminals, is one that performs the following differentiation: 1) "hackers"; 2) "spies"; 3) "terrorists"; 4) "mercenary criminals"; 5) "vandal"; 6) mentally ill persons who suffer from a new mental illness. The proposed classification is considered sufficiently informative and more detailed, making it more suitable for use in the combating cybercrime. Also, author noted that it is not exhaustive. Next groups of cybercriminals should be added: "rapists", that is, those who use informational technologies, in the absence of physical contact, commit violent crimes and "sexual criminals" who are characterized by activities related to the spread of pornographic objects or materials, coercion to acts of sexual nature, committing abusive acts, sexual harassment against a person, including minors, or groups of persons.

The author analyzed the features of the criminal – "hacker" in detail.
Key words: cyber space, cybercrime, forensic characteristics, offender's personality, personality of a cybercriminal.

Вивчення особи злочинця має вагоме значення для виявлення закономірностей злочинної поведінки, необхідності, аби зрозуміти спосіб мислення та скоєння злочину, а також організації протидії кримінальним правопорушенням і їх профілактики. Саме тому в сучасних умовах розвитку інформаційних технологій і збільшення злочинних діянь у кіберпросторі особливої актуальності набуває питання ефективного розслідування вказаної категорії кримінальних правопорушень.

Проблематика особи злочинця загалом та особи кіберзлочинця зокрема була предметом дослідження таких учених, як Н.М. Ахтирська, Р.С. Бєлкін, П.Д. Біленчук, В.М. Бутузов, В.В. Василевич, І.М. Даньшин, Н.І. Клименко, О.Є. Користін, В.К. Лисиченко, Л.П. Паламарчук, М.А. Погорецький, Б.В. Романюк, М.В. Салтевський, В.С. Цимбалюк, В.Ю. Шепітько, Н.П. Яблоков та інші. Однак постійний розвиток науки й техніки вимагає аналізу проведених досліджень з урахуванням сучасного етапу розвитку комп'ютерних технологій.

Мета статті – визначення основних підходів до розуміння поняття «особа кіберзлочинця» як елемента криміналістичної характеристики.

Особа злочинця є предметом комплексного дослідження. Зазвичай учені-криміналісти виділяють чотири основні напрями такого дослідження: кримінально-правове, кримінально-процесуальне криміналістичне і кримінологічне [1, с. 165].

На відміну від інших досліджень особи злочинця, криміналістика, зазначає Л.П. Паламарчук, вивчає передусім «професійні» звички злочинців, які проявляються в основному в певних способах і прийомах учинення злочинів, у характерному «почерку» злочинця, що залишається на місці вчинення злочинів, адже результати кожної злочинної діяльності містять сліди людини, яка їх залишила. Виявлення на місці скоєння злочину речових доказів дає змогу визначити деякі особисті соціально-психологічні ознаки злочинця, його досвід, професію, соціальні знання, стать, вік, особливості взаємодії з потерпілим [2, с. 74].

На погляд М.В. Салтевського, криміналістична характеристика особи злочинця повинна давати опис людини як соціально-біологічної системи, властивості й ознаки якої відображаються в матеріальному середовищі та використовуються для розслідування злочинів. До таких властивостей належать фізичні, біологічні й соціальні. Криміналістична характеристика – це такий опис рис зовнішності і внутрішніх властивостей людини, що дає можливість уявити обличчя людини, її портрет як соціально-біологічної істоти [3, с. 422].

Розкриваючи зміст особи злочинця як елемента криміналістичної характеристики, В.Ю. Шепітько зауважує,

що особа злочинця має певні дані демографічного характеру, деякі моральні якості та психологічні особливості [4, с. 258].

