

ЛІТЕРАТУРА

1. Статистична звітність форми № 1 (річна) «Єдиний звіт про злочинність» // Офіційний веб-сайт Міністерства внутрішніх справ України [Електронний ресурс]. – Режим доступу: <http://www.mvs.gov.ua/mvs/control>
2. Кримінальне право (Особлива частина): підручник / за ред. О.О. Дудорова, Є.О. Письменського. Т.2 – Луганськ : вид. «Ельтон-2», 2012. – 704 с.
3. Задоя К.П. Кримінальна відповідальність за перевищення влади або службових повноважень (ст. 365 КК України): Дис... канд. юрид. наук. – К., 2009. – 231 с.
4. Вирок Козелецького районного суду Чернігівської області від 10 жовтня 2012 р. у справі № 2508/24/2012 [Електронний ресурс] // Єдиний державний реєстр судових рішень : [веб-сайт]. – Режим доступу: <http://www.reyestr.court.gov.ua/Review/27065779>

УДК 343.2:343.4 (477)

ФАКТОРИ ДЕТЕРМІНАЦІЇ КІБЕРЗЛОЧИННОСТІ В СУЧАСНІЙ КРИМІНОЛОГІЧНІЙ ТЕОРІЇ

Кравцова М.О.,

ад'юнкту ад'юнктури та докторантури

Харківський національний університет внутрішніх справ

У статті проведено огляд наукових підходів до факторів кіберзлочинності та їх взаємодії. Встановлено, що чітко не визначено основні поняття щодо кіберзлочинності, її детермінації, а також не встановлено на законодавчому та теоретичному рівні заходів, що сприяють попередженню та запобіганню кіберзлочинності в Україні. На підставі проведеного аналізу визначено, що особливості детермінації кіберзлочинності обумовлені роллю кіберпростору, середовищем кіберпростору та його взаємозв'язком з факторами соціального середовища.

Ключові слова: кіберзлочинність, фактори, детермінація, кіберзлочин, кіберзлочинець.

Кравцова М.А. / ФАКТОРЫ ДЕТЕРМИНАЦИИ КИБЕРПРЕСТУПНОСТИ В СОВРЕМЕННОЙ КРИМИНОЛОГИЧЕСКОЙ ТЕОРИИ / Харьковский национальный университет внутренних дел, Украина

В статье изложен обзор научных подходов к факторам киберпреступности и их взаимодействию. Установлено, что законодательством четко не определены основные понятия относительно киберпреступности, ее детерминации, а также не установлено на законодательном и государственном уровне мероприятий, способствующих предупреждению и прогнозированию киберпреступности в Украине. На основании проведенного анализа определено, что особенности детерминации киберпреступности обусловлены ролью киберпространства, средой киберпространства и его взаимосвязью с факторами социальной среды.

Ключевые слова: киберпреступность, киберпреступление, киберпреступник, детерминация, факторы.

Kravtsova M.A. / FACTORS DETERMINATION CYBERCRIME IN MODERN CRIMINOLOGICAL THEORY / Kharkiv National University of Internal Affairs, Ukraine

The problem of the causes of crime in criminology is the key, as it defines the scientific content of criminological theory and its practical orientation. Detection and study of the causes and conditions of certain types of crimes and crime in general can reveal the essence of the phenomenon, explain the laws of its origin, to identify trends in the structure and level of crime, respectively, define a strategy and develop effective preventive measures.

The article describes an overview of the scientific approach to cybercrime factors and their interactions. Found that the legislation is not clearly defined the basic concepts regarding cybercrime, its determination, and is not installed on the legislative and state level activities to promote the prevention and prediction of cybercrime Ukraine.

Thus, intensive computerization and globalization of the world in the absence of effective mechanisms for economic, political and legal regulation (at both the individual states, and international level) of these processes leads to the criminalization of a large part of their constituents. Thus, the lower level of economic development, political and legal support of information security, the higher the level of cyber crime and cyber threats in general.

The conclusion is that the characteristics of determination due to cybercrime role of cyberspace as a medium formation offender, a set of circumstances that exist independently of the person who committed the crime (the crime environment that defines environment having done so) and its relationship with the relevant factors of the real space (social environment).

Key words: cyber crime, cyber-crime, cyber criminals, determination, factors.

