УДК 343.9.01:004(477)

Мейсар Андрій Андрійович –
студент 5 курсу 8 групи
факультету адвокатури
НЮУ імені Ярослава Мудрого

Andrii A. Meisar –
5th year student of group 8,
Barristers' Faculty,
Yaroslav Mudryi National Law University
(77 Pushkinska Street, Kharkiv, 61024, Ukraine)

Ободовський Дмитро Валерійович –
студент 5 курсу 8 групи
факультету адвокатури
НЮУ імені Ярослава Мудрого

Dmytro V. Obodovskyi –
5th year student of group 8,
Barristers' Faculty,
Yaroslav Mudryi National Law University
(77 Pushkinska Street, Kharkiv, 61024, Ukraine)

Кіберзлочинність: сучасний стан та заходи індивідуального захисту

У цій статті увага була зосереджена на термінологічному аспекті, детермінантах, а також засобах протидії кіберзлочинності яка стає все більш поширеною в кіберпросторі. Саме з термінологічною проблематикою стикаються дослідники даного виду злочинності. Через недосконаліть правової бази існують різні підходи до визначення понять - кіберпростір, кіберзлочин та кіберзлочинність. Така термінологічна розбіжність значно ускладнює кваліфікацію, а отже і розслідування та попередження такого виду злочинності.

Ключові слова: *кіберзлочин, кіберпростір, комп'ютерний злочин, особа кіберзлочинця, кіберзахист.*

В этой статье внимание было сосредоточено на терминологическом аспекте, детерминантах, а также средствах противодействия киберпреступности которая становится все более распространенной в киберпространстве. Именно с терминологической проблематикой сталкиваются исследователи данного вида преступности. Из-за несовершенства правовой базы существуют различные подходы к определению понятий - киберпространство, киберпреступления и киберпреступности. Такие терминологические расхождение значительно усложняют квалификацию, а следовательно расследования и предупреждения даного вида преступности.

Ключевые слова: *киберпреступление, киберпространство, компьютерное преступление, личность киберпреступника, киберзащита.*

A.A. Meisar, D.V. Obodovskyi Cyber Crime: Current State and Activities of Individual Protection

In this article attention was paid to terminology, determinants and methods of combating cybercrime, which are becoming more common in cyberspace. Especially with the terminology problem faced by researchers of this type of crime, which has no boundaries. Due to the imperfection of the legal framework, many countries have a different understanding of key concepts such as cyberspace, cybercrime. Such a terminological difference greatly complicates the qualification, and therefore the investigation and prevention of this type of crime. The dynamics of cybercrime is constantly increasing, as the price of this type of crime increases. Cybercrime can be

committed both individually and by a group of people who may not even be personally acquainted and do not know the real names of each other and communicate through the Internet. Cybercriminals tend to seek some financial gain directly or through the sale of stolen data. There are frequent cases when such a crime is committed on request. However, due to the fact that this type of crime is committed in most cases by young people from the so-called Millennial generation, such motivators as the feeling of success and popularity among peers or in cyberspace are worthy of attention. Given the fact that cybercrime is extremely latent and low statistics on disclosure of the perpetrator, there is a sense of impunity, and some generally do not consider it a crime. We are constantly faced with digital technology. Cyberspace occupies an increasing part of our lives. It is there that we store information, conduct private and official correspondence, carry out entrepreneurial activity, manage finances and much more. However, for such convenience, we paid security. The urgency of the article leads, in particular, to the decline of Ukraine's position in international ratings on the study of cyber security. As an example, in the ranking of national cyber security, which is the Estonian Academy of Electronic Governance, Ukraine - at 26th place, which is 3 positions worse than last year.