Аналіз різних точок зору щодо особи злочинця дає змогу зробити висновок, що ознаки, які характеризують особу кіберзлочинця, доцільно ділити на такі основні групи: соціально-демографічні, моральні та психологічні. До соціально-демографічних зараховують стать, вік, освіту, професію або рід зайняття, сімейний стан, місце проживання, соціальне походження, роль у суспільстві й у сімейно-побутовій сфері. Група моральних ознак, що характеризують особу злочинця, містить дані щодо світогляду, інтересів і потреб, спрямованості, схильності і звичок. Ознаки психологічного змісту характеризують психологічні властивості й особливості: рівень розумового розвитку й інтелект, емоційність, темперамент, здібності, навички й уміння суб'єкта злочину. Незважаючи на різноманітність наявних у криміналістичній літературі думок з приводу криміналістичної характеристики особи злочинця, її дослідження під час досудового розслідування має вирішальне значення в кримінальному провадженні.

Характеризуючи особу, яка вчиняє злочини з використанням інформаційних технологій (кіберзлочини), Л.П. Паламарчук відмічає її основну ознаку: у цю злочинність втягнуто широке коло осіб, від професіоналів до дилетантів. Правопорушники мають різний соціальний статус і різний рівень освіти (навчання та виховання) [2, с. 74]. Поділяючи цю точку зору, варто зауважити, що в криміналістичній літературі мають місце різні класифікації цієї категорії правопорушників.

Найбільш поширеною залишається класифікація, яку наводить Г.Т. Мегрелішвілі, поділяючи кіберзлочинців на декілька груп: До першої групи науковець зараховує осіб, відмінною особливістю яких є поєднання професіоналізму й фанатизму в галузі комп'ютерної техніки і програмування. Такі особи не мають чіткого протиправного наміру, діють виключно для прояву своїх професійних та інтелектуальних здібностей. Вони свідомі й азартні. Підвищення заходів щодо забезпечення комп'ютерної безпеки розглядають як виклик їхнім здібностям. Особливість учинення кіберзлочинів цією групою осіб характеризується відсутністю підготовки і плану дій, оригінальністю способу вчинення, а також тим, що заходи щодо приховування злочину не вживаються. До другої групи входять особи, які страждають на інформаційні хвороби або комп'ютерні фобії, – це новий вид психічних розладів, проте визнаних Всесвітньою організацією охорони здоров'я. Третя група осіб – висококваліфіковані фахівці, які часто мають вищу технічну освіту. Проте, на відміну від першої групи, це професіонали зі стійкими злочинними навичками і яскраво вираженими корисливими цілями [5, с. 180–181].

Подібні міркування щодо наведеної класифікації в науковій літературі висловлює й В.Б. Вєхов [6, с. 134–136]. Поділяючи наведену позицію, варто відмітити класифікацію, що наводиться В.В. Криловим [7, с. 620] і підтримується Л.П. Паламарчук [8, с. 464–465]. Так, залежно від рівня професійної підготовки й соціального стану вони виділяють такі групи кіберзлочинців: 1) «хакери» – особи, які розглядають захист комп'ютерних систем як особливий виклик і зламують їх для одержання повного доступу до системи й задоволення власних амбіцій; 2) «шпигуни» – особи, які зламують комп'ютери для одержання інформації, що можна використати в політичних, військових, економічних та інших цілях. «Шпигун» полює за конфіденційною інформацією, що зберігається чи обробляється в автоматизованих системах або комп'ютерних мережах; 3) «терористи» – особи, які розглядають злом інформаційних систем як створення ефекту небезпеки з метою політичного та іншого впливу; 4) «корисливі злочинці» – особи, які проникають в інформаційні системи для одержання особистої майнової або немайнової вигоди; 5) «вандали» – особи, які зламують інформаційні системи для подальшого руйнування; 6) психічно хворі особи, які страждають від нового психічного захворювання – інформаційної хвороби або комп'ютерної фобії.

На наш погляд, запропонована класифікація є досить змістовною й більшою мірою деталізованою, що робить її придатнішою до застосування під час протидії кіберзлочинам. Разом із тим вона не є вичерпною. Пропонуємо доповнити її такими групами кіберзлочинців.