Проблема причин злочинності у кримінології є ключовою, оскільки визначає науковий зміст кримінологічної теорії та її практичну спрямованість. Виявлення та дослідження причин та умов окремих видів злочинів та злочинності в цілому дозволяє розкрити суть даного явища, пояснити закономірності його походження, виявити тенденції змін у структурі та рівні злочинності, відповідно, визначити стратегію та розробити ефективні запобіжні заходи.

Фактори детермінації кіберзлочинності досліджувалися в рамках різних правових наук такими вченими як Т. Л. Тропина, А. Н. Косенков, А. О. Петренко-Лисак, П. Д. Біленчук та іншими, але в цих дослідженнях можна побачити різні підходи і погляди на досліджувану тематику, що звичайно є позитивним моментом для розвитку науки, але не зовсім зрозумілим для здійснення практичної діяльності.

Метою статті є вивчення та узагальнення поглядів щодо факторів детермінації кіберзлочинності та систематизований їх виклад у прив'язці до потреб прикладного кримінологічного аналізу.

Будь-які явища, якщо їх розглядати з позиції причин та умов злочинності, повинні відповідати низці критеріїв. Що стосується безпосередньо кіберзлочинності, то при вивченні об'єктивних і суб'єктивних причин і умов вчинення злочинів даного виду, необхідно враховувати специфіку їх взаємодії, яка визначає особливості формування мотивів і цілей вчинення злочину. Як справедливо указують фахівці, складність полягає в тому, що мотивація кіберзлочинців формується відразу в двох просторах: реальному і кіберпросторі [1].

Саме дослідження ролі кіберпростору як середовища формування особистості злочинця, а також як сукупності

обставин, що існують незалежно від особи, яка вчинила злочин (середовища вчинення злочину, яке визначає обстановку його вчинення), у взаємозв'язку з відповідними факторами реального простору (соціального середовища) є основою пізнання особливостей детермінації кіберзлочинності і, відповідно, успішної протидії їй.

З урахуванням численності різних видів детермінаційної взаємодії (від лат. *determinare* – зумовлювати існування, розвиток іншого явища [2, с. 14]) для позначення усіх явищ та процесів, що відіграють будь-яку роль у детермінації злочинності, доцільно вживати термін – фактори детермінації (фактори, детермінанти).

Враховуючи певну умовність поділу окремих факторів детермінації на певні групи, обумовлену складністю їх взаємодії та комплексністю впливу на протиправну поведінку, спробуємо визначити та проаналізувати основні фактори детермінації кіберзлочинності.

Політико-правові фактори. З точки зору політичних процесів і політичних чинників поява кіберзлочинності та її зростання обумовлені відсутністю адміністративно-територіальних й інших меж в глобальних інформаційних мережах, неузгодженістю позицій урядів різних держав з питань вільного розповсюдження інформації і дотримання прав і інтересів особи. Також процес досягнення політичної згоди в питаннях, що стосуються кіберзлочинності ускладнюється різними уявленнями держав про те, які дії є кіберзлочинами і потребують кримінально-правової заборони, у тому числі і уявленнями про морально-етичну сторону діянь [3, с. 253].

Необхідною умовою розвитку інформаційного суспільства є забезпечення належного рівня кібернетичної безпеки. Кібернетична безпека країни забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих з установленим порядком доктрин, концепцій, стратегій і програм.

Саме у Стратегії кібернетичної безпеки України доцільно передбачити основні напрями державної політики з питань кібернетичної безпеки України, а саме: забезпечення суверенітету України у кіберпросторі, наповнення кіберпростору достовірною інформацією про Україну; створення сприятливих зовнішньополітичних умов для прогресивного розвитку національного сегменту кіберпростору; запобігання втручанням у внутрішні справи України і відвернення посягань на її Інтернет-ресурси з боку інших держав; забезпечення повноправної участі України в загальноєвропейській та регіональних системах кібернетичної безпеки; участь України в міжнародному співробітництві у сфері боротьби з кіберзлочинністю та кібертероризмом; зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби у кіберпросторі з проявами організованої злочинності та кібертероризму; боротьба з організованими злочинними угрупованнями, в тому числі міжнародними, які намагаються діяти у національному сегменті кіберпростору; забезпечення максимальної ефективності Збройних Сил України у кіберпросторі та їх здатності давати адекватну відповідь реальним і потенційним кібернетичним загрозам Україні; запобігання проявам екстремізму в національному сегменті кіберпростору; посилення державної підтримки розвитку пріоритетних напрямів науки і техніки як основи створення високих інформаційних технологій; забезпечення необхідних умов для реалізації прав інтелектуальної власності у національному сегменті кіберпростору; створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури і ресурсів. Ідеї Стратегії кібернетичної безпеки України повинні отримати розвиток у положеннях базового закону в цій сфері, а також змін і доповненнях до інших законів України, що регулюють відносини у сфері кібернетичної безпеки [4, с. 314–315].