Keywords: *cybercrime, cyberspace, computer crime, person of a cyber criminal, cyber defense.*

Постановка проблеми. На сьогодні в Україні та світі спостерігається стрімкий розвиток інформаційно-телекомунікаційних технологій, який призводить до змін в економічній, соціальній, культурній і політичній сферах. З одного боку, такий динамічний розвиток є дуже позитивним, однак з іншого, використання комп'ютерних технологій із корисливих та інших мотивів може становити не лише особисту небезпеку для громадян, їх службової діяльності, суспільного порядку, моральності, а й створювати загрозу національній безпеці держави та світу в цілому**.**

Актуальність даної теми в час інформаційної війни, активного впровадження електронного документообігу, як на приватному, так і на міждержавному рівні, криптовалют і блокчейн технологій, а також стабільному, стрімкому подорожчанню прав інтелектуальної власності неможливо переоцінити. З проблемами кіберзлочинності стикаються як прості громадяни, так і юридичні особи міжнародного рівня, держави і державні об'єднання. Не дивлячись на вдосконалення засобів які вживаються окремими фізичними та юридичними особами, а також державою, кіберзлочинці успішно продовжують свою діяльність у кіберпросторі. Як наслідок, зростає не лише масштаб, але й ціна даного виду злочинності.

Аналіз останніх досліджень і публікацій. Окремі питання кіберзлочинності неодноразово були предметом наукових досліджень як вітчизняних, так і зарубіжних учених. Зокрема, цій проблематиці присвячені праці О. Амеліна, Ю. Батуріна, В. Бутузова, В. Голубєва, О. Дзьобаня, В. Дзюндзюка, Р. Калюжного, М. Карчевського, М. Кравцової, В. Лісового, В.Навроцького, В. Номоконова, Д. Пашнєва, В. Пилипчука, М. Погорецького, В. Шеломенцева, О. Юрасова та інших.

Невирішені раніше проблеми. На даний момент залишається актуальним питання визначення поняття кіберзлочинності та узгодження його в рамках національного законодавства, а також шляхи захисту фізичних та юридичних осіб від даного виду злочинності.

Метою даної роботи є дослідження наукових праць та норм чинного законодавства для визначення поняття кіберзлочинності, її детермінантів та способів спеціального запобігання в сучасних умовах.

Виклад основного матеріалу. До визначення поняття "кіберпростору" існує значна кількість підходів, що породжує певні проблеми. Так, В. М. Фурашев у своїй праці наголошує на тому, що незважаючи на широке використання поняття "кіберпростір" як у науковій літературі, так і офіційних документах, існують обґрунтовані сумніви щодо можливості його використання у суто практичній площині. Значною мірою через це більшість держав світу продовжують протидію злочинним діям в кіберпросторі, послуговуючись "традиційним" законодавством (наприклад, щодо порушення телекомунікаційних мереж, отримання несанкціонованого доступу до інформації тощо). З огляду на вищезазначену термінологічну невпорядкованість щодо центрального поняття, ще більш складною постає проблема визначення похідних від нього понять, що активно використовуються в офіційних документах

провідних країн світу та безпекових організацій: “кібервійна”, “кібератака”, “кіберзахист”, “кібербезпека”, “кіберзброя”, “кібертероризм” тощо. Визначає його як форму співіснування сукупності матеріальних та нематеріальних об’єктів і процесів, спрямованих на породження, сприйняття, запам’ятовування, переробку та обмін інформацією [1, с. 164].

М. А. Погорецький розумів його як штучне електронне середовище існування інформаційних об’єктів у цифровій формі, утворене в результаті функціонування кібернетичних комп’ютерних систем управління та оброблення інформації й забезпечує користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних обчислювальних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів (надання інформаційних послуг, ведення електронної комерції тощо) [2, с. 80].

У свою чергу Вільям Гібсон пояснює кіберпростір як такий, в якому циркулюють електронні дані всіх комп'ютерів світу.

Законодавство України визначає: «Кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних»

У свою чергу вважаємо, що не слід забувати про безпосередній зв'язок кіберпростору, який деякі називають “віртуальним світом” із реальним. Попри усю абстрактність процесів, наслідки є досить реальними. Навіть якщо ми не можемо їх побачити, доторкнутися до них, ми їх відчуваємо і вони значною мірою впливають на наше життя. До матеріального у кіберпросторі можна віднести: телекомунікаційні мережі, засоби обчислювальної техніки, матеріальні носії та інше. Деякі фахівці відносять до матеріального простору також алгоритми і коди, як невід'ємну частину.

Із поняттям кіберзлочину подібних проблем не виникає. Закон України “Про основні засади забезпечення кібербезпеки України” наведено таке визначення: “кіберзлочин (комп’ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України”.