Зокрема, з подальшим розвитком усесвітньої мережі Інтернет останніми роками виникли нові способи вчинення злочинів, зокрема доведення до самогубств. При цьому новий спосіб доведення до самогубства набирає обертів у світі разом зі зростанням кількості постійних користувачів мережі Інтернет. Набули поширення самогубства підлітків, яких спонукали до цього в так званих «групах смерті» в соціальних мережах. Україна також не стала винятком [9]. Це змусило законодавця до внесення змін до ст. 120 Кримінального кодексу (далі – КК) України «Доведення до самогубства» й установлення кримінальної відповідальності за будь-яке сприяння особі в учиненні нею самогубства чи спроби самогубства [10]. Особи, які вчиняють такі дії, повинні бути виокремлені в самостійну групу – «насильники», тобто особи, які з використанням інформаційних технологій, за відсутності фізичного контакту, вчиняють насильницькі злочини, зокрема доведення до самогубства або до замаху на самогубство.

Відповідно до звіту Європейського центру Європолу з боротьби з кіберзлочинністю, опублікованого у 2017 році [11], сьогодення характеризується розповсюдженням сексуального примусу та шантажу дітей з використанням мережі Інтернет як виду злочину проти дітей. Такі дії набули поширення і стосовно дорослих. Отже, можна говорити про виникнення ще одної групи кіберзлочинців – «сексуальні злочинці». Для них характерною є діяльність, пов'язана з розповсюдженням порнографічних предметів чи матеріалів, примушування до дій сексуального характеру, вчинення розпусних дій, сексуальних домагань щодо певної особи, у тому числі неповнолітніх, чи групи осіб.

Поділяючи точку зору тих науковців, які погоджуються з наведеною вище класифікацією, зупинимось детальніше на хакерах, які становлять особливу групу кіберзлочинців. Більшість науковців факт появи кіберзлочинності в суспільстві пов'язує саме з хакерами, користувачами обчислюваних систем і мереж ЕОМ, які займаються пошуком незаконних методів отримання самовільного доступу до засобів комп'ютерної техніки та баз даних, а також використання їх із корисливою метою. Термін «хакер» (від англ. «hacker») не завжди сприймався як синонім поняттю «злочинець». Дослівно це трудівник, найманий робітник. Спочатку так називали програмістів, які були спроможні розробляти програми без попередньої підготовки й оперативно вносити виправлення до програм, що не мали документації [12, с. 461].

Сутність сучасного хакерства, як зазначає Н.М. Ахтирська, полягає в тому, щоб змусити програмне забезпечення працювати не так, як було задумано розробниками та системними адміністраторами. Мотивами такої діяльності може бути поглиблене вивчення програми із цікавості, намагання зробити закриту інформацію загальнодоступною, для одержання матеріальної вигоди тощо. Науковець не тільки досить вдало розкриває зміст хакерства, а й окреслює його види: 1) хакер мережевий – особа, яка займається дослідженням програмного забезпечення, встановленого на Internet-серверах (або в локальних мережах), з метою одержання несанкціонованого доступу до сервера чи порушення його роботи. Для такого виду діяльності необхідні знання мережевих протоколів та архітектури операційних систем. Виділяють два види мережевого хакерства: а) хакерство велике, яке полягає в самостійному пошуку відомих типів помилок,

б) хакерство дрібне – script-kidding – пошук на сервері; 2) кракери (cracker) – це програмісти високого рівня, які займаються зламом програмного забезпечення, щоб одержати з програм з обмеженими функціональними характеристиками повноцінні комерційні версії; виготовляють програми, необхідні для цієї мети; 3) фрикери (phreaker) – досліджують телефонні мережі з метою знайти можливість здійснювати безоплатні дзвінки (фрикерство вважається першим видом хакерської діяльності 60–70 років XX століття); 4) кардери (carder) – розробляють способи одержання кредитних карток і даних про їх власника. Як правило, така діяльність поєднується з хакерством і вважається найнебезпечнішим видом діяльності, оскільки завдає значної шкоди; 5) особи, які пишуть шкідливі програми (virus – maker), віруси, поштові віруси [13, с. 98–99].