Відсутність належного кримінально-правового регулювання в результаті недосягнення згоди на міжнародному рівні є найважливішим чинником розвитку і зростання кіберзлочинності. Оскільки електронні посягання є проблемою трансграничною за своєю природою, правові основи боротьби з цим явищем повинні розроблятися на міждержавному рівні. Тим часом наразі законодавство різних країн світу є суперечливим: відсутній одноманітний понятійний апарат, зокрема у визначенні кіберзлочинів, не закріплено на міжнародному рівні, які діяння повинні переслідуватися відповідно до кримінального законодавства [3, с. 112–113].

Так, недоліки понятійного апарата у сфері забезпечення кібернетичної безпеки не дозволяють: визначити ознаки та об'єктивно оцінити основні загрози у національному сегменті кіберпростору; визначити найбільш ефективні заходи забезпечення кібернетичної безпеки; чітко сформулювати завдання та функції суб'єктів кібернетичної безпеки тощо. У законодавстві відсутнє визначення не тільки поняття «кібернетична безпека (кібербезпека)», але й таких ключових понять як «кібернетичний простір (кіберпростір)», «кібернетична загроза (кіберзагроза)», «кібернетична атака (кібератака)», «кібернетичний захист (кіберзахист)», «кібернетичний злочин (кіберзлочин)», «кіберзлочинність» тощо. Визначення зазначених термінів передбачає їх широке розуміння, враховуючи вже наявні напрацювання у таких галузях науки як кібернетика, інформатика, безпекознавство, кримінальне право тощо [4, с. 313].

Щодо вад національного законодавства, то поширенню кіберзлочинності та ускладненню запобігання їй сприяють проблеми правового забезпечення системи кібернетичної безпеки України, обумовлені, перш за все, відсутністю чітко розробленого та нормативно закріпленого понятійного апарата у сфері кібернетичної безпеки.

Отже, відсутність належного теоретико-правового забезпечення у зазначеній сфері суттєво ускладнює застосування відповідних кримінально-правових норм, нерідко призводить до прийняття суперечливих рішень у слідчій та судовій практиці [5, с. 8].

Економічні фактори. Світове суспільство сьогодні перейшло до інформаційної фази розвитку, в якій процеси інформатизації все активніше проникають до всіх областей діяльності людини, стають дійовим елементом економіки [6, с. 3]. Економічні фактори детермінації кіберзлочинності пов'язані, перш за все, з процесом глобалізації світової економіки та глобалізації в цілому.

Сьогодні глобального масштабу набуває інтелектуалізація техносфери планети. Модернізація сучасного соціуму шляхом впровадження до життя продуктів комп'ютерної техніки та технологій (КТТ) несе за собою цілу низку новоутворень в соціальному бутті. КТТ є носіями, що втілюють кібервіртуальність, яку ми розуміємо як електронно-технічний тип віртуальності, що являє собою результат технічної творчості соціальних суб'єктів з використанням КТТ та ІКТ (інформаційно-комунікативних технологій). Мобільні пристрої, ПК (персональний комп'ютер) та кібервіртуальність стали не тільки невід'ємними атрибутами, символами сучасності, але й чинниками змін.

Саме з цими процесами пов'язана певна група економічних факторів детермінації кіберзлочинності. Як зазначає Т. Л. Тропіна, група чинників детермінації кіберзлочинності визначається економічним розвитком і впровадженням високих технологій в повсякденне життя країн «золотого мільярда». Доступ все більшої кількості користувачів до глобальних інформаційних мереж, розвиток електронної торгівлі, можливість відкриття банківських рахунків через Інтернет і поява можливості здійснення інших операцій, що не вимагають, як раніше, безпосереднього контакту з контрагентом, обумовлюють

зростання шахрайств в сфері он-лайн торгівлі і операцій з кредитними картами, крадіжок персональних даних, паролів і доступу. Використання високих технологій на підприємствах приводить до зростання промислового шпигунства. При цьому економічна стабільність і стійке матеріальне положення користувачів в розвинених країнах є чинником легковажного відношення до власної інформаційної безпеки [3, с. 113].