Кіберзлочинність законодавець визначив як сукупність кіберзлочинів. Під ним зазвичай розуміється вид злочинності у сфері комп’ютерної інформації і телекомунікацій, незаконний обіг радіоелектронних і спеціальних технічних засобів, поширення неліцензійного програмного забезпечення для ЕОМ, а також деякі інші види злочинності. Дане поняття хоч і коротке, проте влучне з кримінологічної точки зору. Деякі науковці часто плутають кіберзлочинність із кіберзлочином, визначаючи її як передбачене кримінальним законом суспільно небезпечне винне діяння (злочин) з особливою об'єктивною стороною.

Первинний вплив кіберзлочинності - це фінансовий стан, цілісність систем та інформація, що може включати в себе багато різних видів злочинної діяльності, пов'язаної з прибутком, включаючи атаки на вилучення зловмисних програм, шахрайство з електронною поштою та інтернет, а також спроби вкрасти фінансовий рахунок, кредитну картку чи іншу інформацію про платіжні картки. Кіберзлочинці можуть націлюватися на приватну особисту інформацію, а також на корпоративні дані чи комерційну таємницю для перепродажу чи особистого використання. Кримінологічну безпеку людини, суспільства, держави у кіберпросторі пропонується розглядати як об’єктивно-суб’єктивний стан захищеності їх життєво важливих прав та інтересів як у реальному, так і у віртуальному середовищі від зовнішніх та внутрішніх кримінальних посягань і загроз таких посягань, пов’язаних з використанням кібернетичних комп’ютерних систем. Даний стан забезпечує умови реалізації цих прав та інтересів людини, функціонування та розвиток суспільства і держави у кібернетичному просторі [3, с. 344].

До структурних елементів кібербезпеки В. М. Бутузов відносить: державну політику щодо

забезпечення кібербезпеки; державні й громадські інститути й організації, а також суб'єктів приватного сектору, що правомочні вживати заходів для забезпечення безпеки людини, суспільства й держави в кіберпросторі; засоби, способи й методи забезпечення кібербезпеки [4, с. 170].

Кіберзлочинність - це явище міжнародного значення, рівень якого знаходиться у прямій залежності від рівня розвитку та впровадження сучасних комп'ютерних технологій. Таким чином, стрімкий розвиток інформатизації в Україні дає можливість використовувати комп'ютерні технології з корисливих та інших мотивів, що певною мірою ставить під загрозу інформаційну безпеку держави [5, с. 102].

Конвенція Ради Європи "Про кіберзлочинність" визначає її як широкий спектр шкідливих дій, включаючи незаконні перехоплення даних, системні перешкоди, що посягають на цілісність та доступність мережі, а також порушення авторських прав. Інші форми кіберзлочину включають незаконні азартні ігри, продаж незаконних предметів, таких як зброя, наркотики або підроблені товари, а також заклик, виробництво, зберігання та розповсюдження дитячої порнографії.

Дана діяльність може здійснюватися окремими особами або невеликими групами з відносно невеликим технічним вмінням або високо організованими глобальними злочинними групами, до яких можуть входити кваліфіковані розробники та інші особи, які мають відповідний досвід. Для подальшого зменшення шансів виявлення та переслідування злочинці охочіше працюють в країнах із слабкими або відсутніми законами про кіберзлочинність, а також системами запобігання і відповідними відділами правоохоронних органів держави.

Кіберзлочинці постійно перебувають у пошуку нових методів і прийомів для досягнення своїх цілей, одночасно уникаючи виявлення та арешту.

Динаміка кіберзлочинності є позитивною на протязі багатьох років. Статистика таких злочинів велася з 1958 р. Тоді під ними малися на увазі: випадки псування і розкрадання комп'ютерного устаткування; крадіжка інформації; шахрайство чи крадіжка грошей, здійснені із застосуванням комп'ютерів; несанкціоноване використання комп'ютерів чи крадіжка машинного часу. Записи велися у Стенфордському дослідницькому інституті і тривалий час не становили великого інтересу [6, с. 114]. За звітами Департаменту кіберполіції щороку кількість виявлених кіберзлочинів збільшується в середньому на 2,5 тисяч. У 2017 році вони супроводжували близько 7 тис кримінальних проваджень, з них 4,5 тис — винятково кіберзлочини. За одинадцять місяців 2017 року було направлено до суду обвинувальні акти щодо 726 осіб .