За соціологічними та кримінолого-криміналістичними дослідженнями, проведеними вітчизняними й зарубіжними науковцями, за віковими ознаками кіберзлочинців поділено на три категорії. Перша – молодь віком від 11 до 15 років, яка займається переважно злочинами з використанням кредитних карток, телефонних номерів та автоматів по видачі готівки, «зламуючи» коди й паролі. Друга – особи віком 17–25 років, які займаються комп'ютерним хакерством. У більшості випадків це студенти, які з метою підвищення свого «пізнавального» рівня встановлюють тісні стосунки з хакерами інших країн і за допомогою електронних мереж BBS обмінюються з ними інформацією та викрадають її з різних банків даних. До третьої категорії належать особи віком 30–45 років, які вчиняють злочини з корисливою метою та шпигунство [14, с. 107; 15, с. 477].

За результатами цих досліджень також установлено, що вік кіберзлочинця коливається в середньому від 15 до 45 років. У 33% вік злочинців на момент учинення злочину не перевищував 20 років, 13% – старші 40 років і 54% – мали вік від 20 до 40 років. Як приклад наведемо віковий розподіл злочинців, заарештованих у США. Так, близько 83% – чоловіки, тобто жінки становлять близько 17%. Проте частка жінок швидко зростає у зв'язку з комп'ютеризацією робочих місць, які займають переважно жінки: секретар, бухгалтер, економіст, менеджер тощо. Більшість осіб у віці від 14 до 21 року навчались у середніх спеціальних і вищих навчальних закладах. За освітнім рівнем: 20% мали середню освіту, 20% – середню спеціальну і 40% – вищу. Були службовцями державних установ та організацій, які використовували інформаційні технології у своїх виробничих процесах, – 97%. Крім того, 38% діяли без співучасників, тоді як 62% вчинили злочини в складі організованих груп [12, с. 453–455].

Аналіз даних судової статистики про склад засуджених в Україні за 2013–2017 роки за злочини, передбачені ст. ст. 361–363-1 КК України, показав, що на момент учинення злочину на вікову групу від 30 до 50 років припадає 54% засуджених, на другому місці – вікова група від 25 до 30 років – 21,9%, на третьому – група осіб віком від 18 до 25 років – 18,6%, вікова група від 50 до 65 років – 4,9%. Засуджених за ці діяння у вікових групах від 14 до 16 років і від 16 до 18 років немає, а у віковій групі від 65 років і старше засуджено лише 1 особу. Серед засуджених – 95,6% громадян України, громадян інших держав – 4,4%, жінок – 11,5%. Осіб, які раніше не притягувались до кримінальної відповідальності, – 88,5%, і тільки 6% тих, хто має непогашену та незняту судимість, при цьому судимості за іншими категоріями злочинів. У складі групи осіб діяли 24% засуджених і в складі організованих груп – 1,6%.

За освітнім рівнем кіберзлочинці характеризуються так: повну вищу освіту мали 45,9%, базову вищу – 6%, професійно-технічну – 18%, повну загальну – 24%, базову загальну – 6%. Залежно від роду діяльності поділяються так: державні службовці – 4,9%, робітники – 11,5%, приватні підприємці – 7,7%, студенти – 1,6%, працездатні, які не працювати й не навчались, – 55,7%, безробітні – 2,2%, пенсіонери – 1,0% [16].

Отже, найбільша кількість злочинів цієї категорії вчиняється громадянами України у віці від 30 до 50 років, переважно чоловіками, раніше не судимими за кіберзлочини. Серед осіб, які вчинили злочини, домінують особи з повною вищою освітою, професійно-технічною та повною загальною освітою. Ці дані загалом збігаються з наведеними загальними тенденціями кіберзлочинності. Разом із тим в Україні більше ніж половини засуджених – це працездатні особи, які на момент учинення злочину не працювали й не навчались, за проведеними дослідженнями, 97% становлять державні службовці, які використовували інформаційні технології, тоді як у нашій країні – 4,9%. Крім того, досить низький відсоток засуджених осіб у складі організованих груп. Це варто враховувати в практичній діяльності з метою протидії кіберзлочинності.