Слід враховувати, що процес глобалізації має й зворотну негативну сторону, що також має пряме відношення до детермінації кіберзлочинності. Ця зворотна сторона полягає в тому, що при збагаченні одних завжди біднішають інші. А це, як відомо, є потужним криміногенним фактором, насамперед щодо середовища останніх.

Зростає відставання економічного рівня життя країн, що розвиваються, від країн «золотого мільярда», фінансові кризи, які є каталізатором негативних процесів, та інші пов'язані з цим негативні явища є також чинниками детермінації кіберзлочинності. З огляду на ці чинники, зростання кіберзлочинності є одним з наслідків загальної криміналізації економічної діяльності в країнах з економікою, що розвивається. Це стосується країн Латинської Америки, держав колишнього СРСР. Багато людей і господарюючі суб'єкти шукають нові шляхи ведення бізнесу або просто кошти для існування, у тому числі і кримінальні. Безробіття, що зростає, незатребуваність наукових і інженерних кадрів, обумовлюють відтік інтелектуальних ресурсів з легального сектора економіки в кримінальний [3, с. 113].

Таким чином, інтенсивна інформатизація і глобалізація світу при відсутності ефективних механізмів економічного, політичного та правового регулювання (як на рівні окремих держав, так й на міжнародному рівні) цих процесів призводить до криміналізації значної частини їх складових. При цьому, чим нижче рівень економічного розвитку країни, політичного та правового забезпечення її інформаційної безпеки, тим вище рівень кіберзлочинності й кіберзагроз в цілому.

Організаційно-управлінські фактори. Дана група факторів пов'язана, перш за все, з недоліками соціального контролю, які, як зазначає Т. Л. Тропіна, виражаються в ігноруванні керівниками підприємств і простими користувачами вимог інформаційної безпеки, недоліках її фінансування. Крім того, через різні причини потерпілі від кіберзлочинів не повідомляють про ці інциденти в правоохоронні органи, що полегшує вчинення злочинів і обумовлює їх безкарність, і, як наслідок, веде до зростання кількості вчинюваних діянь. Також до недоліків соціального контролю можна віднести низьку підготовленість правоохоронних органів до боротьби з кіберзлочинністю, відсутність кваліфікованих кадрів, неналежне технічне оснащення, що в сукупності з труднощами розкриття кіберзлочинів значно утрудняє процес збору доказів і затримання злочинця [3, с. 113].

Як зазначає П. Д. Біленчук, з розвитком глобальних комп'ютерних мереж набула поширення практика промислового шпигунства. Саме тому проблеми розробки систем захисту та збереження державної, службової та комерційної таємниці набувають сьогодні особливого значення. Чимало проблем виникає у зв'язку з крадіжками послуг, що надають Інтернет-провайдери, зокрема, вторгнення до телефонних мереж та незаконна торгівля послугами зв'язку. Також Інтернет широко використовується торгівцями піратським програмним забезпеченням, порнографією, зброєю та наркотиками, для ведення справ, обміну інформацією, координації дій [7, с. 3].

Серед організаційно-управлінських факторів детермінації кіберзлочинності значна роль належить практично повній відсутності організації дозвілля населення в країні, в першу чергу молоді.

Слід зазначити, що різного роду організаційно-управлінські прорахунки з боку держави призводять не лише

до вчинення кіберзлочинів, але й грають роль в існуванні кіберзлочинності, обумовлюючи можливість її самодетермінації.

Ідеологічні фактори. Відомо, що рівень злочинності в суспільстві напряму залежить від рівня його культури. Вчинення кіберзлочинів, як і злочинів інших видів пов'язане з негативними наслідками зниження загального рівня культури та моральних критеріїв у нашому суспільстві.

Кіберкультура, будучи самостійним соціальним утворенням, інституціонально оформленим і самовідтворюючим цінності і повсякденні ідеології, вступає в конкуренцію з інститутами суспільства у процесах соціалізації та інтеграції. Її учасникам доводиться соціалізуватися одночасно у двох вимірах: соціальній спільності кіберпростору та у мережному соціумі, де вони взаємодіють відповідно до його власних правил гри. Крім освоєння норм і цінностей кіберкультури, користувачу мережі Інтернет доводиться корегувати свою «поведінку» під впливом еволюційних змін як у соціумі реальному, так і віртуальному, де він раніше проходив відповідні етапи соціалізації. Можна припустити, що в рамках кіберкультури, з огляду на її більш рухливу структуру елементів, ресоціалізація має більш високі темпи, ніж у межах домінуючої культури. Очевидно і те, що процес соціалізації в кіберпросторі триває безупинно [8, с. 15].