За оперативними даними начальника департаменту кіберполіції Національної поліції Сергія Демедюка, добовий дохід шахраїв цього профілю перевищує 1 млн грн. Проте переважна більшість жертв не звертаються в поліцію, що свідчить про високу латентність даного виду злочину.

Якщо навести статистику по окремим видам злочину, то перше місце посідає кібершахрайство, коли злочинець намагається шляхом обману заволодіти інформацією про банківські картки. Злочинець використовує обман тільки в момент проникнення в банківську комп'ютерну мережу при подоланні її системи захисту. Методи при цьому можуть застосовуватися різні [5, с. 103]. Це також кардинг — крадіжка даних банківської карти й отримання доступу до інтернет-банкінгу жертви. На другому місці — протиправний контент. Мова йде про захист інтелектуальної власності і боротьбу з поширенням дитячої порнографії. На третьому місці — поширення шкідливого програмного забезпечення і створення майданчиків для продажу викраденої інформації

Проте, враховуючи специфічність кіберзлочинності, слід відповідно підходити і до її виміру. Так, відштовхуючись від складності ідентифікації особи злочинця, а отже і встановлення повторності і сукупності даного виду злочину, а також високу латентність, найкращим показником для виміру кіберзлочинності буде її ціна.

Згідно з даними щорічного дослідження проблем комп'ютерної злочинності, які проводяться Інститутом комп'ютерної безпеки США (Computer Security Institute), сукупний збиток злочинів у сфері використання комп'ютерних технологій за 5 років, з 1997 р. по

2001 р., становить вже більше ніж 1 млрд дол. США [5, с. 102].

Так, на даний момент, стан кібербезпеки в Україні відображається в світових рейтингах наступним чином: за національним індексом кібербезпеки (National Cyber Security Index) знаходиться на 26 місці; за індексом глобальної кібербезпеки (Global Cybersecurity Index) на 54 місці; за Індексом розвитку інформаційно-комунікаційних технологій (ICT Development Index) на 79 місці. Це говорить про те, що хоча, наша держава не пасе задніх у питаннях кібербезпеки, проте, є необхідність впокращенні показників з даного питання.

Дві третини людей в інтернеті - понад два мільярди людей — стали жертвами кіберзлочинців. Їх дані були викрадені або скомпрометовані. Одне опитування виявило, що 64% американців були жертвами шахрайських звинувачень або втрати особистої інформації.

Кіберзлочинці зазвичай прагнуть отримати фінансову вигоду. До цього висновку приходить більшість дослідників. Всупереч тому існує звіт Національного агентства з питань злочинності у Великій Британії (NCA) в результаті якого було виявлено, що більшість злочинців молодого і підліткового віку. Це пов'язано із специфікою об'єктивної сторони складу злочину і необхідними навиками і знаннями для його реалізації. У людей такого віку прослідковується найтісніший зв'язок з новітніми технологіями. Так от багато хто з них не обов'язково мотивується фінансовою винагородою. Фактично, мотиватором слугує визнання серед своїх однолітків, популярність на форумах, до яких вони належать, і відчуття успіху. Для них це найбільш впливові фактори. Як приклад, доповідь включає свідчення, дані 18-річним, який був заарештований за несанкціонований доступ до веб-сайту уряду США. Під час його арешту він сказав: "Я зробив це, щоб справити враження на людей в хакерській спільноті, щоб показати їм, що я маю необхідні навички, щоб зробити це ... Я хотів проявити себе".

Це людина, яка вважає себе розумнішою за інших, наркотичні речовини не вживає, має проблеми в спілкуванні з іншими людьми, слабкий стан здоров’я. Вона здатна приймати відповідальні рішення, любить працювати на самоті, може ночами сидіти за комп’ютером, опановує спеціальну літературу, непогано знає англійську мову [7, с. 75]

Також, до емоційних важелів, що підштовхують таких осіб є гнів, відчай та бажання помсти. Прикладами таких ситуацій може бути: колишнє подружжя, незадоволені або звільнені співробітники, незадоволені клієнти, ворожі сусіди, студенти що отримали погану відмітку. Так, статистика комп'ютерних злочинів у США за 27 років свідчить, що більшість (70%) злочинців - це працівники компаній, які мають доступ до їх комп'ютерів [8, с. 132].