Отже, дані про особу злочинця є невід'ємним складником криміналістичної характеристики кіберзлочинів і, безперечно, ключовим її елементом. Під час розслідування злочинів зазначеної категорії дослідження особи злочинця має важливе практичне значення, оскільки це дає змогу звузити коло осіб, серед яких може знаходитись особа, яка вчинила злочини з використанням інформаційних технологій, висунути обґрунтовані версії щодо мотиву, мети, способу вчинення та приховування злочину, побудувати реалістичний план та організувати ефективне розслідування, вибрати тактику проведення слідчих (розшукових) і негласних слідчих (розшукових) дій.

ЛІТЕРАТУРА

1. Руководство для следователей / отв. ред. В.В. Найденов, П.А. Олейник. Москва: Юридическая литература, 1981. Часть I. 543 с.

2. Паламарчук Л.П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж: дис. … канд. юрид. наук: спец. 12.00.09. Київ, 2004. 215 с.

3. Салтевський М.В. Криміналістика (у сучасному викладі): підручник. Київ: Кондор, 2008. 588 с.

4. Шепитько В.Ю. Криминалистика: курс лекций. 2-е изд., перераб. и доп. Харьков: ООО «Одиссей», 2005. 368 с.

5. Мегрелишвили Г.Т. Криминологический и психологический портрет личности преступников в сфере высоких технологий. Весник Том. гос. ун-та. 2007. № 299. С. 180–181.

6. Вехов В.Б., Голубев В.А. Расследование компьютерных преступлений в странах СНГ: монография / под ред. Б.П. Смагоринского. Волгоград: ВА МВД России, 2004. 304 с.

7. Криминалистика: учебник / отв. ред. Н.П. Яблоков. 2-е изд., перераб. и доп. Москва: Юристъ, 1999. 718 с.

8. Розслідування окремих видів злочинів: навч. посібник / О.В. Бишивець, М.А. Погорецький, Д.В. Сергєєва та ін.; за ред. М.А. Погорецького та Д.Б. Сергєєвої. Київ: Алерта, 2015. 563 с.

9. Доведення до самогубства: правовий аспект. Репортер. 28 березня 2017 року. URL: http://reporter.pl.ua/novini/sytuatsija/26463-dovedennja-do-samogubstva-pravovyj-aspekt.

10. Про внесення зміни до статті 120 Кримінального кодексу України щодо встановлення кримінальної відповідальності за сприяння вчиненню самогубства: Закон України від 8 лютого 2018 року № 2292–VIII. URL: http://zakon.rada.gov.ua/laws/show/2292-19.

11. Сексуальний примус та шантаж через мережу Інтернет як вид злочину проти дітей, травень 2017. URL: https:// rescentre.org.ua/images/Uploads/Files/internet_safety_dl/Europol_online-coersion_ukr.pdf.

12. Криміналістика: підручник / П.Д. Біленчук, В.К. Лисиченко, Н.І. Клименко та ін.; за ред. П.Д. Біленчука. 2-ге вид., випр. і доп. Київ: Атіка, 2001. 544 с.

13. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів: навч. посіб. Київ: ВПЦ «Київський університет», 2018. 229 с.
14. Комп'ютерна злочинність: навч. посіб. / П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк та ін. Київ: Атіка, 2002. 240 с.
15. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. / О.Є. Користін, В.М. Бутузов, В.В. Василевич та ін. Київ: Видавничий дім «Скіф», 2012. 728 с.
16. Судова статистика. Форма № 7 «Звіт про склад засуджених»: URL: http://court.gov.ua/inshe/sudova_statystyka/.