Як вказують фахівці, кіберпростір інакше впливає на мотивацію злочинної поведінки через наступні причини: 1) цей простір є позатериторіальним і заснований на інших консолідуючих чинниках; 2) у кіберпросторі відбувається не тільки взаємодія, взаємопроникнення і змішування національних культур, але і формування свого власного культурного середовища – кіберкультури.

Разом з тим, в кіберпросторі, як фактично у паралельній реальному миру соціальної системи, ті ж процеси, що і в культурній сфері, відбуваються і з соціальними нормами. Можна припустити, що, оскільки кіберпростір відіграє чималу роль в житті молоді, то в свідомості молодих активних користувачів Інтернету відбувається заміщення соціальних норм нормами кіберпростору, так само можуть нівелюватися соціальні норми реального життя, що непридатні в Усесвітній мережі [1, с. 91].

Враховуючи те, що особа кіберзлочинця і мотивація його протиправної діяльності формується відразу в двох просторах: реальному і кіберпросторі, особливого значення набуває той факт, що з реальності кіберзлочинець приносить з собою у кіберпростір установку на вседозволеність. Остання в значній мірі в сучасному суспільстві обумовлюється пануванням культури споживання. Все це приводить до того, що кіберзлочинець реалізує відповідну модель поведінки «господаря життя», або ж банально використовує кіберпростір для досягнення «прозаїчних» реальних життєвих цілей – наживи і збагачення.

Роль даного чинника в детермінації кіберзлочинності полягає в тому, що відбувається формування серед покоління нинішньої молоді певного прошарку індивідуалістів з підвищеними запитами, що живуть тільки сьогоднішнім днем і вважають можливим задоволення потреб будь-якими засобами. Ця молодь орієнтована на швидке досягнення успіху, має певну схильність до ризику, ділову хватку. При цьому низький рівень виявлення та розкриття кіберзлочинів приводить до появи міфу про безкарність подібних діянь, що в сукупності з можливістю вчинення подібних злочинів без ризику для життя створює додаткові передумови залучення до вчинення кіберзлочинів усе нових і нових осіб. Цьому також сприяє популяризація і романтизація образу кіберзлочинців як дуже грамотних людей або якихось Робін Гудів, що борються із «світовим злом» – розвиненими державами і транснаціональними корпораціями [3].

Соціально-психологічні фактори. Як відомо, людина – істота соціальна, тому велике значення для встановлення

детермінаційного комплексу її злочинної поведінки мають криміногенні фактори саме соціального порядку. В свою чергу специфіка середовища вчинення кіберзлочинів обумовлює особливості формування та проявів психології злочинця.

Як слушно вказують у своєму дослідженні Г. О. Чорний та О. М. Косенков, чималу роль в детермінації кіберзлочинності грає такий специфічний психологічний чинник як «ефект он-лайн дезінгібіції» (за термінологією Джона Шулера (John Suler) – ефект, який кіберпростір справляє на людину, роблячи можливим діяти вільніше, ніж в реальному соціумі). Основу цього ефекту складають:

- дисасоціативна анонімність («ти мене не знаєш»), суть якої полягає в тому, що в умовах анонімності люди можуть відокремити свої дії в кіберпросторі від реального світу і реальної особи, у такому разі людина вважає, що може не брати на себе відповідальність за свої дії;

- невидимість («ти мене не бачиш») – дозволяє уникати необхідності встановлення психологічного контакту;

- асинхронність («побачимося пізніше») – можливість спілкуватися в окремих випадках без необхідності негайної реакції на слова або дії співбесідника, що є важливим дезінгібуючим чинником;

- соліптична інтродекція («це все в моїй голові») – вірогідність того, що при он-лайн спілкуванні може виникнути відчуття, що все відбувається виключно в нашій власній уяві;

- мінімізація влади («ми рівні») – виникає через опосередковане сприйняття атрибутів вищого соціального положення, а також можливості їх ігнорувати. Проте, необхідно враховувати, що в кіберсоціумі можна говорити про існування якісно іншої, але все-таки ієрархії [1, с. 90–91].