Наступним важливим фактором є почуття безкарності у злочинців. Вони вважають що це не є злочином у традиційному розуміння того слова, а тому вважають що не будуть піддані покаранню за проведення кібератак.

Кіберзлочинцям характерні такі ознаки: наявність певних технічних знань, нехтування законом або впевненість у тому, що вони не можуть бути проти них застосовані, слабка соціальна спрямованість, бажання домінувати, обхитрити.

Значну увагу в даному питанні слід приділити самозахисту осіб (потенційних жертв кіберзлочину). Варто вміти розпізнавати кіберзлочинність. Це може бути першим кроком, який допоможе захистити необхідні дані. Важливими кроками є також прийняття деяких основних запобіжних заходів. Перш за все слід використовувати антивірусні програми та брандмауери. Ці програми спеціально розроблені для виявлення і ліквідації загроз. Це не є універсальним засобом. Воно не зможе захистити від будь якої атаки. Основними недоліками антивірусних програм є те, що вони захищають лише від конкретно визначених вірусів, що внесені у відповідну базу даних яка постійно оновлюється. Тому від новостворених чи видозмінених вірусів вона безсильна. Антивірусне програмне забезпечення та брандмауери - це дві різних програми безпеки, однак вони призначені для захисту комп'ютерної системи від атак. Брандмауер налаштований для мінімізації шкоди, заподіяної шпигунським програмним забезпеченням, шляхом блокування несанкціонованого доступу, а антивірус використовується для попередження, виявлення та видалення шкідливих програм, включаючи комп'ютерні віруси, шпигунські програми та рекламне ПЗ.

Не слід забувати про встановлення паролів. Вони мають бути складними і не варто їх повторювати. Їх важливо регулярно змінювати. Існують спеціальні програми для керування паролями.

Не варто викладати занадто багато особистої інформації в мережу. Кіберзлочинці можуть отримати вашу особисту інформацію лише за кількома точками даних, то чим менше ви ділитеся з тими, хто знаходиться за межами вашого кола, тим краще.

Програмне забезпечення необхідно постійно оновлювати до останньої версії. Це особливо важливо для операційної системи та програмного забезпечення для захисту інтернету. Кіберзлочинці часто використовують відомі підозри або дефекти у програмному забезпеченні для отримання доступу до системи. Виправлення цих помилок та недоліків може зробити менш ймовірним вчинення злочину.

При таємному листуванні, що може містити комерційну таємницю чи переправленні важливих даних є можливість використовувати пароль шифрування, а також віртуальну приватну мережу (VPN). VPN буде шифрувати весь трафік, покидаючи ваші пристрої, доки він не прибуде до місця призначення. Якщо кіберзлочинці встигають зламати вашу лінію зв'язку, вони не будуть перехоплювати щось, крім зашифрованих даних. Та з цим теж слід бути обережним і використовувати лише надійні перевірені сервіси. Власнику сервера, через який здійснюється перенаправлення і шифрування нічого не вартує отримати відкритий доступ до тої інформації, яка до нього надходить.

Не варто забувати про резервне копіювання важливих даних. Це допоможе моментально відновити втрачену чи викрадену інформацію і мінімізує витрати фінансових та інших ресурсів. Певні дані можуть бути життєво необхідні як для компанії, так і для фізичної особи. Їх крадіжка та втрата через недбалість чи апаратний збій можуть призвести до непоправних збитків, якщо інформацію важко відновити. Зберігати таку копію краще всього на повністю окремій системі. Для більш надійного захисту існує правило: 3-2-1. Воно передбачає створення 3 копій даних (1 основна та 2 резервні копії),
зберігайте дані щонайменше на 2 типах носіїв даних (локальний диск, NAS, касету тощо), зберігайте 1 з них на захищеному сховищі чи хмарі. При застосуванні цього правила навіть при атаці жодні дані не будуть втрачені.

Серед проблем, що заважають створенню ефективно діючої системи протидії загрозам у кіберпросторі, дослідники виділяють термінологічну невизначеність. Відмічається, що першочерговим завданням є створення за участю зацікавлених відомств базового документу із визначеннями основних понять у кібербезпековій сфері — “кіберпростір”, “кібербезпека”, “кібератака”, “кібернапад”, “кіберзахист”, “кібертероризм”, “кіберзлочин”. Слід погодитись з думкою дослідників про доцільність закласти ключові терміни кібербезпекової сфери (а заразом і сфери інформаційної безпеки в цілому) в нову редакцію Закону України “Про інформацію” [3, с. 343].