УДК 343.851

ОРГАНІЗАЦІЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ У ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ, ЩО ВЧИНЯЮТЬСЯ СЛУЖБОВИМИ ОСОБАМИ

ORGANIZATION OF THE ACTIVITY OF LAW ENFORCEMENT AGENCIES IN THE FIGHT AGAINST CRIMES COMMITTED IN THE SPHERE OF ECONOMIC ACTIVITY BY OFFICIALS

Дунас М.О., здобувач
Львівський університет бізнесу та права

У статті розкрито поняття і зміст організаційної діяльності підрозділів правоохоронних органів у запобіганні злочинам у сфері господарської діяльності. Визначено перелік державних правоохоронних і контролюючих органів, які здійснюють протидію зазначеним злочинам. Окреслено основні завдання Департаменту захисту економіки в запобіганні злочинам у сфері господарської діяльності. Розглянуто заходи щодо протидії фіктивній господарській діяльності.
Ключові слова: злочини, господарська діяльність, службові особи, організація протидії, запобігання, заходи забезпечення, правоохоронні органи, фіктивне підприємництво.

В статье раскрыты понятие и содержание организационной деятельности подразделений правоохранительных органов в предупреждении преступлений в сфере хозяйственной деятельности. Определен перечень государственных правоохранительных и контролирующих органов, осуществляющих противодействие указанным преступлениям. Определены основные задачи Департамента защиты экономики в предотвращении преступлений в сфере хозяйственной деятельности. Рассмотрены меры по противодействию фиктивной хозяйственной деятельности.
Ключевые слова: преступления, хозяйственная деятельность, должностные лица, организация противодействия, предотвращение, меры обеспечения, правоохранительные органы, фиктивное предпринимательство.

The article deals with the concept and content of organizational activity of law enforcement agencies in preventing crimes in the field of economic activity. The list of state law enforcement and controlling bodies, which carry out counteraction to said crimes, is determined. The main tasks of the Department for the Protection of the Economy in the Prevention of Crimes in the Field of Economic Activities are outlined. Measures to counteract fictitious economic activity are considered. Today, the main direction of combating crime in the field of economic activity is the transition to European principles of management and the exit from the total economic crisis of the Ukrainian economy, the struggle against the monopolization of commercial activity and the transparency of the banking sector. Of great importance in the prevention of economic crimes belongs to the units of the controlling bodies, which carry out measures of preliminary verification of misuse of budget funds and during the implementation of public procurement. The study of financial and economic activities of business entities in conjunction with operational and investigative measures provides positive results in preventing the theft and legalization of money laundered.
Key words: crimes, economic activity, officials, organization of counteraction, prevention, measures of support, law enforcement bodies, fictitious entrepreneurship.

Сучасні процеси глобалізації економічного розвитку та наявність міжнародної банківської сфери є визначальним фактором, що зумовлює динаміку розвитку злочинності у сфері господарської діяльності, яка набуває характеру системності й вимагає відповідної організації діяльності підрозділів правоохоронних органів. Для здійснення запобіжної діяльності підрозділи правоохоронних органів мають проводити спільні заходи, які потребують відповідного організаційного механізму та засобів забезпечення.

Основи організаційної діяльності правоохоронних органів щодо запобігання злочинам досліджували вчені: Г.А. Аванесов, Ю.М. Антонян, О.М. Бандурка, І.В. Василинчук, О.Ф. Гіда, В.В. Голіна, Л.М, Даньшин, О.М. Джужа, А.П. Закалюк, О.Г. Кальман, І.І. Карпець, Я.Ю. Кондратьєв, О.М. Литвак, Ю.Ю. Орлов, Л.П. Скалозуб, О.О. Юхно й ін.

Метою статті є визначення поняття і змісту організаційної діяльності підрозділів правоохоронних органів у запобіганні злочинам у сфері господарської діяльності.

Протидія злочинам у сфері господарської діяльності здійснюється держаними правоохоронними органами, контролюючими органами та окремими громадськими формуваннями в межах наданих їм законом повноважень [1, с. 14].