В умовах кіберпростору істотно змінюється психологічний зміст взаємозв'язків злочинець – предмет злочину, а також злочинець – потерпілий, які з прямих перетворюються на опосередковані: злочинець – електронний пристрій (Мережа) – потерпілий (предмет

злочину), що веде до усунення матеріальної складової як дій людини, так і соціальної взаємодії. При цьому «віртуальні» предмети психологічно здаються доступнішими, зокрема для незаконного заволодіння ними. Будь-які ж дії в таких умовах сприймаються спочатку як нематеріальні за природою, відповідно, що не заподіюють матеріальних, серйозних наслідків. Інформаційно-комунікаційні технології істотно обмежують зворотний зв'язок, будь-яке відчуття зворотного зв'язку наших дій. Тому відсутній вплив усвідомлення того, що ми заподіяли шкоду, але також ми вважаємо, що наша поведінка не може заподіяти ніякої шкоди, тому що ми не бачимо шкоди [1, с. 88].

Специфічне середовище вчинення кіберзлочинів обумовлює також специфіку взаємозв'язків на рівні кіберзлочинець – жертва злочину.

Дистанційованість і «віртуалізація» шкоди, що заподіюється діями, що реалізуються в кіберпросторі, обумовлює його специфічне уявлення жертвою злочину. З одного боку, жертва злочину, яка виявляє заподіяну їй «нематеріалізовану» шкоду, не в повній мірі усвідомлює її характер і масштаби, відповідно, характер і ступінь суспільної небезпеки вчиненого відносно неї діяння. З іншого боку, жертва злочину часто нездатна в своїй свідомості адекватно сприйняти зв'язок заподіяної шкоди з конкретним (хай неперсоніфікованим) злочинцем. Отже, вчинений відносно неї злочин і заподіяна ним шкода, жертвою часто сприймається як абстрактне «зло», що не має перспективи бути виправленим.

Викладене вище дозволяє стверджувати, що особливості детермінації кіберзлочинності обумовлені роллю кіберпростору як середовища формування особистості злочинця, сукупністю обставин, що існують незалежно від особи, яка вчинила злочин (середовища вчинення злочину, яке визначає обстановку його вчинення), та його взаємозв'язком з відповідними факторами реального простору (соціального середовища).

ЛІТЕРАТУРА

1. Косенков А. Н. Общая характеристика психологии киберпреступника / А. Н. Косенков, Г. А. Черный // Криминологический журнал Байкальского государственного университета экономики и права. – 2012. – № 3. – С. 87–94.
2. Горб Н. О. Наруга над могилою : кримінально-правовий та криминологічний аналіз : автореф. дис. ... канд. юрид. наук за спец. : 12.00.08 «кримінальне право та криминологія ; кримінально-виконавче право» / Н. О. Горб. – К., 2005. – 17 с.
3. Тропина Т. Л. Киберпреступность : понятие, состояние, уголовно-правовые меры борьбы : дисс. ... канд. юрид. наук : 12.00.08 / Т. Л. Тропина. – Владивосток, 2005. – 253 с.
4. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 1 (27). – С. 312–320.
5. Музыка А. А. Законодавство України про кримінальну відповідальність за «комп'ютерні» злочини : науково-практичний коментар і шляхи вдосконалення / А. А. Музыка, Д. С. Азаров. – К. : Паливода А. В. [вид.], 2005. – 119 с.
6. Інформаційне суспільство. Дефініції : людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція / В. М. Брижко, О. М. Гальченко, В. С. Цимбалюк, О. А. Орехов, А. М. Чорнобров / За ред. Р. А. Калужного, М. Я. Швеца. – К. : Интеграл, 2002 р. – 220 с.
7. Біленчук П. Д. Портрет комп'ютерного злочинця / П. Д. Біленчук. – К. : В&В, 1997. – 48 с.
8. Прохоренко Є. Я. Феномен кіберкультури в інформаційно-технологічному відтворенні соціуму : автореф. ... канд. соц. наук за спец. : 22.00.04 «спеціальні та галузеві соціології» / Є. Я. Прохоренко. – Харків, 2008. – 23 с.
9. Кесарева Т. П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет : автореф. дис. на соискание уч. степени канд. юрид. наук : спец. 12.00.08 «уголовное право и криминологія ; уголовно-исполнительное право» / Т. П. Кесарева. – Москва, 2002. – 25 с.