Висновки. Криміногенна ситуація в Україні залишається складною, і питання посилення боротьби зі злочинністю і її превентивний характер мають знаходитись у центрі уваги правоохоронних органів [9, с. 73]. За даними Федерального бюро розслідувань (США) збитки від одного злочину, який вчиняється у кіберпросторі за допомогою комп’ютера, становлять у середньому 500 тис. дол., тобто в 20 разів більше, ніж при використанні інших злочинних методів. Загальна сума збитків від «електронного грабежу» щорічно становить близько 600 млн. дол. Однак і ця значна цифра, на думку спеціалістів, значно занижена, так як більшість електронних злочинів залишаються нерозкритими. Експерти постійно наголошують, що число кіберзлочинів буде постійно зростати, а суми збитків збільшуватимуться, оскільки методи злочинців постійно вдосконалюються [10, с. 9; 11].

Зростаюча небезпека від злочинів, скоєних проти комп'ютерів, або проти інформації на комп'ютерах, починає вимагати уваги. Однак у більшості країн прослідковується недосконаліть правової бази та системи захисту від таких злочинів. Цей недолік правової охорони означає, що підприємства та уряди повинні спиратися винятково на технічні заходи, щоб захистити себе.

З вираженими ризиками, що походить із кіберзлочинністю, легко відчувати себе під тиском з усіх сторін, особливо якщо ви не знаєте,

як захистити себе від загрози, яку ви не можете бачити.

Більшість інцидентів, пов'язаних із кіберзлочинністю, не повідомляється, і лише деякі компанії висувають інформацію про свої втрати. Це не дивно, якщо враховувати ризик репутації організації та перспективи судового розгляду проти тих, хто має право на кіберзлочинність. Кілька найбільших кіберзлочинців були спіймані - багато ще не визначено.

Значна частина кіберзлочинів залишається непоміченою, особливо промисловий шпіонаж, де важко визначити доступ до конфіденційних документів та даних. Існує небезпека того, що бізнес може торгувати невигідно протягом місяців чи навіть років у результаті тривалого, але невиявленого порушення безпеки.

Кібербезпека є складним предметом, розуміння якого потребує знань з багатьох дисциплін, включаючи комп'ютерні науки та інформаційні технології, психологію, економіку, організацію поведінки, політологію, інженерію, соціологію, наукові дослідження, міжнародні відносини та право. На практиці, хоча технічні засоби протидії є важливим елементом, кібербезпека не є лише технічним питанням.

Кібернетична безпека - одне з найбільш актуальних питань сьогодення. Комп'ютерні мережі завжди були об'єктом злочинців, і, ймовірно, небезпека порушень кібербезпеки буде тільки збільшуватися в майбутньому, оскільки ці мережі розширюються, але існують запобіжні заходи, які організації можуть вживати, щоб звести до мінімуму втрати від тих, хто прагне заробити таким шляхом. Проте, проблема кібербезпеки ніколи не буде вирішена раз і назавжди. Ми можемо лише мінімізувати її наслідки. За необхідного рівня підготовки та зовнішньої допомоги спеціаліста, можна зменшити збитки, відновитись від кіберзлочину та його наслідків.

Список використаних джерел:

1. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності / В. М. Фурашев // Інформація і право. – 2012. – № 2. – С. 162-169.
2. Погорецький М. А. Поняття кіберпростору як середовища вчення злочину / М. А. Погорецький, В. П. Шеломенцев // Інформаційна безпека людини, суспільства, держави : наук.-практ. журнал. — К. : НАСБУ. — 2009. — № 2 (2). — С. 77–81.
3. Шеломенцев В. П. Кримінологічна безпека у кіберпросторі: система понять / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2010. – № 23. – С. 342–348.
4. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно – структурний аналіз) : монографія / В. М. Бутузов; Рада нац. безпеки і оборони України, Міжвід. наук.-дослід. центр з проблем боротьби з організованою злочинністю. – К. : КИТ, 2010. – 408 с.
5. Голубєв В. Кримінологічна характеристика злочинів у сфері використання комп’ютерних технологій / В. Голубєв // Підприємництво, господарство і право. – 2002. – № 1. – С. 101–106.
6. Гуцалюк М. Протидія комп’ютерній злочинності / М. Гуцалюк // Право України. – 2003. – № 6. – С. 114–117.
7. Загіка Г. В. Кримінологічна характеристика особистості комп’ютерного злочинця / Г. В. Загіка // Вісн. Одес. ін – ту внутр. справ. – 2001. – № 1. – С. 73–78.
8. Комп’ютерна злочинність : навч. посібник / П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. – К. : Атіка, 2002. – 240 с.
9. Сметаніна Н. В. Наукові підходи до теорії злочинності у сучасній українській кримінології : моногр. / Н. В. Сметаніна; за заг. ред. В. В. Голіни. – Х. : Право, 2016. – 192 с.
10. Ищенко Е. П. Виртуальный криминал / Е. П. Ищенко. – М. : Проспект, 2011. – 232 с.

11. Сметаніна Н. В. Національний і міжнародний досвід визначення та розрахунку ціни кіберзлочинності / Н. В. Сметаніна // Міжнародні стандарти з кібербезпеки та їх застосування в Україні : матеріали «круглого столу» (м. Харків, 19 квіт. 2016 р.). – Харків, 2016. – С. 59–61.

References:

1. V. M. Furashev, Kiberprostir ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti / V. M. Furashev // Informatsiia i pravo. – 2012. – No. 2. – Pp. 162-169.

2. M. A. Pohoretskyi, Poniattia kiberprostoru yak seredovyshcha vchennia zlochynu / M. A. Pohoretskyi, V. P. Shelomentsev // Informatsiina bezpeka liudyny, suspilstva, derzhavy : nauk.-prakt. zhurnal. — K. : NASBU. — 2009. — No. 2 (2). — Pp. 77–81.

3. V. P. Shelomentsev, Kryminolohichna bezpeka u kiberprostori: systema poniat / V. P. Shelomentsev // Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka). – 2010. – No. 23. – Pp. 342–348.

4. V. M. Butuzov, Protydiia kompiuternii zlochynnosti v Ukraini (systemno – strukturnyi analiz) : monohrafiia / V. M. Butuzov; Rada nats. bezpeky i oborony Ukrainy, Mizhvid. nauk.-doslid. tsentr z problem borotby z orhanizovanoiu zlochynnistiu. – K. : KYT, 2010. – 408 p.

5. V. Holubiev, Kryminolohichna kharakterystyka zlochyniv u sferi vykorystannia komp'iuternykh tekhnolohii / V. Holubiev // Pidpryiemnytstvo, hospodarstvo i pravo. – 2002. – No. 1. – Pp. 101–106.

6. M. Hutsaliuk, Protydiia komp'iuternii zlochynnosti / M. Hutsaliuk // Pravo Ukrainy. – 2003. – No. 6. – Pp. 114–117.

7. H. V. Zahika, Kryminolohichna kharakterystyka osobystosti komp'iuternoho zlochyntsia / H. V. Zahika // Visn. Odes. in – tu vnutr. sprav. – 2001. – No. 1. – Pp. 73–78.

8. Komp'iuterna zlochynnist : navch. posibnyk / P. D. Bilenchuk, B. V. Romaniuk, V. S. Tsymbaliuk ta in. – K. : Atika, 2002. – 240 p.

9. N. V. Smetanina, Naukovi pidkhody do teorii zlochynnosti u suchasnii ukrainskii kryminolohii : monohr. / N. V. Smetanina; za zah. red. V. V. Holiny. – Kh. : Pravo, 2016. – 192 p.

10. E. P. Yshchenko, Vyrtualniy krymynal / E. P. Yshchenko. – M. : Prospekt, 2011. – 232 p.

11. N. V. Smetanina, Natsionalnyi i mizhnarodnyi dosvid vyznachennia ta rozrakhunku tsiny kiberzlochynnosti / N. V. Smetanina // Mizhnarodni standarty z kiberbezpeky ta yikh zastosuvannia v Ukraini : materialy "kruhloho stolu" (m. Kharkiv, 19 kvit. 2016 r.). – Kharkiv, 2016. – Pp. 59–61.