До таких державних органів законодавством зараховано насамперед тих, на кого покладені основні функції протидії господарським злочинам. До другої категорії належать підрозділи правоохоронних органів, які опосередковано здійснюють таку протидію в межах виконання інших функцій.

До підрозділів правоохоронних органів, які здійснюють протидію злочинам у сфері господарської діяльності, необхідно зарахувати Департамент захисту економіки (далі – ДЗЕ) Національної поліції України, Державну фіскальну службу України, Державну митну службу України, Державну прикордонну службу України, Службу безпеки України, Державну аудиторську службу та інші, які входять до підпорядкування Кабінету Міністрів України.

Діяльність зазначених суб'єктів виражається в їхніх повноваженнях щодо правових та організаційних заходів, форм і засобів здійснювання ними системи запобігання злочинності.

Поняття кримінологічного запобігання злочинності становлять відносини між підрозділами правоохоронних

органів, спрямовані на виявлення й усунення причин та умов учинення злочинів [2, с. 14].

Діяльність із запобігання злочинам, за визначенням окремих науковців (В.В. Голіна, А.Ф. Зелінський, О.М. Литвак та ін.), полягає в застосуванні комплексу державних заходів, скерованих на вдосконалення господарських відносин, з метою усунення причин та умов їх учинення [3, с. 25].

Заходи протидії господарським злочинам підрозділами правоохоронних органів полягають у їхній діяльності з метою своєчасного виявлення та розслідування господарських злочинів (95%); профілактичної діяльності на підприємствах комерційних структур і в банківській сфері (65%); застосовування заходів щодо відшкодування збитків (88%); забезпечення захисту споживачів (67%); взаємодії з представниками засобів масової інформації щодо стану господарської злочинності й уживання заходів щодо її подолання (72%).

Сьогодні основним напрямом протидії злочинам у сфері господарської діяльності є перехід на Європейські принципи господарювання та вихід із тотальної економічної кризи української економіки, боротьба з монополізацією комерційної діяльності й прозорість діяльності банківського сектору [4, с. 243].

Велике значення в запобіганні господарським злочинам належить підрозділам контролюючих органів, які здійснюють заходи попередньої перевірки нецільового використання бюджетних коштів і під час здійснення публічних закупівель. Дослідження фінансово-господарської діяльності підприємницьких структур у взаємодії з оперативно-розшуковими заходами дає позитивні результати із запобігання викраденню та легалізації грошових засобів, одержаних злочинним шляхом [5, с. 254].

Окремими дослідженнями підтверджено, що в процесі нецільового використання бюджетних коштів у рік викрадається до 1,4 млрд. грн. Водночас за останні п'ять років правоохоронними органами виявляється всього 25 злочинів за ст. 210 Кримінального кодексу України [6, с. 1].

Основні функції щодо запобігання злочинам у сфері господарської діяльності належать підрозділам ДЗЕ Національної поліції України.

До основних пріоритетних завдань у діяльності ДЗЕ на сучасному етапі належить протидія зловживанням посадових осіб у сфері господарської діяльності, забезпечення повного відшкодування матеріальних збитків державі та юридичним і фізичним особам, здійснення заходів щодо забезпечення виконання стратегічних напрямів розвитку. До основних завдань ДЗЕ необхідно зарахувати захист господарських відносин від протиправних дій; запобігання господарським злочинам; виявлення правопорушень у сфері підприємництва; викриття службових осіб, які вчиняють правопорушення у сфері господарської діяльності; відшкодування збитків від учинених господарських злочинів.

Як показав аналіз дослідження, ефективність запобігання господарським злочинам залежить від багатьох факторів, один із яких – наскільки правильно і продумано організована робота підрозділів ДЗЕ, до повноважень яких належить викриття цих злочинів.

Поняття «організація» французького походження, означає *упорядкування*, латинського і грецького – *інструмент, знаряддя.* Отже, організація означає сукупність пов'язаних між собою складових частин (елементів) відповідного об'єкта, а також зв'язків (взаємовідносин) між ними й іншими об'єктами, в результаті чого утворюється певне зовнішнє організоване середовище [7, с. 368].

У запобіжній діяльності організація розглядається як цілеспрямована діяльність керівників підрозділів, яка основана на законних і підзаконних нормативних актах зі створення оптимальних умов функціонування цих підрозділів з метою вирішення поставлених перед ними завдань.

У спеціальній літературі організація підрозділу правоохоронного органу розглядається як система використання наявних сил, засобів, методів у боротьбі з правопорушеннями та злочинами. Отже, на нашу думку, організація запобігання господарським злочинам – комплексна цілеспрямована діяльність уповноважених на те суб'єктів з дотриманням вимог нормативно-правових актів і відомчих інструкцій і наказів з використання наявних сил, засобів, заходів і методів щодо своєчасного, систематичного отримання інформації про підготовку чи вчинення економічній злочинів.

Як свідчить аналіз практичної діяльності й наукових досліджень, позитивні зміни в організації запобіжної діяльності щодо протидії злочинам у сфері господарської діяльності проходять дуже повільно. Це пов'язано з низкою проблем, серед яких, на нашу думку, доцільно виділити принаймні три такі проблеми, а саме: *правову* (неповнота й суперечливість нормативно-правової бази); *організаційну* (відсутність у цій роботі системності й належного контролю передусім на регіональному рівні, завантаження співробітників правоохоронних органів виконанням невластивих функцій тощо); *кадрову* (брак досвідчених, професійно підготовлених працівників, прорахунки в організації їх навчання й перепідготовки, плинність кадрів, недосконаліть реформування правоохоронних органів) [8, с. 10].

Ці та інші проблеми зумовили необхідність формування нової стратегії, основне спрямування заходів якої – удосконалення профілактичної діяльності насамперед під час виявлення господарських злочинів.

Виходячи із цього, а також результатів дослідження, до основних напрямів удосконалення запобігання злочинам у сфері господарської діяльності підрозділів ДЗЕ доцільно зарахувати такі: законодавчу та нормотворчу діяльність (45%); організаційні заходи (34%); роботу у взаємодії з контролюючими органами (32%); належне застосування оперативно-технічних заходів (44%); формування банків даних і взаємного обміну інформацією (55%); організацію навчального процесу (32%); контроль за станом і результатами запобіжної роботи (25%); матеріально-технічне та фінансове забезпечення (40%) тощо.

На нашу думку, вищезазначені елементи є основними, обов'язково повинні входити в процес організації оперативної роботи, залежно від обставин справи та запланованих заходів вони можуть бути розширені або виступати як додаткові.

Одне з особливих місць в організації запобіганням злочинам у сфері господарської діяльності належить правильній організації оперативного обслуговування об'єктів, де можуть учинятись злочини, що сприяє своєчасному безперервному надходженню оперативної інформації про їх підготовку або скоєння.

Для цього здійснюється планування й розстановка оперативних працівників, чітке визначення їхніх функціональних обов'язків, максимальне використання можливостей сил і засобів підрозділів ДЗЕ, використання взаємодії з іншими суб'єктами протидії.

Окремо варто визначити засоби оперативно-розшукової діяльності, які використовуються у протидії фіктивному підприємництву, мають велике значення (88%). Теорія оперативно-розшукової діяльності, яка сформувалась у колишньому СРСР, традиційно вважала засобами оперативно-розшукової діяльності оперативні обліки, оперативну техніку та службово-розшукових собак [9, с. 66].

Такий погляд на засоби оперативно-розшукової діяльності зберігається у вітчизняній науці до цього часу. Разом із тим, на думку вчених, до засобів оперативно-розшукової діяльності варто зарахувати оперативні та інші обліки, розвідувальні комп'ютерні програми, оперативну техніку, житлові, службові й інші приміщення, засоби маскування та імітації, гроші, спеціально навчених тварин [10, с. 279–282].